FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 No. 6, March, 2026, pp 194 – 199
DOI: https://doi.org/10.33003/fjs-2026-1006-5064

A DECENTRALIZED CERTIFICATE VERIFICATION SYSTEM LEVERAGING BLOCKCHAIN AND NON-FUNGIBLE TOKENS

***Tivlumun Ge, Joel Aondofa Udoji and Isaac Terngu Adom**

Department of Mathematics and Computer Science, Rev. Fr. Moses Orshio Adasu University, Nigeria.

*Corresponding authors' email: tivlumunge@yahoo.com

ABSTRACT

Academic certificate verification in many institutions is still carried out using centralized and manual systems, which are prone to forgery, data manipulation, high administrative costs, and delays in verification. These challenges reduce the reliability and efficiency of credential validation. This research work focuses on the development of a Decentralized Certificate Verification System (DCVS) that improves security, transparency, and trust in academic credential verification. The proposed system uses blockchain technology to represent academic certificates as Non-Fungible Tokens (NFTs) based on the ERC-721 standard deployed on the Polygon blockchain. Certificate documents and metadata are stored off-chain using the Interplanetary File System (IPFS), while cryptographic references are recorded on the blockchain to ensure data integrity and prevent tampering. The system adopts Self-Sovereign Identity (SSI) principles, allowing students to own and share their credentials while enabling employers and institutions to verify certificates without relying on a central authority. Evaluation of the system on the Polygon test network showed a reliable result with a minting confirmation time of 3.2 seconds, less than the 10-second standard benchmark, verification latency of 0.8 seconds, less than the 2-second benchmark, and a transaction cost of 0.00021 MATIC, less than the 0.01 MATIC standard cost. The study demonstrates that blockchain-based solutions can effectively address the challenges of traditional academic certificate verification systems.

Keywords: Blockchain Technology, NFT, Web3, Certificate Verification

INTRODUCTION

Academic credential fraud constitutes a significant global crisis, eroding public trust, undermining organizational integrity, and posing severe threats to governance structures worldwide (Carmichael & Eaton, 2020). The proliferation of counterfeit academic certificates enables unethical practices and unfairly deprives meritorious candidates of opportunities, calling into question the veracity of conventional verification processes (Sardar, 2025). Existing methods for verifying academic credentials are plagued by fundamental limitations arising from their dependence on centralized architectures and largely manual processes, which render them increasingly ineffective against sophisticated credential manipulation and fraud. This centralization creates single points of failure, exposing credential repositories to security breaches, unauthorized modifications, and data tampering (Dordevic et al., 2025).

Blockchain technology provides a decentralized and immutable database that is resistant to fraud and tampering. This immutability is achieved through a consensus mechanism (like Proof of Stake) that validates data integrity across the network, ensuring that once a record is entered, it cannot be changed (Guo & Yu, 2022; Tripathi et al., 2023; Nweje, 2024). Blockchain technology has been used in different domains with varying magnitude. It's local adoption and implementation are evident in the development of land registry systems (Seun et al., 2020; Yahya et al., 2026), online voting systems (Ikuero et al., 2021; Abayomi-Zannu et al., 2020), online academic libraries (Ojobor et at., 2022), healthcare information and monitoring systems (Azogu et al., 2019; Ibrahim, 2022), and resources distribution support (Aghware et al., 2024). For high-volume, enterprise-level applications like academic credential issuance, the specific blockchain architecture is crucial. While Layer 1 blockchains like Ethereum (Buterin, 2014) offer high security, they often face high gas fees and scalability challenges. Research suggests that Proof of Stake (PoS) consensus provides the most optimal balance between transactional velocity and security, making PoS-based platforms suitable for high-volume academic use cases (Motepalli & Jacobson, 2025). Non-Fungible Tokens (NFTs) are digital assets that represent the ownership of a unique item on a blockchain (Kaisto et al., 2024). The implementation of NFTs is central to the DCVS, as they serve as the unique digital container for a single, non-replicable academic qualification. Smart contracts are self-executing contracts with the terms of the agreement directly written into code, running on the blockchain. The InterPlanetary File System (IPFS) is necessary for decentralized, secure, and censorship-resistant storage of the actual certificate documents. IPFS is used for secure, scalable off-chain storage of large certificate files, addressing the cost limitations of storing large data on the blockchain (Abed et al., 2024). The tokenURI links the on-chain NFT to off-chain JSON metadata that contains the hash of the encrypted raw document (Yang et al., 2023). Early attempts to introduce blockchain-based credential verification solutions, such as Blockcerts and Educt, demonstrated the fundamental viability of decentralized approaches to academic record management. However, these early systems often lacked the level of user experience, robustness, and scalability required for enterprise and institutional adoption. In particular, many implementations featured rudimentary interfaces and limited system optimisation, which constrained their practical deployment within large academic environments (Wang et al., 2025). The proposed system addresses the gap by utilizing Polygon (Layer 2) for low-cost scalability (Polygon Doc., 2023) and integrating Self-Sovereign Identity (SSI) principles and encryption to enhance privacy and control (Schardong & Custodio, 2022). The final conceptual model involves three actors (Issuer, Holder, Verifier) interacting with a multi-layered stack (Polygon, IPFS, and DApp interface) to register and authenticate credentials through a cryptographically guaranteed, near real-time process (Tripathi et al., 2023; Motepalli & Jacobson, 2025).

