Journal of Computing and Electronic Information Management
ISSN: 2413-1660 | Vol. 14, No. 2, 2024

Research on the decentralized application of blockchain technology in campus information security

Kuiwei Yu, Guanxun Cui

Chongqing University of Technology, Chongqing, China

Abstract: In the digital information age, the traditional centralized storage model is vulnerable to security attacks, which leads to the spread of false information and difficulty in tracing. This study proposes a decentralized campus information security system using blockchain technology and builds a tamper-proof, traceable, and privacy-protected architecture through Ethereum and Inter Planetary File System (IPFS). The system uses zero-knowledge proof and homomorphic encryption technology to ensure privacy and uses IPFS as an off-chain storage mechanism to improve the scalability of the system and data access speed. Experimental results show that compared with traditional digital applications, the system performs well in ensuring the authenticity and security of information and effectively protects user privacy.

Keywords: Blockchain; Decentralization; Privacy protection; Inter Planetary File System.

1. Introduction

In the information age, the security and authenticity of campus internal information are crucial to ensuring the quality of education and the personal information security of teachers and students[1]. At the same time, the widespread use of digital sharing platforms has led to the spread of false information becoming a serious problem[2], which not only threatens personal data security but may also lead to social instability and mislead the public. For example, during the 2020 COVID-19 pandemic, the spread of false medical information on social media led to public panic and misoperation [3]. In addition, recent data breaches, such as the Facebook data breach, have exposed the vulnerability of centralized data management systems in protecting user privacy [4]. This study aims to develop a decentralized campus information security system through blockchain technology to meet the above challenges.

The core characteristics of blockchain technology: decentralization, immutability, and transparency, provide new possibilities for ensuring the authenticity and security of information. By implementing a decentralized verification mechanism, the spread of false information can be fundamentally prevented and user data can be protected from unauthorized access and tampering[5-6].

This study proposes to use the Ethereum blockchain and the Inter Planetary File System (IPFS) to build an information storage and verification platform. Zero-knowledge proof (ZKP) and homomorphic encryption technology are used to further protect user privacy [7], while IPFS is used to achieve efficient data access and improve the scalability of the platform[8-9]. In addition, the traceability of blockchain technology can effectively improve the transparency and trust of information. As described in the literature[10-11], blockchain technology has been successfully applied to finance and supply chain management to ensure the security and reliability of data.

The main results of this paper include (1) designing and implementing a decentralized campus information security system based on blockchain; (2) using encryption technology to ensure the privacy and security of user data; (3) verifying the effectiveness of the system through experiments, showing its advantages in preventing the spread of false information and improving data security. Through these research results, this paper not only provides a technical solution for campus information security but also explores the possibility of further application of blockchain technology in the field of education.

2. Related work

With the widespread application of digital platforms, the campus information environment faces increasingly severe information security and false information dissemination problems. The current centralized information application is prone to attack due to the centralized data storage and management method, resulting in data leakage and thus affecting the authenticity and security of information. To solve these problems, blockchain is used to provide a decentralized solution. Its characteristics include data immutability, decentralized storage, and transparency, which make it a powerful tool for protecting campus information security.

2.1. Application of blockchain technology in information security

In the field of education, blockchain technology is used to ensure the authenticity and secure storage of academic records while preventing the spread of false information. For example, reference[12] shows how blockchain technology can securely share data in an intelligent environment; while reference[13]details the application progress of blockchain technology in ensuring data integrity and preventing data tampering.

2.2. Prevention mechanism against false information

The detection and control of false information is one of the main challenges facing current information applications. Traditional information applications lack an effective verification mechanism, which makes false information easy to spread. Blockchain provides a mechanism to increase the credibility of information through decentralized verification and recording. References[14]and[15]respectively explored

the ability of blockchain to prevent information tampering and improve traceability in supply chain management. These studies show that blockchain technology can effectively reduce the spread of false information.

2.3. Blockchain application in education

Although blockchain technology has been widely used in fields such as finance and supply chain, its research in the field of education is relatively small. Reference[16] reviewed the hot spots of blockchain technology applications in the field of education. Domestic and foreign research on "blockchain + education" mainly focuses on credit certification, academic certificate management, etc., and there is less research on campus information security. The shortcomings of current research and future development directions are pointed out.

