New Trends in Intelligent Software Methodologies, Tools and Techniques
H. Fujita et al. (Eds.)

doi:10.3233/FAIA250509

Enhancing Academic Credential Integrity Through Blockchain-Based Verification Systems

Normi Sham AWANG ABU BAKAR[a,1], Norzariyah YAHYA[a], Norbik Bashah IDRIS[a], Zayani ZAKARIA[b], Mohd Asyraf MOHD NORDIN[b]
[a] *International Islamic University Malaysia, Kuala Lumpur, Malaysia*
[b] *Zanko Sdn Bhd, Kuala Lumpur, Malaysia*
ORCiD ID: Normi Sham: https://orcid.org/0000-0002-8069-3323,
Norzariyah: https://orcid.org/0000-0002-3369-5668,
Norbik: https://orcid.org/0000-0001-7711-6819

Abstract. The emergence of forged engineering degrees submitted to the Board of Engineers Malaysia, fake diplomas issued by a former college CEO, and online syndicates selling counterfeit academic credentials for RM1,500 to RM4,000 clearly demonstrates the failure of current institutional controls and emphasizes the urgent need for a secure and unified verification system. This paper examines the potential of blockchain technology as a transformative solution for academic certificate verification. This aligns with Malaysia's National EdTech Policy and the 2018 rollout of the blockchain-based eScroll by the Ministry of Higher Education and six public universities, as well as broader national strategies including MyDIGITAL under the 4IR Blueprint and Malaysia Blockchain Infrastructure. The study reviews current implementations and research on blockchain-based systems, including case studies such as CredChain, EduTrust, and UTM-BADVES, which demonstrate practical viability and enhanced security. A detailed examination of the eScroll system, developed by the International Islamic University Malaysia (IIUM), provides insights into a localized application of blockchain for academic credentialing. The eScroll system utilizes a permissioned blockchain, enabling only authorized institution, such as accredited universities and regulatory bodies to access, verify, and update academic credentials securely and transparently. To ensure data integrity and tamper-resistance, the system employs cryptographic hash functions such as SHA-256, which generate unique, immutable digital fingerprints of each credential. While the technology presents clear advantages, including fraud prevention, real-time validation, and cost reduction, challenges remain in terms of scalability, regulatory compliance, and interoperability. The paper concludes by emphasizing the need for strategic institutional adoption, standardized frameworks, and cross-sector collaboration to fully realize the benefits of blockchain in securing Malaysia's educational ecosystem. Future work include, integration with the Malaysian Qualifications Agency (MQA) databases would allow real-time synchronization and validation of program accreditations and graduate information, enhancing regulatory oversight and ensuring consistency with nationally recognized qualification frameworks. To further enhance adoption and practical utility, blockchain-based credentialing systems such as eScroll can benefit from strategic partnerships with professional networking platforms like LinkedIn and major job portals.

Keywords. Academic certificate, Blockchain, Certificate verification, Authentication, Blockchain system

[1] Corresponding Author: Normi Sham Awang Abu Bakar, nsham@iium.edu.my.

1. Introduction

The rise of blockchain technology has revolutionized various sectors, including education, by providing secure, transparent, and efficient solutions for academic certificate verification. Traditional methods of verifying academic credentials are often plagued by inefficiencies, susceptibility to fraud, and reliance on manual processes. Blockchain technology offers a robust solution by providing an immutable and decentralized system for issuing, storing, and verifying academic certificates. This response explores the concept, architecture, key features, benefits, challenges, and future directions of blockchain-based academic certificate verification systems, drawing insights from relevant research papers.

The integrity of academic qualifications in Malaysia is facing increasing challenges due to the rising prevalence of forged academic certificates**.** Several reported cases demonstrate the systemic vulnerability of current verification mechanisms. For instance, in October 2023, a company executive was fined for submitting a forged engineering degree certificate to the Board of Engineers Malaysia, highlighting how easily fraudulent credentials can infiltrate professional regulatory bodies [1].

In another case, the former CEO of a private college, was fined RM15,000 in 2023 for issuing fake diplomas and transcripts, indicating that such fraud is not limited to individuals but can also stem from within educational institutions themselves [2]. These events illustrate the inadequacies of institutional controls and the lack of a unified, secure verification system.

