Volume 11 Issue 1 Year 2026 | Page 24-33 ISSN: 2527-9866
Received: ***04-12-2025*** | *Revised:* ***15-12-2025*** | *Accepted:* ***26-12-2025***

Application of Non-Fungible Tokens and ERC-1155 Algorithm in Digital Certificate Verification Process

Azkaarahiilahardi[1], Safitri Jaya[2]
[1,2] Pembangunan Jaya University, Tangerang Selatan, Indonesia
e-mail: Azkaarahiilahardi.2022@student.upj.ac.id[1], safitri.jaya@upj.ac.id[2]
*Correspondence: Azkaarahiilahardi.2022@student.upj.ac.id

Abstract: *Digital certificate forgery remains a real problem in education and employment because traditional verification processes rely on centralized databases, are vulnerable to manipulation, and often take a long time. This study designs and implements a blockchain-based digital certificate verification system that models certificates as Non-Fungible Tokens (NFTs) using the ERC-1155 standard on the Manta Pacific Layer 2 network, and incorporates a Soulbound Token (SBT) mechanism to ensure that certificates cannot be transferred. The research adopts a prototyping method through eight stages, starting from architecture design and prototype development to the integration of ERC-1155 smart contracts with IPFS and wallets, as well as testing of minting functions, QR code-based verification, and rejection of asset transfers. The results demonstrate successful on-chain certificate issuance with significantly reduced transaction costs compared to ERC-72 based certificates on Layer 1 networks reported in previous studies, while maintaining a decentralized audit trail. The SBT implementation successfully rejects every attempt to transfer certificates to other wallets, thereby preventing the sale or illicit transfer of credential ownership. These findings indicate that the combination of ERC-1155, SBT, and IPFS on a Layer 2 network has strong potential as an efficient, secure, and practically adoptable digital certificate verification model for educational institutions.*

Keywords: *Blockchain, NFT, ERC-1155, Digital Certificate, Soulbound Token.*

1. Introduction

The global education and employment ecosystem currently faces significant risks related to the falsification and manipulation of digital certificates, which can undermine public trust in academic credentials [1]. Conventional verification practices that rely on centralized databases and manual checks have proven to be prone to human error and time-consuming to validate the authenticity of documents [2]. Weaknesses in the existing system demand the presence of a new validation mechanism that is transparent, immutable, and easily auditable by various parties without intermediaries [3]. Therefore, the application of blockchain technology is a crucial solution to create a trust infrastructure that guarantees the integrity of certificate data in the digital age [4].

Based on a review of the latest literature, blockchain-based certificate verification designs have been proven to increase resistance to counterfeiting through the use of on-chain identities and cryptography [5]. Previous studies show that modeling credentials as Non-Fungible Tokens (NFTs) can strengthen the non-repudiation aspect while automating the verification process through smart contracts [6]. However, the majority of previous studies still adopt the ERC-721 standard, which has limitations in terms of scalability and high gas costs when applied to mass certificate issuance [7]. In addition, the literature also highlights that audit trails are often broken because certificate metadata is not strongly bound on-chain to distributed storage, thereby reducing the value of long-term proof [8].

This research topic is very important to publish because it offers concrete solutions to the efficiency and cost barriers that have hitherto hampered the widespread adoption of blockchain in educational institutions [9]. This publication fills a knowledge gap regarding the application of the ERC-1155 standard, which enables multi-token management in a single contract to significantly reduce operational costs compared to traditional approaches [10]. Furthermore, the urgency of discussing this topic lies in the development of an architecture that integrates IPFS decentralized storage with Layer 2 networks, which guarantees data availability and transaction speed without compromising security (Ramli, 2023). The dissemination of these research results is expected to serve as a technical reference for the development of an interoperable and cost-effective national verification system [11], [12].

