BIU Journal of Basic and Applied Sciences 10(1): 42 – 55, 2025.

ISSN: 2563-6424

ACADEMIC CERTIFICATE VERIFICATION FRAMEWORK USING BLOCKCHAIN TECHNOLOGY

ONOSHIOZE, O. E., *AHUBELE, B. O. AND OBAHIAGBON, K. O.
Department of Computer Science, Faculty of Science, Benson Idahosa University, Benin City, Edo State, Nigeria
*Corresponding author: bahubele@biu.edu.ng

ABSTRACT
Academic certificate fraud has become a growing concern, with counterfeit degrees and diplomas undermining the credibility of educational institutions and causing significant financial and reputational damage. Traditional methods of certificate verification, which rely on centralized databases, are often vulnerable to tampering and forgery. This project presents a blockchain-based academic certificate verification system that leverages the decentralized, secure, and transparent nature of blockchain technology. The system of verifying academic certificates in this project is built on blockchain technology, utilizing decentralization, security, and transparency to address the possible challenges entailed by the management of academic credentials' integrity and authenticity. It is an innovative system providing a great option by using this decentralized platform. Smart contracts based around student credentials management include certificate issuance and revocation through Ethereum and Solidity. Using blockchain technology to tokenize degrees and diplomas as non-fungible tokens (NFTs), it leverages the immutability and distributed nature of blockchain in creating such a record that cannot be altered for academic certificates, thus making any educational institution, employer, or individual assured about the authenticity of qualifications. The links for verification of certificates are on the blockchain explorer as another measure of authenticity, trust, and credibility. A user-friendly decentralized application (DApp) was built for the administrators to mint certificates and provide the means of downloading the certificate data as Excel files for easy management and record keeping. This innovative approach enhances the integrity, transparency, and efficiency of the processes of academic credential verification, addressing the shortcomings of traditional systems.

KEYWORDS: *Certificate verification, Non-fungible Tokens (NFTs), Ethereum, Blockchain Technology, Smart contracts, Decentralized Application (DApp), Certificate forgery*

INTRODUCTION
Education is essential for everyone. During their studies, students earn various certificates. The certificates issued by educational institutions are important documents for graduates, as they prove qualifications and can be used globally (Suganthalakshmi *et al*., 2022). With their certificates, graduates can apply for jobs in public or private sectors, where

certificates are to be manually verified. However, the presence of advanced and cheap scanning and printing technologies has made it easier to forge certificates, threatening the credibility of both the certificate holder and the institution that has issued the certificate (Warasart and Kuacharoen, 2012). To this effect, identifying fake certificates presented by students is often challenging.

Generally, most institutions or schools rely on traditional paper-based methods to verify and authenticate documents presented or claimed to be issued by them (Umaru and Nzadon, 2021). These methods cannot verify documents presented in real time (Ahmed *et al*., 2017). One of the challenges linked with the manual verification process is that recruiters and employers find it increasingly difficult to validate the authenticity of academic certificates. Yet, educational certificate must be verified to ensure that its content is true to confirm their accuracy and legitimacy (Osman and Omar, 2016).

The increase of counterfeit educational certificates is a global issue, including in Nigeria, where the effect of this malpractice is detrimental to the credibility of education. Traditional strategies to prevent fake certificates have failed, calling for a more sophisticated approach. The main challenges of the current verification system include manual procedures, unverifiable credentials, vulnerability of centralized storage systems, disconnected verification systems, revocation problems, difficulties in communication, and high dependency on the issuers.

Certificate forgery is a growing problem in the Nigerian academic community. Fraudsters keep creating fake certificates to claim graduation from reputable universities and increase employment opportunities. Therefore, document validation and verification have become important tasks to ensure that the certificate presented by a prospective employee is genuine and that the holder is the rightful owner of such credentials.

This research uses smart contracts in developing a framework for verifying academic certificates, providing links for certificate verification on the blockchain explorer. The focus is creating a decentralized academic credential system for Benson Idahosa University using blockchain technology to tokenize degrees and diplomas as NFTs. A user-friendly DApp for administrators to mint certificates was also developed.

Certificate Verification Ecosystem

The educational certificate verification ecosystem consists of four major entities, regulators, issuers, graduates, and recruiters, who work together to achieve the entire verification life cycle (Fig 1). The government, through the respective ministry of education, establishes the regulatory bodies for different types and levels of education in the country. These regulators include the National University Commission (NUC) which is responsible for universities, the National Business and Technical Examination Board (NABTEB) for technical and vocational institutions, West African Examination Council (WAEC), National Examination Council (NECO), the International General Certificate of Secondary Education (IGCSE), that is mandated to oversee national examinations, and the Ministry of Education as the general custodian of education. These bodies are responsible for, among other things, approving the issuers of educational

qualifications in the country. As such, they publish a list of approved issuers to which third parties can refer if they wish to ascertain the legitimacy of the issuing institutions.

