Targeted Poverty Alleviation System Based on Industrialized Blockchain

HaolingMeng *, ChenglunHu, ChenxiLi, XufengWen
East China Jiaotong University, Nanchang Jiangxi, China, 330013
**Corresponding Author.*

Abstract

Toward the existing problems in targeted poverty alleviation system, such as unclear poverty alleviation records, inaccurate poverty alleviation targets, easy tampering of poverty alleviation data and single data storage structure, a targeted poverty alleviation system based on blockchain + IPFS + distributed database is designed.For different links in the industrial field, different consensus schemes are used to balance reliability and performance. Using the characteristics of blockchain technology to ensure that data are traceable and tampering-proof, and then combining this technology with the interstellar file system (IPFS) as data storage to solve the problem of high cost of large files; what's more, the distributed database can play a role in achieving data partition management to solve the problem of single data storage structure. The data nodes are independent of each other, thus, they can realize the efficient control of resources and improve the concurrency and scalability of the system. Through the performance test and comparative analysis of the system, it is proved that the system has a great improvement in throughput, data read-write delay and other indicators.

Keywords*: Blockchain, targeted poverty alleviation, distributed database, industrialization*

I. Introduction

Poverty is a major issue that my country has faced for a long time. With the steady progress of poverty alleviation programs, my country's targeted poverty alleviation work has entered an important stage. The number of poverty alleviation populations is large, the storage of poverty alleviation data, and privacy protection[1], transparency has become the key. Meng Xiaofeng and Feng Dengguo made an analysis on the data element market[2], affirming that data has a positive effect on economic development, production and life, etc. In response to the problem of people losing control over their own data, they proposed to establish a data governance system with data transparency. Liu Lixin and others have launched a blockchain-based transparency research[3], revealing the principle and implementation of data transparency, and verifying the feasibility of data cloud storage service transparency. Liu Yahui, Zhang Tieying and others analyzed the privacy protection issues in the current stage for personal privacy protection in the era of big data, and proposed privacy protection technologies, laws and industry norms[4]. Aiming at the problem of single data storage structure and large amount of data, research scholars such as Chu Zhiqiang and Wu Jiying[5] design a distributed off-chain storage framework based on blockchain. Through distributed deployment of block nodes and storage nodes, the area is guaranteed. The operating efficiency of the blockchain. These provide practical solutions to the problems existing in the current poverty alleviation work.

In order to solve the above problems, this essay designs a targeted poverty alleviation system based on blockchain + IPFS + distributed database. The agreement is executed by smart contracts, and the data is stored by the Interplanetary File System (IPFS) to ensure that the data is traceable and tamper-proof.

II. Key Technology of System

2.1 Blockchain technology

As a technology with the characteristics of intelligence, decentralized accounting and smart contract, blockchain is widely used in various fields. Blockchain is a chained data structure, and the data blocks are arranged in chronological order in the operating environment. Timestamp, Peer-to-Peer Networking (P2P)[6] and other technologies are combined and cleverly used, so blockchain has the characteristics of decentralization, timing and non-tampering. As shown in Fig. 1, the data records generated by creating blocks, the total transaction volume of blocks in the figure, and the unique Merkle root generated in the hash calculation process will be recorded in the block head.

