Blockchain-Based Student Information Management System

Huiling Le[1], Jinsong Xu[1(✉)], Yingying Ding[1], Xuechun Li[2], Yiwen Li[1], and Xingning Chen[1]

[1] Jiangsu Normal University, Xuzhou, China
casxjs2003@jsnu.edu.cn
[2] Peter the Great St. Petersburg Polytechnic University, Saint Petersburg, Russia

Abstract. In colleges and universities, the current stage of information file management suffers many problems, such as easy tampering, data redundancy, low intelligence, and high maintenance costs. This article introduces blockchain technology to solve university information file management problems. Using its characteristics of tamper-proof, traceability, distributed, decentralized, collective data maintenance, and low cost to build a blockchain-based student information management system, which can effectively fit the reality, reduce the burden of student information file managers, help information files to circulate efficiently, securely, openly and transparently among state education departments, universities, employers, and promote more rational and standardized information management. This article offers new ideas in several areas, based on traditional student information management characteristics. In terms of data, this article will draw on the idea of UTXO in blockchain to solve the problem of data redundancy (the amount of data input equals the amount of output) and use the "on-chain + off-chain" dual-chain model to solve deficiencies in data storage. In terms of the system, this article adopts the distributed bookkeeping method of the blockchain (decentralized, timestamped, resource sharing, good scalability) to ensure the consistency, real-time, and traceability of student information and uses the consensus mechanism of blockchain to achieve tamper-proof data and uses the ECDSA encryption technology based on elliptic curve algorithm to ensure the security of information. In terms of relationship building, the EOS platform is used to build relationships between information personnel and generate smart contracts to provide intelligent services for government-related units and students. In conclusion, introducing a blockchain-based student information management system will enable a qualitative leap in managing student information files, which is crucial for the government, universities, employers, and students.

Keywords: blockchain · dual-chain model · distributed bookkeeping · consensus mechanism · ECDSA cryptography · EOS smart contracts

1 Introduction

With the continued advancement of computer technologies such as the Internet, cloud computing, and big data, as well as the vertical extension of theoretical depth, blockchain technology is gradually shining on the big stage of computers, emitting its distinct light.

D. Kumar et al. (Eds.): IEIT 2023, AHSSEH 10, pp. 732–740, 2023.
https://doi.org/10.2991/978-94-6463-230-9_87

Many scientists have made outstanding contributions to this goal of protecting individuals' privacy and ensuring the reliability of transactions. Tim May founded Cryptopunk in 1992. David Chom created the Ecash cryptographic anonymous cash payment system in 1993. Adam Baker wrote Hash Cash [1] in 1997. The use of timestamps ensured the security of digital currencies that could not be tampered with, as well as the sequential order of documents. Since then, blockchain technology has evolved gradually.

Blockchain technology is used in a variety of fields. From Bitcoin's decentralized digital payments to the support of users writing smart contracts to build decentralized DAPPs (Decentralized Applications). The blockchain is then created and applied to specific scenarios in various industries, such as the financial sector, academic sector, internet, and so on.

The government also values blockchain technology and has recently implemented policies and guidelines. President Xi Jinping profoundly clarified the importance of blockchain technology in new technological innovation and industrial change in his important speech at the 18th Central Political Bureau collective studies, which puts forward clear requirements for promoting blockchain technology and industrial development and has strong strategic guidance and practical relevance [2].

In short, blockchains combine blocks of data in a certain chronological order, culminating in a chained data structure. In other words, it is a distributed ledger that is resistant to tampering and forgery. The advantages it offers are pivotal in the student management system discussed in this paper.

2 The Compatibility of Blockchain Technology with this System

2.1 Insufficient Data Storage

Hile electronic filing has become more common in elementary and secondary schools, some colleges still use volume management and have a large number of paper files. Paper archives are vulnerable to external natural conditions that make storage inconvenient, and data damage and loss can occur on occasion. Even if some paper files have been converted to electronic files, the total volume of archival information stored continues to grow, resulting in limited system capacity, a lack of backup space, and attacks on the Internet by unscrupulous elements, which can still expose data to loss and destruction. If a blockchain technology with a dual-chain structure combining on-chain and off-chain storage is used, the data for the information index and key information is first hashed and then stored on-chain, and then the entire student profile is stored in an off-chain database with a mapping to the on-chain database, which can greatly increase the amount of data storage and, to some extent, ensure the integrity of the information.

