

Design and Implementation of the Digital Education Transaction Subject Two-factor Identity Authentication System Based on Blockchain

Gang ZHAO*, Bingbing DI*, Hui HE*

*School of Educational Information Technology, Central China Normal University, Wuhan, China

zhaogang@mail.ccnu.edu.cn, dbb_99@163.com, 1403669152@qq.com

Abstract—In recent years, online education service platform has swept the world due to its high quality, openness and variety of education resource, and user registered in online platform has increased dramatically. However, the traditional centralized information storage method based on the third-party may cause problems such as the loss and disclosure of the transaction subject identity data, seriously threatening the legitimate rights and interests of users. Therefore, based on education service theory, this paper applies blockchain technology to identity authentication to design and implement a blockchain-based digital education transaction subject identity authentication system. The system proposed in this study can store identity information in ciphertext form and is jointly verified and maintained by the entire network node, thus it can guarantee the security and reliability of identity data in the digital identity authentication.

Keywords—blockchain technology, chaincode, education transaction subject, identity authentication, two-factor

I. INTRODUCTION

With the rapid development of online education, more and more online education service platforms have emerged, such as the MOOC [1] (Massive Open Online Course) platform that has a great impact on higher education. As the online education service platform has the advantages of high quality and variety of education resource, the number of registered users has been increasing rapidly. The huge transaction volume requires a secure and reliable identity authentication mechanism. Traditional identity authentication relies on the authoritative attributes of the third party [2]. However, the authentication method which is based on the trusted third party often stores identity information in a central server, which will easily suffer the problem of single point of failure, and finally cause the damage or leakage of the identity data due to poor management, thereby making the legality judgment of identity untrustworthy.

Blockchain is an emerging internet database technology which is the combination of multiple computer technologies, such as distributed storage, peer-to-peer transmission, consensus mechanism, and encryption algorithm. It has the characteristics of traceability, difficulty in tampering, decentralization, and high security. On one hand, in the blockchain network, data encryption transmission and

network-wide node verification can ensure the security of identity information. On the other hand, its decentralization feature can transfer the ownership of personal identity information from third-party platform to individuals, and make data redundancy through multiple backups, avoiding the loss of identity information due to single machine failure. Based on this, this paper considers the complex distributed environment, combines blockchain technology with education transaction subject identity authentication, designs and implements a blockchain-based digital education transaction subject identity authentication system, which will store identity information in ciphertext form and be jointly verified and maintained by the entire network node, thus it can guarantee the security and reliability of identity data in the digital identity authentication.

II. RELATED WORK

The blockchain originated from Bitcoin [3], which is the underlying core technology of the Bitcoin system. In the blockchain network, data is permanently recorded, and these records are called blocks. Each block contains the hash value of the previous block (parent block); a pointer is used to point to the parent block, creating a chain that can be traced back to the first block (the genesis block). The typical blockchain structure is shown as figure1. Therefore, it can be said that the blockchain is a specific data structure that connects all data blocks in a chain manner in chronological order [4], and ensures the data not be tampered with by encryption. As the development of the blockchain, it has reached the 3.0 phase of core of the value internet. At this stage, the blockchain can be used to verify, measure, and store all the information or bytes representing the value in the Internet, enabling assets to be tracked, controlled, and traded on the blockchain. In the era of data, the identity information data registered in the network platform is already the core asset of the company and can't be estimated easily. Therefore, there is urgent need for online education service platform to establish a more secure, highly credible and highly confidential identity authentication mechanism.

As the potential digital identity authentication value of blockchain is proposed by the Ministry of Industry and Information Technology [5]. More and more research institutions all over the world have joined the research.

