

A Proof of Concept for Blockchain-Based Microcredential Verification in Higher Education

Muhammad Fadlan¹, Endyk Noviyantono², Muhammad³

^{1,3}Information System Study Program, STMIK PPKIA Tarakanita Rahmawati, Indonesia

²Informatics Engineering Study Program, STMIK PPKIA Tarakanita Rahmawati, Indonesia

Article Info

Article history:

Received Jan 16, 2026

Revised Feb 23, 2026

Accepted Feb 24, 2026

Keywords:

Blockchain

Proof of concept

Data integrity

Hash-based verification

System prototype

ABSTRACT

The risk of counterfeiting and inefficient verification processes poses challenges for the validation of additional microcredential in higher education institutions, where most verification mechanisms remain manual and depend on the issuing institution. To address this issue, a blockchain-based Proof of Concept will be developed to facilitate the verification process of these microcredential. This Research uses an experimental approach by building and testing a prototype system on a limited scale. The proposed solution utilizes blockchain technology with a hash-based verification approach, where only the digital representation of the microcredential is recorded in a smart contract deployed on an Ethereum based blockchain. The testing process for the developed prototype was conducted using microcredential datasets, both original and modified microcredential, as simulations of forgery. The results indicate that the developed blockchain-based system prototype can distinguish genuine from counterfeit microcredential. These findings demonstrate that blockchain-based verification mechanisms have the potential to reduce reliance on manual verification processes. However, this Research is still at the proof of concept stage on a limited scale, and its implementation in a real world environment still requires further testing.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Muhammad Fadlan,

Information System Study Program,

STMIK PPKIA Tarakanita Rahmawati,

99 Halmahera Street, Oval Ladang IV, Tarakan, North Kalimantan, Indonesia.

Email: fadlan@ppkia.ac.id

1. INTRODUCTION

The development of digital technology has brought fundamental changes to various sectors, including higher education. Digital transformation has not only changed the way educational institutions manage data and deliver learning, but also impacted the mechanisms for issuing and verifying academic credentials. Credentials such as diplomas, transcripts, and microcredential serve as formal evidence of the learning outcomes and skills students acquire during their studies [1], [2]. In an increasingly competitive global job market, academic credentials are now a crucial instrument in the recruitment process, skills recognition, and career mobility of workers.

One form of additional credential increasingly used in higher education is the microcredential or competency certificate. This type of certificate typically indicates mastery of practical skills, such as proficiency in office applications, programming, graphic design, or other technical capabilities relevant to workforce demands [3], [4]. For example, at several Indonesian universities, students may earn microcredential, such as Microsoft Office certification, after completing a comprehensive examination. Such supplementary certificates have strategic value

because they provide concrete evidence of applied skills and complement academic degrees, thereby enhancing graduates' competitiveness in the labor market.

However, the validity and security of academic documents, including microcredential, still face serious challenges. Cases of diploma and certificate forgery continue to occur across various countries, including Indonesia, undermining public trust in individuals' academic credentials. In Indonesia, several cases of diploma forgery have drawn national attention due to the involvement of irresponsible institutions and actors [5], [6]. Moreover, academic document verification is still largely manual, with confirmation obtained directly from the issuing institutions. This process is not only time-consuming but also prone to errors and data inaccuracies, especially when institutions lack an integrated document verification system [7]. These conditions underscore the need for a more secure, efficient, and standardized mechanism for verifying academic documents.

One promising technology to address these issues is blockchain. This technology is characterized by decentralization, transparency, and resistance to manipulation, enabling permanent and immutable data recording [8], [9], [10], [11]. In the context of academic credentials, blockchain can be used to represent certificates in the form of digital hashes that are securely stored within a distributed network [11], [12], [13]. Consequently, the authenticity and integrity of the data can be ensured, while inter-institutional verification can be conducted without requiring third-party intermediaries.

Although there have been a number of studies on the application of blockchain in education, most still focus on primary academic documents such as diplomas or transcripts [7], [14], [15], [16]. Research specifically highlighting the use of blockchain for additional microcredential remains relatively limited, especially in developing countries such as Indonesia. Additional microcredential often have high relevance to the real needs of the workplace and serve as a differentiator of competency between graduates beyond formal academic achievements. This condition indicates a Research gap in the use of blockchain to support the verification of additional microcredential in higher education environments.

