LETTER

Digital education transaction object authentication service based on blockchain technology

Zhao gang¹  |  Di bingbing¹*  |  He hui¹  |  Zhu wenjuan¹

¹School of Educational Information Technology, Central China Normal University, Wuhan, China

*Correspondence

Di bingbing, School of Educational Information Technology, Central China Normal University, Wuhan, China. Email: ddb_99@163.com

With the rapid development of E-Learning, the demand for high-quality personalized education services and resources has increased rapidly. In order to meet this demand, a project called “Digital Education Crowdfunding and Crowdcreating Personalized Service Platform Development and Application Demonstration” was launched in China. The goal of the project is to provide a personalized education resource and service trading platform for producers, suppliers, and users by joint investment and collaborative creation. So how to ensure the authenticity and credibility of the objects (education resources and services) involved in this multi-party participated service platform becomes a challenging task. Blockchain is emerging as a promising technology that enables people to make secure and reliable transactions because of the decentralization and collective maintenance features. Thus in this letter we proposed a novel blockchain-based authentication service for digital education transaction object to resolve the problem of education transaction object authentication among different education institutions. We constructed information models for the two types object and stored the metadata information of the model on the blockchain to make it transparent and safe. And smart contacts are designed to authenticate education transaction object automatically among different education institutions. To improve the performance of blockchain-based authentication service, an improved consensus process for blockchain network is proposed and incorporated into our prototype system. Performance simulation is carried out and the experimental results demonstrate the practicality of our blockchain-based authentication service.

KEYWORDS: blockchain, authentication service, digital education transaction object, consensus algorithm, crowdfunding, crowdcreating, resource sharing

1 INTRODUCTION

In the era of smart education, there is an increasing demand for open and shared resources among different education institutions. Thus, a new model of innovation and personalized education resources sharing on the supply side has been a hot topic in the E-Learning area. In the context, the concept of global knowledge openness and share was proposed in the Open Courseware Project. Subsequently, UNESCO proposed the concept of open education resources. Currently, online education platforms such as Khan Academy and MOOCs have been established. The emergence of online education platform has made it a reality...
to share resources all over the world. For example Digital Education Crowdfunding and Crowdcreating Personalized Service Platform (DECCPSP) project has been initiated in China. The aim of the project is to provide a reliable, secure and efficient education resource transaction and regulatory environment among different education institutions.

However, there are some problems and challenges in practical applications: we suppose Education Resource SuperMarket is a fictional platform which is federated with different education institutions. And it can build a smart authentication application that allows real resources to be uploaded or downloaded by users with permission. When User $U_a$ (registered in institution $O_a$) wants to download resource $R_a$, Where $R_a$ belongs to user $U_b$ (registered in institution $O_b$), $U_b$ should first ascertain whether $R_a$ is real. So how to finish the authentication in multi-party participated digital education resource platform remains an unsettled problem facing us. However, the traditional authentication scheme always bases on a central server, it brings some drawbacks as follows: (1) The centralized authentication needs a server which will easily suffer single point of failure, and finally cause the leakage of the identity data. (2) The central server must be highly trusted by all sub-institutions. However, this requirement is infeasible in the multi-party participated service platform like above DECCPSP project.

Blockchain is emerging as a promising technology that guarantees a secure and reliable transaction in multi-party participated network, and it uses a decentralized network topology, distributed storage and consensus technology to securely store transaction data. So the blockchain concept has attracted widespread attention since it was first introduced by Nakamoto in 2008[2]. In the authentication field, the research in the literature focuses on user authentication by using blockchain technology. Sercan Şahan et al[3] proposed a multi-factor authentication framework, and a distributed ledger-based identity management[4] was introduced by P. Dunphy. Civic[5] was developed to allow users to register and verify their identity information without forgery and fraud. And the utilization schemes of authentication based blockchain technology[6] was proposed by Simon, J. In the other hand, blockchain technology have been incorporated into copyright management research. A blockchain-based DRM mechanism was designed and proposed Zhang, Z. Xu, R et al[7] proposed a blockchain-based digital rights management scheme for network media. And Meng, Z et al[8] provided a blockchain-based timestamp authentication for multiple copyrights. However, there is lack of resource authentication solution based on blockchain technology in the literature.

In order to overcome the shortcomings, we proposed a novel blockchain-based authentication service for digital education transaction object. In our service, the transactions can be verified in a group of unreliable participants[9]. That is to say, each node can be self-verifed, maintained and managed without the third party, thereby it can reduce the capital investment in resource review and authentication. On the other hand, in the blockchain network, each participant will store a copy of the public ledger automatically. So it also has a relatively high fault tolerance. Additionally, a improved consensus algorithm is designed to to guarantee the performance of blockchain-based authentication service. We highlight our main contribution as follows.

1) A novel blockchain-based education transaction object authentication service is proposed. The service can easily resolve the problem of single point failure, and can ensure the authenticity and credibility of the objects involved in the multi-party participated digital education resource creation and trading process.

