A Composite Chain Structure Blockchain Storage Method Based on Blockchain Technology

Junlu Wang[1(✉)], Su Li[1], and Wenyuan Ma[2]

[1] School of Information, Liaoning University, Shenyang 110036, China
wangjunlu@lnu.edu.cn
[2] School of International Education,
Beijing University of Chemical Technology, Beijing 100029, China

Abstract. Blockchain is an effective means to store data securely. Existing blockchain systems mostly adopt the equal mining mode, and all bookkeepers (entities) record ledger books on a single main chain, resulting in random data storage in the whole blockchain. Moreover, in complex or classification scenarios, data in a single main chain cannot be correlated or regularly stored, resulting in low storage efficiency. To solve these problems, this paper proposes a composite chain structure blockchain storage method based on blockchain technology. This method firstly proposes the blockchain model of composite chain structure, then constructs the private chain and alliance chain respectively, and finally realizes the adaptive data association storage in complex or classified scenarios. The experimental results show that a composite chain structure blockchain storage method based on blockchain technology proposed in this paper has great advantages in storage efficiency, storage overhead, security performance, availability and other aspects.

Keywords: Composite chain structure · Private chain · Alliance chain

1 Introduction

Blockchain [1] is a new computing paradigm [2] and collaboration model for establishing trust at low cost in an untrusted competitive environment. Due to its features such as high storage density [3], tamper-proof [4] and traceability, blockchain technology has been more and more widely applied. Blockchain stores data by adding blocks [5], and all data are stored on a single chain. However, with the expansion of time and transaction data, data inflation [6] may result in the reduction of storage efficiency. At the same time, single chain storage mode cannot realize associated storage or regular storage in complex or classified scenarios [7].

For example, in the blockchain system of financial activities, if all financial enterprises (entities) store data in the single chain mode in an equal manner [8], the transaction data of financial enterprises (entities) will be chaotic and random [9]. At the same time, according to the single mode to store all financial enterprises (entities) transaction

Q. Chen and J. Li (Eds.): APWeb-WAIM 2020 Workshops, CCIS 1373, pp. 96–103, 2021.
https://doi.org/10.1007/978-981-16-0479-9_8

data, when the associated relationship between financial enterprises (entities), the headquarters and the branch of the financial enterprise, for example, when the total entity (headquarters) of a financial enterprise entity in legal cases has returned to the bad debts to the branch of the financial enterprise, cannot be achieved in a single storage mode to store their relationship. Therefore, how to establish an efficient blockchain storage method has always been a difficulty in the field of blockchain research.

In view of the above problems, this paper proposes a composite chain structure blockchain storage method based on blockchain technology. The main contributions are as follows:

- To solve the problem of low storage efficiency caused by single blockchain storage structure, a blockchain model with composite chain structure is proposed to realize adaptive data association storage in complex or classified scenarios.
- According to the characteristics of the entity data to be stored and the storage requirements of the entity itself, a private chain is built within each entity [10].
- On this basis, combined with the characteristics of different application modes of blockchain technology, the alliance chain is constructed among different entities [11], and the alliance chain and the private chain are combined to build the composite chain blockchain.

2 Related Work

At present, many scholars have conducted in-depth research on the blockchain storage method and achieved certain research results.

In the building of blockchain storage, literature [12] proposes a method of using blockchain to store data. This method proves that using blockchain to store data has the characteristics of high storage density, traceability and tamper-proof, which provides ideas for subsequent research in the storage field. Literature [13] gives a detailed introduction to the data storage mechanism used in the current popular blockchain system, and points out that due to the limitation of data storage mode, the existing blockchain system has the problems of simple query function and low query performance. Literature [4] proposes a method for storing data in blockchain structure of single chain mode. This method is simple and efficient, but it cannot accurately and completely reflect the association or implied relationship between nodes in complex application scenarios. Literature [14] proposed a method of building multi-fork chain block chain structure to store data. This method can store complex and huge data, but using multi-fork chain structure to store data reduces the efficiency of storage and query.

To sum up, existing methods in blockchain storage have problems such as low storage efficiency and complex storage structure. Therefore, considering the efficiency and accuracy of storage, this paper proposes a composite chain structure blockchain storage method based on blockchain technology.

3 The Model of Composite Chain Structure Blockchain

According to the data storage requirements in complex or classified scenarios, combined with the different application patterns of blockchain technology and the data characteristics of the entities that need to be stored, a model of composite chain structure blockchain is presented.

