Blockchain Based Online Certificate Verification Portal: A Case for Telone Centre For Learning

Sam Masunda[1] Kudzi Loice Madzore[2] Silence Madondo[3]

[1]Electronics and Telecommunications, University of Zimbabwe,

[2]Telone Centre for Learning , National University of Science and Technology Zimbabwe

[3]Electronics and Telecommunications, University of Zimbabwe

Abstract

Academic certificate forgery is a growing concern, undermining trust in educational credentials. Traditional verification methods are often inefficient and vulnerable to fraud. This research explores blockchain technology's potential to revolutionize academic certificate verification at Telone Centre for Learning (TCFL). By leveraging blockchain's decentralized and immutable nature, a tamper-proof and transparent solution for managing and verifying educational credentials is proposed. The study reviews existing verification methods, analyses the advantages and challenges of blockchain-based approaches, and presents a prototype system demonstrating its feasibility. User testing confirms the system's effectiveness in accurate verification, user-friendliness, and performance, while also identifying areas for optimization. The research concludes by discussing future research directions and recommending the widespread adoption of blockchain in academic certificate verification to enhance security and efficiency in the educational ecosystem.

Key Words: Blockchain, Certificate, Verification, Cryptography, immutability

I. Introduction

Problem Statement

The increasing prevalence of academic certificate fraud poses a significant threat to the credibility and trustworthiness of educational credentials (Rustemi, et al., 2023). Traditional verification methods, often relying on manual processes and centralized databases, are susceptible to forgery and manipulation, making it difficult to validate the authenticity of qualifications (Sethia, et al., 2022). This not only exposes institutions like Telone Centre for Learning (TCFL) to potential risks associated with fraudulent interactions but also undermines the reputation of the institution and its graduates (Ahmed, et al., 2022). The lack of a standardized and globally recognized system for verifying academic credentials further exacerbates the issue, creating opportunities for fraudulent actors to exploit inconsistencies and loopholes. The current verification processes are often time-consuming, costly, and lack transparency, leading to delays and inefficiencies in verifying the authenticity of certificates (Gaikwad, et al., 2021). Additionally, graduates have limited control over their digital identities in traditional systems, making them vulnerable to data breaches and identity theft (Ahmed, et al., 2022). To address these challenges and enhance the security, efficiency, and transparency of academic certificate verification, exploring the potential of blockchain technology is crucial.

Research Objectives.

The following were the objectives of this research:

i. Explore blockchain's potential for secure issuance and verification of academic certificates.

ii. Review existing certificate verification systems and technologies.

iii. Identify and address challenges hindering blockchain adoption for diploma verification.

iv. Develop a real-time, blockchain-based system for accurate and immediate certificate verification.

Research Questions

i. How can blockchain technology be leveraged to enhance the security and efficiency of academic certificate verification processes at Telone Centre for Learning (TCFL)?

ii. What are the advantages and challenges of adopting blockchain-based approaches for academic certificate verification compared to existing methods?

iii. How does a prototype blockchain-based system for academic certificate verification perform in real-world testing, and what are the user experiences and feedback regarding its effectiveness?

II. Literature Review

In today's digital age, where information is easily accessible and manipulable, the verification of academic certificates has become increasingly crucial. Certificates are not only important documents for graduates but also serve as proof of their educational achievements. However, the current methods of certificate verification, such as contacting the issuing institution or relying on third-party verification services, are not without limitations. These methods are susceptible to security threats and human error, especially as the number of students and graduates continues to grow each year (Sethia, et al., 2022).

The use of blockchain technology for certificate verification is a promising solution to the issue of fake certificates (Sethia, et al., 2022). This technology provides secure storage and sharing of information, ensuring trust among users (Sethia, et al., 2022). It also offers a more efficient and secure digital certificate validation process (Gayathiri, et al., 2020). The use of Hyperledger Fabric in this context further enhances the tamper-proof and transparent nature of the system (Sethia, et al., 2022). The application of blockchain technology in academic certificate verification is beneficial, although it also presents some challenges. Despite these challenges, the use of blockchain technology in this context is a promising development (Kareem & Shakir, 2023). This paper delves into the transformative potential of blockchain technology for securely issuing and verifying academic certificates. While popularly associated with cryptocurrencies like Bitcoin, blockchain offers a fundamentally different paradigm: a decentralized and transparent ledger system for recording and verifying transactions with unparalleled security. By harnessing the inherent immutability and transparency of blockchain, we can envision a streamlined verification process that eliminates the need for intermediaries and significantly reduces the risk of fraudulent certificates (Gayathiri, et al., 2020).

