University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR)

ISSN: 2714-3627

A Journal of the Faculty of Computing, University of Ibadan, Ibadan, Nigeria

Volume 16 No. 1, January 2026

journals.ui.edu.ng/uijslictr
http://uijslictr.org.ng/
uijslictr@gmail.com

University of Ibadan
Journal of Science and Logics in ICT Research

A Smart Contract–Enabled Private Ethereum Blockchain for Secure Academic Transcript Verification

[1]✉Odeniyi, O. A., [2]Ogbonna, P.A, [3]Akinyede, A.I., [4]Iwasokun, G.B., and [5]Akinyede, R.O.

[1]Odeniyi, O. A., [2]Ogbonna, Precious Agba, [3]Akinyede, Adedamola I., [4]Iwasokun, Gabriel B., and [5]Akinyede, Raphael. O.
[1]Department of Cyber Security, The Federal University of Technology, Akure, Nigeria.
[2]Department of Mathematics & Computer Science, Michael & Cecilia Ibru University, Agbarha-Otor, Nigeria
[3]Department of Food Science & Technology, The Federal University of Technology, Akure, Nigeria.
[4]Department of Software Engineering, The Federal University of Technology, Akure, Nigeria.
[5]Department of Information Systems, The Federal University of Technology, Akure, Nigeria.

Emails of authors:
oaodeniyi@futa.edu.ng; aiakinyede@futa.edu.ng; gbiwasokun@futa.edu.ng; roakinyede@futa.edu.ng

Abstract
Forgery and delayed validation of transcripts by Nigerian universities had necessitated the development of reliable systems. Inadequacies in manual, centralized approaches had been characterized by inefficiencies, high chances of corruption, and forgery of academic documents. In this paper, an Ethereum blockchain solution for the Management of Computerized Instructional Universities (MCIU) was presented to guarantee authenticity, reliability, and confidentiality of student transcripts. This proposed solution incorporated Solidity smart contracts on a private Ethereum network for handling transactions related to the issuance, reissuance, and validation of transcripts where transcript files were stored on the decentralized file storage (Swarm), while only hashes of the transcript files were recorded on the blockchain. React and Node.js technologies were employed in designing both client and server sides of the system. Authorized personnel were able to issue digital verifiable transcripts, and third parties were able to validate issued transcripts within seconds through a secure coding process.

Keywords: Blockchain, Ethereum, Smart Contracts, Academic Transcript Verification, Decentralized Storage, Solidity, Cryptographic Hashing, Nigeria

1.Introduction

Manual and centralized methods of academic transcript verification in Nigerian tertiary institutions are currently used and pose problems like inefficiency and susceptibility to forgery. These factors lead to inefficiencies on behalf of the graduates and even employers, making academic transcripts less credible (Oladejo *et al*, 2024). With advances in forgery technology, there is an urgent need to modernize verification processes (Rahman *et al*, 2023). In this case, blockchain technology, particularly that of private Ethereum networks, can serve as a better alternative due to its feature of having an immutable ledger, in which any entered data is impossible to alter or delete. This increases the effectiveness of the verification process (Kaneriya and Patel, 2023). Studies show that blockchain systems reduce fraud and enable faster, real-time verification through decentralized authentication (Meyliana et al., 2020; Oluwaseyi, 2024). Globally, universities are adopting Ethereum smart contracts combined with decentralized storage solutions like IPFS and Swarm to improve security, scalability, and transparency (Chaniago et al., 2021; Gondhalekar et al., 2021). At present, the manual approach employed by MCIU to verify transcripts is both ineffective and time-consuming owing to the issues associated with delay, workload, and possible file losses and tampering with the records. The verification process can take several weeks or even months to be completed, and the use of the centralized approach exposes the process to being hacked since there will only be one point of access

Odeniyi, O. A., Ogbonna, P.A, Akinyede, A.I., Iwasokun, G.B., and Akinyede, R.O. 2026). A Smart Contract–Enabled Private Ethereum Blockchain for Secure Academic Transcript Verification. *University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR),* Vol. 5 No. 1, pp. 170 – 179

(Kaneriya and Patel, 2023). Implementation of a private blockchain system is effective due to data integrity, quickness, and privacy in the form of cryptographic hashing, without uploading transcript information. Therefore, this study proposes the development of a private transcript verification system using Ethereum.

2. Literature Review

Blockchain technology marks the beginning of a new era whereby data management will be conducted using a decentralized approach towards keeping records. Blockchain technology entails a network architecture composed of blocks of transaction data which have been encrypted using cryptographic methods. Introduced in the Bitcoin Paper by Satoshi Nakamoto in 2008, blockchain technology is well known for its reliability, transparency, and security. As a result, the technology is highly accepted in academic circles, industries, and governments worldwide (Ferdous et al., 2020). Another important characteristic of blockchain technology is immutability since once data is recorded, none is able to alter it.

Based on the above discussion, some important characteristics of blockchain technology are decentralization, distributed ledger, transparency, hashing, consensus, and immutability (Lin & Liao, 2017). Due to its uniqueness in characteristics, blockchain technology can be used in managing information where confidentiality is paramount, for example, verifying academic records. There are three basic forms of blockchain technology namely, public, consortium, and private. Private blockchain technology is better than others due to enhanced security and confidentiality.