In addition to the limitations of the research focus, many other studies still place blockchain at a conceptual level, emphasizing system models without accompanying implementation or functional testing. While this approach provides critical theoretical contributions, it fails to fully address the technical feasibility of implementing the proposed model. Therefore, studies are needed that not only discuss the concept but also provide preliminary evidence through real-world implementations to test whether blockchain-based verification mechanisms can be implemented as intended. The objective of this research is to develop a Proof of Concept (PoC) for a blockchain-based system to verify supplementary microcredential. The system developed in this research will utilize a digital representation of the certificate in hash form, along with metadata such as the certificate holder's name, certificate number, exam date, and graduation status. Furthermore, to minimize storage burden on the blockchain test environment and maintain data privacy, this proposed approach will not store the original certificate document on the blockchain, but only its hash value representation. The system prototype was then tested using a dataset comprising original and modified certificates to simulate forgery, with the aim of evaluating its ability to distinguish valid from invalid certificates.

The novelty emphasized in this research lies in its focus on supplementary microcredentials, rather than primary academic documents such as diplomas or transcripts commonly examined in prior studies. From an academic perspective, this work extends the discussion of blockchain applications in educational credential ecosystems by addressing the practical context of non-primary certificates relevant to workforce needs. From an implementation perspective, the proposed Proof of Concept provides initial empirical evidence that a hash-based, smart contract-supported verification mechanism can be functionally realized within a limited experimental scope.

Unlike established blockchain-based credential platforms or standardized verifiable credential frameworks, this study does not aim to propose a new credential standard or threat model. Instead, it focuses on a lightweight Proof of Concept designed to demonstrate the functional implementation of an off-chain, hash-based verification workflow for supplementary

microcredentials commonly issued in higher education institutions. The novelty of this work lies in providing empirical evidence through a working prototype, addressing the gap between conceptual proposals and practical implementation for microcredential verification.

2. RELATED WORKS

Blockchain technology was first introduced through the Bitcoin cryptocurrency system, but it has since evolved into a digital infrastructure used across various domains, including education. Its core characteristics, decentralization, transparency, and data immutability, make blockchain a potential solution for ensuring the integrity and authenticity of information in digital environments [17], [18], [19], [20]. In the field of education, blockchain has been widely explored to support the storage, distribution, and verification of academic credentials, as every transaction or piece of data recorded on the network is permanent and cannot be modified [1], [14], [21], [22].

Several previous studies have demonstrated that blockchain can accelerate the validation of academic documents and reduce the risk of forgery, for example, by developing blockchain-based diploma verification models that speed up document validation [23], [24], [25]. Other studies emphasize that blockchain enables the creation of a more open digital credential ecosystem, where educational institutions, industries, and certification bodies can interact securely without relying on third-party intermediaries [11], [26], [27], [28]. Beyond diplomas and transcripts, several studies have begun applying blockchain to support microcredentials or competency certificates. Blockchain-based microcredentials can strengthen the concept of lifelong learning by allowing individuals to collect digital evidence of specific skills they have acquired [29], [30]. Collectively, these studies reinforce the understanding that blockchain is not merely a data storage tool but also a trust mechanism that can enhance the efficiency and security of academic administrative processes. However, most of these studies still focus on global-scale systems or general online platforms, with limited examination of their application in the context of higher education in developing countries such as Indonesia.

Other studies on the application of blockchain in education indicate increasing interest in the topic. However, most remain in the early stages of conceptual development. Most of these studies focus solely on system architecture design or theoretical models without presenting real-world implementation results or proving feasibility through proof of concept (PoC) [1], [2], [14], [16], [21]. This condition indicates that the implementation aspects of blockchain technology in the higher education ecosystem remain underexplored. However, implementation evidence is needed to assess the extent to which the proposed model can function effectively in real situations, including in the context of additional competency certificate verification that requires direct validation of data authenticity and integrity. This gap then serves as the basis for this study, which presents a PoC based approach as empirical evidence of blockchain application in the higher education sector.

