A New Home-Based Pension Mutual Aid Framework Based on Blockchain

Ridong Huang, Jianmao Xiao(✉), Siqi Cheng, Ronglin Zhang, Hao Zeng, Xin Huang, and Zuoyi Liao

School of Software, Jiangxi Normal University, Nanchang 330027, China
{jm_xiao,xinhuang}@jxnu.edu.cn

Abstract. In the context of the public's response to home-based care, the "Time Bank" care model has attracted more and more attention as an effective supplement to home-based care. Although there are cases of Time Bank implementation in China, it still has many problems such as extreme centralization, lack of credibility, and opaque and imperfect circulation of time currency. In response to this, this paper integrates blockchain technology based on the traditional time banking model and proposes a new home-based care mutual assistance framework driven by blockchain technology, which utilizes the distributed decentralization, collective maintenance, and data immutability of the blockchain. The characteristics of the blockchain provide credit guarantees by combining the community-based management agency and the channelization of the service network. Time-based transaction process service matching, smart currency scoring module. And use their respective financing agreements and other technologies to safely circulate, jointly establish a chain-wheel interoperability chain, and cooperate with various contract models to jointly establish various on-chain contracts. Experimental analysis shows that the new framework involved can realize secure encrypted storage and transmission of information, solve the problem of cross-regional storage and exchange, and provide a new feasible solution for home care.

Keywords: Blockchain · Smart contract · Decentralization digital signature · Shared ledger · Time bank

1 Introduction

According to the data of the seventh national census, the population aged 60 and above reached 263 million, accounting for nearly 18.70%, and it is expected to reach 487 million in 2050, accounting for 34.9% of the total population. The degree of aging in China continues to deepen. Combined with changes in population structure, urban and rural labor flow, and demand for elderly care services, the pressure on elderly care has intensified, the function of family elderly care is lacking, and the problem of elderly care is serious. Based on the promulgation of a series of support policies by the country, various socialized elderly care institutions have emerged in the context of expanding market opportunities, and

Y. Cao and X. Shao (Eds.): MONAMI 2022, LNICST 474, pp. 32–47, 2023.
https://doi.org/10.1007/978-3-031-32443-7_3

elderly care has increasingly become a "sunrise industry" in which capital is chasing after each other. Problems such as uneven distribution of pension resources, shortage of professional nursing staff, and insufficient pensions between large cities and small and medium-sized cities have gradually become acute [1]. The elderly service is in a difficult situation and urgently needs new feasible solutions.

Compared with the traditional old-age care model, the community is used as a link for the acquisition of old-age care services, and the platform helps intelligent home-based care for the elderly. Realizing the multi-directional interaction between the elderly, children, service centers, and the government, active monitoring and other functions of the new home-based care model. In the context of the public's response to home-based care, the "Time Bank" care model has attracted more and more attention as an effective supplement to home-based care. Time Bank motivates volunteers in a "paid" way. Short-term volunteer time coins can be exchanged for daily necessities and long-term exchange for equivalent services, to solve the problem of volunteer needs and alleviate the insufficient supply of elderly care services. Although there are many examples of time bank development in some areas of China, such as the "Bu Lao Time Bank" in New Taipei, Taiwan in 2013, and the "Time Bank of Shanghai Hong Kou Changning elderly care service" in 2019, the current pension model in China is still dominated by family pensions, and there are extreme risks. The traditional pension model has pain points such as centralization, lack of credibility, opaque circulation of time currency, and imperfect operation model [2]. The development of practice is slow and it is difficult to implement.

Blockchain is a distributed database system and a distributed technology system in that multiple parties jointly maintain public ledgers. It is characterized by decentralization, openness and transparency, traceability, security, and information encryption. The chain nodes constitute a distributed ledger, and the completion of the transaction conveys the confirmation of each point, and the result is collected together. The decentralization feature enables Time Bank to transmit service requirements point-to-point, we use algorithms to intelligently generate keys, accurately match service requirements, and ensure data security. The above advantages prove that the effective use of blockchain can provide strong technical support for time banking issues.

This paper designs and implements a blockchain-based time chain model by analyzing the pension dilemma, and the time bank process, and combining blockchain technology and fabric institutions. The experimental analysis is feasible to carry out tests in terms of transaction throughput response time to ensure the implementation.

The contribution of this paper is:

- A time banking system solution based on blockchain technology is proposed. By analyzing the current problems of time banking, according to the actual business needs of the time banking system, combined with the blockchain, it analyzes and proposes solutions.
- Designed a blockchain-based time banking system framework.

– Through a series of experimental tests, the performance of the system is analyzed, and it is shown that the new framework can realize the secure encrypted storage and transmission of information.