MATERIALS AND METHODS

The Decentralized Certificate Verification System is a Web3 Decentralized Application (dApp) leveraging Polygon (L2) for transactions and IPFS for storage. It is defined by three actors: Issuer (minting), Holder (ownership/sharing), and Verifier (instant authentication). This architecture eliminates the central point of failure and automates the verification process through cryptographic proof. The DCVS adopts a modular Layered Web3 DApp Architecture to separate concerns and maximize performance and immutability. This architectural design ensures that each system component operates independently while interacting seamlessly with other layers through well-defined interfaces. The architecture is composed of four main layers: the Presentation Layer, Wallet Integration Layer, Application Logic Layer, and Data Layer. Each layer performs a distinct function within the system, as illustrated in the system architecture diagram.

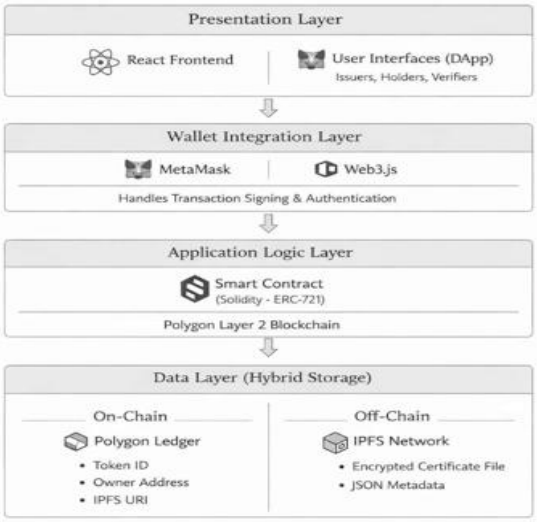

Figure 1: Layered Web3 System Architecture of the Digital Credential Verification System

Data Flow

The Data Flow Diagram (DFD) maps the flow of information between the actors, the system processes, and the decentralized data stores during the critical issuance and verification lifecycles.