The results of the review of previous studies indicate that the adoption of blockchain technology in higher education environments remains primarily focused on Research on conceptual frameworks, architectural designs, and theoretical discussions. This review also shows that empirical studies on how proposed blockchain-based models operate through live implementation and functional testing in blockchain environments remain limited, especially in higher education. This gap indicates that the feasibility of blockchain-based verification mechanisms in higher education has not been sufficiently investigated through an experimental approach. Furthermore, existing implementation-oriented studies primarily focus on primary academic documents, such as diplomas and transcripts. At the same time, empirical Research on additional microcredential remains rare. This highlights the need for research that combines an experimental perspective with the context of blockchain-based applications for microcredential that represent practical skills and employability.

3. RESEARCH METHOD

3.1. Research Stages

This study employs an experimental Research approach using a Proof of Concept (PoC) model to design, implement, and evaluate a prototype of a blockchain-based competency certificate verification system within a limited scope. The PoC approach is adopted to demonstrate the

feasibility of the proposed concept through direct implementation rather than solely conceptual modeling. The overall Research process consists of several interrelated stages, as illustrated in Figure 1.

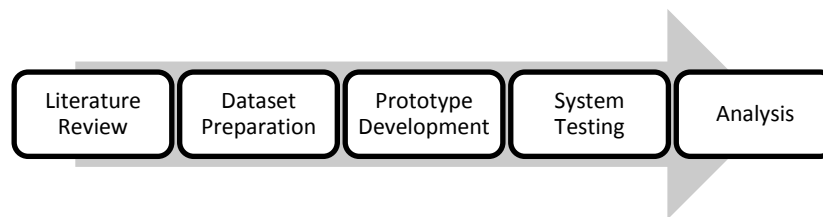


Figure 1. Research stages

As shown in Figure 1, the first stage of this research is a literature review of prior work, particularly on blockchain technology for academic document verification and credential management. This stage is crucial for identifying blockchain technology implementations and identifying the limitations of existing approaches. The second stage is the preparation of a competency certificate test dataset. In this study, the dataset includes valid certificates and modified certificates designed to simulate a certificate forgery scenario. In this study, only essential information is recorded, including certificate hashes and metadata such as the certificate holder's name, certificate number, exam date, and graduation status. This dataset serves as the basis for evaluating the system's ability to distinguish between genuine and fraudulent certificates. The SHA-256 algorithm will be used to hash each certificate before it is stored and verified on the blockchain network.

The next stage is prototype development. A simple smart contract in Solidity is implemented to record and verify certificate hashes on the blockchain. The prototype is implemented in an Ethereum test environment, with Remix IDE used for smart contract development and testing. This setup allows for controlled experimentation. Following prototype development, system testing is conducted to evaluate the functional correctness of the proposed verification mechanism. Testing focused on the system's ability to correctly distinguish between valid and modified certificates. Verification results were determined from the Boolean output, a true or false value, returned by the smart contract during the certificate verification process.

Next, the analysis of the results was the final stage of this research. This stage will interpret and review the functional test results based on the scenarios used. This analysis focused not only on assessing whether the developed proof-of-concept prototype could effectively support certificate verification through hash-value comparison, but also on identifying limitations and potential future development directions for the use of blockchain technology for verification in higher education institutions.

3.2. Experimental Scope

This Research was conducted within a limited experimental scope, focusing on functional validation rather than performance benchmarking or large-scale system evaluation. The primary objective of the experiment was to demonstrate the feasibility of a blockchain-based verification mechanism for supplementary microcredential through a Proof of Concept (PoC). Accordingly, the implementation was intentionally constrained to a small dataset and a controlled testing environment.

The evaluation of the proposed system focused on functional correctness, assessed by examining its ability to distinguish between valid certificates and those that had been modified. Verification outcomes were determined by the Boolean results, true or false returned by the smart contract during the verification process. The evaluation results were analyzed descriptively to determine whether the developed PoC performed certificate verification as intended and met the defined Research objectives within its limited scope. This experimental scope does not include adversarial attack simulation, replay attack analysis, or cryptographic threat modeling. The

objective of this study is limited to demonstrating functional tamper evident verification under a controlled environment.

4. RESULTS AND DISCUSSION

4.1. Prototype System Implementation

In this study, a smart contract in the Ethereum environment, implemented in the Remix IDE, was used to develop a Proof of Concept prototype for a competency certificate verification system. This implementation, using a smart contract on Ethereum, aims to demonstrate that the blockchain verification concept can be functionally implemented through a hash-based certificate recording mechanism without the need to store the certificate documents directly. A general outline of the proposed system workflow implemented in this study can be seen in Figure 2.