The composite chain structure model of blockchain is composed of private chain and alliance chain. The private chain is built inside the entity to represent the transaction information of the entity. Based on the private chain, the alliance chain between entities is constructed to form the composite chain structure blockchain model. The blockchain model of composite chain structure is shown in Fig. 1.

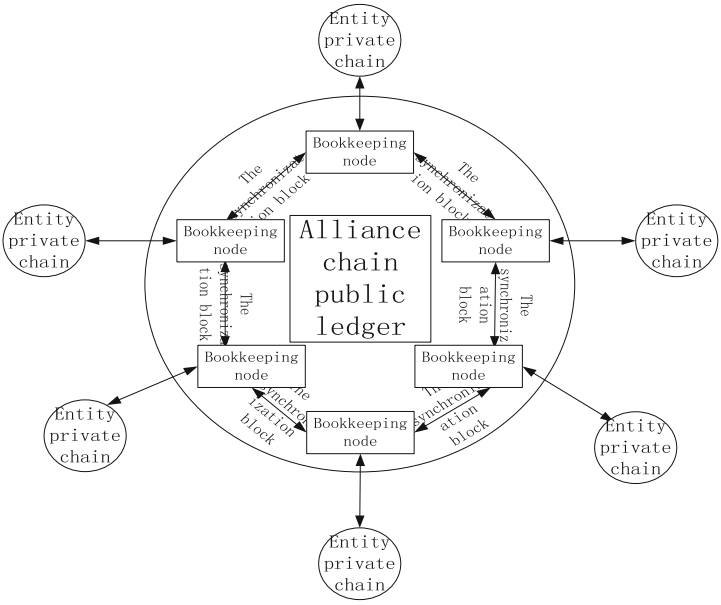

Fig. 1. The blockchain model of composite chain structure

4 The Construction of Composite Chain Structure Blockchain

Based on the composite chain blockchain model, according to different storage requirements, the private chain block structure based on Merkle tree and the alliance chain block structure based on Merkle Patricia tree were established respectively, and finally the composite chain structure of the block chain was constructed.

4.1 Private Chain Block Structure Based on Merkle Tree

The private chain introduces the ECDSA algorithm to generate two different keys (the public key and the private key), which encrypts the data and decrypts it with the public

key when the transaction data needs to be verified. Each block consists of two parts of the head and the block body, head by last the block Hash value (Prev Hash), time stamps, random number (Nonce) and trade to the Root of the Hash (Root Hash), the "transaction type" index table, "suspicious transactions" index table, by adding block hash, root hash and random number information, the hash algorithm is used to generate the hash value of the current block, each block of the preceding block pointer links constitute the whole block link relations in time order. The private chain block header data is shown in Table 1.

Table 1. The private chain block header stores information

The property of the block header	Meaning
The Version number	The version number of the data block
Prev Hash	Hash value obtained by hashing data such as Merkle Root and timestamp of the previous block
The timestamp	the approximate time at which the block is generated
The random number	The random number of solutions to the current block consensus process
Merkle roots	The root of the Merkle tree for all transactions in the block body through a hash operation
Transaction type index table	Record the type of transaction to which the transaction for that block belongs
Suspicious transactions Index table	Record the Hash value of a suspicious transaction

The block body stores all the transaction information, and each transaction information is converted into a string of unique hash values through the hash function and stored on the leaf node of the Merkle tree. The hash value of the upper node is generated layer by layer through the hash function, and each data set corresponds to a unique hash root. If the underlying transaction record is tampered, the Merkle root value will also change.

Before the transaction data is stored in the block, all the transaction types carried out by the entity should be counted and numbered uniformly. When the transaction data is stored in the block, the transaction type information of the transaction should be added to the index table of "Transaction Types". Then suspicious transaction rules are formulated. When data is stored in the block, suspicious transaction rules are used to determine whether the transaction is a suspicious transaction. If so, after calculating the Hash value of the transaction, the Hash value is stored in the Merkle tree and the Hash value is also stored in the "suspicious Transaction" index table in the block head.

4.2 Alliance Chain Block Structure Based on Merkle Patricia Tree

As described in Sect. 4.1, each entity's private chain will serve as an account in the alliance chain. The contact between entities will be established in the form of signing contracts, and the alliance chain block structure based on Merkle Patricia tree will be

established for data storage. The block structure diagram of the alliance chain is shown in Fig. 2.

