Journal of Engineering and Technology for Industrial Applications

ITEGAM-JETIA

Manaus, v.10 n.49, p. 35-41. September/October, 2024.
DOI: https://doi.org/10.5935/jetia.v10i49.1145

ISSN ONLINE: 2447-0228

RESEARCH ARTICLE OPEN ACCESS

A BLOCKCHAIN-BASED DIGITAL EDUCATIONAL CERTIFICATE VERIFICATION SYSTEM

Tolulope Ifeyemi[1], Ajibola Oyedeji[2] and Fiyinfoluwa Adebiyi[3]

[1 2, 3] Department of Computer Engineering, Olabisi Onabanjo University, Ago-Iwoye, Nigeria

[1]http://orcid.org/0009-0002-1057-6460 , [2]http://orcid.org/0000-0002-0180-492X , [3]http://orcid.org/0009-0001-5494-5216

Email: toluwalopeifeyemi@gmail.com, oyedeji.ajibola@oouagoiwoye.edu.ng, adebiyifiyinfoluwa8@gmail.com

ARTICLE INFO

Article History
Received: June 09th, 2024
Revised: September 14th, 2024
Accepted: September 14th, 2024
Published: October 04th,2024.

Keywords:
Certificate Verification,
Blockchain,
Celo,
User Experience.

ABSTRACT

The reliance on paper-based educational certificates and the lack of a robust and tamper-proof system for verifying academic credentials in the Nigerian education system make them vulnerable to forgery and alterations. The situation poses challenges in guaranteeing the legitimacy of such qualifications, and a need arises for a secure system to verify academic credentials. The proposed solution is a blockchain-based digital certificate verification system (BCVS) that utilizes the Celo blockchain as the underlying blockchain platform to store each digital certificate hash and meta-data, which is unique, secure, and permanently recorded on the blockchain. The system also includes a QR code feature to verify the certificate's authenticity instantly. Ten users evaluated the system, and the average scores are as follows: the user interface had 78%, the application database security scored 66%, the blockchain data security achieved 82%, the revocation mechanism achieved a score of 67%, and the maintainability achieved a score of 46%. While the system is designed to cater to university requirements and can revoke certificates if needed, it represents an advancement in certificate verification, thereby simplifying the process and improving the overall experience for everyone involved, with the potential to be scaled and customized for other universities, institutions, and use cases.

Copyright ©2024 by authors and Galileo Institute of Technology and Education of the Amazon (ITEGAM). This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

I. INTRODUCTION

The issue of certificate forgery is widespread in most developing countries, and the reliance on paper-based certificates makes them vulnerable to fraud, forgery, and unauthorized alterations [1]. There needs to be a robust and tamper-proof system for verifying academic credentials in the Nigerian education system to address certificate forgery. In the education system, there is a need for a secure method to verify academic credentials to combat certificate forgery. This poses challenges in guaranteeing the legitimacy and reliability of qualifications [2-4].

With the rapid development and deployment of information technology, developing solutions for diverse problems across various domains has become pertinent [5]. Blockchain technology (BT) is an emerging technology that has significant benefits across various application areas such as cross-border payments, identity management, real estate management, and supply chain [6], [7]. Blockchain provides an immutable electronic certification system, making it considerably more challenging for individuals to manipulate academic credentials [1]. BT is witnessing a broad research focus and adoption in various countries across different domains [8-10].

Using blockchain technology to uphold the integrity of certificates from forgery and make verification processes efficient is a reliable approach [11]. Using distributed ledger technology allows for transactions without the need for intermediaries. It functions as a system that guarantees tamper-proof and immutable transaction records, making it an ideal option for certificate verification systems [12]. This project aims to design, implement, and evaluate a user-friendly, secure, and scalable blockchain-based digital certificate verification system (BCVS) leveraging blockchain technology to revolutionize how certificates are generated and verified.

Several review studies highlight key contributions, challenges, and future focus of blockchain-based systems for academic certificate verification [2],[4]. The papers show that blockchain has the potential to manage the certificate verification process securely. Additional benefits lie in cost, ease of making

decisions, customer attraction, and potential for exponential growth of businesses [13], [14]. Research developed a blockchain-based model for transcripts in Saudi Arabia in a bid to achieve digital transformation in the educational sector [15]. The Ministry of Education Transcript Verification blockchain (Saudi Arabia) (MOETVBC) framework proposed a novel hyper ledger fabric blockchain using distributed and decentralized ledgers across global P2P Network nodes. The system uses smart contracts to provide a secure method for the verification of students' certificates and degrees.