This study embarks on a review of existing systems and technologies relevant to certificate verification, including online portals and emerging blockchain-based solutions. We will systematically analyse their advantages, limitations, and potential impact on the future of academic credential validation. By gaining a deeper understanding of these technologies and their transformative potential, we pave the way for a more secure, efficient, and trustworthy landscape for verifying academic certificates.

Numerous blockchain-enabled solutions have been proposed so far to achieve the goals of certificate verification and reduce the instances of false certificate forgeries. This section

provides a brief review of a couple of these. (Bahrami, et al., 2020)proposed a tamper-proof certificate verification system. The proposed system aims to fill these gaps by leveraging blockchain technology for decentralized verification. The challenges and gaps in the paper are the inefficiencies of traditional certificate verification methods in preventing fraud and the need for a more secure and robust system to address forgery and manipulation (Bahrami, et al., 2020).

Another proposal was given by (Gaikwad, et al., 2021). They argued that the process of verifying academic credentials can be completed in a matter of seconds instead of days with a blockchain-based verification system (Gaikwad, et al., 2021). They sought to address challenges in the lengthy document verification process, the significant overhead due to document transfer, and the need for an automated credential verification system.

In their work, (Tariq, et al., 2022)argued that traditional credential verification solutions are usually expensive, time consuming, and bureaucratic. The challenges and gaps (Tariq, et al., 2022) include the time consuming, costly, and bureaucratic nature of legacy credential verification systems, the detrimental effects of corruption in the education domain, the opacity and cumbersomeness of most credential verification mechanisms, the existence of loopholes for fraud and crime, and the nascent stage of interoperability protocols. The paper also suggests the need to devise integration solutions for Cerberus in a unified platform to explore new features and opportunities (Tariq, et al., 2022).

In their work, (Saleh, et al., 2020), postulated that the Hyperledger Fabric Framework is the foundation for a blockchain-based system for certifying educational credentials. The challenges and gaps in the paper include the complexity and tedious nature of document verification processes, the need for customized verification and authentication practices for diverse types of documents, the difficulty in detecting skilfully generated fake certificates, and the jeopardy to the credibility of document holders and issuing authorities due to the increase in forged documents. Their work explicitly mentions identifying gaps and loopholes in current blockchain based educational certificate verification solutions (Saleh, et al., 2020).

Another realization was made in research by (Gresch, et al., 2018), where they claimed the possibility of implementing a blockchain-based diploma management system. The challenges and gaps in the paper include the widespread issue of diploma fraud, the vulnerability of the current paper-based diploma system to fraud, the drawbacks of centralized database systems, and the need for strict regulation to prevent diploma falsification (Gresch, et al., 2018).

(Duwadi, 2021) systematically reviewed the literature on blockchain technology in education. The author defines blockchain technology and explains its key features, such as decentralization, immutability, and security. The paper also discusses potential applications of blockchain in education, including secure storage and verification of educational credentials, personalized learning, and incentivization of learning. The author identifies several challenges to the adoption of blockchain in education, including scalability, interoperability, lack of technical expertise, and cost. The author concludes by suggesting that future research should focus on addressing these challenges and exploring the potential of blockchain to transform education. A notable gap in this paper is the lack of empirical evidence to support the claims made about the potential benefits and challenges of blockchain in education. The author primarily relies on theoretical arguments and examples from other industries.

Research by (Rodrigues, et al., 2020)"A Technology-driven Overview on Blockchain-based Academic Certificate Handling," suggested that to accomplish the objectives of certificate verification and lower the frequency of false certificate forgeries, several blockchain-enabled solutions need to be adopted (Rodrigues, et al., 2020). The inefficiencies in confirming the legitimacy of certificates, the possibility of abusing this inefficiency, and the requirement to strike a balance between secrecy and transparency in blockchain-based solutions for certificate verification are among the difficulties and shortcomings in their work. Furthermore, the technical factors that impact the link between confidentiality and transparency are also emphasized, along with application needs like dependability and performance in comparison to blockchain features.

