KARYA ILHAM PUBLISHING
CONNECTING MINDS, BRIDGING IDEAS, INSPIRING READERS

International Journal of Advanced Research in Computational Thinking and Data Science

Journal homepage:
https://karyailham.com.my/index.php/ctds/index
ISSN: 3030-5225

Blockchain Technology for Secure and Efficient Mobile Certificate Verification

Nor Hafiza Abd Samad[1,*], Nor Shamshillah Kamarzaman[1], Eliza Suraiya Tahir[1], Rukhiyah Adnan[1], Nurshafinas Roslan[1], Mohd Akmal Mohd Azmer[1]

[1] Faculty of Computing and Multimedia, Universiti Poly Tech Malaysia 56100 Cheras Kuala Lumpur, Malaysia

ARTICLE INFO

Article history:
Received 7 January 2025
Received in revised form 4 February 2025
Accepted 3 March 2025
Available online 5 March 2025

Keywords:
Block-chain; certificate; verification; smart contract

ABSTRACT

Increased fraudulent certificate cases have highlighted significant weaknesses in traditional certificate verification systems. Consequently, the demand for secure, transparent, and efficient methods to authenticate genuine certificates is more urgent than ever. This paper explores the use of blockchain technology to address the inherent challenges of certificate fraud and improve the security and effectiveness of certificate verification processes. Blockchain's tamper-proof nature and decentralized architecture provide an innovative solution to combat certificate fraud. This research examines integrating blockchain technology into a mobile certificate verification system, proposing a comprehensive framework to enhance security and efficiency. Smart contracts will be utilized to automate the verification process. When a certificate is issued, a smart contract is triggered to validate the certificate against predetermined criteria. This automation reduces human intervention and increases verification efficiency. The system will be developed using solidity programming tools and Ethereum smart contracts. Experimental certificates will be created to obtain and verify the certificates, and mobile Android apps will be developed. Upon project completion, certificates generated by UPTM will be embedded and verified on the blockchain, operating as a real-time system.

1. Introduction

The first blockchain protocol and infrastructure was implemented as Bitcoin [1]. Blockchain technology has built-in cryptographic algorithms to secure transactions and immunity against illegal modification. The system is automatically run and monitored by a smart contract to ensure non-interference and modification beyond the prescribed agreed rules in the smart contract. Thus, the stored data's security, integrity, immutability, privacy, and transaction mechanism are preserved

* *Corresponding author.*
E-mail address: hafiza@uptm.edu.my

https://doi.org/10.37934/ctds.5.1.18a

without third-party intervention. These characteristics are suitable for applications that need the prescribed features, including a certificate verification system. Due to these characteristics, it is a good idea that academic institutions have such systems for secure, reliable, and faster transactions.

Several previous works were related to implementing blockchain for certificate verification. Somehow, most of the smart contracts that administer the blockchain did not follow the standard practice of Ethereum's smart contract as suggested by professional practitioners and communities. The first principle is to have the source code of the smart contract exposed and accessed by the public. This is because the blockchain contains confidential information and involves financial storage, and transactions for third-party verification are not required. It is automatically self-regulated, executed, and digitally signed for secure and faster execution. The purpose is to verify the smart contract's correctness and provide the users' confidence [2].

2. Research Problem

In today's rapidly evolving digital landscape, verifying certificates and credentials is a critical process spanning various sectors such as education, employment, and professional certifications. Traditional verification methods often involve centralized databases and third-party intermediaries, leading to challenges such as data breaches, identity fraud, and inconsistent validation procedures. These vulnerabilities underscore the need for a more secure, transparent, and tamper-proof approach to certificate verification.

Blockchain technology has emerged as a potential solution due to its inherent features of decentralization, immutability, and cryptographic security. However, while growing interest and enthusiasm surrounds blockchain integration into certificate verification systems, a comprehensive understanding of the technical mechanisms, practical implementations, and potential benefits of blockchain-based verification systems remains elusive.

This paper addresses this knowledge gap by providing a comprehensive overview of how blockchain technology is harnessed for certificate and credential verification. While anecdotal evidence suggests that blockchain has the potential to enhance trust and security in the verification process, there is a lack of systematic analysis and empirical data to support these claims. Additionally, the challenges associated with integrating blockchain into existing verification systems, ensuring user privacy, scalability, and compliance with regulatory frameworks require thorough investigation.