ShoCard and aviation IT companies collaborated to develop a digital identity authentication mechanism based on blockchain technology which was designed to simplify the identity authentication process of passengers [6]. Sony Global Education developed a blockchain-based platform to share academic level and performance record, which enabled student-related information to be delivered securely among different education institutions. In the same year, a blockchain-based identity management platform named Civic [7] was introduced to allow users to register, verify, and lock their personal identity information without forgery and fraud. A digital identity startups in Hong Kong launched a global identity storage and verification platform named ExistenceID, expecting to create a new solution for digital authentication through distributed ledgers [8]. Human biometrics can be measured or automatically verified, and it has the characteristics of extensiveness, uniqueness and stability. Therefore, biometrics have a good anti-counterfeiting performance, are difficult to be forged or stolen, and easy to carry with. However, blockchain authentication applications today which are in a biometrics authentication way are fewer, although there are still some successful applications. For example, Shocard stores personal documents on the blockchain and performs quick security checks through face matching. Hammudoglu [9] combined blockchain technology with biometric authentication, and developed a blockchain-based identity authentication system which stores fingerprints to the blockchain, but the scheme directly stores unencrypted fingerprints undoubtedly poses a security risk. To resolve this problem, this paper designs and implements a blockchain-based education transaction subject two-factor identity authentication system. The system proposed in this study can store identity information (E.g fingerprint and iris) in ciphertext form, thus it can guarantee the security and reliability of identity data in the digital identity authentication.

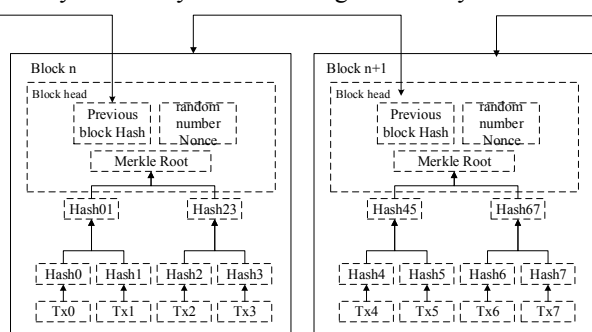


Figure 1. Block structure^[10]

III. THE DESIGN OF DIGITAL EDUCATION TRANSACTION SUBJECT TWO-FACTOR IDENTITY AUTHENTICATION SYSTEM BASED ON BLOCKCHAIN

A. The Design of System Architecture

The system adopts a hierarchical architecture, which is divided into four parts: hardware layer, blockchain network layer, chaincode layer and application layer from bottom to top. The system architecture is shown in figure2:

The hardware layer mainly provides basic hardware for the construction of the blockchain network. The system mainly implements the subject identity authentication function, so the CA node is required to issue certificates. Thus, a total of seven servers are configured in the hardware layer, in which four peer nodes, two CA nodes, and one order node are set.

The blockchain network layer mainly accepts transaction verification, achieves consistency, generates block data, and stores identity information data of all the subjects. Among the blockchain network, each node is with equal rights and obligations.

The chaincode layer mainly realizes the corresponding business logic of the system. The application layer can complete the corresponding functions by invoking the chaincode through the REST API+SDK.

The application layer mainly implements subject identity information registration, subject identity authentication, and subject identity information management functions.

