JIKO (Jurnal Informatika dan Komputer) Accredited KEMDIKTISAINTEK, No.0173/C3/DT.05.00/2025
Vol. 9, No. 1, April 2026, pp. 85-92 p-ISSN: 2614-8897
DOI: 10.33387/jiko.v9i1.11356 e-ISSN: 2656-1948

IMPLEMENTATION OF BLOCKCHAIN IN A SEMINAR SYSTEM FOR ELECTRONIC CERTIFICATE VERIFICATION USING SMART CONTRACTS

Sahri Ramadan[1*], Sawali Wahyu[2], Budi Tjahjono[3], Riya Widayanti[4]

[1, 2] Department of Informatics Engineering, Faculty of Computer Science, Universitas Esa Unggul, Bekasi 17214, Indonesia
Email: [*1] sahriramadan000@student.esaunggul.ac.id, [2]sawaliwahyu@esaunggul.ac.id,
[3]budi.tjahjono@esaunggul.ac.id, [4]riya.widayanti@esaunggul.ac.id

(Received: 18 January 2026, Revised: 02 February 2026, Accepted: 12 March 2026)

Abstract

The increasing adoption of electronic certificates in academic and professional environments raises critical challenges related to authenticity, data integrity, and verification reliability. Conventional certificate management systems commonly rely on centralized architectures and manual validation procedures, which are vulnerable to manipulation, duplication, and single points of failure (SPoF). This study proposes a blockchain-based electronic certificate verification system implemented on a private Hyperledger Fabric network using smart contracts. The system records certificate verification metadata on a distributed ledger to ensure integrity and traceability while maintaining storage efficiency. Smart contracts automate the issuance and validation lifecycle, enabling transparent and tamper-resistant certificate management. The verification process is conducted by comparing document authentication data with records stored on the blockchain. Experimental evaluation demonstrates that the proposed system can accurately identify document alterations and consistently distinguish between valid and invalid certificates. The results indicate that the integration of blockchain and smart contracts as an active validation mechanism enhances transparency, reduces dependence on centralized authorities, and improves trust in mobile-based digital credential systems. Therefore, the proposed approach provides a secure and reliable framework for electronic certificate verification in academic environments.

Keywords: *Blockchain, Electronic Certificates, Smart Contracts, Hyperledger Fabric, Hash-Based Verification*

**Corresponding Author: Sahri Ramadan*

1. INTRODUCTION

Digital transformation in academic services has accelerated the adoption of electronic certificates in various activities, including seminars, training programs, and competency development initiatives. Compared to physical documents, digital certificates provide greater efficiency in terms of distribution, storage, and accessibility. However, these advantages also introduce new challenges, particularly with respect to document authenticity, data integrity, and long-term verification reliability. Most existing certificate management systems continue to rely on centralized databases and manual validation procedures, which increases their vulnerability to unauthorized modification, duplication, and administrative errors. Furthermore, dependence on a single authoritative entity creates a single point of failure and limits the transparency and accountability of the authentication process. [1], [2].

In recent years, blockchain technology has been increasingly adopted as a potential solution to address these limitations. Its distributed and immutable characteristics enable data to be permanently recorded and resistant to unauthorized modification, making blockchain particularly suitable for applications that require a high level of trust and reliability [3]. Several studies have demonstrated that the application of blockchain in digital certification systems can significantly enhance data integrity, transparency, and information traceability [4], [5]. Furthermore, the integration of automated validation mechanisms through smart contracts has been shown to streamline verification processes and reduce dependence on manual inspections and institutional intervention [6]. In addition, the utilization of QR codes facilitates rapid

access to verification services and improves overall user convenience and system usability[7].

Nevertheless, most existing approaches continue to position blockchain primarily as a passive recording medium rather than as an active validation mechanism integrated into system workflows. Centralized architecture remains dominant in many electronic certificate implementations, requiring external parties to directly contact issuing institutions to verify document authenticity. Such procedures are often inefficient, time-consuming, and susceptible to human error [8], [9]. Furthermore, several studies have reported that conventional systems lack automated mechanisms for detecting unauthorized data modifications, making document tampering difficult to identify without extensive manual inspection and administrative intervention [10].

