# Design of Academic Authentication System Based on Blockchain

Zongyou, Y, Yang
Beijing University of Posts and Telecommunications(BUPT), dryang0624@bupt.edu.cn

Zhouhe, Z, Zhang
Beijing University of Posts and Telecommunications(BUPT), zhangzhouhe2020213304@bupt.edu.cn

Zijie, W, Wang
Beijing University of Posts and Telecommunications(BUPT),Wzj_cc@bupt.edu.cn

Jinyue, Y, Yang
Beijing University of Posts and Telecommunications(BUPT), SG196CM@.bupt.edu.cn

Peizhen, Y, Yang
Beijing University of Posts and Telecommunications(BUPT), yang.peizhen@bupt.edu.cn

Yuwei, M, Min
Beijing University of Posts and Telecommunications(BUPT), 2020213325@bupt.cn

**Abstract**

Abstract: The characteristics of the blockchain , such as decentralization, traceability, consensus mechanism and non tampering, have attracted the attention of higher education researchers. This paper summarizes the current situation of the application field of blockchain in higher education and analyzes and demonstrates the functions of the academic authentication system based on the blockchain.Then this paper constructs the architecture of the academic authentication system based on the blockchain consensus mechanism and provides a new technical solution for the authentication of learning achievements in the community education environment. At the same time, it looks forward to the deficiencies of the current blockchain application in the field of education.

CCS CONCEPTS • Applied computing • Education • Learning management systems

**Keywords :** Blockchain, Academic Authentication, Smart Contract

# Catalogue

## 1. SITUATION ANALYSIS

In recent years, blockchain technology has accelerated its evolution, constantly integrating with finance, logistics, energy, manufacturing, life science, healthcare, sales and other fields. Blockchain technology has also attracted the attention of higher educators. Many countries have formulated strategic plans to promote the application of blockchain higher education. For example, Estonia launched the Disciplina project, which aims to use blockchain to help students monitor their educational records and help teachers establish personal files; the Netherlands established a blockchain alliance to help higher education institutions meet the blockchain application challenge; and the German federal government funded a higher education certificate verification project based on blockchain technology.

The rapid development of information technology prompted higher education institutions to provide students with multiple forms of learning opportunities, how to record, verify, share all forms of learning, realize the data exchange between students, higher education institutions and potential employers, avoid education record fraud, and protect the copyright of open education resources has become the challenge of higher education institutions. In the field of education, blockchain applications have the advantages of reliable, credible, safe and high efficiency, with the ability to store, transmit, verify test reports, academic performance, academic achievements, career interest, diploma and so on. Through distributed data storage, peer-to-peer transmission, consensus mechanism, encryption algorithms and other technologies, blockchain allows students to control their own data, simplify the activities of educational institutions, improve the security of data access and verify students' academic qualifications, which provides support for higher education institutions to meet the challenges of informatization. Currently, different educational institutions are trying to use blockchain technology to meet the challenges. For example, the Holburton School uses blockchain technology to help students record learning behavior and classroom activity performance; the Lithuanian BitDegree platform provides learning opportunities for employees to record and verify test scores, homework, and problem solving skills, and supports the use of Bitcoin to pay for course fees and apply for scholarships.

The results of the research show that the main areas of blockchain higher education applications include digital certificate management, fees and reward / funding and student employment, as shown in Figure 1. Among the selected sample, 25 higher education institutions (66%) use blockchain technology to issue, store, share and certified digital certificates; 10 higher education institutions (26%) allow students to pay tuition fees, grant scholarships, grants and donations, etc.; 9 higher education institutions (24%) use blockchain technology to link students, educational institutions and potential employers to help students find jobs. Blockchain has few applications in enrollment, digital identity, learning files, evaluation and guidance, learning environment, credit transfer, data review, academic activities, knowledge protection, etc. Selected samples, using the block chain technology record learning files, for students and teachers to evaluate and guidance, manage the learning environment of higher education institutions each have 3, using block chain technology, credit transfer and knowledge protection of enrollment of institutions of higher education each has 2, using block chain technology management digital identity, audit data of higher education institutions each have 1, no higher education institutions using block chain technology management of academic

activities.