According to Nigerian regulations, they also evaluate the educational qualifications awarded outside the country, determine their comparability with the Nigeria qualifications standard, and issue a comparable certificate called the statement of result. This is done at every level of education by the respective regulator to ensure that these qualifications are understood and recognized by employers, educational institutions, and other authorities in Nigeria. Issuers are learning institutions or government authorities that have the right to produce, maintain, and issue educational qualifications. They award certificates to students who have met the graduation requirements and retain certification records in their registries for reference during verification or other purposes. Apart from awarding a certificate, they can also revoke it if issued by mistake or if the graduate commits academic or non-academic misconduct.

After receiving a certificate, graduates can present it to prospective recruiters during job applications, admissions, or other purposes. Recruiters must verify the validity of the certificates presented to ensure that they do not enlist candidates with forged credentials. However, they cannot achieve this task without the support of the issuers and regulators. Therefore, when performing internal verification, recruiters usually consult with issuers to verify certificates issued by institutions within the country. In case of certificates granted outside the country, the recruiters consult the regulators, who are responsible for assessing and issuing equivalent statements for foreign awards. Due to the possibility of certificate forgery, the recruiters expect to confirm that the learning institution exists legally. However, doing this will require a lot of financial burden to hire a list of approved issuers published by the respective regulators on their websites. The existing system will provide certificate verification for the required recruiters but such a process entails the manual process of validating educational certificates. The traditional system will be improved by implementing NFTs and Smart contracts on the blockchain for certificates verification. Each certificate is added to the blockchain by the working of consensus algorithm-A consensus algorithm is a procedure through which all the peers of the blockchain network reach a common agreement about the present state of the distributed ledger.

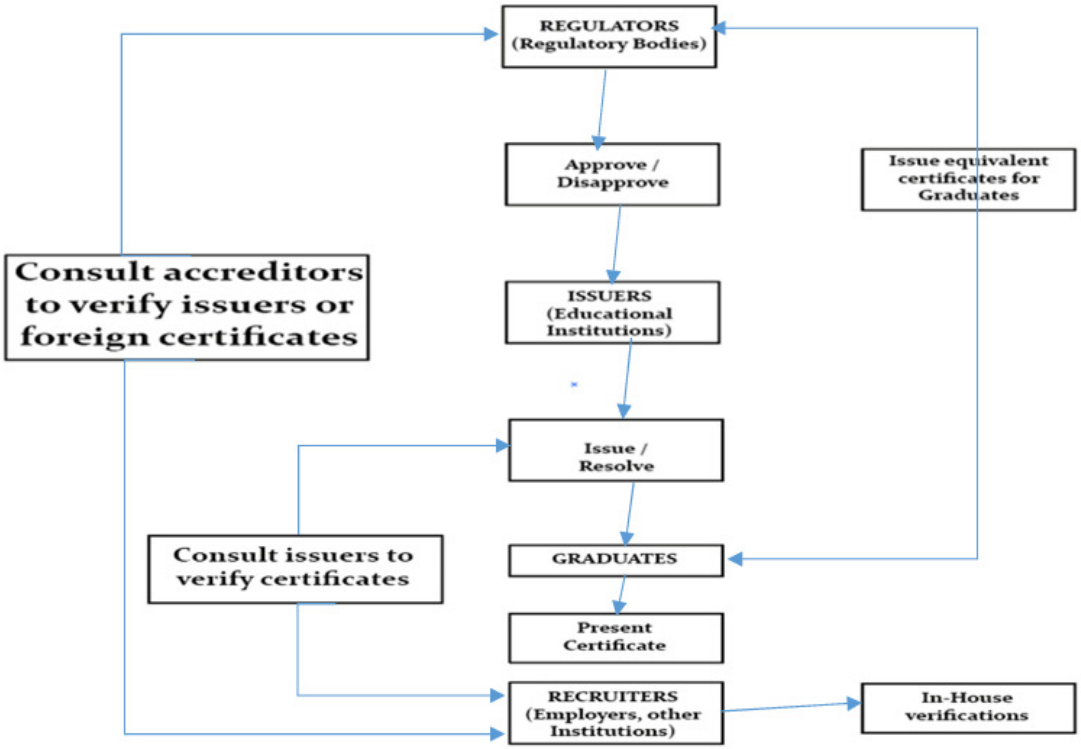

Fig. 1: Educational certificate verification ecosystem in Nigeria

This approach ensures tamper-evident records, eliminates reliance on central authorities, and enables real-time, transparent verification. Blockchain's immutability and security significantly reduce the risk of forgery and enhance trust among all stakeholders. However, the existing academic certificate verification system faces several critical challenges such as centralization and vulnerability, slow verification processes, and lack of transparency.

Blockchain-Based Certificate Verification System

This paper leverages blockchain technology to enhance the issuance, verification, and management of academic credentials using Benson Idahosa University (BIU) as a case study. By integrating the Ethereum blockchain, Solidity smart contracts, and a decentralized application (DApp), the system offers a secure, transparent, and efficient solution for managing student certificates. The DApp provides a user-friendly interface where administrators can input student details and mint certificates. Users can connect their MetaMask wallets to interact securely with the blockchain.

