ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202201_5(1).0057

A Lifelong Education Records Tracking Solution Based on Public Ethereum Blockchain Platform

Daoyang Ming[1], Weicheng Xiong[2, *]

[1]Huawei Institute of Information Technology, Baoshan University, Baoshan, Yunnan, 678000, China

[2]School of Mathematics and Big Data, Guizhou Normal College, Guiyang, Guizhou, 550018, China

Abstract

In order to adapt to the underlying and diversified needs of the learning-oriented society for the tracking of learners' lifelong education records, this paper designs a decentralized lifelong education record tracking solution, namely the Educhain blockchain platform solution, based on the blockchain technology. It points out that the Educhain solution takes the open-source public blockchain platform "Ethereum" as the underlying platform, and adopts the secure multiparty computation based on homomorphic encryption as well as smart contract, consensus algorithm and incentive mechanism. The Educhain solution fully combines the features of blocking chain such as security and decentralization, and forms a twin education space integrating virtuality and reality in conjunction with educational entities. It not only contributes to tracking the learners' learning records at various stages of education and promoting the distribution, sharing, analysis and application of learning data among different educational institutions, but also helps to realize the data-driven educational intelligence, and provide more accurate personalized learning support and service for learner.

Keywords

Blocking chain; Education records; Lifelong education; Ethereum.

1. Introduction

Since the United Nations Educational, Scientific and Cultural Organization proposed the concept of "lifelong education" [1] in 1965, countries in the world have entered the wave of lifelong education; the Chinese government also repeatedly emphasized to build a learning-oriented society for national and lifelong learning [2]. In the background of the times of building a learning-oriented society, how to store and track the process of educational growth of individuals at different education stages and in different educational institutions has become an important research issue in the field of educational information technology. Take Chinese higher education as an example, for the students who enter the universities after they pass the national unified entrance examination, colleges only can have preliminary understanding of their previous learning conditions through the information of their subject results in the national college entrance examination, but cannot have an in-depth and detailed image analysis on students. As a result, it is difficult for them to provide personalized learning guidance and assistance for students according to the characteristics of their learning. Additionally, despite China has established a nationally unified higher-education student information network, namely the CHSI network (websites: https://www.chsi.com.cn/), the network only can provide query of information such as student status, education background and subject results in some entrance examinations whilst it cannot adapt to the comprehensive, underlying and diversified needs of the learning-oriented society for the tracking of individuals' education records. Therefore, based on blockchain technology, the research in this paper intends to design a decentralized lifelong education records tracking solution, namely the Educhain, aiming to protect the lifelong learning record data of individual learners, and at same time realize the credible flows and secure sharing of individuals' education record data between different educational institutions, different employers such as enterprises and public institutions, and social agencies by using more secure and effective blockchain technology and with full protection of personal privacy.

2. Blockchain Technology and Proposal of the Educhain Solution

2.1. Introduction of Blockchain Technology

Blockchain technology was first applied in the Bitcoin projects in 2009 [3]. As the distributed ledger platform behind Bitcoin, blockchain technology can realize stable operation of Bitcoin network and support huge amounts of trade in the cases without centralized management. As a result, it is gradually attracting the worldwide attention. At present, various distributed ledger scenario applications based on blocking chain have been taping the increasingly great potential of the technology.

It is generally recognized that the first descriptive literature on blocking chain is the paper Bitcoin: A Peer-to-Peer Electronic Cash System, which was self-published by a mysterious people under the pseudonym "Nakamoto" in 2008 [4]. It mainly introduces the underlying working mechanism of Bitcoin system, and instead of presenting a clear definition to blocking chain, it only points out that blocking chain is a data structure to realize historical records of Bitcoin transaction ledger. In the definition given in the "Wikipedia", blocking chain, as a distributed database technology, can help support continuously increasing and tamper-proof data records by maintaining the chain structure of data blocks [5]. The core supporting technologies of blocking chain consist of distributed ledger technology, asymmetric encryption algorithm and smart contract, and it can provide guarantee of the features such as decentralization, tamper resistance, security and reliability without introducing third party intermediaries. Therefore, all the online transactions or interactions which directly or indirectly need the guarantee of third party organizations can get the benefits from blockchain technology.