This study aims to design and implement a digital certificate system that models certificates as NFTs with the ERC-1155 standard to improve the efficiency, scalability, and security of the verification process. The first specific objective is to analyze and model the application of blockchain technology for verifying the authenticity of digital certificates, including issuance mechanisms, decentralized metadata storage, and transparent and publicly auditable on-chain validation. The second specific objective is to design, develop, and evaluate the implementation of NFT technology based on the efficient ERC-1155 algorithm to support the verification process of digital certificate authenticity with more optimal multi-token asset management capabilities. Based on these objectives, this study was formulated to answer two main research questions: (1) How to design an ERC-1155 NFT-based digital certificate verification system architecture integrated with IPFS and Layer 2 networks to ensure the integrity, traceability, and non-repudiation of certificates? (2) To what extent can the application of the ERC-1155 standard on Layer 2 networks reduce transaction costs and improve the efficiency of the verification process compared to the ERC-721-based approach commonly used in previous studies?

The contribution of this research to society is significant, especially in providing a digital trust infrastructure that can protect intellectual property rights and qualifications from misuse. For the general public and industry, this system provides practical benefits in the form of quick and accurate verification of job applicants' credentials without the need for complicated bureaucratic procedures [13]. Educational institutions also benefit from the efficient management of secure and permanent digital archives, thereby reducing the long-term administrative burden [14]. Ultimately, this research contributes to creating a more integrity-driven education ecosystem where every academic achievement is valued and protected transparently.

2. Literature Review

This research makes a significant contribution by developing a digital certificate authenticity verification mechanism that is not only resistant to manipulation, but also offers high efficiency in managing large-scale academic data. In terms of its novelty, this research lies in the design of a system architecture that intelligently combines the security of blockchain technology with the flexibility of the ERC-1155 algorithm standard. This method enriches digital asset governance by integrating batch minting capabilities for mass certificate issuance in a single transaction, then systematically binding the certificate metadata to a decentralized storage system to ensure long-term data availability. This approach results in a verification model that is far more responsive and cost-effective, providing a strong alternative to older standards such as ERC-721, which tend to burden the network and are less efficient for institutional needs [15]. The practical and operational implications of this research are highly relevant, as by adopting the system logic applied to EduVerse, this model can be said to be effective as a transparent self-validation tool, helping universities and industries to instantly verify job applicants' credentials without complicated manual procedures. This has great potential to cut administrative bureaucracy, close loopholes for document falsification, and ultimately create a more trustworthy and modern education ecosystem.

Previous research has consistently highlighted the potential of blockchain technology to revolutionize the security of academic document verification systems, with many studies agreeing that the immutable nature of distributed ledgers is the key solution to overcoming the prevalence of fake diplomas. Several previous studies have made significant contributions by proving that decentralized architecture can eliminate dependence on manual verification, which is prone to errors and time-consuming. However, these studies still leave room for improvement, particularly regarding scalability issues and high transaction costs (gas fees) when applied to institutions with large volumes of graduates. [1], [2]. Several other studies have successfully demonstrated the use of NFTs to create transparent traceability for physical and digital assets, but their implementations tend to still use single token standards that trigger high computational overhead on the network [16]. Meanwhile, other studies have attempted to design a secure web-based certificate issuance system, but this model is still limited to managing one type of asset per transaction, making it less effective for complex and mass certificate management needs [17]. On the other hand, challenges regarding cross-platform data interoperability and portability are also emphasized in the literature, which asserts that modern verification systems must allow certificate data to be easily accessed by third parties without compromising the integrity of on-chain metadata [18]. Technical inspiration also comes from approaches that propose IPFS storage integration to reduce blockchain storage load, although they have not fully explored its combination with multi-token standards for cost efficiency [19].

A key limitation identified in previous studies is the dominant use of the ERC-721 standard, which is inherently not designed for large-scale operational efficiency. To provide a clearer understanding of the technical justification for the choice of token standard in this study, Table 1 presents a comprehensive comparison between ERC-721 and ERC-1155.

Table 1. Comparison of ERC-721 and ERC-1155

Aspect	ERC-721 (Single Token)	ERC-1155 (Multi-Token)
Basic Concept	Each token is unique with a global ID; one contract manages only one type of asset	A single smart contract can manage various types of tokens (fungible and non-fungible) at once.
Contract Structure	Requires separate contract deployment for each certificate category, increasing management complexity	All certificate categories are managed in a single contract with internal token IDs as differentiators.
Issuance Mechanism	Minting is done one by one; each certificate requires an independent transaction	Supports batch minting, which allows the issuance of hundreds of certificates in a single transaction.
Gas Cost Efficiency	High for mass operations because each transaction incurs a separate gas fee	Significantly low; batch operations reduce the total gas required for mass issuance scenarios
Scalability	Limited; not optimal for institutions with thousands of graduates per year	High; designed for managing large volumes and diverse types of digital assets
Transfer Flexibility	Transfers can only be made one token per transaction.	Supports batch transfers of various types and quantities of tokens in a single transaction
Ideal Use Cases	Single and unique digital assets such as NFT artworks or exclusive virtual properties	Systems that require efficient management of diverse asset categories such as academic certificates, tickets, or vouchers

