

NFTcate: A Soulbound Non-Fungible Token Decentralized User-Centered Certificate Verification System

¹Khadija S. Ladan, ^{*1}Olayemi M. Olaniyi, ²Abraham A. Alfa,
¹Abdullateef E. Salihu and ³Bello Kontagora Nuhu

¹Department of Information Systems and Technology National Open University of Nigeria, Abuja, Nigeria.

²Confluence University of Science and Technology, Osara, Kogi State, Nigeria.

³Federal University of Technology, Minna, Niger State, Nigeria.

*Corresponding authors' email: omolaniyi@noun.edu.ng

ABSTRACT

Many countries, with emphasis on Nigeria, face a critical challenge with the undermining of educational systems and graduate qualification credibility. Popular physical and hardcopy-based certificates linked to centralized databases are vulnerable to fraud and inefficiency while also limiting the accessibility of these processes across institutions. This paper presents NFTcate, a decentralized certificate verification system that leverages Soulbound Non-Fungible tokens (SBTs) built on the Ethereum blockchain. The system ensures that certificates are permanently bound to the recipient wallet, immutable, and can be publicly verified by institutions and employers, thus preventing transfer and replication. The system uses a combination of smart contracts, IPFS-based decentralized storage, and an intuitive web interface, which helps users' ability to interact with the system without prior blockchain knowledge. Evaluations of the presented system were done across four metrics: cost-efficiency, speed, universality, and testability, which show that the system performed comparatively better than existing systems. The cost of issuing a certificate was also significantly lower during testing as compared to the Mainnet and Testnet. NFTcate does not limit institutions, and if an institution is verified on the system, they can distribute certificates to students' wallets.

Received: 29 July 2026

Accepted: 17 Aug. 2026

Published: 15 Sept. 2026

Keywords: Academic Skill, Blockchain, Fraud, Integrity, Soulbound Tokens, Validation

INTRODUCTION

Educational competencies are important to a person's personal development and professional journey. In Nigeria, certificates are a way to validate a person's skills, academic achievements, and worthiness for a particular job or position. Unfortunately, due to the widespread issue of certificate forgery and manipulation, the integrity of these documents is being diminished. According to Essien (2024), employers often encounter fake or doctored credentials during the recruitment process. This has led to distrust in credentials and has made employers need to go through complex and elaborate means to verify these certificates. Motuz et al. (2024) further emphasized that this trust is further weakened across institutions because of the lack of educational standards and a centralized verification protocol.

The majority of blockchain use cases relate to data management and data verification, with the most popular sector being the finance sector, with governmental institutions being significantly slower to adopt (Kaspars & Renāte, 2018). While various approaches have been introduced to counter document fraud, such as the solutions by Aini et al. (2023) and Goswami et al. (2024). These solutions remain largely centralized or require a certain level of blockchain knowledge, high operation costs, and low usability. Moreover, cross-border authentication is hampered by a lack of interoperability and shared standards. As highlighted by (Barone & Herbaut, 2024), such systems are also inaccessible to marginalized populations, deepening educational inequality.

The rise of blockchain technology has brought us Non-fungible Tokens (NFTs), which are a new model for digital certificate issuance and verification. NFTs are unique tokens stored on a blockchain. They can be used as assets or, in this

context, Cryptographic proof of ownership or validity for certain digital or physical goods. NFTs are unique, indivisible, and interoperable as they rely on blockchain standards like ERC-721 and ERC-1155. Their uniqueness when used in asset management makes them much more valuable, and by mid-2024 was projected to have a total market value of about \$69 million. NFTs are widely used in gaming, collectibles, art, and decentralized finance (DeFi) (Ma et al., 2025).

The ability of NFTs to be moved across digital wallets is a crucial feature that determines their use cases and market dynamics. This category includes assets that can be traded freely as well as tokens that are permanently associated with a particular identity.

The most prevalent and commercially oriented NFT type is the Transferable NFT. These tokens facilitate seamless platform and marketplace interoperability by conforming to standards such as ERC-721 and ERC-1155. Open commerce is a natural fit for their concept, allowing people to buy, sell, and give freely. The economic value of transferable NFTs is greatly influenced by their perceived cultural or utility-based relevance, scarcity, and supply-demand dynamics (Ma et al., 2025).