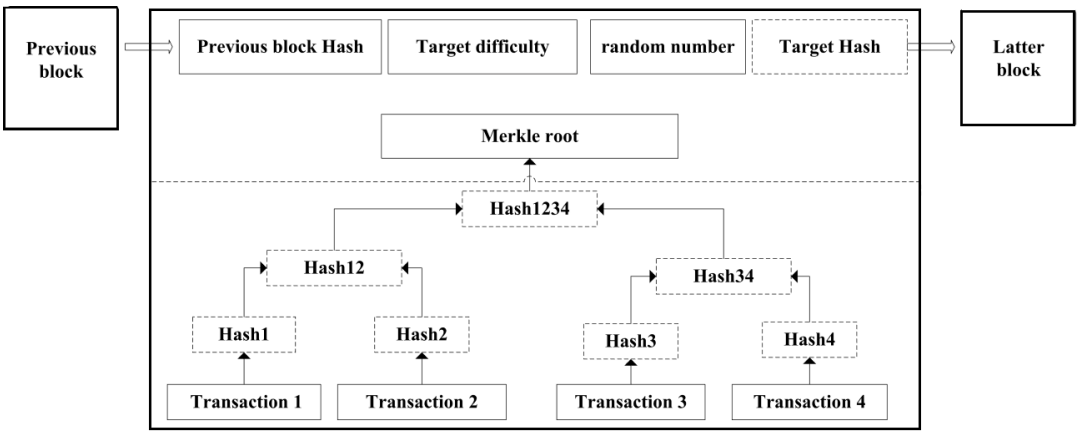

Figure1: Blockchain structure

2.2 IPFS technology

IPFS is a new generation of Internet protocol. It has the advantages of Git warehouse, BitTorrent group, self-certified file system and so on. It can transmit and save data safely and quickly. As a point-to-point distributed hypermedia distribution protocol, IPFS processes data into a number of 256kb data fragments and stores several nodes, providing a permanent decentralized storage method[7].The commonly used hash algorithms in IPFS networks are SHA1, SHA-256 and BLAKE2. When any hash algorithm is used to encrypt the data, a short-length and fixed hash value hash generated by the hash algorithm, which facilitates the storage and query of files between different nodes. The schematic diagram of the hash function is shown in Fig. 2.

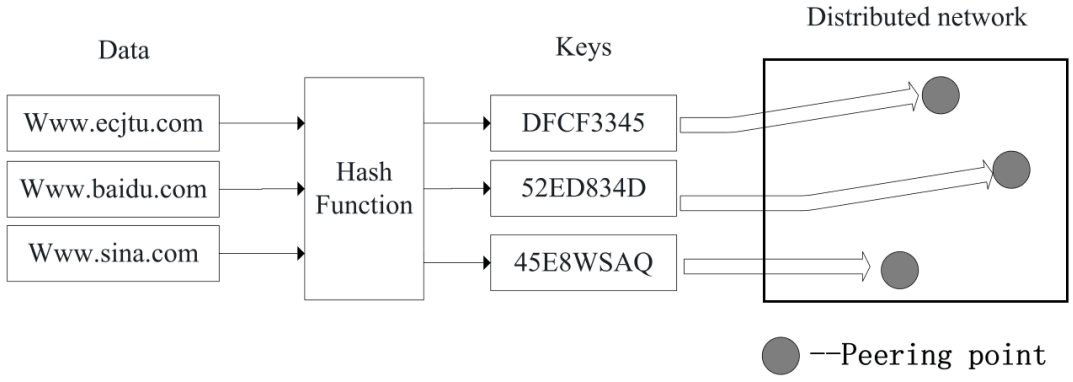

Fig 2: Hash function diagram in IPFS network

III Design of Targeted Poverty Alleviation System Based on Blockchain

3.1 Integrated design

The targeted poverty alleviation system is mainly divided into three parts, including presentation layer, business logic layer and data access layer. The presentation layer is a bridge between users and systems, users can interact with each other. Business logic layer deals with business-related parts, playing a connecting role in data exchange. The data access layer uses IPFS file storage system and Ethernet platform to store, update and retrieve data models. As shown in Fig. 3.