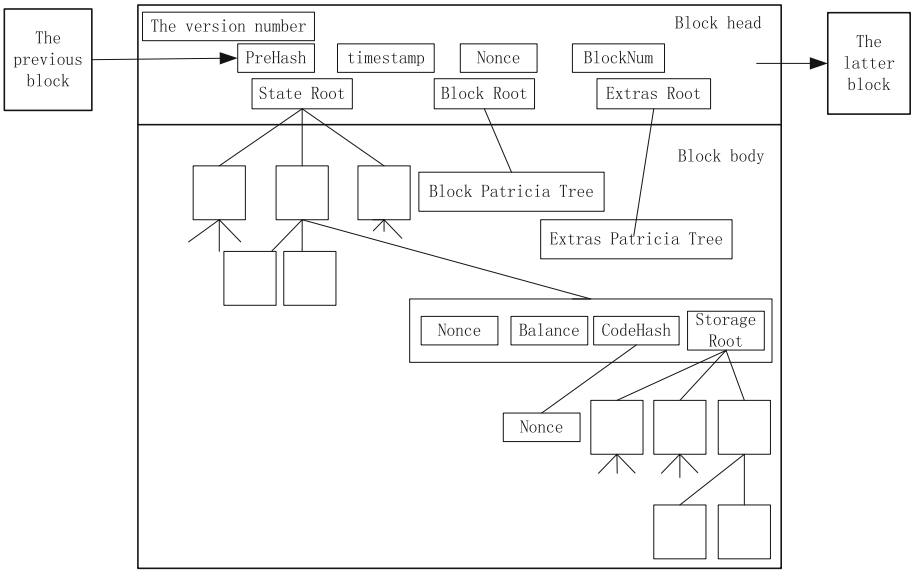

Fig. 2. Block structure of alliance chain

The alliance chain also introduces ECDSA algorithm to encrypt data. The block header consists of the Prev Hash, timestamp, random number (Nonce) of the previous block, and the root hashes of the three Merkle Patricia trees, which correspond to the state tree, the transaction tree, and the receipt tree respectively. The transaction information is stored in the block body. Three levelDB databases are established in the alliance chain, namely BlockDB, StateDB and ExtrasDB. BlockDB stores block headers and transaction records, StateDB stores entity status data, and ExtrasDB stores contract information signed between entities. Based on this, the underlying database of the alliance chain is built. Each block contains the root hash of the entire state tree, which is updated with period T.

5 Experiment and Analysis

The experimental data set is the data on the website of the Tonghuashun. The experiment selects the data from the Tonghuashun to calculate, and verifies the effectiveness of the block chain storage method based on the composite chain structure based on the block chain technology through the aspects of storage efficiency and cost respectively, and compares with the single chain structure and the multi-chain structure.

5.1 Storage Efficiency Analysis

The experiment simulates the efficiency comparison of the blockchain storage structure with the single chain storage structure and the multi-chain storage structure. The x-coordinate represents the storage entity data set, and the y-coordinate represents the storage time required. The experimental results are shown in Fig. 3.

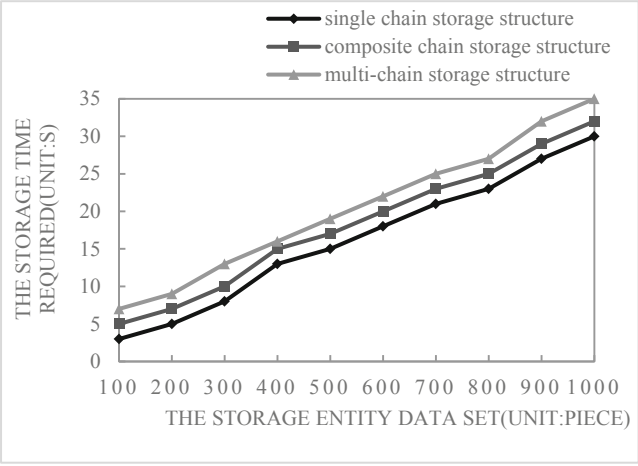

Fig. 3. Comparison of storage efficiency

It can be seen from Fig. 3 that the storage efficiency of the blockchain storage structure of the composite chain structure proposed in this paper is between the single chain structure and the multi-chain structure.

5.2 Storage Cost Analysis

The experiment simulates the cost comparison between the blockchain storage structure of composite chain structure, single chain storage structure and multi-chain storage structure. The x-coordinate represents the storage entity data set, and the y-coordinate represents the amount of space required for storage. The experimental results are shown in Fig. 4.