There are also partially transferable NFTs that operate according to conditional transfer rules that are built into their smart contracts. Several restrictions are necessary to ensure that ownership can only shift in authorized or predetermined situations. Transfer restrictions, which go beyond conventional NFTs, provide an additional layer of governance and security. They may be determined by community consensus, user roles, time, or compliance checks (Ji et al., 2024).

The less popular NFTs, as it relates to user awareness, are the non-transferable NFTs, often referred to as Soulbound Tokens (SBTs), which were introduced as a solution to the problem of personal qualities or credentials not being able to be represented on-chain (Ohlhaber et al., 2022). SBTs by design are non-transferable and permanently linked to a particular wallet, or "soul". Their nature to remain fixed to one "soul" forever fits in well with use cases pertaining to trust, identity, and non-replicable accomplishments such as academic credentials.

The current method for certificate verification in Nigeria faces limitations that hinder its reliability and accessibility. The common way of paper verification in West Africa is long, hard, and inconsistent. It often requires direct contact between institutions, which can be time-consuming (Nwaocha & Oloyede, 2022). This is largely due to a lack of a strong centralized platform, which has given rise to the spread of false academic records, and the popular manual methods are ineffective due to sophisticated and modern forgery methods (Emeka, 2024). Similarly, (Effiong et al., 2022) spotlighted that traditional systems find it hard to differentiate between originals and fake certificates, which can be said to be particularly due to the existence of unregulated accreditation bodies.

Regardless of their widespread adoption, blockchain-based certificate verification systems have several structural and practical issues. These systems are often restricted in their scalability and accessibility because they require some sort of technical know-how of blockchain from the users. Some NFT-based systems usually face transfer and illegal sale issues, which compromise the security and legitimacy of these systems (Utsahawattanasuk et al., 2024). Additionally, current implementations of these systems are often restricted to a single institution, which is critical to building a trustworthy educational ecosystem (Jha et al., 2023).

Still on the limitations of blockchain systems, there is a need to consider revocation, real-time verification, and cost-effective deployment methods (Ruan et al., 2023). This study focuses exclusively on academic certificates issued by National Universities Commission-accredited universities. The NFTcate system is developed and tested on the Sopolia Ethereum Testnet, which provides a means to work and test a Testnet that works exactly like how the Ethereum Mainnet functions. Non-academic and vocational certifications are outside the scope.

By establishing a blockchain-based system that supports not only decentralized issuance through NFTs but also includes public verification, this research addresses gaps left by centralized certificate verification systems. This also promotes digital inclusiveness by introducing a system that is accessible to non-technical users. NFTcate contributes both a proof-of-concept and a working implementation to the growing body of educational blockchain applications, offering Nigerian universities a future-proof, secure, and cost-effective alternative. The remainder of this paper follows Section 2, related work that explores other implementations of blockchain in certificate verification and issuance. Section 3 presents the materials, methods, and system architecture used. Section 4 discusses system implementation, results, and comparison with a few similar systems. Lastly, Section 5 offers a conclusion and summary of the system as well as suggestions for future iterations.

Related Work

Latest advances in blockchain technology have inspired the development of certificate verification systems specialized for the educational ecosystem with a focus on verifiability,

fraud prevention, portability, and automation. These implementations range from NFT-based frameworks that can go further into Soulbound tokens to mobile-first implementations. Some of these frameworks are theoretical while others bring proof of concept, but each of them addresses key challenges in academic credential issuance and verification. Studies have emerged both globally and in the African context, including Nigeria, showing that blockchain-based digital credentials have been adapted for the administration of local infrastructure, realtors, justices, and the needs of users. The following systems represent a diverse selection of innovative efforts aimed at improving trust, accessibility, and automation in the academic certificate landscape.

Kandwal et al. (2025) introduced a universal NFTCert, which is a blockchain-based certification framework in which institutions can issue credentials as NFTs while targeting a fiat payment interface to remove typical cryptocurrency usage barrier issues. This significantly reduces friction between users who may not be familiar with crypto technology, thereby enhancing accessibility. The system has great potential to extend to global micro-certification ecosystems and short-term educational programs where verification, ownership, and issuance transparency are crucial. However, this system, despite its advantageous simplicity and transparency, inherits limitations from the use of the standard NFT protocols, most notably its inability to restrict resale and transfer of token ownership due to the absence of Soulbound characteristics of the tokens or built-in revocation mechanisms that ensure tighter control over credential validity and ownership.