2) Information models for the two types of digital education transaction object are constructed. The storage of the metadata of the two models in the authentication consortium blockchain can make the identity information transparent and safe.

3) An improved consensus process compared to traditional practical byzantine fault tolerance (PBFT) model for the blockchain network is proposed to guarantee the performance of blockchain-based authentication service. Experiments results demonstrate the practicality of our blockchain-based authentication service.

2.1 A NOVEL DIGITAL EDUCATION TRANSACTION OBJECT AUTHENTICATION SERVICE

2.1 An overview on the Digital Education Crowdfunding Personalized Service Platform Project

In order to meet the new requirements of high-quality personalized education services and resources, a project called “Digital Education Crowdfunding and Crowdcreating Personalized Service Platform Development and Application Demonstration” was launched in China. The program makes some efforts in achieving effective resources supply, sharing and use by joint investment and collaborative creation. In the project, crowdfunding refers to the extensive recruitment of high-quality digital education resource which belongs to different education institution or individuals (producers, suppliers and users). And the meaning of crowdcreating is to recreate some new education resources by effective utilization of the recruitment resources. In this way, it can give full play to the value of high-quality education resources, achieving absolute sharing among producers, suppliers and users. Digital education crowdfunding and crowdcreating personalized service platform is shown in Figure 1.
2.2 Education Transaction Object Authentication Service based on Blockchain

The new education transaction object authentication service firstly needs to store the metadata information of the object to the blockchain, so the information model of digital education transaction object has been constructed. Then we designed a digital education transaction object authentication service and prototype system. Finally an improved consensus process for blockchain network is proposed and incorporated to the system.

2.2.1 Information Model of Digital Education Transaction Object

Digital education transaction object refers to electronic data in non-paper media such as optical and magnetic media, digital education transaction object can be categorized into two types: the physical transaction object (often in the forms of text, images, sounds, videos, etc.) and the service transaction object (such as one-to-one counseling service). According to Information Model Specification (CELTS-3), information models for the two types of digital education transaction object have been constructed as Figure 2. The physical education transaction object information model is designed as $M_{\text{physical}} = [\text{Title}, \text{Alias}, \text{Keyword}, \text{Description}, \text{Type}, \text{Format}, \text{Size}, \text{Source}, \text{Provider}, \text{Copyright}, \text{Owner} \text{and Language}]$, and the service education transaction object model as $M_{\text{service}} = [\text{Title}, \text{Alias}, \text{Keyword}, \text{Description}, \text{Type}, \text{Source}, \text{Provider}, \text{Copyright}, \text{Owner} \text{and Language}]$. Among the information model, the Copyright field will record the access rule information of digital education resource.

![Information model of digital education transaction object](image)

2.2 Education Transaction Object Authentication Service based on Blockchain

If $U_a$ (registered in institution $O_A$) wants to upload physical education transaction object $R$ to the Education Resource Super-Market, $U_a$ need to send a upload request through a transaction $tx_c = [(tx_c)_{ID}, (R)_{ID}, \text{Title}, \text{Alias}, \text{Keyword}, \text{Description}, \text{Type}, \text{Format}, \text{Size}, \text{Source}, \text{Provider}, \text{Copyright}, \text{Owner} \text{and Language}, \text{timestamp}]$, where $(tx_c)_{ID}$ is the unique transaction ID, $(R)_{ID}$ is the unique object ID and $\theta = E[\text{Hash256}(tx_c)_{ID}, (R)_{ID}, \text{Title}, \text{Alias}, \text{Keyword}, \text{Description}, \text{Type}, \text{Format}, \text{Size}, \text{Source}, \text{Provider}, \text{Copyright}, \text{Owner} \text{and Language}]$, $SK_{U_a}$ represents the transaction signature;

Digital education transaction object authentication service $S$ checks if there already exists a register resource contract $C_C$ in the blockchain. If not, $S$ sends to a contract request transaction for a valid register resource contract $C_C$;

Transaction $tx_c$ then enters the consensus stage, $tx_c$ is sent to the consensus node set $N=[N0, N1, N2, N3]$, the primary node $N0$ will send the proposal message $<M_p, \theta>$ to the rest slave node $N1, N2, N3, N1, N2, N3$ will check if this transaction is valid,
if it is, N1, N2, N3 will send a signature message <M_s> \( \theta(i_{node}) \) to N0, where \( i_{node} \) represents the number of slave nodes. After receiving the consensus signature of N1, N2, N3, N0 will verify the signature message by using the sender’s public key. If a consensus confirmation message is sent back from all slave nodes, it is considered that the consensus has been completed. If N0 fails to receive the signature message of all slave nodes within a certain time threshold, that is to say, there are some malicious nodes. We will switch to the two-stage consensus: When \( tx_c \) is verified by N1, N2, N3, N1, N2, N3 will send a signature message <M_s> \( \theta(i_{node}) \) to all the rest nodes respectively. When the signature message is verified by N, we can say that set N has completed the consensus. Finally, the register resource contract \( C_C \) will check the submission information and response based on the preset trigger condition and response rules in the \( C_C \) automatically. Because of the limit of block size, we store the object metadata information into the blockchain to ensure block size \( \leq 1.0 \text{M} \). And the source file is stored in the local database to guarantee efficiency Transaction Per Second (TPS);