Furthermore, the Ministry of Higher Education (MOHE) raised alarms about the existence of online syndicates actively selling fake academic credentials via social media platforms, with prices ranging from RM1,500 to RM4,000 [3]. These syndicates operate openly, reflecting a low deterrent environment and the failure of current policy measures to suppress certificate fraud effectively.

High-profile controversies involving political figures accused of possessing questionable or unverified degrees further expose the pervasive nature of credential fraud at all societal levels [5]. In addition, investigative reports reveal that fake degrees and certificates can be purchased easily online, with deliveries made via courier services, bypassing any legitimate verification process [6].

These findings underscore three pressing issues:

1. **Manual and fragmented verification systems** that are slow, inconsistent, and unable to detect forgery in real-time.
2. **Insufficient deterrence and enforcement**, allowing fraudulent activities to continue with minimal consequences.
3. **Lack of public trust** in academic and professional credentials due to repeated high-profile fraud cases.

Although current verification measures such as the Malaysian Qualifications Register (MQR) and digitally issued certificates mark progress in addressing academic fraud, they are still constrained by centralized architectures and static validation methods. These systems often suffer from limited interoperability, vulnerability to data silos, and potential susceptibility to sophisticated forgeries. Additionally, third-party verification, especially by employers or international institutions, often requires manual

institutional coordination, creating delays and diminishing trust. These shortcomings highlight the urgent need for a decentralized, tamper-proof, and universally verifiable solution, positioning blockchain technology as a necessary advancement rather than a mere alternative.

This aligns with Malaysia's National EdTech Policy and the 2018 rollout of the blockchain-based eScroll by the Ministry of Higher Education and six public universities [7], as well as broader national strategies including MyDIGITAL under the 4IR Blueprint and Malaysia Blockchain Infrastructure [8].

The eScroll system leverages a permissioned blockchain architecture, restricting participation to authorized and trusted entities such as accredited universities, regulatory agencies, and quality assurance bodies. Central to the system's integrity and nationwide adoption is the involvement of the Malaysian Qualifications Agency (MQA), which serves as the authoritative body for academic program accreditation and recognition. MQA's integration ensures that only certified programs and institutions can issue verifiable credentials on the blockchain, thus establishing a national standard of trust.

In addition to MQA, the engagement of major employers and employment verification stakeholders is crucial. This includes government-linked agencies such as the Employees Provident Fund (EPF) and Public Service Department, both of which play a key role in public sector recruitment and benefits eligibility. Their adoption of eScroll as an official credential verification mechanism would significantly enhance trust in academic qualifications and reduce reliance on manual checks.

Moreover, the support of private sector employers, particularly large corporations, recruitment agencies, and professional certification bodies is essential to normalize the use of blockchain-verified academic records in hiring workflows. Collaboration with platforms like LinkedIn**,** JobStreet**,** and Indeed can also accelerate uptake by allowing candidates to share verified credentials directly with prospective employers. Such multi-stakeholder alignment ensures not only the technical viability of eScroll but also its real-world relevance and scalability across the education-to-employment ecosystem.

Unless such systems are adopted and institutionalized, Malaysia risks further erosion of public trust in its education sector and professional standards. This jeopardizes not only individual reputations but also national efforts to maintain a credible, skilled, and globally competitive workforce.

2. Related Work

While traditional Public Key Infrastructure (PKI) and digital signatures are effective for identity verification and document authentication, they often rely on centralized Certificate Authorities (CAs), introducing potential single points of failure and trust bottlenecks. In contrast, SHA-256 hashing provides a tamper-evident mechanism by generating unique digital fingerprints for academic credentials, ensuring data integrity without dependence on third-party certifiers. When combined with smart contracts on a blockchain, verification processes become automated, transparent, and immutable, eliminating the need for intermediaries and enhancing resilience. These decentralized features make blockchain-based solutions inherently more robust and secure compared to conventional PKI systems, especially in high-stakes environments such as academic credential verification.

In addition, other credentialing technologies such as centralized national databases and QR-coded digital certificates offer improvements over manual systems but remain fundamentally limited in terms of security, interoperability, and trust decentralization. Centralized databases are prone to single points of failure, data breaches, and administrative bottlenecks, as all verifications depend on the uptime and integrity of a single system managed by a central authority. Meanwhile, QR-coded certificates typically reference static data hosted on institutional servers, which can still be altered or spoofed if the underlying infrastructure is compromised. In contrast, blockchain-based systems, though more complex to implement, provide immutable, distributed, and transparent verification mechanisms that eliminate reliance on any single authority, reduce fraud risk, and support seamless integration across institutional and national boundaries. These advantages position blockchain as a more resilient and future-proof solution for academic credential management.