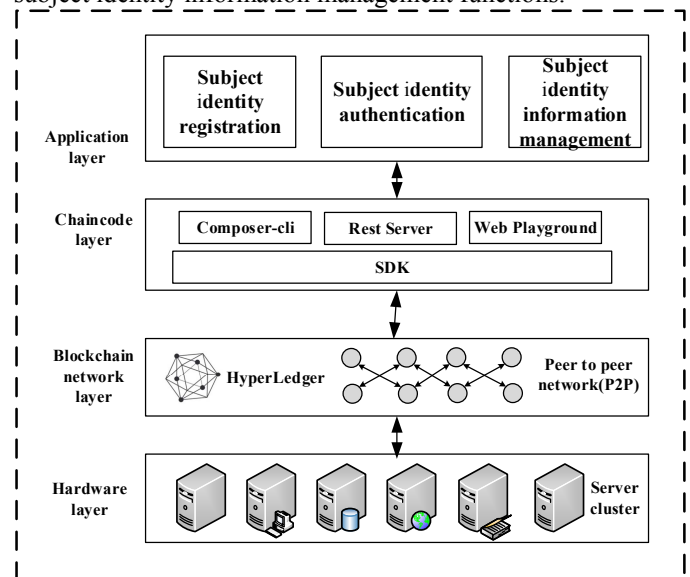


Figure 2. Subject identity authentication system architecture

B. The Design of Identity Information Model

Education service plays a very important role in the lifelong learning process [11]. It includes not only education resources, but also customized education services (such as tutoring services). By analyzing the common characteristics, we can divide the transaction subject (producers, suppliers and users) into two types: natural person user and institution user. As we all know, a well-structured and clear transaction subject identity information model can improve transaction speed and make the identity information management easier. Thus, this paper constructs identity information models for the two transaction entities types. Firstly, the basic identity information property of transaction entity, such as name, account address, user type and so on, belongs to the basic information dimension. Secondly, the education service transaction subjects have their own unique service needs, such as the need to sell education products, or to purchase these

education services on the platform. This paper attributes the different service demand to the preference dimension. Finally, this paper attributes the transaction records such as copyright information, etc. to the public record dimension. In summary, the identity information model of the subject will be constructed from the three dimensions in this paper: the basic identity information, service preferences and public records. Concretely speaking, the model of natural person user is defined as $M_{\text{natural}} = [\text{name, account address, user address, identity card number, email, password, Fingerprint, Iris, age, sexual, educationLevel, user type, transaction ID, trading time, trading event, transaction originator}]$, and the model of institution user as $M_{\text{institution}} = [\text{name, account address, institution address, Institutional business scope, Institutional unified social credit code, Institutional corporation, identity card number, email, password, Fingerprint, Iris, age, sexual, educationLevel, user type, transaction ID, trading time, trading event, transaction originator}]$.

C. The Design of System Function

The process of identity registration and authentication is shown in figure4-5:

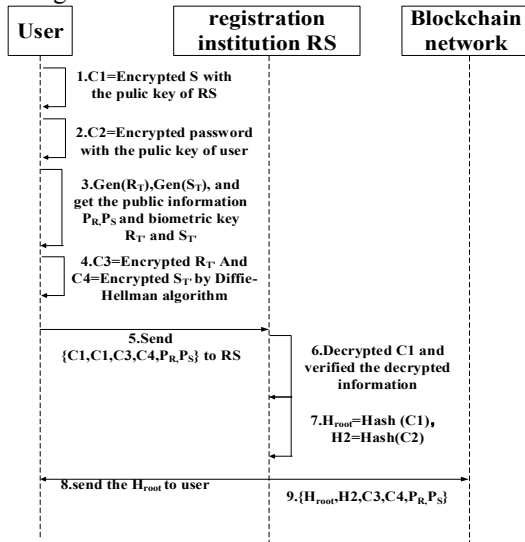


Figure 3. The registration function

1) Registration process: The identity information set $S = [\text{ID}_{\text{region}}, \text{user type, name, phone number, } R_T, S_T, \text{password}]$ is encrypted with the public key of the registration institution RS, where $\text{ID}_{\text{region}}$ corresponds to the area ID and it will be used to locate the identity chain which the user belongs to, R_T is fingerprint feature point set, and S_T defines the iris feature point set. Then the cipher text $C1 = E(\text{PU}_{\text{RS}})[\text{ID}_{\text{region}}, \text{user type, name, phone number, } R_T, S_T, \text{password}]$ is obtained. Meanwhile, we choose password and the biometrics R_T and S_T as the identity authentication factor, encrypt password with his own public key and get $C2 = E(\text{PU}_{\text{user}})[\text{password}]$, and the R_T and S_T are processed by the random key generation function $\text{Gen}()$ to generate the fingerprint key R_T' and the public information P_R , and the iris key S_T' and the public information P_S . Then, the biometric key R_T' and S_T' are encrypted through the Diffie-Hellman algorithm to obtain $C3 = E_{\text{key}}(R_T')$ and

$C4 = E_{\text{key}}(S_T')$. After receiving the information $\{C1, C2, C3, C4\}$, the registration institution decrypts $C1$ with its own private key PR_{RS} , obtains the user's detailed identity information, and verifies the registration information. If it is valid, the hash value of $C1$ and $C2$ is calculated separately, we name $H1 = \text{hash}(C1)$ and $H2 = \text{hash}(C2)$. Then RS will calculate the root hash value $H_{\text{root}} = \text{hash}(C1, C2)$ and send the H_{root} to the user. Finally $\{H_{\text{root}}, H1, C3, P_R, C4, P_S\}$ will be broadcast and recorded in the consortium blockchain.