One of the developments in blockchain technology includes the creation of smart contracts that allow for processes to be automatically executed without requiring third parties. According to Buterin (2014), Ethereum uses this technique extensively, and in it, institutional policies are encoded. In transcript management, they aid the issuance, verification, and cancellation of academic records in a transparent way (Christidis & Devetsikiotis, 2016). For securing data in this case, encryption methods such as SHA-256 will be used, but for storing large files like transcripts, off-chain storage networks like InterPlanetary File System and Swarm will be adopted since only the hashes of large documents will be kept on the blockchain (Benet, 2014; Wood, 2016).

Blockchain-based systems can also benefit from the relevant theories. Decentralization Theory by Don Tapscott and Alex Tapscott (Tapscott & Tapscott, 2016) highlights the importance of transitioning from centralized trust mechanisms to decentralized ones. On the other hand, the Technology Acceptance Model put forward by Fred Davis (1989) sheds light on how technology is accepted based on two important factors, namely, usefulness and ease of use. Moreover, Information Theory presented by Claude Shannon (1948) supports cryptography-based data integrity and security measures.

In the Nigerian context, the process of managing and verifying academic transcripts would be characterized by the use of centralized, manual, and paper-based systems that are inefficient and susceptible to fraud, corruption, and forgery. Consequently, it is necessary that the management of these transcripts is efficient, automated, and secure.

Additionally, some Nigerian researchers have proposed certain insights into the application of blockchain technology for managing academic transcripts. For example, in Akuma et al.'s study in 2024, one of the methods for verifying academic transcripts through blockchain is by establishing decentralized storage and automatic hashing of data to reduce fraud (Akuma et al., 2024). According to these scholars, manual transcript verification has been characterized by questions regarding the validity of transcripts due to inefficiencies and lack of transparency.

Moreover, another Nigerian study conducted at the Dominican University, Ibadan examined the potentialities of creating a blockchain-based certificate verification system. According to Ogunleye et al. in 2023, this system can authenticate certificates in under two seconds, with the ability to identify any form of forgery (Ogunleye et al., 2023).

Moreover, another experiment carried out by Ifeyimi et al., (2024) involved the creation of the Blockchain Certificate Verification System (BCVS) using the Celo blockchain technology.

According to their findings, further usage of paper certificates would enhance the chances of tampering with academic credentials, which may lead to certificate duplication. The BCVS had the hashes of the certificates stored on it, hence making sure that they were tamper-proof.

However, as noted during research in this field, a number of impediments to blockchain adoption were identified by different authors, including those relating to privacy, scalability, and organizational readiness (Badhe et al., 2020; Gondhalekar et al., 2021). These obstacles may even be amplified due to infrastructure challenges in Nigeria, as well as organizational opposition to novel technologies.

Therefore, given the outlined limitations, the present paper focuses on creating a smart contract-based private blockchain using the Ethereum platform. This blockchain will be designed to improve the efficiency of academic transcript validation.

3. Methodology

3.1 System Architecture Design

The architecture of the proposed system consists of the deployment of a single permissioned Ethereum blockchain for the issuance and validation of transcripts for MCIU students. This differs from both public and semi-public architectures in being entirely permissioned, meaning that nodes in the network will be under university control. This architecture will enhance privacy, cut down cost, and provide greater control without undermining blockchain security.

Figure 1 is the design of a Multi-layer Blockchain Architecture used for verifying transcripts. This model uses a bottom-up approach and comprises front-end interfaces and decentralized storage along with infrastructural base.

1. User Interface (UI) Layer

At the highest level, there are three separate entry points to the system:

- Admin Portal – for university management of record keeping and issuance of transcripts.
- Student Portal – for students to access their own records and create share links/QR codes.
- Verifier Portal – for external parties to verify documents.

2. Microservices & Backend Layer

It is referred to as the "Brain" of the entire system as it consists of the logic and communication part:

- Auth & Notification Services: These microservices perform the user authentication (auth logic) and notifications (notification logic) automatically.
- API Gateway (Node.js): The main microservice performs routing from the ports of the UI to the corresponding services of the backend layer as well as the blockchain.

3. Security Layer

Incorporated in the backend layer, it helps secure the data present in the backend layer:

- Access Control: Consists of WAF, IDP, and multi-factor authentication.
- Intrusion Detection Systems (IDPS): It monitors the activity of any malicious attacks.
- Key Management Service (KMS): This helps the users access their private keys safely for transactions on the blockchain.

4. Blockchain & Storage Layer

"The Source of Truth"

- Blockchain Layer (Ethereum): It has the smart contract. Rather than storing the complete document in the blockchain as it would incur high costs, only its cryptographic hash gets stored in the blockchain.
- Storage Layer (IPFS): The recordings will be saved on IPFS, and their security will be guaranteed by the security layer.