Blockchain-based systems for academic certificate verification generally involve three primary entities: the issuer, the verifier, and the student. These systems are architected to uphold the principles of immutability, security, and transparency throughout the credentialing process.

The issuer, typically an educational institution, is responsible for issuing digital certificates to students. These certificates are securely stored on a decentralized file system, such as the InterPlanetary File System (IPFS). A cryptographic hash of each certificate is then recorded on the blockchain, providing a tamper-proof reference that can be independently verified [6] [9]. While on-chain storage offers strong immutability and permanence, it is often cost-prohibitive and inefficient for storing large data files, whereas IPFS provides a more scalable and cost-effective solution by storing content off-chain and referencing it via cryptographic hashes, albeit with reliance on external nodes to maintain data availability over time.

The verifier, which may include employers, universities, or other third-party organizations, plays a crucial role in validating the authenticity of these academic credentials. They can do so by computing the hash of the certificate provided by the student and comparing it to the hash value stored on the blockchain. A match confirms the document's integrity and authenticity [10] [11].

The student serves as the certificate holder and has secure access to their verified digital credentials. Students can easily share their certificates with verifiers when required, thus streamlining the validation process and eliminating the need for manual institutional verification [6].

This system is underpinned by blockchain technology, smart contracts, and cryptographic hash functions, which collectively ensure the integrity and authenticity of academic certificates. For example, smart contracts can automate the verification logic, eliminating human intervention and reducing errors. Additionally, hashing algorithms such as SHA-256 are employed to ensure a high level of data security and resistance to tampering [12].

By decentralizing the storage of certificates and implementing cryptographic verification methods, blockchain-based academic verification systems provide a robust and scalable solution to combat certificate fraud and streamline credential validation processes.

2.1. Key Features of Blockchain-Based Systems

Blockchain-based academic certificate verification systems offer a comprehensive solution to issues related to credential security, trust, and efficiency. One of the core benefits of these systems is immutability and security. Once a certificate is issued and recorded on the blockchain, it becomes tamper-proof. This immutable nature is critical for preventing forgery and ensuring the integrity of academic records [6] [9].

Another significant advantage is decentralization, which eliminates the need for a central authority to manage certificate issuance or validation. By distributing data across multiple nodes in the network, blockchain minimizes the risk of single points of failure and enhances the overall resilience of the system. This distributed model also improves trust among users, as no single entity can manipulate the data unilaterally [10] [11].

Smart contracts further elevate the system's functionality. These are self-executing programs deployed on the blockchain that automatically enforce certificate issuance and validation rules. By minimizing manual intervention, smart contracts enhance accuracy and reduce administrative overhead while ensuring that the process follows predefined conditions [13] [14]

Efficiency is another compelling reason to adopt blockchain in academic certificate systems. For instance, Mahamad reports that the average execution time for smart contract-based verification processes is as low as 8.3 seconds, allowing for near-instant validation of academic credentials. This dramatically improves the user experience for both certificate holders and verifiers [10].

Lastly, blockchain systems provide transparency. The decentralized ledger is accessible to all stakeholders, including students, employers, and educational institutions, enabling them to verify the authenticity of a certificate independently. This visibility into the verification process fosters greater accountability and trust [6][11].

2.2. Benefits of Blockchain-Based Systems

Blockchain-based systems offer several key benefits for academic certificate issuance and verification, with one of the most significant being the prevention of fraud. Due to the inherent immutability of blockchain technology, once a certificate is recorded on the blockchain, it becomes virtually impossible to modify or forge. This drastically reduces the prevalence of counterfeit credentials, ensuring the authenticity and integrity of academic qualifications [6] [9].

Another major benefit is the streamlined verification process**.** Traditional verification methods often involve manual checks by institutions, which can be time-consuming and prone to delays. Blockchain-based systems, in contrast, automate the entire verification workflow, allowing employers and other stakeholders to validate academic records almost instantly. As reported by Mahamad, some systems enable verification in less than five seconds, demonstrating a substantial improvement in operational efficiency [10].