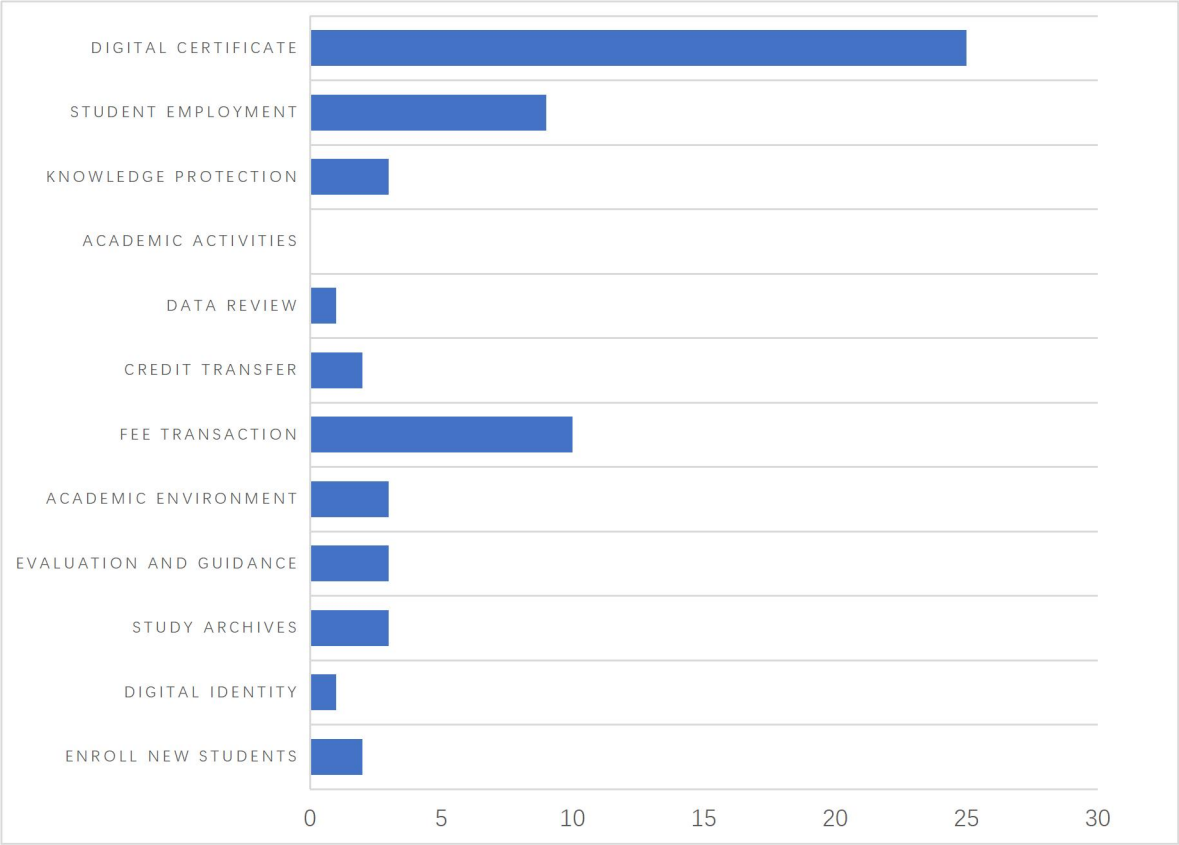


Figure 1: the main areas of blockchain higher education applications

Blockchain technology can realize multi-input, distributed storage of data, deal with the lack of trust caused by multi-input, realize non-intermediary transactions, automatic transactions according to specific rules, use transaction logs for verification, and realize value storage, etc. Under the background of the rapid development of information technology, blockchain technology has a positive role in higher education reform. It can not only carry out an all-round and accurate portrait of education, give students the autonomy and control over their learning records, improve the work efficiency of higher education institutions, but also promote the reconstruction of the new relationships between higher education institutions, students and potential employers. At present, higher education institutions apply blockchain technology to different educational situations in various innovative ways, among which digital certificate management, cost and reward / funding, and student employment are the most important applications. At the same time, higher education institutions have begun to explore the application of blockchain technology in learning archives, evaluation and guidance, learning environment, credit transfer, knowledge protection, digital identity and data review.