It can be seen from Fig. 4 that the storage cost of the blockchain storage structure of the composite chain structure proposed in this paper is between the single chain structure and the multi-chain structure.

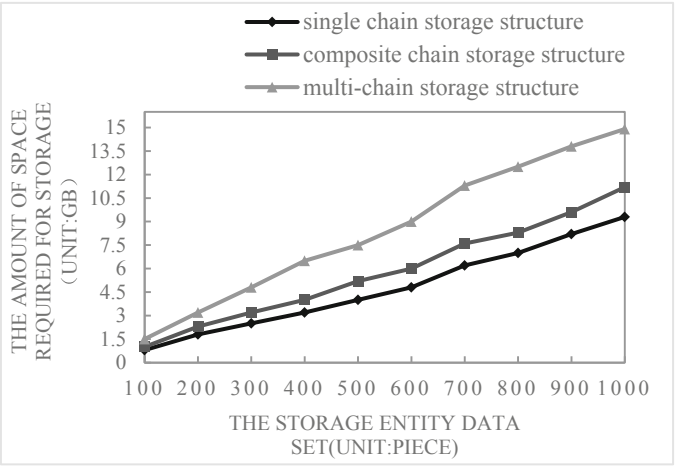

Fig. 4. Storage overhead comparison diagram

6 Conclusion

Blockchain is an effective means to store data securely. Blockchain is used for data storage by adding blocks. Data is stored in single chain mode. With the expansion of time and transaction data, data will expand, which may lead to the problem of storage efficiency reduction. At the same time, the single chain storage mode cannot realize the adaptive data association storage in complex or classified scenarios. To solve these problems, this paper makes an in-depth study of the block chain storage structure method, and proposes a composite chain structure blockchain storage method based on the blockchain technology. This method firstly proposes the blockchain model of composite chain structure, then constructs the private chain and alliance chain respectively, and finally realizes the adaptive data association storage in complex or classified scenarios.

References

1. Yuan, Y., Feiyue, W.: Development status and prospect of blockchain technology. J. Autom. **42**(4), 481–494 (2016). (in Chinese)
2. Bartoletti, M., Bracciali, A., Lande, S., et al.: A general framework for blockchain analytics. In: Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, Las Vegas, Nevada, pp. 11–15 (2017)
3. He, P., Yu, G., Zhang, Y.F., et al.: Prospective review of blockchain technology and application. Comput. Sci. **44**(4), 1–7 (2017). (in Chinese)
4. Iemieux, V.L.: Trusting records: is blockchain technology the answer. Rec. Manag. J. **2** (2016)
5. Wang, S., Dinh, T.A., Lin, Q., et al.: ForkBase: an efficient storage engine for blockchain and forkable applications. In: Proceedings of 44th International Conference on Very Large Data Bases, Rio de Janeiro, pp. 1137–1150 (2018)
6. Halpin, H., Piekarska, M.: Introduction to security and privacy on the blockchain. In: European Symposium on Security and Privacy Workshops (2017)

7. Lind, J., Naor, O., et al.: Teechain: reducing storage costs on the blockchain with offline payment channels. In: SYSTOR 2018, pp. 125–125 (2018)
8. Karlsson, K., Jiang, W., Wicker, S., et al.: Vegvisir: a partition-tolerant blockchain for the internet-of-things. In: International Conference on Distributed Computing Systems, pp. 1150–1158. IEEE Computer Society (2018)
9. Iuon-Chang, L., Tzu-Chun, L.: A survey of blockchain security issues and challenges. Int. J. Network Secur. **19**(5), 653–659 (2017)
10. Dannen, C.: Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners. Apress, Berkeley (2017)
11. Dinh, T.T.A., Wang, J., Chen, G., et al.: BLOC- KBENCH: a framework for analyzing private blockchains. In: International Conference on Management of Data, pp. 1085–1100 (2017)
12. Shao, Q., Jin, C., Zhang, Z., Qian, W., Zhou, A.: Blockchain technology: architecture and progress. J. Comput. Sci. **05** (2018). (in Chinese)
13. Wang, Q., He, P., Nie, T., Derong, S., Yu, G.: Overview of data storage and query Technology of blockchain system. Comput. Sci. (2018). (in Chinese)
14. Jin, H., Dai, X., Xiao, J.: Towards a novel architecture for enabling interoperability amongst multiple blockchains. In: International Conference on Distributed Computing Systems, pp. 1203–1211. IEEE Computer Society (2018)