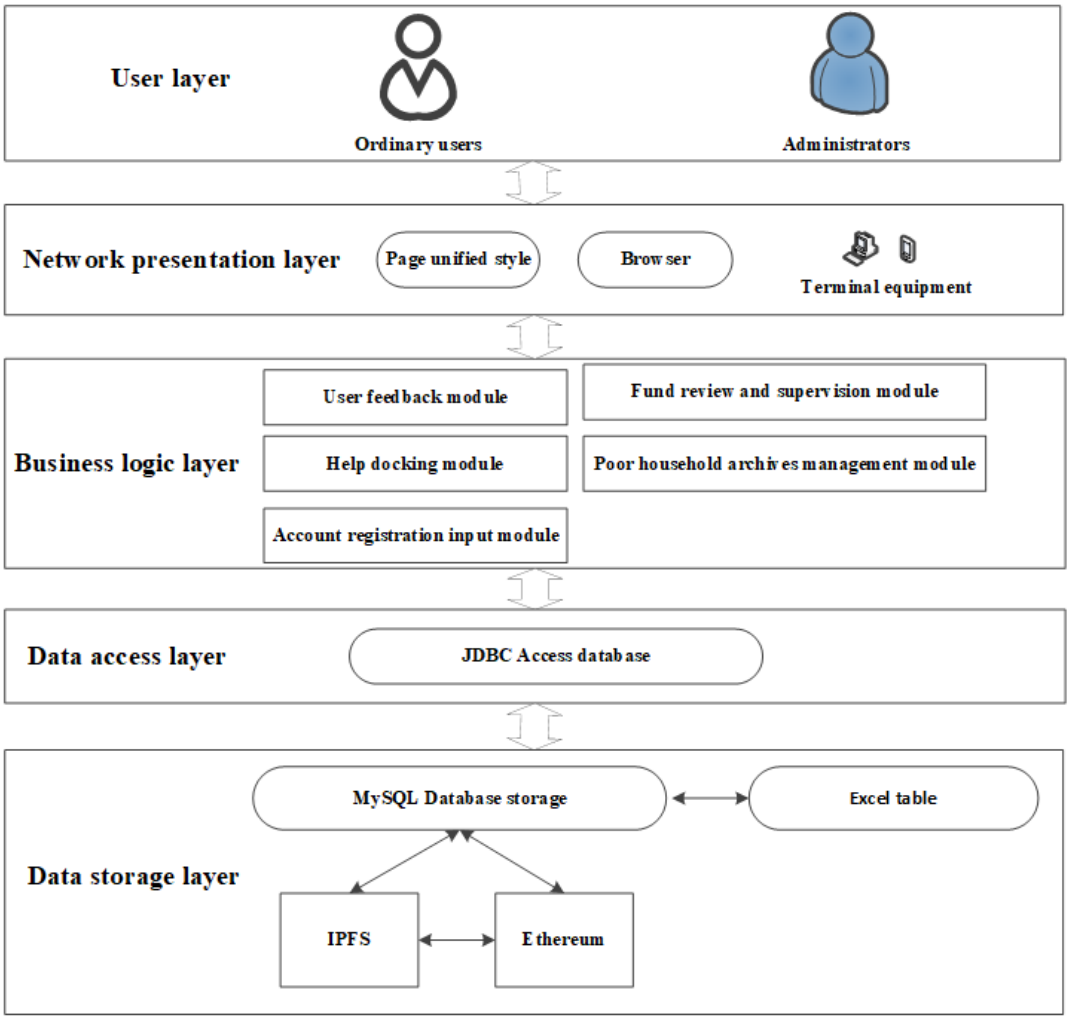

Fig 3: Overall design

3.2 User interface design

The system consists of four types of users: system administrator, supervisor, poverty alleviation staff and poor households. When users enter the targeted poverty alleviation website, they need to use the private key to login (the private key will explain below), and the system will determine the user's permissions and jump to the corresponding page. The user interface design of targeted poverty alleviation system classifies the user access rights of various types, so that users can enter different interfaces. Implement interface management components and listener components, use listener components to listen to trigger events, and then mobilize the interface for the next step. User interface design is shown in Fig. 4.