However, most higher education institutions have only proposed relevant plans or are in the pilot test stage. The application of blockchain technology in the field of higher education is still in the initial stage, and its widespread application still faces many problems and challenges. From the technical perspective, the application of blockchain technology in higher education faces challenges such as scalability, integration, data privacy, data security, delay and standardization; From the promotion perspective, the blockchain technology education application still has low promotion degree, large digital divide and high implementation cost. Higher education institutions should be fully aware of the advantages and disadvantages of blockchain technology, eliminate the obstacles of applying blockchain technology, and seize the opportunities of blockchain reshaping higher education in the future.

Higher education institutions should strengthen the research on blockchain technology and improve the maturity of blockchain technology. Although blockchain technology can achieve data security through decentralization, it still faces the risk of being attacked. Higher education institutions should avoid the problems such as data tampering and leakage, protect the data privacy and security of students, teachers and institutions, strengthen the mapping relationship between students' alias and real identity, and avoid the data monitoring problems caused by the excessive anonymity. At the same time, we should also improve the scalability of blockchain technology and break the bottleneck of low blockchain transaction speed, in order to meet the challenges of the large number of students and huge education data in higher education institutions. In addition, higher education institutions should design or choose simple operating interface platforms or programs to provide technical support for all teachers and students to improve the availability and acceptance of block chain; increase the cost of blockchain application, encourage researchers to strengthen the design and development of blockchain technology platform or program, purchase data storage equipment and application equipment, and ensure data storage and management.

## 2. SYSTEM REQUIREMENT AND FUNCTION ANALYSIS

To cope with traditional academic certificates that are forged and improperly kept unilaterally by educational institutions, while exploring the application of promoting blockchain technology in the fields of academic certification, job seeking and employment, and improving the credibility of digital certification. Propose the use of blockchain to deal with issues related to certificate authentication

The trusted authentication system based on blockchain mainly relies on the consensus mechanism of blockchain, which can effectively increase the credibility of authentication. Its academic degree authentication mechanism mainly has the following characteristic features, which make the blockchain-based authentication system designed by it have the characteristics of non-tampering, non-repudiation and decentralisation. Relying on the smart contract mechanism in the blockchain, the authentication process is carried out strictly in accordance with the contract requirements, without human involvement, and the trustworthy mechanism is neutral and secure.

Generally speaking, for a certificate management process, three parties are involved: the issuing authority, the certificate holder and the certificate verifier.

For traditional certificate management platforms, digital certificates convert existing paper certificates into electronic data, which are uploaded by the issuing authority to a third-party certificate registration platform for validation with the help of digital signatures.

In the blockchain system, the certification authority is responsible for importing data from the original data system and checking the certificate results. After importing the data, the certification authority signs the certificate and stores it on the chain, and confirms the authenticity and validity of the certificate. Each certificate is given a unique digital identifier, which serves as an "ID" for circulation on the chain.

For the certificate verifier, there is no need to manually verify or check the authenticity of the certificate with the issuing authority, but to directly initiate a certificate verification request and verify it through the blockchain certificate management platform.

Any operation on the certificate management platform, such as adding a certificate, requires the caller to be authorised by a registered certification authority.

Therefore, for certificate holders, in addition to academic certificates, they can also submit other skill level certificates to the certification authority, which will be reviewed by the certification officer and added to the blockchain ledger, together with the certificate record.

Taking a degree certificate as an example.

(1) The Education Bureau unifies the uploading of academic degree certification information and skills certification assessment certificates directly under the Ministry of Education. The unified entry by the Ministry of Education ensures the authenticity and reliability of the data source and also improves the efficiency of the entry, preventing the information entered by various institutions from being out of sync and causing some inconvenience to users.

(2) The school enters information about each semester of a student's studies, including the semester's GPA, awards, sanctions and overall performance, which reflects the student's learning situation. It is also possible to check the learning status of students in school, making it easier to manage them.