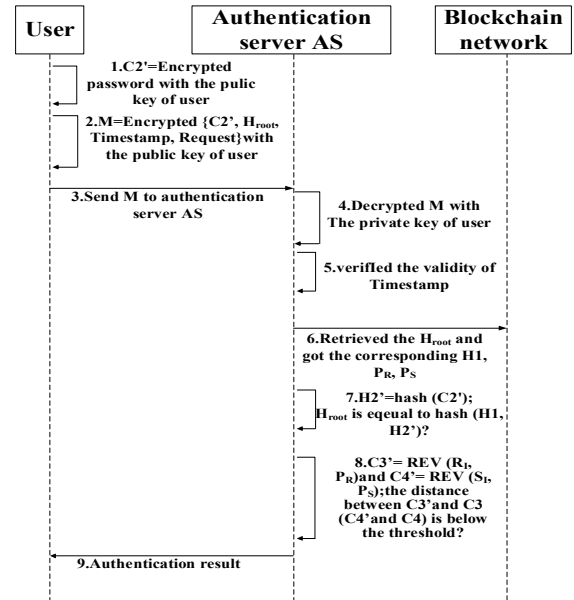


Figure 4. The authentication function

2) Authentication process: The user U encrypts the identity authentication factor password with his own public key leaving $C2' = E(\text{PU}_{\text{user}})[\text{password}]$. Then a transaction $\text{Tx} = \{C2', H_{\text{root}}, \text{Timestamp}, \text{Request}\}$ is generated and encrypted with the public key PU_{AS} of the authentication server AS, the result $M = E(\text{PU}_{\text{AS}})[C2', H_{\text{root}}, \text{Timestamp}, \text{Request}]$ is sent to AS and is decrypted with its private key. Then it will verify the validity of Timestamp. If it is valid, the AS will retrieve the H_{root} in the consortium blockchain. If H_{root} does not exist in the blockchain, it means that the identity has not been registered. If it exists, $H1, P_R, P_S$ corresponding to H_{root} is obtained. Then, the hash value of $C2'$ is calculated to obtain $H2' = \text{hash}(C2')$, and the biometrics private information $C3$ and $C4$ is recovered by the recovery algorithm REV and get $C3' = \text{REV}(R_i, P_R)$ and $C4' = \text{REV}(S_i, P_S)$. Finally whether the H_{root} is equal to $\text{hash}(H1, H2')$, or whether the distance between $C3'$ and $C3$ ($C4'$ and $C4$) is below the threshold is verified. If one of the conditions is verified, it means that the identity is legal, and then the transaction is performed, otherwise the authentication fails.

IV. THE IMPLEMENTATION OF DIGITAL EDUCATION TRANSACTION SUBJECT TWO-FACTOR IDENTITY AUTHENTICATION SYSTEM BASED ON BLOCKCHAIN

In this system, the fabric network is deployed on the Ubuntu system, using hyperledger composer to develop

chaincode and utilizing composer-rest-server to generate the API of the business logic. Each time the user submits the information, the transaction record is subsequently packaged into blocks by other nodes and recorded on the blockchain. Once the transaction record is stored in the blockchain, it cannot be tampered.

A. The Development Platform

This paper uses the web3.js class library to complete the interaction between the web page and the consortium blockchain, and builds the consortium blockchain on the Ubuntu 16.04 system with the support of the IBM Hyperledger fabric client. The development of chaincode was completed by using the Hyperledger Composer. The system development platform and development tools are shown in Table 1.