Authors in Ifeyemi et al., (2024) developed a prototype in Nigeria that issues certificate hashes and associated metadata on the Celo blockchain, which is accessible through QR codes. This prototype was evaluated based on UI design (78%), revocation (67%), and maintainability (46%). Its application included providing portable, low-cost verification tools for Nigerian universities. Although this prototype is practical and mobile-friendly, it lacks decentralized minting, suffers from maintainability gaps, and depends heavily on the centralized user.

Authors in de-Souza-Daw & Ross, (2023) integrated blockchain into the auditing procedures of accreditation to minimize repudiation and enable inside and outside investigation. The method accommodates practical requirements like grade or name corrections. Better flexibility and mistake management are the main advantages. On the other hand, because corrections need to be authorized and tamper-conscious, which could affect auditability and confidence, complexity rises.

A theoretical framework by Nielson (2023) posited that institutions should issue non-transferable (SBT-based) degrees that can be validated by peers and employers. The main goals of this design are to avoid certificate reselling and to improve security. The benefits include fraud prevention and complete user control without the need for middlemen. However, implementation is slowed by unresolved legislative difficulties around digital credentials, a lack of user-friendly interfaces, and technical institutional obstacles.

The author in Akowe, (2023) developed a platform that is commercially used in Nigeria and collaborates with significant telecom companies and academic institutions. It prevents certificate fraud by using blockchain-hashed credentials and wallet-based access. Although it effectively interfaces with current systems and mobile infrastructure, institutional users still need to receive blockchain training, and it is still heavily reliant on telecom backends.

The integration of NFTs into blockchain increases the verification and authentication procedures for educational qualification and certification across institutions, learners, and employers (Naik & Naik, 2024). This overcomes the weaknesses in conventional certification without trust, proof of ownership, and low transferability. The system was built with the ERC721 NFT standard, OpenZeppelin smart contract, and several tools like Pinata Cloud, Alchemy, and Hardhat. It could be extended to cases like university certification verification.

The use of blockchain-based technology, particularly NFTs for the issuance and verification of academic credentials, was undertaken by (Delgado-von-Eitzen et al, 2024). It maintains and complies with the General Data Protection Regulation when issuing certificates and rewarding achievements virtually. Although it highlighted the privacy concerns of blockchain systems, more efforts are needed to provide better control and management of data subjects and entities in the digital/virtual space.

MATERIALS AND METHODS

This paper proposes a decentralized certificate verification system called NFTcate, designed to combat academic credential fraud by issuing non-transferable digital certificates as Soulbound NFTs on the Ethereum blockchain. Employers, institutions, and other stakeholders can instantly verify the authenticity of a student's academic record through a publicly accessible API that checks smart contract data and immutable metadata stored on IPFS. In NFTcate, the paper implements a permissioned minting process where only verified institutions can issue certificates to students, ensuring trusted issuance and control. By combining SBTs with decentralized storage and revocation mechanisms, NFTcate enhances security, prevents unauthorized resale or duplication of credentials, and simplifies real-time verification.

The proposed system is built on a public Ethereum test network and integrates wallet-based authentication for both issuers and recipients. Only accredited institutions are authorized to mint certificates, while students retain sole ownership without the ability to transfer them, ensuring integrity and permanence in academic recognition. Figure 1 shows the system architecture showcasing the flow of each node and their relationships with each other.