5. Layer of Infrastructures

The base layer is present in the bottom most a part that provides both physical and virtual features required for the operation of the system:

- Computing: Virtual machines (EC2), Docker Containers (Kubernetes) for executing the software.
- Networking: Load balancing for handling the traffic and VPC.
- Environment of Cloud: Working together with the cloud service providers for scaling (Auto-scaling) and database management services.

3.2 System Analysis

System analysis entails the evaluation of the current system used to verify transcripts at MCIU, identification of its shortcomings, and the proposal of an alternative blockchain system that would help solve such problems. The main drawbacks associated with the manual verification system include susceptibility to fraud, use of only one centralized database, long verification periods, heavy administrative workload, lack of transparency, and limited access for third-party verifiers – see figure 2.

To mitigate the problems discussed above, a private Ethereum blockchain verification process is proposed. The system utilizes a permissioned network run by the MCIU, the use of smart contracts for automated issuing and verifying transcripts, and off-chain data storage (IPFS/Swarm) using on-chain hashes. Figure 3 indicates three roles of users, namely administrators, students, and verifiers, which allows for fast, secure, and decentralized transcript verification not relying on the university itself.

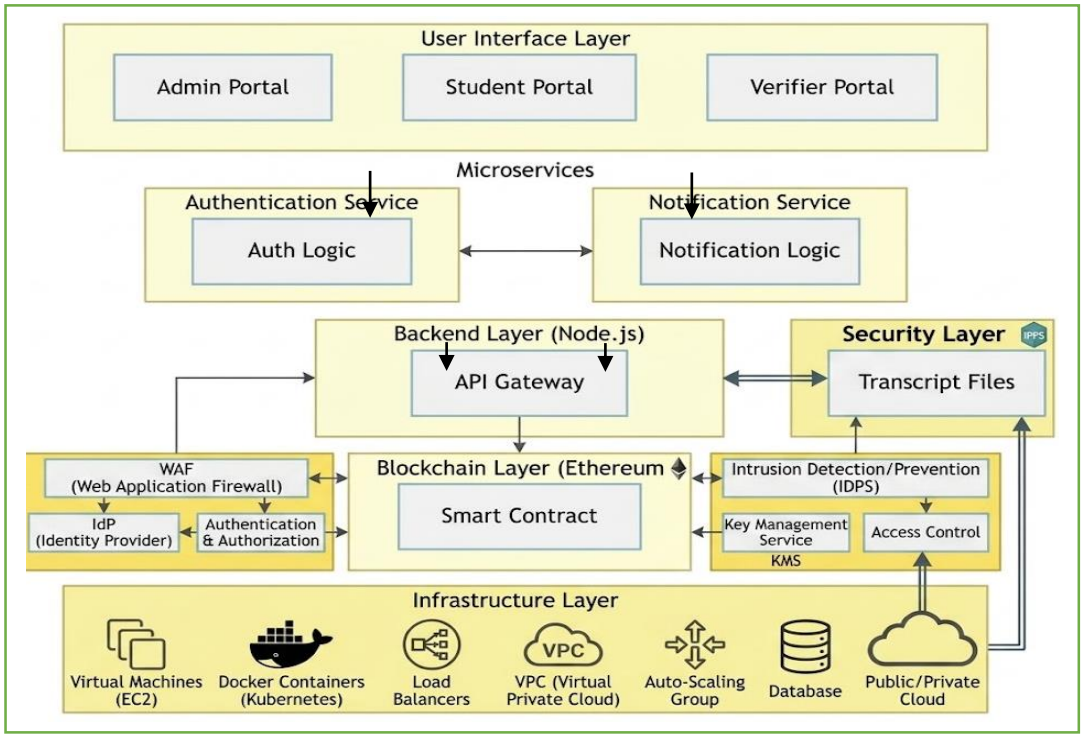

Figure 1: Multi-layered Blockchain Architecture

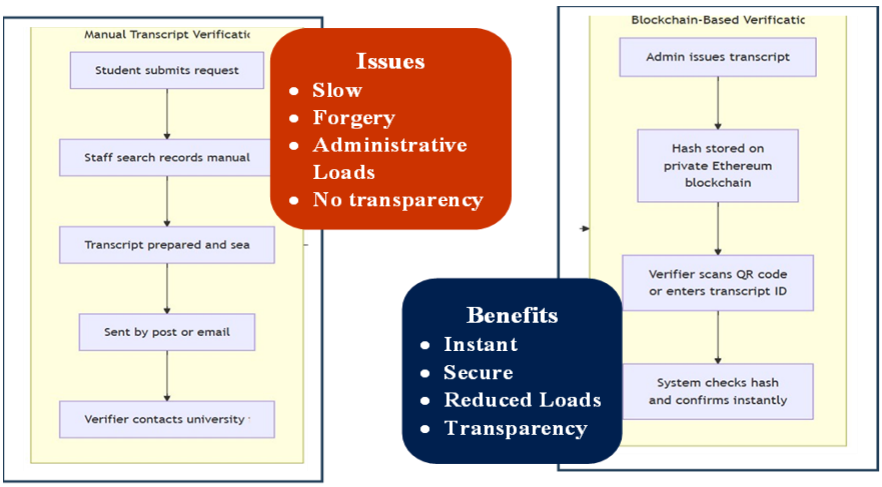

Figure 2: Comparison between a manual system and a blockchain system

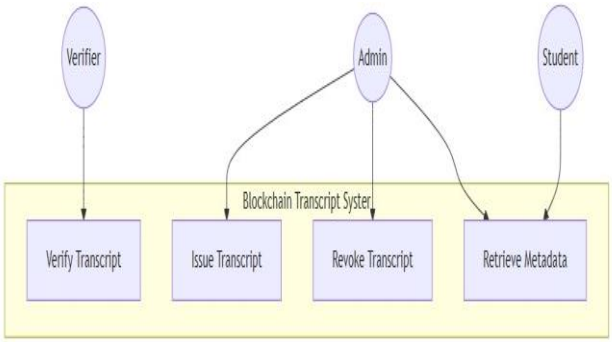

Figure 3: Roles interacting with system.

3.3 System Design

The system is organized into four modules. The Blockchain Module manages transcript issuance, verification, and revocation through smart contracts. The Storage Module handles file storage on IPFS or Swarm, generating content identifiers linked to blockchain hashes. The Backend Module, built with Node.js and Express, provides APIs for blockchain interaction and user management. The Frontend Module, developed with React.js, offers interfaces for administrators and verifiers, including QR code generation and verification dashboards.

