2022 IEEE 2nd International Conference on Power, Electronics and Computer Applications (ICPECA) | 978-1-6654-4276-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICPECA53709.2022.9719286

Application of Blockchain Digital Identity Technology in Healthcare Consumer Finance System

Lin Zou
College of Business and Administration
Hunan University
Changsha, China
zoulin2800@126.com

Jin Chen
College of Business and Administration
Hunan University
Changsha, China
825275907@qq.com

Qiujun Lan
College of Business and Administration
Hunan University
Changsha, China
lanqiujun@hnu.edu.cn

Zhongding Zhou
College of Business and Administration
Hunan University
Changsha, China
acrowise@126.com

Chaoqun Ma
College of Business and Administration
Hunan University
Changsha, China
cqma1998@hnu.edu.cn

Zheng Yang
College of Business and Administration
Hunan University
Changsha, China
yangzheng@tianhecloud.com

***Abstract*—In order to solve the problems of information leakage, data silos and uncontrolled identity caused by centralized storage in the existing healthcare consumer finance system, this paper proposes a design of healthcare consumer finance system based on distributed digital identity architecture. The article introduces the overall architecture and application process of the system, and builds a corresponding demonstration system based on Hyperledger Indy blockchain technology platform, implements the key functions of the system and conducts feasibility verification. It is proved that the system model has good security and time efficiency, and can realize secure and efficient information sharing between financial institutions and financial consumers.**

Keywords—consumer finance, healthcare, blockchain, information security, distributed digital identity system

I. INTRODUCTION

Consumer finance is a modern financial service provided by legally established consumer financial institutions, following the principle of small amount and decentralization, to provide loans to individuals for consumption purposes. According to MobTech's research report, China's consumer finance business has been developing rapidly in recent years, with its market size increasing year by year from 2.3 trillion RMB in 2012 to 15 trillion RMB in 2020, which brings convenience to people's life and greatly promotes the transformation and upgrading of China's consumption and economic development[1]. Physical and mental health is the basic needs of people's lives, and in recent years, with the improvement of the national standard of living, people's demand for medical beauty, fitness, health and psychological counseling and other consumer medical and health projects is increasing day by day. According to the statistics of Analysys, the market size of medical aesthetics alone has soared from 52.5 billion RMB in 2015 to 156.6 billion RMB in 2019[2]. The emergence of consumer finance has greatly reduced the threshold of consumption, enabling more consumers to purchase the medical consumer products and services they desire[3].

In the process of consumer financial services, information management system is the key infrastructure connecting consumers, medical institutions and financial institutions, which is directly related to the smoothness, security, efficiency and quality level of services[4]. Therefore, how to reasonably optimize the design of the system to meet business needs is a great concern for developers, operation and maintenance personnel, managers and scholars [5].

It should be noted that the existing consumer financial service platforms are generally centralized, which can meet most of the business needs, but there are many challenges. Typically, consumer credit institutions have to spend a lot of time, manpower and costs to control risks. For example, in addition to verifying the identity, income, or other assets of the consumer, creditors must also verify the authenticity and legitimacy of the health care provider, as well as the authenticity and reasonableness of the cost of the health care purchase[6]. The cumbersome process and the large amount of information collected repeatedly undoubtedly discourage medical and health care institutions and consumers[7]. Despite this, malicious medical practices, fraud, loan fraud, and loan fraud are still rampant. More importantly, consumers' identity, health and consumer data are private, and traditional information systems do not provide them with reliable privacy and security[8].

Blockchain technology is an emerging technology based on distributed ledger with features of security, confidentiality, decentralization and irrevocability[9], which is a potential tool to solve the problems of social trust crisis, proliferation of false information, privacy information leakage and information silos. Blockchain can be divided into public chain, private chain and federated chain, public chain is completely public and decentralized, such as Bitcoin and Ether. Private chains can only be accessed and verified by authorized nodes, and are more centralized, such as the blockchain used by central banks to issue digital currencies[10]. The federated

chain provides a trusted technical solution for the realization of digital identity, which can effectively solve the problems of identity verification and operation authorization. It is a blockchain managed by several organizations or institutions and is more suitable for collaboration between multiple entities. This paper proposes a technical solution for a healthcare consumer financial system based on blockchain technology, which is based on blockchain digital identity technology and can effectively solve the above- mentioned challenges[11]. In particular, consumers have full autonomy over their identity data in this system, which can effectively avoid the misuse of information, and consumer credit and medical service providers can easily verify the authenticity of the information submitted by consumers, effectively prevent false information and fraudulent loans, and improve the efficiency of medical consumer credit auditing[12].

