Journal of Applied Technology and Innovation
Vol. 09, Issue 1, 2025, pp. 05-09
e-ISSN:2600-7304-ISSN
Doi: https://doi.org/10.65136/jati.v9i1.23

Blockchain E-Certificate System with Ethereum Network and IPFS.

Joshua Samual [1*], Wong Yi Xing [1]

[1] Faculty of Computing and Technology, Asia Pacific University of Innovation and Technology Kuala Lumpur, Malaysia
*Corresponding Author: joshua.samual@apu.edu.my

Abstract

The certificate system is essential for academic organizations to provide proof of study or the level of skills and education. However, simply providing a physical cert or a virtual cert can be easily forged, and it will be difficult to be verified and authenticated. Many techniques are proposed to protect certificate's authenticity such as Digital Watermarking Technology, RSA Digital Signature. Furthermore, there are also Blockchain approaches such as integration of existing system and private blockchain. However, those systems have weaknesses such as the vulnerability to be cracked and efficiency in verification of the certificate. The aim of this research is to provide a system that is capable of securing certificate authenticity from activities of certificate fraud. In this research, we proposed a blockchain e-certificate system for academic organization and public to issue and verify e-certificate with a simple web-based user interface. By combining the advantages of using decentralized ledger for key information and utilize IPFS to store the certificate file, it can solve the problem of the vulnerability of the existing system.

Keywords: *Penetration Testing, Cybersecurity, Information Gathering, Security Assessment, Vulnerability Assessment, Reconnaissance.*

1. Introduction

Blockchain technology is one of the emerging revolutionary tools that is capable of fostering transparency and trust across various domains. One of its promising applications is in the issuance and verification of e-certificates [1][2][3]. As the trend of educational institutions and organizations shift toward digital certification, the need for a secure and tamper-proof system is essential. Blockchain-based e-certificate systems focus on addressing these needs by leveraging decentralized ledgers to provide authenticity, immutability, and accessibility [4][5][6]. This innovation is critical in combating challenges such as certificate forgery, fraudulent claims, and inefficient verification processes that plague traditional system. There are multiple proposed solutions and existing research for the demand of issuance and verification of e-certificates. For example, Digital Watermarking Technology [3], RSA Digital Signature on Certificate [5], Integration of blockchain and off-chain capabilities for the certificate. However, the existing research and approach for the e-certificate is having research gaps and weaknesses, such as the approach is still likely to be cracked and vulnerable to be forged, the algorithm used makes the issuance and the verification process slow and inefficient, or even the privacy can't be ensured when the data is uploaded into the public blockchain.

The integration of blockchain technology into the e-certificate system could be a solution, but there would be limitations. One pressing question is whether these systems can be widely adopted by institutions. Moreover, the challenges such as user privacy, interoperability, and the prevention of malicious use of public ledger should be addressed [9][10][11]. In a nutshell, it is crucial to overcome those technical and operational barriers to provide robust system that is capable of secure authenticity of academic certificate and be adopted. The primary objective of this research is to develop a blockchain-based e-certificate system to secure the authenticity of academic certificates by leveraging the immutability and temper-proof features of blockchain technology. This system aims to prevent the loss of certificates through the decentralized and immutable nature of blockchain and to provide a solution for employers and educational institutions to directly verify issued certificates. Furthermore, the study addresses critical problems, including vulnerabilities in credential authentication, inefficiencies in verification processes, and the need to protect user privacy while utilizing blockchain. The proposed system integrates the Ethereum blockchain with the Interplanetary File System (IPFS) as a platform for organizations to issue and verify certificates, ensuring a cost-effective, user-friendly, and secure solution accessible via web interfaces for computers and smartphones.