2 Related Work

2.1 Blockchain

With the increasing popularity and development of virtual digital currencies such as Bitcoin, the underlying blockchain technology has received widespread attention [3]. The blockchain is essentially a decentralized, tamper-proof, and trustworthy new distributed database, which is integrated and innovated by existing technologies. It integrates distributed data storage, p2p data transmission, consensus mechanism, and technologies such as encryption algorithms and smart contracts. Each data block contains the data information of transactions on the network for a certain period to verify whether the information is valid and generate the next block. A block consists of a block header and a block body. The block body contains a certain number of transaction sets. The association with the previous block is maintained by PrevHash to form a chain structure. So that every transaction in the block is traceable and well-documented. At the same time, the integrity of the block transaction set is quickly verified through the root hash (Root hash) generated by MKT (MerkleTree) [4].

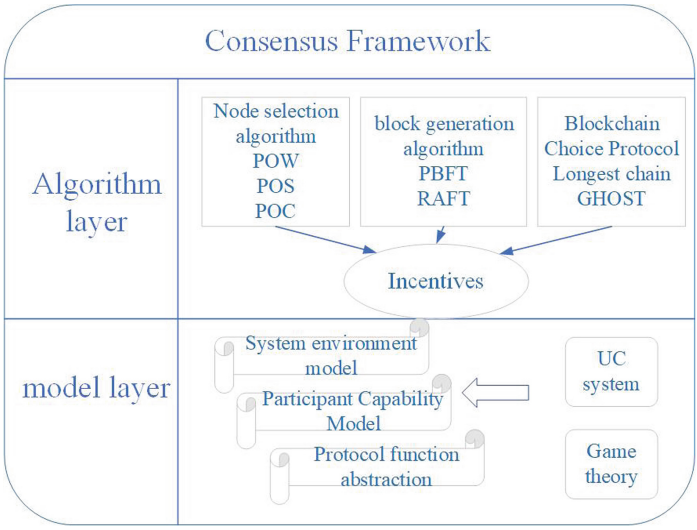

Fig. 1. Blockchain Consensus Framework

The blockchain consensus framework diagram as shown in the Fig. 1. Decentralization is the most significant feature and core idea of the blockchain, which

adopts the P2P network structure. So - called decentralization means that it does not rely on the central node for accounting, and all nodes in the network have equal status and jointly manage the data in the system. This kind of data management is based on the blockchain structure to verify and store data, use consensus algorithm to generate and update data, use cryptography to transmit and protect data, and jointly supervise each node on the network, so as to achieve no need for a third-party trust agency. Endorsement [5]. Every node participating in the blockchain network are both a client and a server. When a node on the chain initiates a transaction, other nodes in the network will conduct consistency verification of its accuracy and validity to achieve transactions after consensus is added to the blockchain. In the blockchain, in a distributed trust less environment [6], the consensus mechanism is used to achieve consensus among nodes.

Due to the two characteristics of process credibility and decentralization, blockchain can build a trust base in a low-cost way in the scenario of multistakeholder participation, aiming at reshaping the social credit system. In the past two years, the blockchain has developed rapidly, and people have begun to try to apply it in the fields of finance, education, medical care, and logistics.

2.2 Time Chain Research for Time Bank

Operating Mechanism Model. The time bank mutual assistance pension model is a mutual aid pension model in which people with self-care ability and social behavior ability provide services for the elderly, to save time, and withdraw time to obtain services when needed. The specific operation mechanism is: the user registers as a member of the time bank and establishes a time account. Elderly care service demanders publish their elderly care needs through the Time Bank, and participants contact the demanders through this intermediary platform to provide services. After the end of the service transaction, the demander of the old-age service deducts the corresponding time collateral, and the supplier gets the time collateral. The converted time collateral is chained to TBC (time chain Time Block Chain), that is, by generating new transactions (the owner of the time collateral recorded in the transaction is the elderly care service provider) and send transaction information to the TBC [7]. In the future, the suppliers of old-age services will be transformed into demanders of old-age services, and the above process will form a complete closed loop [8]. The system operation process is shown in Fig. 2.

Theoretically speaking, the timing chain designed in this paper is a brand new blockchain, and it does not belong to the public chain, private chain, or consortium blockchain. Compared with the public chain, users using the timing chain need to be authenticated, but it can also realize complete anonymity between users. Compared with the consortium blockchain and private chain, all users on the timing chain can participate in the consensus process of the system and can obtain all the data on the chain.