Through the above-mentioned related work section, this paper clarifies the necessity and feasibility of using blockchain technology in campus information systems and provides a theoretical and practical basis for subsequent experimental design and implementation. In addition, by citing related research, the potential and advantages of blockchain technology in improving the security of campus information systems and preventing the spread of false information are emphasized.

3. Related technologies

3.1. Decentralized applications

Decentralized applications (DApp) are applications built on blockchain technology and smart contracts. They use blockchain as the core of data storage and processing. The decentralized nature of DApp reduces the risk of single-point failures and enhances the transparency and security of applications[17]. In the campus information assurance platform, DApp can ensure the authenticity and immutability of information, automatically execute preset logic through smart contracts, and ensure that only authorized users can publish and manage information.

3.2. Smart Contracts

Smart contracts, first proposed by Nick Szabo in 1997[18], are self-executing agreements stored on the blockchain that can automatically execute operations when predetermined conditions are met. These contracts run on the Ethereum Virtual Machine (EVM), ensuring transaction automation and security. Figure 1 shows the operating principle of smart contracts.

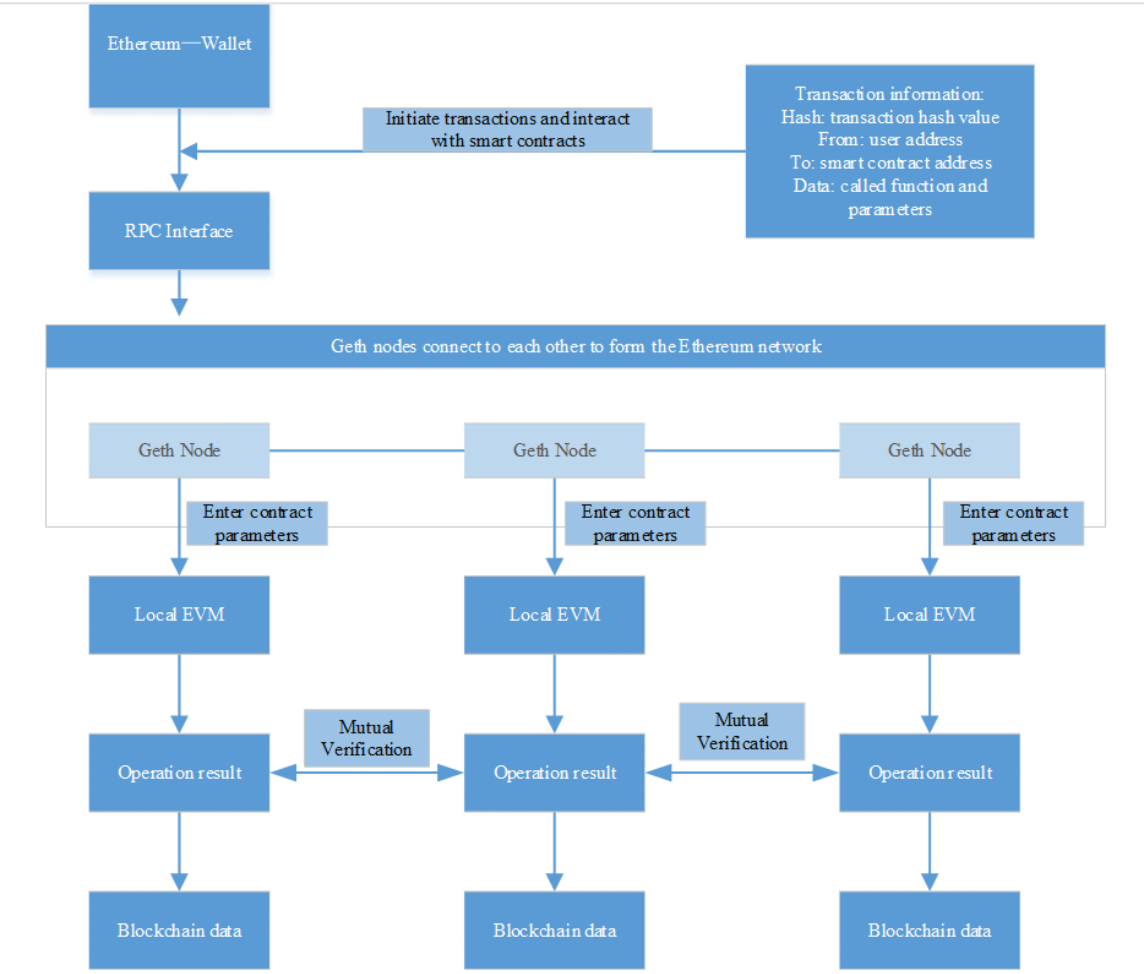

Figure 1. Smart contract operation principle

3.3. 3.3 Web3.js

The Web3 JavaScript app API (Web3.js) is the primary JavaScript API library for interacting with the Ethereum blockchain. It communicates with local nodes via RPC calls and can be used with any Ethereum node that exposes the RPC layer. If a local node is connected to the application, the node can store keys, sign transactions, read, and interact with the Ethereum blockchain. Figure 2 shows the interaction between Web3.js and Ethereum.