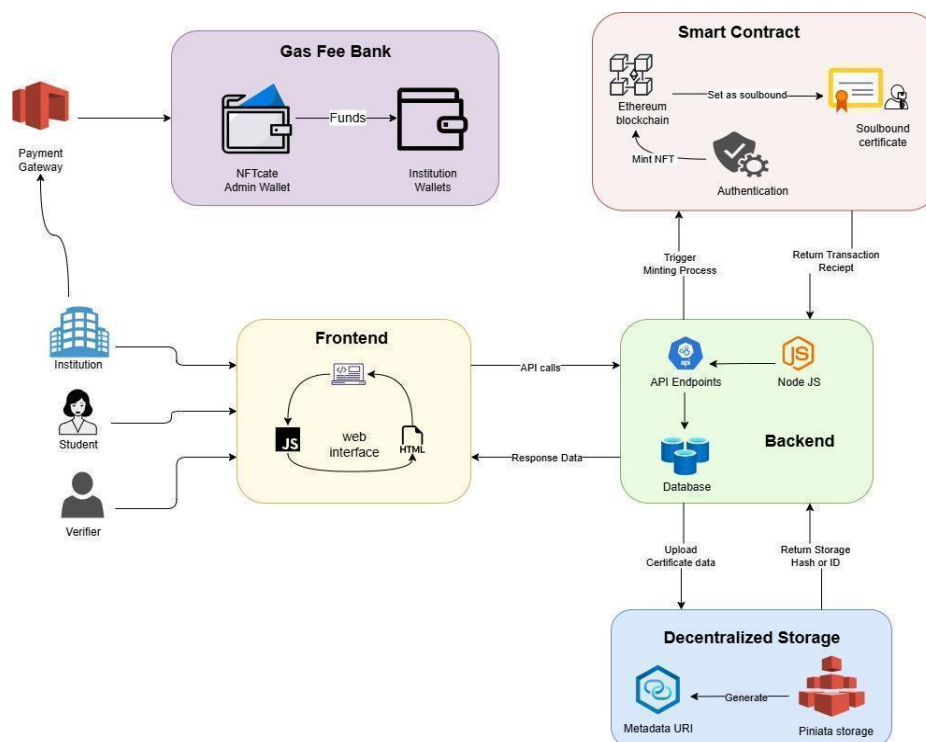


Figure 1: System Architecture for NFTcate

NFTcate uses a smart contract-driven workflow based on Soulbound non-fungible tokens (SBTs) to provide a safe, open, and impenetrable certificate issuance and verification procedure. Only accredited educational institutions are permitted to mint certificates, which are permanently linked to a student's wallet address and are not transferable or

resellable. NFTcate removes the need for middlemen and human verification by utilizing Ethereum smart contracts for token issuance and validation and IPFS for decentralized information storage. Figure 2 shows the system flowchart as used in the smart contract.

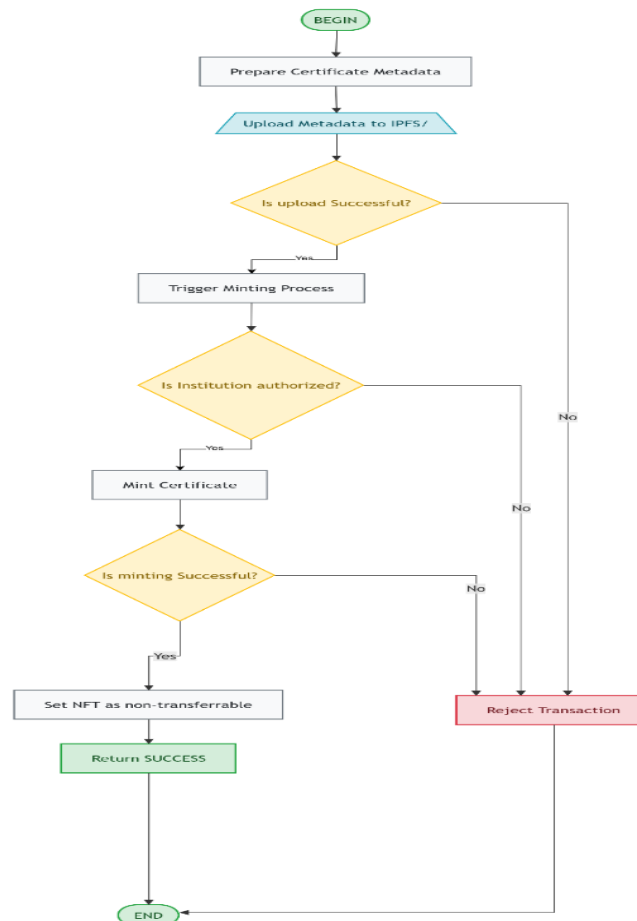


Figure 2: System Smart Contract Flowchart

The full lifecycle of certificate issuance, ownership, and verification within the NFTcate ecosystem is described as follows:

First, an accredited institution logs into the NFTcate platform through a secure authentication system and initiates certificate issuance and minting. The system verifies authorization, and the certificate data (such as name, degree, course of study, date) is compiled into a metadata file and uploaded to InterPlanetary File System (IPFS) for decentralized storage. The smart contract then mints the NFT, embedding the IPFS hash and issuing it to the student's Ethereum wallet. The student receives a permanently bound non-transferable NFT to their wallet whose ID they can share with verifiers to validate the certificate in real time without needing to contact the issuing institution.