As shown in figure 4, the workflow begins when an administrator uploads a transcript, generating a hash and CID. The hash is stored on the blockchain while the file is stored off-chain. Verifiers then submit a transcript ID or QR code, and the system compares the computed hash with the stored value to confirm authenticity within seconds.

3.4 Smart Contract Design and Logic

The smart contract handles the processes of issuing, verifying, and revoking transcripts. Functions include *issueTranscript()*, which stores the transcript hash and metadata, *verifyTranscript()*, which verifies authenticity, *revokeTranscript()*,which voids the records, and *getTranscriptDetails()*, which provides administrative privileges. A transcript is modeled as an object that includes the hash, program, year of graduation, and validity of the record. The records are mapped for efficient access. Access control ensures that only authorized administrators have the capability of creating and deleting the transcripts. Verification entails local hashing of the transcript against the hash stored on the blockchain. Matching and logging are key elements of the verification process; failure to which the transcript cannot be valid. The security features include tamper-proof blockchain transaction, auditability, exclusive access to the private network, and legitimate input. Off-chain transactions are conducted using IPFS or Swarm technology.

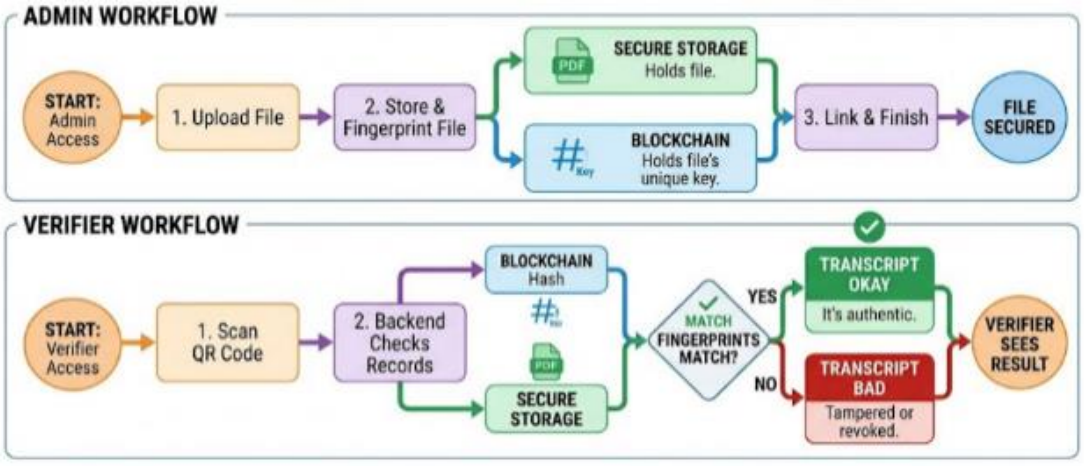

Figure 4: Blockchain-based transcript issuance & verification system flowchart

4. IMPLEMENTATION AND DISCUSSION

4.1 System Setup and Configuration

This application has been constructed on a private blockchain Ethereum (Ganache) for rapid, free tests. These technologies include Solidity, Remix, Truffle, Node.js (Express), React.js, Web3.js/ Ethers.js, and Swarm (Dockerized) for storing files decentralized, designed in Visual Studio Code. Swarm performed all operations of files storage where all transcripts were assigned unique identifiers (CIDs). The backend offers API's for issue and verification, as well as email services of transcript and keys sending to students.

4.2 Smart Contract Deployment

As shown in figures 5 and 6, the smart contract had functionalities of issuing, verifying, revoking and obtaining of transcript data in hash format. Smart contract development was done in Remix, after which it was deployed into Ganache via Truffle.