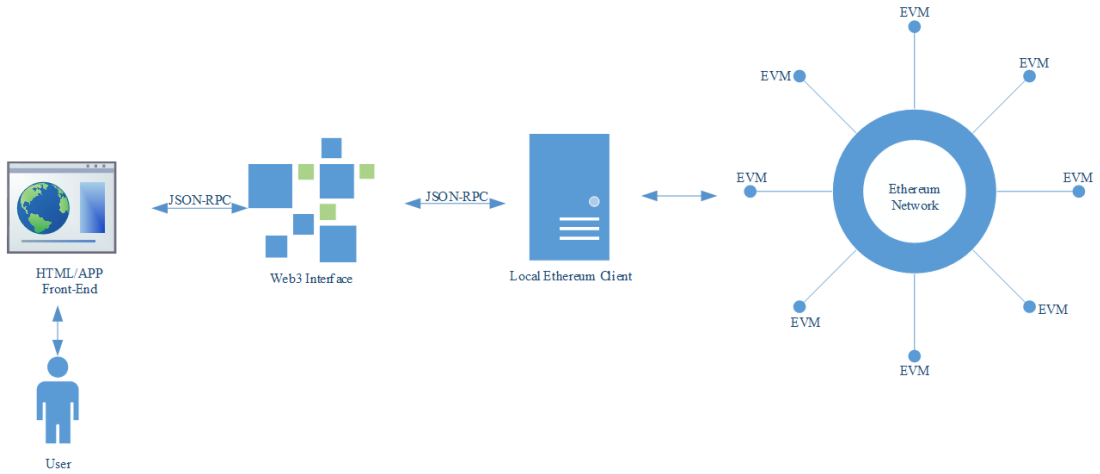

Figure 2. Web3.js interacts with Ethereum

3.4. Interstellar file system

Inter Planetary File System (IPFS) is a peer-to-peer (P2P) distributed file system that can directly transmit data between nodes without the need for a central server. It accesses data through hash value addressing of file content instead of location addressing, ensuring the uniqueness and immutability of data. When a file is uploaded to IPFS, it is split into multiple small blocks, which are stored in various nodes in a distributed manner. The distributed storage method improves data reliability and access speed.

4. System Design

4.1. System Implementation

The system is based on the Ethereum blockchain and combines the Interstellar File System (IPFS) as an off-chain data storage solution to achieve efficient management and secure storage of data. The front-end interface is developed using the React and Bootstrap frameworks, and the Meta Mask wallet is integrated to facilitate user authentication and interactive operations. It communicates with the blockchain backend through Web3.js to achieve data query and transaction functions. The back-end logic is implemented by smart contracts deployed on Ethereum. The back-end logic is implemented by smart contracts deployed on Ethereum. Smart contracts consist of identity contracts, information contracts, and control. The contract structure is responsible for processing the verification and storage of information. IPFS is used to store large volumes of non-transaction data. The design includes IPFS integration, allowing users to store files. In a decentralized network, relevant metadata (such as the hash value of a file) is stored on the blockchain.