Blockchain introduces a distinct paradigm through its distributed, transparent, and tamper-resistant recording mechanisms. In the context of certificate verification, blockchain can function as a single source of truth by permanently storing verification-related information and enabling continuous auditability [11]. To ensure storage efficiency, the system does not require the entire certificate file to be stored on the distributed ledger. Instead, cryptographic hash values are utilized as unique digital representations of documents. Due to their high sensitivity to data alterations, even minor modifications to certificate content generate significantly different hash values, allowing unauthorized changes to be automatically detected [12], [13].

The role of blockchain is further reinforced through the implementation of smart contracts, which enable validation rules to be executed automatically, consistently, and transparently without reliance on third-party intermediaries. Through this mechanism, certificate issuance and verification processes are no longer dependent on centralized authorities but are instead governed by predefined and verifiable logical rules embedded within the system architecture [6], [14]. Recent studies further indicate that permissioned blockchain networks, such as Hyperledger Fabric, are particularly suitable for academic environments, as they provide robust access control, configurable authorization policies, and efficient audit and governance mechanisms [11], [15].

Based on the identified challenges, this study proposes a blockchain-based electronic certificate validation system integrated into a mobile application environment. The system utilizes a private Hyperledger Fabric network as its core infrastructure, while smart contracts are employed to automate certificate recording and verification processes. Instead of storing complete certificate files, the system records cryptographic hash values on the blockchain ledger to ensure data integrity and storage efficiency. Certificate verification is performed through QR code scanning, enabling users to independently, rapidly, and objectively authenticate document validity.

The primary contribution of this study lies in the implementation of blockchain as an active validation mechanism rather than merely as a digital archive. Unlike previous approaches that are predominantly conceptual or limited to web-based platforms, the proposed system provides an end-to-end mobile-based verification workflow. Through this design, the system enables automatic detection of unauthorized data modifications, enhances transparency, and reduces dependence on centralized authorities. These findings are expected to serve as a reference framework for developing secure, reliable, and adaptable digital certification systems in modern academic environments [5], [11], [16].

2. RESEARCH METHOD

This study adopts a systems engineering approach that emphasizes the systematic design, implementation, and evaluation of a blockchain-based electronic certificate validation system within a mobile application context. This approach was selected because the primary objective of the research is not only to analyze specific phenomena but also to develop a functional system that can be practically deployed to address digital document authentication challenges. Consistent with several previous studies, the systems engineering approach is considered appropriate for developing blockchain-based solutions that require the integration of software architecture, security mechanisms, and user interaction workflows [11], [15].

In this study, blockchain is positioned not merely as a passive storage medium but as an active validation component that determines certificate authenticity based on records maintained on a distributed ledger. This approach aligns with the single source of truth principle, which is widely applied in digital credential verification systems, where validity decisions are no longer dependent on centralized databases [11], [12].

2.1 System Architecture

The system is developed using a private blockchain network based on Hyperledger Fabric, which belongs to the category of permissioned blockchains. This architecture enables comprehensive identity management, configurable access control, and the enforcement of authorization policies in a controlled environment, making it particularly suitable for academic institutions that require strong governance and transparent audit mechanisms [11], [15]. Unlike public blockchain platforms, this approach provides greater flexibility in defining organizational roles, such as administrators, organizers, and students, while preserving fundamental principles of transparency and data integrity.

In addition, Hyperledger Fabric supports modular smart contract implementation, allowing certificate

recording, issuance, and verification rules to be explicitly encoded as programmable logic. This mechanism ensures that all transactions comply with predefined procedures and are executed automatically, thereby reducing dependence on manual operations and minimizing the risk of human error.

