Research and Design of the Mutual Aid Tokenized Economy Structure Based on Blockchain Technology: Taking Time Bank as an Example

Xu Qing
School of Software, Beijing University of Posts and Telecommunications
Xitucheng Road 10
Haidian District, Beijing , China
18810623560,+86
3467133430@qq.com

Liu Feng*
Institute of Artificial Intelligence and Change Management/
Shanghai University of International Business and Economics
Gubei Road 620
Changning District, Shanghai, China
13218779868, +86
lsttoy@163.com

Xiao Zilong
School of Data and Computer Science, Sun Yat-Sen University
Waihuan East Road 132
Panyu District, Guangzhou, China
18173019525, +86
shenciyou@gmail.com

ABSTRACT
In the current time bank system, problems such as difficult time token to circulate, difficult to trust data, and insecure data exist. In order to solve these problems, a design and implementation of a time bank system architecture based on blockchain technology is proposed. Firstly, analyze the business process of the time bank system and draw the use case diagram; then layer the overall architecture of the system: the application interface layer and the blockchain layer; then carry out a detailed architecture design, including the division of system functional modules: login registration module, publishing service requirements module, accepting service requirements module, managing service recipients, performing public service module, token management module, and drawing the main function flow chart of the system, and the design of the table in the server database of the system. The time bank system based on blockchain technology reduces the difficulty of time token flow, realizes data tamper-resistance through timestamp technology, distributed storage guarantees data security, and reduces the difficulty of time banking system operation.

CCS CONCEPTS
•Software and its engineering~Software creation and management~Designing software~Software design engineering

Keywords
blockchain, time bank, architecture, tokenization, function module division

1. INTRODUCTION
With the accelerated development of China's population aging, the characteristics of the aging and empty nesting of the elderly are becoming more and more obvious[1].With the accelerated development of China's population aging, the characteristics of the aging and empty nesting of the elderly are becoming more and more obvious.Faced with the status of family solitary, the problem of old-age care cannot be solved by relying only on families and traditional old-age care institutions such as nursing homes."Time Bank" was first proposed by the United States, which means that volunteers store time for participating in non-profit services into the time bank, and can draw "serviced time" from the time bank when they need it. Today, time bank has been implemented in many countries and regions. As early as 2008, Switzerland has implemented a time bank pension project[2],China's Nanjing, Shanghai and other cities have also established time banks. At the current time bank, volunteers earn time token by participating in public welfare activities. Time token can not only be exchanged for the length of time they are being served, but also enjoy some social benefits. For example, a certain number of time token in Nanjing can be used for free on public transportation.

In the current time bank, the following problems still exist: 1) The problem of time points deposit and withdrawal. In today's society, the mobility of the population is increasing. Volunteers who use time bank may face the problem of unavailability of time token after relocating to other places. 2) Data trust issues. The functional characteristics of the time bank lead to a large time span, and it is difficult for volunteers to believe the validity of their time token. 3) Data security issues. At present, banks are centrally managed by the central institution, and all data is stored in the database of the central institution. Once destroyed, the data cannot be recovered. Most of the above problems exist in systems implemented based on traditional Internet technologies, so new technical means are needed to solve the above problems.

Nowadays, blockchain technology is more and more listed as the preferred technology in many fields due to its decentralization, immutability, distributed storage and other characteristics[3-5], which can better solve the above problems. Therefore, this article will design the architecture of the time bank system based on the principles of blockchain technology, including the overall hierarchical architecture design and detailed functional module division, and implement the system with the traditional Internet technology.

2. Features and Application Innovation of Blockchain

2.1 Main Technical Principles and Characteristics of Blockchain
Blockchain was originally used for Bitcoin transactions, and then gradually applied to many fields such as finance. It is regarded as the main method to solve the problem of trust[6]. The blockchain is essentially a distributed storage database. Because of its digital signature technology, smart contracts, consensus mechanisms and other information technologies, it effectively guarantees the authenticity and immutability of data, and builds a trustworthy basic environment.