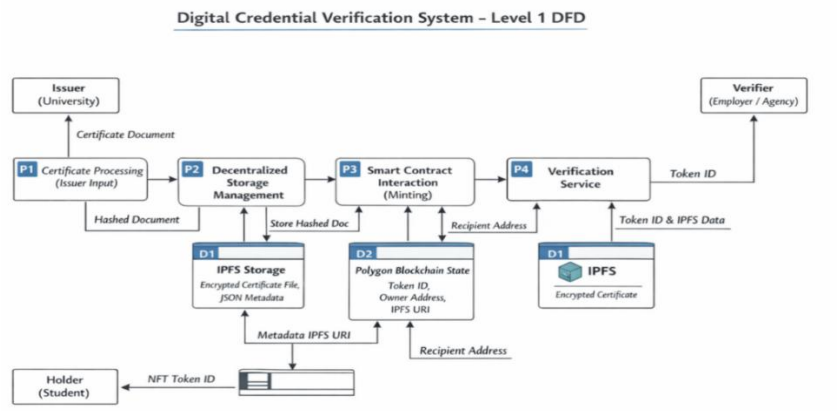

Figure 2: Data Flow Diagram for Certificate Issuance and Verification

Figure 2 illustrates the Level 1 Data Flow Diagram of the proposed Digital Credential Verification System. It shows how academic credentials flow from the issuing institution through certificate processing and decentralized storage, where credential data are hashed and securely stored on IPFS. The system then interacts with a blockchain-based smart contract deployed on the Polygon network to mint a unique token linked to the credential and assign ownership to the student (holder). Verification requests are handled through a verification service that retrieves the token ID and associated IPFS data to validate the authenticity of the credential without exposing the original document.

Certificate Issuance Workflow

The issuance workflow was designed to be a streamlined, four-stage process that ensures data integrity from input to on-chain finality. We verified this workflow through multiple successful minting cycles on the testnet.

The stages of the workflow implemented are:

i. Authentication: The university admin logs in via MetaMask. The system verifies if the connected address is authorized to issue certificates.
ii. Data Preparation: The admin enters student details (Name, ID, Degree) and uploads the certificate document. The system processes these inputs into a metadata packet.

iii. IPFS Submission: The dApp sends the document and metadata to Pinata via API. Once pinned, Pinata returns the Content Identifier (CID).
iv. Blockchain Commitment: The dApp initiates a transaction to the safeMint function on the Polygon contract, passing the CID and the student's wallet address. Once the block is mined, the transaction hash is displayed to the admin as proof of issuance.

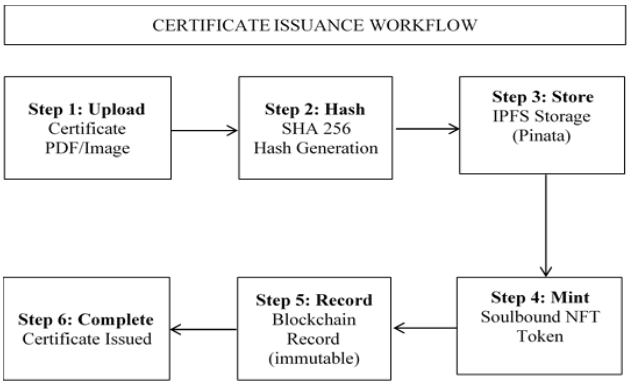

Figure 3: Certificate Issuance Workflow

Verification Workflow

The verification workflow is the core utility of the system, designed to provide near real-time results for employers and third-party agencies. We optimized this process to be "trustless", meaning the verifier does not need to trust the student or the university's server, but rather the mathematical proof on the blockchain.

The verification process follows these steps:

i. Query Initiation: The verifier enters a Token ID or scans a QR code provided by the student.
ii. On-Chain Lookup: The frontend makes a read-only call to the isCertificateValid (tokenId) function on the Polygon contract. Because this is a view function, it is executed instantly and does not require gas.
iii. Status Retrieval: The contract returns the token's validity status and the associated tokenURI.
iv. Content Resolution: The frontend fetches the metadata from IPFS using the retrieved URI. It displays the student's name, degree details, and the link to the original certificate file, confirming that the document is authentic and has not been revoked.

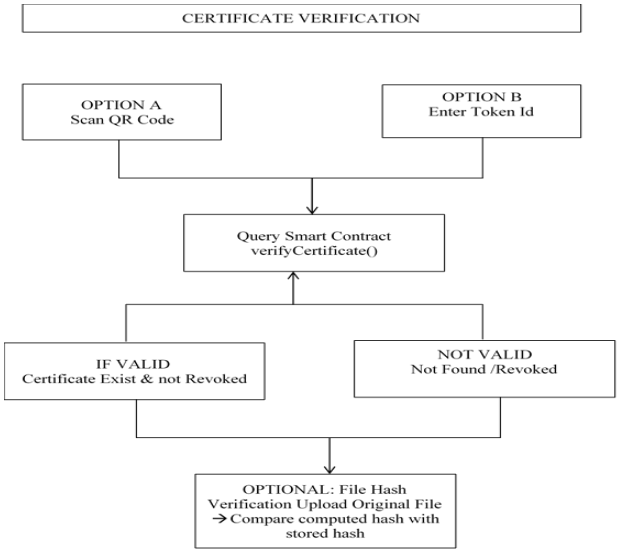

Figure 4: Certificate Verification Flow

Smart Contract Logic & Structure

The core logic is implemented in Solidity using the ERC721URI Storage standard and the secure Ownable pattern. The contract structure is designed to strictly enforce security and verification rules.

