Research on Key Technologies of Student Electronic Depository System Based on Blockchain

Sheping Zhai1,2, Jing Li*, Cheng Qiu1, Yuanyuan Yang1 and Weixing Zuo1

1School of Computer Science & Technology, Xi'an University of Posts and Telecommunications, Xi'an, 710121, China
2Shaanxi Key Laboratory of Network Data Analysis and Intelligent Processing, Xi'an, 710121, China

*Corresponding author’s e-mail: 13759964066@163.com

Abstract: Aiming at the problem that a large number of students' electronic deposit data is easy to forge and destroy, a student electronic deposit application architecture based on blockchain is proposed. There are some features on blockchain, such as decentralized, the non-tamperable of data, the consensus mechanism and data encryption features, and the electronic depository network. All these features provide a secure and credible storage environment, ensures the traceable of the student's electronic deposit information, the trust of the entire network, and the security of the data. At the same time, an improved PBFT consensus algorithm is proposed, which eliminates the certificate elimination phase to reduce network resource consumption, and constructs a decentralized electronic depository platform in combination with the blockchain to realize the authenticity, integrity and reliability of the electronic certificate data. The further development and application of blockchain technology is prospected, hoping to provide inspiration and reference for future related research.

1.Introduction
Blockchain is a new decentralized application mode that combines distributed data storage, Peer-to-Peer transmission, consensus mechanism, encryption algorithm and other computer technologies[1], which integrates these computer-based technologies flexibly and efficiently, and constructs a set of efficient and safe value Internet system. Its decentralized, traceable, non-tamperable, secure and credible technical features effectively ensure the safe sharing of data and the practicability of blockchain, and all these features is decisive for the wide application of blockchain. Blockchain is originally a reliable database technology to solve the problem of non-trusted third party in traditional transaction. Up to now, the blockchain technology has surpassed the digital currency field[2], and its applications in combination with big data, artificial intelligence, cloud computing and other technologies has been used in the Internet of Things, electronic deposit, intellectual property protection and other fields, showing unique application value and market prospects.

The traditional electronic deposit is a means of proving the facts of the case through the materials and evidence stored by the computer, and its biggest function is to convert the existing paper documents into electronic data for reliable and safe storage, and to produce an independent evidence between the evidence and the documentary proof[3], which can comprehensively and continuously reflect the data related to the case. Traditional electronic deposit certificates can be done by providing evidence documents such as certificates, notes, correspondence records, but these are not strictly
because the evidence is very easily falsified and destroyed. The completing of the proof rely on a strong chain of evidence, on which the participant must not be forged and destroyed. The traditional data security problems of electronic certificates can be solved through the advantages of blockchain of decentralized, non-tamperable, safe and credible[4].

In view of the above problems, an application architecture of student electronic certificate based on blockchain is proposed. A real distributed system is realized through the centralized synchronization of accounting features, which can provide a secure and credible environment, ensuring the trustworthy and traceable of students’ electronic certificate information through the non-tamper features. The mutual trust mechanism of the network and the security of electronic storage network data is enhanced and ensured through the trust-based consensus mechanism and data encryption features of blockchain. At the same time, an improved PBFT consensus algorithm is proposed to eliminate its certificate elimination phase to reduce the consumption of network resources, and to construct a centralized electronic depository platform based on blockchain to realize the authenticity, completeness and reliability of electronic data, and to promote the further development and application of blockchain technology.

2. Related knowledge

Blockchain technology[5] is a cryptography-based distributed peer-network co-trust Intelligent Ledger technology, that is, through the decentralized way to maintain a reliable database technology. The blockchain technology architecture referenced in this paper integrates the following key technical principles: (1) The data structure of Merkle tree block; (2) Peer-to-Peer network structure; (3) consensus mechanism; (4) asymmetric encryption technology. The introduction and innovation portfolio of all these key technologies will create an open, secure, and highly intelligent electronic Depository system.

Merkle Tree block Data structure: The Merkle tree is a two-fork or multi-fork data structure used to synchronize the consistency of a database[6], which hashes each leaf node and continuously recursively, and finally constructs a tree structure. As shown in Figure 1, the block does not save the hash of each transaction, but instead constructing all the trades into such a Merkle tree, the hash of the root node of the Merkle tree are taken as a map of all trading contents, and stored in the head structure of the block, thus data integrity is guaranteed. Prevent malicious tampering at the same time greatly to reduce the computation, improve the efficiency of the operation, and once the data has been tampered with can be quickly located.