Consensus mechanism is a rule that allows multiple distrusting objects to agree on the same issue. The consensus mechanism on the blockchain is that each node does not have to trust other nodes or a central institution. It only needs to trust that all nodes will spontaneously and honestly abide by pre-established rules to

achieve self-trust. And how to make each node spontaneously comply with the formulated rules is the content of the consensus mechanism. Blockchain is a chain formed by the blocks formed after each transaction is packaged together in order by timestamp[7], each node is continuously receiving the transaction information to be packaged and packaged into blocks to wait for the chain. The consensus mechanism determines the next block connected to the blockchain. The consensus mechanism is essentially some rules that stipulate that the blocks to be packaged should be packaged on the chain by nodes through certain measures, and the successfully packaged nodes will also receive some incentives. For example, nodes in the Bitcoin system will receive some Bitcoin as a reward. In this way, each node has its own interests and needs and has a competitive relationship with each other, it will hardly become a "co-op" of deception, so it can ensure that each node spontaneously adheres to the rules. The current consensus mechanisms include Proof-of-Work (PoW), Proof-of-Stake (PoS), Proof-of-Stake (DPoS) and Practical Byzantine Fault Tolerance Algorithm (PBFT)[8] .

contract is a landmark product of Blockchain 2.0. Blockchain 1.0 is dominated by virtual currencies such as Bitcoin. In Blockchain 2.0, the emergence of smart contracts has led to the widespread use of blockchain in the financial field. The symbol of the 2.0 era is Ethereum. Smart contracts are computer protocols that build and execute contracts through computer code, its operation form is: a smart contract is triggered when the condition is met, and the two parties to the transaction automatically execute the content of the contract. For example, when A completes a task, the smart contract will control B to transfer money to A. The realization of smart contracts makes it possible for blockchain-based services and also enables blockchain technology to be used in a wider range of fields.

Digital signature is an effective technology to ensure the authenticity and non-tamperability of data on blockchain. Digital signature is composed of digital digest and asymmetric encryption technology. Asymmetric encryption technology includes a pair of secret keys, public key and private key[9]. Data encrypted by public key can only be decrypted by private key; on the contrary, data encrypted by private key can only be decrypted by public key. The process of digital signature is as follows: shorten the data information to be sent to a fixed length string through a series of algorithms, which is the data digest of data information. Then asymmetric encryption technology is used to encrypt the digital summary to form a digital signature, and then the digital signature and data information are broadcast together. The node receiving the information can decrypt it with the corresponding secret key. By verifying the consistency, the node can judge whether the data has been tampered and whether the data is true.

2.2 Application Innovation of Blockchain

In recent years, the blockchain has penetrated into various fields, tracing the origin of agricultural products using the blockchain[10], power system security evaluation management system based on blockchain[11], applying blockchain technology for Digital Media Asset Copyright Protection[12] ... "Blockchain +" has become a trend. "Blockchain +" Time Bank, using the technical characteristics of the blockchain, can effectively solve the current pain points in the field of time banking. 1) The non-tamperable modification of the blockchain can guarantee the authenticity and validity of the time token of the volunteers, that is, once the time token records are written on the blockchain, they cannot be deleted or tampered with, even after decades token is still valid. 2) The distributed storage of the blockchain can ensure the security of the data, that is, each node has a copy of the data, and the possibility of the data of all nodes being destroyed is extremely low; meanwhile, the distributed storage also allows the nodes to come and go free , which reduces the difficulty of time bank maintenance.

3. Time bank system business

The use case diagram of the time banking system based on blockchain technology is shown in Figure 1, and the main user behavior view is shown in Figure 2.