Currently, blockchain technology in China has turned from the pure technological research and the discussion of application scenarios to the stage of application and implementation, and it has been gradually playing a vital role in the fields such as data storage, authentication, digital signatures, financial transactions and asset management [6]. In 2016, the China Blockchain Technology and Application Development White Paper, issued by the Ministry of Industrial and Information Technology, pointed out that the features of blockchain system such as transparency and data tamper resistance are completely applicable to the credit management, education and employment, academy, qualification certificates of students, as well as collaboration between industry and school, etc. and it has important value for the healthy development of education and employment [7]. In the 18th group study session of the Political Bureau of the CPC Central Committee in 2019, general secretary Xi Jinping emphasized to take blocking chain as the important breakthrough of the independent innovation of core technologies, and accelerate the innovation and development of blockchain technology and industries [8].

The application of blockchain technology in education draws attention from both the domestic and international educational researchers. The educational application of blockchain technology mainly focuses on qualification certificate, sharing of resources and school and enterprise consortium. It shows the following advantages: a. blocking chain can truthfully record education activities in the tamper-proof manner, and the feature of transparency that it has reflects the "Openness, Fairness and Justice" in education; b. smart contract of blocking chain can build digital contracts for the various production relations in social production and life; c. incentive mechanism of blocking chain can be used to motivate learning, for example, educational and training organizations can provide positive incentives and value guidance for students according to their achievement, contribution to activities, integrity evaluation, etc. and teachers can use virtual digital currency to reward the students for their professional innovation and outstanding performance.

2.2. Proposal of the Educhain Solution

With the advent of a new era of data-driven artificial intelligence, how to record learners' learning activities in different educational stages, and meanwhile implement a secure and effective mechanism to allow the learning data to be distributed, shared, analyzed and applied between different educational institutions, has currently become an issue that urgently needs to be solved in education. The security and decentralization feature of blocking chain provides technical support for the solution to these difficult issues.

The blockchain education application project "Learning is Earning" [9], launched by the Institute for the Future and the American College Testing (ACT) Foundation, aims to use the blockchain distributed storage technology to track the learning records of students in different stages. Based on blockchain technology, this project not only records students' academic achievement, but also records the credits generated in other informal learning activities such as school contests, social practices and community service so that students' activities at any time and in any places all can be recorded; when learners finish their studies, it will also generate an e-portfolio automatically which contain students' learning achievements in their education period. In addition, blockchain technology is also directly used to solve the authorization, management and delivery issue of educational resources between educational service providers and learners, the representative case of which is a platform named "On-demand Education Marketplace" (ODEM) [10] [11]. To avoid various intermediate links, the ODEM platform uses smart contract to realize the direct interconnections between educational service providers and learners. Learners can find all types of courses that they need through the ODEM platform, which consequently reduces the learning cost to a great extent.

The blockchain education applications in China are generally still at the early stage, and they only focus on the discussion and analysis of the educational application scenarios while there are few concrete application cases and related empirical research on specific application scenarios [12] [13]. For instance, Yang Jianmin et al [14] point out that blockchain technology has great application potential in education, and it is hopefully to play a critical role in the construction of the "Internet+Education" ecology and promoting the reform of educational system; Li Qing et al argue that blocking chain can be used to realize the distributed storage of learners' education records, establish credible low-cost certificate system for online education, etc. and as a result it can improve the openness and public credibility of education through technology.

Through in-depth analysis and survey of the domestic and international research achievements of blockchain technology in educational application, this paper proposes a lifelong education record tracking solution, namely the Educhain blockchain platform solution (which is hereafter abbreviated as the "Educhain solution"). It aims to give full play to the role of blockchain technology in educational application, solve the issue of intellectual property protection and traceability of educational resources, construct fair, objective and transparent credit records and assessment system targeting individuals and enterprises, and realize the credible reserve certificate and tracking of lifelong educational records.