(3) Training providers upload the assessment criteria for each course and record them in the system so that they can be reviewed. At the end of each course, the student's performance throughout the course will be uploaded and a certificate of competence for the course will be uploaded for those who have passed the assessment.

(4) The BIA will audit the training providers' participation in the blockchain and will conduct inspections at certain times based on the assessment criteria uploaded by the training providers to prevent training providers from issuing certificates in bad faith.

(5) Individual users can check all their skills certificates and academic degree certification information, and check all semesters of study at the school according to the graduation institution of the academic degree.

(6) Employers can check the authenticity of a candidate's academic and skills certificates, as well as his or her performance and studies during the period of qualification, in order to make a better selection.

However, it is clear that the above-mentioned functions alone are not enough to exploit the advantages of blockchain. For the relevant chain described in this paper, the following technical challenges need to be realised.

(1) User identity security authentication: certificate authentication involves the flow of personal information. Educational resource sharing platforms often hold a large amount of

In order to ensure the privacy and security of users, anonymous user identities are used and the private keys of users are kept in their own hands.

(2) Two-way authentication: In the process of certificate authentication, not only is the user authenticated by the institution, but the user is also authenticated by the institution. Two-way authentication can increase the trust of users and increase the usage of users. It is also possible to detect malicious behaviour of users or organisations in time.

(3) Malicious user traceability: For education resources sharing, the number of users is large. This ensures that when a malicious user appears in the system, the malicious user can be recorded on the local and cross-domain blockchain in a timely manner, and the user can no longer be served. This will prevent malicious users from re-registering with other institutional nodes.

(4) Trusted metric mechanism

A trustworthy metric mechanism is adopted to measure the trustworthiness of the static and dynamic behaviors in the chain, and the trustworthiness is fed back to other nodes in the network in time to ensure the real-time trustworthiness of the authorized node set.

Translated with www.DeepL.com/Translator (free version)

## 3. SYSTEM ARCHITECTURE AND FEASIBILITY ANALYSIS

### 3.1. System Architecture

The system architecture of the blockchain-based academic certification is shown in Figure 2. The system can be divided into 3 modules, view layer, functional layer and blockchain layer.

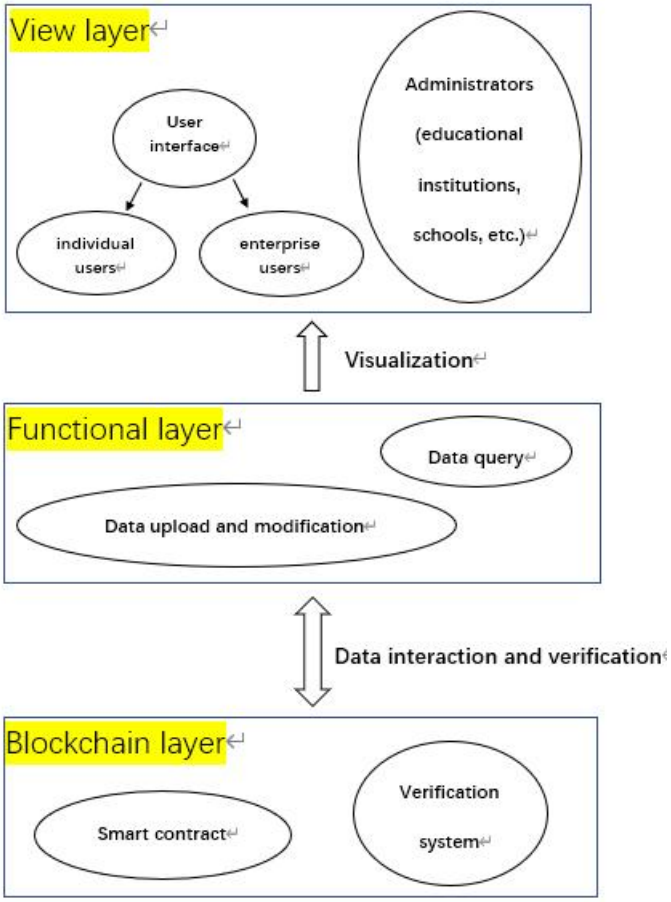


Figure 2: Schematic diagram of system architecture

#### *3.1.1. View layer*

The view layer is mainly used for non-core business logic processing and interface display. Sensitive information cannot be stored, and all core data needs to be extracted from the blockchain. Therefore, in order to improve efficiency, it is optimized in two aspects. On the one hand, data persistence is improved to improve the time for the view layer to cache data. On the other hand, when the authorized node set is screened, trusted nodes with higher performance are preferred to achieve the purpose of quickly providing data to the view layer.