The challenge of adapting existing architectures in the context of implementing blockchain systems for higher education institutions is the difficulty of achieving automatic generation of diplomas without intermediaries and the lack of an existing public platform for HEIs that enables this process. The paper also acknowledges that while automatic generation is difficult, it is not impossible, and it emphasizes the need for further research to address this challenge. Overall, the paper suggests that adapting existing architectures to enable automatic generation of diplomas without intermediaries is a complex and unresolved issue in the field of blockchain technology for academic certificate verification (Rustemi, et al., 2023).They highlighted several obstacles to widespread adoption of blockchain technology for diploma verification. Automation of processes, the immutability of smart contracts, expensive maintenance, lack of training (knowledge), off chain transfer, big data management through blockchain systems, energy consumption, adaptability, and identity verification are some of these issues (Rustemi, et al., 2023)

III. Methodology

The methodology used in the study involves reviewing existing systems and technologies relevant to certificate verification, systematically analysing their advantages and limitations, identifying gaps in current blockchain-based educational certificate verification solutions, conducting tests to verify the core function of authenticating blockchain certificates, and gathering feedback from a sample of thirty-two users.

System Design

The primary goal of this proposal was to show that publishing certificates on the blockchain will enhance their legitimacy and benefit certificate issuers, holders, and other stakeholders. The process of verifying a physical certificate can be time consuming and laborious if the issuing organization is foreign, has ceased operations, or if the certificate is lost, damaged, or counterfeited. Given the high degree of cryptography in the blockchain, known as proof-ofwork, certificates on the suggested platform can no longer be forged. If the issuing entity ceases to exist, employers would no longer require a central point of authority to confirm the certificate's authenticity, making it easier for them to do so. A working prototype of the intended platform was created to validate this idea, enabling certificate-offering institutions to sign up and then issue certificates on the blockchain network. The proposed system architecture is shown in Figure 1, and the process flow diagram is shown in Figure 2.