Based on Table 1, it can be seen that the ERC-1155 standard directly addresses the scalability and cost efficiency weaknesses that were major obstacles in previous studies [20]. The batch minting

capability and multi-token management in a single contract make ERC-1155 a far superior architectural choice for implementing certificate verification systems in educational institutions with high issuance volumes [21]. In addition, integration with IPFS decentralized storage can be strengthened with this multi-token standard to create a system that is not only secure, but also cost-effective and scalable [21]. Based on the results of the literature review, there are still a number of important gaps that have not been optimally filled, especially in the development of a framework that combines the efficiency of the ERC-1155 algorithm with the security of decentralized metadata for cost-effective and scalable certificate verification. This research is specifically aimed at filling these gaps by designing a system architecture that integrates the ERC-1155 standard, the Manta Pacific Layer 2 network, and IPFS storage into a single cohesive framework.

3. Methods

This research adopts the Prototyping methodology as the main approach in developing a blockchain-based digital certificate verification system. This methodology was chosen because it allows for iterative system development with stakeholder needs validation at each stage, resulting in solutions that meet the real needs of educational institutions and end users. Prototyping enables rapid iteration, continuous feedback, and design adjustments based on user input prior to final implementation, thereby significantly minimizing the risk of implementation failure. This methodology is particularly suitable for the development of blockchain and NFT systems that involve complex technologies and require validation of ease of use from a non-technical user perspective.

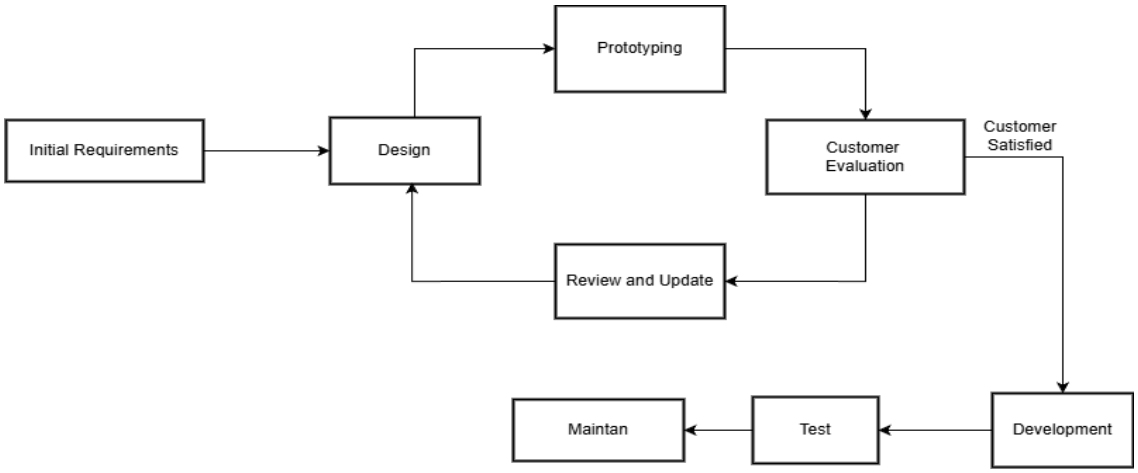

Figure 1. Research Method

Figure 1 visualizes the Prototyping methodology flow applied in this study. The system development process was carried out through eight systematically integrated stages, starting with Initial Requirements Gathering, which included literature studies and determining technology specifications such as ERC-1155 Smart Contract, IPFS, and MetaMask digital wallet integration, followed by System Design to develop the architecture and user interface, then Initial Prototyping to build an initial version of the system with basic functionality. The next stages include Customer Evaluation to gather feedback from students, lecturers, or industry partners, Review & Update to optimize UX and gas fee efficiency, and Full System Development, which includes deploying smart contracts to the Manta Pacific network and integration with Thirdweb SDK and Goldsky Indexer. The Testing phase is carried out through unit testing of smart contract functions, blockchain-IPFS data synchronization integration testing, and security audits, while the Maintenance phase includes routine monitoring of system performance using block explorers and analytical tools. These eight stages ensure that the system is developed comprehensively from conceptualization to implementation and long-term maintenance.