3. Design of the Educhain Solution

3.1. Design Framework of the Educhain Solution

The design framework of the Educhain solution is shown in Figure 1. In the Educhain solution, educational institutions jointly create and maintain the Educhain blockchain platform, which is used to record, share and verify the results such as discipline construction, scientific research and professional training, and learners' information, academic performance, academic qualifications, qualification certificates, skills identification, honors and awards, etc.

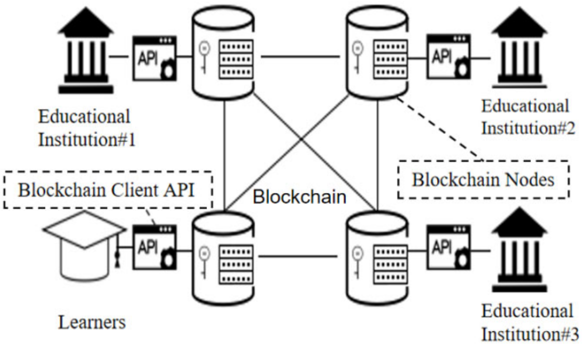

Figure 1. The design framework of the Educhain solution

The main participants of the Educhain solution are the individual learners and educational institutions. Blockchain network, as a P2P network, realizes the peer-to-peer connections between different participants. The connected nodes in blockchain network determine the validity of a certain transaction through consensus algorithm, and when the most nodes recognize that a certain transaction is valid, the transaction data will be submitted to blocking chain (public account) for permanent storage. To ensure the security of data, the data stored in blocking chain is encrypted with the private keys of individual learners.

3.2. The Detailed Design of the Educhain Solution

Considering the node records of blocking chain have the feature of tamper resistance, it can examine if the node records of blocking chain are credible, and otherwise it can find the fake information. At the same time, considering the node data of blocking chain has the feature of openness, transparency and credibility, the Educhain can be used in the unified identification, calculation and sharing of students' course credits in the following scenarios such as entrance to higher school and transfer to another school, interschool communication and combined training.

In terms of the smart contract application of blocking chain, based on smart contract, educational institutions can construct the teaching resources such as specialty courses, off-campus practices, communication of results, combined training and scientific experiments which are mutually recognized cross schools, and students can freely select the instructional curriculums and research topics of related educational institutions on the Educhain blockchain platform according to their needs for personality development. Educational institutions should build new professional training systems on the Educhain blockchain platform by means of smart contract according to the needs of scientific and technological development as well as talent market in order to facilitate the implementation and development of the Educhain solution.

In addition, by using the incentive mechanism of blocking chain, the Educhain blockchain platform can share knowledge and connect to the employment needs of enterprises to form consortium. The Educhain blockchain platform can use virtual digital currency as reward to attract teachers and students to participate in the sharing and discussion of related specialty courses, scientific research topics and innovation projects. Virtual digital currency can be used to start new topics and projects or as a reward for question answering, and it also can be used to build virtual digital banks on the Educhain blockchain platform to simulate real financial market. Connecting to enterprise consortium to link students' learning to their employment not only enables students to make career plans earlier, and meet the demands of talent market, but also provides convenience for enterprises to select the best talents.

(1) Representation of education records

To realize secure and effective data sharing and tracking, it first needs to represent individual learners' Lifelong Education Records (LR) as the basic type of data structure of blockchain Merkle tree. Merkel tree is a basic form based on binary tree, the leaf nodes at the bottom of the tree contain the stored data and its Hash value, and the values of intermediate nodes consist of the Hash values of their child nodes. The Hash value of the Merkel tree root obtained recursively can be used to quickly check the data of all the records in blocks.

The characteristic of the Merkel tree is that any change of the underlying data will be passed to their parent node until it reaches the tree root so that the block header only needs to contain the root Hash without needing to encapsulate all the underlying data. The advantage of the Merkel tree is that it can rapidly induce and check the integrity of block data, which enable its Hash calculation to efficiently run on the mobile devices such as smartphone. By using the Merkel tree, education records are represented as shown in Figure 2, in which the uppermost nodes on the Merkel tree are the root nodes of blocking chain, and the values of nodes in each level on the tree are calculated by Hash function. Each block transaction contains the following four parts, namely Hash function, signature, resource URL and index: Hash function selects the SHA256; signature is used to guarantee the private access to educational institutions or individuals; resource URL is mainly used to realize the reference to the resource locations of education records; index is used to look up learning records in order to avoid from disclosing too much sensitive information on learners' education records.