The view level is mainly divided into 3 types of operation interfaces, individual users, enterprise users and administrators (educational institutions, schools, etc.), to meet the operational needs of mobile end and web end, will use HTML5 standards to develop front-end web pages and WeChat Mini Program to develop mobile end pages.

### *3.1.2. Functional layer*

The functional layer mainly performs data query, upload and modification.

The write function will complete the academic information provided to individual users, such as: personal information, school grades, and proof materials, such as: scanned copies of award certificates, and enter them into the system. The process is as follows: 1) The system pops up the resume input window after receiving the instruction to request input information. 2) The user fills in the academic information and uploads the proof materials in the form of a file. 3) The system transmits the received information to the blockchain layer for verification, and it will be put on the chain after the verification is successful. Enterprise users and administrators cannot use the write function.

The modification function meets the needs of individual users to modify the wrong resume information and the administrator to deprive them of their degrees. After the user sends a modification application, he needs to fill in the resume information again and submit it to the system. The system will verify the authenticity of the received information again, and store the information on the chain if it is correct. Otherwise, the user will be prompted again to verify the correctness of the information. The administrator cannot directly modify the user's academic information. In the process of implementing the "modification" function, the essence is to add an invalidation statement to the user's corresponding academic information.

The data query function is for ordinary users and administrators. The system reads the requested data from the blockchain and provides it to the user. Users are divided into individual users and enterprise users. The difference is that individual users can only view their resume information, while enterprise users can view the academic authentication information of all candidates. After the user sends a viewing request to the system, the system will first determine the user type. Yes, individual users will find the corresponding academic authentication information according to the user's identity authentication information, and then show it to the user; if it is an enterprise user, submit an application to the individual user according to the condition information provided by it, and return the corresponding information after obtaining authorization.

Data storage is the core function of the system. The data storage module provides data access services to other modules in the system. Due to the large amount of data to be stored and the few change operations, the erasure code redundancy algorithm can be used for data handling and storage at this stage.

The module generally uses the RS code in the erasure code as the main coding and decoding method. The core idea is to sharding the received database first to obtain k sharding data. Then add m check data through RS coding to form n coding data, and store the coded data on the chain. When performing reduction, the system reads coding data from more than or equal to k alliance chains, and can be multiplied by generating the inverse matrix of the corresponding data matrix and the coding data column vector to obtain the original data source.

### *3.1.3. Blockchain layer*

A smart contract is a set of digitally defined conventions, including agreements on which contract participants can enforce those conventions. The basic idea of a smart contract is that various contract terms can be embeddings into the hardware and software people use, making it costly for attackers to attack [1].

In short, smart contracts are contracts that are automatically executed by programs that replace legal language with computer language to record terms.

This concept was proposed by cryptographer Nick Saab in the 1990s. Due to the lack of a trusted execution environment at that time, smart contracts were not applied and developed. It was not until the emergence of Ethereum that smart contracts were "resurrected". Its operation process in the blockchain is shown in Figure 3