2. Literature Review

In Study [1] has proposed that academic institutions can build up their own private permissioned blockchain to allow external organizations to verify the certificate by requesting the academic institution. This solution seems alright, but it doesn't provide transparency and public verifiability on the certificate, it doesn't utilize the decentralize nature of blockchain as the verification can still be solely dependent on the personnel of in charge of verifying the certificate, which makes no difference of just directly use a normal local database for the academic institution to verify the certificate. In another study [2] has proposed a blockchain-based digital certificates system that is both privacy and security-aware by making the system having off-chain storage and operation. For this solution, the integration of off-chain capabilities significantly increases the complexity of implementation, and it forces the system to rely on centralized elements, which undermines the decentralization features of the blockchain. In [3] has proposed a solution of utilizing digital watermarking technology in e-certificate. This technique has achieved that the watermark can be incorporated into files or images but not noticeable by human eyes. The issuance and verification of the certificate will be completely relying on the watermark. Nevertheless, this technology is vulnerable to be attacked, people can use techniques such as cropping, resizing, compression to the file, which can potentially degrade or remove the digital watermark, which makes the solution is not secured or suitable real-world implementation.

[4] has proposed a system of embedding QR code with the information of digital signature for educational institution to issue the certificate. The main problem of the solution is that the way of directly showing QR code on the certificate makes the solution unreliable, everyone can just copy and paste the QR code into another file then the file will be authenticated by the system. In [5] proposed a technique of using RSA digital signature algorithm to ensure the authenticity of any kind of e-certificate. The use of this technique is particularly on having the digital signature on the name section of the certificate, which means it is embedded to one part of the sub-image inside of the certificate file. However, it is pointed out that the computation cost of the RSA operation can be really high.

3. Proposed Architecture

The proposed architecture shown in Figure 1 comprises three main components: a web application, the Ethereum network, and Interplanetary File System (IPFS) storage. The web application utilizes MetaMask as a tool for connecting and interacting with the Smart Contract deployed on the Ethereum network. Meanwhile, the backend of the application integrates with Pinata APIs to upload and pin files on IPFS.

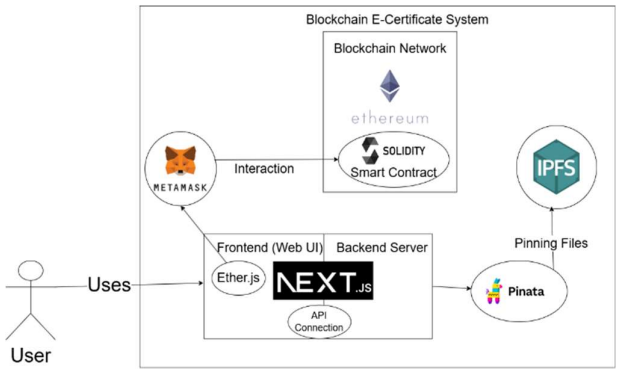

Figure 1 Architecture Diagram.

To ensure the security of issued certificates, several mechanisms have been designed and implemented throughout the certificate issuance process. First, only authorized organizations or personnel are permitted to issue certificates. When an approved user requests certificate issuance, they must undergo nonce verification through MetaMask, allowing the backend to proceed with the request. Once the certificate is generated, its unique Cert ID is encrypted using the AES-256 GCM algorithm and embedded into the file before being uploaded to IPFS storage and the Blockchain network. When users attempt to verify their certificates on the proposed system, only files containing the embedded encrypted Cert ID—generated by the system—can be successfully verified. This is achieved by decrypting the Cert *ID and matching it against the record stored on the Blockchain.*

The use of Ethereum blockchain acts as a decentralized, immutable ledger to store critical data for the system, such as unique cert ID generated by the system. By using smart contract to interact with the Blockchain network, the features of transparency and auditable record-keeping can ensure the certificate to be verified without intermediaries. Moreover, the use of Ethereum ensures global accessibility and robust security, which makes it ideal for issuing and managing digital credentials. IPFS is a distributed file system that enables efficient, secure, and decentralized storage of certificate PDF files. Unlike traditional storage, IPFS creates unique content-addressable links for each file, ensuring immutability and resistance to tampering. These characteristics of IPFS storage allows reliable retrieval of certificates globally, with lower storage costs and high scalability. AES-256 -GCM ensures the confidentiality and integrity of sensitive certificate information. The process of encryption protects data from unauthorized access and data tampering. By encrypting certificate ID before embedding them in files or storing them, the system is able to safeguards against malicious activities and ensures secure communication between users and the platform.