A prototype model based on the security features of BT and cloud storage to verify and validate educational credentials is presented [1]. The digital assets pass through a temporary storage phase where a unique certificate's distinct identifier is generated through a hashing algorithm. Further, a cryptographic encryption technique has been added to improve system security [1]. A Smart contract, Certi, was developed for storing certificates based on Ethereum, which provides a platform for potential employers or admission teams to authenticate stored certificates [11].

Similarly, Verificate is a system that leverages blockchain technology to store and authenticate certificates submitted securely and assures students of the secure storage of the certificate [16]. The system achieves its goal using distributed systems like IPFS and Ethereum. Verificate proves to be successful in preventing document counterfeiting [16]. Furthermore, a blockchain-based verification system utilizes technology for certificate verification, employing an authentication scheme for owners and storing students' time and space information as blocks on the blockchain to achieve a secure and tamper-proof digital asset [17].

While there are undeniable benefits, it is essential to acknowledge that several challenges still need to be overcome to successfully implement blockchain-based systems to their full potential [7]. Blockchain-based verification systems have been widely adopted in several fields to ensure the integrity and credibility of certificates; however, these potentials have seen limited application in Africa and Nigeria, specifically in the educational system where certificates are issued [13].

The aim of this project is the development of a blockchain-based certificate verification system for digital certificates. In addition, the proposed solution will be able to issue digital certificates for the subscribed institution, with a case study of Olabisi Onabanjo University, Ago-Iwoye, Nigeria.

II THEORETICAL REFERENCE

The following sections describe requirement gathering, system design, implementation, testing, and deployment stages taken for the completion of the system using a modified waterfall model, as shown in Figure 1 [18].

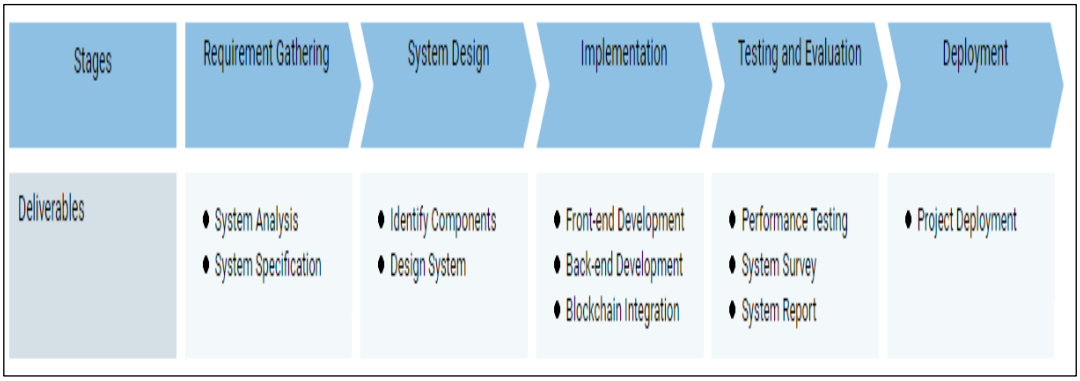

Figure 1: Project Methodology.
Source: Authors, (2024).

II.1 REQUIREMENT GATHERING

The major functional requirements of the system are presented as follows;

i. The creation of a record of the certificate by the issuer of a certificate on the blockchain.
ii. The certificate would be securely signed using the issuer's key.
iii. Publication of the signed certificate on the blockchain.
iv. Individuals who wish to verify the authenticity of a given certificate can utilize this solution.

II.1.1 ISSUING APPLICATION

The key functionalities and components of the Issuing Application include:

1. **User Authentication**: This feature ensures secure access to the Application. It verifies the identity of all users before granting them access.
2. **Administration Dashboard**: This interface allows administrators to effectively manage data, user privileges, and other administrative tasks.
3. **Certificate Auditing**: This function enables the review and verification of certificates to ensure their validity and integrity.
   i. Certificate Viewing: The Application provides several viewing options for different certificate states:
   ii. Signed and Published Certificates: This feature allows users to view certificates that have been signed and are currently active.
   iii. Revoked Certificates: This feature allows users to view revoked certificates.
4. **Certificate Revocation**: This critical function allows the application system admin to revoke certificates when necessary, rendering the certificate status invalid.