The selection of the prototyping methodology is based on a strategic approach to ensure the validity and reliability of the developed system. The validity of findings is ensured through Iterative Validation and User Engagement mechanisms, where continuous stakeholder involvement enables direct verification of the system's functional suitability to real user needs, thereby minimizing the risk of design mismatch. Reliability is strengthened through Early Problem Detection and Risk Mitigation, which enable the identification of technical obstacles and bug fixes from an early stage, ensuring that the system operates consistently and stably before entering the production phase. The flexibility of this method also accommodates the rapidly changing dynamics of blockchain technology, ensuring that the resulting digital certificate verification application is not only technically tested but also has a high level of accuracy and reliability for implementation in the education and industrial sectors.

4. Results and Discussion

A. Results of the Implementation of the Certificate Issuance Process

This section describes the technical implementation of an ERC-1155-based digital certificate verification system on the Manta Pacific network, integrated into the EduVerse platform. The discussion follows the certificate lifecycle, from validation of completion, minting, integration of IPFS decentralized storage, and demonstration of the anti-transfer security feature (Soulbound Token). Each stage is illustrated through a user interface on the EduVerse platform, which has been successfully implemented in a system prototype. The implementation results demonstrate that the designed architecture is capable of functioning in accordance with the stated research objectives.

Figure 2. Course Display Image

The process begins in the user interface on the student's learning dashboard. The system is designed to ensure that certificates are only accessible after academic prerequisites are met. As seen in the course interface, the course completion status must reach 100% before the certificate issuance feature is activated. At this point, the "Get Certificate" button becomes active and accessible to the user, indicating that the pre-minting validation logic on the frontend is working properly to verify user eligibility before interacting with the smart contract.

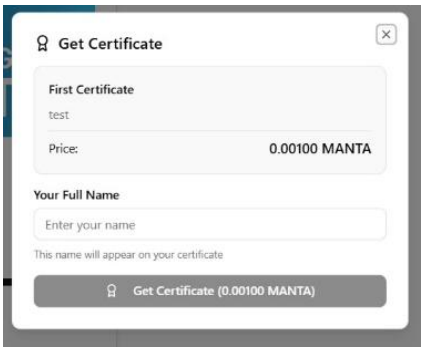

Figure 3. Name Input Form on Certificate

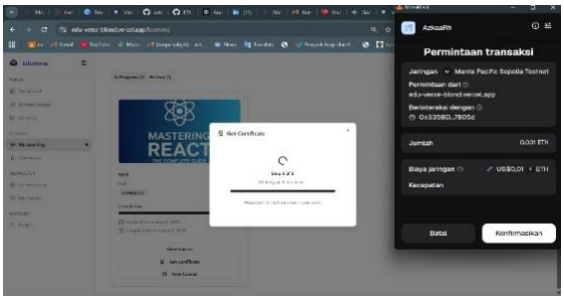

Figure 4. Transaction View in MetaMask

After the user initiates a certificate request, the system displays a data input form, as shown in Figure 3, for certificate personalization. The user is prompted to enter their full name, which will be permanently imprinted into the NFT metadata, ensuring the accuracy of the recipient's identity data. After name confirmation, the system automatically triggers an interaction with the MetaMask digital wallet. At this stage, the user approves the blockchain transaction, as shown in Figure 4. The transaction details show that the system runs on the Manta Pacific Sepolia Testnet network with highly efficient gas fees, demonstrating the advantages of using Layer 2 for scalable implementation in educational institutions.