Next, four essential components of the proposed NFTcate system were highlighted. The first component is the *schema*, which follows the certificate data structure in the database, which includes fields such as student name, institution, degree title, issuance date, and a link to metadata stored on IPFS. The second component is the *minting process*, which is permissioned and restricted to verified institutions. When minting, the smart contract creates a non-transferable certificate NFT bound permanently to the student's wallet, embedding a reference to the decentralized metadata. The third component is the *verification process*, which enables any third party such as employers or academic institutions to validate certificate authenticity and ownership by checking the issuer address, token metadata, and revocation status directly on the blockchain. As NFTcate issues certificates as soulbound tokens, transferability is permanently disabled by

design, and trading or resale of academic credentials is not supported within the framework.

Schema

In NFTcate, each certificate minted by an accredited institution is represented and stored using a structured schema in the backend database. This schema enables proper linkage between the physical representation of the certificate, its blockchain transaction, and the respective identities of the issuer and recipient. It differs from the NFT metadata itself by focusing on how the system internally organizes, tracks, and manages certificate records after minting.

Each certificate entry in the database includes a unique identifier (id), a publicly accessible *imageUri* hosted via IPFS, a *metadataURI* pointing to the decentralized metadata file, a serialized transaction receipt from the blockchain minting process, and foreign keys (*issuerId* and *ownerId*) that associate the certificate with a verified institution and a student.

This schema allows the system to track the exact blockchain transaction related to each certificate, link each certificate to its verifiable on-chain metadata and image through IPFS, maintain an audit trail of certificate issuance, and prevent unauthorized minting or duplication through tight issuer-recipient relationships.

By separating backend certificate records from the metadata attached to the NFT itself, NFTcate supports robust verification, institutional traceability, and compliance with decentralized record-keeping standards.

Table 1 shows a summary of the tech stack used in the development of NFTcate.

Table 1: Tech Stack Summary

Component	Technology	Reasoning
Smart Contract	Solidity + Hardhat	Industry standard for Ethereum development
Frontend	React + TailwindCSS	Responsive, fast UI with minimal complexity
Backend	Node js + TypeScript	Flexible and typesafe API development
Storage	IPFS via Pinata	Decentralized and cost-effective
Blockchain	Ethereum Testnet	Public, permissionless

RESULTS AND DISCUSSION

Results

Minting Process

To illustrate the minting process in NFTcate, the paper presents a schematic issuance of a certificate to a student named Aisha Bello who has successfully graduated from the National Open University of Nigeria (NOUN). Once NOUN verifies that the student has completed all academic requirements, they initiate a request to NFTcate to mint a verifiable digital certificate.

To bridge the gap between technicality and usability in NFTcate, the minting process is fully managed by the platform. Upon the institution's request, NFTcate generates a metadata JSON object containing essential details. Specifically, the student's ID, full name, and the URI of the certificate image hosted on IPFS. This metadata is uploaded to IPFS, and the resulting content-addressed URI (*metadataURI*) is included in the minting request to the smart contract. NFTcate then interacts with the Ethereum testnet smart contract to mint a soulbound NFT representing the certificate.

Once the minting is successful, the NFT is immediately transferred to the student's wallet address. The smart contract logs this transaction and establishes the institution as the issuer and the student as the owner. The on-chain state records the issuer and owner addresses.

In parallel, NFTcate also stores a certificate record in its backend database for indexing and querying. A typical certificate document in the backend contains the IPFS URI of the image, the metadata URI, the full transaction receipt (stringified), and foreign keys linking the record to both the

issuing institution and the recipient student. This streamlined minting flow ensures that ownership is established on-chain the moment the NFT is created, enabling immediate verification and preventing any intermediate states where the certificate exists without a defined owner. The creator address on-chain remains publicly verifiable and corresponds to the institution's registered wallet on NFTcate, providing cryptographic proof of origin for each certificate issued.

Verification Process

The ease with which physical certificates can be faked or altered, as well as the frequently time-consuming and expensive process of confirming, makes verification ineffective and unsafe. Using Soulbound Non-Fungible Tokens (SBTs), NFTcate provides an inexpensive and tamper-proof verification method to address these issues. Only approved organizations can mint these tokens, which are permanently attached to the recipient's wallet to stop illegal transfers. Every time a certificate is issued, NFTcate keeps ownership and transactional metadata off-chain in a safe backend database, while storing important data on-chain. By using public blockchain data and cryptographic hash signatures, the process of verifying the legitimacy of certificates becomes transparent.

