Received: 17 July 2022 | Revised: 28 July 2022 | Accepted: 19 August 2022 | Published online: 15 September 2022

RESEARCH ARTICLE

Journal of Global Humanities and Social Sciences
2022, Vol.3(3)63-65
DOI: 10.47852/bonviewGHSS2022030307

BON VIEW PUBLISHING

# Research and Implementation of Certificate Authentication System Based on Blockchain Technology

**Gang Wu[1], Xiangbo Zhu[1], Guoliang Ou[1] & Zhigang Zhou[1,*]**
[1]*Shenzhen Polytechnic, China*

**Abstract:** Nowadays, in the process that the state attaches importance to the development of higher education, it is necessary to strengthen the management of students' degree certification, award certificates, examination certification, etc., so as to ensure the efficiency and transparency of education operation and protect students' future development. Taking the research and implementation of certificate authentication systems based on blockchain technology as an example, this paper studies the design part of the certificate authentication system and analyzes the implementation of chain code deployment of a certificate authentication system based on blockchain technology. In this way, the level of certificate management in colleges and universities can be improved, the development of students can be better maintained, and the talents needed for national development can be trained.

**Keywords:** Certificate authentication system; Blockchain technology; System study

## 1. Introduction

Blockchain is a technology that emerged under the influence of Bitcoin technology. It is based on the distributed architecture of the P2P network and has the characteristics that transactions cannot be deleted or changed easily. When blockchain technology is applied to national development, it can quickly promote the development of financial payment, copyright protection, sharing economy and many other aspects, and even help the development of higher education. Especially after the education industry has become the research focus of the teaching industry with the subject of blockchain plus education, this technology is applied to the certificate authentication system to strengthen the level and efficiency of certificate authentication management in colleges and universities and promote the further development of colleges and universities.

## 2. Certificate authentication system based on blockchain technology

Nowadays, the blockchain platforms are mainly Ethereum, Bitcoin and Super Ledger. First, Bitcoin and Ethereum are based on mining mechanisms, and most of them are used in the construction of public chain, which has the characteristics of poor privacy protection and low transaction processing efficiency. Second, the super ledger is Hyperledger, which is often used in the construction process of alliance chain and private chain, among which there are characteristics such as channel isolation mechanism and member management mechanism, which further promotes the detailed division of tasks among nodes and improves the overall transaction efficiency and ability of blockchain. At present, there are many blockchain platforms based on Hyperledger, which help the development of related industries. Therefore, in order to ensure the design effect of the college certificate authentication system, it is necessary to attach importance to the application of Hyperledger Fabric, so as to lay the foundation for system design and implementation (Zheng et al., 2021).

### 2.1 Designing the overall technical architecture of the system.

This system takes the Hyperledger Fabric in the super ledger as the basic structure, which makes the specific functions of the system can be divided into foreground and background (Song et al., 2021). The first system foreground uses the Web interface to provide a specific operation interface for the users of the alliance chain. Secondly, the foreground system promotes the realization of user's operation and interaction, and the background system is the concrete foundation for the realization of foreground functions. In the design process of the system, users are mainly divided into three types: system administrators, ordinary users and users of regulatory agencies. The specific analysis is as follows.

First of all, ordinary users refer to ordinary students who need certification, colleges and universities that need certification, employers, government agencies and other individuals and organizations that need to obtain accurate information for certification verification. At this time, the functions realized for ordinary users are registration, query and change, as well as revocation and verification of

**Corresponding Author:** Zhigang, Zhou
Shenzhen Polytechnic, China.
Email: detiger@szpt.edu.cn

certificate information. Secondly, the system administrator is to assign the management and authority of front-end users, as well as various activities at the system level. Finally, users of regulatory agencies. Mainly users of educational administrative units and universities, are responsible for supervising the activities that the certificate pays attention to, and ensuring that the certificate information is credible to the world. Combined with the above content, it is found that the certificate authentication system mainly consists of the business layer, alliance chain infrastructure and application layer. Among them, the application layer mainly develops language and technology with the help of the front-end such as HTML5, so as to ensure users' registration, login and operation of certificate information, and realize many functions such as historical data recording, so as to meet the needs of ordinary users' certificate authentication and service. At the same time, business achievements exist as back-end services, providing many interactive interfaces, certificate management, user management and other management functions for Web front-end functions, and connecting with other third-party business certificate systems to ensure that the certificate information of third-party systems can be automatically synchronized and updated. In addition, the infrastructure layer of the alliance chain includes CA (certificate authority node), Peer node, Orderer (ordering node) and so on, so as to guarantee the realization of many functions such as intelligent contract service and consensus service of block volume, member management service, chain code service and so on. At the same time, with the help of SDK such as JAVA and NodeJS, it interacts with the business layer to ensure that the upper business can be supported. CA provides management services for membership and provides functions such as registration or cancellation of identity certificates when joining and leaving the nodes in the alliance chain. In addition, the sorting node is to realize the sorting transaction, package and generate blocks, and add them to the Peer node. At this time, the Peer node is the goal of calling and submitting and endorsing Fabric, deploying chain codes, carrying out the work of logging in and changing certificates, showing and querying elders more, and updating the account book status stored in CouchDB (Wang, 2021).