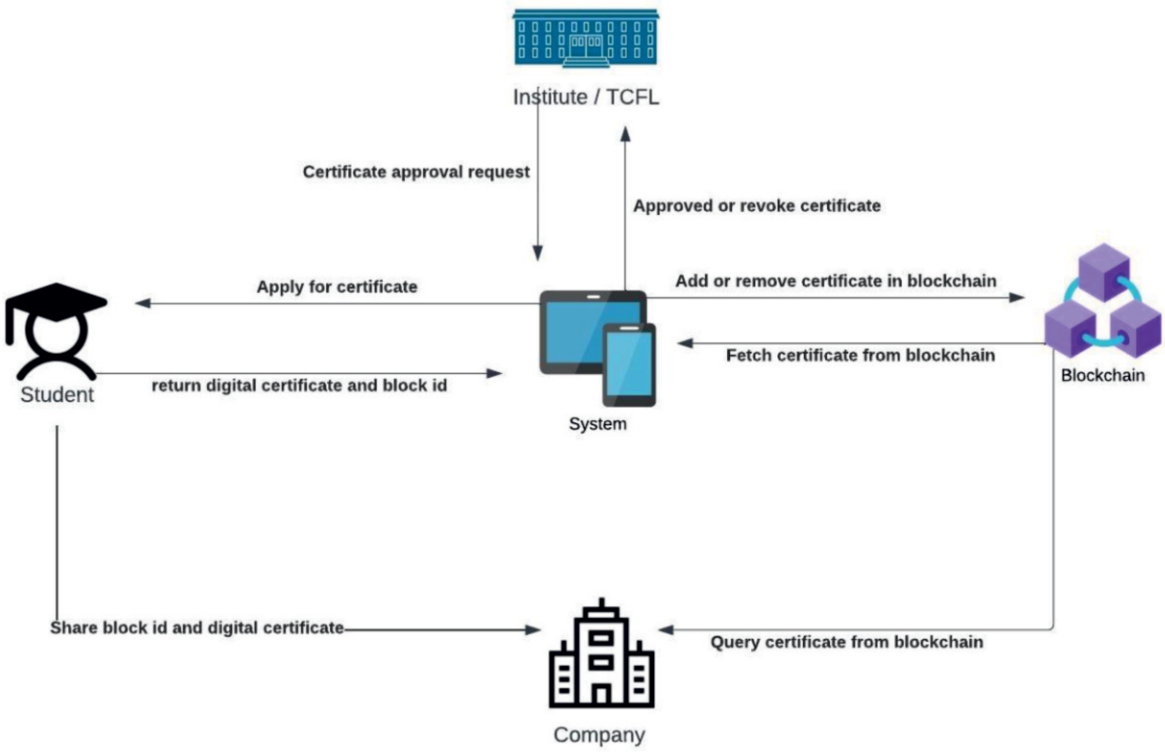

Figure 1 Proposed TCFL System Architecture

This enables issuers to register with them and issue certificates on the blockchain network.

According to Figure 1, in the proposed architecture, the institution (TCFL) creates a digital certificate and stores it on the blockchain. The recipient receives the certificate and can share it with others for verification purposes. The smart contract sends a request to one or more verification nodes on the blockchain network to verify the certificate's authenticity. Independent validation nodes leverage the immutable and distributed nature of the blockchain to verify the authenticity and integrity of the certificate. This process involves cross referencing the certificate against the issuer's digital signature and the historical record of the blockchain to ensure it has not been tampered with since its origination. Upon successful verification, a smart contract automatically appends a tamperproof record of this validation to the blockchain, ensuring transparency and accessibility for all authorized participants within the network. If any verification step fails, smart contract execution halts, preventing any modifications to the blockchain. Subsequently, an informative error message is generated and transmitted to the requesting party, detailing the specific point of failure encountered during the validation process.