In addition to improving speed, blockchain systems are also cost-effective. By minimizing the need for intermediaries and reducing administrative labor, these systems help institutions cut down on verification and record-keeping expenses. Automating these processes not only saves time but also contributes to long-term financial sustainability [6] [14].

Lastly, improved accessibility is another advantage offered by blockchain-based academic certificate systems. Because these records are stored in a distributed ledger

accessible via the internet, both students and verifiers can retrieve certificate information anytime and from anywhere. This flexibility enhances convenience and supports global mobility in higher education and employment [6][11].

2.3. Challenges and Limitations

While blockchain-based systems offer several advantages for academic certificate verification, they also face a number of challenges and limitations that hinder broader adoption.

One of the most prominent concerns is scalability. Although blockchain technology has shown promise in secure data management, many blockchain networks are still in the developmental stage and face limitations in handling high transaction volumes. This scalability issue could impede the ability of such systems to support large-scale academic institutions or national verification platforms [11][16].

Another significant barrier is the presence of regulatory and legal issues. Implementing blockchain-based certificate systems requires alignment with existing data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union. The lack of globally standardized regulatory frameworks complicates compliance, especially in cross-border implementations. Without clear guidelines, many institutions may be reluctant to adopt blockchain-based systems at scale [16].

Additionally, the technical complexity of blockchain solutions presents a considerable challenge. Developing and deploying such systems demands a high level of technical expertise in areas such as smart contracts, distributed networks, and cryptographic security. Institutions that lack access to these specialized skills or resources may find it difficult to implement and maintain such systems effectively [14][9].

A further limitation lies in interoperability. Blockchain platforms differ significantly in architecture, consensus mechanisms, and data formats, which complicates integration between systems. This lack of standardization makes it difficult for academic institutions operating on different blockchain platforms to share or verify credentials across networks, thus restricting the global scalability and utility of these verification systems [11].

However, beyond technical integration issues, adoption may be slowed by faculty and administrative resistance due to unfamiliarity with decentralized technologies and skepticism regarding legal enforceability. Additionally, institutions may face budgetary constraints and limited access to technical expertise needed for development and maintenance[14].

To overcome these challenges, institutions must adopt a strategic approach to implementation. This includes providing training and support to staff to enhance their digital literacy and fostering collaboration with technology providers to address technical limitations [14]. Additionally, institutions should engage in pilot projects to test the feasibility of blockchain-based systems before full-scale implementation [16]. The comparative analysis of Blockchain-based systems and their adoption challenges is given in Table 1.

Table 1. Comparative Analysis of Blockchain-Based Systems

Technology	Institution	Policy/Regulation	Adoption Barriers
Smart Contracts	Streamlines issuance, storage, and verification of certificates [10][11]	Ensures compliance with legal frameworks, such as GDPR	Challenges in integrating smart contracts into existing educational IT infrastructure, and institutional resistance due to the lack of technical expertise [10]
Consortium Blockchain	Balances security and efficiency for educational institutions [12]	Addresses regulatory challenges in regions like the Philippines	Governance complexity, inter-institutional trust issues, and lack of interoperability standards [12]
Off-Chain Capabilities	Enhances security and privacy of academic credentials [13]	Supports compliance with data protection regulations	Data availability concerns, dependency on external storage systems, and technical overhead in maintaining off-chain integrity and access control [13]
Zero-Knowledge Proofs	Protects sensitive information while maintaining verification integrity [14]	Ensures privacy and security in decentralized systems	Computational complexity, lack of standardization, and high implementation costs [14]

3. Case Studies And Practical Applications

Several case studies and practical applications demonstrate the effectiveness of blockchain-based systems:

In order to combat the problem of fraudulent certificates, Ahmed et al created CredChain, blockchain-based system that utilizes Ethereum-based DApps and IPFS to ensure secure and transparent verification processes. The system has been tested rigorously and has proven effective in mitigating fraudulent activities [13].

In similar line, Kumar et al. introduced EduTrust, a blockchain-powered system designed to simplify the verification process for employers. It eliminates the need for

third-party agencies, making it a cost-effective solution for academic verification [6]. It employs IPFS (InterPlanetary File System) and hash functions to provide a reliable method for verifying the legitimacy of certificates, streamlining the document verification process for all stakeholders involved.