The following paper is organized in this way, first introducing the blockchain digital identity technology used in this paper. Then the design concept of the healthcare consumer finance system and the design scheme are presented, followed by highlighting the key business processes, functional modules and implementation techniques. Finally, the developed experimental demonstration system is shown, its performance, security and feasibility are explained, and relevant conclusions are drawn.

II. BLOCKCHAIN DIGITAL IDENTITY TECHNOLOGY

A. Blockchain

Distributed digital identity is based on distributed infrastructure, which gives the control of identity data to users themselves and fundamentally solves the problems of user identity privacy and data security[13].It is a new type of self-sovereign and verifiable digital identity, which completely changes the traditional centralized digital identity management mode. Blockchain, as a representative technology of distributed system, changes the attribute of electronic data that can be easily tampered with by using the data structure of hash chain, solves the data consistency problem of distributed system by using "block + consensus algorithm", and ensures that the system running across entities is not affected by the malicious behavior of a few nodes based on Byzantine fault tolerance mechanism, thus solving the trust problem at the business level. It is expected to establish interconnection protocols between service providers to ensure secure communication[14]

B. Distributed Digital Identity

In the distributed digital identity system, Decentralized ID (DID) [15] and Verifiable Claim (VC) [16] are the core components. DID is a new type of globally unique identifier defined by W3C, which is a specific formatted and unmemorable string used to represent the digital identity of an entity. A DID identifier can identify only one DID entity, but an entity can generate multiple DIDs through personal wallets (as shown in Figure 1), which can effectively avoid user identity information being associated. Each DID correspond to a DID document, which contains the public data of that DID, such as the public key, authentication protocol, and available service endpoints, and other entities can use this information to establish peer-to-peer encrypted communications with that DID entity.

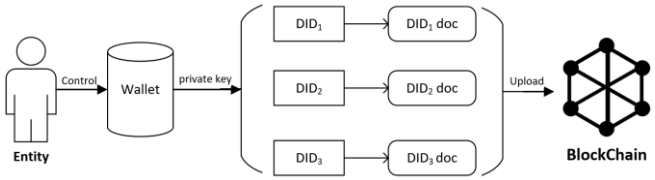

Fig. 1. The relationship between the entity user and the DID

Entity identity is represented by DID, while the attribute information of an entity is represented by a verifiable credential (VC). a VC is a tamper-proof credential signed and encrypted by the issuer, which records the attribute information associated with the identity, such as name, age, education, occupation, etc. a VC is cryptographically secure, privacy-protected, and machine-readable, and each VC has a corresponding credential schema provided by the credential issuer and. The flow of VCs in the distributed identity system is shown in Figure 2, where each participant interacts based on the DID. The credential issuer receives the identity owner request and issues the VC and uploads the abstract to the chain; the identity holder stores the credential encrypted under the chain and chooses to submit it to the credential verifier autonomously; the credential verifier, without interfacing with the credential issuer. The authenticity of the VC can be verified by retrieving the identity registry (blockchain) without interfacing with the credential issuer.

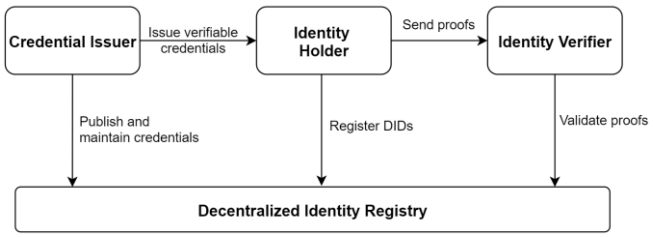

Fig. 2. Application of verifiable credentials

III. SYSTEM DESIGN SOLUTION

A. System Overview

The system introduces blockchain digital identity technology and utilizes blockchain decentralization, traceability and tamper-evident features to build a solution for the healthcare industry regarding consumer financial services. The main business participants of the system include: healthcare institutions, consumer financial institutions, healthcare consumers and government agencies. Figure 3 shows the logical model of the system, which is built based on Hyperledger Indy's blockchain open-source technology platform. Entities with DIDs are registered on the blockchain, and an identity-to-identity authentication system is established through VC, and credential schemas and credential definition information will be registered and published to the blockchain by relevant institutions and continuously maintained[17]. The responsibilities and functions of each participant in the system are specified as follows.

Definition 1: Government departments issue certificates. Government departments, as the main issuing agencies, will examine and certify the identity information of participating institutions and individual consumers, such as issuing verifiable credentials such as medical institution operating licenses, physician credentials, and personal ID cards.