Figure 2. Architecture of the proposed blockchain-based competency certificate verification system

Figure 2 shows the prototype architecture of the blockchain-based verification system proposed in this research. The process begins with the issuer, the university or institution, issuing the microcredential or certificate in the form of a digital document. The microcredential is then stored and processed off-chain, and then converted into a digital representation in the form of a hash value using the SHA-256 algorithm. At this point, the certificate has been converted into a hash value. The hash value representing the certificate is then recorded in the blockchain via a smart contract. This process demonstrates that the blockchain actually stores the hash of the microcredential, not the microcredential or certificate file itself. Next step, the verification phase begins, in which the verifier authenticates the microcredential using a PoC prototype by comparing the tested certificate's hash with the previously stored hash in the blockchain, without directly accessing the original certificate document. This architectural workflow is implemented as a Proof of Concept and is intended to demonstrate functional feasibility rather than a production-ready verification infrastructure.

The proof-of-concept prototype was implemented by building and deploying an Ethereum-based smart contract to a test blockchain environment after the system architecture design was completed. From a functional perspective, the Ethereum-based smart contract developed in this research consists of two main functions: *registerCertificate* and *verifyCertificate*, as shown in Figure 3.

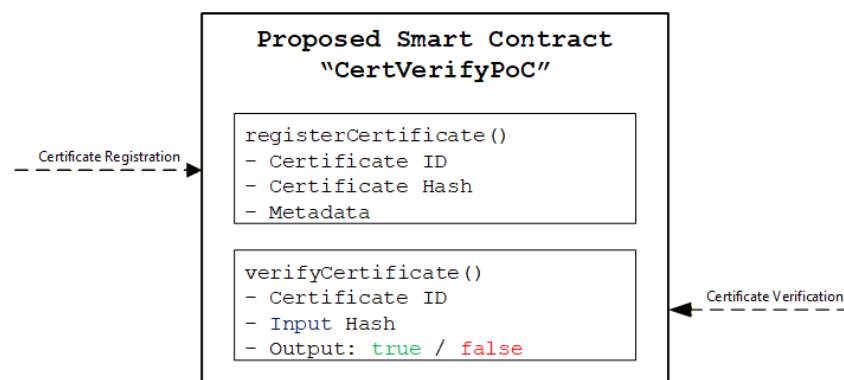


Figure 3. Overview of smart contract functions used in the proposed system

Figure 3 presents an overview of the logical structure of the Ethereum blockchain-based smart contract developed in this study, along with its two main functions. The first function is

registerCertificate, which is used by universities or issuers to record hashes and key metadata related to certificates into the Ethereum blockchain network. In this Proof of Concept, issuer authentication is assumed at the system level rather than explicitly enforced on-chain. The smart contract is deployed and interacted with by a predefined issuer address controlled by the issuing institution. Consequently, only this authorized address is permitted to register microcredential hashes during the experimental phase.

In this Proof of Concept, access control is enforced directly at the smart contract level using an ownership-based restriction mechanism. The registerCertificate function is protected by an *onlyOwner* modifier, which restricts certificate registration exclusively to the deploying address representing the issuing institution. Any attempt by non-owner addresses to invoke the registration function will be rejected through a require (*msg.sender == owner*) validation. While more advanced identity management or role-based access control models are not implemented in this prototype, the ownership-based restriction ensures that unauthorized parties cannot register fraudulent certificate hashes during the experimental phase.

The second function is verifyCertificate, which is used to verify the authenticity of microcredential by comparing the hash of the certificate being tested with the hash value data previously stored in the blockchain via the registerCertificate function. Figures 2 and 3 demonstrate that in this study, the certificate verification process is carried out entirely through a hash-based verification mechanism without storing the original certificate document within the blockchain network. The deployment results of the PoC prototype in this study indicate that the developed smart contract can be run properly and is ready to accept transactions for the competency certificate registration and verification process through the certificate hash value representation. This implementation also confirms that the system prototype has functioned according to the initial design objectives and is ready for use in the competency certificate verification testing phase.