Therefore, this paper's primary problem is: How can blockchain-based certificate verification systems be effectively designed, implemented, and adopted to ensure trust, security, and efficiency in verifying certificates and credentials across diverse domains? By delving into the technical underpinnings, practical use cases, challenges, and potential solutions, this research endeavors to contribute to the establishment of a more reliable and future-proof approach to certificate verification in the digital era.

3. Literature Review

Blockchain technology has emerged as a transformative solution in various sectors, and its application in academic certificate verification has garnered significant attention. This review aims to assess the efficiency and efficacy of utilizing blockchain technology to enhance the security and reliability of academic certificate verification processes based on the insights provided by the selected literature. The integration of blockchain protocols and smart contracts offers the promise of greater efficiency, transparency, and security in the verification process. However, critically evaluating the effectiveness and practical implications of these solutions is essential.

Previous studies have argued that blockchain integration can make academic certificates immutable and tamper-resistant [3]. They emphasize blockchain's decentralized architecture and its potential to mitigate issues related to fraudulent certificates. However, they lack a comprehensive empirical evaluation to demonstrate the proposed solution's real-world efficiency.

In contrast, blockchain implementation on certificate verification has potential positive impacts as discussed in [4]. They highlight blockchain's security-enhancing properties and its ability to address existing challenges. While the review provides valuable insights into the theoretical benefits of blockchain, it lacks concrete evidence of the technology's effectiveness in practical scenarios. In addition, other works proposed a more empirical approach to developing a blockchain-based application with smart contracts to automate the verification process [5,6]. While [6] lacks an empirical evaluation of the technology, [5] focuses on evaluation and provides evidence of improved accuracy and reduced errors in certificate verification. However, a broader scope in evaluating the technology's scalability, performance, and practical implementation on a large scale could enhance the comprehensiveness of the studies.

Quite several blockchain-based certificate verification methods have been published [7]. The application consists of additional components of QR code as part of certificate identity and certificate verification is done from the website. Somehow, the article did not show the source code of the smart contract, and there was no evidence that the application was tested for security and correctness. The work [8] was quite similar to [7], which used desktop GUI to interact and input the certificates. Several studies [9,10] proposed blockchain architecture for certificate verification without using QR codes. The authors [11,12] suggest adopting blockchain to provide tamper resistance for storing registry records and certificates. However, another study [13] proposed an integration of Certificate Authorities (CA) using Public Key Infrastructure with blockchain technology for storing and accessing the certificates.

More recent works that utilize smart contracts on blockchain have been done which include [14] developing a prototype that uses a hybrid proof-of-authority blockchain network to securely record curriculum vitae data and combat fake degrees or document frauds using QR Block CV and [15] proposed a permission blockchain-based system for verifying academic records using Hyperledger Fabric and InterPlanetary File System (IPFS) platform that supports smart contracts and private transactions among authorized participants. Tara Chandra et al. [16] also proposed a model based on blockchain technology that will publish, verify, and store the academic credentials of university stakeholders through the trustworthy proof of authority (PoA) as its consensus mechanism, which utilizes a smart contract for issuing the certificate to the blockchain network and file listing mechanism for revocation of issued digital certificate.

The previously mentioned did not show the smart codes and proof of experiment testing for security and correctness. Thus, there was no concrete evidence that the applications were completed, tested, and ready to be deployed. This application will be designed, coded, and tested to be ready to be deployed as a working system.

In conclusion, the reviewed literature collectively supports blockchain technology's great promise in transforming academic certificate verification systems. While the papers present valuable insights into the benefits of blockchain, there remains a gap in empirical evidence that robustly demonstrates the efficiency and efficacy of these solutions in real-world scenarios. To advance the field, future research should focus on rigorous empirical evaluations of the proposed solutions to provide a clearer picture of the technology's impact on efficiency, security, and reliability in academic certificate verification.

4. Research Objectives

The primary objective of this research is to:

i. To develop blockchain and innovate contract software for mobile certificate applications. This will ensure accessibility, protect graduates' certificates, simplify the verification system for employers and academic institutions, and reduce administrative burdens, enhancing productivity and streamlining the certification process
ii. To test the system's prototype to meet the standard secure and correct application requirements.
Blockchain technology improves security by utilizing decentralization, data integrity, and cryptographic algorithms to ensure UPTM certificate authenticity and reliability. Digital uploads create a transparent academic qualification ledger, reducing counterfeit certificates. Cryptographic methods secure the validation process, and digital signatures prevent cybercriminals from forging or modifying certificates. Decentralization prevents system failure and counterfeiting.