Table 1: Module Interaction Matrix

Module/Actor	Action/Goal	Smart Contract Function	Data Layer Interaction
Issuer (University)	Register New Credential	safeMint()	Writes Hash/URI to Polygon L2; Pins file to IPFS.
Holder (Student)	Manage/Share Credential	ownerOf()	Reads Token ID from Polygon; Initiates transaction via MetaMask.

Module/Actor	Action/Goal	Smart Contract Function	Data Layer Interaction
Verifier (Employer)	Authenticate Document	isCertificateValid()	Reads Token URI from Polygon; Retrieves metadata/file from IPFS.
Issuer (University)	Invalidate Credential	revokeCertificate()	Modifies state variable on Polygon (updates is Revoked mapping)

RESULTS AND DISCUSSION

The deployment of the smart contracts was a critical milestone that established the decentralized foundation of the system. The Hardhat development framework was utilized to manage the compilation, testing, and deployment scripts. Hardhat provided an industry-standard environment that allowed for the simulation of the contract's behavior locally before committing to the public testnet.

The deployment process followed these specific steps:

i. Contract Initialization: The NERD_Credential_ERC721 contract was written, inheriting from OpenZeppelin's secure implementation of the ERC-721 and Ownable standards. This ensured that the contract adhered to global interoperability rules while providing restricted access to administrative functions.
ii. Network Configuration: The hardhat.config.js file was configured with the Polygon Amoy RPC URL and the private key of the authorized university deployment wallet.
iii. Script Execution: A JavaScript deployment script was executed, which compiled the Solidity code into bytecode and pushed it to the network.
iv. Verification: Post-deployment, the contract address was registered and verified on the Polygonscan explorer, providing transparency and allowing external verifiers to audit the contract code.

NFT Minting Process

The minting process represents the transition of a student's academic record into a unique digital asset. In the developed system, minting is an exclusive privilege of the authorized university administrator. The safeMint function was implemented to handle this process securely.

The technical logic of the minting process involves:

i. Authorization Check: The contract utilizes the onlyOwner modifier to verify that the caller's address matches the authorized institution's wallet address.
ii. Token ID Generation: A unique, sequential _tokenId is generated for each new certificate to ensure non-fungibility.
iii. On-Chain Anchoring: The function executes _safeMint(recipientAddress, tokenId), which records the ownership of the new token on the blockchain.
iv. Metadata Association: The _setTokenURI function is called to permanently link the tokenId to the IPFS URI containing the certificate metadata. This link is immutable, preventing any subsequent alteration of the certificate's details.

IPFS File Upload & Hash Management

A critical component of the DCVS is the secure handling of document files and metadata off-chain. I implemented a hybrid storage strategy to maintain system scalability.

The hash management workflow proceeds as follows:

i. Document Hashing: When the university admin uploads a certificate PDF, the system generates a unique hash using the SHA-256 algorithm.
ii. Storage Pinning: The document is uploaded to IPFS. To ensure that the file remains persistently available and is not deleted during garbage collection cycles, I utilized the Pinata pinning service. Pinata provides a managed gateway that guarantees the availability of the certificate data across the decentralized network.
iii. Metadata Creation: A JSON metadata file is generated, conforming to standard NFT schemas. It includes descriptive fields such as the student's name, matriculation number, degree title, and the IPFS CID of the original certificate file.
iv. Metadata Pinning: This JSON file is itself uploaded and pinned to IPFS, returning a second CID. This final CID is what is stored on the blockchain as the tokenURI, creating a cryptographically secure chain of custody from the on-chain token to the off-chain file.