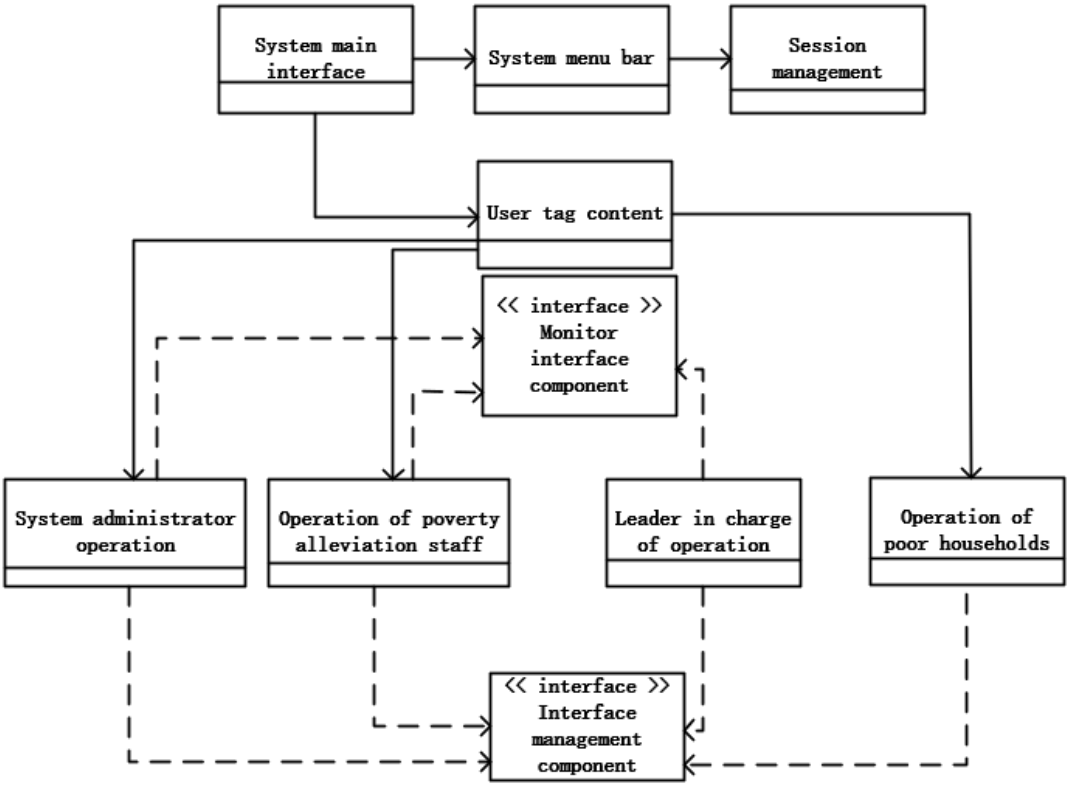

Fig 4: User interface design

3.3 Module design

The system puts forward five modules according to the process of targeted poverty alleviation, account registration and entry module, poor household file management module, help docking module, fund review and supervision module, user feedback module. The specific module division is shown in Fig. 5.