Smart contracts deployed on the Ethereum blockchain manage the minting, storage, and revocation of certificates, ensuring the immutability and security of student credentials. Administrators can mint new certificates by inputting student metadata, including the first name, last name, email, department, and year of completion. The system also allows for the revocation of certificates, which maintains the integrity of the credentialing process. Each minted certificate is linked

to a transaction on the blockchain, viewable on a blockchain explorer like BaseScan, ensuring transparency and ease of verification for external parties. The DApp includes options to download the list of minted certificates and specific certificate details as Excel files, supporting data management and sharing needs. Robust security protocols are implemented to protect the integrity of data and interactions with the blockchain, including secure methods for wallet connections and data handling. The responsive design of the DApp ensures accessibility and usability across various devices, including desktops, tablets, and smartphones.

There are also other questions regarding the choice of Ethereum as a blockchain technology, such as its relatively rich and well-structured ecosystem, a vibrant developer community, and compatibility with smart contracts, which make it a relatively secure platform for developing decentralized applications. However, transaction costs and concerns of private key management may be considered restricting in that regard and influence usage and accessibility.

By leveraging blockchain technology, the system ensures that academic credentials are tamper-proof and secure from unauthorized alterations. The use of a public blockchain provides transparency, allowing anyone to verify the authenticity of the certificates directly on the blockchain explorer. Automated processes for minting and verifying certificates reduce the time and effort required for credential management, and the ability to download certificate data as Excel files facilitates better data management and record-keeping. The revocation feature ensures that any certificates issued in error or fraudulently can be invalidated, maintaining the system's credibility. The research addresses the limitations of traditional database management systems and offers a modern, secure, and efficient solution for managing academic credentials in Benson Idahosa University (BIU). Fig. 2 shows the Blockchain-based certificate verification framework.

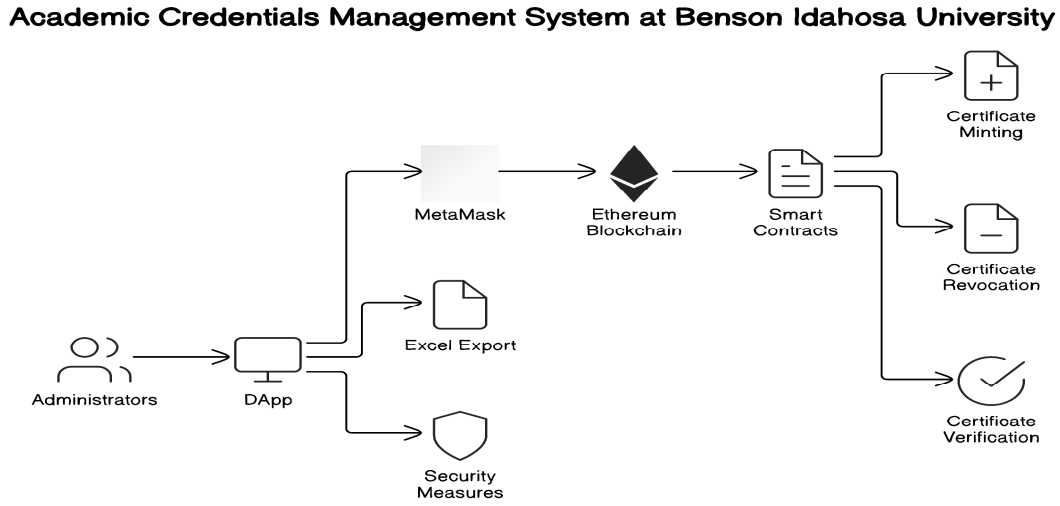

Fig. 2: Blockchain-based Certificate Verification Framework

Benefits of the Developed Certificate Verification System

Most of the limitations of the current verification system in Nigeria emanate from paper certificates and manual verification procedures. The framework in fig. 2 can eliminate both by introducing digital certificates and automating the tasks involved in the issuance and verification process. Recruiters will be able to verify certificates by a simple search on the blockchain system and easily get reliable results in real time, eliminating burdensome, lengthy, costly, and inefficient verification processes.

One further problem with current paper-based certificates or certificates of equivalence is that the embedded security features (e.g. holograms, signatures, etc.), which act as proof of their authenticity, are not verifiable by the recruiters because of their unfamiliarity with them and lack of specialized tools. However, digitally signed certificates, along with their metadata stored on the blockchain, resolve this issue. The hash value—a unique cryptographic code generated from certificate data and stored immutably on the blockchain—acts as proof of authenticity. Recruiters can easily retrieve and verify this hash value through a blockchain lookup, ensuring the certificates' validity without requiring specialized equipment.

Smart contracts play a pivotal role by automating the verification process. When a verification request is initiated, the corresponding smart contract autonomously validates the stored information. This automation significantly reduces the time and effort traditionally required for manual verification processes. Employers and academic institutions benefit from swift, reliable, and real-time verification, enhancing operational efficiency and reducing administrative overhead.

METHODOLOGY AND SYSTEM DESIGN APPROACH

To develop a robust decentralized academic credential system, a structured methodology and system design approach were employed. This section outlines the key phases of system development:

A. Requirement Analysis:
- Conducted stakeholder interviews with administrators, employers, and graduates to identify challenges in existing credential verification systems.
- Defined key system requirements, such as immutability, decentralization, user-friendliness, and real-time verification.