System Flow Chart

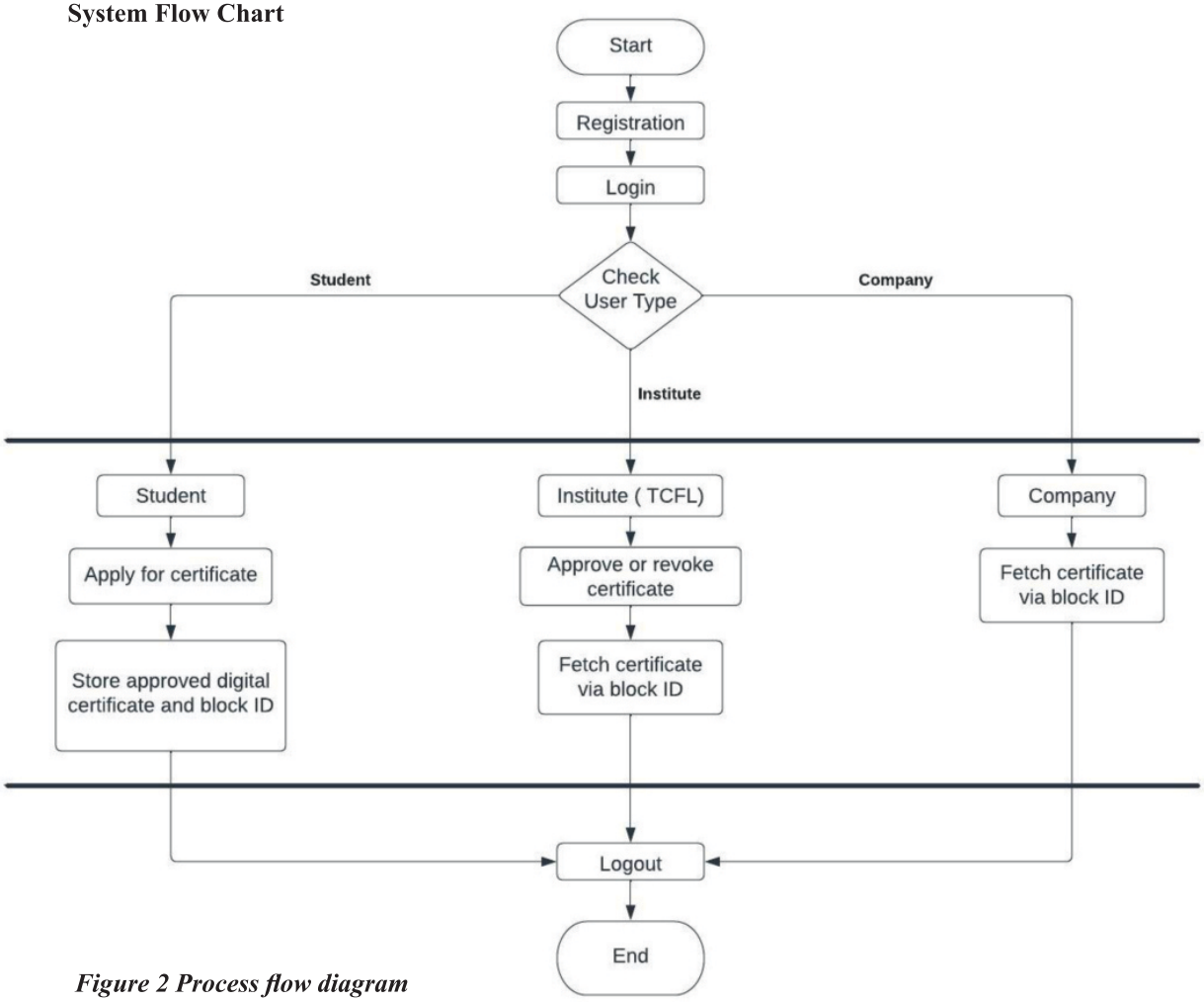

Figure 2 Process flow diagram

Figure 2 above shows the series of steps involved in blockchain verification that ensure the integrity and security of transactions on the blockchain network. To simulate the design, the prototype was made for three main roles: the institution, the student, and the company (third party). In this system, the first step is student registration. In this registration phase, students fill in the details and set the password for login. In the next step, students do the login with their credentials and then log into their account on the blockchain network using their private key. Depending on whether the user is a student, issuer, institution, or company, the user initiates a transaction by sending a request to the network. The graduate searches to verify if their certificates are the same as the ones in the institution's database. Their privileges also involve searching for and reprinting their certificates if the first one goes missing. The institution (TCFL) is the certificate issuer (administrator). The administrator, known as the issuer, has so many roles in the system, which include adding another admin, managing stored certificates, and entering the data on the date of issuance. An independent party (third party) acts as a gatekeeper, evaluating the employee's certificate for its validity and adherence to established criteria. The third-party privileges are only to verify whether a certificate is authentic or fake. Figure 3 is a graphical representation of actors, components, and the use case diagram.