Definition 2: Consumer control over identity. consumer information is a core element in the consumer finance

business, which requires continuous replenishment and improvement of consumers' static and dynamic personal information. Consumers are the managers of their personal information throughout the business system, and blockchain digital identity technology empowers each consumer to control and use their digital identity autonomously. Consumers store their identity data on their personal devices and can effectively share their identity data to verifying parties without relying on a central repository of identity data.

Definition 3: Healthcare institutions achieve efficient customer acquisition. Healthcare institutions are mainly responsible for providing consumers with consumer medical and health items such as plastic surgery, fitness and dentistry, and issuing corresponding personal health information credentials for consumers. At the same time, the blockchain system makes the information about the medical and health industry more transparent, so that consumers can more easily choose the right healthcare institutions for consumption, thus helping healthcare institutions achieve efficient customer acquisition.

Definition 4: Consumer financial institutions achieve efficient information review. Consumer financial institutions are mainly responsible for developing risk strategies, pricing strategies and sales strategies for consumer credit business after establishing cooperation with healthcare institutions, and providing consumers with medical and health consumer financial services. Its main business includes: customer risk control investigation, line management, and business decision making. By combining blockchain digital identity management technology consumer financial institutions can review multi-dimensional information on consumers, such as education, credit, income and other information, providing multi-dimensional proof and material for financial judgment.

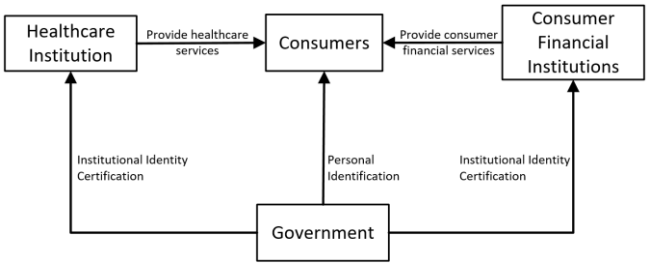

Fig. 3. System Logic Model

B. System Architecture Design

As shown in Figure 4, the basic architecture of the system is divided into four layers. Among them, the infrastructure layer mainly includes basic resources such as hardware equipment including computing servers, computing and storage facilities, networks and other hardware, and is mainly responsible for providing the required computing and storage resources for the upper layer. The application support service layer adopts a component-based design and provides basic services such as identity authentication, data encryption and decryption, and the underlying blockchain, and its functions can be extended with the development of the system. The application layer mainly provides a variety of application layer protocols to realize functions such as verifiable credential management and information maintenance, and to provide an interface for interaction between users and the network. The user layer implements different server-side interfaces by calling the lower layer structure.

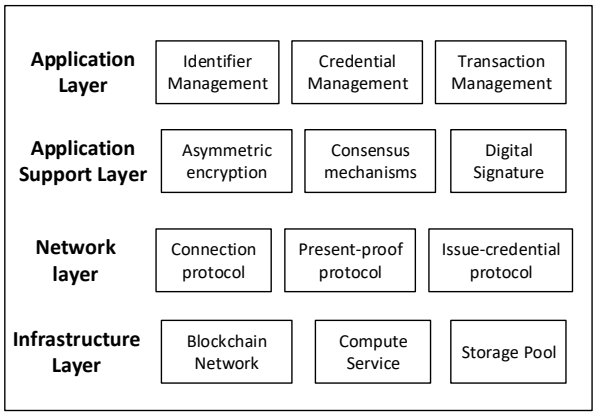

Fig. 4. System Architecture Model

C. System core function design

The core functions of this healthcare consumer finance system are mainly the identity interaction processes involved in the digital identity module, including the use of registered DIDs and establishing connections, the issuance of verifiable credentials by the government, and the verification of verifiable credentials by consumer financial institutions.

a) Register DID and establish connection

All entities interact based on DIDs, and entities with DIDs establish secure peer-to-peer data exchange channels by exchanging keys. As depicted in Figure 5, the process design for a user to register a DID and establish a connection with a healthcare institution.

- The user initiates an identity registration request to the healthcare institution.
- The healthcare institution sends a connection request, DID public key information and encrypted random numbers to the user using the public DID.
- The user uses an agent to generate a DID with which to communicate and store the corresponding key.
- the encrypted connection message, the DID's public key information and random numbers are then sent to the healthcare institution.
- The healthcare institution receives the message, decrypts it using the private key and completes verification before uploading the user-generated DID transaction to the chain.

