ISSN: 2688-9323

# Design of Trusted Storage System for Financial Big Data based on Blockchain Technology

Jingpei Feng

Hua'an Security and Stock Co., Yuexiu District, Guangzhou, China

## Abstract

**With the rapid development of blockchain technology and financial big data, the transmission, transmission, storage and calculation of various data have brought convenience to the development of the financial industry, but also some problems have emerged, which have brought unprecedented challenges in security and storage. This paper uses hyperledger technology to design and implement financial big data trusted storage system. Firstly, the system requirements, user modules, information query and update, information verification and authorization, information management information are analyzed. After passing the practice test of each unit, each used unit can reach the intended purpose, the continuity and efficiency of the system is simple and easy to use for users, and the safety and efficiency of the whole system have been significantly improved.**

## Keywords

**Blockchain Technology; Financial Big Data; Storage Technology.**

## 1. Key Technology of Blockchain

In general, blockchain is a distributed storage database with various mining techniques. Electronic money was introduced based on the blockchain. From a small perspective, a block is a set of data that can form a list of related data in a specific order, and different encryption methods ensure that this data is not corrupted. Broadly speaking, blockchain is a distributed architecture that uses distributed storage, distributed algorithms, and cryptographic security methods to create smart contracts that store and manipulate data and business files. The key technologies are as follows:

### 1.1. Consensus Mechanism

By design, it enables distributed nodes to make decisions in different regions. If the data are valid, it's easy to reach a consensus. The main solution to the blockchain consensus layer is for discrete nodes to unite and build trust. For example, if a node is valid, all nodes in the blockchain must agree to form a unified view. The system implemented in this paper adopts DPOS system to form blockchain consensus layer.

The main idea of POW is to propagate the computation at the end of the nodes using the fog calculation method, and then by propagating these nodes, the sha-256 algorithm is used to complete the verification of the node workload to reach the target POW value under the security zone. The formula is shown here

$$T=m/dif$$

The workload of the search method has been proved to have efficiency errors, so the Ethash algorithm can be used to avoid the difference in the impact of each node's efficiency. The essence of this algorithm is that the point at which the algorithm improves efficiency is

ISSN: 2688-9323

independent of memory and bandwidth, and the speed is determined by I/O. SHA256(Parent BlockHash+MerkleRoot+Nonce+...) ≤T.

The disadvantage of the above method is that the method of target finding is continuous calculation, and the Ethash algorithm can be used to suppress the influence of the efficiency difference of each node. The essence of this algorithm is that the point at which the algorithm improves efficiency has nothing to do with memory and bandwidth, only I/O determines speed. The formula of Ethash algorithm is as follows:

$$D(h,n)\leq M/d$$

## 1.2. Smart Contract

It has universal features such as smart contracts, distribution and blockchain design, and is in fact regulated by specific code or blockchain. as a script or application, the contract is deployed to each node and has deployment and deployment capabilities. Not every problem on every node will affect the entire contract.

## 1.3. Communication System

Blockchain scatter devices are based on transmissions, such as specific nodes that create a biometric identification block of data. This node is then sent to the blockchain P2P network node for authentication of all nodes; If the user communicates with this data, signatures and files are created for this data operation. Full network broadcast is to confirm new data on this node, not to be rejected by the whole network. To ensure that data is served only over the network, each node receiving the data must be identified. If the authentication is incorrect, the data block is discarded and cannot be sent to the whole network. Nodes distribute the collected data at a given time, find evidence of a difficult load through calculation, and finally broadcast it to the entire network.

## 1.4. Certification System

Each node will confirm the amount received in the data block, send valid data, otherwise send discard incorrect data, valid data will be added to the main chain.

## 1.5. The P2P Network

P2P networks are called peer-to-peer networks. P2P network is the predecessor of blockchain. The main difference between P2P network and B/S or C/S architecture is that there is no root server or weak center. All data is equal and can be shared and accessed using resources. Unlike B/S or C/S architectures, B-ends and C-ends are less common, but less effective. These nodes are developers and consumers. Blockchain is a distributed structure that connects blocks into chains and then creates P2P networks. The development of P2P networks has led to the birth of blockchain.

In normal C/S mode, the B/S architecture consists of a basic server that accesses the Web system through a browser. Users cannot save or access small caches that only meet the needs of the user's browser. The system is a single user. The C/S architecture has the same basic server as the B/S architecture, but the operations and calculations that users can control are more difficult. The package configured by users is larger than usual, which is called the fat client.