2.2 Data Redundancy

At the present stage, our country lacks some laws and regulations specifically for the management of student records in universities, and there are no unified standards for records management. At the same time, the university student records management system is diverse and complicated. When there is a change of management, the document

files are missing and need to be filled in again, resulting in a lot of wasted resources and the re-entry of information can be intermingled and messy. The problem of misplaced data redundancy will be effectively solved if the UTXO (Unspent Transaction Output) mechanism is borrowed so that the amount of data input equals the amount of output each time. When generating a block, the message entry operator collects information from the network about the student, which contains the signature of the person's private key entering the node. First, the entry clerk verifies that the signature is correct; if not, it cannot be modified. If correct, the signature is considered to be a modification of the information approved by the original information entry person, and the information entry clerk traces back the information from the previous blockchain and compares whether this modification has never been modified before, and then records the person who modified the information this time to create a new block.

2.3 Information Tampering Security Issues

The confidentiality of student information files currently leaves a lot to be desired, and file management has been challenged and questioned, with issues such as hijacked domain names, compromised servers, and malicious content alteration. The current popular method of filling in collected information in universities using Kingsford documents does not guarantee that the information will not be tampered with, and part of the management model is still manual filling, which leads to a significant reduction in security and confidentiality. If blockchain technology can be used effectively to ensure the tamper-proofness and security of data, it can significantly reduce all kinds of undesirable phenomena caused by student privacy leakage. For example, the loss of property and contacts as a result of student information leakage; the rewriting of life trajectories as a result of a university place being replaced by someone else more than a decade ago. Protecting student information and putting an end to such phenomena will result in a significant increase in the credibility of schools and governments.

If a distributed system using blockchain is used [3], each node in the system has the power to initiate information in terms of information distribution and transmission, while neighboring nodes can exchange information and transmit information openly throughout the network, meaning that students' information can be transmitted openly and transparently. Using distributed bookkeeping, nodes can get the right to bookkeeping in the database as long as they follow the rules of the consensus mechanism and complete the corresponding workload, and this record is traceable in real-time and difficult to be tampered with, then the student information entry person makes a workload setting for the student information and can enter the information to form a record, and this record is traceable and tamper-proof to ensure the security of the information. Take advantage of distributed storage, using a distributed way to record the ledger and hit the time stamp when recording information processing, block data is thus generated and disseminated through the network, and the data is formed in the blockchain, which means that every student information entry will be time-stamped, and each node that can enter student information can be previously updated with real-time records of student information, further ensuring the traceability and real-time data.

Of course, distributed bookkeeping is not perfect, and consistency must be ensured. In other words, it is critical to ensure that the result is consistent across the various clusters of collections that use distributed processing.

3 System Building

3.1 Introduction to the System Flow Diagram

3.1.1 General Information Management Diagram

As shown in Fig. 1, this block diagram mainly consists of the main node (education authority), the supervisory node (government), other nodes (college student information filling personnel, college student information supervisors, employing enterprises, training institutions), student information uploading (college student information filling personnel filling information, college student information supervisors review information), student information query (education authority authorization, employing enterprises or colleges) which are composed of several parts, the following is the connection and introduction between each part [4].