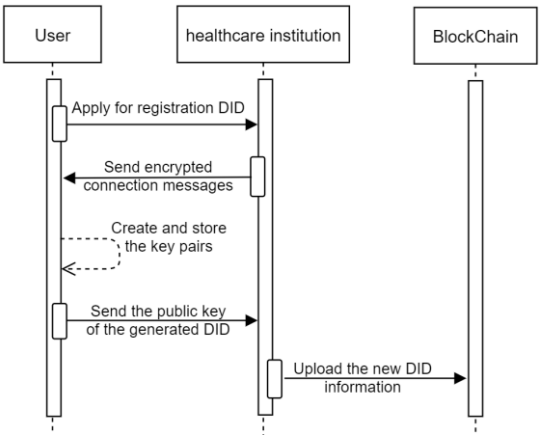

Fig. 5. Flow chart of DID connection

b) Issue verifiable credential

The identity issuer can define the name, version number, and related basic attributes of the credential schema, after which the identity owner requests credentials from the credential issuer, and the issuer issues certificates to the user and signs them for storage control by the user, Figure 6 shows the process of issuing verifiable credentials by the government.

- The government department obtains the required credential schema from the chain.
- The government department creates and publishes the corresponding credential definition based on the content of the credential.
- The user sends a credential request to government department.
- The government department creates a message used to generate the credential based on the received offer.
- The government encrypts the message with the user's public key and then signs it with its own private key, and sends the message packaged with the parameters for generating the credential to the identity owner.
- The user verifies the message, synthesizes the credentials and stores them in a personal wallet.
- The credential publisher updates the version and status of the credential on the chain.

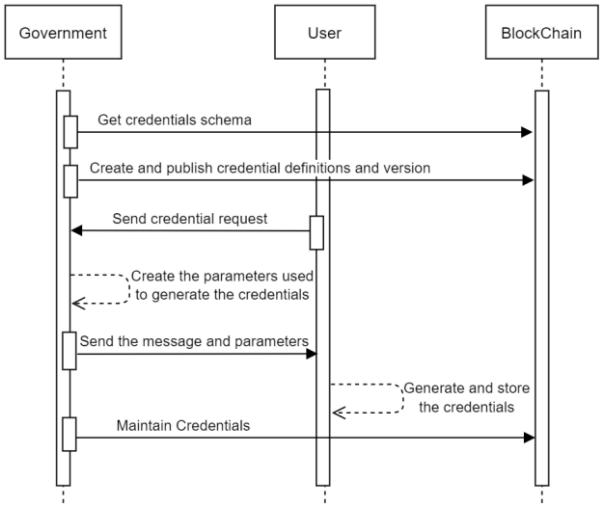

Fig. 6. Flow chart of issuing credentials

c) Verify credential information

For credential information stored in the user's digital wallet, the identity holder can choose any combination of attributes to prove. By packaging the identity information to generate a proof document for encrypted transmission to the verifier, the verifier then verifies the information in the proof document through the records on the blockchain. As shown in Figure 7, the specific process of a consumer financial institution verifying consumer identity information to complete the account opening process is shown.

- Application by the consumer to the consumer financial institution to open an account.
- The consumer financial institution sends the required proof content.
- The user receives the proof request and looks up the matching credential content from the local wallet agent.
- The user obtains valid proof content from the distributed ledger.
- The generation of proof documents using proof content and credentials.
- Encrypting the proof file using the public barium and signing it with the private key and sending it to the consumer financial institution.
- Decrypting the message by the consumer financial institution and verifying the authenticity and validity of the credential.
- Return the verification result to the consumer to complete the account opening.

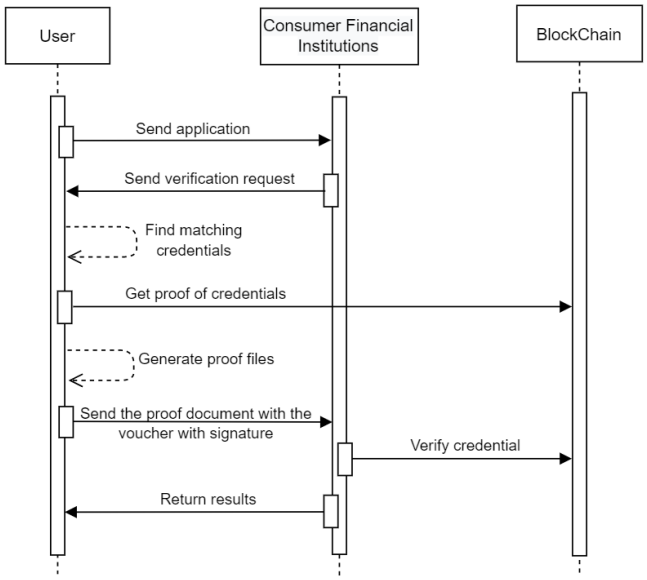

Fig. 7. Flow chart of validation credentials

IV. System Implementation

In order to verify the feasibility of this system solution, we specially designed and developed a corresponding simulation demo system. Due to the limitation of space, the following is a brief overview of the key implementation technologies such as the construction of the blockchain node network, the configuration of the initialized ledger and nodes, and the development of the functional modules and front-end interface of the system using Node.js.