II.1.2 VERIFICATION APPLICATION

The verification applications are responsible for checking the authenticity and integrity of the certificates issued before. It can be verified using two methods with steps as follows:

1. **Using the file upload method:**
   i. The user uploads the digital copy of the certificate in PDF format.

ii. The system calculates the hash value of the uploaded digital file.
iii. The client sends a request to the API endpoint.
iv. Then, an interaction with the blockchain to fetch the required data for verification
v. The system applies the verification logic to compare the calculated hash value with the retrieved hash value from the blockchain to ensure data integrity.
vi. The system checks the database to confirm if the calculated hash value exists and extracts other required information.

2. Using the certificate ID method:

i. The user enters the Certificate ID.
ii. The client sends a request to the API endpoint.
iii. Then, an interaction with the blockchain to fetch the required data for verification
iv. The system applies the verification logic to compare the certificate ID with the retrieved certificate ID from the blockchain to ensure data integrity.
v. Check the database to confirm the existence of the certificate ID value.

II.2 SYSTEM DESIGN

During this phase, the focus is on developing the system design for the blockchain-based certificate verification system, including the architecture and the need to identify the components required for the system, including the blockchain type, the technology stack, and several other tools. As shown in Figure 2, the system briefly consists of five components in the system architecture overview: verification application, issuing Application, the Celo Blockchain, and MongoDB Database.

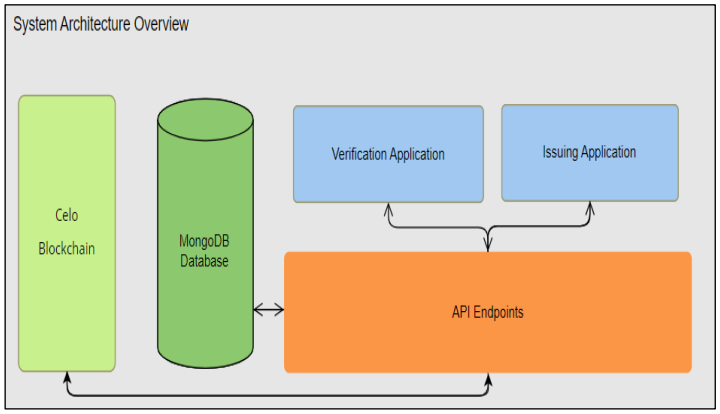

Figure 2: System Architecture Overview.
Source: Authors, (2024).

The blockchain serves as a component of trust for a distributed database. These data include the generated hash from all the certificates issued and more.

II.2.1 Celo Blockchain and Technology Selection

The blockchain acts as the infrastructure of trust for saving authentication and other metadata using a distributed database. Typically, these data include the generated hashed data from all the certificates issued. The Celo blockchain is suitable for developing a digital certificate verification system due to its carbon-negative status, cost-effectiveness, and energy-efficient proof-of-stake consensus mechanism tokenized carbon credits that enable composable ecological assets. The Celo blockchain also has a native accounting unit, the cryptocurrency CELO, which is used to implement cryptocurrencies or tokens as contracts. Moreover, the Celo blockchain serves a purpose as both the primary currency and an ERC 20 compatible token on the Celo blockchain. These characteristics position the Celo blockchain as an option for establishing a certificate authentication system [19], [20]. The Celo network means that even wallet users with high latency, low bandwidth, or high-cost data tariffs can use Celo. Celo removes the need to check every header before a received header can be trusted.

II.2.2 Mongodb

The MongoDB is employed as the database since it successfully manages JSON-based data, which provides more storage for other metadata. MongoDB is a NoSQL database used to manage JSON-based data structures [21]. It provides storage for other related metadata of the certificate on the system. This metadata can include various information related to the certificates, such as the issuer's details, the recipient's details, the date of issue, and more, providing a comprehensive and efficient database solution for the blockchain-based certificate verification system.

II.2.3 Verification Application

The verification application checks the authenticity and integrity of the digital certificates initially generated and issued by the Issuing Application. This is achieved through two primary methods: the file upload method and the certificate ID method.

In the file upload method, the user uploads the digital copy, which is the certificate's PDF file. The system then calculates the hash value for the digital copy, which serves as a unique identifier for the certificate. The client then requests the blockchain, interacting with the blockchain API to fetch the transaction message associated with the certificate. The logic of the verification process involves comparing this transaction message with the verification data. This includes verifying the hash value on the certificate to ensure there has been no tampering and confirming if the hash value is present in the database.