B. Conceptual Design:
- Designed a high-level architecture for the system, including the integration of blockchain for data storage and a decentralized application (DApp) for user interaction.
- Selected Ethereum as the blockchain platform for its mature ecosystem and Solidity as the programming language for smart contracts.

C. Smart Contract Design:
- Developed smart contract blueprints to define functionalities such as certificate minting, storage, and revocation.
- Incorporated metadata fields, including student name, email, department, and completion year, ensuring comprehensive data representation.

D. User Interface (UI) Prototyping:

- Created prototypes for the DApp using design tools to visualize user workflows.
- Ensured the interface was intuitive, responsive, and accessible across devices.

E. Security Planning:
- Identified potential security threats, such as unauthorized data access and transaction tampering.
- Proposed encryption techniques and access controls to safeguard system integrity.

F. Data Flow and Workflow Analysis:
- Defined data flow diagrams to map interactions between the UI, smart contracts, and blockchain network.
- Designed workflows for core functionalities, including certificate issuance, verification, and revocation.

Implementation Guidelines

Implementation guidelines serve as a roadmap for translating the conceptual design of a system into a tangible, operational reality. In the context of developing a decentralized academic credential system using blockchain technology, the implementation guidelines encompass several key aspects to ensure a successful deployment such as:

A. System Setup:
- Establish the necessary hardware and software infrastructure required to support the decentralized academic credential system.
- Ensure that all hardware components, such as servers or cloud resources, meet the system's performance and scalability requirements.
- Install and configure blockchain-specific software, including Ethereum client software, to interact with the blockchain network.
- Set up development environments, such as Remix IDE or Truffle Suite, for smart contract development.

B. Smart Contract Development:
- Define and implement the smart contracts that govern the functionality of the academic credential system.
- Use Solidity, the programming language for Ethereum smart contracts, to write the code for the smart contracts.
- Develop smart contract functionalities for managing student metadata, issuing academic credentials as non-fungible tokens (NFTs), and recording transactions on the blockchain.
- Conduct thorough testing of the smart contracts to identify and resolve any bugs or vulnerabilities before deployment. Figure 3 depicts the Remix IDE for deploying the smart contracts.

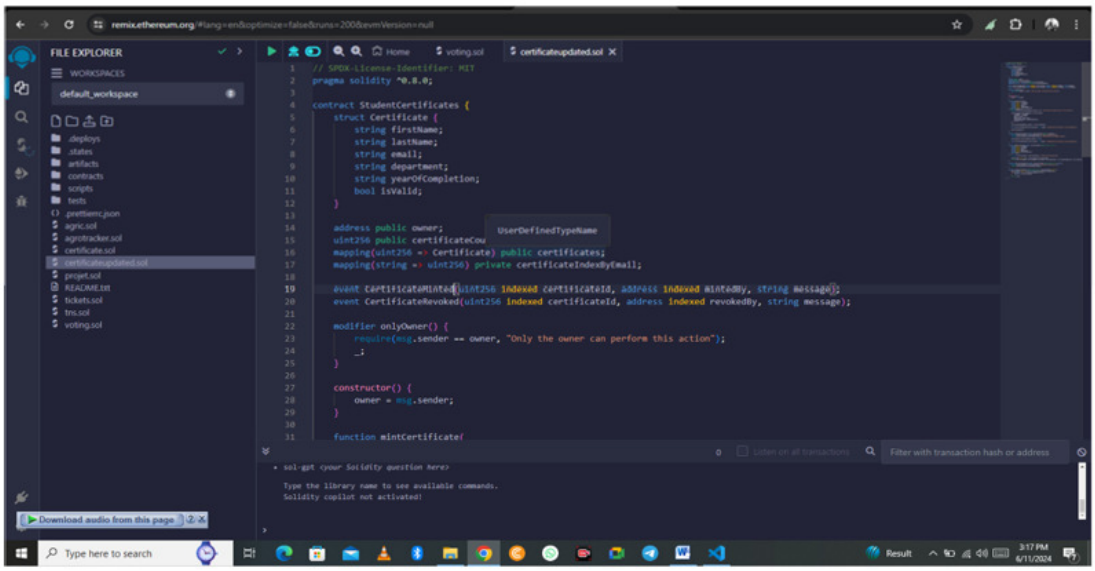

Fig. 3: Remix IDE for smart contract deployment

C. User Interface Design:

- Create intuitive and user-friendly interfaces for interacting with the decentralized academic credential system.
- Develop web-based interfaces using HTML, CSS, and JavaScript to allow users to input student metadata, view academic credentials, and interact with the blockchain using VS Code.
- Ensure that the user interfaces are responsive, accessible, and compatible with different devices and screen sizes to accommodate diverse user needs.

Figure 4 illustrates the VS Code environment for interface design.