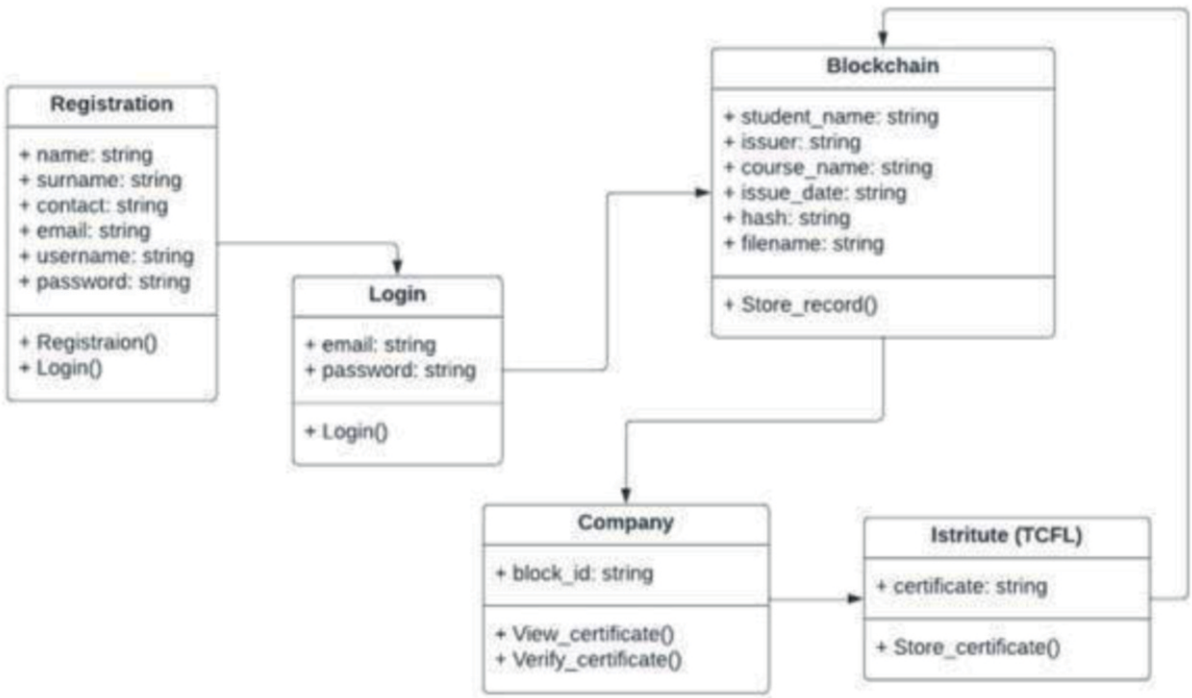

Figure 3 Proposed case diagram for the certificate verification at TCFL

VI. Findings and Results

Validation

The test successfully verified the system's core function: accurately authenticating blockchain certificates. By comparing document hashes, smart contracts flagged alterations, leading to 87.5% user approval. However, some desired verification beyond single pages suggests room for improvement. Additionally, security features like encryption passed rigorous testing, ensuring system protection.

Verification

The system demonstrably met its primary goal in this verification test. All thirty-two users confirmed that submitted certificates were processed swiftly and efficiently, with no reported delays or bottlenecks. This suggests the system can handle verification requests at scale without compromising performance.

User Friendliness

To assess the system's user-friendliness for students, companies, and administrators, we recruited thirty-two users who tested a total of sixty certificates including those that were not issued by Telone. Telone students ensured feedback directly addressed their needs, while experts from varying technical backgrounds found usability issues and learnability hurdles. Motivated volunteers rounded out the group, fostering a productive testing environment. By involving both novice and expert users, we aimed to uncover navigation difficulties, gauge the ease of learning, and guarantee a representative sample size. Testing covered key functionalities like certificate verification, issuance, and managing non-existent certificates. User feedback continuously refined the system, with final improvements ensuring intuitive functionality and a user-friendly interface for all stakeholders. This feedback prompted a comprehensive redesign to elevate the visual appeal and user experience.