5. Methodologies

The proposed project focuses on developing and testing prototype software to meet the standard requirement. Thus, the methodology will focus on three aspects:

i. Mastering the design and programming skills for constructing smart contracts and blockchain.
ii. Designing system architecture and programming the smart contract and blockchain.
iii. Testing the prototype based on standard secure and correct blockchain application requirements.

5.1. Identification of Application Specification and Requirements

This stage focuses on doing the Literature Review and understanding the system specification and requirements. This includes understanding the cryptographic components of a blockchain and understanding the tools and programming requirements for coding the application.

5.2. System Architecture and Coding

This stage focuses on designing and coding the application. Figure 1 depicts the general architecture of the application which involves the stakeholders and computing components. The stakeholders involve the graduates, the university, and the employer. The flow of the process is quite straightforward. Once the student graduates, the university issues the certificate to the students and, at the same time, will store the certificates in the blockchain. The employer will check, using the app, the authenticity of the certificate presented by the potential job applicant. The apps will verify the certificate with the blockchain, which is publicly accessible, and the apps will respond whether it is valid or not.

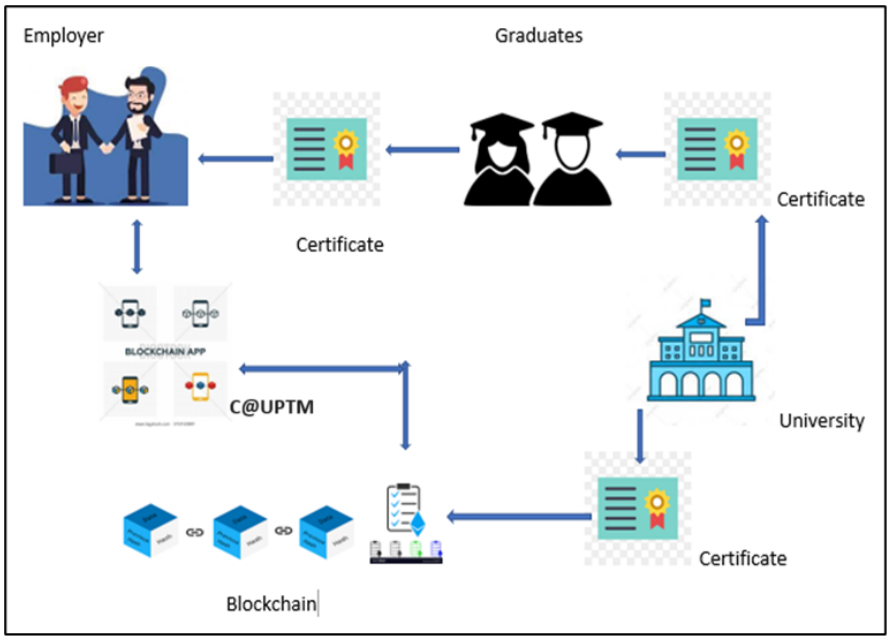

Fig. 1. Architecture of C@UPTM Blockchain Certificate Verification Application

5.3. System Design

This stage focuses on the stakeholders' user interfaces. The UPTM e-SCROLL system is designed to streamline and simplify verifying academic qualifications issued by Universiti Poly-Tech Malaysia (UPTM). The system's architecture is typically based on a client-server model, where users can interact with the system to confirm the authenticity of academic credentials.

5.3.1. Web application components

- User Interface
  The UPTM e-SCROLL system's user interface (UI) is designed to be appealing and easy to use, providing a seamless experience for end users. Key features include result displays, input forms, and navigation menus, all contributing to the overall functionality and user experience.
- Verification Form for Certificates
  The verification process within the UPTM e-SCROLL system is designed to be user-friendly and secure. Robust validation methods ensure the accuracy and completeness of the information provided. By incorporating real-time validation, error feedback, and user support features, the system facilitates a seamless and efficient verification experience for all users.
- Display of Verification Result
  This is the part where the validity status is shown. When the verification process is completed, the UPTM e-SCROLL system presents the result, indicating whether the certificate is valid or invalid. Additionally, the result display provides detailed information, including program specifics, certification timestamps, and certificate holder details.