In P2P network architecture, the node verifies the authenticity of the received data adjacent to the node. If the data is valid, the node merges the data and continues to send it to other nodes. If they are invalid, they will not proceed to the next propagation step. in this way, the entire network provides only data, and each node receives data that needs to be verified. if the authentication is incorrect, the data block is discarded and cannot be sent to the whole network. The nodes will mark the data collected at a given time, find some difficult evidence through

ISSN: 2688-9323

calculation, and then send it to the whole network nodes to occupy more core technology. Distributed storage is a technology that makes it impossible to break a single data type.

## 2. System Requirements Analysis and Overall Architecture

### 2.1. System Architecture Design

The system architecture consists of four layers: user layer, business management layer, contract layer and basic platform. The system architecture diagram is shown in Figure 1

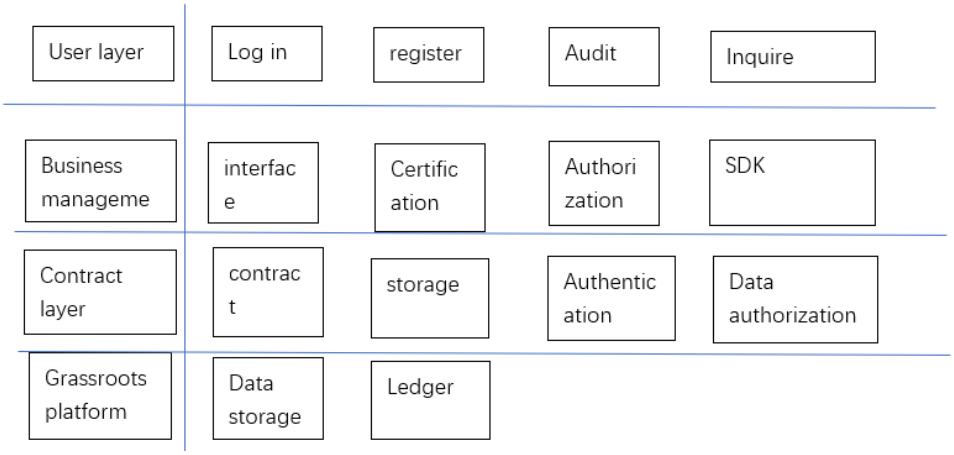


**Figure 1.** System architecture diagram

The grassroots platform is a distributed blockchain network composed of client nodes, CA nodes and financial blocks. For CA nodes, only users with PKI authority can hold nodes, and data is stored based on ledgers. The main platform is a distributed blockchain network composed of user nodes, CA nodes and financial blocks. For CA nodes, only users with PKI authority can control the nodes, and there are multiple ledger pools in the state.

### 2.2. System Operation Process Design

The interactive page uses Java technology and the Solidity language for smart contracts, as well as network interfaces and network builds. The running process is shown in Figure 2.

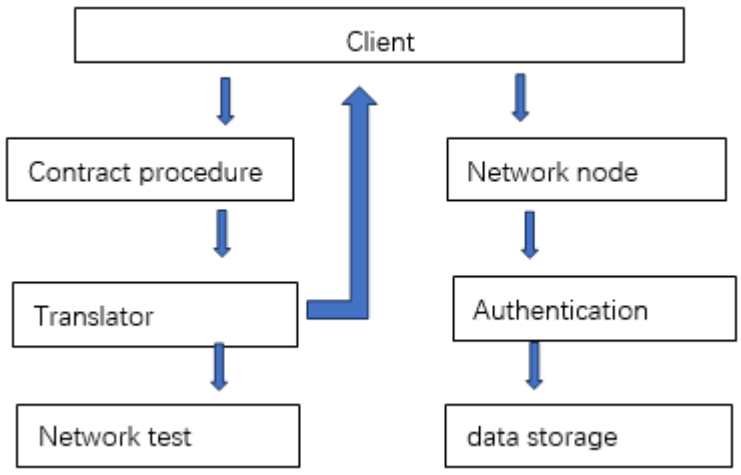


**Figure 2.** System operation flow chart

ISSN: 2688-9323

In the system operation flowcharts, smart contracts are implemented in the Solidity language. Data is transmitted to the smart contract compiler through the contract interface program, which converts the contents of the contract into digital code and then into digital code. Contracts are moved to the front end of the system. The content is deployed over the network, the results can be used to test the system, and once authenticated, the contract content is saved in the back-end database.