A. Building Blockchain Network

The demo system is built on the blockchain network architecture of Hyperledger Indy, a digital identity project initiated by the Sovrin Foundation, which provides various modular tools and components for building a distributed digital identity network platform. The blockchain network part of the system contains three ledgers and four types of nodes, which provide different functions in the network. The three core ledgers are: Domain ledger, Pool ledger and Config ledger, where the Domain ledger is the main bookkeeping ledger, recording all identity interaction data, such as new DIDs, uploaded credential templates, revoked credentials, etc. The Pool ledger mainly records the information of all nodes in the system, such as the identity of nodes, key information and

issued credentials, etc. Config ledger is the ledger for recording configuration information, which records the configuration information of each node and the initial state of the system.

The nodes in the blockchain network are divided into four categories: authorized nodes, trust anchor nodes, verification nodes and ordinary nodes, each of which has corresponding functions and permissions, as described below.

(1) Authorized nodes: Authorized *n*odes are the highest authority nodes in the network and have the right to add other node roles in the blockchain network and to monitor and maintain the transaction information written to the ledger. Such nodes are generally written into the initial configuration of the ledger when the blockchain is created. Trust-granting nodes are generally run by industry regulators such as the Market Supervision Administration, the Banking Regulatory Commission, and the National Health Commission.

(2) Trust anchor node: Trust anchor nodes are responsible for registering new DIDs and keys to the ledger, thus enabling the formation of an authenticated and encrypted communication channel between any pair of entities. These nodes are generally run by, various consumer finance companies. When a consumer chooses to create a new DID to communicate with, the trust anchor node will upload the transaction of the new DID with the corresponding public key information to the chain.

(3) Verification Node: Verification nodes are mainly responsible for participating in the Plenum consensus algorithm, writing transaction data to the ledger, and verifying the ledger. These nodes are generally operated by credit departments and credit review departments of consumer financial institutions, which are mainly responsible for reviewing customer information and writing review results into the ledger.

(4) Ordinary node: It is mainly responsible for tracking the growth of the blockchain, providing data reading service, and can become a validation node if needed. These nodes are widely used in the mobile devices of individual users, who can check the public information on the chain, such as public DIDs, published credential definitions, etc.

Various types of nodes are responsible for different responsibilities. In realistic scenarios, often an organization can have multiple node roles, and each node cooperates with each other to maintain the ledger. The blockchain environment of this system is built using docker, which turns the system into a standardized and portable component through Linux Container technology, thus allowing the system to be developed, debugged, and run on different machines. The configuration of the blockchain network is done through the configuration file docker-compose. After completing the configuration, create the containers of the relevant nodes in turn and start the test system.

After a smooth start, you can see four running nodes and a web server image using the “docker ps” command, indicating that the blockchain network is running successfully at this point. At this point, if you visit the server's address in your browser, you should see the following screen, with four blue circles indicating that the nodes are running properly. As shown in Figure 8 below.