The certificate ID method follows a similar process. The user enters the Certificate Issue Code, and the client requests the blockchain. The blockchain API is again used to fetch the transaction message. The verification logic involves checking the hash value on the certificate to avoid tampering and confirming if the hash value is both in the database and on the blockchain.

These methods support the primary function of the verification application, which is to check the authenticity and integrity of the digital certificates that have been initially generated and issued. By fetching the transaction message through an API endpoint and comparing it with the verification data, the Application ensures that each certificate is valid and trustworthy. This robust verification process contributes to the overall reliability and security of the certificate system.

II.2.4 Issuing Application

The issuing application is responsible for the main business logic of issuing and signing the certificate. It serves as the backbone of the certificate verification system in handling critical tasks of generating and issuing, thereby ensuring the system's integrity, reliability, and security. There is a dedicated interface for system administrators. It allows them to manage various aspects of the system and audit the certificates by viewing various types of certificates, including issued and revoked certificates. This ensures transparency and accountability in the certificate issuance process.

It also has the revoking certificate functionality, which allows for the invalidation of certificates when necessary, which could be due to a variety of reasons such as expiration, errors, fraudulent activities, or institution disciplinary measures.

II.2.5 Api Endpoints

The role of the API endpoints is pivotal and crucial because they serve as the communication gateway between the frontend, backend, and blockchain system, as illustrated in Figure 3. The stored metadata can be retrieved through specific API endpoints. These endpoints are designed to handle requests from the front end of this system, fetch the requested data from the MongoDB database, and return it in a structured format. This process ensures that all relevant information about an issued certificate is readily available and can be accessed efficiently.

Leveraging the power of MongoDB for metadata storage and retrieval helps enhance the system's robustness. It keeps the blockchain less cluttered, as only the essential certificate data is stored, while MongoDB handles the rest. This design choice contributes to the scalability and performance of the system, ensuring it remains fast and responsive even as the number of issued certificates grows.

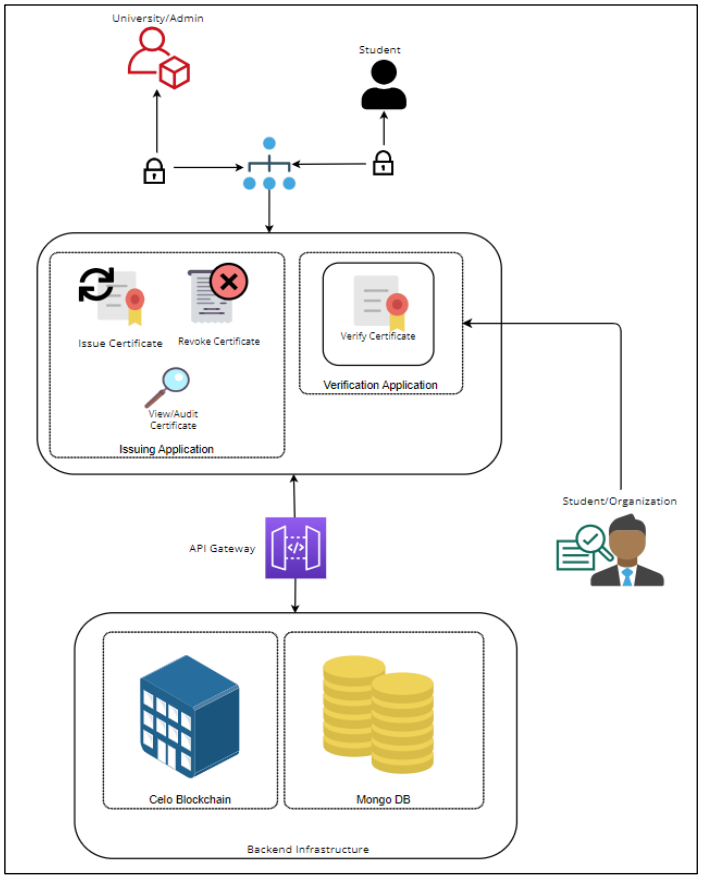

Figure 3: Illustration of the system architecture design.
Source: Authors, (2024).