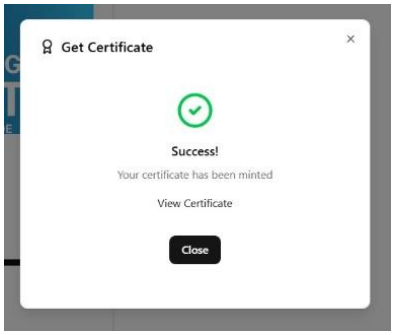

Figure 5. Successful Minting Process

Figure 6. Certificate

The system then processes the token minting transaction onto the blockchain. The interface provides visual feedback in the form of a "Minting on blockchain" progress bar to keep the user experience informative throughout the block validation process. The success of this process is indicated by a "Success" notification, confirming that the certificate has been successfully issued as a unique digital asset and is immutably recorded on the blockchain network, ready for viewing or verification.

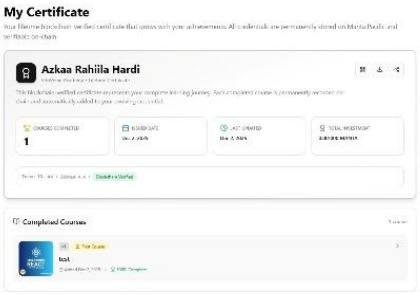

Figure 7. Dashboard "My Certificate"

After issuance, the generated certificate is immediately integrated into the user's "My Certificate" dashboard, as shown in Figure 6. This view provides comprehensive information including the Token ID, issuance date, and active blockchain verification status. In addition to the application dashboard, asset ownership can also be monitored directly through the digital wallet interface (MetaMask) in the NFT menu or during asset review. This indicates that the certificate metadata has been correctly stored in IPFS and successfully indexed by the digital wallet, enabling data interoperability beyond the campus' internal platform.

Figure 8. QR Code Certificate

To facilitate transparent external verification, the system generates a unique QR Code that links a public verification URL to a user-specific token ID. This feature bridges the gap between the physical and digital worlds, allowing third parties (such as company HR or other institutions) to instantly audit the certificate's authenticity simply by scanning the code. This mechanism eliminates the need for slow manual document legalization, replacing it with cryptographic proof that can be accessed within seconds.

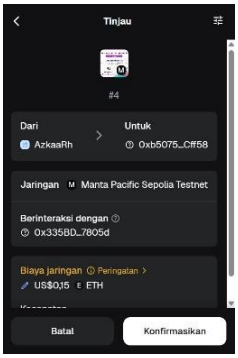

Figure 10. Certificate Transfer Trial

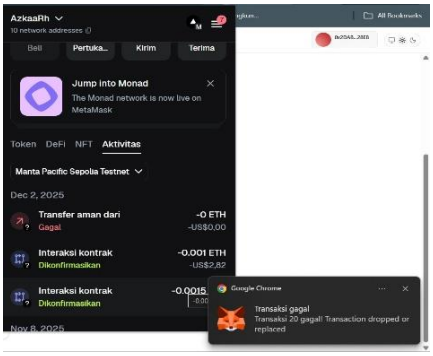

Figure 9. Certificate Transaction Failed

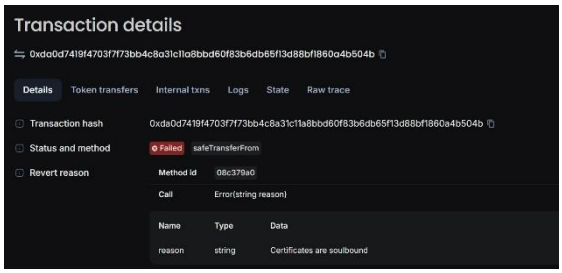

Figure 11. Soulbound Token Security Testing Through Asset Transfer Failure

The most crucial aspect of this system's security is the implementation of the Soulbound Token (SBT) property, which was tested through a forced transfer attempt. Figure 9 shows a user's wallet activity history, with a red entry marked "Failed" under the "Secure transfer from" transaction type. This indicates that when the user attempted to send their certificate to another wallet address, the network automatically aborted the transaction, as shown in Figure 8. Technical evidence of this failure is corroborated by data from the block explorer in Figure 10, which explicitly records the revert reason with the message: "Certificates are soulbound." This error message stems from the overriding logic of the safeTransferFrom function in the smart contract, which was deliberately programmed to block any attempt to transfer ownership. This finding empirically proves that the verification system is capable of preventing the practice of buying and selling certificates or counterfeiting ownership, because the certificate is permanently bound to the original recipient's wallet address.