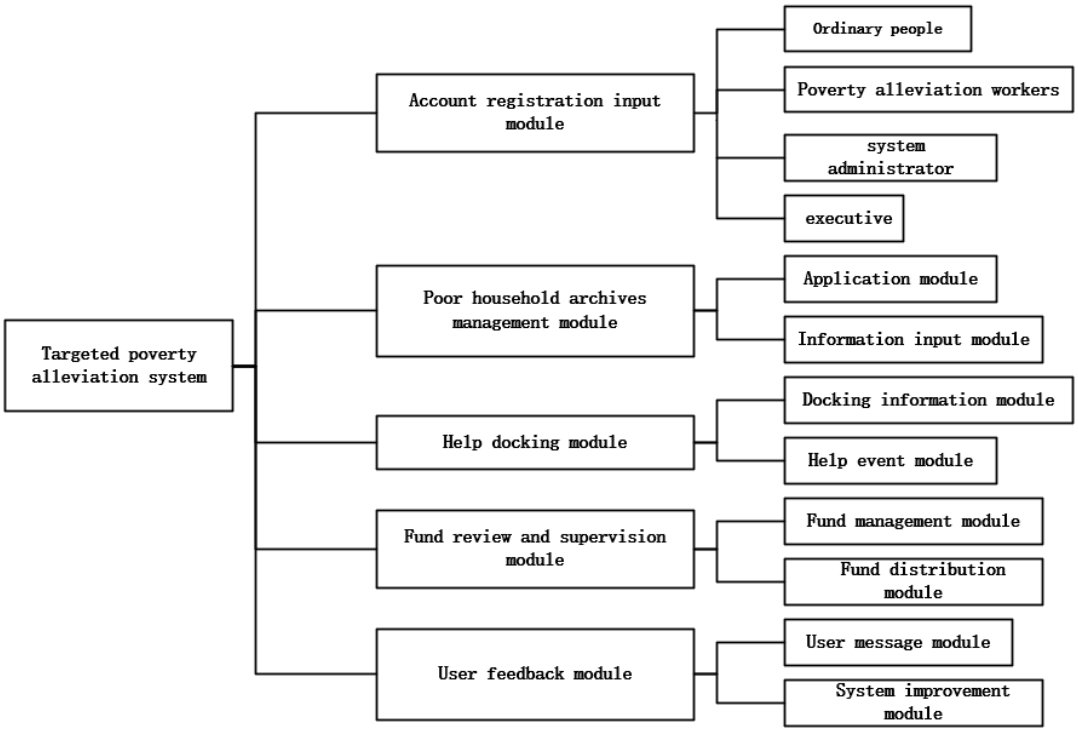

Fig 5: Module design

3.3.1 Account registration entry module

Account registration entry module is divided into four categories of users, the public, poverty alleviation staff, system administrators, supervisor leadership. Users can log in only after registration, and they need to select roles first, then enter personal information such as name, age, gender, and region, and finally click the key generation button. After verification by multiple system administrators, the system automatically generates public key and private key pair, and users retain their private key and submit the public key to the system, and write the registration information into the blockchain. If not, a denial of registration message is issued, and the user is refused to generate the key[8]. The user registration flow chart is shown in Fig. 6.

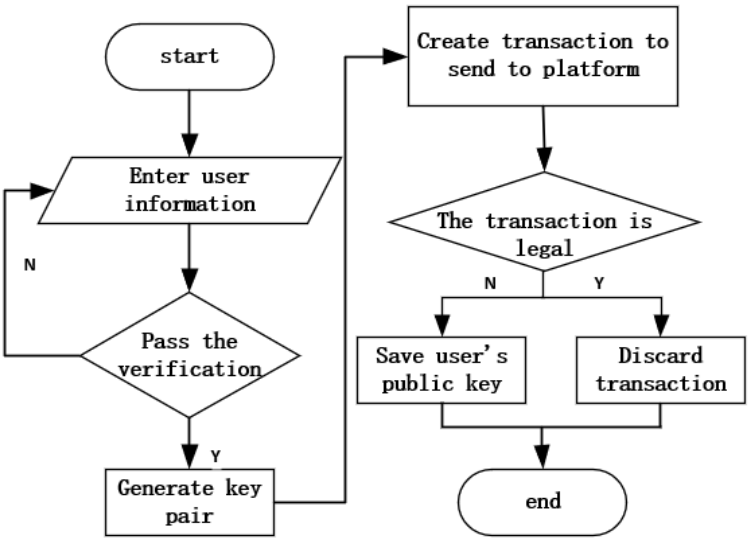

Fig 6: Flow chart of user registration

3.3.2 Archives management module for poor households

The front end of the system provides the function of file management and entry for poor households. The ordinary people first submit the poverty application form, and then upload it to the system after the poverty alleviation staff audit the archives of poor households. Archives data will be uploaded to the database by the system front desk, and java language realizes the data interface of hash table. Bit strings are generated from the file data uploaded by poverty alleviation personnel through hash function[9], and the bit strings are sent to the API interface through post request. The server can obtain a trusted time stamp in the bit string, as shown in Fig. 7.