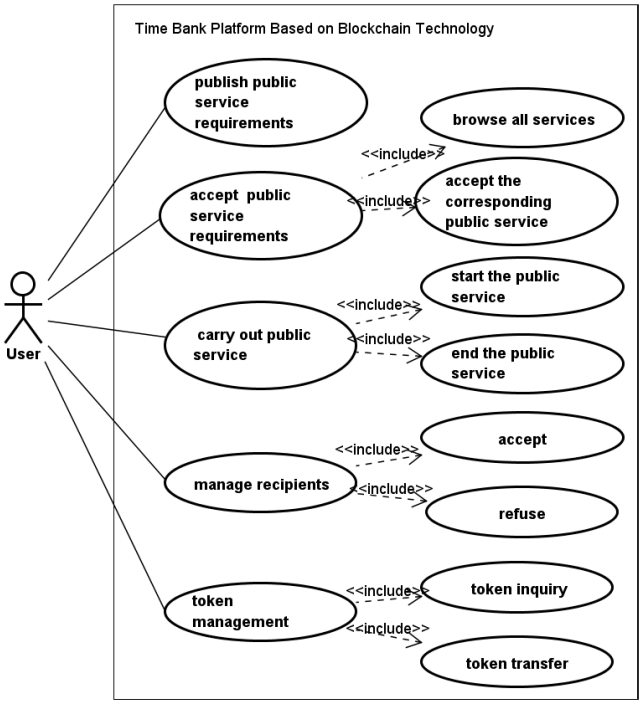

Figure 1. Use case diagram for time bank system.

1)Publish public service requirements: After logging in to the system, users can choose to publish public service requirements. On the requirements page, relevant information such as service name, service content, service time, service location, number of people required, etc. will be filled out. Then the service requirement will be published and wait for acceptance.

2)Accept public service requirements: After logging in to the system, the user can choose to view and browse all public services, can view its detailed information, and select a certain public service requirement to apply for services according to his/her own conditions, waiting for the service publisher to accept.

3)Management service provider: After submitting the service requirements, users can view the service recipients, and they can choose to accept the services provided by them or refuse according to their credit or previous evaluation.

4)Carry out public service: After the service publisher accepts the service provider, both parties can confirm that the service can be started after the service time arrives. At this time, the start time will be recorded, and the end time will be recorded when the two parties confirm the end. At the same time, the transfer of corresponding token will be completed.

5)Token management: After logging in to the system, users can check the remaining token and transaction records at any time, and they can also designate other accounts to transfer token.

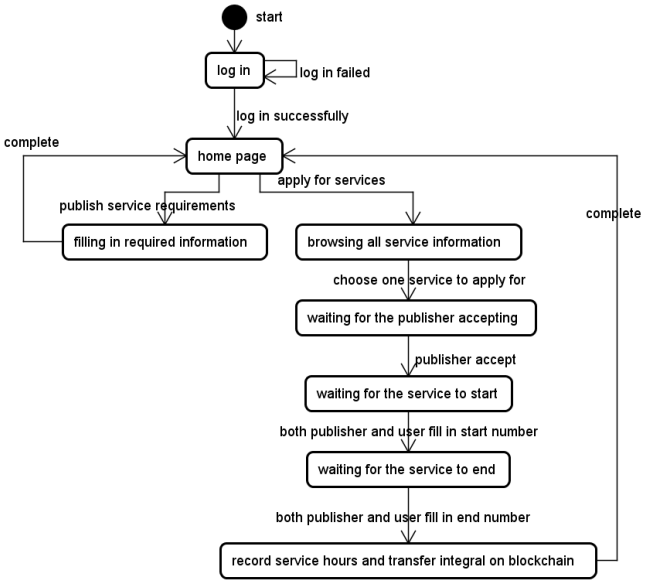

Figure 2. User behavior view in time bank system.

4. Overall Architecture Design

The time bank system designed in this paper uses the B / S structure and is divided into two layers: the application interface layer and the blockchain layer. The overall hierarchical structure of the time banking system is shown in Figure 3.

The blockchain layer mainly includes the account management module and the smart contract module. The account management module is mainly responsible for the users' account creation on the blockchain and the query of token balance; the smart contract module is also a more important module of the blockchain layer, responsible for the code logic of token issuance and automatic token transfer.