MetaMask enabled transaction signing, and deployment included institution-specific details. All tests passed, confirming correct functionality.

4.3 Certificate Upload and Verification Workflow

Upload Process: Metadata and file uploaded by administrator → file stored in Swarm → hash generated → hash uploaded to blockchain → certificate sent to students by post.

Verification Process: Data and access key provided by user → hash generated by system → comparison made on blockchain → file retrieved → verification result shown.

Time required to verify certificate reduced from weeks to seconds.

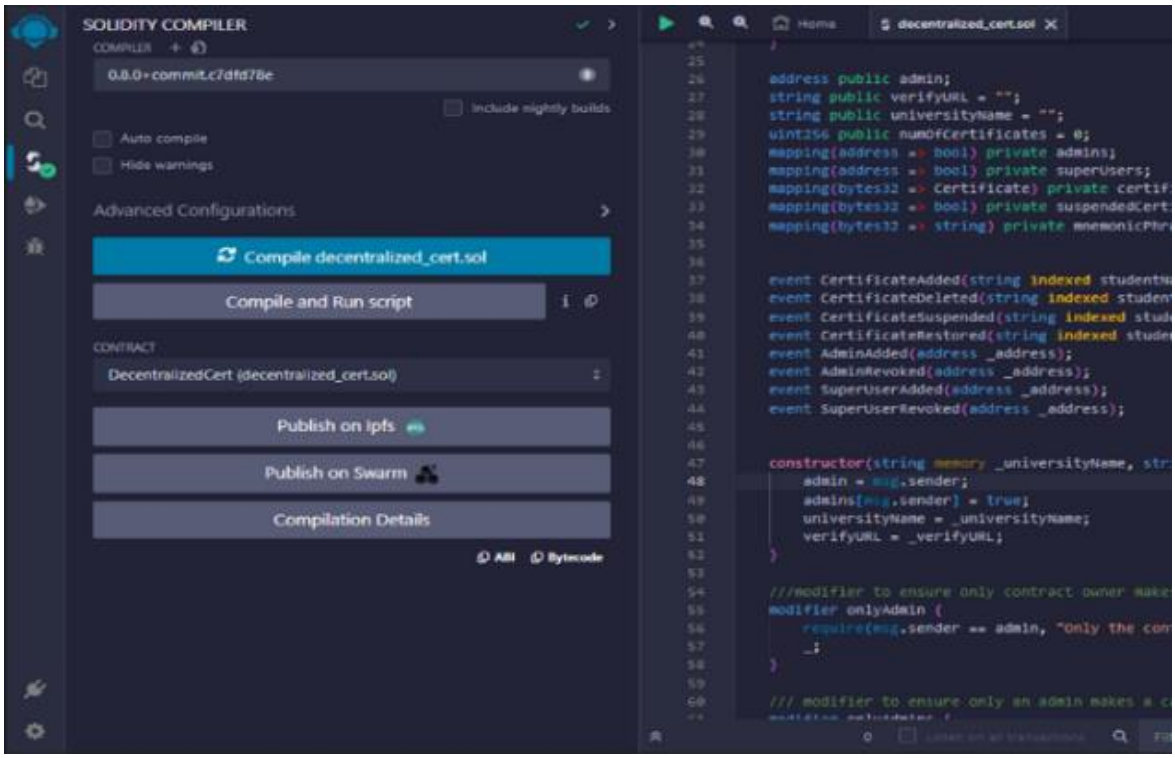

Figure 5: Compiling the smart contract

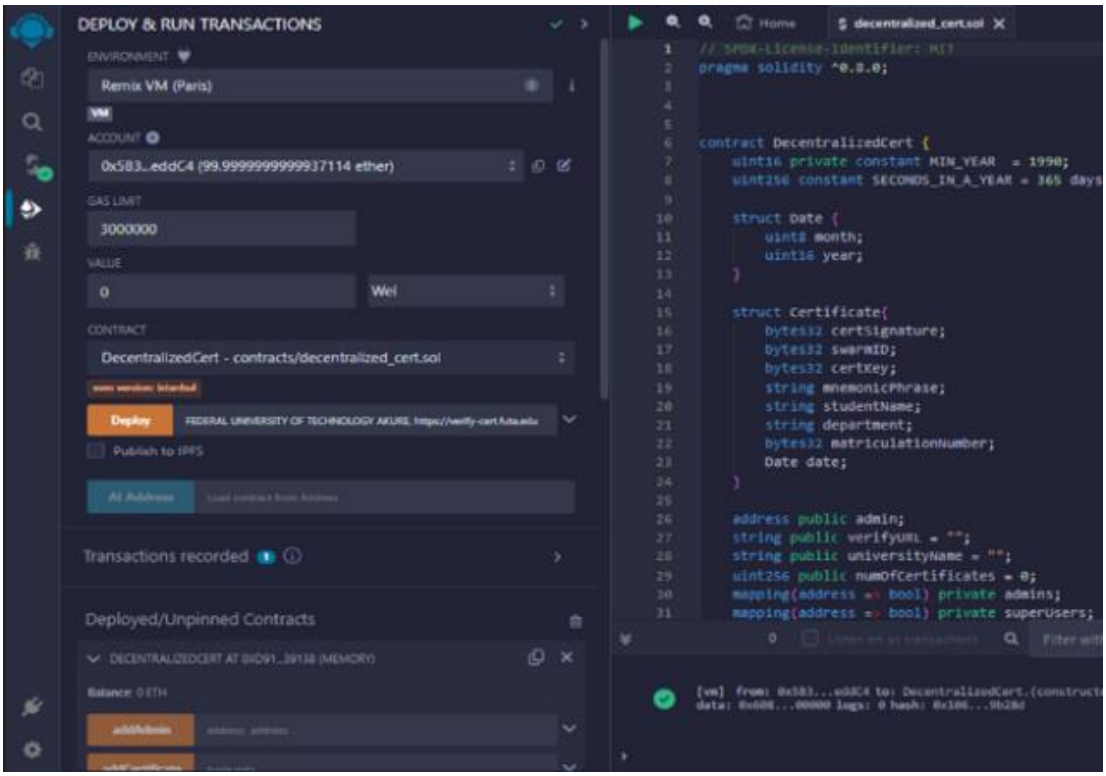

Figure 6: Deploying the smart contract with initial parameters

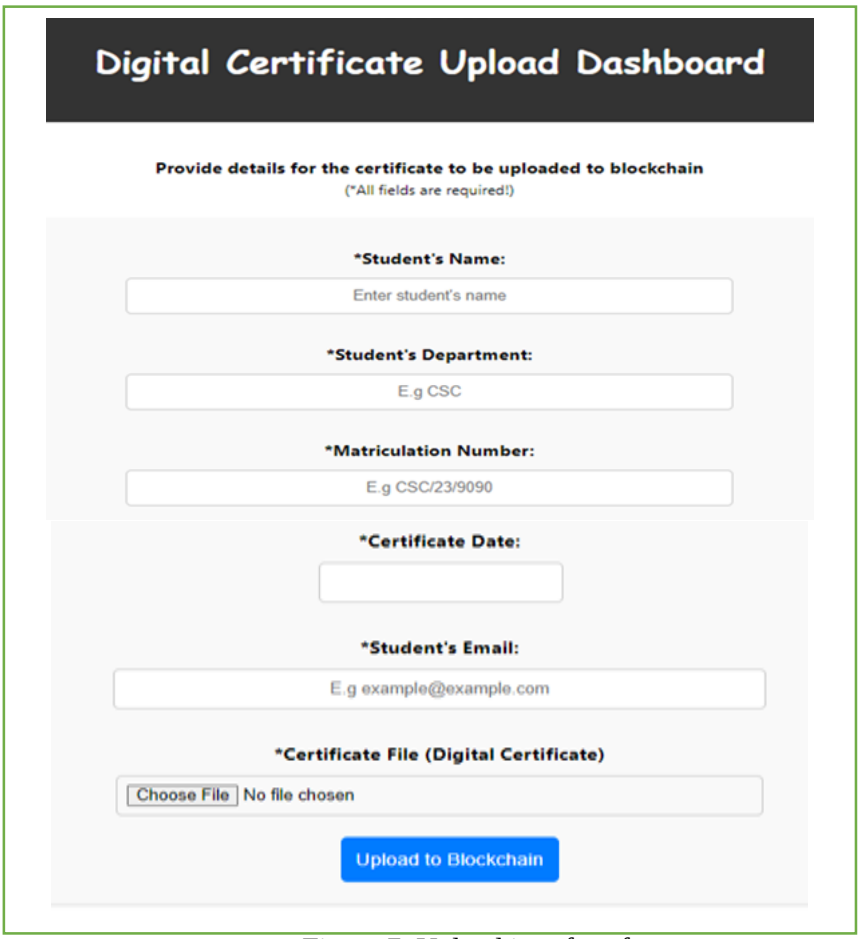

Figure 7: Upload interface form

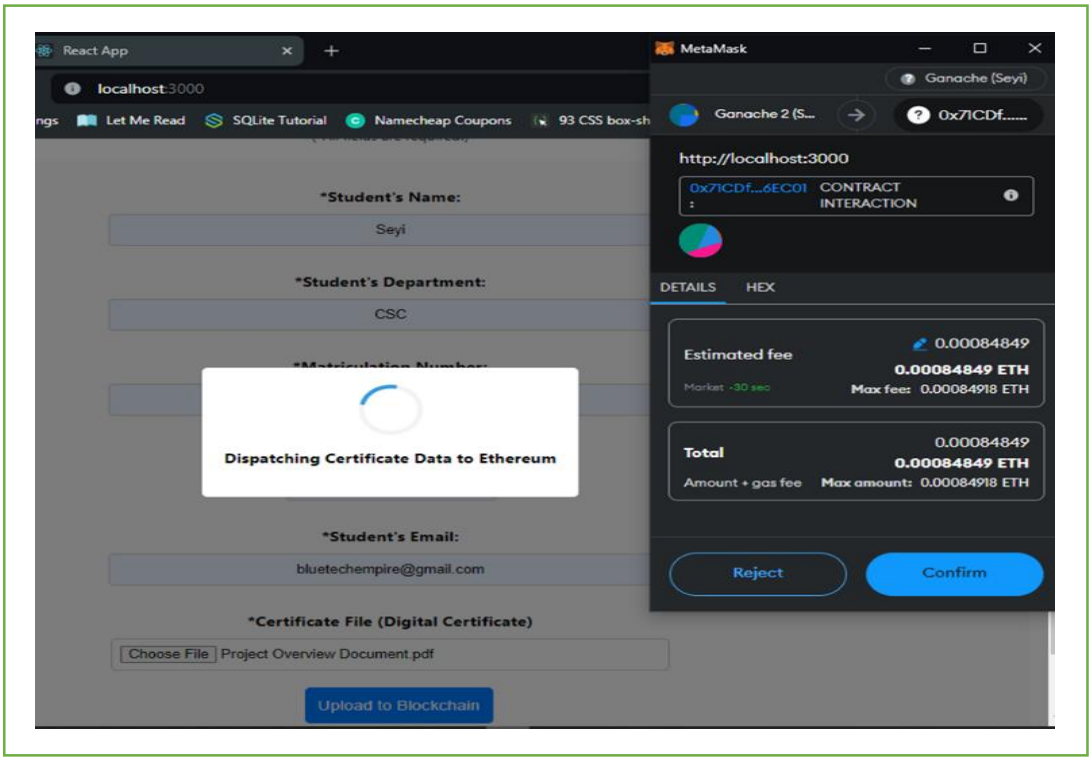

Figure 8: Certificate Upload and Blockchain Transaction Confirmation Process

Figures 7 and 8 illustrate the upload process, where the certificate metadata and digital file have been submitted through the browser and the metadata is being sent to the Ethereum