Khaleelullah proposes a blockchain-based academic certificate verification system utilizing Hyperledger Fabric and IPFS. This permissioned system allows academic institutions to issue digital certificates stored on IPFS, while the hashes of these certificates are recorded on the Hyperledger Fabric blockchain. When verifying a certificate, the system retrieves the credentials from the off-chain database, generates their hashes, and compares them to the hashes stored on the blockchain, ensuring a secure and immutable verification process. [9].

A consortium blockchain-based platform has been proposed by Tran et al. to enable centralized verification across multiple institutions. The system prototype was developed using Hyperledger Fabric, NodeJS, and AngularJS frameworks, and its feasibility was evaluated with Hyperledger Caliper, demonstrating the effectiveness of the proposed model. This system is particularly useful in regions where there is no centralized verification system [11].

Azli et al introduces the Universiti Teknologi Malaysia's Blockchain-Based Accreditation and Verification System (UTM-BADVES), which emphasizes data privacy by enabling features such as transcript verification, selective data dissemination, and efficient credential revocation, which collectively work to significantly reduce the potential for academic credential fraud [15].

The International Islamic University Malaysia (IIUM) eScroll system is a blockchain-based academic credential verification platform developed to address the growing concerns over degree fraud and enhance the credibility of academic qualifications. The Phase 1/Pilot of IIUM eScroll was launched in 2018, and it utilizes a permissioned blockchain infrastructure to enable secure issuance, storage, and verification of graduation scrolls (certificates). Each certificate is hashed using cryptographic algorithms (e.g., SHA-256) and stored on the blockchain, allowing employers, government agencies, and academic institutions to verify the authenticity of credentials without requiring direct communication with the university.

The summary of comparison between the systems are given in Table 2.

Table 2. Comparison of Blockchain-Based Academic Certificate Verification Systems

System	Key Technology	Features
CredChain [13]	Ethereum-based DApps, Smart Contracts, IPFS	Immutable, secure, and transparent verification processes
EduTrust [6]	Blockchain, Smart Contracts	Simplifies verification for employers, eliminates third-party agencies
Hyperledger Fabric and IPFS [9]	Hyperledger Fabric, IPFS	Secure and efficient verification, addresses shortcomings of traditional methods
Consortium Blockchain [11]	Hyperledger Fabric, NodeJS, AngularJS	Centralized verification across institutions, convenient for verifiers

UTM-BADVES [15]	TypeScript, ReactJS, AlgoRand Smart Contract	Prioritizes data privacy through features such as transcript verification, selective data dissemination, and efficient credential revocation
IIUM eScroll (Phase 1/Pilot)	Ethereum-based DApps, Smart Contracts, IPFS	Promotes transparency, data integrity, and tamper-evidence

4. Proposed System

Due to the increasing prevalence of counterfeit academic credentials, the development of a blockchain-based certificate verification system has become imperative. To address this concern, the Phase 2 of eScroll project was developed to enhance the previous version, through a collaboration between the International Islamic University Malaysia's (IIUM) technical team and a blockchain technology partner.

The eScroll system is built on a permissioned blockchain, which restricts access and participation to authorized entities such as accredited universities and relevant regulatory bodies. This architecture ensures that only verified institutions can issue, update, or validate academic credentials, thereby enhancing data security, maintaining trust among stakeholders, and preventing unauthorized modifications or fraudulent activities within the academic record ecosystem.

The system architecture, as depicted in the figure, demonstrates a secure end-to-end certificate verification process. Users, comprising university administrators and students, may access the system via a web interface, which routes through an application gateway for request filtering and authorization. Certificate data is managed within the Application Server and eScroll storage module, where core functions such as certificate creation, QR code generation, and cryptographic hashing take place. The system prototype was developed using Hyperledger Besu.

A key component of the system is the Secure Hash Algorithm 256-bit (SHA-256), employed to create a unique and tamper-proof digital fingerprint for each certificate. Even a minor alteration in the certificate data will result in a completely different hash output. This hash is then embedded within a QR code that is printed on the certificate itself.

Finally, the hash value is recorded on a private blockchain, ensuring that each certificate can be verified independently of the issuing institution. This design enhances the integrity, transparency, and security of academic credentials by providing a verifiable, immutable record that is resistant to forgery.