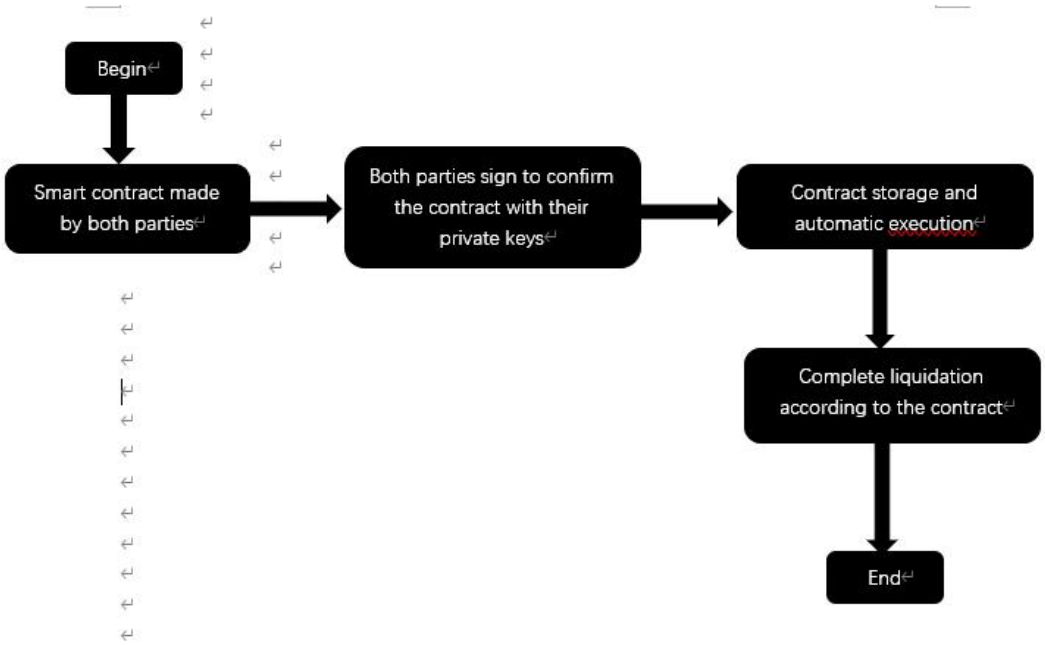


Figure 3: A smart contract operation process in the blockchain

Compared with traditional contracts, smart contracts have three characteristics:

1. The content of the contract is open and transparent

Smart contracts are deployed on the blockchain, and their contract content can be queried by all nodes.

2. The content of the contract cannot be tampered with

Like the transaction information in the block, if the attacker wants to modify the contract, he needs to continuously calculate the hash value of the parent block until the genesis block. The whole process requires at least 51% of the computing power of the entire block chain system, so the content of the contract can hardly be tampered with.。

3. Permanent operation

The smart contract running on the blockchain is also jointly maintained by the network nodes on the blockchain. As long as the blockchain is there, the smart contract can continue to be maintained and run.

Therefore, compared with traditional contracts, smart contracts mainly have the following advantages:

1. To trust.

Because the content of the smart contract is open, transparent and cannot be tampered with. It greatly enhances the trust between both parties to the transaction, thus promoting the safe conduct of the transaction.

2. Economical and efficient

Compared with traditional contracts, disputes often arise due to differences in understanding of contract terms; smart contracts can avoid differences through computational language, thereby reducing the cost of reaching consensus.

3. No need for third-party arbitration

Smart contracts execute automatically based on the final result, thus avoiding third-party arbitration.