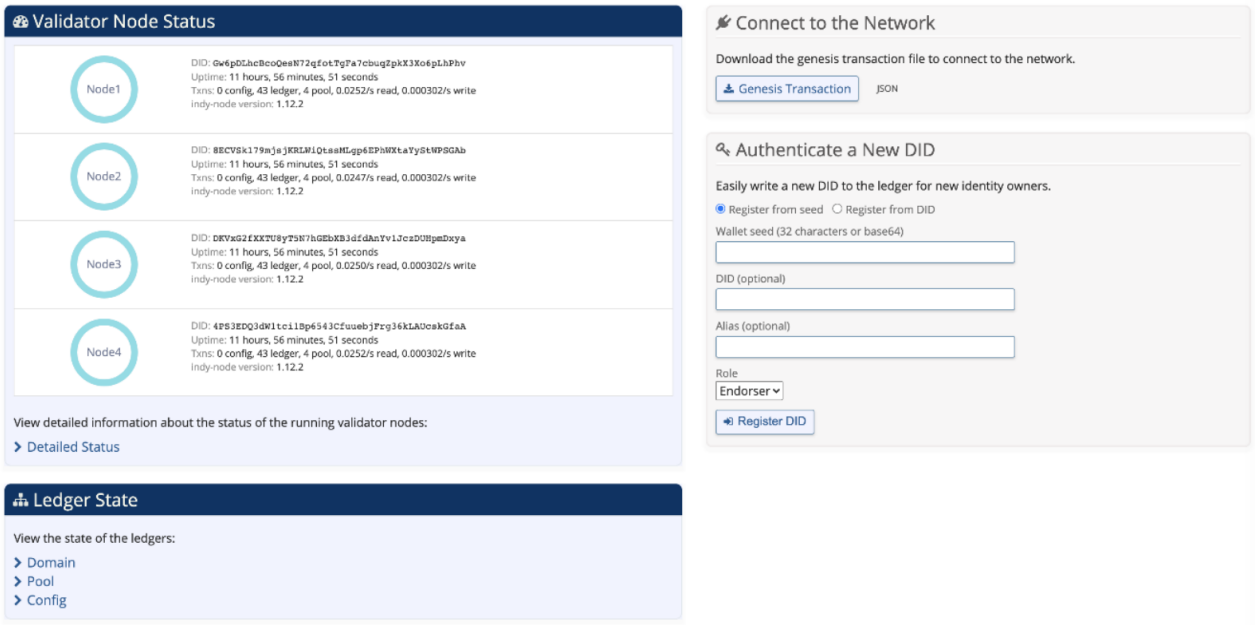

Fig. 8. Flow chart for issuing credentials

B. Function Implementation

The environment for the demo was built in VMware with Ubuntu 16.4 and Docker as the runtime environment. The virtual machine was set up as follows: 4 GB of RAM, 2 processors, and 40 GB of hard disk. the business layer of the demo system requires the use of Node.js to implement the module functionality, so Node.js needs to be installed on the server, and then interact with the underlying blockchain platform by introducing the Indy-SDK module. The module contains various methods to help developers create distributed digital identities, and by calling these methods various functional requirements of the application layer can be implemented. express is a Node.js-based web application development framework, and a fully functional website can be built quickly using Express. Therefore, this system was developed and designed using the Express framework.

The front-end windows of the demo system mainly include the DID connection interface, personal credential interface, credential issuance interface and credential verification interface. In this demo system program, the client port of the consumer (Stitch) is specified as port 3000, and the port numbers of the server side of financial institutions and Healthcare institutions, etc. are 3001~3006. After the terminal successfully starts the system, the corresponding interface can be accessed by entering the corresponding URL and port number in the browser.

V. System Simulation Testing and Analysis

A. Autonomy Analysis

To illustrate that the system functionality satisfies the autonomous and controllable nature of identity information, functional testing is performed by the following steps. In this example, user Stitch already holds a verifiable credential issued by his employment regarding his own income proof, as shown in Figure 9, which is Stitch's personal wallet interface, with his work-related information recorded on the credential and a summary record has been uploaded to the chain. In order to obtain a healthcare consumer loan, the consumer financial institution needs to verify Stitch's income first. After Stitch agrees to share the corresponding data, the consumer financial institution can verify the authenticity of his income information in conjunction with the records on the blockchain. Figure 10 shows the user's authorized access to the income information interface and the interface for the consumer financial institution to verify the information. Finally, we can see that the credential information is correct and the income situation is successfully verified.

In this process, identity information can only be shared with the verifying party after the user authorizes it, i.e., the user can independently decide with whom to share what information, ensuring the autonomy of digital identity. At the same time, the use of data needs to be recorded on the chain and monitored by regulators, so it can prevent the misuse of user identity information by consumer financial institutions or platforms to a certain extent.