### 2.3. System Function Modules

(1) User units. To use the system, users usually need to log in after entering their account and password. As a new user, you must first open your own account and enter your identity and relevant information into the system before you can receive the relevant system. law. The users of this system are mainly individual users and unit users. For unit users, in addition to all the functions of individual users, individual users can also be defined. The process of two users using the system is very similar, but because of the different data structure, the application interface is also different.

(2) Query and replace the unit. The query function mainly includes system data and related information query. Some official information does not require manipulation. You can directly enter keywords for the query. However, the relevant data must require access rights. Administrators who request permissions can request permissions for each user on the system website by assigning authorizations; more closely apply major changes and operations in accounting to update the original data. At present, in order to ensure data security, the system should verify the legality of the action, and the changed action should be saved in an account that is convenient for future data tracking, and the corresponding authority should be obtained before the action.

(3) Confirmation and management of authorization. The authentication function is mainly user information, work history, etc. For personal information, such as unit users, the unit personnel information should be verified first. Provide the user ID. The system and the data are indeed effective, which makes the system get a particularly important release.

(4) Data storage unit. It mainly stores users' personal information and personal information. Personal user information usually includes ID number, address, work experience, work history, contact information, email, etc. Blockchain. When storing the chain code, it is saved through Hyperledger. If the data is stored, it is sufficient for the system administrator to send a ledger request through the appropriate interface to retain the data.

## 3. System Function Realization

### 3.1. System Working Environment

The operating system is Ubuntu 16.04.1 LTS, development tools VScode and Node.js 8.16.

### 3.2. Create a Network Node

The creation of a blockchain network basically includes two parts, one is the establishment of a blockchain network, and the other is the establishment of an agile business system. When building a blockchain network, first use the CP authentication tool to generate the MSP certificate that can create the first block. As Hyperledger is deployed on other network nodes, the registered node is a blockchain network management node that can send chain codes for external use.

### 3.3. Run Program Node

Some application nodes must be designed such that system modules can provide the services they need, because the business layer must provide Web services and use SDK nodes to send data to other layers. Since the authentication system uses Express as the service standard, the

ISSN: 2688-9323

SDK URI request method first creates a routing method to communicate with the blockchain infrastructure network and receive services.

### 3.4. Contract Planning

Smart contract is the core business of the system, which makes the business between two parties a reality. Changing the identity data of the same party in the transaction is done in the smart unit of the contract. In this way, various interferences from the outside world can be prevented and the security of business information can be ensured. The user communicates with the blockchain system through the transaction interface. For communication, the communication process is connected and shared with the application program in the background of the system and the blockchain layer. Provide chain code through daemon call and store the result of Hyperledger operation.

## 4. Conclusion

Combining blockchain technology and WEB development technology for the design and implementation of financial big data storage systems, because blockchain technology has the characteristics of distributed storage, disinfection and centralization, and conforms to the various advantages of blockchain technology. The problem of verifying system credentials, and using Hyperledger technology as the framework for developing this system. The system solves authentication problems such as spoofing by integrating blockchain technology, and the scheme has achieved certain success.

## References

[1] Ai Yingdong,Li Jianbing,Han Yingjie.Design and Implementation of a Microcomputer Laboratory Management System Based on Python Language and Flask Framework[J].Information and Computer (Theoretical Edition), 2019,06:107-108.

[2] Zhu Zheliang, Deng Lujuan. The design of a dynamic safe depository system for financial data based on the Internet of Things[J]. Modern Electronic Technology, 2019, 4216: 58-61+66.

[3] Han Yulong, Han Haiting, Wang Zhenghong, Liu Jian, Liu Yaoyong, Liu Yong, Wang Yanbo. Design and implementation of an IoT card transaction management system based on blockchain and secure terminals [J]. Electronic Design Engineering, 2019, 2721: 32- 35.

[4] Su Huigui. A preliminary study on the design and implementation of a vault security monitoring storage system based on Weishi cloud[J]. China Security, 2017, 06: 101-105.

[5] Zhou Zhiwei. Design and Implementation of Information Sharing System for Financial Institutions Based on Microservice Architecture[J]. Financial Technology Times, 2021, 06: 74-77.

[6] Zhang Liang, Zhang Hanlin, Kong Fanyu, Yu Jia. Design and implementation of real estate supply chain system based on Ethereum[J]. Computer Engineering and Applications, 2020, 5603: 214-223.