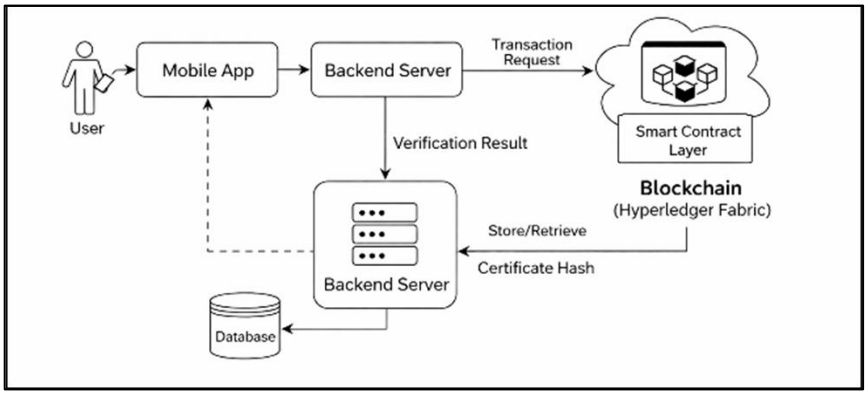

Figure 1. Blockchain-Based Certificate Validation System Architecture

As illustrated in Figure 1, the system architecture is structured into three primary layers: the mobile application, the backend server, and the blockchain network. This layered design aims to preserve system modularity, facilitate maintainability and development, and enhance scalability without affecting existing components [4]. Furthermore, functional separation across layers contributes to improved system security, as each component operates with clearly defined responsibilities and limited privileges.

The mobile application functions as the primary user interface, enabling students and external stakeholders to access digital certificates and initiate verification procedures. At this layer, users interact exclusively with informational content and do not have direct access to blockchain recording mechanisms. The backend server is responsible for managing core application logic, including processing user requests, retrieving certificate-related metadata, and securely forwarding validation requests to the blockchain network.

Meanwhile, the blockchain network functions as the primary validation layer that permanently and immutably stores certificate hash values. Through this mechanism, the system does not retain complete certificate documents on the distributed ledger; instead, it records only cryptographic representations, thereby ensuring storage efficiency without compromising security.

Under this architectural separation, conventional databases are utilized solely for storing operational data, such as user information and certificate-related metadata, and do not participate in determining document authenticity. Validation decisions are derived exclusively from blockchain records, thereby reducing manipulation risks, enhancing transparency, and minimizing dependence on centralized authorities [3], [11]. This design positions blockchain as the single source of truth within the digital certificate verification framework.

2.2 Certificate Recording Mechanism

The certificate recording mechanism in the proposed system is implemented by generating a cryptographic hash value for each issued certificate document. This hash value serves as a unique digital representation of the document's content, such that even minor modifications result in significantly different outputs. Owing to this property, hash values can be utilized as reliable indicators of document authenticity without requiring the complete file to be stored on the blockchain. This approach is widely adopted in blockchain-based verification systems, as it enhances storage efficiency while maintaining data integrity. [12], [13].

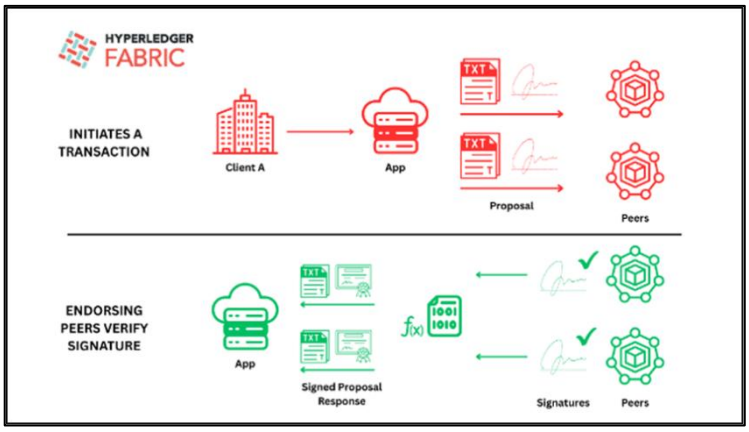

Figure 2. Proposal Submission and Endorsement Process in Hyperledger Fabric

As illustrated in Figure 2, after the hash value is generated, the corresponding data are submitted as a transaction proposal to the Hyperledger Fabric network. This proposal is subsequently evaluated by multiple endorsing peers in accordance with the rules specified in the deployed smart contract. Each peer verifies whether the transaction complies with predefined endorsement and validation policies, thereby ensuring that only transactions meeting the required criteria are authorized to proceed. This mechanism enables a distributed verification process that does not rely on a single controlling entity, thereby enhancing system reliability and trustworthiness [15] .