The verification process successfully allowed third-party verifiers, upon receiving the token ID or link (such as <https://QmT6abc123xyzDEF987ghijkLMN...>), to validate certificates in real-time. The backend searches for its certificate collection using this CID and returns the certificate records, such as student and issuer/institution details. This returns an output as shown in Figure 3.

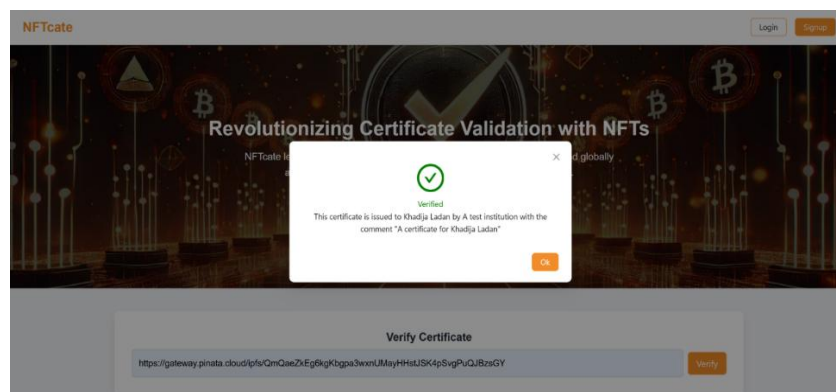


Figure 3: Interface of Completed Verification Process

For additional visual confirmation, the verifier can open the imageUri provided in the certificate record to view the actual digital certificate stored on IPFS. This image is the officially issued certificate and includes visible details such as name, matric number, course of study, and issuing institution.

By striking a balance between openness, security, and data efficiency, this hybrid on-chain/off-chain procedure allows third-party verifiers to instantly verify a certificate's provenance and authenticity without needing access to internal institutional systems.

Discussion of Findings

The evaluation of NFTcate reveals a system that is not only functionally sound and technically efficient but also socially relevant and contextually optimized for Nigerian higher education. By testing and analyzing the system's behavior under practical conditions, its suitability for production deployment becomes evident—particularly in terms of its affordability, responsiveness, robustness, and user accessibility.

A major highlight of NFTcate is its cost-efficiency. In blockchain-based systems, especially those using public networks like Ethereum, transaction (gas) costs are a common concern. To test the real-world affordability of NFTcate, the average gas consumption required to mint a certificate was measured to be approximately 171,511 gas units, with a gas price of 0.0229 gwei on the Sepolia testnet. When extrapolated to Ethereum mainnet gas prices and converted to the Nigerian Naira, this translates to between ₦641 and

₦1283 per certificate depending on prevailing ETH-to-Naira rates and gas congestion levels. This cost is markedly lower than traditional certificate issuance or verification letters in Nigerian universities, which can range from ₦10,000 to ₦15,000 per request. This stark difference suggests that NFTcate could revolutionize certificate access by dramatically reducing the financial burden on graduates and institutional administrators. A log of the gas used and total cost on the Sepolia testnet can be seen in Figure 4.

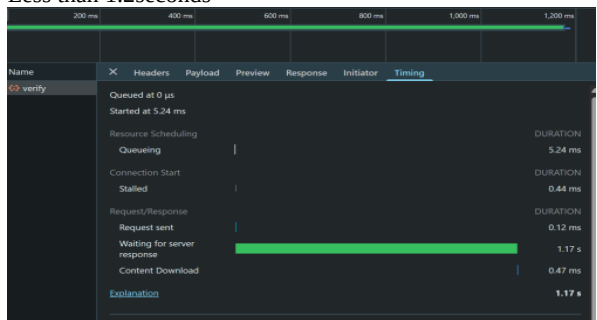
```
Gas Used: 171511
Gas Price: 0.022994941 gwei
Total Gas Cost: 0.000003943885325851 ETH
```

Figure 4: A Console Log of the Gas Used, Gas Price, and Total Cost on the Testnet

In terms of system responsiveness, Table 2 shows that NFTcate exhibits performance metrics that are on par with, or better than, many mainstream web applications. Uploading certificate metadata to IPFS consistently took less than one second, while the actual minting process on the blockchain averaged between 11 and 20 seconds. Certificate

verification—whether by students, employers, or third parties—was achieved in under 1.2 seconds through the public verification page. These figures position NFTcate as a near-real-time solution, making it viable for use in high-pressure situations such as job interviews, visa applications, or scholarship reviews.