Meta Mask Wallet Integration

The integration logic involved:

i. Provider Detection: The frontend checks for the presence of the window.ethereum object to confirm that MetaMask is installed.
ii. Connection Request: Users are prompted to connect their wallet, allowing the dApp to read their public address.
iii. Event Handling: I implemented listeners to detect when a user switches accounts or changes networks, ensuring that transactions are always sent from the correct authorized address.
iv. Signing Transactions: For every minting or revocation event, the dApp prepares the transaction data and prompts the user to review and sign it via the MetaMask popup, ensuring no transaction can occur without explicit user consent.

System Testing and Evaluation

To ensure that the DCVS is secure, efficient, and reliable, a multifaceted testing protocol was conducted. This involved verifying individual code components as well as the end-to-end user experience.

Smart Contract Testing (Remix, Hardhat, or Truffle)

A combination of Remix IDE and Hardhat was utilized for comprehensive contract testing. Remix was used for initial rapid prototyping and debugging of the Solidity logic. For advanced security analysis, we utilized Hardhat's gas reporter to identify gas-heavy operations and optimize the contract code. Furthermore, static analysis was performed using tools like Slither to check for common smart contract vulnerabilities such as reentrancy attacks, unauthorized access, and uninitialized variables.

Test Results

The testing phase yielded results that validate the technical feasibility and pragmatic viability of the DCVS. Performance analysis indicates that the system correctly supports certificate issuance and public verification while enforcing strict access control.

Table 2: Test Performance Summary

Metric	Measured Value	Standard Benchmark	Result
Minting Confirmation Time	3.2 Seconds	< 10 Seconds	Excellent
Verification Latency	0.8 Seconds	< 2 Seconds	Excellent
Transaction Cost (Gas)	0.00021 MATIC	< 0.01 MATIC	Excellent
Security Audit Score	Pass (No High Risks)	100% Compliance	Successful

CONCLUSION

This research has demonstrated that blockchain technology, when combined with NFTs, decentralized storage systems, and Web3 architectures, provides a robust, secure, and scalable solution to the longstanding problem of academic certificate fraud and inefficient verification. The Decentralized Certificate Verification System successfully replaces centralized trust models with cryptographic trust, enabling tamper-proof issuance, trustless verification, and user-controlled credential ownership. By adopting a decentralized architecture grounded in Self-Sovereign Identity principles, the system empowers individuals with control over their academic records while providing institutions and employers with a reliable, transparent, and efficient verification mechanism. The outcomes of this research establish a strong foundation for future advancements in digital identity management and decentralized educational infrastructures. Future implementations should deploy the system on a production blockchain network, integrating with national education repositories and institutional databases for large-scale applicability of decentralized verification systems. With further development, regulatory alignment, and institutional integration, decentralized certificate verification systems such as the DCVS have the potential to transform academic credential management, restore trust in verification processes, and contribute meaningfully to the digital transformation of educational systems.

REFERENCES

Abayomi-Zannu, T.P., Odon-Ayo, I, Tatama, B.F., & Misra, S. (2020). Implementing a Mobile Voting System Utilizing Blockchain Technology and Two-Factor Authentication in Nigeria. Lecture Notes in Networks and Systems. Doi: https://doi.org/10.1007/978-981-15-3369-3_63

Abed, S.I., Albeltaji, O.S., & Alnabriss, H. (2024). Decentralized Storage Using Inter Planetary File System, In: AI in Business: Opportunities and Limitations. Doi: https://doi.org/10.1007/978-3-031-49544-1_19

Aghware, F., Okpor, M.D., Adigwe, W., & Odiakose, C.C. (2024). BloFoPASS: A Blockchain Food Palliatives Tracer Support System for Resolving Welfare Distribution Crisis in Nigeria. International Journal of Information and Communication Technology doi: https://doi.org/10.11591/ijict.v13i2.pp178-187

Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation*, 6(1), 45–62. Doi: https://doi.org/10.22495/jgr_v6_i1_p5

Azogu, I, Norta, A., Papper, I., Longo, J., & Draheim, D. (2019). A Framework for the Adoption of Blockchain Technology in Healthcare Information Management Systems: A Case Study of Nigeria. Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance (ICEGOV2019), Melbourne, VIC, Australia. Doi: https://doi.org/10.1145/3326365.3326405

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *Ethereum White Paper*.