In this system, the operation process of the smart contract is as Figure 4

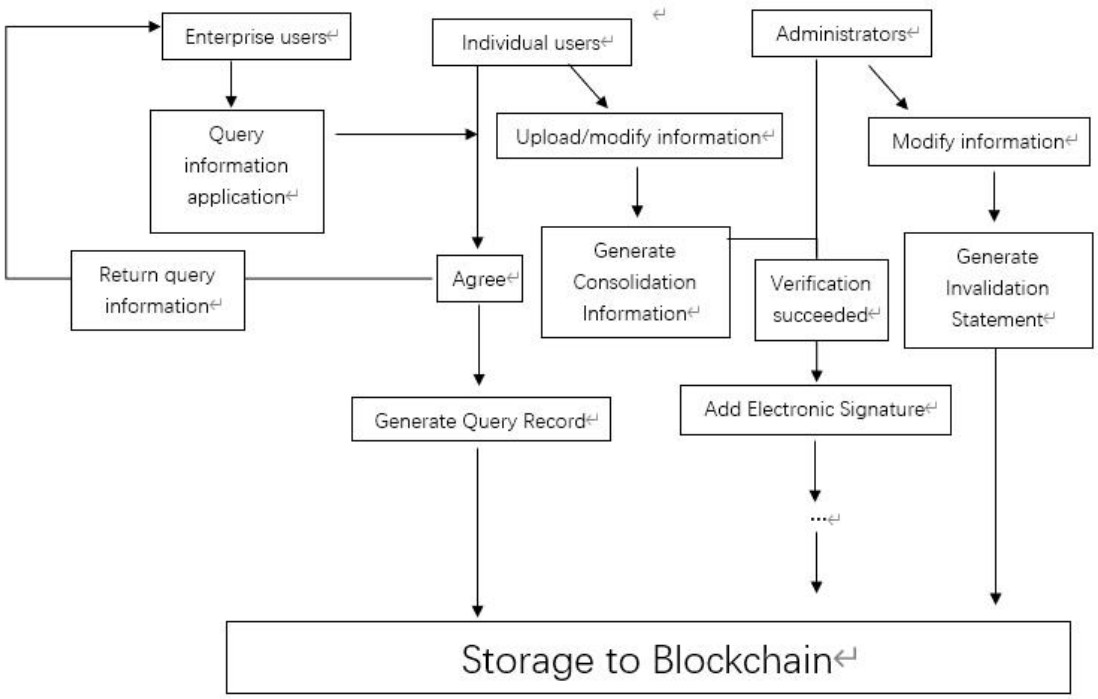


Figure 3: System operation diagram

The interface used is shown in Table 1.

Table 1: Interface variable definition

| Data name | Data Type | Data meaning |
|---|---|---|
| Address | String | Issuing department |
| Name | String | Name |
| Id | Uint | Unique id identifier |
| Num | Uint | Certificate number |
| Time | Uint | Issue time |

The verification system uses an electronic signature algorithm to encrypt and verify the stored content.

### 3.2. Feasibility analysis

#### *3.2.1. Technical feasibility*

With the help of blockchain technology, the efficiency and reliability degree of data storage in the system and the security of information sharing can be guaranteed. Combined with erasure code technology, the reliable preservation of the original data source can be realized and the demand for storage resources can be reduced. The decentralization and immutability of the blockchain are mainly used when depositing certificates. In each data node to maintain a backup, even if a single node is tampered with by the attack information, the correctness of the original data source can still be guaranteed by the remaining nodes; in addition, the update authentication will leave an immutable record in multiple nodes to ensure data authenticity.

*3.2.2. Market feasibility*

**R & D Capability/Cycle**

The government and enterprises conducted research and found that there are still large-scale vacancies in the market for competing products, the demand for products is still strong, and the products will be competitive in the market after the research and development is completed.

Funding Requirements/Allocation

The initial reserve funds will support the initial research and development of the product, the first round of financing will be carried out after the initial formation of the product, and the project will be properly supported by special project subsidies from the Ministry of Education and the Ministry of Finance.

**Market demand**

At present, due to the cumbersome steps in the process of student academic certification and verification, the phenomenon of academic fraud still exists and there is a lack of simple and efficient solutions. Job seekers use fraud to obtain interview opportunities or even be hired, which seriously damages the interests of enterprises and ordinary applicants. Under this circumstance, the academic certification system based on blockchain has great market potential. Due to the traceability, transparency and immutability of the blockchain system, the security and authority of the system are guaranteed, which can well meet the market demand.

## 4. DEFICIENCIES AND PROSPECTS

Combining with the above, it is not difficult to find that, in the education of the terminal block chain application range is very wide and effective, is expected to further enhance the education mode and education form, the information age to improve the information in such aspects as education information into the open, transparent, greatly solve the current degree fraud, fraud problems such as paper, is a big block chain under the application field of branches.