Table 2: Performance Timing of the Proposed System

Operation	Average Duration
IPFS upload	Less than 1 second
	<pre>> nftcate-backend@1.0.0 dev > ts-node src/app.ts Connected to MongoDB Server running on port 3000 IPFS Upload Time: 0.605 seconds IPFS Upload Time: 0.62 seconds</pre>
Minting Transaction	Approximately 11-20 seconds depending on network stability and file size
	<pre>> nftcate-backend@1.0.0 dev > ts-node src/app.ts Connected to MongoDB Server running on port 3000 Mint Duration: 20.18 seconds Mint Duration: 11.937 seconds</pre>
Certificate verification	Less than 1.2seconds
	

However, speed alone is insufficient without reliability. To verify system correctness, a suite of unit tests was developed using Hardhat, Mocha, and Chai frameworks. These tests achieved over 95% code coverage, ensuring that all core smart contract functions, including minting authority, metadata assignment, and transfer prevention, behaved as expected. For

instance, attempts to transfer a certificate token from one address to another were correctly rejected by the contract, thereby validating the soulbound logic embedded within the override. The system was compared to some related papers, some of which relied on a private blockchain infrastructure. NFTcate demonstrated the following advantages.

Table 3: Comparative Analysis with Related Systems

Related work	1	2	3	4	5	6
NFTcate	✓	✓	✓	✓	✓	✓
NFTcert (Zhao & Si)	✓	✓	✗	✗	✗	✗
Ifeyemi et al. (2024)	✓	✓	✓	✗	✗	✗
de Souza-Daw et al. (2023)	✓	✓	✓	✗	✗	✗
Nielson (2023)	✓	✓	✓	✓	✗	✗
Akowe (2023)	✓	✓	✓	✗	✗	✓

Keys – 1: Supports both academic and non-academic certificates, 2: Only accredited institutions can issue certificates, 3: Certificates are verifiable on a public blockchain, 4: Uses soulbound NFTs for stronger ownership protection, 5: Designed with UX for non-technical users, 6: Includes a robust admin dashboard for institutions, ✓: considered, ✗: not considered.

CONCLUSION

This paper presents NFTcate, a decentralized system designed to combat certificate fraud in Nigerian universities. The system uses blockchain's immutability and transparency alongside non-transferable soulbound tokens (SBTs) to provide a secure and publicly verifiable alternative to traditional, centralized methods.

NFTcate enables authorized institutions to generate cryptographically secured certificates on the Ethereum blockchain, storing metadata on IPFS. Through distinct token IDs, this makes it simple for students and verifiers to obtain certificate information. Additionally, the system is very user-friendly, abstracting complicated blockchain procedures into an intuitive web interface that eliminates the need for wallet expertise or cryptocurrency transactions. The NFTcate's adaptable design goes beyond academia; in the future, it can support a blockchain-powered credentialing ecosystem by protecting digital identities, job checks, health information, and professional licenses. To improve accessibility, particularly in places with poor internet, future upgrades will incorporate offline verification through QR codes and Progressive Web Apps (PWAs). Additionally, its fundamental design exhibits potential for voter IDs and health data, underscoring its wide range of applications and beneficial social effects.

This research focused on getting a proof-of-concept while showing cost efficiency, speed, and universality. However, more elaborate testing within actual scenarios is planned for future work, including looking into user and educational body surveys to compile a standardized format for student and certificate data for maximum uniformity while engaging willing Nigerian universities for real-life testing. Authors intend to evaluate the usability of the NFTcate system among students, verifiers, and institutions to determine its performance.

ACKNOWLEDGEMENT

The authors wish to acknowledge the support of National Open University of Nigeria Under grant Number: NOUN/SG25/FACOM/004 and all those whose efforts, suggestions and encouragements have contributed to the successful completion of this research.

REFERENCES

Aini, Q., Harahap, E. P., Santoso, N. P., Sari, S. N., & Sunarya, P. A. (2023). Blockchain based certificate verification system management. *Aptisi Transactions on Management*, 7(3), 1–0. <https://doi.org/10.34306/atm.v7i3>

Akowe, E. B. (2023). Commercial deployment of blockchain-based certificate verification in Nigeria (Industry Report).