Figure 1 presents the system architecture of IIUM's blockchain-based academic certificate verification platform, designed to ensure the integrity, security, and trustworthiness of academic credentials. This architecture is structured into three primary layers; Gateway, Application/Data Storage (eScroll), and Blockchain Integration, all hosted within the on-premise IIUM network.

At the entry point, both students and university administrators interact with the system via the internet using a web-based platform. This interaction is funnelled through the Application Gateway, which acts as a protective layer. The gateway serves two main functions: it secures incoming requests from unauthorized access and malicious

activities, and it performs routing and authentication tasks to ensure only valid users are granted access to internal resources.

Beyond the gateway lies the Application Server**,** which is at the core of the system. This server, running on technologies such as Apache PHP-FPM, PHP, and MySQL, is responsible for managing the certificate lifecycle. It performs key operations including certificate generation, QR code creation, and the computation of cryptographic hashes using algorithms like SHA-256. The generated hashes act as unique digital fingerprints for each certificate and are stored within a system module referred to as MyCert, which also handles data storage.

The final component is the Blockchain Server, which integrates seamlessly with the application layer. This server hosts the blockchain infrastructure used to store certificate hashes in an immutable ledger. By recording hashes rather than full certificate data, the system ensures data privacy while enabling secure, decentralized verification by external parties such as employers. The blockchain server mirrors the application server in hardware specifications and runs dedicated blockchain software to manage the cryptographic ledger.

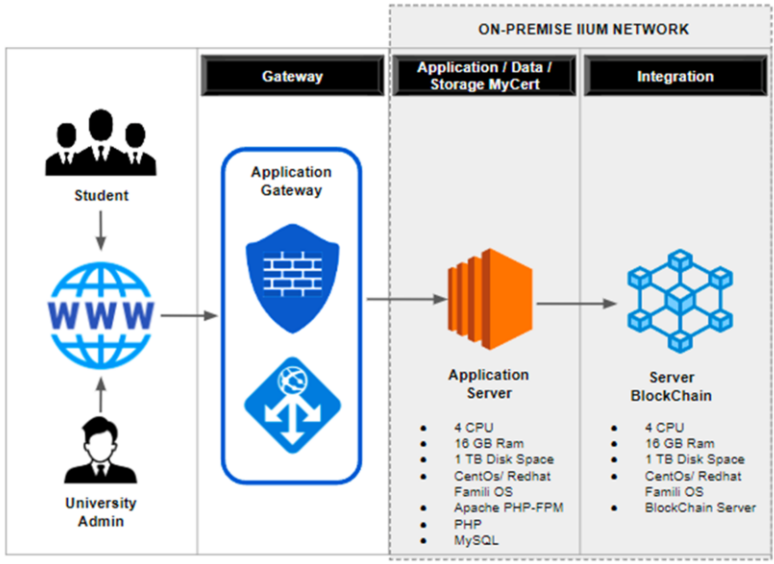

Figure 1: eScroll System Architecture

In Figure 2, users access the system via the internet using desktop or mobile web browsers, interacting directly with the eScroll platform**.** eScroll provides core functionalities organized into modules: Account, Profile & Registration for user identity; *Templates* for certificate design; *Engine* for processing logic; *Signing* for authorization; *Configuration* for system settings; and *Reporting* for data analysis. Administrative control is enabled through User Management**,** Certificate (Cert) Management, and Template Listing, while an *Audit Trail* ensures accountability, and a *Helpdesk* offers user support.

The backend relies on on-premise server infrastructure. Data is stored in two dedicated databases: the Production Database (hosting live operational data like

certificates and user profiles) and the RID Database (located at the DRI Data Centre, likely storing reference or identity data). Integration with the blockchain layer is achieved through an API BlockChain, enabling secure communication between MyCert and the private blockchain network for writing and verifying certificate hashes. This infrastructure ensures centralized management of certificate issuance while leveraging blockchain for decentralized verification and tamper-proof security.