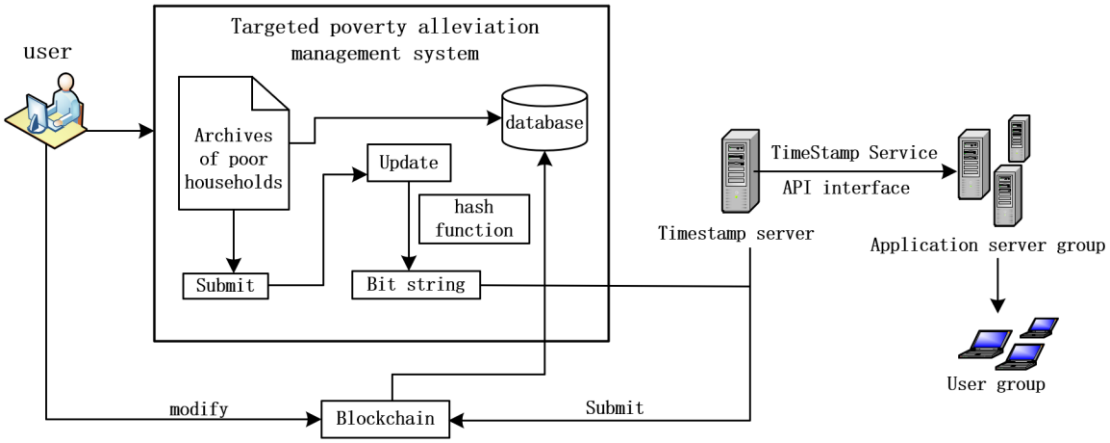

Fig 7: Archives management system for poor households

3.3.3 Help docking module

The block body is composed of multiple transactions. It records when, under what conditions and in what order the transaction is stored by blockchain. The two parties of the transaction are the initiator and the processing party, the sender is the user, and the processing party is the system. After the transaction is processed, it is sent to the upper chain. This transaction cannot be tampered with and ensures the safety of the transaction. Transaction data, block data, node information and block state information can be easily found through the query interface designed by this system. The query of poor households is based on the public key. If the poor households' accounts do not receive transactions, users cannot query the transaction data, indicating that there is no entry of assistance-related information. Transactions are received if entry is verified.

3.3.4 Fund review supervision module

The system records data flow in real time, using distributed ledgers, open and transparent. When someone proposes to modify and query the application, the application will be packaged into transactions and sent to the platform. The transaction is submitted to the block chain. At that time, the node in the block chain confirms the transaction to reach a consensus and judges whether the application is legal. If it is legal, it agrees to the request and submits the transaction to the platform, returns the query data and modifies the license to the user. Otherwise, it rejects the application and realizes the authority management and tamper proof of fund review supervision. The updated data can be found by the newly generated hash value[10].

3.5 Contract design

The smart contract used by the system is an event-driven, stateful, multi-party recognized program that automatically processes assets under pre-conditions[11].All data of the precision poverty alleviation system are stored in the block chain, and the web3.js library is used to call the intelligent contract to realize data exchange. The system is written in solidity language. Solidity is similar to JavaScript language, and the development tools around solidity are complete.

For the intelligent contract itself, the code and node consensus mechanism are written into the specified block of block chain. In the contract code, the scenario of running the contract, the program to deal with specific scenarios, some predefined states and the operation rules under each state are configured. The operation of intelligent contracts is based on certain conditions. Only when the real-time state is monitored by the block chain, and the data source is verified, and the operation conditions are confirmed to meet[12].

IV. System Realization

4.1 System environments

The system adopts B/S architecture, and the operating environment is CentOS 7.2.1511 operating system. Data storage uses MySQL5.7.19 database, and JDK version 1.8.0-261 is controlled by git version. It has very strong adaptability to various system interfaces, and has excellent openness, scalability, and ease of use.

4.2 System function realization

4.2.1Network environment construction

The construction of block chain network is divided into three main steps, building a single main group and multi node alliance chain, environmental deployment and contract call. After installing the dependent software package, the alliance chain is started, the process is checked, and the change of the network environment is monitored in real time through log management. Compile parallel contracts to meet the concurrent scenarios, while the contract privacy protection, signature authentication.

4.2.2 User authority management

Each account can send structured Action to other accounts and define the processing script after Action is accepted[13]. To determine whether a specific action has been properly authorized, each account can be controlled by any weighted combination of other accounts and private keys. When the account contract action is taken, the name permission level of the account itself will be mapped. In the process of identifying permission mapping, the multi-signature threshold program will be started to verify the signature authorization, and the authorization is correlated with the name permission. If it fails, it will traverse the parent permission upward, and finally find the permission of its owner.

4.2.3 Distributed log

In a distributed system, the log system is the operation log of the chain, which records the state change process of the chain. Log-centered design is mainly divided into two ways: one is the main standby mode, one is the state machine replication[14]. The system uses the state machine to copy, and writes the operation into the log first. All nodes generate the local state by subscribing to the log and performing the operation. Since there is no master node, the system uses the POP consensus to synchronize all nodes to ensure that the log system of all network nodes achieves consistency.

4.2.4 Web development

The front-end and back-end interfaces are separated, and the Restful API style interface specification is used. The front-end is designed and developed by vue.js, and the back-end is designed by SpringBoot. The bottom calls the designed intelligent contract. The user logins by entering the Ethernet address, and distributes to different interfaces through user rights management.