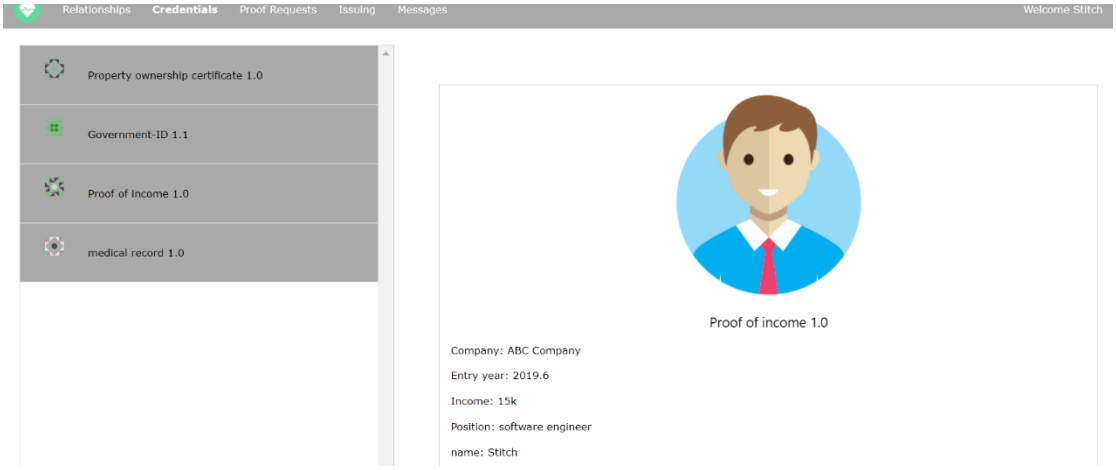

Fig. 9. Personal Digital Wallet Interface

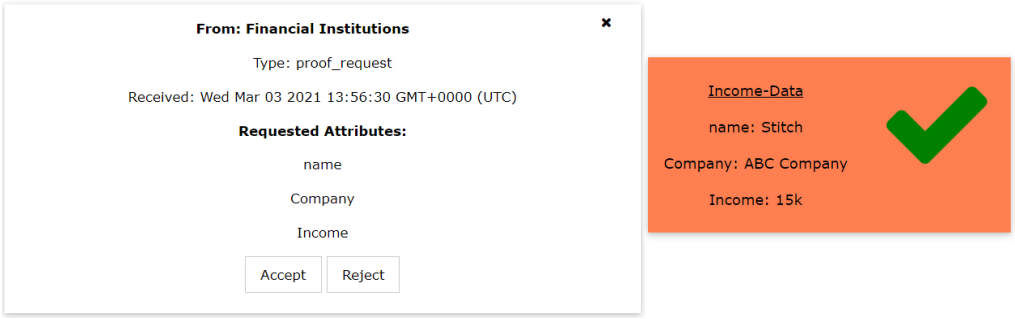

Fig. 10. Credential information authorization and verification interface

B. Security Analysis

The system designed in this paper uses digital identity technology associated with DID and VC to ensure the privacy and security of data interactions, and uses cryptographic principles to ensure the confidentiality and tamper-evident transmission of information. The process of submitting supporting information from the consumer to the consumer financial institution will be described next as an example.

Assume that the DIDs and corresponding key pairs used by both parties for communication are: healthcare consumer (DID_p, sk_p, pk_p), consumer financial institution (DID_f, sk_f, pk_f). Assuming that the consumer has the income proof credential *cred* in his personal wallet, and the issuer's public key information pk_h, credential version $epoch_v$ and credential revocation status $state_v$ etc. related to the credential are stored on the chain, the credential information verification process is as follows.

Definition 1: Generating proofs. After the consumer selects the attributes to be proved, he uses the public key pk_I of the credential to encrypt the selected credential and generates the corresponding proof document proof. Then the proof document is signed with the private key sk_p and the verifiable credential together with the public key pk_f of the financial institution to generate the identity proof message Pres and send it to the consumer financial institution. Equation

(1), (2) illustrates its encryption generation process.

$$proof(cred, pk_I) \rightarrow proof \quad (1)$$

$$Pres = encode\{sig(proof)_{sk_p}, cred\}_{pk_f} \quad (2)$$

Definition 2: Credential information validation. After receiving the identity proof message Pres, the consumer financial institution uses the private key sk_f to decrypt it and the public key pk_h of the other party to verify whether the credential has been tampered with, and then verifies the issuer of the credential, the version number and the irrevocable status of the credential. Equations (3), (4), (5)illustrate the process.

$$decode\{Pres\}_{sk_f} \quad (3)$$

$$verifysig\{sig(proof)_{sk_p}$$

$$verifysig\{sig(proof)_{sk_p}, cred\}_{pk_h} \quad (4)$$

$$verify_{cred}\,(cred, proof, epoch_V, A, state_V)$$

$$verify_{cred}\,(cred, proof, epoch_V, A, state_V) \quad (5)$$

The above is the process of credential information verification, and it can be seen that the credential data exchange between DIDs are encrypted with the key associated with the DID, and the communication is carried out by asymmetric encryption, so that even if the third party obtains the message, it cannot decrypt or tamper with the content, thus ensuring the security of the information. And each interaction with different organizations and information verification process consumers can register a new DID and key pair for communication, also effectively avoid the consumer's identity information is associated.

C. Performance Analysis

Performance issues are a major challenge for many blockchain systems, and one of the important performance indicators is transaction latency, i.e., the response and processing time of the blockchain to transaction requests. In order to test the performance of this system, this paper simulates the process of initiating credential requests from the client (user) to the server (financial institution), and records the change of response time of the server with the increase of the number of users. The test results are shown in Figure 11, where the horizontal coordinates indicate the number of users initiating the request and the vertical coordinates indicate the average response time of the hospital.