The entities involved in the system are system users and identity verifiers.

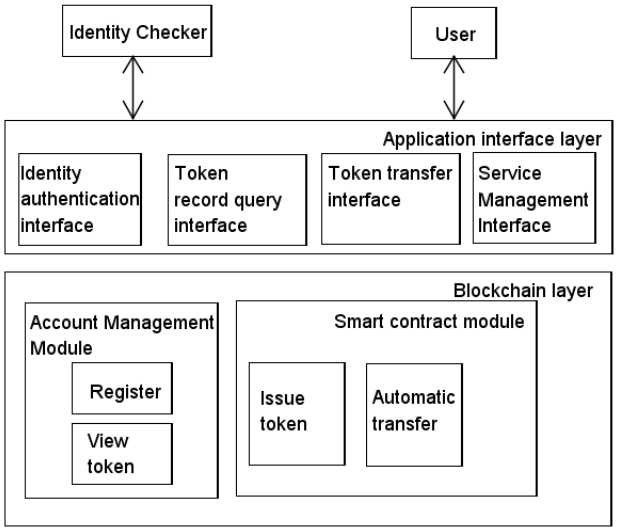

Figure 3. The overall hierarchy of the time banking system.

5. Detailed Architecture Design

5.1 Functional Module

There are six functional modules in the time bank system, which are the login and registration module, the publishing service requirements module, the accepting service module, the carrying out service module, the management of service recipients module and token management module. The functional module diagram is shown in Figure 4.

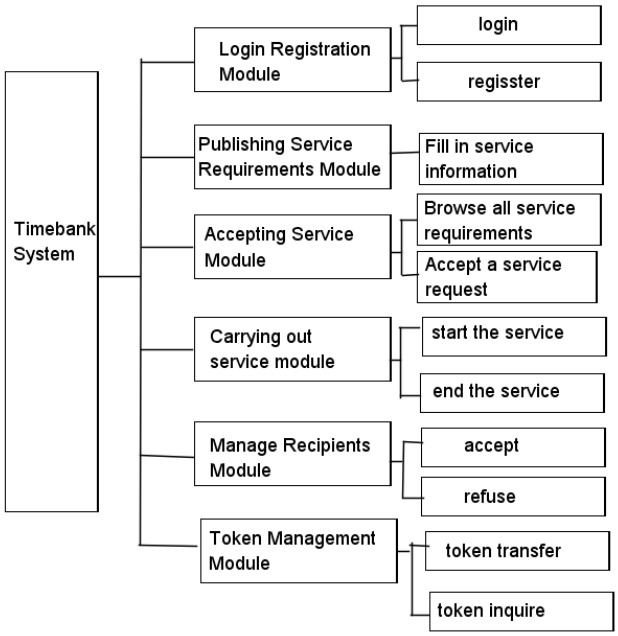

Figure 4. Function module diagram of time bank system.

1)Login registration module: The user must submit information such as mobile phone number when registering. The server receives the information data and verifies the identity through the authentication interface. After the verification is passed, the user is requested to set a username and password. After receiving the data, the server will create new account information in the database and at the same time, the blockchain is requested to establish a corresponding account. After the account is successfully created, the smart contract will issue a fixed amount of token for it. After the operation is successful, the registration is successful. The user submits the information to the server when logging in. After the server authenticates, the login is successful.

2)Publish service requirements module: The user chooses to publish the requirements, and the server requests relevant information from the user. The user fills in the requirements information including the service name, service content, estimated service start time, estimated service end time, required number of services, and service location. After server receiving the data, server will create a new service record, and return to the user after the creation is successful.

3)Accept service module: The user chooses to accept the service, that is, requests the server for alternative service requirements. The server filters out multiple records that meet the conditions from the database and returns them to the user. The user can browse and view a detailed description of a service requirement and can choose to accept it. After choosing to accept, the relevant information is passed to the server, and the server initiates a

request to the database to modify the relevant attributes of the corresponding service record.