Firstly, the members of the chain are introduced: university student information fillers, university student information authorities, employing enterprises, training institutions, government, and education authorities, among which education authorities are the main node and government is the supervisory node. Second, the data required to complete the chain include student performance points, awards and punishments, award and merit information, school recommendation forms, and other student-related information. Thirdly, the permission to access information on student records is set: if all subjects in the chain want to view information about a student, they need the consent of the educational authorities to access the information to a certain extent (in terms of time and scope). Fourthly, the student information filling personnel and the competent department of university student information can upload the information to the chain in real-time according to the daily performance of students, and the information will be jointly maintained by the whole network nodes after the consensus of the whole

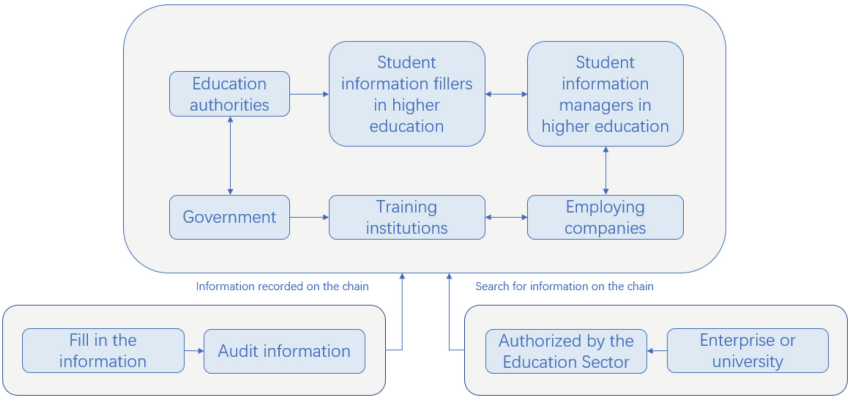

Fig. 1. General block diagram of the blockchain-based student information management system

network nodes to ensure that the information on the chain is true and traceable. Fifth, the education authorities and the government need to take the lead in signing the rules of the contract [5], and each subject to negotiating a signature authentication after the generation of smart contracts, the contract should provide for the automatic decryption of student information time, automatic review of student access rights, automatic authentication of student viewing applications, etc. when the contract is triggered automatically to implement the contents of the contract. Finally, the nodes on the chain can view or recall the information stored on the chain at any time after being granted certain permissions by the education authorities.

3.1.2 Flow Chart for Information Collection and Listening

As Fig. 2 shows, the information collection and listening process is mainly composed of front-end, student information database, smart contract, event, university, enterprise, and service listening modules. The following steps are explained separately.

(1) details of student information entered by the user, such as name, student number, class, awards, etc.

(2)(3) The front end uploads the student's own photo and introductory text (for communication between the university and the company) and returns the link (hash) corresponding to the content uploaded.

(4)(5) The front end will invoke a smart contract to store the student information and link to the chain. When the contract successfully deposits the information into the blockchain, an event is triggered which contains all the information of the student.

(6)(7)(8) The server listens for blockchain events and when the event is triggered by a system contract, the server reads the content of the event and inserts the student information into the database.

Simply repeat the process when you start to implement the student information change and re-upload operation.