\( U_b \) (registered in institution \( O_B \)) sends an access request to the blockchain through a transaction \( tx_a = [tx_aID, H(PK_{Ub}), (R)ID, \text{Title}, \text{timestamp}] \), and \( \theta = E[\text{Hash256}((tx_aID, H(PK_{Ub}), (R)ID, \text{Title}, \text{timestamp}), SK_{Ua}] \);

Service S checks if there is an object R, which education institution the \( (R)ID \) belongs to, and if there exists an authentication contract \( C_D \) in the blockchain. The consensus node set \( N = [N0, N1, N2, N3] \) will check if this transaction is valid; if it is valid, education institution \( O_A \) will verify whether the user has the permission to use R according to contract \( C_D \) by decrypting the metadata information and compare the owner property with \( (U_b)ID \). If the values of the two are equal, S will call a download contract \( C_E \) to finish resource download automatically. In this way, digital education transaction object authentication is completed.

![FIGURE 3 Education transaction object authentication process](image1)

We have developed a system to guarantee a safe and reliable object authentication among different education institutions, the effect of the system is shown in figure 4.

![FIGURE 4 Digital education transaction object authentication](image2)
2.2.3 The Improved Consensus Algorithm

The transaction throughput in blockchain-based systems is lower than traditional centralized database systems due to the consensus computing requirement in the distributed blockchain networks. It may lead to bad system performance and the authentication service may be unpractical. So an improved consensus process compared to traditional practical byzantine fault tolerance (PBFT) model for the blockchain network is proposed to guarantee the performance of blockchain-based authentication service.

In the traditional PBFT model, each time a consensus is obtained, two times full-node broadcasts are required, which severely consumes network bandwidth. Furthermore, there is always an access control in the consortium blockchain environment, so the demand for Byzantine fault tolerance is weak, but concurrency performance is the most urgent need. To balance the fault tolerance and concurrency performance, an improved consensus process can be designed by a simplified process of traditional PBFT model.

Our simplified PBFT model divides the consensus process into two cases. Firstly, we consider the case where there is some malicious node, we degraded the three-step consensus to two-step consensus, reducing one full-node broadcast process. So in the case with malicious nodes, the consensus complexity can be reduced from $O(2N^2 - N)$ to $O(N^2)$. And in the no malicious node case, we make the client send its message to all the consensus nodes. In the way, the proposal message and pre-generated block can be generated by the primary node and slave node respectively. Thus, the slave node just needs to verify whether the data stored in the proposal message is consistent with its pre-generated block. Then, the signature message can be sent to the primary node. After receiving the consensus signature of all the slave nodes, a consensus confirmation message is sent back, it is considered that the consensus has been completed. That is to say, in no malicious node case, communication only occurs between the primary and slave nodes, canceling the communications between slave nodes. So the consensus complexity can be reduced to $O(N)$.

3 SIMULATION RESULTS

To evaluate the performance of the proposed digital education transaction object authentication service, we have carried out the simulation experiment on authentication service for digital education transaction object. The experiments were taken in a 5 virtual nodes of consortium blockchain. The authentication consortium blockchain was built on the Ubuntu 16.04 system. And the experiment was completed by using the Hyperledger Caliper.

The transaction throughput of blockchain-based system is usually measured by Transactions Processed per Second (TPS). The level of TPS directly reflects the load ability. And latency mainly refers to the time it takes to transmit in the medium. The level of latency reflects the performance to some extent. So we do the simulation experiment on the TPS and latency. The simulation result on our authentication service is shown in figure 5: (a) shows performance in TPS, and (b) demonstrates performance in latency. We can know the average TPS and latency achieved 26tps and 5.12s respectively, it proves that our authentication service is meet the need of practicality in daily life.

![FIGURE 5 The performance of blockchain-based digital education transaction object authentication service](image-url)
4 CONCLUSION AND FUTURE WORK

Combined with the consortium blockchain technology, we proposed a blockchain-based digital education transaction object authentication service in this paper, which realized the registration and authentication of digital education transaction object, and make it possible to share education transaction object among different institutions.

With the large-scale deployment of our authentication service, there will be tremendous amount of digital education transaction objects to be processed. Although the complexity of our consensus process have been reduced from $O(2N^2 - N)$ to $O(N^2)$ or $O(N)$ level, the performance of the blockchain-based system should be further improved. Thus more effective consensus algorithms will be studied and developed in the future research work.

ACKNOWLEDGMENTS

This work has been financially supported by the National Key R&D Program of China(Project No. 2017YFB1401300, 2017YFB1401304). This work is also supported by the self-determined research funds of CCNU from the colleges’ basic research and operation of MOE(No.CCNU18GF003).

References