II.2.5 DEPLOYMENTS

The deployment phase involves transitioning our blockchain-based certificate verification system from a development setting into a real-world operational environment. The backend logic provides the ability to write and read certificate meta-data and interact with the local database (MongoDB). The system's backend, built on NodeJS for the server configuration and API endpoints, was deployed on Render. The front end, constructed using React, is being deployed on Vercel and is available at https://bcvs.vercel.app. Furthermore, a provisioned Celo account loaded with Celo cryptocurrency allows transactions and store records on the Celo blockchain to be executed seamlessly.

III. RESULTS AND DISCUSSION

The BCVS has been implemented with a user-friendly interface, as shown in Figure 4, depicting the landing page with login options for students and administrators.

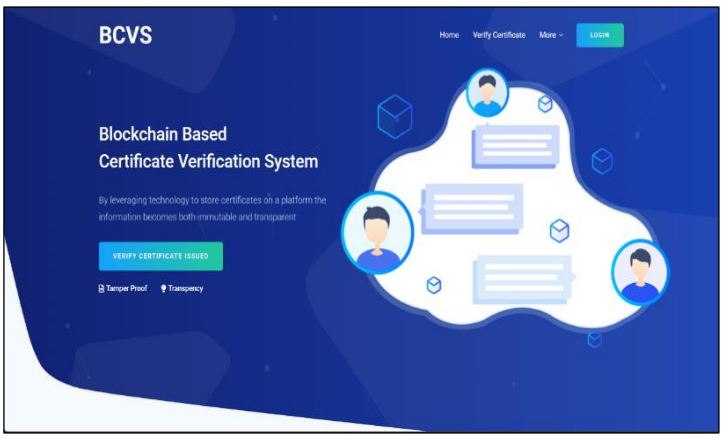

Figure 4: BCVS Landing Page.
Source: Authors, (2024).

III.1 DIGITAL CERTIFICATE ISSUING

The admin issues the digital certificate by correctly entering the candidate's details in the form in Figure 5. After clicking the Submit button, a preview of the submitted form details is prompted for confirmation. The digital certificate is created when action is taken, followed by the certificate hash value and certificate ID stored on the Celo Blockchain public ledger. Figure 6 is a sample of the generated certificate. An essential feature of this certificate is including a QR code, which serves the purpose of verification.

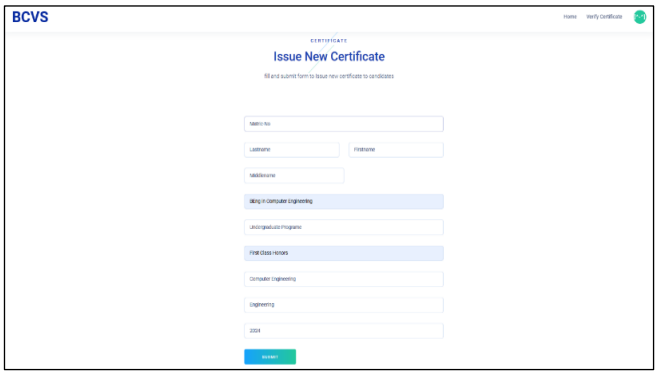

Figure 5: Certificate Issuing Form.
Source: Authors, (2024).

Figure 6: A Generated Digital Certificate.
Source: Authors, (2024).

III.2 DIGITAL CERTIFICATE ISSUING

An organization or legal entity requiring verification of an issued certification can either upload a PDF file of the issued digital certificate or use the certificate ID, as shown in Figures 7 and 8, respectively. Figure 9 is the result of the verification, showing the valid status of the certificate.

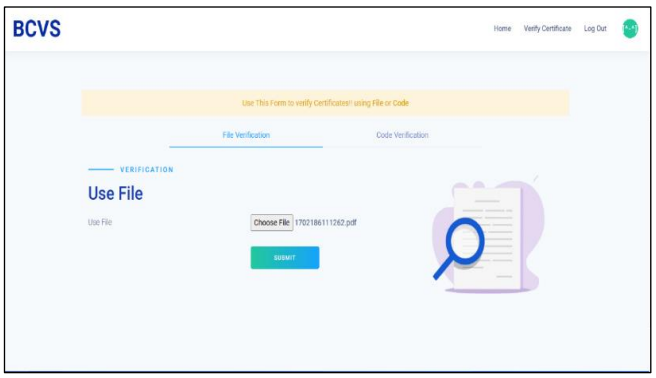

Figure 7: Verification with file upload.
Source: Authors, (2024).