Once the endorsement policy is satisfied, the transaction is forwarded to the ordering service, where it is assembled into a block before being permanently committed to the distributed ledger. This stage ensures that transaction sequencing remains consistent across all network nodes and prevents potential data conflicts. Through this process, recorded data cannot be modified or removed, thereby fulfilling the immutability property that characterizes blockchain technology [11], [4].

Furthermore, each successfully committed transaction generates a unique transaction identifier that functions as an auditable record. This identifier enables transparent and verifiable tracing of certificate history by both institutional authorities and external stakeholders, thereby strengthening overall system accountability [11].

2.3 Certificate Verification Process

The certificate verification process is designed to be independently performed by users through QR code scanning embedded within digital documents. The QR code functions as an initial identifier that directs the system to retrieve corresponding certificate hash data stored on the blockchain network. This approach enables authentication to be conducted efficiently without requiring direct interaction with issuing institutions. In addition to improving operational efficiency, this mechanism enhances user convenience by providing flexible and on-demand access to verification services [7].

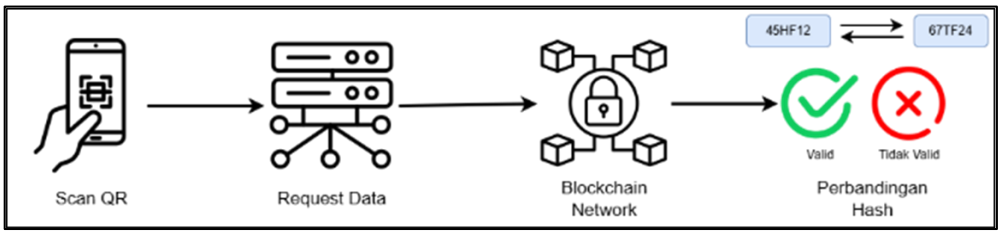

Figure 3. Blockchain-Based Certificate Verification Workflow

As illustrated in Figure 3, after the hash data are retrieved from the blockchain, the system recalculates the hash value of the certificate document submitted by the user. The newly generated hash value is then compared with the corresponding value stored on the distributed ledger. This comparison constitutes the primary basis for determining document authenticity. If both hash values are identical, the certificate is classified as valid. Conversely, any discrepancy indicates that the document has been altered or does not correspond to the recorded data and is therefore classified as invalid.

This mechanism positions blockchain as the single source of truth in the validation process, rather than centralized databases [3], [11]. Consequently, verification decisions are derived from permanently and distributively recorded data rather than institutional claims or subjective assessments. This approach enhances the objectivity of the validation process and significantly reduces the potential for data manipulation.

The utilization of cryptographic hash values as document representations ensures data integrity, as their high sensitivity to data alterations enables automatic detection of unauthorized modifications [12], [13]. Through this approach, the system not only verifies certificate authenticity but also provides early detection of even minor changes in document content without reliance on subjective manual inspection.

2.4 Scope of System Testing

System testing in this study is primarily focused on evaluating the reliability of the blockchain-based validation mechanism rather than on interface aesthetics or user experience aspects. This focus was adopted because the main objective of the research is to assess the system's capability to preserve data integrity and to determine certificate authenticity objectively. Accordingly, testing activities are directed toward the core system functionalities, including data recording, storage, and verification processes within the blockchain network. A similar evaluation approach has been adopted in previous studies that emphasize security, data consistency, and verification reliability [5], [11].

All testing scenarios are designed to examine the extent to which the system can maintain the tamper-resistant and fault-tolerant properties that represent key advantages of blockchain technology [15]. The system is expected to consistently produce accurate verification results even in the presence of unauthorized data modifications or partial network disruptions.