B. Interface System Discussion

A discussion of the implementation and testing results indicates that the system design successfully addresses the research objectives and corroborates the findings of the literature review. Regarding certificate authenticity verification, the end-to-end flow, from meeting academic prerequisites through minting, storing metadata in IPFS, and finally verifying via QR code, is consistent with a decentralized verification framework that emphasizes reducing reliance on centralized databases and slow manual legalization. Modeling certificates as ERC-1155 NFTs on the Manta Pacific Layer 2 network effectively addresses the scalability and high gas fees often criticized for ERC-721 implementations on Layer 1 networks, aligning with studies highlighting the advantages of multi-token standards and batch minting techniques for large-scale asset issuance. The finding of transaction fees of approximately US$0.01 per certificate demonstrates the feasibility of this architecture for institutions with high graduate volumes and reinforces the argument that the combination of Layer 2, batching, and multi-token is key to operational efficiency.

In terms of security and ownership integrity, the implementation of Soulbound Token (SBT) with a block transfer function expands the concept of non-repudiation discussed in previous NFT research, while also closing the gap in the sale and transfer of credentials that is still possible with transferable NFTs. The integration of IPFS as an on-chain metadata store linked to ERC 1155 fills a gap in the literature that previously only examined IPFS or multi-token separately, while also approaching the interoperability principle proposed in studies of blockchain-based academic certificate systems and decentralized authentication schemes. Methodologically, the use of prototyping with user involvement supports the recommendation that blockchain systems in the educational realm must be validated not only from a technical perspective, but also for usability and user experience. Therefore, the main contribution of this research lies in the unification of three pillars blockchain, multi-token NFTs, and IPFS in a single certificate verification framework that is proven to be secure, efficient, and ready for adoption by educational institutions.

5. Conclusions

This study concludes that the ERC-1155 NFT-based digital certificate verification system on the Manta Pacific Layer 2 network can improve cost efficiency, data integrity, and ease of verification through the integration of IPFS and the Soulbound Token mechanism. However, the findings are still at the prototype stage with limited test scenarios. The prototyping approach used allows for rapid iteration but also limits the generalizability of the results due to the number and diversity of test users, dependence on specific wallets (such as MetaMask), and potential vendor lock-in risks on the third-party network and infrastructure used. Therefore, further academic research is needed to expand the test scenarios by involving more institutions and user profiles, comparative evaluation with other development methods, exploration of interoperability across wallets and networks, and in-depth analysis of security, privacy, and scalability aspects in the context of real-world implementation in the national education ecosystem.

References

[1] S. I. Mouno, T. Rahman, A. M. Raatul, and N. afees Mansoor, "Blockchain-Enhanced Academic Certificate Verification: A Decentralized and Trustworthy Framework," in *2024 International Conference on Advances in Computing, Communication, Electrical, and Smart Systems (iCACCESS)*, IEEE, Mar. 2024, pp. 1–5. doi: 10.1109/iCACCESS61735.2024.10499524.

[2] O. S. Oluwaseyi and R. O. Akinyede, "ISSN : 2249-0868 Foundation of Computer Science FCS," 2024. [Online]. Available: www.ijais.org

[3] D. Hawashin, M. Nemer, K. Salah, R. Jayaraman, D. Svetinovic, and E. Damiani, "Blockchain and NFT-based traceability and certification for UAV parts in manufacturing," *J Ind Inf Integr*, vol. 39, p. 100597, May 2024, doi: 10.1016/j.jii.2024.100597.

[4] H. Gaikwad, N. D'Souza, R. Gupta, and A. K. Tripathy, "A Blockchain-Based Verification System for Academic Certificates," in *2021 International Conference on System, Computation, Automation and Networking (ICSCAN)*, IEEE, Jul. 2021, pp. 1–6. doi: 10.1109/ICSCAN53069.2021.9526377.

[5] Tedyyana, Agus, et al. "Transforming the voting process integrating blockchain into e-voting for enhanced transparency and securiy." *TELKOMNIKA (Telecommunication Computing Electronics and Control)* 22.2 (2024): 311-320.

[6] A. M. B, K. B, S. M, and K. S, "Digital Certification – Certification Credential as Non Fungible Token (NFT)," in *2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, IEEE, Jun. 2023, pp. 1–7. doi: 10.1109/ICAECA56562.2023.10199759.