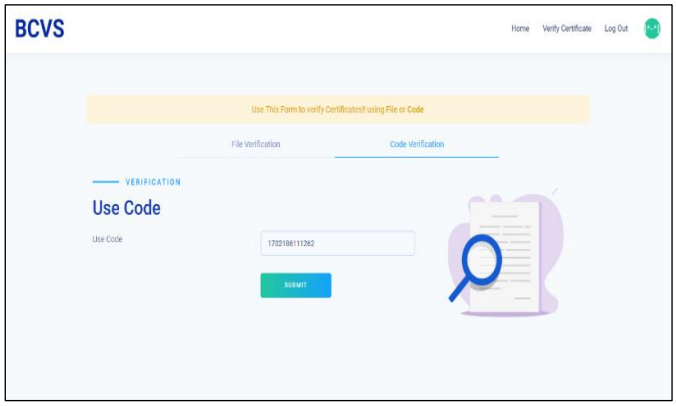

Figure 8: Verification with a certificate ID.
Source: Authors, (2024).

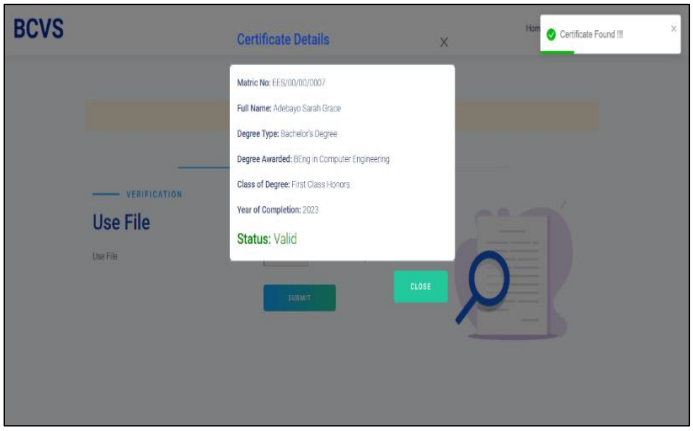

Figure 9: A Verified Digital Certificate.
Source: Authors, (2024).

III.3 CELO BLOCKCHAIN TRANSACTION

The Celo Blockchain Transaction system serves as the foundation for the certificate verification system. Each transaction can represent actions like issuing, verifying, or revoking a certificate. Important information included in these transactions usually consists of the certificate's identifier, the issuer's details, the recipient's information, and the timestamp. In Figure 10, the transactions on the blockchain provide transparency and traceability. This ensures that every transaction is permanently recorded and easily auditable by any participant in the network. The transparency offered by this system helps establish trust among users and dramatically reduces the risks associated with fraud and unauthorized modifications.

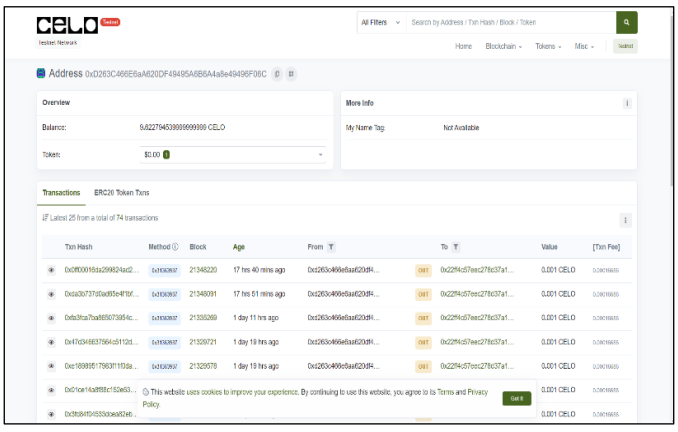

Figure 10: Transactions on Celo by the System.
Source: Authors, (2024).

III.4 EVALUATION RESULT

Ten users (A-J) tested the BCVS to determine the system's performance and acceptability. The system was scored on a scale of 0 – 10, with 0 being the worst and 10 being the best, based on the criteria presented in Table 1. The user interface achieved a score of 78%, the certificate data security by the application database achieved a score of 66%, the blockchain data security achieved an accuracy of 82%, the revocation mechanism achieved a score of 67%, and the maintainability achieved a score of 46%.