The results of each testing scenario are subsequently analyzed to evaluate the effectiveness of blockchain as an active validation infrastructure for digital certificates. Through this approach, the evaluation considers not only technical functionality but also system resilience to data manipulation, consistency of validation outcomes, and the ability to sustain user trust in document authenticity.

3. RESULTS AND DISCUSSION

This section presents the results of implementing the proposed blockchain-based certificate validation system and discusses its reliability, security, and operational effectiveness. The evaluation focuses on the system's capability to ensure data integrity, detect unauthorized document alterations, and provide an objective verification mechanism independent of centralized authorities. These characteristics are essential for digital certification systems, where institutional credibility and user trust play a critical role.

Recent studies have emphasized that blockchain-based credential systems can enhance transparency, traceability, and verification reliability in academic environments [11], [12], [16]. In particular, multiple case studies have demonstrated that distributed ledger technologies significantly improve trust in digital certificates by eliminating single points of failure and reducing institutional dependency [17].

The results obtained from system implementation and testing are analyzed to examine the extent to which blockchain technology fulfills these requirements. Furthermore, this section discusses how the proposed mechanism improves operational efficiency, mitigates data manipulation risks, and strengthens confidence in electronic certificate authenticity.

3. 1 Implementation of the Blockchain-Based Certificate Validation System

The implementation results indicate that blockchain can function as an active validation infrastructure rather than merely serving as a data storage medium. Unlike conventional systems that rely on centralized databases and manual verification procedures, the proposed system positions blockchain as the primary source of truth for determining document authenticity. Consequently, certificate validity is established through distributed ledger records rather than institutional confirmation.

This design is consistent with decentralized credential systems developed using Hyperledger Fabric, which emphasize permissioned network architecture, smart contract automation, and distributed endorsement mechanisms [16], [18]. By adopting this approach, the system ensures that verification decisions are generated objectively by network consensus.

In the developed architecture, certificate files are not stored directly on the blockchain. Instead, verification-related metadata is recorded to maintain storage efficiency and data integrity. This strategy enables automatic detection of unauthorized modifications while minimizing computational and storage overhead [12], [17].

The integration of the mobile application, backend services, and blockchain network allows users to perform certificate verification independently. Users initiate verification by scanning QR codes embedded in certificates, which triggers authentication and validation processes across system layers. This mechanism improves verification speed, enhances transparency, and reduces administrative dependency [7] , [16].

Furthermore, the immutability of blockchain records reinforces user trust in verification outcomes. Since validation data cannot be altered unilaterally, the system ensures that authenticity decisions remain objective and resistant to manipulation. As a result, blockchain functions not only as a technical platform but also as a core component in institutional decision-making.

3. 2 Results of the Certificate Recording Mechanism Implementation

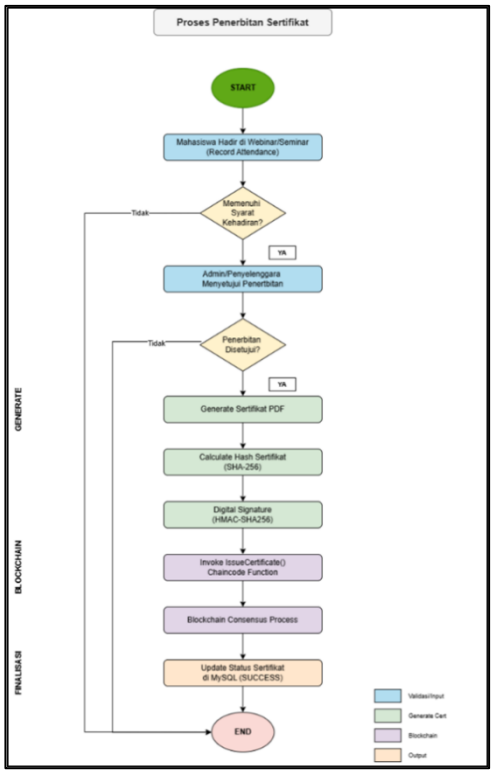

Figure 4. Certificate Recording Mechanism Based on Hyperledger Fabric

As illustrated in Figure 4, the certificate recording process begins with the verification of participant attendance in academic activities. Attendance records are evaluated based on predefined eligibility criteria. Certificates are issued only when these requirements are satisfied, ensuring systematic enforcement of participation standards.