4. Results and Discussion

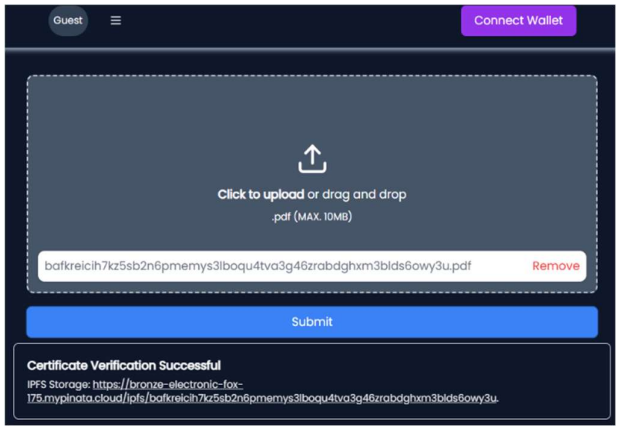

Figure 2 Certificate Verification.

Figure 2 is the home page of the proposed system; everyone who accesses the website is able to upload a file to know if it is an authenticate certificate from the system. The file will go through the authentication mechanism of the system to verify the file. Figure 3 shows the admin site; the admin is able to view all the organization and approve for organization to issue their certificate on the proposed system. Only these approved organizations have the access to issuing certificates.

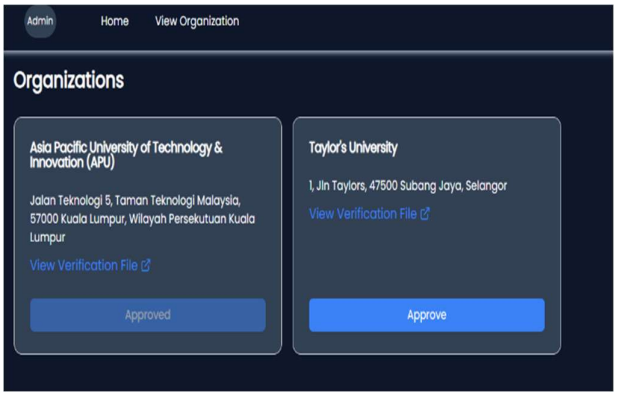

Figure 3 Admin View Organization

Figure 4 shows the MetaMask prompt for approving smart contract interaction. Whenever there is a need for smart contract interaction such as recording the certificate information inside of the blockchain. There is also a need for user approval from MetaMask to make sure the process is secure.