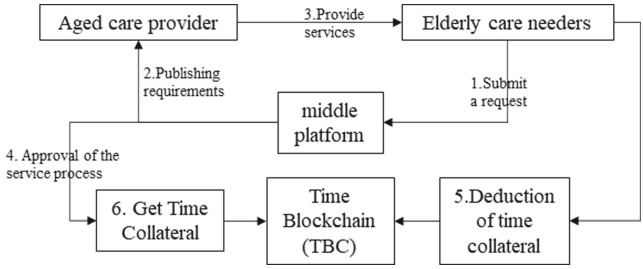

Fig. 2. Operating Mechanism Model

3 Blockchain-Based Time Banking Framework Model

3.1 System Architecture

The time bank system based on blockchain technology designed in this paper adopts the Hyperledger Fabric consortium chain architecture. The Hyperledger Fabric consortium chain is a distributed system that ensures the security and reliability of transaction data. Different servers are configured as different nodes and play different roles during actual operation, to realize the functions of each module in the system architecture. The system is divided into four levels: data layer, transaction business layer, security layer, and user layer as shown in Fig. 3 [9].

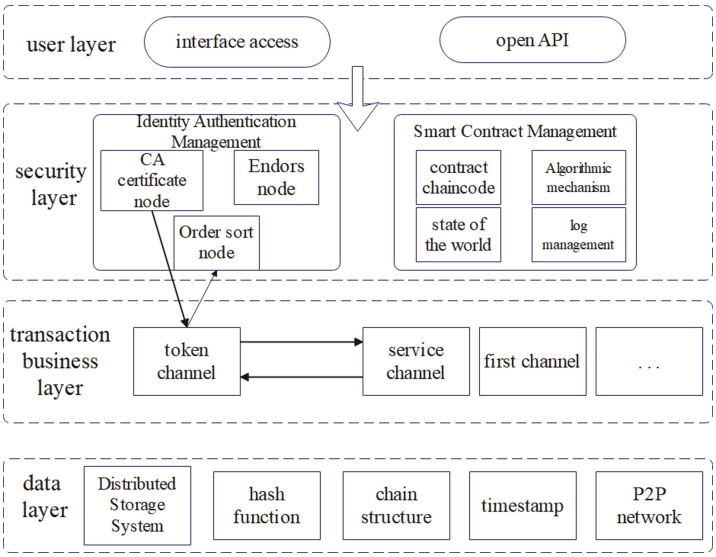

Fig. 3. System Architecture Diagram.

3.2 System Data Layer

The data storage structure and data organization method of the system are based on the fabric consortium blockchain architecture. The system data layer organizes data records into blocks and organizes the blocks into a chain structure by recording the hash value of the previous block in the block header of each block. Since the Time Bank network itself is a decentralized network, the participating nodes are completely autonomous, and there is no unified node responsible for management and maintenance. For this reason, each user of the network needs to use P2P technology. The P2P network [10,11] is used in the blockchain, which can establish a trust-enhanced blockchain P2P topology through fast and reliable broadcasting [12]. The correct information is broadcast to the entire blockchain network through a series of encoding sequences formed by specific hash functions [13,14] and encoding functions such as base58 and base64, and timestamps are added to realize data broadcasting and update node state information and ledger information as shown in Fig. 4.

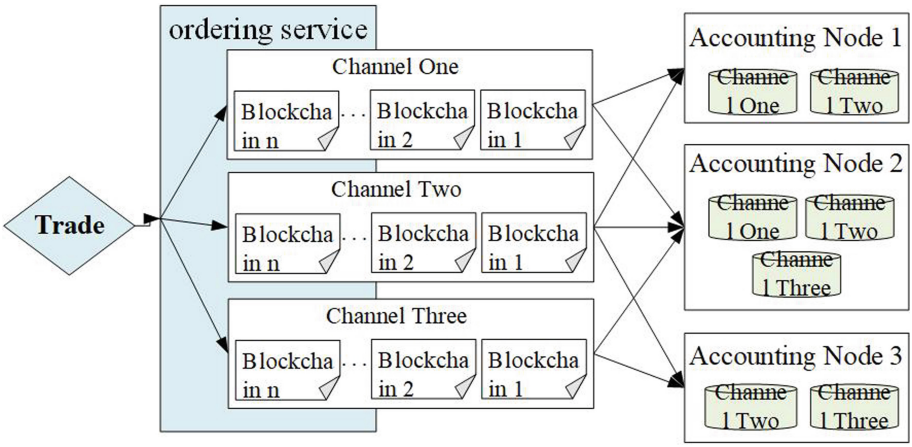

Fig. 4. Time Banking System Data Layer.

Once wrong information or network virus invades the entire blockchain network, in the process of blockchain P2P topology transmission, each node must determine whether all the information is correct. The character sequence formed by the hash function calculation and the encoding function will be greatly changed. The node compares the original correct encoding sequence with the public and private keys of the digital signature. If the sequence does not match, the node will refuse to accept the information. At the same time, the consensus mechanism in the time chain ensures the consistency of node information in the entire Time Bank network [15]. If the user is hacked and modified, the Time Bank network will trace the timestamp of the information to find the wrong information, delete the wrong information through the information rollback mechanism,

and Re-update the node's state information and ledger information through the consensus mechanism. In the face of irresistible damage, as long as there is one node in the entire time chain network, all nodes can restore the data information in the entire time bank network as shown in Fig. 5.