After approval, the system automatically generates certificate documents in PDF format. Prior to blockchain submission, verification metadata is generated and secured using cryptographic mechanisms. This information is subsequently transmitted to the blockchain network for permanent recording.

The recording process is executed through the invocation of the issueCertificate() function within the smart contract. Submitted transactions undergo endorsement and consensus procedures based on predefined network policies. This process ensures that only valid and authorized records are committed to the distributed ledger, consistent with Hyperledger Fabric governance principles [15], [18].

Once validated, certificate records are permanently stored and synchronized with the operational database. This workflow positions blockchain as an active validation component rather than a passive storage layer.

The immutability of blockchain records guarantees that stored data cannot be modified after confirmation. Each transaction also generates a unique identifier that functions as an audit trail, enabling transparent monitoring of certificate issuance activities [11], [17]. These results demonstrate that the implemented recording mechanism supports accountability and distributed validation, distinguishing it from conventional centralized systems.

Figure 5. Certificate Verification Result Interface in the Mobile Application

Figure 6 illustrates verification outcomes displayed through the mobile application interface. The system presents validity status in a concise and user-friendly format, enabling users to interpret results without technical complexity.

At this stage, the mobile application functions exclusively as a presentation layer. All validation decisions are generated by blockchain-based processes, ensuring protection against client-side manipulation and centralized interference. These findings further confirm blockchain's role as the primary validation infrastructure in digital certification systems [11], [16].

3. 3 Results of the Blockchain-Based Validation System Testing

System testing was conducted to evaluate the reliability and consistency of the blockchain-based validation mechanism under various operational conditions. Testing scenarios included authentic certificates, modified documents, unregistered QR codes, and multi-node data retrieval.

Table 1. Results of the Blockchain-Based Certificate Validation System Testing

No.	Test Scenario	Expected Result	Actual Result
1	Authentic certificate	Valid	Valid
2	Modified certificate	Invalid	Invalid
3	Unregistered QR code	Invalid	Invalid
4	Data retrieval from different nodes	Consistent	Consistent

The system consistently classified certificate status across all test scenarios. Authentic certificates were correctly identified, while modified and unregistered documents were automatically rejected.

Multi-node retrieval tests confirmed data replication consistency within the distributed network.

This property ensures system reliability even under partial node failures, thereby reducing single-point-of-failure risks [15], [18]. Overall, the results demonstrate that blockchain actively contributes to system robustness, objectivity, and operational reliability.

3. 4 Discussion

The implementation and evaluation results demonstrate that blockchain can function as an active validation infrastructure rather than merely serving as a digital archive. By positioning the distributed ledger as the primary source of truth, the system determines certificate authenticity objectively without institutional dependency. This finding is consistent with recent case studies and framework-based analyses emphasizing blockchain's role in strengthening digital credential trust [16], [17].

Compared to conventional systems, the proposed approach offers several advantages. First, distributed validation enables automatic detection of document inconsistencies. Second, decentralized data recording enhances transparency and auditability. Third, QR code integration improves user accessibility and verification efficiency [7], [16].

Nevertheless, the system presents certain limitations. Blockchain deployment requires relatively complex infrastructure and specialized network management. System performance is influenced by endorsement policies, node distribution, and network latency. These factors may affect scalability in large-scale institutional environments.

3. 5 Comparison with Existing Studies (State-of-the-Art Analysis)

Several recent studies have explored blockchain-based digital certificate systems in academic contexts. Jaafar and Alsaad [11] integrated Hyperledger Fabric with IPFS to enhance decentralization and data availability. Noorhizama et al. [7] implemented QR-code-based verification using the Ethereum platform, emphasizing public blockchain transparency. In addition, recent case studies have demonstrated that blockchain adoption improves institutional trust and administrative efficiency[17].