4.2. System Functions

The system is divided into five parts: user identity management, information release and management, audit mechanism, shared information, and off-chain storage. The overall system architecture is shown in Figure 3.

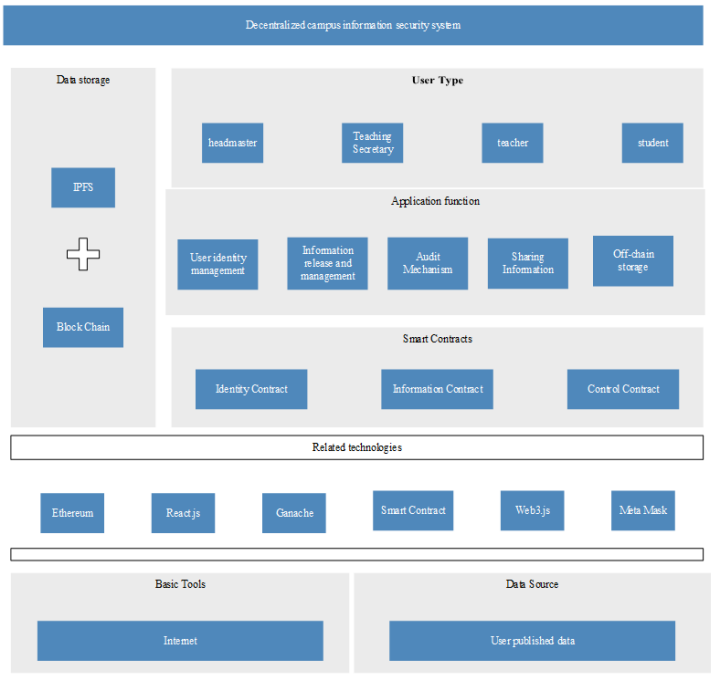

Figure 3. System architecture

The system functions are designed as follows:

1) User identity management: Users use Meta Mask to

generate a blockchain-based identity and submit relevant identity information (such as role type and contact information). The registration information must be reviewed and approved by the authorized manager (teaching secretary). Users who pass the review can authenticate their identity through their blockchain address and Meta Mask to log in to the system for subsequent operations.

2) Information publishing and management: Authorized users can create and submit notifications or messages. These contents need to be reviewed by users with corresponding permission levels before being published. Once the content passes the review, it will be published in the system and all users can view it.

3) Audit mechanism: Users with audit permissions are responsible for auditing newly submitted information. Only information that has passed the audit will be publicly released.

4) Shared information: Information disclosed in the system can be accessed and shared by any successfully registered user to promote the widespread dissemination and availability of information.

5) Off-chain storage: For large data or data that needs to be stored persistently (such as pictures, documents, etc.), the system uses IPFS to ensure data security and high accessibility. Users can access and download this data through the system's unique content-addressed hash (CID).

4.3. Partial Algorithm Implementation

4.3.1. User registration and verification: users register through blockchain addresses, and the system uses zero-knowledge proof technology to verify user identities without exposing user private information.

Algorithm1:User Registration and Verification Zero-Knowledge Proof：

a) function userRegist (userInfo):
(publicKey, proof) = createZKP(userInfo);
submitRegistration(publicKey, proof)
b) function createZKP(Info):
(pk, sk) = generateZKPKeyPair();
proof = generateZeroKnowledgeProof(pk, userInfo);
c)function submitRegistration(publicKey, proof);
d)function verifyProof(publicKey, proof):
return ZKPVerify(publicKey, proof);

4.3.2. Information release: When users release information, the information is encrypted and stored through homomorphic encryption technology to protect content security.

Algorithm2:Information publishing and information encryption and decryption：

a) function post(content):
encryptedContent= homomorphicEncrypt(content);
b) function homomorphicEncrypt(content):
return EncryptUsingPublicKey(content, getPublicKey()) ;
c)function decryptedContent(contentID):
decryptedContent = decryptContent(retrieveContent(contentID));
display(decryptedContent);
d)function decryptContent(encryptedContent):
return DecryptUsingPrivateKey(encryptedContent, getPrivateKey());

4.3.3. File upload and download: Users upload files to IPFS and store the returned content-addressed hash (CID) on the blockchain for subsequent verifiable and persistent access. Subsequent users retrieve and download the source file through the CID.