4.2. Verification Result

Testing of the verification mechanism to evaluate the functional correctness of the prototype system developed in this research was conducted after the successful registration of the microcredential. In this research, verification testing was conducted by comparing the microcredential hash value generated from the test document with the previously stored hash value in the blockchain network via a smart contract.

The testing process was conducted through two main scenarios. In the first scenario, testing was conducted using the original, unaltered, supplementary microcredential data. Next, the microcredential data was converted to a hash using the SHA-256 algorithm, and the resulting hash was verified in a specially developed smart contract using the verifyCertificate function. The overall results of the verification execution for the first scenario are shown in Figure 4.



Figure 4. Blockchain-based verification result of a valid competency certificate

Figure 4 shows the success of the verification process through the developed smart contract, indicated by the Boolean value "true" in the decoded output, which is one of the execution results of the verifyCertificate function within the smart contract. Further evidence can be seen in

the CertificateVerified event recorded in the logs, indicating that the verification process was executed and recorded by the blockchain system correctly without any errors.

Next, a second scenario was conducted, simulating microcredential forgery. This was done to test the system prototype's resilience to data changes made to the microcredential. The second scenario involved modifying part of the certificate's content, such as the issuance date or the certificate holder's name. In a hash-based approach, even the slightest change can significantly alter the hash value. The modified certificate was then re-hashed and verified using the exact mechanism as in scenario 1. An example of the verification results for a modified certificate is shown in Figure 5. Figure 5 shows the verification/testing results for the second scenario. The results indicate that the developed blockchain-based system prototype can return a false value in the decode output. This means the certificate is declared fake due to a discrepancy between the hash value of the altered certificate and the hash value of the original certificate stored in the blockchain network. A summary of the microcredential verification test results can be seen in Table 1.



Figure 5. Blockchain-based verification result of a modified competency certificate

Table 1 shows that the system prototype can distinguish between original and modified certificates, although testing in this study was limited. The change scenarios included changes to the date, the owner's name, the certificate number, and even graduation status. Based on these test results, the blockchain-based verification mechanism using the verifyCertificate function implemented in this study was proven to consistently perform its primary function: verifying the authenticity of microcredential by comparing the hash value previously stored in the blockchain network with the new hash of the certificate that has undergone data changes, thus changing the overall hash value. All test scenarios demonstrated agreement between the expected results and the system output, both for original certificates and certificates with various modifications.

Table 1. Summary of verification test results

No	Certificate ID	Test Scenario	Expected Result	System Result
1	31/E/03xxx062	Original microcredential	True	True
2	31/E/03xxx062	Date modification	False	False
3	31/E/03xxx062	Owner name modification	False	False
4	31/E/03xxx062	Certificate number modification	False	False
5	31/E/03xxx062	Passing status modification	False	False

The Certificate ID presented in Table 1 is partially masked to preserve data privacy. Nevertheless, all verification experiments were conducted using complete and consistent Certificate ID values in the internal test logs to ensure experimental replicability. This masking does not affect the validity of the experimental results, as the verification process relies solely on hash consistency rather than the visual representation of the identifier.

Based on the results of the two scenarios, this study indicates that this proof-of-concept approach for hash-based certificate verification on the Ethereum blockchain network is highly sensitive to data changes. Any modification, even the slightest modification to key microcredential attributes such as the owner's name, exam date, graduation status, or microcredential number, results in significantly different hash values that can be detected by the blockchain-based system prototype developed in this study. This certainly confirms that the implemented mechanism is capable of maintaining data integrity and supporting authenticity verification under institutional

trust assumptions without requiring the original documents to be stored on the blockchain. This research also demonstrates that the developed Proof of Concept prototype demonstrates technical feasibility as a mechanism for additional competency microcredential verification within a limited scope. Although the testing in this study was simple, it was controlled, providing initial evidence that the blockchain-based microcredential verification concept can be implemented functionally and has the potential for further development in higher education settings.

4.3. Role of the Proof of Concept and Its Implications

It is important to clarify that the objective of this Proof of Concept is not to introduce a novel cryptographic mechanism, but to demonstrate the technical feasibility of applying an established hash-based integrity approach within a blockchain-based microcredential verification workflow. While the smart contract enforces ownership-based access control for certificate registration, the legitimacy of the issuer remains an institutional governance assumption. The blockchain functions as an integrity anchor that ensures immutability of registered hashes, but it does not autonomously validate the real-world authority of the issuing institution.