Framework-oriented studies have further proposed decentralized credential systems based on Hyperledger Fabric, highlighting the importance of governance mechanisms, endorsement policies, and participatory validation models [16], [18]. However, most existing approaches still treat blockchain primarily as a recording medium and retain partial dependence on centralized administrative procedures.

In contrast, the proposed system adopts blockchain as an active validation mechanism that directly governs certificate issuance and verification through smart contracts. The validation process is fully integrated into a mobile application environment, enabling end-to-end authentication without institutional intervention.

Furthermore, the emphasis on real-time verification, distributed endorsement, and automated decision logic distinguishes this study from predominantly web-based and institution-centered implementations. The integration of mobile access, smart contract automation, and distributed validation provides a scalable and practical framework for academic deployment.

Therefore, this study contributes not only a technical implementation but also an operational model for blockchain-based certificate verification in real institutional environments.

4. CONCLUSION

This study has presented the design and implementation of a blockchain-based electronic certificate validation system using Hyperledger Fabric and smart contracts. The proposed system enables secure, transparent, and decentralized certificate issuance and verification by positioning blockchain as the primary source of truth. Experimental evaluation demonstrates that the system can accurately distinguish between valid and invalid certificates, reduce institutional dependency, and enhance user trust in digital credentials.

Despite these contributions, several limitations should be acknowledged. First, the current implementation has been evaluated within a limited institutional environment, which may not fully represent large-scale or multi-institutional deployment scenarios. Second, system performance is influenced by network configuration, endorsement policies, and node distribution, which may affect scalability under high transaction volumes. Third, the proposed framework has not yet been integrated with national or international credential interoperability standards, which may limit cross-institutional adoption.

Future research should address these limitations by conducting large-scale performance evaluations involving multiple institutions and geographically distributed nodes. Further studies may also explore the integration of the proposed system with standardized digital credential frameworks and national education databases. In addition, advanced privacy-preserving techniques, such as zero-knowledge proofs or selective disclosure mechanisms, can be incorporated to enhance data confidentiality. Finally, optimizing consensus mechanisms and smart contract execution efficiency may further improve system scalability and real-time responsiveness.

Overall, the proposed system provides a practical foundation for developing secure and trustworthy blockchain-based digital credential services in academic environments. With further refinement and large-scale validation, this approach has strong potential to support sustainable and interoperable digital certification ecosystems.

Acknowledgment

The authors would like to express their sincere gratitude to the Faculty of Computer Science, Universitas Esa Unggul, for the academic support and facilities provided throughout the course of this research. Appreciation is also extended to the academic supervisors and colleagues who offered constructive feedback during both the system design phase and the manuscript refinement process. Their contributions were invaluable in ensuring that this study was completed systematically and in accordance with scientific writing standards.w

5. REFERENCE

[1] C. Gayathri, M. Rani, P. Sai Kumar, M. D. Mushaarof, B. Tech, and T. S. Reddy, "Decentralized Certificate Authentication with Blockchain Technology," 2025. [Online]. Available: www.ijerst.com

[2] D. Setiowati *et al.*, "A Blockchain System for Digital Sertificate Verification On E-Learning," *Kumpulan jurnaL Ilmu Komputer (KLIK)*, vol. 08, no. 3, 2021.

[3] N. and Y. Xu, "Development of Blockchain-Based Academic Credential Verification System," *OAlib*, vol. 11, no. 09, pp. 1–20, 2024, doi: 10.4236/oalib.1112130.

[4] A. Djajadi, K. S. Lestari, L. E. Englista, and A. Destaryana, "Blockchain-Based E-Certificate Verification and Validation Automation Architecture to Avoid Counterfeiting of Digital Assets in Order to Accelerate Digital Transformation," *CCIT (Creative Communication and Innovative Technology) Journal*, vol. 16, no. 1, 2023.

[5] H. Wijayanto and P. M. Waliyullah, "Aplikasi Verifikasi Sertifikat Berbasis Website Menggunakan Blockchain," *Jurnal InFact Sains dan Komputer*, vol. 8, no. 02, pp. 35–42, Aug. 2024, doi: 10.61179/jurnalinfact.v8i02.586.