Algorithm4: File upload and download：

a) function upload(file):
cid = IPFS.add(file)
Blockchain.store(cid)
return cid
b) function download(cid):
return IPFS.get(cid)
c)class IPFS:
return ipfsClient.add(file)
return ipfsClient.get(cid)
d)class Blockchain:
blockchainClient.store('CID', cid)

5. Experimental results and analysis

5.1. Experimental environment

The experiment used Ganache to simulate the Ethereum network on MAC OS, tested smart contracts on Remix IDE, installed and built IPFS using ipfs-desktop, and switched between different types of users using the Google Chrome plug-in Meta Mask.

5.2. Experimental results

As shown in Figure 4 User Registration, Xiaoming, who is a student, needs to pass the review after registration before he can successfully join. After passing the review, you can directly see each user's information in the member list. As shown in Figure 5, publishing and sharing notification information, when a user publishes a notification, its address and block number, publishing time, and content will be displayed. After the notification is shared, the block number will change, but the original information can still be traced back through the original address. Each user who shares the information will leave the address for easy traceability. As shown in Figure 6, through IPFS uploading and downloading, after users upload files to IPFS, they will receive the returned IPFS CID and save it to the Ethereum network. Through this CID, users can download their own and shared files at any time.

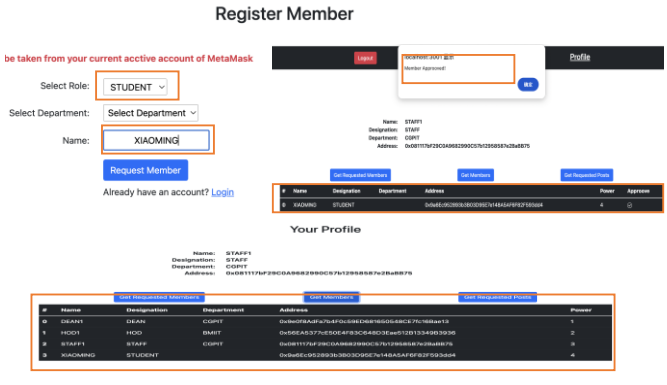

Figure 4. User registration

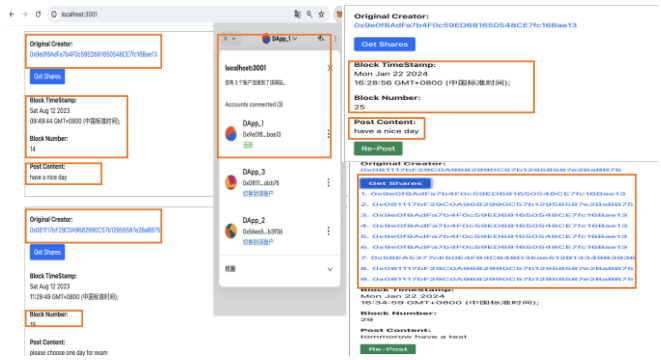

Figure 5. Information publishing and sharing

Figure 6. IPFS upload and download

5.3. Experimental cost

Smart contract operation cost (as shown in Table 1):

Table 1. Smart contract operation cost

Smart Contract Name	Cost to deploy and execute smart contracts	Gas consumption	Gas consumption limit
Identity Contract	0.0024 ETH	2756	3000
Info Contract	0.0021 ETH	2368	3000
Control Contract	0.0002 ETH	223	3000

As of June 2024, 1 ETH = 17631.4 CNY (data from the Internet: https://www.xe.com/). Therefore, the costs of the three smart contracts are converted into RMB: 42-yuan, 37 yuan, and 4 yuan respectively. Compared with ordinary digital applications, the development cost of decentralized applications using blockchain platforms is lower, which is conducive to multiple experiments to pursue ideal results.