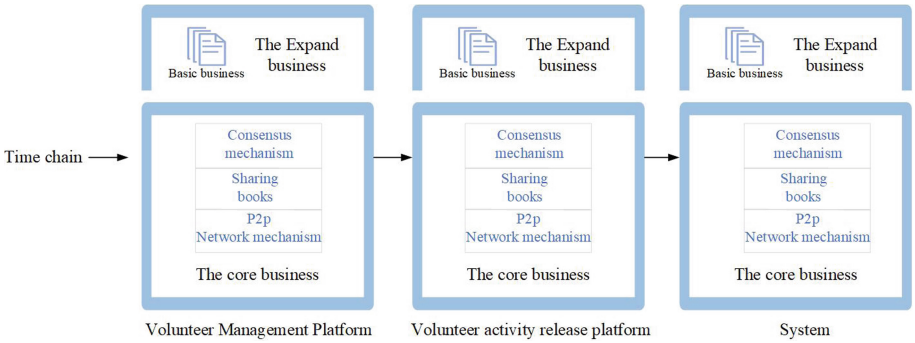

Fig. 5. Time chain structure diagram

3.3 Security Layer

The security layer module ensures the information security, decentralization, and non-tampering characteristics of the system through decentralized CA nodes, fabric network establishment of hierarchical channels, workload proof, block consensus broadcasting, and system node division.

Service Network Channelization. The Fabric network we built consists of three distinct channels. The first is called the Service Channel (SC), which handles all service-related network issues. The second, called the Token Channel (TC), is responsible for collecting all wallet data from the ledger. The third is called the grading channel (GC), which allows registered members to rank each other. Each channel is attached with Chaincode running on peers and provides a platform for program execution to transmit transactions. In the Fabric framework, all transactions are evaluated and agreed upon at the ordering stage. Finally, all transactions are sent to a special entity called the "orderer". The orderer puts all transactions in order of execution and updates them on the ledger, the same for the original channel for endorsing and non-endorsing peers.

Proof of Work. After the time bank system has been running for a while, the local settlement point will integrate all the valid data collected during this period to make it a collection of transaction data, and then use the Merkle Tree algorithm to achieve Merkle Root Hash (assuming this hash value is MRash) is generated, and then assembled with the random number Nonce and other related

fields, and finally, it becomes the data of the blockchain header, we assume that the header data is Headdata, and then continuously adjust the value of Nonce, so that Hash (Headdata is always less than Difficulty, where Difficulty refers to the correct value of the speed of the Nonce random number obtained by the system during the adjustment process of the end node. In this process, With the help of the first calculated Nonce random number specific settlement node, the acquisition of the settlement power in this round is realized, to realize the generation of new blocks and broadcast them.

3.4 Transaction Business Layer

The transaction business layer mainly provides technical support for the time currency transaction, and the timing chain provides the core business of the time bank system by implementing the underlying mechanism of the fabric blockchain, such as time currency settlement, transfer, query, etc. The full-service nodes in the entire time banking system run the timing chain, provide channels for the circulation of time coins in the entire system, and provide blockchain services for the audit platform and third-party business systems through the restful service interface.

Time Currency Transaction. In the time bank chain, the most important part of the whole service process of volunteers and the elderly being served and the process of time currency transfer, inheritance, and lending between users is the module involving time currency transactions.

The entire time currency transaction process is divided into three steps. First, the time currency sender (A) fills in the transaction information and sends the transaction information to the time currency receiver (B); The information is digitally signed; finally, the entire transaction information is encrypted and broadcast to the entire time bank system through the P2P network. All members of the system can use the public keys provided by A and B to verify the transaction information after receiving the broadcast information as shown in Fig. 6.

The digital signature [16] and encryption algorithm [17] adopted by the time chain ensures that the data transmission [18–20] between nodes is safe and shared. The system adopts elliptic curve encryption algorithm [21] and elliptic curve digital signature [22,23]. The digital signature should meet the following requirements:

1) The signature cannot be forged.
2) The signature is non-repudiation.
3) The identification and application of the signature is relatively easy, and anyone can verify the validity of the signature.
4) The signature cannot be copied, and the signature and the original text are an inseparable whole.
5) The signed message cannot be tampered with. Any bit data is tampered with, and its signature changes with it. Anyone can verify and refuse to accept the signature.