Fig. 2. C@UPTM Blockchain Certificate Verification Application Dashboard

5.3.2. Use case diagram

The use case diagram is an important component of the certificate verification system with blockchain technology for UPTM project analysis. It provides a graphical representation of the system's functionalities and interactions among various actors, laying the groundwork for understanding the system's dimensions, essential actors, and interactions. Figure 3 shows the use case diagram for this project.

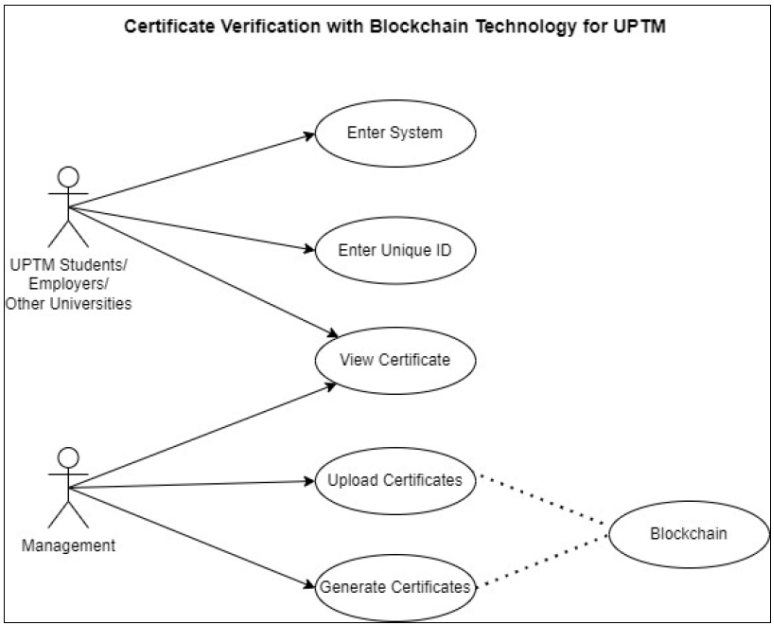

Fig. 3. Use Case Diagram of C@UPTM Blockchain Certificate Verification Application

The use case graphic illustrates how users can interact with the system by highlighting the important use cases, such as uploading certificates and generating the certificates using blockchain. It also emphasizes the connectivity of various use cases and actors, highlighting how they collaborate and share information to accomplish the expected outcomes. This understanding is necessary for

developing system functionality and providing a consistent user experience. The use case diagram is a framework for the certificate verification system's extensive analysis and design.

6. Expected Finding

It is expected that at the end of the project, the real certificates produced by UPTM can be embedded and verified in the Blockchain and run as a real-time system. Thus, improve the security and effectiveness of certificate verification processes to combat certificate fraud.

7. Conclusion

The effective integration of blockchain technology in UPTM's certificate verification initiative has significantly enhanced security and transparency. Using smart contracts and blockchain technology to create a web system is a significant and impactful effort, resulting in a shift towards a user-centered approach and seamless functionality. After a successful user demonstration, the project demonstrates the team's dedication to ongoing enhancement, flexibility in response to new technology, and stakeholder involvement, all of which contribute to a safe, open, and effective ecosystem.

As institutions grapple with verifying academic credentials and combating certificate fraud, blockchain's potential remains compelling. Future research endeavors should address the existing gaps by conducting rigorous evaluations that showcase the technology's efficiency and scalability and examine its integration challenges, potential bottlenecks, and long-term sustainability.

In closing, the system developed proof of blockchain technology's potential to revolutionize academic certificate verification systems. However, further research is essential to bridge the gap between theoretical promises and practical implementations, ensuring that blockchain-based solutions can truly deliver on their potential to reshape the landscape of academic credential verification.

Acknowledgment

We gratefully acknowledge the extensive support offered by Universiti Poly-Tech Malaysia, which includes full provision for this project under the auspices of the UPTM University Research Grant (URG).

References

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." *Satoshi Nakamoto* (2008).

[2] Emmons D. "How to Verify and Publish on Etherscan." *Coinmonks* (2022).

[3] Rahardja, Untung, Achmad Nizar Hidayanto, Panca Oktavia Hadi Putra, and Marviola Hardini. "Immutable ubiquitous digital certificate authentication using blockchain protocol." *Journal of applied research and technology* 19, no. 4 (2021): 308-321. https://doi.org/10.22201/icat.24486736e.2021.19.4.1046

[4] Kumutha, K., and S. Jayalakshmi. "The impact of the blockchain on academic certificate verification system-review." *EAI Endorsed Transactions on Energy Web* 8, no. 36 (2021).