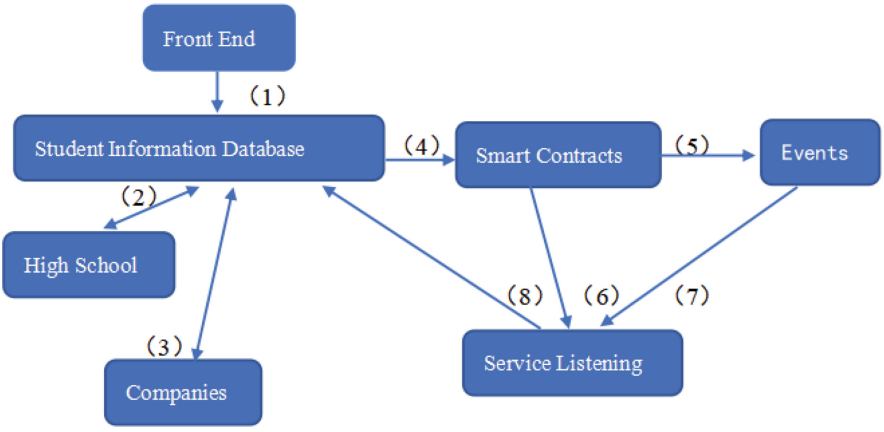

Fig. 2. Flow chart of information collection and listening

3.2 Introduction to System Key Technologies

3.2.1 ECDSA Encryption Algorithm

ECDSA (Elliptic Curve Digital Signature Algorithm) [6]is an analog of DSA (Digital Signature Algorithm) using ECC (Elliptic Curve Cipher). Compared to the general RSA (Rivest Shamir Adleman) and DSA (Digital Signature Algorithm) signature algorithm, the ECDSA key size is smaller and more broadband and space efficient in the same level of a cryptosystem, which can compensate for the limited computing power and storage space of this system. In addition, unlike AES (Advanced Encryption Standard), which encrypts data, ECDSA does not encrypt data and does not prevent others from seeing or accessing your data, thus ensuring that it cannot be tampered with.

ECDSA is primarily used to create a digital signature on data (e.g. a file) to facilitate the verification of its authenticity without compromising the security of the content of the message. In particular, it is proposed that ECDSA signatures differ from authentic signatures in that an ECDSA signature cannot be forged, not only does it recognize part of the signature, but also it cannot be forged by others who are unaware of the existence of the signature or are unaware of it. Whereas with a genuine signature, you don't need to know who signed it and what kind of person signed it, just follow the handwriting and copy it.

Once you understand the advantages and features of ECDSA, how do you construct ECDSA? Imagine drawing a curve on an arbitrary plane, taking a random point on that curve as the origin, then taking a random number and using it as the private key, and using that random number and the origin to calculate another point on that curve through a series of irreversible or hard-to-reverse mathematical formulas, which is the public key.

Signature of documents related to the application of ECDSA signatures to the management of student information systems (student information, applications given by the university, etc.). The public key is bundled with the application or device and used to verify the signature to ensure that the data has not been modified, while the private key is stored locally in a private location. We can use the public key to verify the signature, but we cannot use it to create or forge new signatures so that we can distribute the public key with the application or device without any worries.

ECDSA uses only integer maths [7], no floating point numbers, and the number of bits used in the signature determines the range of integers, with more bits expanding the range of numbers and naturally increasing security as it becomes more difficult to "guess" the exact number used in the equation. In general, ECDSA uses 160 bits, which can represent very large numbers, up to 49 digits, and this provides a high degree of security.

3.2.2 EOS Relationship Platform Construction

There are many reasons for using EOS (Embedded Operating System) as the underlying blockchain platform. Firstly, it supports multiple applications running simultaneously, providing an underlying template for developing DAPPs. Secondly, EOS solves the latency and data throughput challenges by way of parallel chains and DPOS (Delegated Proof of Stake), which can handle thousands of events per second compared to Bitcoin's 7 per second and Ether's 30–40 per second. Again, EOS has no fees [8] and is

more accessible to the masses. Finally, when developing a DAPP on EOS, the relevant resources that need to be used can be allocated in proportion to the EOS owned by the developer, and owning an EOS is equivalent to owning a piece of land, with the option of renting it out to others for farming, or choosing to grow it yourself and be self-sufficient.

3.2.3 The Agile Thinking

Agile thinking is value-driven, so resources and time are relatively fine-grained, requirements change with the market and internal factors, and can be validated and adjusted in a shorter time frame. Borrowing this thinking will make for a more dynamic, real-time system that can better meet the needs of both the business and university sides.

This paper uses agile development thinking to implement a decentralized DAPP. The full student information features will be included in each of the 8 iteration cycles and through each sprint, we will have a release-ready version. The first two sprints focus on the use and framework to implement the school-enterprise contract, which includes the design, development, compilation, deployment, and testing of the contract.

4 Summary and Outlook

4.1 System Summary

This paper uses blockchain technology to achieve efficient management of university student information and solve the chaos of some information management in universities [10]. The paper focuses on the analysis of the problems in the management of student information in universities and proposes solutions based on the problems under the influence of the blockchain concept, integrating the various blockchain technologies required in the system, making a reasonable distribution of functions and finally proposing a newer blockchain-based student information management system [9].