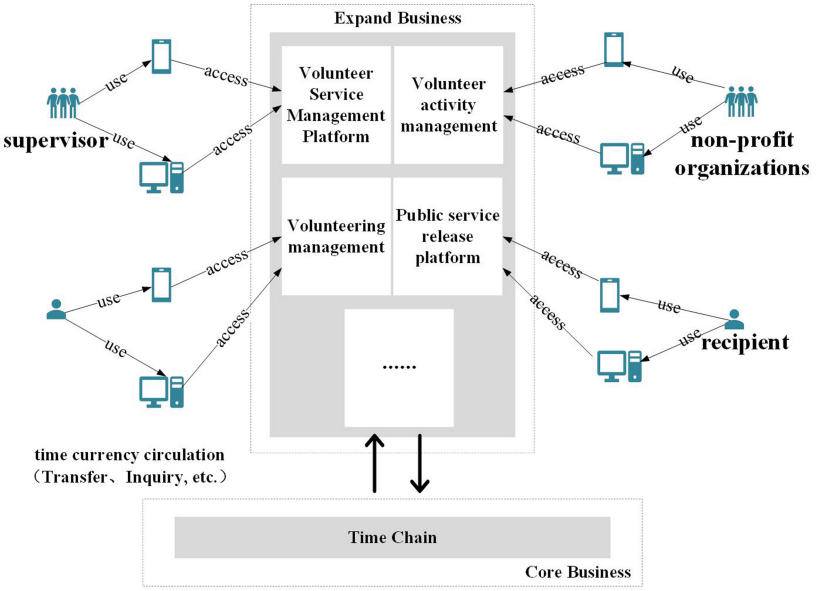

Fig. 6. Time Coin Circulation Chart

Elliptic curve digital signature core code: A function to generate a digital signature for a tx object as shown in Fig. 7.

```
func SignTx(tx *Transaction, s Signer, privatekey *ecdsa.PrivateKey) (*Transaction, error){
    h := s.Hash(tx)
    sign, err := crypto.Sign(h[:], privatekey)
    if err != nil {
        return nil, err
    }
    return tx.WithSignature(s, sign)
}
```

Fig. 7. Digital signature function

It can be seen from the body of the SignTx() function after the Signer. The Hash() method provides the content to be signed (that is, the hash of some members of the Transaction object after RLP encoding), and the main work of generating the signature is handed over to the Sign() function to complete.

Elliptic curve digital signature verification principle [24,25]:

$$\frac{hG}{s} + \frac{xK}{s} = \frac{hG}{s} + \frac{x(kG)}{s} = \frac{r(h+xk)G}{h+kx} = rG \tag{1}$$

Elliptic curve encryption algorithm:

1) Select an elliptic curve Ep(a, b) and take a point on the elliptic curve as the base point P.
2) Select a large number k as the private key and generate the public key Q = kP.
3) Pass Ep(a, b) and points Q and P to the user.
4) After receiving the message, the user will encode the plaintext to be transmitted to the point M on Ep(a, B) and generate a random integer R.
5) Public key encryption (ciphertext C is a point pair):

$$C = \{rP, M + rQ\} \tag{2}$$

6) Private key decryption (M + rQ − k(rP), the decryption result is point M)

$$M + rQ - k(rP) = M + r(kP) - k(rP) = M \tag{3}$$

7) Decode the point M to get the plaintext.

Assuming that in the encryption process, there is a third party H, H can only know the elliptic curve Ep(a, b), the public key Q, the base point P, the ciphertext point C, and the private key k is obtained through the public key Q and the base point P Or it is very difficult to obtain the random number r through the ciphertext point C and the base point P, so the security of data transmission can be guaranteed.

Encryption:

$$Ecc\_points\_mul\,(\&c2x, \&c2y, px, py, \&r, a, p) \tag{4}$$

$$Ecc\_points\_mul\,(\&tempx, \&tempy, qx, qy, \&r, a, p) \tag{5}$$

$$Two\_points\_add\,(\&mx, \&my, \&tempx, \&tempy, \&c1x, \&c1y, a, zero, p) \tag{6}$$

Timecoin transaction is the core of the entire time chain and provides security for the entire transaction process through digital signatures and encryption algorithms. Digital signature and encryption algorithms greatly improve the security of data in the process of writing, transmitting, and reading, and the data association method between blocks through the concatenation of hash values and the data writing mechanism based on the consensus algorithm [26] to confirm the block It also makes the data on the blockchain extremely difficult to tamper with.

Transaction Process. Based on the Fabric architecture, the system proposes an overall framework combining six modules. The transaction process is divided into three major processes: service matching, token transfer, and scoring system as shown in Fig. 8.