However, the solutions and applications of blockchain in education and other aspects are never perfect, and there are still some shortcomings and drawbacks that need to be solved. First, the storage mechanism costs resources. This is the drawback caused by the operation mechanism of the blockchain itself. Every node of the blockchain system synchronized the complete ledger data in real time to realize its data tamper-proof and anti-destruction. However, this mode produces a large amount of redundant data, and will consume a lot of storage resources with the growth of data storage capacity and data operation volume of blockchain; At the same time, each node will also consume a lot of computing resources and power to process data synchronization. In 2017, it was reported that the blockchain volume of a single node of a digital currency had exceeded 180GB, and new users would spend a lot of time synchronizing this data. It can be seen that as time goes by, the storage pressure of each node will increase, and the access difficulty of new nodes will also increase, which is not conducive to the deployment and expansion of the system. Second, the operating mechanism affects efficiency. Every data modification in the blockchain will affect the synchronous update of ledger data of all nodes in the system, which means that each operation process needs to consume a lot of time, and this operation mechanism will also bring great test to the network where the system is located. Because each operation is the behavior of the entire network, a large number of operations in a short period of time will cause network congestion. According to foreign media reports, due to the increased trading volume of a digital currency, the time required for each exchange increased from 10 minutes to more than 24 hours at the longest. News of the collapse of the blockchain network is also everywhere. Therefore, if blockchain technology is used in key areas, its operation mechanism still needs to be structurally optimized.

In addition, regardless of the technical level, the development of blockchain combined with the development of education itself also has some logical problems worth us to think about. First of all, an undeniable fact is that the learning style, learning process and learning form in the information age have changed, but the certification of learning outcomes still keeps the traditional way. The appearance of credit bank is to solve this problem to some extent. However, in the practice of credit bank construction, we still try to use the traditional way of thinking to solve a new problem, hoping to build a powerful and huge "centrosome" to store and identify all the formal, informal and informal learning outcomes of all learners. This "centrosome" hopes to have the personal information and learning outcome records of all learners within its jurisdiction, authoritatively identify the level and quality of all learning outcomes, and guide and standardize the interconversion of all learning outcomes. That is to say, although we used the chain block such a "decentralized" technology to avoid fraud, but the application of such a technology really need government or relevant background is quite credibility institution for endorsement, it essentially still failed to jump out the concept of "centralized" such a gap. In the future, the application of blockchain in education still needs long-term reform and exploration, not only in the technical improvement, but also in the logical transformation of the way of education certification.

## REFERENCES


[1] 徐宁 & 樊郁徽.(2020). 基于区块链技术的商品交易智能合约设计. 怀化学院学报(05),99-104. doi:10.16074/j.cnki.cn43-1394/z.2020.05.020.

[2] 邓瑞,温月阳 & 舒益新.(2021).基于 PBFT 算法的区块链学历认证系统. 信息技术与信息化(07),16-18.

[3] 王晓欣 & 陈志德.(2022). 基于教育区块链与无证书签名的身份认证方案. 计算机系统应用(03),178-187. doi:10.15888/j.cnki.csa.008407.

[4] 张芬 & 李腾跃.(2022).基于区块链的数字证书及电子印章系统架构. 信息系统工程(08),8-11.

[5] 周春天,王利朋,贾志娟 & 陈舒祥.(2021). 基于区块链的学历证书可信认证系统. 计算机时代(02),34-37. doi:10.16644/j.cnki.cn33-1094/tp.2021.02.009.

[6] 张东宁.(2020). 基于区块链的学业履历存证共享系统的研究与实现(硕士学位论文,北京邮电大学).https://kns.cnki.net/KCMS/detail/detail.aspx?dbname=CMFD202101&filename=1021024127.nh

[7] 宋雨,赵晓永 & 张海峡.(2021).基于区块链的专业技能认证系统研究. 信息与电脑(理论版)(19),148-151.

[8] 王越,李国,叶珉铨,陈子鑫 & 王译正.(2022).面向医疗样品跟踪系统的智能合约设计与部署. 现代信息科技(11),153-156. doi:10.19850/j.cnki.2096-4706.2022.011.039.

[9] 林家茂.(2022).基于区块链的医疗信息系统及智能合约设计. 科技资讯(01),27-31. doi:10.16661/j.cnki.1672-3791.2112-5042-4469.