Table 1 System Evaluation Result

User	User Interface	Certificate Data	Blockchain Data Security	Revocation mechanism	Maintainability
A	8	6	8	7	5
B	9	6	8	6	6
C	7	7	9	7	4
D	7	7	8	7	5
E	8	6	7	6	5
F	8	8	8	8	4
G	8	6	8	6	5
H	9	7	9	7	3
I	7	6	9	6	4
J	7	7	8	7	4
Average Rating	0.78	0.66	0.82	0.67	0.45
Percentage	78%	66%	82%	67%	45%

Source: Authors, (2024).

The SWOT (strengths, weaknesses, opportunities, and threats) analysis of the BCVS is presented in Figure 11 below.

STRENGTHS	OPPORTUNITIES
• The utilization of blockchain guarantees that every certificate is unique, secure and permanent. This greatly helps to minimize the chances of certificate forgery. • The system simplifies the procedure of issuing and verifying certificates. The inclusion of QR code further helps improve accessibility.	• The current design is tailored for Olabisi Onabanjo University certification. However, there is an opportunity for adoption by other organizations. • Opportunity for integration with existing document verification systems in use by other institutions.
WEAKNESSES	**THREATS**
• BCVS is currently limited for verification of certificates from OOU generated from the system. • The security and functionality of the system is dependent on the blockchain platform used. • Maintenance of the system requires specialized knowledge of web3 technologies, which could serve as a barrier for administrators and developers in charge.	• Adoption of the BCVS may face resistance from institutions due to the technicality of blockchain systems, and reluctance to change from already existing processes. • Rapid advancements in technology could require new integrations to the system or else could potentially make the system obsolete. • Changes in regulation or policies related to data privacy and blockchain technology could impact the operation or viability of the system.

Figure 11: SWOT Analysis.
Source: Authors, (2024).

The BCVS focuses on certificate verification. It only inherently supports other documents if incorporated into the code base. The system's security fundamentally depends on the underlying blockchain platform, the hosting provider, and the database used for metadata storage. Therefore, any vulnerabilities or potential breaches in these areas could compromise the system's integrity.

IV. CONCLUSION

This project aims to develop an efficient and scalable certificate verification system for Olabisi Onabanjo University that can issue and verify certificates through the Celo blockchain platform. The system is designed to cater to university requirements and can revoke certificates. It represents an advancement in certificate verification, simplifying the process and improving the overall experience for everyone involved. The user evaluation result revealed an acceptance with a recommendation for regular maintenance.

The user's recommendations to improve BCVS include strengthening security measures, integrating additional document verification, and improving the user experience. As blockchain technology continues to advance, there are possibilities to improve the system's abilities and expand its usage to many other universities and industries besides Nigeria and Africa's education sector.

V. AUTHOR'S CONTRIBUTIONS

Conceptualization: Tolulope Ifeyemi, Ajibola Oyedeji and Fiyinfoluwa Adebiyi
Methodology: Tolulope Ifeyemi, Ajibola Oyedeji and Fiyinfoluwa Adebiyi
Investigation: Tolulope Ifeyemi, Ajibola Oyedeji and Fiyinfoluwa Adebiyi
Discussion of results: Tolulope Ifeyemi, Ajibola Oyedeji and Fiyinfoluwa Adebiyi
Writing: Tolulope Ifeyemi, Ajibola Oyedeji and Fiyinfoluwa Adebiyi
Supervision: Tolulope Ifeyemi, Ajibola Oyedeji and Fiyinfoluwa Adebiyi
Approval of the final text: Tolulope Ifeyemi, Ajibola Oyedeji and Fiyinfoluwa Adebiyi

VI. REFERENCES

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

[2] A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," *IEEE Access*, vol. 11. 2023, doi: 10.1109/ACCESS.2023.3289598.

[3] O. S. Saleh, O. Ghazali, and M. E. Rana, "Blockchain based framework for educational certificates verification," *Journal of Critical Reviews*, vol. 7, no. 3. 2020, doi: 10.31838/jcr.07.03.13.

[4] S. Pathak, V. Gupta, N. Malsa, A. Ghosh, and R. N. Shaw, "Blockchain-Based Academic Certificate Verification System—A Review," 2022, pp. 527–539.

[5] A. O. Oyedeji, O. Folorunsho, O. R. Abolade, and N. I. Eigbiremonlen, "Development of a web-based system for matching losers and finders of personal items," *Mindanao J. Sci. Technol.*, vol. 19, no. 1, pp. 293–306, 2021, doi: 10.61310/mndjsteect.1006.21.