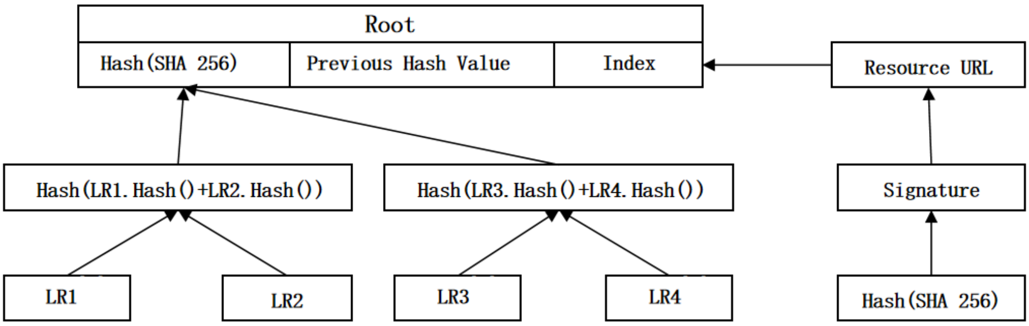

Figure 2. Representation of education records

(2) Use of smart contract

Smart contract is a transaction protocol that can be automatically executed through computer whilst smart contract in blocking chain refers to the script stored in blockchain which has the unique identity. As a programmatic agreement embedded in blockchain, smart contract provides a program-controlled software defined system which can realize the on-demand customized business process automation.

Based on the open-source public blockchain platform "Ethereum", smart contract will automatically execute the partially predefined business logic of the tracking of education records according to the latest education experience of individual learners. For example, when they participate in new training, individuals' employers or related educational institutions can automatically receive the education record information that they have updated. Through smart contract, all the business logic of the tracking of education records will not depend on a centralized system, and therefore it can effectively guarantee the private information of individual learners.

The structure of smart contract as well as the relationships between its different parts is shown in Figure 3. Specifically, smart contract mainly includes the following three parts, namely contract registry, contract summary and contract relationship. The information of contract registry mainly includes the individual account name as well as its Eth address —— it should be noted that the "Eth address" here means the public key of individuals in blockchain network, which is the unique identity of both transactions and data exchange in system; contract summary not only contains the principal information of contract, but also defines the following information such as the Policy of Records Sharing and Transferring (PRST), and execution of contract history —— in addition to data sharing and transferring, PRST in smart contract also can be used to update or adjust the mapping to a certain existing registered identity in system; contract relationship mainly include owners, information access and query, management, privilege, "mining" reward, etc. and once individuals' education records are registered in smart contract, it firstly needs to identify and judge the identity of contract callers, and further clarify the relationships between the callers and the entities defined in contract.