2.2 Design the specific nodes of the system.

With Hyperledger Fabric as the infrastructure, the certificate authentication system has the network node architecture of three alliance organizations such as ABC and the block system such as the Kafka cluster. At this time, the CA node is the core of managing the members of the alliance chain, user identity management, etc., and provides many functions such as residence, distribution, extension, revocation, etc. At this time, the members need to conduct the following data transaction process.

2.2.1 Initiate the transaction day at the client, and then transfer the proposal.

2.2.2 After the endorsement node checks the certificate, confirm the transaction and return it to the client.

2.2.3 Upload the transaction to the sorting node through the client, and write the block.

2.2.4 After writing into the block, broadcast it to all anchor nodes, and finally complete the account book synchronization. In this way, the transaction speed of the system is constantly improved, and the partition named zero is created in the process of system operation so that the whole process of the transaction processing is in an orderly state. In addition, a channel is built in the blockchain network to ensure that the organizational nodes have the same chain, so as to ensure that the goal of data information sharing can be realized.

## 3. The realization of chain code deployment of certificate authentication system based on blockchain technology.

3.1 CA deployment

If the certificate authentication system supported by blockchain technology wants to realize chain code deployment, it is necessary to attach importance to CA deployment. Specifically, the following aspects are achieved. First, TLS is enabled, that is, the communication between fabric-ca-server and fabric-ca-client is encrypted, and the environment variables are configured to ensure the normal operation of the system. Secondly, after the startup is completed, the corresponding files will be generated, with the help of which the goal of security and happiness can be achieved. Then, when the account is registered, the certificates of the corresponding organizations and nodes will be generated. In this case, we can verify the identity and skill certificates of college students and ensure their future development.

3.2 Data verification based on smart contracts

In addition, when applying the certificate authentication system based on blockchain technology to realize the deployment of chain codes in colleges and universities, it is necessary to pay attention to the development of data verification based on smart contracts. Because the smart contract is the core content of the blockchain, it is the trigger code when users trade, and it is also the business logic of mutual recognition between users. In the blockchain, there are corresponding information and status data. At this time, considering the transaction process, it is found that after the transaction is completed, the data will be divided into different blocks and distributed in the corresponding node database. In this way, if we want to ensure the realization of the certificate authentication system, we should pay attention to the development of this work, improve the level of certificate authentication in colleges and universities, ensure that the information and status of certificates are in a complete state, and ensure the training effect of students (Qi et al., 2020).

## 4. Conclusion

To sum up, in the process of rapid development of the country, in order to ensure the effectiveness of the certificate authentication system in colleges and universities, we must attach importance to the application of blockchain technology, fully design the framework and nodes of the certificate authentication system, and play the role of CA deployment and data verification. In this way, we can promote the development of college certificate certification in an unchangeable, open and transparent direction, improve the quality of talent training in colleges and universities, train the learned talents for the further development of the country, and help the country achieve the goal of building a strong country.

## Acknowledgement

The research on the implementation path and scheme of national credit bank based on blockchain technology, funded by Shenzhen Social Science Fund and Shenzhen Polytechnic SZ2020D038.

## Conflict of Interest

The authors declare that they have no conflicts of interest to this work.

## References

Zheng, A., Zhang, F., Wang, B., Wang, P., & Chen, L. (2021). Application value and practical conception of blockchain technology in school sports operation and management. *Sports Boutique*, 40(6).

Song, Z., Yu, Y., Chen, T., Zhang, Y., Song, J., & Zhai, D. (2021). E-government oriented blockchain authentication model research. *E-Government*, 6.

Wang, X. (2021). The application of digital certificate system based on blockchain in e-government extranet. *Information Security Research*, 7(1).

Qi, H., Yu, C., Chen, G., & Wang, F. (2020). Research and implementation of certificate authentication system based on blockchain technology. *Journal of Chuzhou University*, 22(5).

**How to Cite:** Wu, G., Zhu, X., Ou, G., & Zhou, Z. (2022). Research and Implementation of Certificate Authentication System Based on Blockchain Technology. *Journal of Global Humanities and Social Sciences*, *3*(3), 62–64. https://doi.org/10.47852/bonviewGHSS2022030307