[6] A. R. Febriansyah, Nazulasari, and N. Ramadhona, "Optimalisasi Smart Contract Untuk Sistem Sertifikasi Digital Pada Public Blockhain," 2024.

[7] N. K. Noorhizam, Z. Abdullah, S. Kasim, I. Rahmi, A. Hamid, and M. Anuar, "Verification of Ph.D. Certificate Using QR Code on Blockchain Ethereum," 2023. [Online]. Available: www.joiv.org/index.php/joiv

[8] L. Van Tan and P. M. Hung, "Driving Digital Transformation in Certificate Management: A Blockchain-Based Solution for Vinh University," *International Journal of Information and Education Technology*, vol. 14, no. 1, pp. 119–124, 2024, doi: 10.18178/ijiet.2024.14.1.2031.

[9] M. R. Hidayat, D. Gusman, and H. Adeswastoto, "Portal E-Sertifikat dengan QR Code Menggunakan PHP dan MYSQL," *Jurnal Pengabdian Masyarakat dan Riset Pendidikan*, vol. 1, no. 1, pp. 13–26, Sep. 2022, doi: 10.31004/JERKIN.V1I1.1.

[10] A. Bhise, C. Pardeshi, M. Vajale, P. Bhongale, S. Shirke, and M. Jagtap, "Blockchain Based Certificate Validation System," 2025. [Online]. Available: www.ijfmr.com

[11] R. A. Jaafar and S. N. Alsaad, "Enhancing Educational Certificate Verification With Blockchain and IPFS: A Decentralized Approach Using Hyperledger Fabric," *TEM Journal*, vol. 12, no. 4, pp. 2385–2395, Nov. 2023, doi: 10.18421/TEM124-51.

[12] S. P. Dash, A. K. Jena, and D. K. Murala, "A Hyperledger-Based Secure Framework for Academic Certificate Authentication Using Blockchain," *International Journal of Safety and Security Engineering*, vol. 15, no. 6, pp. 1185–1195, Jun. 2025, doi: 10.18280/ijsse.150610.

[13] T. Rahman, S. I. Mouno, A. M. Raatul, A. K. Al Azad, and N. Mansoor, "Verifi-Chain: A Credentials Verifier using Blockchain and IPFS," Jul. 2023, [Online]. Available: http://arxiv.org/abs/2307.05797

[14] S. Oknora Firza and F. Ilmu Komputer, "Teknologi Blockchain dalam Keamanan Sertifikat Menggunakan Smart Contracts dan Distributed Ledger pada Platfrom Edutech," 2024.

[15] B. Zhong, H. Wu, L. Ding, H. Luo, Y. Luo, and X. Pan, "Hyperledger fabric-based consortium blockchain for construction quality information management," *Frontiers of Engineering Management*, vol. 7, no. 4, pp. 512–527, Dec. 2020, doi: 10.1007/s42524-020-0128-y.

[16] A. Farabi, I. Khandaker, J. Ahsan, I. K. Shanto, N. Jahan, and M. J. Khan, "ShikkhaChain: A Blockchain-Powered Academic Credential Verification System for Bangladesh," Oct. 2025, [Online]. Available: http://arxiv.org/abs/2508.05334

[17] C. E. Pulmano, M. R. J. E. Estuar, M. M. De Leon, H. C. L. Tan, N. A. S. Co, and L. P. V. Tamayo, "Towards the development of a blockchain-based decentralized digital credential system using hyperledger fabric for participatory governance," in *Procedia Computer Science*, Elsevier B.V., 2023, pp. 99–106. doi: 10.1016/j.procs.2023.01.269.

[18] P. Dias, H. Gonçalves, F. Silva, J. Duque, J. Martins, and A. Godinho, "Blockchain Technologies: A scrutiny into Hyperledger Fabric for Higher Educational Institutions"," in *Procedia Computer Science*, Elsevier B.V., 2024, pp. 213–220. doi: 10.1016/j.procs.2024.05.098.