TABLE 1. SYSTEM DEVELOPMENT PLATFORM AND DEVELOPMENT TOOLS

name ^o	platform and tools ^o
PC operating system ^o	Ubuntu 16.04 ^o
development tools ^o	Hyperledger fabric1.1 + node.js ^o
Smart contract development environment ^o	Hyperledger Composer ^o
running environment ^o	PC end ^o

B. The Implementation of Function Module

1) Subject identity information registration module: It mainly completes the registration and collection of identity information of education transaction entities. The user selects the user type according to the actual situation, and proposes the registration requirement to the system. The system initiates a chaincode to review the demand, pushing the corresponding identity information model. We configure the metadata file and the network connection configuration file (connectionProfile) required for the identity card generation by registration chaincode. According to the metadata and connectionProfile file, the identity card of the registered user is generated by the IdCard class library of composer-common and imported into the identity card package. The concrete realization effect is shown in figure5.

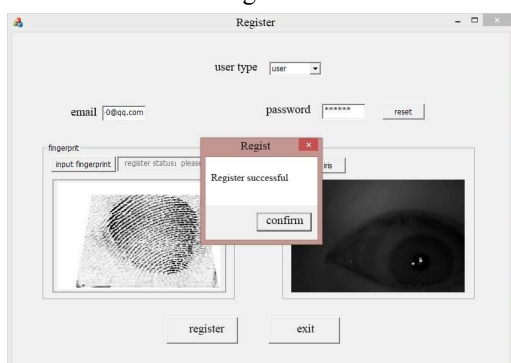


Figure 5. The snapshot of registration and information collection

2) Subject identity authentication module: The user inputs the account and password or iris and fingerprint information on the system login interface, and submits the

login request to the system. The system initiates a chaincode to review the requirement and determines the limit of authority. If the requirement is legal, the system initiates another chaincode to push the detailed identity information of the user. The concrete realization effect is shown in figure6.

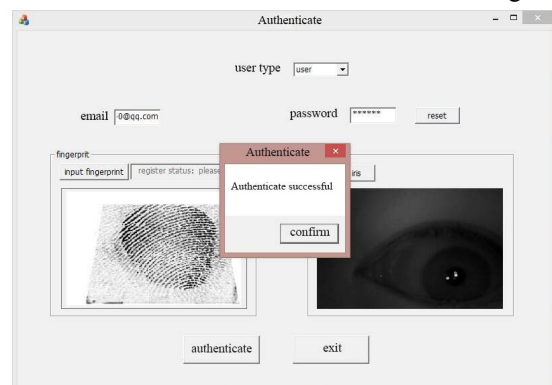


Figure 6. The snapshot of user authentication

3) Subject identity information management module: It mainly realizes the function of querying, updating and deleting. In the identity information query module, when the system receives a query request, the identity information data block will be obtained according to the ID_{identity}, and the block data is fed back to the application interaction layer. The access control of the query function is mainly implemented by configuring the permission.acl file, we adopt a rule-based matching method and set a condition “condition (r.getIdentifier()===p.getIdentifier())”, where r represents education resource and p stands for transaction subject, indicating that the query function can be provided only when the resource belongs to the transaction subject. In the identity information update module, each time the identity information is changed, a new transaction needs to be recreated. When the system receives the identity information update transaction, firstly, the transaction entity ID_{identity} is obtained according to the mapping relationship between the login account and the ID_{identity}, then a new identity information block is generated, and the update information will be added to the new block. In the identity information delete module, when the user sends a delete request, the system obtains the transaction subject ID according to the mapping relationship, and calls the delete() function to complete the delete transaction. In the end, all the corresponding identity information can be deleted. The concrete realization effect is shown in figure7.