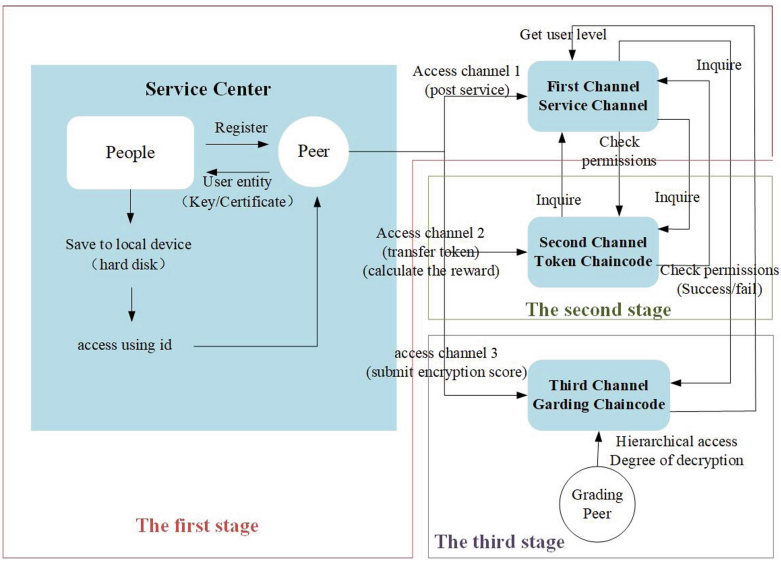

Fig. 8. Service Match

Before talking about service matching, services need to be released first, and registered members on the chain publish their service-related data (i.e. proposals) on the blockchain. They can use their key pair to access peers, upload their service proposal, and call the PostService function on the service Chaincode in SC. Users have access to different peers, which means they can travel to different timebank centers as long as those peers belong to the same channel. On this basis, after a member's service proposal is published on SC, the proposal system tries to find a match as much as possible. Without loss of generality, this paper only uses a simple (intuitive) matching scheme to find matches, while the adoption of other complex matching algorithms will improve the matching performance [27,28]. Either SP or SR needs to compare all attributes (except location-related attributes) to find a matching service. In addition, there is an important factor to consider when looking for a match by considering various attributes, which is the level of service involved in our matching process. Those low-ranking members should be punished systematically in order to preserve the core values of the Time Bank. One possible solution is to make it harder for those lower-ranked members to get matched. In other words, a lower rank indicates a lower priority and probability that he or she can be matched with others.

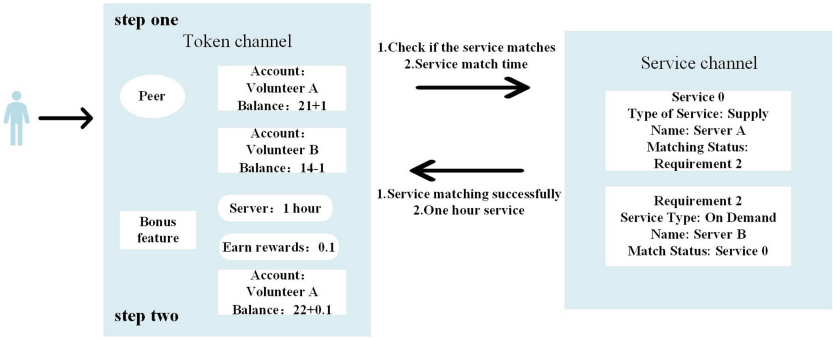

Fig. 9. Token conversion

The next stage is the token transfer as shown in Fig. 9. The token transfer between SR and SP in TC after service exchange. The whole process (taking volunteers A and B as an example). First, the user executes the application to access the TC and calls the token transfer function to embed the token Chaincode. In this case, after the SR and SP have exchanged their services, the SP wants to receive time credits for the services he or she provides. Due to the passive nature of the blockchain, tokens are only transferred when users access it and invoke smart contracts on it. Since only SPs have an incentive to obtain time coins, the transfer of tokens must be activated by SPs. He or she can call the token transfer function in TC directly through the app and get time credits in return.

3.5 User Layer

The user layer interacts with the underlying timeline through the restful service interface. In this time bank system, all users need to be authenticated by the CA (Electronic Authentication Service) system, and only after passing the authentication can they become a legal user in the time bank chain, and at the same time obtain a certificate and key that can encrypt data.

New members are added to the timeline. If a new member joins by himself and there is no recommender, his new member information will be reviewed by all members in the system. If the new member fills in the recommender information, the recommender will review the user information of the new member. Audit information includes personal information, digital signatures, and more. After all, information is reviewed and approved, new members will have a limited publicity period. If any members object to joining, or malicious behavior is detected, the system will automatically remove new members. If the new member successfully joins the Time Bank Chain, the recommender will be rewarded with corresponding work points, that is, the recommendation reward mechanism of higher-level recommender: recommender: me = 5:3:2. The entire registration review process is open and transparent, and all members jointly certify new

members, which further guarantees the security and stability of the entire system in operation. The recommendation reward mechanism will promote the flow of the entire system and encourage members to join the timing chain.