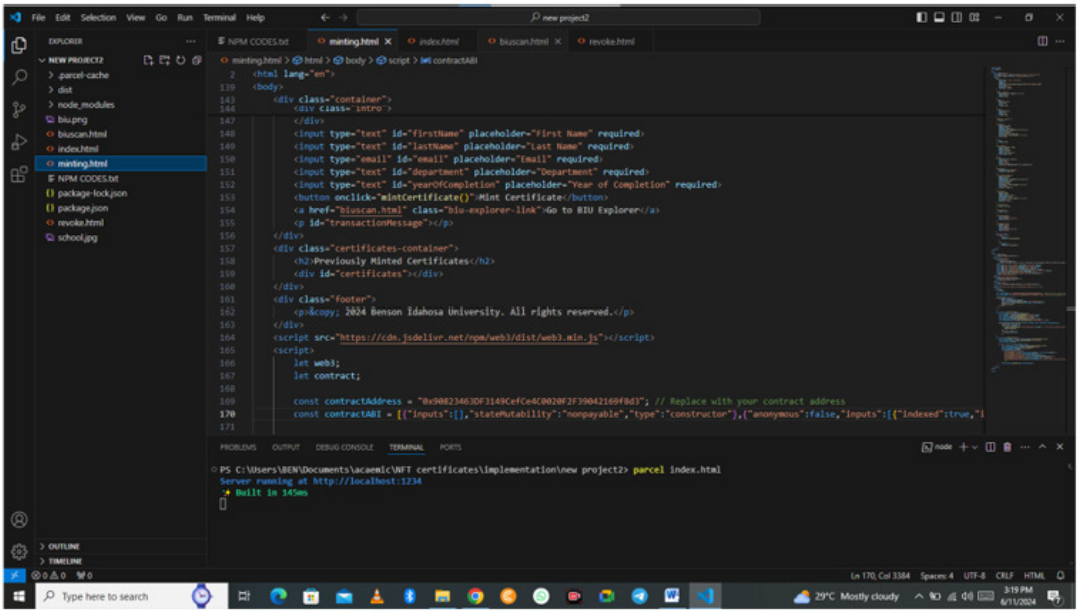

Fig. 4: User interface design backend using VS code

D. Integration and Deployment:

- Integrate the developed smart contracts with the user interfaces to create a cohesive system.
- Deploy the smart contracts to the Ethereum blockchain network using deployment tools like Remix IDE or Truffle.
- Configure the user interfaces to interact with the deployed smart contracts, enabling seamless communication between the frontend and the blockchain backend via contract address and Application Binary Interface (ABI) code

E. Security Measures:

- Implement robust security measures to safeguard the decentralized academic credential system against potential threats and attacks.
- Utilize encryption techniques to protect sensitive data, such as student metadata and academic credentials, stored on the blockchain.
- Implement access controls and authentication mechanisms to restrict unauthorized access to system functionalities and resources.
- Regularly audit and update security protocols to address emerging threats and vulnerabilities.

F. Documentation and Training:

- Document the system architecture, design decisions, and implementation details to facilitate system maintenance and future enhancements.
- Provide comprehensive training and support to system administrators, developers, and end-users on how to use the decentralized academic credential system effectively.
- Develop user manuals, tutorials, and other educational resources to assist users in navigating the system's features and functionalities.

G. Monitoring and Maintenance:

- Establish monitoring tools and procedures to monitor the performance, availability, and security of the decentralized academic credential system.
- Implement proactive maintenance practices to address software updates, bug fixes, and system optimizations.
- Continuously monitor blockchain network activity and performance metrics to ensure the reliability and scalability of the system over time.

RESULTS

The implementation of the decentralized academic credential system at Benson Idahosa University yielded significant improvements in the issuance, verification, and management of academic credentials. The system successfully integrated blockchain technology, specifically the Ethereum blockchain, and Solidity smart contracts, to provide a secure, transparent, and tamper-proof solution. The decentralized application (DApp) developed for this project proved to be user-friendly and efficient, allowing administrators to mint and revoke certificates seamlessly.

One of the notable results was the enhanced security and immutability of academic credentials. By using the Ethereum blockchain, each certificate minted is stored in an immutable ledger, ensuring that the data cannot be altered or deleted. This addresses a major concern with traditional database systems where data can be manipulated or lost. The smart contracts deployed on the blockchain handle the minting, storage, and revocation of certificates, guaranteeing

the integrity and authenticity of each credential.

The system's ability to revoke certificates added an essential layer of functionality. This feature ensures that any certificates issued in error or due to fraudulent activities can be invalidated, maintaining the credibility of the credentialing process. The revocation status is clearly indicated in the DApp, providing transparency and trust in the system. Additionally, the verification mechanism via blockchain explorer links enables external parties, such as employers and other educational institutions, to easily verify the authenticity of the certificates. Verification time was significantly reduced to under a minute, compared to several hours or days in traditional systems. This verification feature enhances the reliability and trustworthiness of the academic credentials issued by Benson Idahosa University.