4)Manage recipients module: After the service publisher releases the requirements, he can view the users who accept the service, that is, volunteers at any time on the "I initiated" page, and can click on the volunteers to view the user details including credit and comments, and then choose to accept or refuse. After the service publisher chooses to accept or refuse, the request is passed back to the server. The server initiates a data modification request to the database. The database modifies the "status" attribute of the corresponding service record. After the modification is completed, the server sends a prompt to the user that the operation is successful.

5)Carry out public service module: After both the service publisher and service provider confirm the start, the server will record the start time and request the database to modify the "status" attribute of the service record; after both parties confirm that the service is over, the server will record the end time accordingly to calculate the service duration and write it to the database; at the same time, the server initiates a request to the blockchain to trigger the smart contract to perform the token transfer. After the transfer is completed, the server returns the token transfer notification to the service publisher and service provider respectively; both parties also can comment on the service, and the comment will be written into the database. At this time, the public service was completely over.

6)Token management module: Users can view their own token record details at any time. The user selects "token details", and can choose the date to view the details, such as the most recent month, and send a request to the server. The server get blocks' hash from the database that records the transaction information about the user, and then initiates a request to the blockchain for specific contents of the blocks according to the blocks' hash, then the server reconstructs the contents and returns them to the user, then the user can view the token details. The user can also choose to give token. The user fills in the account of the token recipient. After the server verifies that the account exists, the user chooses amount of token to transfer. After the server confirms that the user's remaining token are greater than or equal to the amount, the smart contract is triggered to perform transfer operation. After the operation completes successfully, the user is prompted for the success.

5.2 Detailed Design of Main Functions

The main function flowchart of the system is shown in Figure 5.

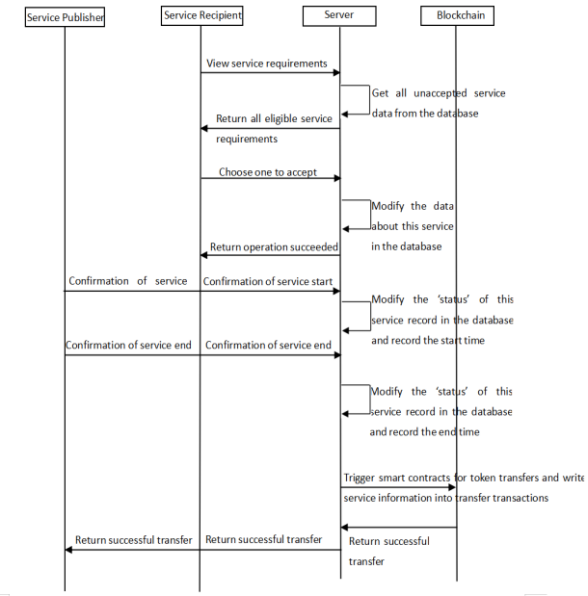

Figure 5. Functional flowchart of time bank system.

5.3 Database Design

In the time bank system designed in this paper, because the blockchain stores data at a cost and it takes a long time to read and write data directly from the blockchain, a database is needed to store unnecessary data on the chain and data to be saved in the short term. The database contains three tables: the user table, the service table, and the service record table.

The structure of the tables in the database is shown in Figure 6. The primary key of the User table is the field "tel"; the primary key of the Service table is the field "id"; the primary key of the Service Record table is the field "service" and the field "completer".

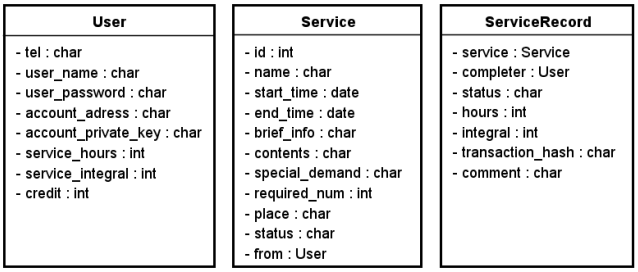

Figure 6. Table structure of database in time bank system.