V. System Test

The system mainly adopts black and white box alternating test, which is subdivided into function + dynamic test

and performance test. In the functional test, the use-case test method of equivalence class + boundary value is adopted, and a large amount of input use cases (input, output, boundary state) are adopted. Different roles are used to log in and act in the five modules respectively. The function under different roles is tested to check whether the system is normal, to check whether there is an error prompt after input, and to ensure the robustness of the whole system. Table 1 shows the strategy of system functional testing and some results.

Table 1 Function test table

Test Object	Test Function	Test Describes	Test Results
system administrator	Check account registration	entry interface, check account information and register through account	pass
	Distribution of poverty alleviation objects	Enter the help docking page to allocate poverty alleviation objects for poverty alleviation staff.	pass
	Distributing poverty alleviation funds	Access to the funds distribution page to distribute funds for designated poverty alleviation staff	pass
	Query poverty alleviation projects	Access poverty alleviation project interface, query progress and user information	pass
the poverty household	View targeted poverty alleviation policies	Access to the system home page to view recent poverty alleviation policies and funding time passes	pass
	Query funds transfer	Enter the fund management page, real-time query funds transfer is normal and issuance records, etc.	pass
	User Message Feedback	Enter the user feedback module, real-time feedback user experience and other help information.	pass

The performance test of the system generates a huge load on the server, network and object by simulating a large amount of requests from the Web client and carrying relevant data. The test results are shown in Fig. 8.

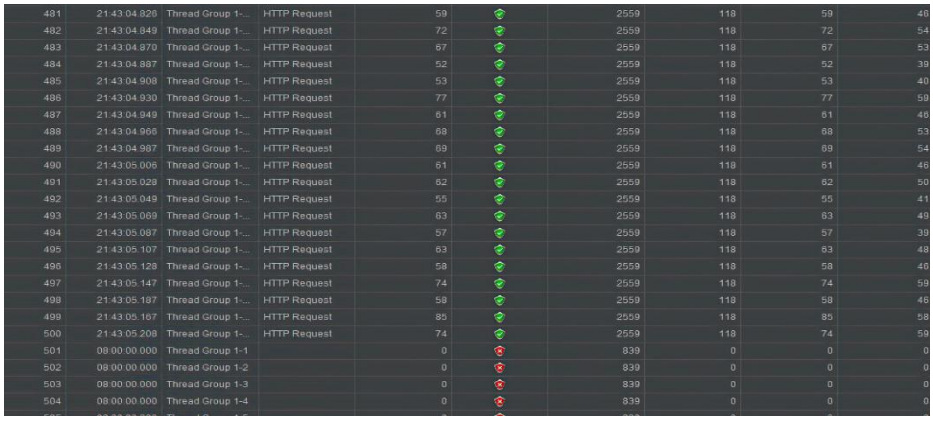

Fig 8: Requests load results

It can be seen from the figure that the connection time and sample time of the system gradually change again by increasing the request load, but the transmitted data flow can still guarantee the integrity of 118 bytes. When the request reaches 500 times/s, the system performance is almost saturated; After more than 500 times, the system requests begin to make mistakes and cannot be processed in time, but they are sufficient to cope with specific business scenarios in life. By setting different pressure values, the response time, operation efficiency, throughput and data read-write delay of the system are tested. The results are shown in Fig. 9.