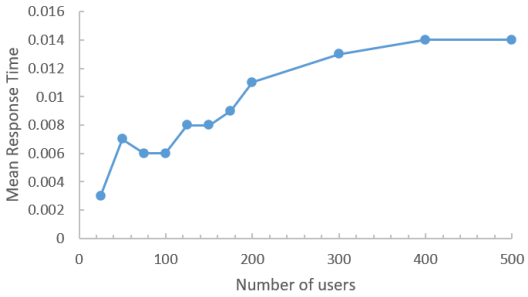

Fig. 11. Server response time

From the test results, we can see that with the increase of the number of users, the server side can still maintain a fast response rate. Although the specific response time of the server side is related to the network condition when the request command is issued, its average response time is maintained at about 15ms, and the interface display does not show obvious lag, which has a good user experience. Therefore, the system has a good performance in terms of transaction latency.

VI. Conclusion

This paper designs a blockchain-based healthcare consumer loan system based on Indy's blockchain network, which is used as a basis to upload the basic information and interaction behaviors of all participating subjects onto the chain and realize the authenticity of transaction contents and transparency of transaction process by using the features of decentralization, tamper-evident and traceability of blockchain. At the same time, this paper innovatively combines distributed identity identifiers (DIDs) and verifiable credentials (VC) model, and combines them with Indy blockchain network architecture to build a distributed digital identity credit system, which helps healthcare consumers and healthcare institutions improve their credit information construction and further simplifies the process of information review of consumers by financial institutions. Based on this, a demo version of the system is developed to validate its key technologies. From the results of the simulated interaction between the client and the server, it can be shown that the system is technically feasible in realizing the user's autonomy to control personal privacy data while effectively avoiding fraudsters from using false identity documents to obtain loans.

Acknowledgment

This research was supported by the National Natural Science Foundation of China (No. 71871090) and the Hunan Provincial Science \& Technology Major Project (2018GK1020) and the Hunan Provincial New and High-tech Industry Science \& Technology Innovation Leading Project(2020GK2005).

References

[1] Mob Research Institute. 2020 China Consumer Finance Industry Research Report [R]. Shanghai: MobTech, 2020.

[2] Econo Analytics. 2019 China Healthcare Consumer Finance Market Development Special Analysis [R]. Beijing: Beijing Econet Intelligence Network Technology Co.

[3] Li Zhongchao. Design and implementation of personal consumer credit loan management system for commercial banks [D]. Jiangsu University, 2016.

[4] Bian Lishun. Design and implementation of consumer finance business system [D]. Shanghai Jiaotong University, 2019.

[5] Ma Chi. Project Management Study on Upgrading the New System of Personal Consumer Loan of Postal Reserve Bank[D]. Jilin University, 2016.

[6] Shao, Quan Quan, Hao, Tianqi. Health risk, medical insurance and consumption[J]. Insurance Research, 2020(12):18-37.

[7] Wang Qisheng. The practice and reflection of scenario-based consumer finance[J]. China Finance,2020(14):27-28.

[8] Deng Jianpeng, Zhou Heping. How to protect financial consumers' information without "stepping on mines"[J]. China Rural Finance, 2021(6):95-96.

[9] He Pu, Yu Ge, Zhang Yanfeng, et al. A prospective review of blockchain technology and applications[J]. Computer Science, 2017(4).

[10] Zhao Lei. Legal interpretation and regulation ideas of blockchain typology[J]. Legal Business Research, 2020(4):46-58.

[11] Guo Y, Liang C. Blockchain application and outlook in the banking industry[J]. Financial Innovation, 2016, 2(1):24.

[12] Kosba A, Miller A, Shi E, et al. Hawk: The Blockchain Model of

Cryptography and Privacy-Preserving Smart Contracts[C]. 2016 IEEE Symposium on Security and Privacy (SP). IEEE, 2016.

[13] Alexander Mühle, Christoph Meinel, et al. A survey on essential components of a self-sovereign identity[J]. Computer Science Review,2018,30.

[14] Cai Yingfang. An exploration of blockchain storage methods for electronic records management applications[J]. Archival Research, 2020, No.175(04):106-111.

[15] Drummond Reed, Manu Sporny, et al. Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations [R]. W3C, Tech. Rep., 2021

[16] Manu Sporny, Dave Longley, et al. Verifiable Credentials Data Model 1.0 Expressing verifiable information on the Web [R]. W3C, Tech. Rep., 2019

[17] Deng S.H., Zhu N.H., Huang L., et al. Research on blockchain-based identity hosting model[J]. Computer Engineering and Applications, 2020, 56(4):7.