The system solves the problems faced by the current student information management system in two main ways: on the one hand, it proposes a new idea in algorithms, which greatly improves security, and on the other hand, it uses the blockchain mechanism to ensure the standardization of student information management, which effectively ensures that the advantages of the blockchain are maximized, leading to the integration of student information management processes and simpler and more standardized staff operations [10].

Overall, the system is a great solution to the professional needs of student information managers. However, it is important to note that the system only helps in information management. To achieve real progress in information management in universities, the support of the government, the university, and the community is still needed to achieve a faster and safer flow of information and to eliminate the information silo effect.

4.2 Prospects in Other Areas

The concepts discussed in this article could be applied to other fields in the future. For example, in terms of commercial secrecy, its asymmetric encryption technique could be

utilized in combination with the circulation of information in big data, generating new ideas.

Simultaneously, blockchain technology has made significant contributions to addressing some of the shortcomings of the existing financial system. High fees, long transaction times, and time-consuming processes for transferring funds across borders plague the current financial industry. The use of blockchain technology allows users to make payments without the need for third-party approval, reducing the number of intermediaries and increasing the affordability of remittances. At the same time, the district-centric approach accelerates and improves the flow of funds, and there will be more room for the development of similar cross-border rapid movement.

References

1. VictorS.Miller. (1986) Use of Elliptic Curves in Cryptography. Lecture Notes in Computer Science, 218.1. https://doi.org/10.1007/3-540-39799-X_31.
2. Chaoying Zhai. (2021) Research on the Application of Block Technology Chain in Capital Account Management. Financial Theory and Practice, 03:51-57. doi:https://doi.org/10.3969/j.issn.1007-1423.2021.12.012.
3. Xuelu Guo. (2021) A Preliminary Exploration of the Application Model of Blockchain Technology in the Field of Accounting Information Technology - Distributed Database in a Virtual Organization. Finance and Accounting for International Commerce, 06:90–92+96. https://doi.org/10.3969/j.issn.1673-8594.2021.06.021.
4. Xiaoyun Zhou. (2019) Application Modes of Blockchain Technology in Student Archive Management. Journal of Nanjing University of Science and Technology (Social Sciences Edition, 32(06): 52–57. CNKI:SUN:NJLD.0.2019–06–010.
5. Jie Sun, Jialiang Cai, Lichen Zhang, Ran Li, Peng Jia, Zhi Li. (2018) Oil Purification Project Based on Internet of Things and Blockchain Technology. Chinese Hydraulics & Pneumatics, 328(12):54-59. https://doi.org/10.11832/j.issn.1000-4858.2018.12.010.
6. Liang Chen. (2011) Survey of Smart Contract-Based Access Control in Internet of Things. Hangzhou Dianzi University, https://kns.cnki.net/kcms/detail/detail.aspx?FileName=1011125438.nh&DbName=CMFD2011.
7. Mingzhu Gao, Tingrui Xu, Yangting Liu, Yanru Chen. (2021) Research Overview of Privacy Protection Data Release Based on Differential Privacy. Modern Computer, 720(12):66–69+73. https://doi.org/10.3969/j.issn.1007-1423.2021.12.012.
8. Lijing Zhang, Zhen Li, Xueru Yan, Haoyu Shen, Han Zhao. (2020) Exploration and Practice on the Linkage Mechanism of the Educational Administration and tudents' Affairs under the Background of Online Teaching in Colleges. China Modern Educational Equipment, 337(09):10-12. https://doi.org/10.13492/j.cnki.cmee.2020.09.003.
9. Yigao Hu. (2019) Application of Block Chain Technology in Single Set System of Electronic Archives. Lantai World, 563(09): 59-62. https://doi.org/10.16565/j.cnki.1006-7744.2019.09.14.
10. Hui Li. (2021) Research on the Application of Blockchain in Student Growth Archives. IT Education in Primary School and Middle School, 01:80-83. https://doi.org/10.3969/j.issn.1671-7384.2021.01.026.