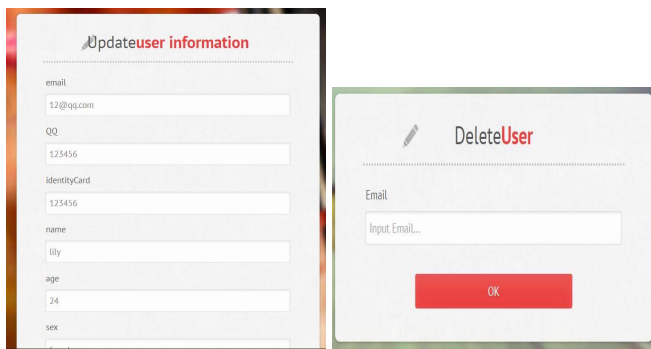


Figure 7. The snapshot of identity information management

V. CONCLUSIONS

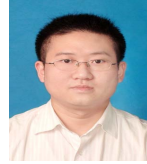
Compared with storing data in third-party organizations, blockchain technology has inherent advantages in data security. The operation of each transaction in the blockchain system is supervised by the entire network node and the data recorded on the blockchain is stored in ciphertext form and can't be tampered with. Thus, it can effectively prevent personal identity information from being maliciously altered and leaked, which brings new opportunities for solving the problem of identity fraud and information disclosure. Based on this, this paper applies the blockchain technology to the authentication of digital education transaction subject, designs and implements a blockchain-based digital education transaction subject authentication system, which enhances the security of the identity information of the transaction subject.

ACKNOWLEDGMENT

This work has been financially supported by the "National Key R&D Program of China" (2017YFB1401300, 2017YFB1401304).

REFERENCES

- [1] Li Heng. Research on Online Education Ecosystem and Its Evolution Path [J]. China Distance Education, 2017(01):62-70.
- [2] Zhou Zhicheng, Li Lixin, Guo Song, Li Zuohui. Biometric and password two-factor cross domain authentication scheme based on blockchain technology[J]. computer application, 2018, 38(06):1620-1627.
- [3] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. 2016-11-29. [https:// bitcoin.org/bitcoin.pdf](https://bitcoin.org/bitcoin.pdf).
- [4] Ana Reyna *, Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz. On blockchain and its integration with IoT. Challenges and opportunities[J]. Future Generation Computer Systems, 2018:173-190.
- [5] Su Han. The Ministry of Industry and Information Technology released the White Paper on China's Blockchain Industry Development in 2018 [J]. China Auto Parts Market, 2018 (02): 15.
- [6] Stan Higgins. The Application of Air Passenger Identity Authentication Based on Blockchain. [Online] Available: <http://chainb.com/?P=Cont&id=1027> (May 26, 2016).
- [7] Wang Yuandi, Li Jing, Hu Si. A Review of Blockchain Research[J]. Journal of China University of Mining & Technology (Social Science Edition), 2018, 20(03): 74-86.
- [8] Sally. ExistenceID uses blockchain for digital identity information storage and verification. [Online] Available: http://www.sohu.com/a/125788749_543182 (February 8, 2017).
- [9] Hammudoglu J S, Sparreboom J, Rauhamaa J I, et al. Portable Trust: biometric-based authentication and blockchain storage for self-sovereign identity systems[J]. arXiv preprint arXiv:1706.03744, 2017.
- [10] Sun H., Hua S., Zhou E., Pi B., Sun J., Yamashita K. (2018) Using Ethereum Blockchain in Internet of Things: A Solution for Electric Vehicle Battery Refueling. In: Chen S., Wang H., Zhang L.J. (eds) Blockchain – ICBC 2018. ICBC 2018. Lecture Notes in Computer Science, vol 10974. Springer, Cham.
- [11] Liu Fengyuan, Zhao Jianmin, Chen Wei, Xu Zhenguo. Exploration of Education Resource Sharing Framework Based on Blockchain[J]. Modern Educational Technology, 2018, 28(11):114-120.



Gang ZHAO was born in Jiangxi Province of China in 1981. He got his Ph.D. degree in the Department of Electronics and Information Engineering, Huazhong University of Science and Technology in 2005. He is currently a professor in the School of Education and Information Technology, Central China Normal University, Wuhan, Hubei, China. His research area include artificial intelligence and block-chain technologies.



She is a Ph.D. candidate of School of Educational Information Technology, Central China Normal University. She received B.E. degree at School of Education, Henan University in 2016. Her current research interests are in the area related to blockchain and information security.



Miss HE is a Ph.D. candidate of School of Educational Information Technology, Central China Normal University. She received B.S. degree at School of educational information and technology, Hubei Normal University in 2017. Her current research areas is blockchain and privacy protection.