[5] Leka, Elva, and Besnik Selimi. "Development and evaluation of blockchain based secure application for verification and validation of academic certificates." *Annals of Emerging Technologies in Computing (AETiC)* 5, no. 2 (2021): 22-36. https://doi.org/10.33166/AETiC.2021.02.003

[6] Chaudhari, Smita, Soham Mohite, Shreya Kumbhakarn, Viren Rathod, and Sakshi Khairnar. "Blockchain based solution for academic certificate management system using smart contract." *International Journal of Science and Research Archive* 8, no. 1 (2023): 291-297. https://doi.org/10.30574/ijsra.2023.8.1.0037

[7] Cheng, Jiin-Chiou, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen. "Blockchain and smart contract for digital certificate." In *2018 IEEE international conference on applied system invention (ICASI)*, pp. 1046-1051. IEEE, 2018. https://doi.org/10.1109/ICASI.2018.8394455

[8] Poorni, R., M. Lakshmanan, and S. Bhuvaneswari. "DIGICERT: a secured digital certificate application using blockchain through smart contracts." In *2019 International Conference on Communication and Electronics Systems (ICCES)*, pp. 215-219. IEEE, 2019. https://doi.org/10.1109/ICCES45898.2019.9002576

[9] Gayathiri, A., J. Jayachitra, and S. Matilda. "Certificate validation using blockchain." In *2020 7th International Conference on Smart Structures and Systems (ICSSS)*, pp. 1-4. IEEE, 2020. https://doi.org/10.1109/ICSSS49621.2020.9201988

[10] Xie, Rui, Yuhui Wang, Mingzhou Tan, Wei Zhu, Zhongjie Yang, Jiaji Wu, and Gwanggil Jeon. "Ethereum-blockchain-based technology of decentralized smart contract certificate system." *IEEE Internet of Things Magazine* 3, no. 2 (2020): 44-50. https://doi.org/10.1109/IOTM.0001.1900094

[11] Nurhaeni, Tuti, Indri Handayani, Frizca Budiarty, Desy Apriani, and Po Abas Sunarya. "Adoption of upcoming blockchain revolution in higher education: Its potential in validating certificates." In *2020 Fifth International Conference on Informatics and Computing (ICIC)*, pp. 1-5. IEEE, 2020. https://doi.org/10.1109/ICIC50835.2020.9288605

[12] Vidal, Fernando Richter, Feliz Gouveia, and Christophe Soares. "Revocation mechanisms for academic certificates stored on a blockchain." In *2020 15th Iberian conference on information systems and technologies (CISTI)*, pp. 1-6. IEEE, 2020. https://doi.org/10.23919/CISTI49556.2020.9141088

[13] Zhao, Jian, Zexuan Lin, Xiaoxiao Huang, Yiwei Zhang, and Shaohua Xiang. "TrustCA: achieving certificate transparency through smart contract in blockchain platforms." In *2020 International Conference on High Performance Big Data and Intelligent Systems (HPBD&IS)*, pp. 1-6. IEEE, 2020. https://doi.org/10.1109/HPBDIS49115.2020.9130581

[14] Seng, Vincent Lew Kok, Au Thien Wan, Ibrahim Venkat, Ravi Kumar Patchmuthu, and Serina Hj Mohd Ali. "Blockchain technology in securing academic credentials: Mobile QR block CV." In *AIP Conference Proceedings*, vol. 2968, no. 1. AIP Publishing, 2023. https://doi.org/10.1063/5.0181098

[15] Khaleelullah, Shaik, Sai Teja Vangapalli, Malavika Gaddam, Vitesh Sai Hanumakonda, and Uday Kiran Goud Gangapuram. "Verifcation of academic records using hyperledger fabric and ipfs." In *2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN)*, pp. 210-217. IEEE, 2023. https://doi.org/10.1109/ICPCSN58827.2023.00040

[16] Chandra, Tara, Mandeep Kaur, Nitin Rakesh, Monali Gulhane, and Sudhanshu Maurya. "Novel blockchain-based framework to publish, verify, and store digital academic credentials of universities." *International Journal of Information Technology* (2024): 1-9. https://doi.org/10.1007/s41870-024-01842-w