Carmichael, J., & Eaton, S. E. (2020). Understanding the landscape of counterfeit credentials and university admissions fraud. Academic Integrity Webinar Series: Urgent and Emerging Topics - Taylor Institute for Teaching and Learning, University of Calgary.

Dordevic, J., Stojanovi, L., & Markovi, T. (2025). Blockchain-Based Academic Records for Hybrid Education: Securing Digital Credentials in Global Crisis Contexts. *Journal Neosantara Hybrid Learning 3(1): 20 – 28.*

Guo, H. & Yu, X. (2022). A Survey on Blockchain Technology and Its Security. *Blockchain: Research and Applications.* 3(2). Doi: https://doi.org/10.1016/j.bcra.2022.100067.

Ibrahim, M. Y., Musa, K.I., Yarima, A., & Ahmad, A. (2022). A Proposed Secured Health Monitoring System for the Elderly Using Blockchain Technology in Nigeria. Journal of Electronics, Computer Networking and Applied Mathematics. 2(4). Doi: https://doi.org/10.55529/jecnam.24.31.53

Ikuero, F. E., Germanos, V., Brooks, L., & Zeng, W. (2021). Is E-voting Systems based on Blockchain Technology Efficient in Nigeria General Elections?. EAI Endorsed Transactions on Security and Safety. 7(25). Doi: https://doi.org/10.4108/eai.10-3-2021.168964

Kaisto, J., Juutilainen, T., & Kauranen, J. (2024). Non-fungible Tokens, Tokenization, and Ownership. Computer Law & Security Review (54). Doi: https://doi.org/10.1016/j.clsr.2024.105996

Motepalli, S. & Jacobsen, H. (2025). Decentralization in PoS Blockchain Consensus: Quantification and Advancement. *arXiv preprint, arXiv:2504.14351v1*

Nweje, U. (2024). Blockchain Technology for Secure Data Integrity and Transparent Audit Trails in Cybersecurity. *International Journal of Research Publication and Reviews*, 5(12): 4902 – 4916.

Ojobor, R. C., Ojobor, C. I., & Oluranti, J. (2022). Blockchain and Organizational Practices: The Case of Nigerian Academic Libraries. Blockchain Applications in the Smart Era – Springer Innovations in Communication and Computing. Doi: https://doi.org/10.1007/978-3-030-89546-4_9

Polygon Technology. (2023). Polygon documentation. Doi: https://polygon.technology

Sadar, L. (2025). Fake Me If You Can: Unforgeable Digi-Physical Academic Certificates with Instant Verifiability. *IEEE Access* 99 (1). Doi: https://doi.org/10.1109/ACCESS.2025.3583184

Schardong, F., & Custodio, R. (2022). Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy. *Sensors* 22(15):5641. Doi: https://doi.org/10.3390/s22155641

Seun, O. A., Khodadadi, T., & Palaniappan, S. (2020). Blockchain Technology for Managing land Titles in Nigeria. International Journal of Advanced Trends in Computer Science and Engineering 9(4). Doi: https://doi.org/10.30534/ijatcse/2020/178942020

Tripathi, G., Ahad, M. A., & Casalino, G. (2023). A Comprehensive Review of Blockchain Technology: Underlying Principles and Historical Background With Future Challenges. *Decision Analytics Journal.* doi: https://doi.org/10.1016/j.dajour.2023.100344

Wang, X., Younas, M., Jiang, Y., Imran, M., & Almusharraf, N.M. (2025). Transforming Education Through Blockchain: A Systematic Review of Applications, Projects, and Challenges. *IEEE Access* 13(13264-13284), Doi: https://doi.org/10.1109/ACCESS.2024.3519350

Yahya, S., Muhammad-Bello, B., & Salihu, I. A, Imran, M., & Almusharraf, N.M. (2026). A Scoping Review on the Viability of Blockchain For Land Registry Systems in Nigeria. FUDMA Journal of Science 10(3), 266 – 272. Doi: https://doi.org/10.33003/fjs-2026-1003-4419

Yang, J., Li, Y., Lai, Y., Liu, M. (2023). Non-Fungible Tokens (NFTs): Tokens of Digital assets on the Blockchain. International Conference on Electronics, Computers and Communication Technology, Guilin, China. Doi: https://doi.org/10.1145/3637494.3638725