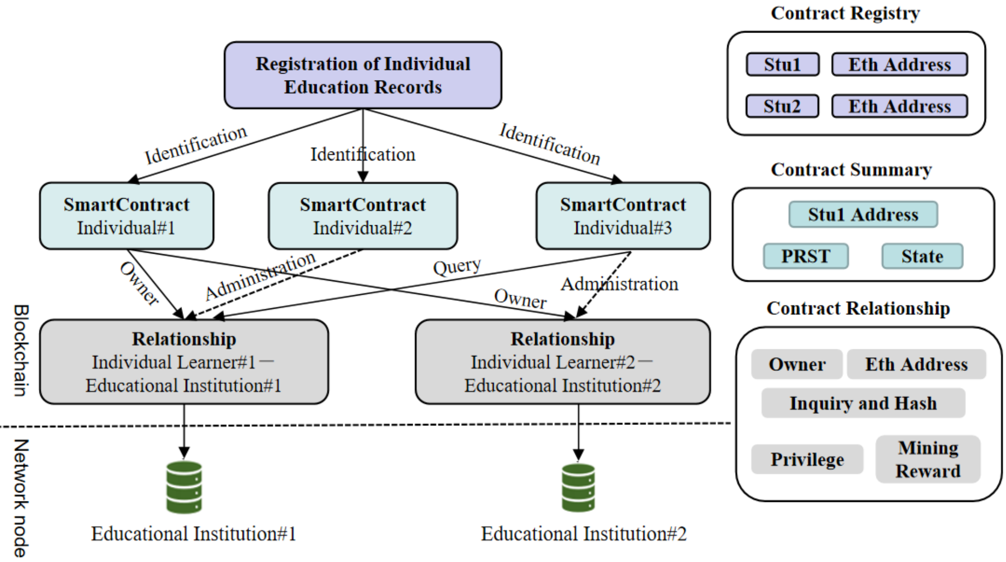
Registration of Individual Education Records
Identification
Identification
Identification
SmartContract Individual#1
SmartContract Individual#2
SmartContract Individual#3
Owner
Administration
Query
Owner
Administration
Relationship Individual Learner#1－Educational Institution#1
Relationship Individual Learner#2－Educational Institution#2
Blockchain
Network node
Educational Institution#1
Educational Institution#2
Contract Registry
Stu1
Eth Address
Stu2
Eth Address
Contract Summary
Stu1 Address
PRST
State
Contract Relationship
Owner
Eth Address
Inquiry and Hash
Privilege
Mining Reward

Figure 3. The structure of smart contract as well as the relationship between its different parts

4. Implementation and Application of the Educhain Solution

4.1. The Key Technology of the Implementation of the Educhain Solution

The Educhain solution takes the open-source public blockchain platform "Ethereum" as underlying platform, and it adopts the secure multiparty computation based on homomorphic encryption as well as smart contract, consensus algorithm and incentive mechanism. All the "transaction" participants in the network establish a mutually trusted mechanism through this network computing environment, which can simplify the design and reduce the complexity of subsequent technological realization to the maximum extent. The blockchain network contains a distributed ledger to record the transaction data of all the members in network. Blocks are the basic data structure of ledger, and they are chained together in the sequence they are produced to form the blocking chains in order to realize the logging of the changes in the state of the whole ledger. Participants in the blockchain network can update the transaction records in the ledger according to the distributed consistency protocol in the case without third party arbitration. To ensure the security and effectiveness of all the transactions in network, blocking chain adopts the following key technologies:

a. The secure multiparty computation based on homomorphic encryption. The blockchain distributed ledger technology not only can effectively record and track individuals' lifelong education data, but also can secure users' sensitive data. The secure multiparty computation uses homomorphic encryption to solve the collaborative computing problem that a group of mutually distrusted participants preserve privacy, and in the case without trusted third party, it allows participants to calculate a result together through specific logic without disclosing their own private information. Individuals' lifelong education data can be further used through the secure multiparty computation based on homomorphic encryption, which gives full play to the role of data while protecting individual privacy.

b. Smart contract. Smart contract is a set of commitments which are defined in digital form (including the agreement on how contract participants fulfill these commitments), and it constitutes of transaction processing, preservation mechanism and a complete state machine which is used to describe input information processing logic. Through smart contract, an automatic intelligent data sharing and processing mechanism can be formed between individual learners and educational institutions as well as between educational institutions.

c. Consensus algorithm and incentive mechanism. Consensus algorithm is a mechanism to ensure that only one node takes responsibility for the writing of each block in blocking chain, including the Proof of Work (POW) used in Bitcoin network and the Proof of Stake (POS) used in the "Ethereum" as the two common consensus algorithm mechanisms. Educational institutions can form trust based on consensus algorithm, and use their own resources such as brand, reputation and talent training to promote the coordination and planning of education programs, or cooperate with other educational institutions; individual learners can use consensus algorithm to obtain credit accumulation, regulate learning behaviors, make learning plans and balance capability development. Incentive mechanism is used to facilitate the sustainable development of platform, encourages nodes to actively participate in the construction and operation of blockchain system, and attract more node participants to form an ecosphere.