[6] L. Zhang, L. Ci, Y. Wu, and B. Wiwatanapataphee, "The real estate time-stamping and registration system based on Ethereum blockchain," *Blockchain Res. Appl.*, vol. 5, no. 1, p. 100175, Mar. 2024, doi: 10.1016/j.bcra.2023.100175.

[7] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing," *Futur. Internet*, vol. 14, no. 11, p. 341, Nov. 2022, doi: 10.3390/fi14110341.

[8] A. Al Hussain, M. A. Emon, T. A. Tanna, R. I. Emon, and M. M. H. Onik, "A Systematic Literature Review of Blockchain Technology Adoption in Bangladesh," *Ann. Emerg. Technol. Comput.*, vol. 6, no. 1, pp. 1–30, Jan. 2022, doi: 10.33166/AETiC.2022.01.001.

[9] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in *2017 IEEE Technology & Engineering Management Conference (TEMSCON)*, Jun. 2017, pp. 137–141, doi: 10.1109/TEMSCON.2017.7998367.

[10] S. H. Ammous, "Blockchain Technology: What is it Good for?," *SSRN Electron. J.*, 2016, doi: 10.2139/ssrn.2832751.

[11] N. Malsa, V. Vyas, J. Gautam, A. Ghosh, and R. N. Shaw, "CERTbchain: A Step by Step Approach Towards Building A Blockchain based Distributed Appliaction for Certificate Verification System," in *2021 IEEE 6th International Conference on Computing, Communication and Automation (ICCCA)*, Dec. 2021, pp. 800–806, doi: 10.1109/ICCCA52192.2021.9666311.

[12] Y. C. Elloh Adja, B. Hammi, A. Serhrouchni, and S. Zeadally, "A blockchain-based certificate revocation management and status verification system," *Comput. Secur.*, vol. 104, p. 102209, May 2021, doi: 10.1016/j.cose.2021.102209.

[13] S. Pu and J. S. L. Lam, "The benefits of blockchain for digital certificates: A multiple case study analysis," *Technol. Soc.*, vol. 72, 2023, doi: 10.1016/j.techsoc.2022.102176.

[14] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telemat. Informatics*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.

[15] S. Alangari, S. M. Alshahrani, N. A. Khan, A. A. Alghamdi, J. Almalki, and W. Al Shehri, "Developing a blockchain-based digitally secured model for the educational sector in Saudi Arabia toward digital transformation," *PeerJ Comput. Sci.*, vol. 8, 2022, doi: 10.7717/PEERJ-CS.1120.

[16] T. Thakare, T. Phatak, G. Wadhani, T. Karotra, and R. L. Priya, "Verificate – Transforming Certificate Verification Using Blockchain Technology," *Signals Commun. Technol.*, vol. Part F2283, pp. 211–220, 2024, doi: 10.1007/978-3-031-49593-9_12.

[17] K. Kumutha and S. Jayalakshmi, "The Impact of the Blockchain on Academic Certificate Verification System-Review," *EAI Endorsed Trans. Energy Web*, p. 169426, Jul. 2018, doi: 10.4108/eai.29-4-2021.169426.

[18] A. O. Oyedeji, M. O. Osifeko, O. Folorunsho, O. R. Abolade, and O. O. Ade-Ikuesan, "Design and Implementation of a Medical Diagnostic Expert System," *J. Eng. Sci.*, vol. 10, no. 2, pp. 103–109, 2019, [Online]. Available: https://www2.kuet.ac.bd/JES/.

[19] cLabs, "Celo: A Multi-Asset Cryptographic Protocol for Decentralized Social Payments," 2018.

[20] H. Rawhouser *et al.*, "'Scaling, blockchain technology, and entrepreneurial opportunities in developing countries,'" *J. Bus. Ventur. Insights*, vol. 18, p. e00325, Nov. 2022, doi: 10.1016/j.jbvi.2022.e00325.

[21] K. Chodorow, "MongoDB: The Definitive Guide: Powerful and Scalable Data Storage," p. 432, 2013, [Online]. Available: https://books.google.co.uk/books?hl=en&lr=&id=uGUKiNkKRJ0C&oi=fnd&pg=PP1&dq=MongoDB&ots=h9mwLfcRAf&sig=JyYXcMiVgJ4rLC_FUvKE10fgwpA.