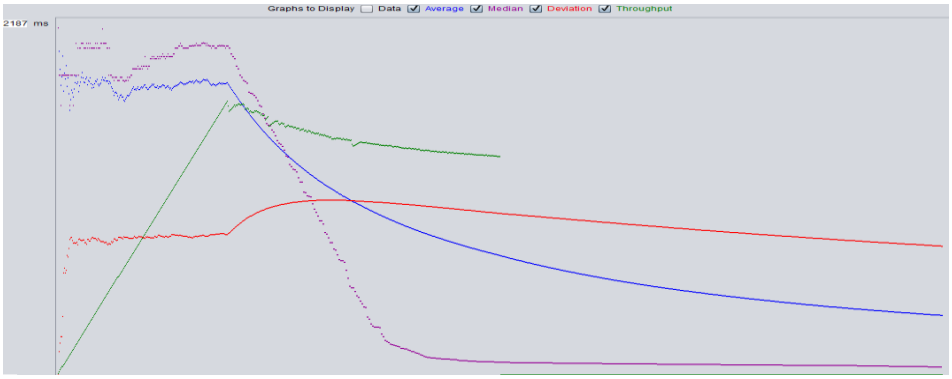

Fig 9: Pressure performance test

It can be seen from the figure that when the pressure value increases continuously, the throughput (green curve) of the system increases linearly. Operating efficiency (purple curve) is also on the rise, but the change is relatively slow; System response time is also in a relatively stable state (purple curve); The delay of data reading and writing increases slowly. However, when the pressure exceeds the peak value, the pressure continues to increase, and the delay of data reading and writing decreases, which reflects that the ability of distributed database to process concurrency has been greatly improved compared with traditional data centralized storage.

VI. Ending

With the goal of building a well-off society in an all-round way approaching, whether people ' s living conditions and quality can be effectively guaranteed has become the focus of close attention. According to the needs of modern targeted poverty alleviation, this essay designs a system based on blockchain + targeted poverty alleviation + distributed database. Blockchain technology makes up for the shortcomings of current targeted poverty alleviation work, effectively ensures the safety and integrity of targeted poverty alleviation data, and provides a reliable solution for the storage of targeted poverty alleviation data. This system has solved the shortcomings of the current poverty alleviation work technically, which is in line with the relevant poverty alleviation policies and strategic guidance, and is convenient for poverty alleviation work. However, the blockchain technology itself is not perfect, and researchers need to continue to explore in depth to gradually improve the entire blockchain system.

References

[1] S.W. Gao, C.C. Zhou. “Differential privacy data publishing in the big data platform of precise poverty alleviation,” Soft Computing, vol. 24, pp. 1-9, 2019.
[2] X.F.Meng, D.G.Feng. “Preface,” Computer research and development, vol. 58, no. 2, pp. 235-236, 2021.
[3] X.F.Meng, L.X.Liu. “Data transparency based on blockchain: problems and challenges,” Computer research and development, vol. 58, no. 2, pp. 237-252, 2021.
[4] Y.H.Liu, T.W.Zhang, X.L.Jin, et al.,“Personal privacy protection in the era of big data,” Computer research and development, vol. 52, no. 1, pp.229-247, 2015.
[5] Z.Q.Chu, J.Y.Hou, L.Xu, et al.,“Design of distributed off-chain storage framework based on blockchain,” Information network security, vol. 21, no. 2, pp. 87-93, 2021.
[6] A.D.Donet, P.S. Cristina, H.J. Jordi. “The bitcoin P2P network,” Workshop on Bitcoin Research, Shanghai：Springer, 2014.
[7] X.L.Fan, C.X.Fan, Y.X.Wu. “Based on blockchain and IPFS technology to achieve food supply chain privacy information protection,” Journal of Applied Sciences, vol. 37, no. 2, pp. 179-190, 2019.
[8] L.Yu, X.F.Zhao, Y.Sun, J.Zhang, et al.,“Implementation of fair contract exchange protocol based on blockchain technology,” Journal of Software, vol. 31, no. 12, 2020.
[9] J.D.Cui, S.W.Wang, Y.C.Xin. “Research on the technical framework of smart grid data management from the perspective of block alliance chain,” Journal of China Electrical Engineering,vol. 40, no. 3, pp. 836-848, 2020.
[10] Y.Q.Sun, Q.C.Wang. “College performance management system based on blockchain technology,” Cryptography, vol. 5, no. 5, pp. 568-578, 2018.

[11] Y.He. “Overview of intelligent contract technology and application based on blockchain,” Computer research and development, vol. 55, no. 11, pp. 2452-2466, 2018.
[12] B.Li, W.Z.Cao, J.Zhang, et al.,“Multi-energy system trading system and key technologies based on heterogeneous blockchain,” Power system automation, vol. 42, no. 4, pp. 183-193, 2018.
[13] J.F. Li et al.,“A blockchain-based authority management framework in traceability systems,” International Journal of Computational Science and Engineering, vol.24, no. 1, 2021.
[14] Alexander Thomson et al. Fast Distributed Transactions and Strongly Consistent Replication for OLTP Database Systems. ACM Transactions on Database Systems (TODS), vol. 39, no. 2, pp. 1-39, 2014.