To complement studies of blockchain implementation in higher education, which have focused primarily on the conceptual aspects of blockchain technology, this study proposes a Proof of Concept (PoC) approach to demonstrate how blockchain-based competency microcredential verification can be implemented functionally within a limited scope. The results of this study indicate that the hash-based microcredential verification mechanism is fully operational using a simple Ethereum-based smart contract and can distinguish between original, unaltered microcredentials and modified microcredentials. These findings demonstrate that the hash-based verification approach is highly sensitive to changes in microcredential data and can maintain information integrity without storing the original documents on the blockchain. The findings of this study also provide initial evidence that the approach discussed in previous research is technically feasible when implemented in practice. However, this study does not necessarily aim to generalize the performance of the developed system prototype on a broader scale.

This study does not assess transaction costs or scalability, as the implementation was conducted within a controlled test environment. In real-world deployments, particularly on public Ethereum mainnet, transaction costs may pose a constraint for large scale or frequent microcredential verification. Accordingly, future research may investigate cost analysis, scalability performance, and alternative deployment options, such as permissioned blockchains or Layer-2 solutions. For real-world adoption, the proposed verification mechanism illustrated in Figure 2 may be integrated with existing student information systems, where microcredential issuance forms part of institutional academic records. In such a scenario, students act as credential holders, while employers or third-party platforms function as verifiers. Although user experience design and identity binding mechanisms are not represented in the current prototype architecture, these aspects were not implemented in this Proof of Concept and represent important considerations for future system development and large-scale deployment. From an information systems perspective, the architecture shown in Figure 2 positions blockchain as a supporting infrastructure for trust and verification rather than a replacement for existing academic information systems.

This research has implications for the academic domain by providing an implementation illustration of blockchain implementation for additional competency microcredential verification through an Ethereum blockchain-based smart contract. This research's contribution is to complement the existing literature with an initial implementation example that can serve as a reference for further research, particularly in evaluating technical aspects before developing a more complex system integrated with higher education systems. Another practical implication of this research is that the microcredential verification process can be conducted without storing the original documents on the blockchain. This ensures data integrity is maintained without compromising the privacy of the microcredential data. Furthermore, although the prototype developed is still limited, this approach is expected to provide an initial insight into the potential use of blockchain technology as a supporting mechanism for additional competency microcredential verification in higher education settings. This should also be understood as an

initial step that requires further testing and adjustments before being implemented in broader operations.

5. CONCLUSION

Based on research conducted through the implementation of smart contracts in an Ethereum-based blockchain environment and functional testing on a blockchain-based test network, this study demonstrates that a hash-based microcredential verification mechanism can be implemented in practice. The results indicate that the developed prototype system is capable of distinguishing genuine microcredentials from fake ones, as they have been modified through true and false verification outputs. The proof-of-concept approach used in this study provides initial evidence of the technical feasibility of implementing blockchain for additional competency microcredential verification. Furthermore, although the implementation was carried out on a limited scale, the results of this study complement existing conceptual studies by illustrating a real-world implementation, which can serve as a baseline for future research and development of blockchain-based competency microcredential verification systems, particularly for higher education institutions.

Future research is recommended to explore the evaluation of system performance and scalability on a larger number of certificates, as well as review usability aspects from a user perspective. Furthermore, testing on a public blockchain network, analysis of transaction costs, and integration with existing higher education information systems can also be conducted to assess the system's readiness for more complex operational environments.

ACKNOWLEDGEMENTS

The author would like to express sincere gratitude to STMIK PPKIA Tarakanita Rahmawati for the support and funding provided for the implementation of this Research.

