Research on the Learning and Information System Based on Blockchain

Shuhong Liu
Jilin University of Architecture and Technology, Changchun 130012, China.

Abstract: With the development of The Times, the number of various diploma forms at home and abroad has increased sharply. At the same time, there are many problems such as falsification of academic certificates, and it is urgent to strengthen the real control of various diploma certificates. As a new generation of data management technology, blockchain technology can provide a new path and a new method for the authenticity of academic certificates. With the help of the decentralization, immutability, openness and independence of blockchain, a blockchain technology based academic certificate guarantee system is built from the aspect of talent security to protect the authenticity control of academic certificates.

Keywords: Blockchain; Learning and Information System; Implementation Plan

1. Blockchain Technology

1.1 Development of blockchain technology

Blockchain originated from Nakamoto's Bitcoin, which is actually one of the underlying technologies in Bitcoin applications. With its continuous development, people have summarized that it is essentially a decentralized database, which is a technical solution to collectively maintain a reliable database through decentralized and intermediary free methods. With the increasing improvement of blockchain technology, its application value has gradually emerged in different industries and has received high attention from governments of various countries. In recent years, China has also attached great importance to the development of blockchain technology. As a result, we have welcomed the wave of blockchain technology in the era. At this stage, blockchain technology is developing rapidly, and its application scope will also involve various fields of our country and all aspects of society. However, the development of blockchain technology based on key algorithm encryption cannot be separated from the development of key algorithms. At present, RSA and ECC algorithms are the most commonly used in blockchain applications. Compared to these two algorithms, ECC algorithm has higher security performance and requires less storage space when the key length is the same. Although the SM2 algorithm developed in China and the ECC algorithm are based on the same elliptic curve algorithm established on the esrncryption algorithm, but compared with the ECC algorithm, China is in the initial stage of blockchain system design, but also need to consider the compatibility of domestic cryptographic algorithm and other initial problems, so the application is also behind the ECC algorithm. Therefore, China still needs to increase the research and development of domestic key algorithm and blockchain construction, and further promote the overall development of blockchain.

1.2 The principles and characteristics of blockchain technology

1.2.1 Non-tampering, confidentiality

Blockchain technology is a data processing technology that uses asymmetric key encryption to encrypt data. A public key corresponds to a private key, and the public key is calculated in the forward direction to obtain the private key. However, reverse calculation of the private key is extremely difficult and almost impossible. The principle is to use an asymmetric key algorithm, and the blockchain established from this can play a role in data confidentiality. By auditing each piece of data on

the chain, a data block is formed, and then the entire blockchain is formed from each block.Because each block has a specific time stamp, it forms a blockchain that updates data in real time by being guided by a time chain. Therefore, it is impossible to tamper with and falsify the information on the blockchain. Therefore, it has the function that data cannot be tampered with.

1.2.2 Security and openness

The blockchain technology supports the establishment of a point-to-point distributed ledger, which is composed of distributed nodes, so that all information can be fully accessed at any node. The blockchain established thus has no total data center, and the phenomenon of complete loss of data when the database is attacked in the past will not occur. Each node is backed up by the other, and this decentralization makes it have high security. The database established through the blockchain realizes the sharing of data, so the information in the blockchain database has the characteristics of openness and transparency, and all the data is open to the monitoring and review of the public, which prevents the occurrence of data fraud and is more conducive to the realization of social equity.

1.2.3 Traceability

According to the above content, each node links the data and information according to the time sequence to form a blockchain. The chain attribute of this blockchain enables people to query the relevant data and status of every node in the past, so as to grasp the complete chain information of the content you want to query, which is the traceability function of blockchain technology.