6. Conclusion

This paper studies the decentralized application of digital information, aiming to establish a safe campus information environment and ensure the authenticity and effectiveness of information dissemination on campus. Through experiments and tests, the application has significant advantages in data traceability, storage optimization, and research costs. To further improve the practicality and feasibility of the solution, future research will focus on the following aspects: improving the security of access by different users through technical improvement and optimization; further studying and solving the problem of system data consistency to ensure system stability and reliability; Research and explore the legal and regulatory compliance of decentralized applications to ensure the legitimacy of the system. Through these efforts, the solution proposed in this paper is expected to play a role in a wider range of application scenarios and promote the further development of blockchain technology.

References

[1] Ma Wei. Construction of network information security assurance system for digital campuses in universities [J]. China Information Industry, 2024, (03): 139-141.

[2] Fallis, Don. “What Is Disinformation?” Library Trends 63 (2015): 401 - 426.

[3] Wang Jian, Wang Yucui, Huang Mengjie. False information in social networks: definition, detection, and control [J]. Computer Science, 2021, 48(08): 263-277.

[4] Meng Xi. Research on the influence mechanism of false information identification intention of social media users [J]. Modern Intelligence, 2023, 43(04): 39-50.

[5] Liu, Y., He, D., Obaidat, et al. (2020). Blockchain-based identity management systems: A review. Journal of Network and Computer Applications, 166, 102731. https://doi.org /10.1016/j.jnca.2020.102731.

[6] M. Westerkamp, S. Göndör and A. Küpper, "Tawki: Towards Self-Sovereign Social Communication," 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), Newark, CA, USA, 2019, pp. 29-38, doi: 10.1109/DAPPCON.2019.00014.

[7] Wei Chengxin. Innovation and application of data encryption technology for education data privacy protection [C]//Henan Private Education Association. Proceedings of the 2024 Higher Education Development Forum (Volume 2). Guangxi University of Chinese Medicine; 2024:2.

DOI:10.26914 /c.cnkihy.2024.009247.

[8] Song Chuangang, Li Leixiao, Gao Haoyu. A review of key methods for blockchain system performance optimization[J]. Computer Engineering and Applications, 2023, 59(16): 16-30.

[9] Wang Feng ,Zhang Qiang, Liu Yang, et al. Blockchain from the perspective of scalability[J]. Journal of Computer Application Research, 2023, 40 (10): 2896-2907.

[10] Ziyan Li, "Research on Enterprise Strategy Based on Block Chain Security Sharing Mechanism", Mobile Information Systems,vol. 2022, Article ID 9941444, 11 pages, 2022.

[11] Ge Lina, Xu Jingya, Wang Zhe, et al. Research status and challenges of blockchain in supply chain applications[J]. Computer Applications, 2023, 43(11): 3315-3326.

[12] Qin Sihang, Dai Weiqi, Zeng Haiyan, et al. Research on secure sharing of power application data based on blockchain[J]. Information Network Security, 2023, 23(08): 52-65.

[13] Li Yan, Ma Haiying, Wang Zhanjun. Research progress of key blockchain technologies[J]. Computer Engineering and Applications, 2019, 55(20): 13-23+100.

[14] BULLÓN PÉREZ J J, QUEIRUGA-DIOSA, GAYOSO MARTÍNEZV, et al.Traceability of ready-to-wear clothing through blockchain technology[J].Sustainability,2020,12(18): No.7491.

[15] LENG K, BI Y, JING L, et al.Research on agricultural supply chain systems with double chain architecture based on blockchain technology[J].Future Generation Computer Systems,2018,86: 641- 649.

[16] Sun Chunmei, Wang Zhuo. A review of hot topics in the application of blockchain technology in the field of education at home and abroad [J]. China Education Informatization, 2022, 28(05): 59-66.

[17] M. Madine, K. Salah, R. Jayaraman, Y. Al-Hammadi, J. Arshad and I. Yaqoob, "appXchain: Application-Level

Interoperability for Blockchain Networks," in IEEE Access, vol. 9, pp.87777-87791,2021,

doi:10.1109/ACCESS.2021.3089603.

[18] Szabo N. Formalizing and securing relationships on public networks [J]. First Monday, 1997, 2(9).