6. Conclusion

Aiming at the existing problems in the current time banking system such as difficulty of time integration, data security and data trust , this paper proposes the idea of building a time bank system based on blockchain technology, and briefly describes the principles and characteristics of blockchain technology and the advantages of the blockchain for time bank: First, the timestamp technology of the blockchain ensures that the data cannot be tampered with, so that the data on the chain is still authentic and has not been tampered with even after decades; the second is the blockchain distributed storage greatly improves data security, and each node implements "autonomous management", which reduces the cost of maintaining the system. Based on the above

advantages, this paper designs the architecture of a time bank system that uses blockchain to store time credits, and realizes the basic functions of the system.

The time bank system project designed in this paper is still in the promotion stage. At present, the basic functions of the system web page have been completed. The next research work will mainly focus on the development of the mobile terminal.

7. ACKNOWLEDGMENTS

This paper was supported by National Key Research and Development Plan in China(2017YFB0803304), National Natural Science Foundation of China(7123100291546121) and National Social Science Foundation Of China(16ZDA055).

8. REFERENCES

[1] 陈际华.“时间银行”互助养老模式发展难点及应对策略——基于积极老龄化的理论视角[J].江苏社会科学, 2020:1-7

[2] 佟才录.瑞士的“时间银行”养老.思维与智慧, 2015(21):72-72

[3] Zhu YJ, Yao JG, Guan HB. Blockchain as a Service: Next Generation of Cloud Services[J]. Journal of Software, 2020, 31(1): 1-19

[4] 刘峰. 区块链热与企业机遇[J]. 企业管理, 2018, No.442(06):19-21.

[5] Feng Liu, Mengke Wang, Ji’an Tang, Xuanyong Wu, Yidan Yuan. Research on Home-Based Pension System Based on Blockchain Technology[J]. Software Engineering and Applications, 2019, 8(6): 275-282.

[6] Wu Jiying, Du Cong, Ma Zhiyuan, Zheng Gang. Blockchain Architecture Design for Food Traceability System.Computer Applications and Software, 2019, 36(12):46-50.

[7] XIE Hui,WANG Jian. Study on Block Chain Technology and Its Applications[J]. Netinfo Security, 2016(9):192-195.

[8] ZHANG Liang，LIU Baixiang，ZHANG Ruyi，et al. Overview of blockchain technology [J). Computer Engineering,2019，45 (5)： 1 -12.

[9] 药晓东,冯科.关于区块链技术应用创新与其局限性的思考.农村金融研究:2016.12

[10] 马明明.基于区块链的农产品溯源体系研究.农场经济管理, 2019(11):20-22.

[11] 姜海涛,王祥,李志,孔庆祝,黄伟.基于区块链的电力系统安全测评管理系统研究及应用.电力信息与通信技术, 2020:1-7

[12] Zhou Xiaoqian, Liu Lihua, Ren Jinluan, Cai Lin. Application of Blockchain Technology in Copyright Protection of Digital Media Assets[J]. Service Science and Management, 2019, 8(2): 75-80.

Columns on Last Page Should Be Made As Close As Possible to Equal Length

Authors’ background

Position can be chosen from:

Prof. / Assoc. Prof. / Asst. Prof. / Lect. / Dr. / Ph. D Candidate / Postgraduate / Ms.

Paper ID	Position , Full Name, Working unit & nation	Email address	Research Interests	Personal website (if any)
A2021	Prof. Liu Feng, Shanghai University of International Business and Economics, China	lsttoy@163.com	Blockchain and Finance	http://www.suibe.edu.cn/ai/2020/0114/c7528a96242/page.htm
A2021	Dr. Xiao Zilong Sun Yat-Sen University, China	shenciyou@gmail.com	Blockchain and Finance	
A2021	Ms. Xu Qing, Beijing University of Posts and Telecommunications,	3467133430@qq.com	Blockchain	

	China			

***This form helps us to understand your paper better, so please fill in the information of all authors. The form itself will not be published.**