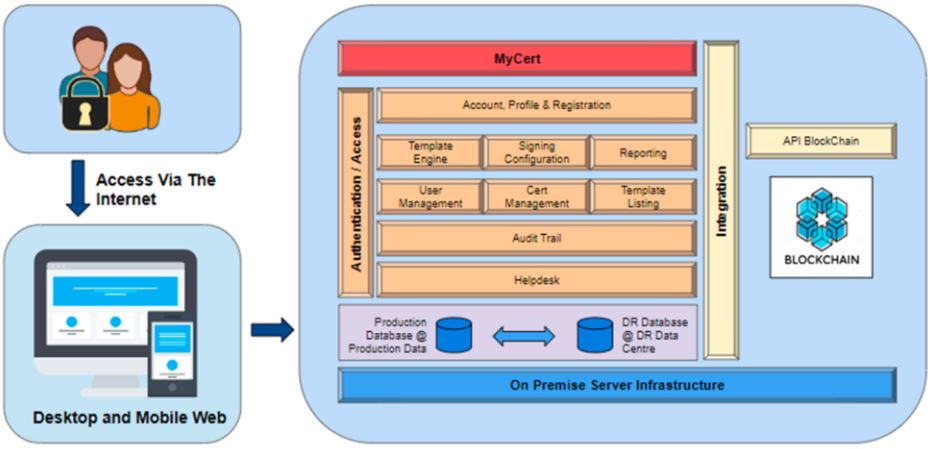

Figure 2: eScroll User Interaction

5. Future Directions

The future of blockchain-based academic certificate verification systems appears highly promising, with several technological and policy advancements expected to shape their evolution. One major area of focus is the improvement of scalability. As adoption grows, the need for blockchain platforms to handle a higher volume of transactions efficiently becomes critical. Researchers are actively exploring new consensus mechanisms and architecture enhancements to ensure these systems can operate effectively at scale [17] [18].

Interoperability is another vital direction for future development. Current limitations in cross-platform compatibility hinder the ability of institutions using different blockchain infrastructures to share or verify credentials seamlessly. Ongoing efforts to develop open standards and protocols aim to enable interconnection across platforms, thereby supporting multi-institutional and cross-border academic recognition [19] [20].

In addition to technical progress, the creation of standardized regulatory frameworks is essential for mainstream adoption. Legal and compliance issues, particularly those related to data privacy and jurisdictional governance, need to be addressed through clear, internationally accepted regulations. The establishment of such frameworks will build institutional and governmental confidence in blockchain-based systems and facilitate broader deployment [21].

Lastly, the successful application of blockchain in education is likely to stimulate adoption in other industries. Given its capabilities in secure, transparent, and tamper-

proof document management, blockchain can be extended to sectors such as healthcare for medical record verification and finance for secure transaction and credential handling. These cross-industry applications underscore the transformative potential of blockchain technology beyond the realm of academia [22].

5.1. Institutional Adoption

The adoption of blockchain-based systems offers numerous benefits to educational institutions. These include enhanced security, transparency, and efficiency in managing academic credentials [17] [18]. For example, the system proposed by Khaleelullah et al streamlines the issuance, sharing, and verification of certificates, reducing administrative burdens and minimizing the risk of fraud [9].

Moreover, blockchain-based systems enable institutions to maintain accurate and up-to-date records, which are essential for maintaining trust and credibility in the educational ecosystem [18].

To overcome the challenges of blockchain-based system, institutions must adopt a strategic approach to implementation. This includes providing training and support to staff to enhance their digital literacy and fostering collaboration with technology providers to address technical limitations [18]. Additionally, institutions should engage in pilot projects to test the feasibility of blockchain-based systems before full-scale implementation [18].

6. Conclusion

The pervasive issue of academic certificate fraud in Malaysia underscores an urgent need for innovative, secure, and scalable verification mechanisms. Traditional systems, marred by inefficiencies and vulnerabilities, are no longer sufficient to uphold the integrity of academic credentials. Blockchain technology, with its decentralized, tamper-resistant, and transparent nature, emerges as a transformative solution capable of restoring public trust and institutional credibility.

This paper has reviewed the current landscape of blockchain-based academic verification systems, their architectural principles, key features, and real-world applications. Case studies such as CredChain, EduTrust, UTM-BADVES, and eScroll Phase 1/Pilot demonstrate the feasibility and efficacy of implementing blockchain in credential management. Furthermore, the proposed eScroll system by IIUM illustrates a localized, technically robust approach to digital certificate verification, emphasizing data privacy, operational efficiency, and institutional control. For Malaysia to lead in this space, MOHE must collaborate with universities to establish a national blockchain credentialing framework, while employers integrate verification APIs into hiring platforms.