2. Theoretical scheme of blockchain technology to ensure the authenticity of academic qualifications

2.1 Working principle

First of all, the use of blockchain and strong encryption, define a block structure, the specific block should include two parts of the block and the block body, the block mainly includes the parent block hash value, child block hash value, time stamp and other information. The block information is a digital file, which mainly contains the basic information of the certificate, such as name, major, student number, certificate number, and photo. Secondly, in the encryption algorithm, the private key in the secret drug pair is used to encrypt the certificate data, and then the certificate is signed; Then create a hash value according to some rules, encrypt the whole certificate data, once the data information is changed, you can judge by the hash value; Finally, the private key in the secret drug pair in the encryption algorithm is used again to record the new record created on the Bitcoin blockchain, which can prove when the corresponding academic certificate was issued and who was issued.

2.2 Design scheme of Xuexin system

Select the underlying application platform built with the support of blockchain technology. The original approach is to copy the original code of Bitcoin and then modify the underlying code, including the network protocol, consensus mechanism and encryption algorithm. This method is not only time-consuming and laborious, but also requires users to be proficient in Bitcoin technology. Later, people tried to encapsulate the underlying code, and the Ethereum platform, the representative technology of the blockchain 2.0 era, emerged. It is a non-centralized application platform that encapsulates the underlying technology of Bitcoin. Blockchain application developers can avoid the distress of studying the underlying code of Bitcoin and directly develop related development based on the Ethereum platform, so that developers can focus on the application itself. This greatly reduces the difficulty of applying blockchain. We choose the Ethereum platform to realize the design of the Xuexin system, and realize the protection of academic information by deploying smart contracts, certifying individual learners, certifying personal learning records and results, and viewing learning records and results.

3. Research on the implementation scheme of the basic blockchain learning and credit system

Step1: Environment construction Local development environment, operating system window10, Ethereum development

platform, truffle framework, Solidity development language, Atom editor.

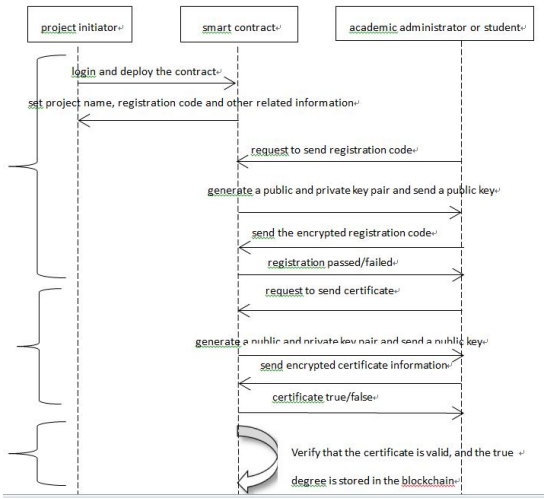
Step2: Complete the deployment of a smart contract with Truffle Realize the configuration and operation of Ethereum development framework Truffle, and complete the deployment of a smart contract with Truffle.

Step3: Run a degree-managed smart contract with Truffle framework.

Step4: To interact with smart contracts in the console.

Step5: Use web pages to interact with smart contracts.

The main process of system operation is as follows:



4. Closing remarks

Blockchain technology is a new architectural idea or a new design scheme, and there is still a long way to go to cover the application. After forming a basic understanding of blockchain, the public, especially scholars in various fields, should study blockchain related knowledge and technology more deeply and actively, dialectically combine the characteristics of blockchain data sharing and data encryption, and maximize its benefits. At the same time, the problems existing in blockchain technology should be fully recognized and improved or circumvented. Only in this way can the major features of blockchain be better utilized to benefit the people.

References

[1] Li CC, Xu XL, et al. Research on the Application of Block Chain Technology in the Garment Industry[J], 2022(22):97-100.

[2] Liu SH. Application and practice of blockchain in learning system[J], 2020 (11): 167-168.

[3] Li WX, Cao WD. Civil Aviation Passenger Privacy Information Protection Scheme Based on Blockchain [J]. 2023.

[4] Jin B, Sun Y, et al. Research on Archival Data Quality Assurance Based on Blockchain Technology [J]. 2023.

Fund project: Youth support project key projects of JiLin University of Architecture and Technology: Design and research of blockchain-based Credit system. Item number: School Kezi [2020]004