blockchain. The administrator is required to confirm the transaction, as a small amount of ETH is used as a gas fee. This verification process is made possible through MetaMask, which serves as the interface between the browser and the Ethereum blockchain network.

4.4 Performance Evaluation and Feedback from Users

Performance tests conducted on 30 users were met with high satisfaction rates, as follows:

- Efficiency rate of 92%
- Reliability rate of 95%

The system was efficient, secure, and provided transparency.

However, minor issues arose concerning the user interface design and user guidance.

Compared to the manual process, the system provides no delay, human error, and security threats. The system's high performance was guaranteed through the blockchain attributes of immutability, access control, off-chain data storage, and audit trails -see figure 9.

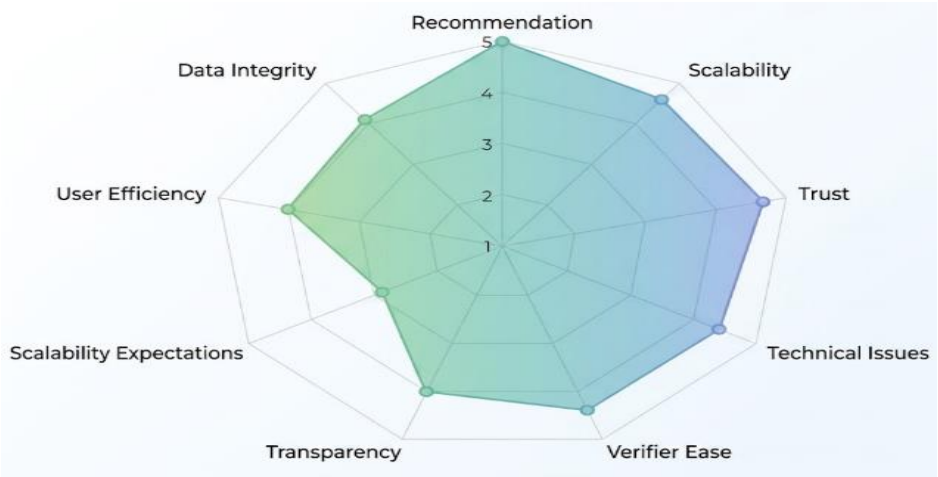

Figure 9: System Performance RADAR Chart

Figure 9 ("spider diagram") enables a comprehensive overview of the entire performance of the system. While the conventional bar graph focuses more on quantification of variables, here, one can see the balance of the different objectives of this particular project; security, speed, and the user's level of satisfaction with the system.

Insights from the Diagram's Structure

- Performance Peak (the Outliers): The values of recommendation (5.0) and transparency (~4.9) reach the furthest end of the web structure. Therefore, it can be concluded that the probability of recommending the use of this system by its users is very high. Thus, it is true that the "open ledger" concept of the blockchain has worked well in generating a level of trust within an institution.
- Scalability Trade-off: It can be seen that there seems to be an "incline" on the Scalability Expectation (at around 3). From the context of the blockchain system, such a term refers to the "Blockchain Trilemma," whereby increasing the security and decentralization may decrease the transaction speed per second compared to a normal database.
- The Advantages of the System (the "Strong Side"): The plot places emphasis on the top and right portions of the graph, implying that Security Enhancement, Verification Process, and Technical Stability constitute the advantages of the system.