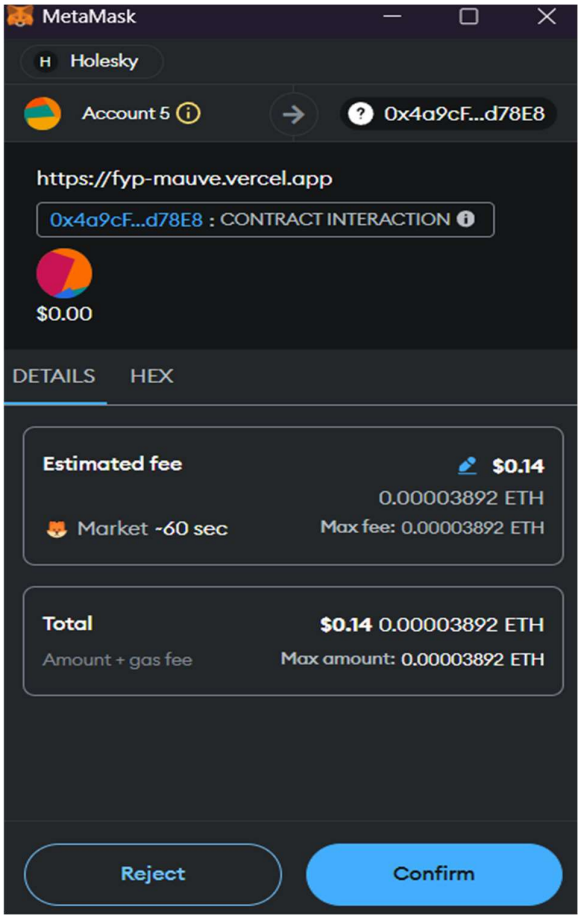

Figure 4 Metamask Request Approve for Contract Interaction

5. Conclusion

The need for security and verification of the issued certificate has been a big demand for employers and academic organizations. In this paper, it is presented a web application system that utilizes the features of decentralization by using Ethereum Blockchain network and IPFS Storage. In the system, the encryption by AES-256-GCM algorithm is the way of securing the data while the blockchain ledger and the IPFS storage is the place of storing the critical information and file storage. For future enhancement, it is essential that the system can leverage batch processing for organizations to issue large amount of certificate at once, the batch processing can be used by reading a dataset provided by organization, generate certificates based on the dataset, and potentially can also send the certificates via email to students.

References

[1] A. Tariq, H. B. Haq, and S. T. Ali, "Cerberus: A Blockchain-Based Accreditation and Degree Verification System," IEEE Transactions on Computational Social Systems, 2022, doi: https://doi.org/10.1109/TCSS.2022.3188453.

[2] M. Fernanda, M. Gustavo, and B. Carlos, "A privacy and security-aware blockchain based design for digital certificate," CLEI Electronic Journal, vol. 26, no. 1, May 2023.

[3] A. S. Al-Ajlan, "E-Learning Certificate Using Digital Watermarking Technology," IOSR Journal of Computer Engineering, vol. 16, no. 4, pp. 81–93, 2014, doi: https://doi.org/10.9790/0661-16458193.

[4] A. Singhal and R. S. Pavithr, "Degree Certificate Authentication using QR Code and Smartphone," International Journal of Computer Applications, vol. 120, no. 16, pp. 38–43, Jun. 2015, doi: https://doi.org/10.5120/21315-4303.

[5] K. Somsuk and M. Thakong, "Authentication system for e-certificate by using RSA's digital signature," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 18, no. 6, p. 2948, Dec. 2020.

[6] Nupur Vikhankar, Ankita Andhare, I. Barne, Prof. Anand Dhawale, and Sadaf Kauchali, "E-Certificate Verification Using Blockchain," International Journal of Engineering Research & Technology, vol. 13, no. 5, May 2024.

[7] J. A., P. Mahadik, S. Sanskar, T. Gupta, and Y. Meshram, "Certificate Issuing and Verification Application Using Blockchain," International Journal of Software Computing and Testing, vol. 10, no. 1, Jan. 2024, doi: https://doi.org/10.37628/ijsct.

[8] M. K. Pawar, P. Patil, R. Sawhney, Prem Gumathanavar, S. Hegde, and Kavya Maremmagol, "Performance Analysis of E-Certificate Generation and Verification using Blockchain and IPFS," 2022 International Conference on Inventive Computation Technologies (ICICT), pp. 345–350, Jul. 2022, doi: https://doi.org/10.1109/icict54344.2022.9850830.

[9] Qurotul Aini, Eka Purnama Harahap, L. Santoso, Siti Nurindah Sari, and Po Abas Sunarya, "Blockchain Based Certificate Verification System Management," Aptisi Transactions on Management (ATM), vol. 7, no. 3, pp. 1–10, Nov. 2022.

[10] P. Khati, A. K. Shrestha, and J. Vassileva, "Student Certificate Sharing System Using Blockchain and NFTs," arXiv (Cornell University), Jan. 2023, doi: https://doi.org/10.48550/arxiv.2310.20036.

[11] Pratik Thantharate and Anurag Thantharate, "ZeroTrustBlock: Enhancing Security, Privacy, and Interoperability of Sensitive Data through ZeroTrust Permissioned Blockchain," Big data and cognitive computing, vol. 7, no. 4, pp. 165–165, Oct. 2023, doi: https://doi.org/10.3390/bdcc7040165.