4 Experiment Analysis

4.1 System Transaction Throughput

Transaction Throughput is an important performance indicator of the Time Bank blockchain network, that is, the number of transactions that can be processed per second, which represents the business processing efficiency of the Time Bank blockchain system. This paper uses the Fabric blockchain network performance test tool Hyperledger Caliper to test the transaction throughput. The specific operations are divided into two types: time bank ledger write operation (invoke) and ledger query (query) operation, each of which initiates 10,000 transactions The request is divided into multiple rounds, and a different transaction sending frequency (Send Rate) is set for each round to test the transaction throughput. The specific test data of transaction throughput are shown in Table 1.

Table 1. Time Bank System Transaction Throughput Record Table.

Test round	Transaction Type	Number of transactions	Sending frequency(tps)	Transaction throughput(tps)
1	invoke	10000	25	25
2	invoke	10000	50	43
3	invoke	10000	75	55
4	invoke	10000	100	59
5	invoke	10000	125	52
6	invoke	10000	150	48
7	query	10000	50	50
8	query	10000	100	81
9	query	10000	150	134
10	query	10000	200	181
11	query	10000	250	202
12	query	10000	300	193

Figure 10 and Fig. 11 show the write throughput versus sending frequency and the query throughput versus sending frequency. Analysis of the transaction throughput chart data shows that for the ledger write throughput, when the sending frequency is below 100tps, the ledger write throughput increases with the increase of the sending frequency. When the sending frequency reaches

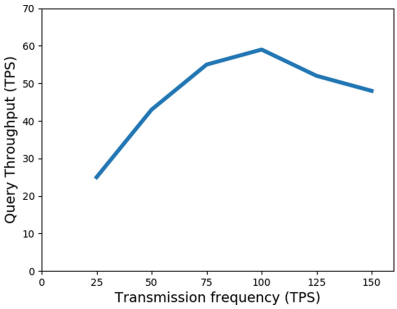

Fig. 10. Write throughput varies with send frequency

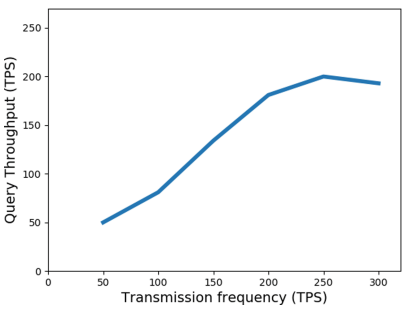

Fig. 11. Query throughput varies with sending frequency

100tps, the ledger write throughput reaches 100 tips. The peak value is 60tps, and when the sending frequency exceeds 100tps and continues to increase, the ledger writes throughput decreases slowly and fluctuates around 50tps; for the ledger query throughput, when the sending frequency is below 250tps, the ledger query throughput increases with the increase of the sending frequency. It keeps increasing. When the sending frequency reaches 250tps, the ledger write throughput reaches a peak value of 198tps. When the sending frequency exceeds 250tps and continues to increase, the ledger query throughput decreases slowly. Ledger writing requires multi-organization endorsement consensus, but the ledger query does not. Therefore, the ledger writing operation takes extra time, making the ledger query throughput higher than the ledger writing throughput, which is consistent with the test results. Based on the above analysis results, it can be concluded that the transaction throughput of the Time Bank blockchain network meets the system performance requirements.

5 Conclusion

Given the extreme centralization, insufficient credibility, opaque circulation of time coins, and imperfect operating models in the service of pension services, this paper proposes an innovative model of blockchain + time bank for mutual assistance in-home care. The time bank is used as a blockchain distributed ledger, collectively maintained, removing the centralization of the traditional time bank, and using the blockchain to integrate the work point and point system, while ensuring transparency and security, and improving credibility. In the orderly advancement of the time bank project, at the current stage, the application of core technologies and the construction of the basic platform have been completed, and the follow-up will expand the application of the system and improve the functions of the platform, and in the next stage, further research will be carried out according to practical investigation and experimental analysis. The timing chain of "blockchain + time bank" innovation will be widely used in all

aspects of the field of pension services in the future, alleviating major pressure for social pensions, enhancing personal value, and promoting social pension services to move forward in the emerging direction, and will eventually form a "time conversion, time shuttle" pension public welfare ecosystem.

Acknowledgements. This work is supported by the Foundation of Jiangxi Educational Committee under Grant No. GJJ210338, the National Natural Science Foundation of China (NSFC) under Grant No. 61962026, the National Natural Science Key Foundation of China grant No. 62262030 and No. 62067003, the National Natural Science Foundation of China under Grant No.62002143 and the Natural Science Foundation of Jiangxi Province under Grant No. 20192ACBL21031.