The DApp's responsive design ensured accessibility across various devices, including desktops, tablets, and smartphones. This flexibility allowed administrators to manage academic credentials from different locations and devices, improving the overall efficiency and usability of the system. The DApp's intuitive design, clear action buttons, and search functionality reduced the learning curve for administrators. The ability to download certificate data as Excel files provided a practical solution for data management and record-keeping. Administrators could easily generate reports and share credential information as needed, further streamlining the administrative processes.

Another significant outcome was the transparency brought about by the blockchain technology. All transactions related to the minting and revocation of certificates are recorded on the blockchain, providing a transparent audit trail that can be reviewed by authorized parties. This transparency is crucial for maintaining the integrity of the academic credentialing process and ensuring that all actions taken within the system are verifiable and accountable.

In terms of user experience, the DApp was designed to be intuitive and straightforward, reducing the learning curve for administrators. The inclusion of clear action buttons and search functionalities made it easy to navigate and use the system effectively. Feedback from users indicated a high level of satisfaction with the system's performance and ease of use. In conclusion, the decentralized academic credential system implemented at Benson Idahosa University demonstrated significant improvements in security, transparency, and efficiency. By leveraging blockchain technology and developing a robust DApp, the project addressed the limitations of traditional database management systems and provided a modern solution for managing academic credentials. The successful integration of smart contracts, user-friendly interface, and comprehensive security measures ensured that the system met the needs of the university and provided a reliable platform for issuing and verifying academic credentials.

Index Page

The Index Page as shown in Fig. 5 serves as the entry point to the DApp. It is designed to be visually appealing and professional, with a welcoming

introduction to the purpose of the application. The page includes a prominent header displaying the name of the university, Benson Idahosa University, and a footer for additional information. The page also features a button for users to connect their MetaMask wallets, allowing secure access to the DApp. The design incorporates animations and a background image to enhance the user experience, making the page not only functional but also engaging. The figure 5 below represents index.htm

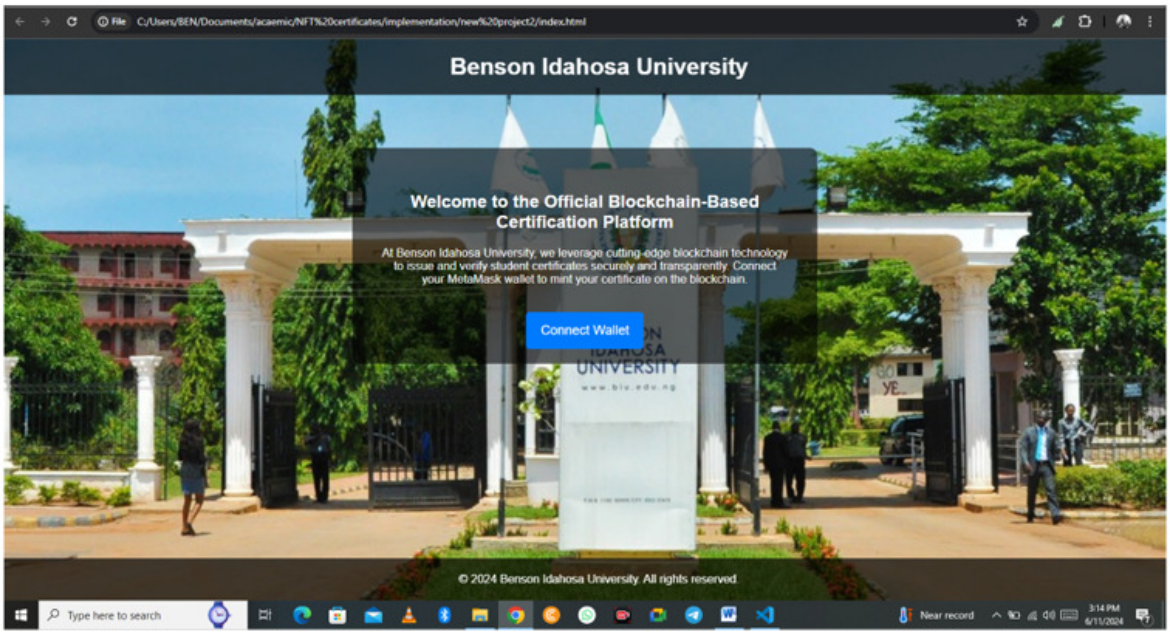

Fig. 5: The index page

The BIUSCAN Page

The BiuScan Page (in Fig. 6), also known as the Blockchain Page, displays all previously minted certificates. Each certificate block includes detailed information such as the student's name, course of study, GPA, year of completion, and revocation status. The page is designed with a header that prominently displays "BIU Private Blockchain" and includes the BIU logo and a search bar for easy navigation. Additionally, the page provides a download option to export certificates as Excel files and a link to the Revoke Page for certificate revocation. This design ensures that all necessary information is readily available and easily accessible, enhancing the transparency and usability of the system.