5. CONCLUSION

The current work introduced an individualized Ethereum framework for efficient and safe verification of transcripts in MCIU that will help to address problems such as fraud, delay, and inefficiencies associated with traditional verification procedures. From the results, it was clear that the duration required for verifying transcripts was reduced from several days or even weeks to less than five minutes; there was no possibility of fraud, and user satisfaction was relatively high (92%-95%). Hash verification provides quick and reliable validation without the need for any manual intervention, while mnemonic codes aid in protecting users' data privacy.

This research paper introduces another powerful blockchain solution that can be easily scaled up in Nigerian universities through smart contracts and ensuring user data privacy. It is recommended that the implementation of the proposed system should follow a phased approach and future studies concentrate on privacy protection measures such as zero-knowledge proofs.

6. DECLARATION

This research was sponsored by the Tertiary Education Trust Fund (TETFund) Institution-Based Research (IBR) through the Centre for Research and Development (CERAD) at the Federal University of Technology, Akure, Nigeria.

7. ACKNOWLEDGEMENT

We sincerely appreciate the Federal Government of Nigeria for funding this research through TETFund IBR. Our gratitude also goes to the management of the Federal University of Technology, Akure, for their support through CERAD.

8. REFERENCES

Akuma, C., Okeke, P., & Ibrahim, S. (2024). A blockchain framework for transcript verification in Nigerian universities. International Journal of Digital Management, 12(2), 45–58.

Badhe, V., Nhavale, P., Todkar, S., Shinde, P. and Kolhar, K., (2020). Digital certificate system for verification of educational certificates using blockchain. International Journal of Scientific Research in Science and Technology, 7(5), pp.45-50.

Benet, J. (2014). IPFS: Content-addressed, versioned, peer-to-peer file system. arXiv. https://arxiv.org/abs/1407.3561

Buterin, V. (2014). Ethereum: A next-generation smart contract and decentralized application platform. https://ethereum.org/en/whitepaper/

Chaniago, N., Sukarno, P. and Wardana, A. A., (2021). Electronic document authenticity verification of diploma and transcript using smart contract on Ethereum blockchain. Register: Jurnal Ilmiah Teknologi Sistem Informasi, 7(2), pp.149-163.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Claude Shannon (1948). *A mathematical theory of communication*. Bell System Technical Journal, 27(3), 379–423; 27(4), 623–656.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

Don Tapscott & Alex Tapscott (2016). *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world*. New York, NY: Portfolio/Penguin.

Ferdous, M. S., Chowdhury, M. J. M., & Hoque, M. A. (2020). Blockchain and its applications in education: A systematic review. IEEE Access, 8, 150103–150121. https://doi.org/10.1109/ACCESS.2020.3017042

Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A. and Colman, A., (2020). Blockchain consensus algorithms: A survey. arXiv preprint, arXiv:2001.07091.

Fred Davis (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

Gondhalekar, M., Kadam, S., & Patil, P. (2021). Blockchain for secure transaction systems: A review. International Journal of Computer Applications, 174(25), 1–6.

Ifeyemi, T., Oyedeji, A., & Adebiyi, F. (2024). A Blockchain-Based Digital educational certificate verification system. ITEGAM-JETIA, 10(49), 35-41. https://doi.org/10.5935/jetia.v10i49.1145

Kaneriya, J. and Patel, H., (2023). Blockchain-based academic credential verification system. Journal of Computer Science and Technology, 23(4), pp.45-56.

Lin, I. C. and Liao, T. C., (2017). A survey of blockchain security issues and challenges. International Journal of Network Security, 19(5), pp.653-659.

Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. International Journal of Network Security, 19(5), 653–659.

Meyliana, Hidayanto, A. N. and Budiardjo, E. K., (2020). Blockchain for academic credential verification: Challenges and opportunities. Journal of Theoretical and Applied Information Technology, 98(15), pp.2987-2998.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

Oladoja, I. P., Adeyemo, A. B. and Oluwaseyi, O. A., (2024). Blockchain-driven solutions for academic transcript management in Nigerian universities. African Journal of Computing and ICT, 17(1), pp.23-34.

Oluwaseyi (2024). *Decentralized verification systems using blockchain*. [Details such as journal/publisher not specified].

Rahman, T. M., Mouno, S. I., Raatul, A. M., Al Azad, A. K. and Mansoor, N., (2023). VerifiChain: A credentials verifier using blockchain and IPFS. International Conference on Information, Communication and Computing Technology, Singapore. Springer Nature, pp.361-371.

Shannon, C. E. (1948). A mathematical theory of communication. Bell System Technical Journal, 27(3), 379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. Penguin Random House.

Vitalik Buterin (2014). *A next-generation smart contract and decentralized application platform*. Retrieved from https://ethereum.org/en/whitepaper/

Wood, G. (2016). Ethereum: A secure decentralized generalized transaction ledger (Ethereum Yellow Paper). https://ethereum.github.io/yellowpaper/paper.pdf

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352–375. https://doi.org/10.1504/IJWGS.2018.095647