4.2. The Typical Application Scenarios of the Educhain Solution

The typical application scenario of the Educhain solution is shown in Figure 4. The Educhain blockchain platform is mainly composed of educational institution nodes, individual learner nodes and the "miners" surrounding the core blockchain architecture network. Based on the distributed duplication technology of blocking chain, all educational institution and individual learner nodes (including teacher nodes) contain the same replica data. Educational institutions take responsibility for adding or updating the node data such as teaching resources and students' achievement and academic certificates in the Educhain blockchain. "Miners" can be either educational institutions or teachers and students. All the records data, operation behaviors and incentive contracts on the Educhain blockchain platform protect individual privacy based on the consensus and incentive algorithm and identity-based signature and authorization of blockchain, and the secure multiparty computation based on homomorphic encryption is used to guarantee the authenticity and credibility, and traceability and tamper resistance of data.

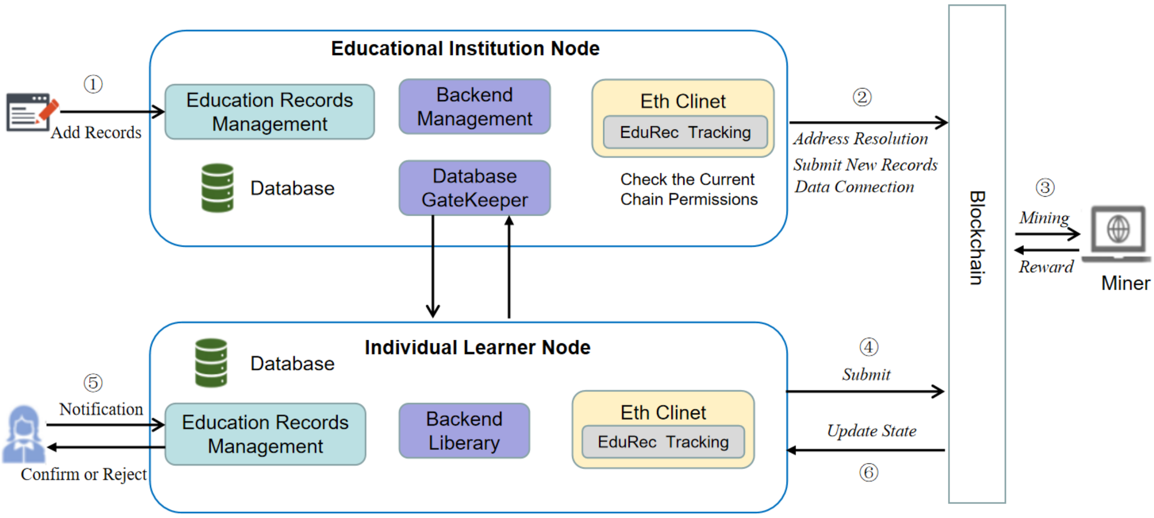

Figure 4. The typical application scenario of the Educhain solution

During the tracking of individuals' lifelong education records, the educational institutions responsible for education or training will add the following information of individual learners such as learning process records, course grade, education background, student status and certificates. For convenience of management, the information will first be added to the local database servers in educational institutions, and then be released on blockchain network through the "Ethereum" client and back-end API repository. After the database Gatekeeper checks blocking chain and confirms the right of access, use, etc. that it has, individual learners can retrieve and download the data. Considering the requirements of the learning-oriented society for individual lifelong education, learners can continuously supplement and improve their education information, and after meeting the certification rules related to the database Gatekeeper, they can submit the information to the blockchain network through the components in system.