REFERENCES

- [1] W. Suktam, S. Lapchit, J. Supsin, S. Sonwa, and C. Suthamdee, "Blockchain in Education: Transforming Learning, Credentialing, and Academic Data Management," *Journal of Education and Learning Reviews*, vol. 1, no. 6, pp. 37–46, Oct. 2024, doi: 10.60027/jelr.2024.739.
- [2] R. Arenas and P. Fernandez, "CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials," in *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, Stuttgart: IEEE, 2018. doi: 10.1109/ICE.2018.8436324.
- [3] J. Kaneriya and H. Patel, "A Secure and Privacy-Preserving Student Credential Verification System Using Blockchain Technology," *International Journal of Information and Education Technology*, vol. 13, no. 8, pp. 1251–1260, Aug. 2023, doi: 10.18178/ijiet.2023.13.8.1927.
- [4] D. Liu, H. Wu, C. Huang, J. Ni, and X. Shen, "Blockchain-Based Credential Management for Anonymous Authentication in SAGVN," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 10, pp. 3104–3116, Oct. 2022, doi: 10.1109/JSAC.2022.3196091.
- [5] D. Julisa Sistyawan, R. Vallentino Neonbeni, M. Rizal, and A. Cesar Divian Candra Kusuma, "Fake Diplomas, Real Consequences: Legal and Ethical Challenges in the Legal Profession," *CONSTITUTIONALE*, vol. 5, no. 2, pp. 137–156, 2024, doi: 10.25041/constitu.
- [6] I. K. Kamaluddin, P. Masyitoh, and A. D. Santoso, "Criminal Counterfeiting Deed Authentic Shaped Diplomas By A Notary; Fiqh Legal Perspective Jinaya, Indonesia," *Jurnal Indonesia Sosial Teknologi*, vol. 4, no. 11, pp. 2056–2067, Nov. 2023, doi: 10.59141/jist.v4i11.788.
- [7] M. Kamil, P. A. Sunarya, Y. Muhtadi, I. R. Adianita, and M. Anggraeni, "BlockCert Higher Education with Public Key Infrastructure in Indonesia," in *2021 9th International Conference on Cyber and IT Service Management, CITSM 2021*, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/CITSM52892.2021.9589018.
- [8] R. Widayanti, Q. Aini, H. Haryani, N. Lutfiani, and D. Apriliasari, "Decentralized Electronic Vote Based on Blockchain P2P," in *2021 9th International Conference on Cyber and IT*

- Service Management, CITSM 2021*, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/CITSM52892.2021.9588851.
- [9] Q. Aini, D. Manongga, U. Rahardja, I. Sembiring, and R. Efendy, "Innovation and Key Benefits of Business Models in Blockchain Companies," *Blockchain Frontier Technology*, vol. 2, no. 2, pp. 24–35, Oct. 2022, doi: 10.34306/bfront.v2i2.161.
 - [10] L. K. Oh, "A Comprehensive Study on Public and Private Blockchain Performance," *Journal of Current Research in Blockchain*, vol. 2, no. 1, pp. 13–27, Mar. 2025, doi: 10.47738/jcrb.v2i1.25.
 - [11] I. T. Imam, Y. Arafat, K. S. Alam, and S. Aki, "DOC-BLOCK: A blockchain based authentication system for digital documents," in *Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021*, Institute of Electrical and Electronics Engineers Inc., Feb. 2021, pp. 1262–1267. doi: 10.1109/ICICV50876.2021.9388428.
 - [12] O. Salau and S. A. Adeshina, "Secure Document Verification System Using Blockchain," in *2021 1st International Conference on Multidisciplinary Engineering and Applied Science, ICMEAS 2021*, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/ICMEAS52683.2021.9739812.
 - [13] Q. . Aini *et al.*, "Security Level Significance in DApps Blockchain-Based Document Authentication," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 2, no. 3, pp. 292–305, 2022.
 - [14] S. R. Azahra, "Exploration of The Potential of Blockchain Technology in Securing Data and Educational Credentials," *Educational Technology Journal* |, vol. 4, no. 1, pp. 28–34, 2024, [Online]. Available: <https://journal.unesa.ac.id/index.php/etj>
 - [15] U. Chotijah, I. Teguh Prayudha, and A. Rifki, "Blockchain-Based E-Certificate System: Secure and Transparent Credential Management," *JUSIFO (Jurnal Sistem Informasi)*, vol. 10, no. 2, pp. 49–58, Dec. 2024, doi: 10.19109/jusifo.v10i2.24421.
 - [16] U. Rahardja, A. N. Hidayanto, T. Hariguna, and Q. Aini, "Design Framework on Tertiary Education System in Indonesia Using Blockchain Technology," in *2019 7th International Conference on Cyber and IT Service Management (CITSM)*, Jakarta: IEEE, 2019, p. 1. doi: 10.1109/CITSM47753.2019.8965380.
 - [17] K. K. Vaigandla, M. Siluveru, M. Kesoju, and R. Karne, "Review on Blockchain Technology: Architecture, Characteristics, Benefits, Algorithms, Challenges and Applications," Dec. 10, 2023, *Mesopotamian Academic Press*. doi: 10.58496/MJCS/2023/012.
 - [18] W. Viriyasitavat and D. Hoonsopon, "Blockchain characteristics and consensus in modern business processes," *J Ind Inf Integr*, vol. 13, pp. 32–39, Mar. 2019, doi: 10.1016/j.jii.2018.07.004.
 - [19] A. de Alwis, A. Shrestha, and T. Sarker, "Exploring Governance for accreditation in the education sector using blockchain technology: a systematic literature review," *Discover Education*, vol. 4, no. 1, Dec. 2025, doi: 10.1007/s44217-025-00449-y.
 - [20] E. Bandara *et al.*, "Casper: a blockchain-based system for efficient and secure customer credential verification," *Journal of Banking and Financial Technology*, vol. 6, no. 1, pp. 43–62, Jun. 2022, doi: 10.1007/s42786-021-00036-3.
 - [21] S. H. Said, M. A. Dida, E. M. Kosia, and R. S. Sinde, "A Blockchain-based Conceptual Model to Address Educational Certificate Verification Challenges in Tanzania," *Engineering, Technology and Applied Science Research*, vol. 13, no. 5, pp. 11691–11704, Oct. 2023, doi: 10.48084/etasr.6170.
 - [22] B. Awaji and E. Solaiman, "Design, Implementation, and Evaluation of Blockchain-Based Trusted Achievement Record System for Students in Higher Education," in *14th International Conference on Computer Supported Education (CSEDU 2022)*, SCITEPRESS – Science and Technology Publications, Apr. 2022, pp. 225–237. doi: 10.5220/0011044200003182.