References

1. Jiang, Q.: Current situation and future development of institutional pensions in my country. Coop. Econ. Technol. (16), 3 (2021)
2. Boc's "time bank" public welfare mutual aid platform to explore the development of time bank with Chinese characteristics. Chin. Civil Aff. (2), 1 (2022)
3. Chuangchuang, Luan, H., Yang, X., Guo, X., Lu, Z., Niu, B.: Overview of blockchain technology research. Comput. Sci. **48**(S02), 9 (2021)
4. Cai, X., et al.: The principle of blockchain and its core technology. Chin. J. Comput. **44**(1), 48 (2021)
5. Shen, M., Zhang, H.: Overview of blockchain technology research. Wirel. Internet Technol. **17**(10), 3 (2020)
6. Liu, F., Chen, Y.: A review of blockchain technology research. J. Shandong Normal Univ. Nat. Sci. Ed. **35**(3), 13 (2020)
7. Xiao, K., Wang, M., Tang, X., Jiang, T.: Public welfare time banking system based on blockchain technology. J. Comput. Appl. **39**(7), 6 (2019)
8. Tao, S., Zhang, Y.: The mechanism and path of "time bank" mutual aid for the elderly: from the perspective of time and money, (2), 7 (2022)
9. Xia, Q., Dou, W., Dou, W., Liang, G., Zuo, C., Zhang, F.: Overview of blockchain consensus protocols (2021)
10. Zhou, Y., Fang, J., Jia, Y., Jia, L., Shi, W.: Consortium chain consensus algorithm based on PBFT. Comput. Sci. **48**(11), 9 (2021)
11. Sun, Z., Zhang, X., Xiang, F., Chen, L.: Research progress of blockchain storage scalability. J. Softw. **32**(1), 20 (2021)
12. Tetarave, S.K., Tripathy, S.: PJ-sec: secure node joining in mobile p2p networks. CCF Trans. Pervasive Comput. Interact. (4) (2020)
13. Wu, Y., Li, J.: The evolution process of blockchain P2P network protocol. Appl. Res. Comput. **36**(10), 7 (2019)
14. Deng, Y., Ji-Tao, M.A., Hai-Hong, W.U., Liu, W., Zhang, R.B.: Analyse operation mechanism and management styles for the public service network of science and technology which is built under the principle of "innovation-driven"-take the joint construction and application of scientific instruments and equipments. China Soft Science (2011)
15. Liu, F., et al.: Blockchain cross-chain asset interaction protocol based on improved hash time lock. Comput. Sci. **49**(1), 9 (2022)
16. Baccara, M., Lee, S.M., Yariv, L.: Optimal dynamic matching. CEPR Discussion Papers (2018)

17. Carrara, G.R., Burle, L.M., Medeiros, D.S.V., de Albuquerque, C.V.N., Mattos, D.M.F.: Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking. Ann. Telecommun. **75**(2) (2020)
18. Liu, F., Yang, J., Qi, J.: Research on two-party elliptic curve digital signature algorithm of blockchain based on hash proof system. Inf. Netw. Secur
19. Wang, R., Tang, Y., Pei, X., Guo, S., Zhang, F.: Blockchain privacy protection scheme based on lightweight homomorphic encryption and zero-knowledge proof. Comput. Sci. **48**(S02), 5 (2021)
20. Qian, W., Shao, Q., Zhu, Y., Kim, C.-C., Zhou, A.: Blockchain and trusted data management: problems and methods brief. J. Softw. **29**(1), 10 (2018)
21. Liu, S., Liao, S., Yang, C., Fan, J.: Research on real world data sharing system based on blockchain. Inf. Secur. Res. **8**(1), 6 (2022)
22. Wang, G., Ding, H.: Blockchain-based business collaboration data security sharing scheme. Inf. Secur. Res. **7**(7), 9 (2021)
23. Liu, Y., Lang, X., Pei, S.: Encryption algorithm based on ECC and homomorphic encryption. Comput. Eng. Des. **41**(5), 5 (2020)
24. Zhang, P., Li, Y.: A forward-secure elliptic curve digital signature scheme. Comput. Eng. Appl. **56**(1), 6 (2020)
25. Xiao, S., Wang, X., Pan, F.: An elliptic curve digital signature algorithm based on modular inverse operation. Comput. Eng. Appl. (2020)
26. Zhang, X., Li, Q., Fu, F.: Confidentiality verification method of blockchain transaction amount based on digital commitment. Comput. Sci. **48**(9), 6 (2021)
27. Chen, C., Long, X., Jiang, Z., Liu, Z., Meng, Q., Long, L.: Research progress on the application of time banking model in the field of elderly care. J. Nurs. Training **36**(12), 4 (2021)
28. Li, C., Jiang, M.: Research on the optimization strategy of blockchain embedded "time bank". Changbai Acad. J. (4), 7 (2021)