Peer-to-peer Network Structure: Peer-to-peer network[7] is an Internet system that does not have a central server and relies on user groups to exchange information. Due to the lack of a centralized
It makes it inherently resistant to attack, high fault tolerance, and equal status of each node. Each node has a record of the complete database information, when one node receives data from another, the node verifies the identity of the other node. If the validation succeeds, the information received is broadcast to the entire network, so the attack on some nodes or networks has little impact on the entire system. The process of validating, storing, maintaining and transmitting data in the blockchain network is based on the structure of peer network, so the robustness of the blockchain network is ensured and the integrity and consistency of transaction data on blockchain are ensured.

Asymmetric Encryption: Asymmetric encryption is a cryptographic technique integrated into the blockchain to meet security requirements and ownership verification requirements, including RSA, Elgamal, Rabin, D-H, ECC, and so on. The asymmetric encryption algorithm is a cryptographic method consisting of a pair of unique public and private keys. The public key and the private key are a pair, if the data is encrypted with the public key, only the corresponding private key can be decrypted, if the private key to encrypt the data, then only the corresponding public key can be decrypted. Asymmetric key pair has two features, the first is to use one of the key (public or private key) to encrypt the information, only another corresponding key can be solved, followed by the public key can be exposed to others, the private key is confidential, the other person can not deduce the corresponding private key. Blockchain technology uses asymmetric encryption algorithm to meet the security requirements of data transaction, ensuring the source of information.

Consensus Mechanism: one of the core strengths of blockchain technology is the ability to effectively reach a consensus on the effectiveness of block data in decentralized systems where decision power is highly fragmented. Many researchers have improved the traditional Byzantine Fault Tolerance (BFT) algorithm to solve the data consistency problem. The improved Practical Byzantine Fault Tolerance (PBFT) algorithm is an executed algorithm based on message passing, which solves the problem of communication delays of original Byzantine fault tolerant algorithm by optimizing the PBFT algorithm. The algorithm complexity is reduced from the point to the polynomial level, so that it can be applied to the blockchain network to solve the problem of message loss, corruption, delay, also it can adapt to the dynamic join and exit of the node, and can withstand a variety of artificial or non-human fault, and for any network environment has a good fault tolerance.

3. Student Electronic certificate system model

In view of the large number of documents need to be stored in the management of campus students, this paper proposes a model of student electronic information depository framework by using blockchain technology, and then comprehensively applies the basic principles of block data structure, encryption algorithm, distributed storage and consensus algorithm based on Merkle tree, from the storage layer of computer system, Network layer, consensus layer and application layer, the paper studies the specific architecture and key technologies of the blockchain electronic depository platform, and then validates it, so that the student's certificate information can be stored in real-time and efficiently, and the time, content and owner one by one correspond to ensure the security and effectiveness of the electronic certificate information.

This paper makes use of the features of the blockchain underlying architecture in privacy protection, anti-tampering and anti-attack, and realizes the restoration of the authenticity, uniqueness and completeness of the student's electronic certificate data technically. In data security, consistent maintenance, from the storage layer, network layer, consensus layer to digital encryption, and these four key technologies can carry out the research work, which ensure the data integrity can be the most important technology. The technical processing framework taken in this article is shown in Figure 2.
4. Student E-Certificate process

Student Electronic Certificate Application is a distributed and anonymous data protocol based on blockchain consensus protocol, which gives blockchain technology the ability to expand into wider application scenarios. In addition, users do not need to hold an encrypted currency account or use the platform's system functions. The specific process of the electronic certificate model in this project is divided into the following four steps:

(1) Hash operation: Student achievement, certificate, scientific research paper, degree certificate and other electronic data after hash operation, generate a fixed length of the original data unique features of data, called the original data "digital fingerprint". The "digital fingerprint" has the following features: ① cannot launch the contents of the original data by the "digital fingerprint"; ② the regenerated "digital fingerprint" is unpredictable after any changes to the original data.
(2) Digital signature: Using asymmetric encryption technology, the storage party to the data after the private key signature sent to the blockchain network, the purpose of the signature is clear that the source of data is not repudiation, and ensure that the transmission process can not be tampered with.

(3) Record to block: The certificate data sent to the blockchain network will be packaged into block after a consensus, and synchronized to the various nodes in the network, and the data are stored distributed.

(4) Certificate: The user needs to store the data to complete the certificate, the user needs to prove, the system can give authoritative proof report. The specific process is shown in Figure 3.