- [23] B. Mardisentosa, U. Rahardja, K. Zelina, F. P. Oganda, and M. Hardini, "Sustainable Learning Micro-Credential using Blockchain for Student Achievement Records," in *2021 6th International Conference on Informatics and Computing, ICIC 2021*, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/ICIC54025.2021.9632913.
- [24] G. Capece, N. L. Ghiron, and F. Pasquale, "Blockchain technology: Redefining trust for digital certificates," *Sustainability (Switzerland)*, vol. 12, no. 21, pp. 1–12, Nov. 2020, doi: 10.3390/su12218952.
- [25] H. A. Alsobhi, R. A. Alakhtar, A. Ubaid, O. K. Hussain, and F. K. Hussain, "Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review," *Knowl Based Syst*, vol. 265, p. 110238, 2023, doi: <https://doi.org/10.1016/j.knosys.2022.110238>.
- [26] K. Singh, O. Dib, C. Huyart, and K. Toumi, "A novel credential protocol for protecting personal attributes in blockchain," *Computers and Electrical Engineering*, vol. 83, May 2020, doi: 10.1016/j.compeleceng.2020.106586.
- [27] D. Serranito, A. Vasconcelos, S. Guerreiro, and M. Correia, "Blockchain Ecosystem for Verifiable Qualifications," in *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, Paris: IEEE, Sep. 2020, pp. 192–199. doi: 10.1109/BRAINS49436.2020.9223305.
- [28] O. S. Oluwaseyi and R. O. Akinyede, "Utilizing Blockchain Technology for University Certificate Verification System," *International Journal of Applied Information Systems (IJ AIS)*, vol. 12, no. 45, pp. 23–40, 2024, [Online]. Available: www.ijais.org
- [29] H. A. Alsobhi, R. A. Alakhtar, A. Ubaid, O. K. Hussain, and F. K. Hussain, "Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review," *Knowl Based Syst*, vol. 265, p. 110238, 2023, doi: <https://doi.org/10.1016/j.knosys.2022.110238>.
- [30] A. Bigiotti, M. P. F. Bottoni, and G. Nalli, "Blockchain in E-Learning Platform to Enhance Trustworthy and Sharing of Micro-credentials," in *Advanced Information Systems Engineering Workshops*, J. P. A. Almeida, C. Di Ciccio, and C. Kalloniatis, Eds., Cham: Springer Nature Switzerland, 2024, pp. 5–17.