[7] "13.+Mathew+Sonita+365-371 (2)".

[8] S. Gangwar, "Blockchain-based Authentication and Verification System for Academic Certificate using QR Code and Decentralized Applications," 2024.

[9] K. Vo, T.-T. Ta, H.-T. Nguyen, and T.-A. Nguyen-Hoang, "Blockchain Solutions for Scalable and Sustainable Education: Enhancing Credentialing and Resource Management," in *Proceedings of the 17th International Conference on Computer Supported Education*, SCITEPRESS - Science and Technology Publications, 2025, pp. 216–223. doi: 10.5220/0013202500003932.

[10] H. Singh and A. Singh, "Blockchain and ESG," in *Sustainability Reporting and Blockchain Technology*, London: Routledge, 2024, pp. 3–14. doi: 10.4324/9781003378341-2.

[11] S. A. Faaroek, A. Saulina Panjaitan, Z. Fauziah, and N. Septiani, "Design and Build Academic Website with Digital Certificate Storage Using Blockchain Technology," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 3, no. 2, pp. 175–184, Apr. 2022, doi: 10.34306/itsdi.v3i2.562.

[12] Tony Haryanto and K. Ramli, "Secure Cybersecurity Information Sharing for Sectoral Organizations Using Ethereum Blockchain and IPFS," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 7, no. 3, pp. 670–680, Jun. 2023, doi: 10.29207/resti.v7i3.4956.

[13] "Blockchain Credentials : Revolusi Sistem Sertifikasi Pendidikan." Accessed: Nov. 29, 2025. [Online]. Available: https://bipk.uma.ac.id/2025/03/25/blockchain-credentials-revolusi-sistem-sertifikasi-pendidikan-yang-transparan-dan-anti-palsu/

[14] Wi. Swastika, H. W. Santoso, and O. H. Kelana, "RANCANG BANGUN WEBSITEAKADEMIK DENGAN PENYIMPANAN SERTIFIKAT DIGITAL MENGGUNAKAN TEKNOLOGI BLOCKCHAIN," *Jurnal Teknologi Informasi dan Ilmu Komputer* , vol. 9, pp. 33–40, Feb. 2022.

[15] "Panduan Anda untuk ERC-1155: Membandingkan ERC-721 dengan ERC-1155." Accessed: Jun. 06, 2025. [Online]. Available: https://www.alchemy.com/blog/comparing-erc-721-to-erc-1155

[16] "ERC721 vs. ERC1155: Key Differences, Use Cases & How to Choose | Speed Run Ethereum." Accessed: Jun. 06, 2025. [Online]. Available: https://speedrunethereum.com/guides/erc721-vs-erc1155

[17] S. Wanotayapitak, "Architecture for the Academic Certificate System on the Ethereum Layer 2 Solution," *CommIT (Communication and Information Technology) Journal*, vol. 19, no. 1, pp. 29–43, Apr. 2025, doi: 10.21512/commit.v19i1.11539.

[18] M. U. Hassan, Y. Abbas Bangash, W. Iqbal, A. Chehri, and J. Iqbal, "PRIDA-ME: A Privacy-Preserving, Interoperable and Decentralized Authentication Scheme for Metaverse Environment," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 493–515, 2025, doi: 10.1109/OJCOMS.2024.3523518.

[19] P. Rani, R. K. Sachan, and S. Kukreja, "Educert-chain: a secure and notarized educational certificate authentication and verification system using permissioned blockchain," *Cluster Comput*, vol. 27, no. 7, pp. 10169–10196, Oct. 2024, doi: 10.1007/s10586-024-04469-5.

[20] Y. Tan, Z. Wu, J. Liu, J. Wu, Z. Zheng, and T. Chen, "Bubble or Not: Measurements, Analyses, and Findings on the Ethereum ERC721 and ERC1155 Non-fungible Token Ecosystem," Jan. 2023, [Online]. Available: http://arxiv.org/abs/2301.01991

[21] Y. Wang *et al.*, "iBatch: saving Ethereum fees via secure and cost-effective batching of smart-contract invocations," in *Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, New York, NY, USA: ACM, Aug. 2021, pp. 566–577. doi: 10.1145/3468264.3468568.