![Figure 3. Student Electronic data certification process.](image)

5. Evidence block consensus algorithm

5.1 consensus algorithm

In this paper, the Byzantine fault-tolerant algorithm used in the electronic certificate system is designed, the algorithm can ensure the normal operation of the electronic certificate system if the error node in the consensus calculation is not more than \( f = \lfloor \frac{(n-1)}{3} \rfloor \), where \( n \) is the total number of the consensus nodes in the whole network, and \( F \) is the maximum number of allowed error nodes in the network.

In student electronic depository system, a consensus from the beginning to the end of the data used by the collection is called the view. Each view has a number of \( V \), numbering starting from 0. If the node in the current view can not reach a consensus to replace the view, then the number \( v \) gradually increment until the consensus reached. Once a new block is created, a new round of consensus is opened immediately, and the view number \( v=0 \) is reset. The consensus algorithm flowchart is shown in Figure 4, assuming that the student electronic deposit system in the generation of block time is \( T \), under normal circumstances, the user from a node to the electronic depository system to transmit evidence information, \(<m>_{si} \) is the node i of the message m digital signature. The algorithm executes as follows:

(1) The Management node first detects whether the surviving nodes in the network meet the requirements of the trigger consensus algorithm, that is, the number of surviving nodes is \( c \geq n-f \). If compliant, the management node calculates the speaker node P, and receives the user evidence information node to the whole network broadcast evidence information; if not, then the certificate network waits for the new node to join, meanwhile, the node receiving the user evidence information broadcasts the evidence information to the network;
(2) The entire network node receives the broadcast evidence information in the network, and records in the memory;

(3) The speaker sends the proposal \(<\text{Prepare Request}, h, v, P, \text{block}, <\text{block}>_\sigma P>\) after the time \(t\);

(4) After receiving the proposal, the member verifies the proposal and verifies that the pass is sent \(<\text{Prepare Response}, h, v, i, \text{block}, <\text{block}>_\sigma i>\), where in the verification rule is: on the one hand, in the node participating in the consensus algorithm, at least \(n-f\) have the same initial state, that is, the whole network node \(i\) to have the same block height \(h\) and view number \(v\). In the system, block synchronization is achieved to achieve the consistency of block height, and the consistency of view number can be achieved by changing the view. On the other hand, the block information generated by the member \(i\) is verified with the block information generated by other members and the block information generated by the speaker;

(5) Any node \(i\) in the network including the management node after receiving at least \(n-f\) \(<\text{block}>_\sigma i\), consensus reached and released a complete block;

(6) Any node after the block is added to the blockchain, the evidence information that joins the block is purged from the cache and the next round of consensus is started.

![Figure 4. PBFT consensus algorithm flowchart.](image)

5.2 Node authentication protocol

The main purpose of the protocol are to maintain the scale of information stored in the node, and to resolve the recovery of certificate information, thus reducing the memory overhead of the node. In the PBFT mechanism, the checkpoint protocol is defined through the timing negotiation between nodes and then purged, so the elimination of expired certificates is also a whole network agreed process, which is bound to carry out the 3-phase commit process, resulting in a waste of communication. This paper is based on the time stamp of the optimal block in the blockchain to clear the certificate. Blockchain is linked to the generation of blocks in the form of a link, when a block is added to the blockchain, the certificate before the block timestamp has been verified, that is, the status of these certificates in the node has been broadcast, and can be purged, and the information of the certificate is always in the form of blocks in the node. The addition of block events is therefore monitored, and whenever a block is added to the blockchain, the certificate before the block timestamp in that node is purged. The whole process do not need to communicate with each other, but also to ensure the timely cleaning of certificates.

After all the nodes in the certificate network have reached a consensus, the new node becomes the management node through the internal data of the message authentication node, then the whole network broadcasts and joins to the blockchain network, the other nodes receive and store the information of the management node, and the node authentication protocol process is shown in Figure 5. In this paper, when the blockchain state of a node is inconsistent with other nodes, the block hash of blocks to be added to the \(2f+1\) node in the view is requested, and the block hash is a 256 byte array which can uniquely identify the block, when there are not less than the block hashes returned by the
F+1 nodes. It is considered that the block hash corresponding to the block in the whole network to reach consensus. The node first looks in the Pre-prepare certificate for the existence of a certificate for that block hash, does not exist, and then adds the block to the blockchain for synchronization by asking one of the nodes for the block hash corresponding to the block.

| New node | Deposit network node |
|----------|----------------------|
|          | Management node      |
|          | Ordinary node        |
| Apply to join the network | Certification related data  |
| No       | verify Yes           |
|          | Broadcast new node information to other nodes on the whole network |
|          | Receive and store new node information for consensus verification |
|          | New node joins the network |

Figure 5. Node authentication protocol flowchart.