Barone, C., & Herbaut, E. (2024). Decision-making mechanisms, information and educational inequalities. In

Research handbook on intergenerational inequality (pp. 387–399). Edward Elgar Publishing.

de Souza-Daw, T., & Ross, R. (2023). Fraud in higher education: A system for detection and prevention. *Journal of Engineering, Design and Technology*, 21(3), 637–654. <https://doi.org/10.1108/JEDT-01-2022-0051>

Delgado-von-Eitzen, C., Anido-Rifón, L., & Fernández-Iglesias, M. J. (2024). NFTs for the issuance and validation of academic information that comply with the GDPR. *Applied Sciences*, 14(2), Article 706. <https://doi.org/10.3390/app14020706>

Effiong, M., Norta, A., Udokwu, C., & Hattingh, M. (2022). Adoption of blockchain technology in academic certificate-verification systems. In 2022 IEEE 1st Global Emerging

Technology Blockchain Forum: Blockchain & Beyond (iGETBlockchain) (pp. 1–6). IEEE. <https://ieeexplore.ieee.org/document/10087108>

Emeka, A. G. (2024). Verification and processing of academic certificates using web services. *PERSPEKTIF*, 13(1), 311–318.

Essien, U. E. (2024). Using QR code and a smartphone to provide University of Cross River State (UNICROSS) certificate authentication. *Information Technology*, 7(2), 35–42.

Goswami, K., Vaithyanathan, D., Verma, P., & Kaur, B. (2024). Document verification using blockchain. In 2024 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE) (pp. 1–7). IEEE.

Ifeyemi, T. A., Oyediji, O. S., & Adebisi, M. O. (2024). A prototype for Celo-based certificate issuance and verification in Nigeria. *Nigerian Journal of Computer Science*, 11(2), 45–60.

Jha, S., Modak, A., Pise, R., & Patil, S. (2023). Certifier DAPP-decentralized and secured certification system using blockchain. In 2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) (pp. 1–6). IEEE. <https://doi.org/10.1109/icbds58040.2023.10346509>

Ji, Z., Zhang, J., Guan, S., & Man, K. L. (2024). Intellectual property data trading through NFTization. In 2024 2nd International Conference on Big Data and Privacy Computing (BDPC) (pp. 179–185). IEEE.

- Kandwal, N., Agarwal, K. L., & Upadhyay, D. (2025). Universal System for Higher Accreditations (USHA): Novel blockchain-based educational transcripts issuance and verification architecture. In 2025 2nd International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 336–343). IEEE.
- Ma, K., Huang, J., He, N., Wang, Z., & Wang, H. (2025). SoK: On the security of non-fungible tokens. *Blockchain: Research and Applications*, Article 100268.
- Motuz, T., Dynovych, A., Babelchuk, O., Bykasova, S., & Gulevets, D. (2024). Examination of methods for assessing educational quality, the role of standardisation, and mechanisms for enhancing educational programme efficiency. *Multidisciplinary Reviews*, 7, Article 2024spe011. <https://doi.org/10.31893/multirev.2024spe011>
- Naik, G. R., & Naik, P. G. (2024). Role of non-fungible tokens in transforming academic credentials for trust and transparency. In 2024 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 1–9). IEEE.
- Nielson, L. M. (2023). Educational tokenization via soulbound tokens: A theoretical approach to non-transferable academic credentials. *Journal of Digital Education*, 2(1), 12–25.
- Nwaocha, V. O., & Oloyede, A. (2022). Towards the development of an enhanced certificate verification system for West African institutions. *Advances in Multidisciplinary and Scientific Research Journal*, 8(3), 79–85.
- Ohlhaber, P., Weyl, E. G., & Buterin, V. (2022). Decentralized society: Finding web3's soul. SSRN. <https://ssrn.com/abstract=4105763>
- Ruan, Z., Ye, W., Xie, Y., Li, H., Zhang, C., & Wei, L. (2023). Private status retrieval for blockchain-based certificate revocation system. In ICC 2023 - IEEE International Conference on Communications (pp. 6565–6570). IEEE. <https://doi.org/10.1109/icc45041.2023.10278733>
- Utsahawattanasuk, P., Mahapakulchai, S., & Jariyanorawiss, T. (2024). NFT-based verification of academic credentials: Case study for GSPP certificate, Graduate School, Kasetsart University. In 2024 International Technical Conference on Circuits/Systems, Computers, and Communications (ITC-CSCC) (pp. 1–5). IEEE. <https://doi.org/10.1109/ITC-CSCC62296.2024.10628144>
- Zile, K., & Strazdina, R. (2018). Blockchain use cases and their feasibility. *Applied Computer Systems*, 23(1), 12–20. <https://doi.org/10.2478/acss-2018-0002>