The "mining" in the research of this paper differs from the Bitcoin "mining". The Bitcoin "mining" is a "calculation problem" facing all the "miners", and the smaller the value is, the more difficult it will be calculated as it needs huge computation capability very often to solve such a "puzzle". The blockchain "miner" in the Educhain solution proposed in the research of this paper is an instance to add blocks to blocking chain, and the system will encourage all educators and researchers involved to participate in the network "mining" as the "miners" of blocking chain; as the reward for "mining", "miners" can obtain the right to use partially anonymous data. Additionally, differing from the POW mechanism adopted by the underlying Bitcoin blocking chain, the Educhain solution designed in the research of this paper can manage to develop the distributed consistency protocol in the case without third party arbitration with low computation capability. This is mainly because the educational institutions in system are mutually trusted, and nodes themselves can provide interest certificate. Therefore, the individuals' education data records for transactions can be explained by all the authenticated authorization units, which guarantees the consistency of blocking chain to a great extent.

5. Summary

Based on blockchain technology, this paper develops research on the tracking of lifelong education records in the learning-oriented society; meanwhile, with the open-source public blockchain platform "Ethereum" as underlying platform, it designs a decentralized solution to the tracking of lifelong education records, namely the Educhain blockchain platform solution, by fully combining the following features of blocking chain such as security and decentralization. Through the Educhain solution, while enjoying the more precise personalized learning support and service, individual learners can have total control of the data rights related to their lifelong education records, prevent their individual private information from being abused, and furthermore they do not need to spend extra time and effort to manage their own education record data. Educational institutions can create an environment for joint construction and sharing of big data in education, aiming to supply each other's needs, communicate and share, and be improved together; through the in-depth and diversified image analysis on learners and the encryption of personal privacy, they can provide more secure and humanistic learning support service for learners. What needs to be pointed out is that the Educhain solution designed in the research of this paper remains theoretical currently; in the follow-up study a prototype system will be developed according to the solution, and specific empirical research will be conducted.

References

[1] Faure, Edgar; And Others.Learning To Be:the World Of Education Today And Tomorrow[M].United Nations Educational, Scientific, and Cultural Organization, Paris (France):1996:170-182.

[2] Center for Higher Education Research of National Institute of Education Sciences.Empirical Research on the Index System of "Forming a Learning Society Basically"[J].Educational Research,2012,(1):100-109.

[3] YUAN Yong,Wang Fei-Yue.Blockchain: The State of the Art and Future Trends[J].Acta Automatica Sinica,2016,(4):481-494.

[4] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[OL]. <https://bitcoin.org/bitcoin.pdf>

[5] Wikipedia.blockchain[OL]. <https://zh.wikipedia.org/wiki/blockchain>

[6] China Blockchain Technology and Industry Development Forum.White Paper on Blockchain Technology and Application Development in China(2016)[OL].<http://WhitePaperonBlockchainTechnologyandApplicationDevelopment inChina.pdf>

[7] QUAN Lixin, XIONG Qian, XU Jianbo.Transition of Learning Space and Transformation of Learning Paradigm[J].e-Education Research,2018,(8):78-84.

[8] Sharples M, Domingue J. The blockchain and kudos: A distributed system for educational record, reputation and reward[A]. European Conference on Technology Enhanced Learning[C]. Berlin: Springer, 2016:490-496.

[9] Han M, Li Z G, He J, et al. A novel blockchain-based education records verification solution[A]. Proceedings of the 19th Annual SIG Conference on Information Technology Education[C]. New York: ACM, 2018:178-183.

[10] DING Bao-gen,YANG Shu-wang,ZHAO Yu.Reality, Problems and Suggestions of the "Blockchain + Higher Education" Reform[J].Modern Educational Technology,2019,(7):45-51.

[11] Jin Yifu.Requirement Analysis and Technology Framework of Blockchain+Education[J].China Educational Technology,2017,(9):62-68.

[12] YANG Xianmin, LI Xin, WU Huanqing, ZHAO Keyun.The Application Model and Challenges of Blockchain Technology in Education [J].Modern Distance Education Research,2017,(2):34-45.

[13] Li Qing, Zhang Xin.Blockchain: A Technology to Win Open and Trust in Education[J].Modern Distance Education Research,2017,(1):36-44.

[14] Turkanović M, Hölbl M, Košič K, et al. EduCTX: A blockchain-based higher education credit platform[J]. IEEE Access, 2018,6:5112-5127.