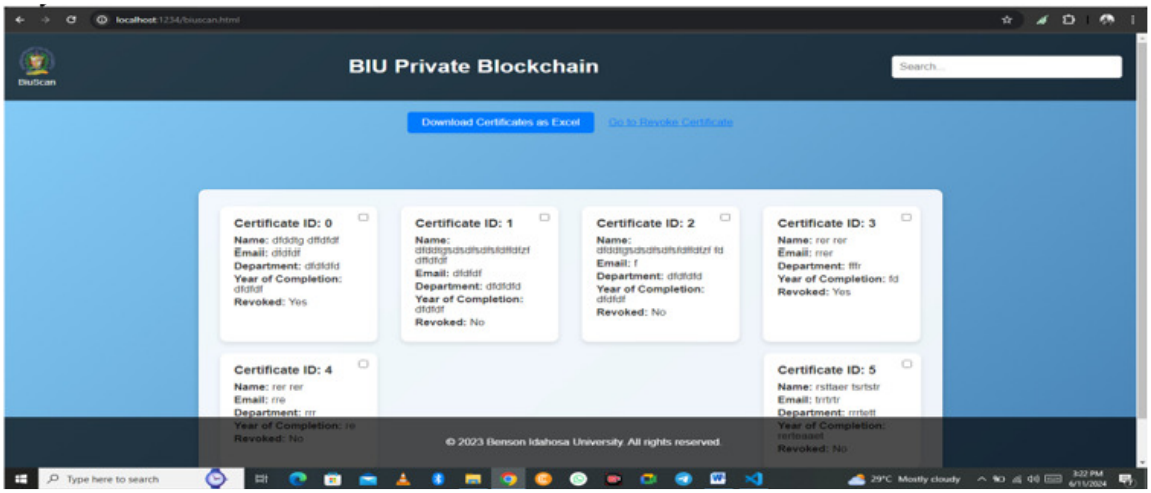

Fig. 6: The BiuScan page

The Revoke Page

The Revoke Page as shown in Fig. 7, allows administrators to revoke certificates. It includes a form where administrators can input the Certificate ID to be revoked. Upon revocation, the certificate's status is updated and displayed in the previously revoked certificates section below the form. This section lists all revoked certificates with their respective details, such as Certificate ID, student's name, email, department, year of completion, and revocation status. The page is designed to be consistent with the rest of the application, ensuring a cohesive user experience. The inclusion of a link to view the transaction on the blockchain enhances transparency and trust in the system. The figure 7 below represents revoke.html.

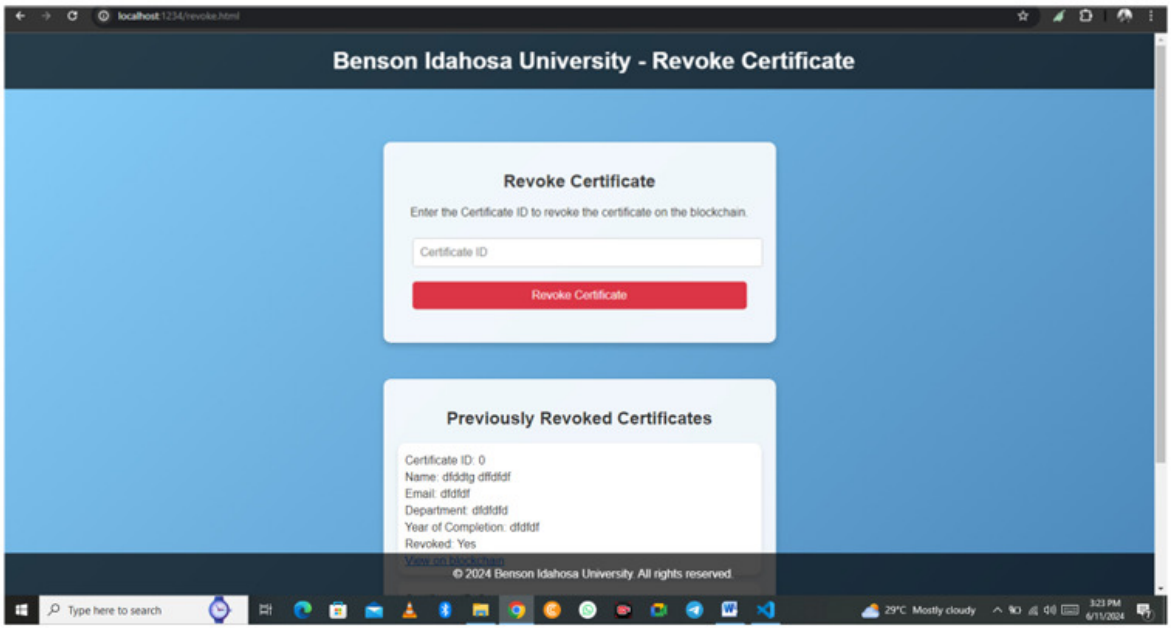

Fig. 7: The Revoke page

The Minting Page

The Minting Page (in Fig. 8) reveals where the administrators input student metadata to mint new certificates. The page features a form that collects information such as the student's first name, last name, email, department, and year of completion. The "Mint on Blockchain" button ensures that the data is only processed when all fields are correctly filled. Below the form, the page displays previously minted certificates, including details like Certificate ID, student's name, email, department, year of completion, and revocation status. This section helps administrators keep track of all issued certificates and their statuses. The page design is intuitive and professional, facilitating efficient and accurate data entry. The figure below represents minting.html.