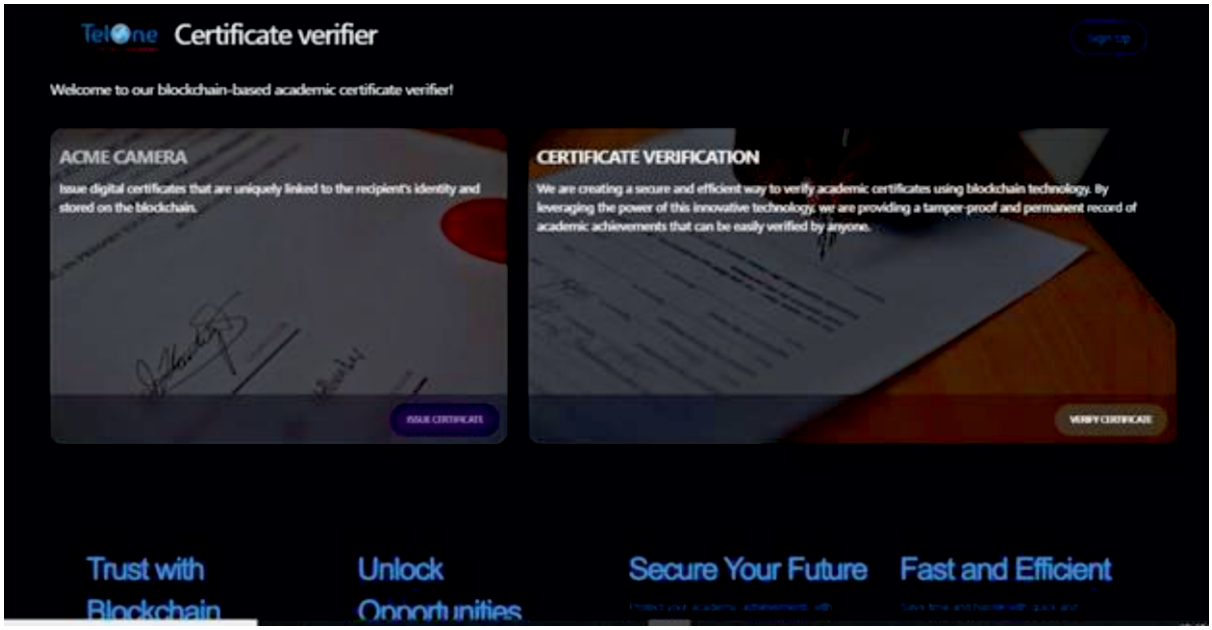

Figure 4 Final system outlook after the tests

Discussion of Results

Overall, the tests paint a promising picture of the system's potential while also highlighting crucial areas for improvement. Testing demonstrated the system's effectiveness in accurately verifying certificates (87.5% user approval), and some desired deeper verification for complex documents. User friendliness saw success with easy learning for 71.4%, but initial training could be enhanced for the remaining users. The appearance revamp is crucial, as 57.2% found it basic. Responsiveness needs optimization, with 28.6% experiencing slower speeds. Overall, the system shows promise, but addressing these areas will refine it for wider adoption and user satisfaction.

V. Conclusions and Recommendations

In conclusion, this research underscores the transformative potential of blockchain technology in revolutionizing academic certificate verification at Telone Centre for Learning (TCFL) and beyond. The prototype system's successful demonstration of secure issuance, efficient verification, and user-friendly interface highlights the feasibility and benefits of blockchain adoption in this domain. However, several challenges must be addressed to realize the full potential of this technology.

Future research should prioritize enhancing the system's interoperability with other educational institutions and credential verification platforms, ensuring seamless integration and broader acceptance. Exploring the automation of certificate issuance and revocation through smart contracts could further streamline processes and bolster security. Integrating Decentralized Identifiers (DIDs) would empower individuals with greater control over their academic credentials, facilitating secure and verifiable sharing across diverse platforms.

Addressing privacy concerns related to storing sensitive academic data on a blockchain is paramount. Implementing robust encryption and privacy-preserving mechanisms will be crucial to comply with data protection regulations and maintain user trust. Additionally, investigating the scalability of the blockchain solution to accommodate growing numbers of certificates and users is essential for long-term sustainability.

By tackling these challenges and incorporating the suggested future directions, blockchainbased academic certificate verification systems can evolve into a global standard, fostering trust, efficiency, and security in the educational ecosystem. The widespread adoption of such systems would not only mitigate fraud but also empower individuals by granting them ownership and control over their academic achievements, contributing to a more transparent and equitable educational landscape.

References

Ahmed, M. R., Islam, A. M., Shatabda, S. & Islam, S., 2022. Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey. *IEEE Access*.

Bahrami, M., Movahedian, A. & Deldari, A., 2020. *A comprehensive blockchain-based solution for academic certificates management using smart contracts.* s.l., IEEE.

Duwadi, N., 2021. A Systematic Review on Blockchain in Education: Opportunities and Challenges.. *Nepalese Journal of Management Science and Research 4.*

Gaikwad, H., D'Souza, N., Gupta, R. & Tripathy, A. K., 2021. *A blockchain-based verification system for academic certificates..* s.l., IEEE.

Gayathiri, A., Jayachitra, J. & Matilda, S., 2020. *Certificate validation using blockchain..* s.l., IEEE.

Gresch, J. et al., 2018. *The proposal of a blockchain-based architecture for transparent certificate handling..* s.l., Springer International Publishing.

Kareem, A. & Shakir, A., 2023. Verification Process of Academic Certificates Using Blockchain Technology.. *Kirkuk University Journal for Scientific Studies,* Volume 18.

Rodrigues, B. et al., 2020. A technology-driven overview on blockchain-based academic certificate handling.. *Blockchain Technology Applications in Education,* pp. 197-223.

Rustemi, A., Fisnik, D., Vladimir, A. & Aleksandar, R., 2023. A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification. *IEEE Access.*

Saleh, O. S., Ghazali, O. & Rana, M. E., 2020. Blockchain based framework for educational certificates verification.. *Journal of critical reviews* .

Sethia, G., Namratha, S., Srikanth, H. & Sreeja, C. S., 2022. *Academic certificate validation using blockchain technology..* s.l., IEEE.

Tariq, A., Haq, H. B. & Ali, S. T., 2022. Cerberus: A blockchain-based accreditation and degree verification system. *IEEE Transactions on Computational Social Systems 10*, pp. 1503-1514.