5.3 View Replacement Protocol

View replacement occurs primarily when there is a problem with the Access node. The main idea is to synchronize information. The following diagram process takes place without limiting memory space. As shown in Figure 6, the view replacement will have three stages, namely the view-change, view-change-ack and new-view phases. View-change messages are sent to other nodes when the node considers the primary node to be problematic, and the node with the lowest node number currently surviving becomes the new primary node. When the new primary node receives a view-change message from a 2f other node, it proves that there are enough nodes to believe that the primary node is problematic, and then it broadcasts to the other nodes.

Figure 6. PBFT algorithm view replacement.

6. Security analysis and proof of electronic certificate system

In this paper, the student electronic data storage system uses the blockchain technology to innovate the data management and data record of the university, and maintains a blockchain data network which
can not be changed permanently and based on timestamp record. This paper analyzes the security of the system through the following points: (1) If one of the nodes will tamper with forensics information, the information of forensics data block will be removed from the chain to prevent the data from being tampered with in the forensics Blockchain, and (2) the Management node and the node authentication mechanism is added in the blockchain calculation process. Prevent the deception and collusion of the nodes; (3) for the Consensus network composed of n consensus nodes, \( f=\lfloor (n-1)/3 \rfloor \) is provided with the fault tolerance, which is safe and available and suitable for any network environment.

7. Conclusion
This paper puts forward a application scenario of the Blockchain student information electronic certificate, designs and realizes the improvement PBFT consensus mechanism, by canceling the main node authentication generating block, from the node to whether the block in the whole network consistency synchronization reached consensus, to some extent, to solve the resource waste and non-trust problem, In this paper, the improvement of the cancellation certificate removal operation for the checkpoint protocol in the PBFT algorithm of the electronic depository system reduces the communication consumption of the network data transmission amount to some extent. This paper deeply studies the application model of blockchain technology in the field of electronic depository, which can provide useful inspiration and reference for future research.

Acknowledgments
Thanks to the Xi'an University of Posts and Telecommunications Graduate Innovation Fund (CXJJ2017006) project and the Ministry of Industry and Information Technology Communication Soft Science Project (2018-R-26) for support.

References
[1] Yuan Y., Wang F.Y. (2016) The Status Quo and Prospect of Blockchain Technology Development. Acta Automatica Sinica, 42: 481–494.
[2] Cai W.D., Yu L., Wang R., Liu N. (2017) Research on Application System Development Method Based on Blockchain. Journal of Software, 28: 1474–1487.
[3] Xia Q., Zhang P.J., Zuo C. (2017) Overview of Consensus Mechanism of Encrypted Digital Currency System. Journal of Computer Systems, 26: 1–8.
[4] He P., Yu G., Zhang Y.F. (2017) A Preview of Blockchain Technology and Application. Journal of Computer Science, 44: 2–15.
[5] Zhu L.H., Gao F., Shen M. (2017) A Review of Research on Blockchain Privacy Protection. Journal of Computer Research and Development, 54: 2170–2186.
[6] Zhou P., Tang X.D. (2017) Blockchain and Value Internet Construction. Information Security & Communication Security, 8: 53–59.
[7] Yin G.Q. (2017) Literature Status Quo and Potential Problems of Blockchain Technology. Times Financial, 6: 299–301.
[8] Wang Q., Qing S.D., Ba J.R. (2017) Discussion on the Application of Blockchain in Credit Information Industry. Telecommunications Network Technology, 6: 37–41.
[9] Wang J.C., Gao L.C., Dong A.Q. (2017) Research on Data Security Sharing Network System Based on Blockchain. Journal of Computer Research and Development, 54: 742–749.
[10] Wei H.F. (2016) Research on Distributed Data Consistency Technology. Nanjing University, 63: 41–53.
[11] Castro M, Liskov B. (1999) Practical Byzantine fault tolerance // Proceedings of the 3rd Symposium on Operating Systems Design and Implementation. New Orleans. 99: 173–186.
[12] Kraft D. (2016) Difficulty control for blockchain-based consensus systems. Peer-to-Peer Networking and Applications, 9: 397–413.