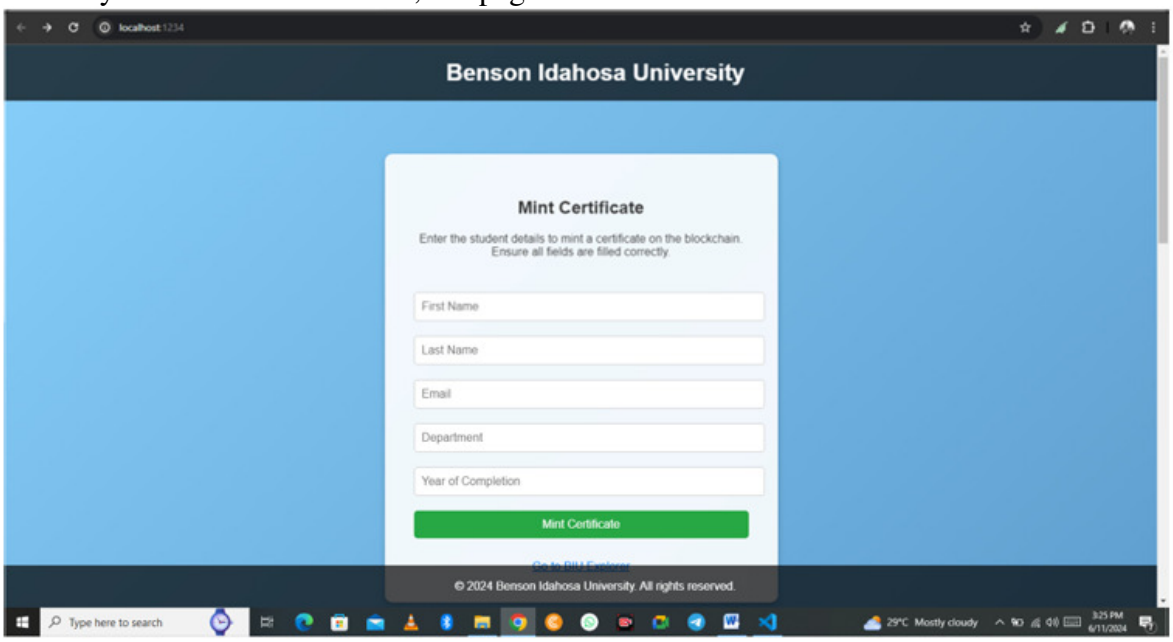

Fig. 8: The Minting page

Each of the figures discussed above contributes to the overall functionality and effectiveness of the decentralized academic credential system. They ensure that administrators can efficiently manage the issuance, verification, and revocation of academic certificates, enhancing the security, transparency, and credibility of the credentialing process at Benson Idahosa University.

SUMMARY

Academic certificate verification is a crucial process that ensures the authenticity and integrity of educational qualifications. Traditional certificate verification methods often rely on centralized databases and paper-based records, which can be prone to fraud, forgery, and inefficiencies. Certificate forgery has been a major challenge in the country's ever-growing situation. Forgery as we have seen can lead to catastrophic situations when the forged certificate holder utilizes the same to secure employment in an organization. However, the need for certificate verification becomes expedient. Blockchain

technology offers a promising solution to address these challenges. This study designed a system for verifying academic certificates at all educational levels using the decentralized network, Blockchain Technology.

RECOMMENDATIONS

Based on the findings from this study, we recommend that more research works should be done in certification verification and vast literature reviews should be carried out on the domain. After successfully implementing and testing the effectiveness of the certificate verification system, to realize the intended purpose of the study, we also recommend the prototype to be adopted by various institutions, private and public Organizations, and the government as a decentralized software for both local and international certificate verification systems. Conclusively, the insights gained from the research can inform decision-making, shape future research agendas, and guide practical applications in real-world settings.

REFERENCES

Ahmed, H. A., Jang, J.-W., and Hamdi, A. A. (2017). Higher Educational Certificate Authentication System Using QR Code Tag. *International Journal of Applied Engineering Research*, 12(20). 9728-9734.

Umaru, C. B. and Nzadon, D. T. (2021). Design and Implementation of Web-Based Certificate Verification System (Case Study Adamawa State University Mubi). *Multidiscip. Int. J. Res. Dev*., 1(02): 22-34.

Osman, G. and Omar, S. S. (2016). Cloud-Based Graduation Certificate Verification Model. Proceedings of Academics World 54th International Conference, Malacca, Malaysia. https://www.worldresearchlibrary.org/up_proc/pdf/571-14861269431620.pdf

Suganthalakshmi, R., Praba, G. C., Abhirami, K. and Puvaneswari, S. (2022). Blockchain-Based Certificate Validation System. *International Research Journal of Modernization in Engineering Technology and Science*, 4(7): 3816-3819.

Warasart, M. and Kuacharoen, P. (2012). Paper-based Document Authentication using Digital Signature and QR Code. *International Conference on Computer Engineering and Technology.*