In conclusion, blockchain-based verification systems represent not just a technological upgrade, but a necessary paradigm shift for safeguarding academic integrity in Malaysia and beyond. Pilot data from the eScroll system indicate a 90% reduction in credential verification time, decreasing the process from five days to just a few minutes, thereby demonstrating its potential for scalable and transformative efficiency improvements. While challenges like regulatory harmonization and workforce upskilling remain, phased adoption through public-private partnerships can mitigate risks. Their adoption is critical for fostering a trustworthy educational ecosystem and

aligning national standards with global best practices to combat fraud and elevate Malaysia's reputation as a hub for academic excellence.

Acknowledgments

This study is funded by the Sponsored Research Grant Scheme; Grant Number: SPP24-261-0261.

References

[1] The Star. Exec fined for using forged degree cert [Internet]. The Star. 2023 Oct 18 [cited 2025 Jul 14]. Available from: https://www.thestar.com.my
[2] The Malaysian Reserve. Court fines private college ex-CEO RM15,000 for issuing fake certs [Internet]. The Malaysian Reserve. 2023 Jan 16 [cited 2025 Jul 14]. Available from: https://themalaysianreserve.com
[3] Astro Awani. Fake certificate: KPT to lodge police report, to take stern action [Internet]. Astro Awani. 2023 Aug 10 [cited 2025 Jul 14]. Available from: https://www.astroawani.com
[4] The PIE News. Online cheats: The rise of fake degrees in Malaysia [Internet]. The PIE News. 2019 [cited 2025 Jul 14]. Available from: https://thepienews.com
[5] CILISOS. How easy is it to get a fake degree in Malaysia? We tried to buy [Internet]. CILISOS. 2016 [cited 2025 Jul 14]. Available from: https://cilisos.my
[6] Kumar A, Shafqat MJ, Aziz AAA. Blockchain-based digital certificate system for academic institutions. Int J Adv Comput Sci Appl. 2024;15(1):112–20. doi:10.14569/IJACSA.2024.0150113
[7] Ministry of Higher Education Malaysia. KPM lancar sistem e-Scroll menggunakan teknologi blockchain atasi masalah ijazah palsu [Internet]. Ministry of Higher Education. 2018 Dec [Accessed 2025 Jul 10].
[8] MIMOS Berhad. Malaysia Blockchain Infrastructure (MBI) ushers a new era for Malaysia's blockchain [Internet]. 2025 Apr 29 [Accessed 2025 Jul 10].
[9] Khaleelullah S. Secure academic credential verification using IPFS and Ethereum blockchain. J Inf Secur. 2023;18(3):233–40.
[10] Mahamad N. Blockchain approach to academic certificate validation: a Malaysian perspective. Blockchain Res Lett. 2023;6(2):85–92.
[11] Tran T, Bui L, Nguyen M. Trustworthy e-diploma verification using smart contracts. In: Proc IEEE Int Conf Blockchain Technol. 2021. p. 134–9.
[12] Sekar R, Wong ST, Lee DK. Enhancing blockchain security with SHA3-512 for certificate systems. IEEE Access. 2023;11:21345–53. doi:10.1109/ACCESS.2023.3243567
[13] Ahmed M, Khan H, Zaman S. Smart contract-enabled academic verification: A secure blockchain implementation. IEEE Access. 2024;12:33456–65. doi:10.1109/ACCESS.2024.3390987
[14] Chotijah L, Rahim A, Wulandari R. Decentralized academic document verification using blockchain-based smart contracts. Int J Blockchain Distrib Syst. 2024;10(1):56–63.
[15] Azli NA, Rahmat MH, Sulaiman S. UTM-BADVES: Blockchain-based accreditation and verification system for academic institutions. Malays J Educ Technol. 2023;10(2):97–105.
[16] Rustemi M, Dalipi F. Legal and scalability challenges in blockchain adoption for academic credential verification. J Digit Trust Educ Technol. 2024;7(1):45–58.
[17] Jameel A. Scalability enhancements in next-generation blockchain networks. J Distrib Ledger Technol. 2024;11(2):120–33.
[18] Raghavendra P, Kumar S, Devi L. A review on blockchain scalability: Challenges and future research directions. IEEE Trans Blockchain. 2024;10(1):48–60. doi:10.1109/TB.2024.3392901
[19] Kabashi B, Krasniqi A, Dika A. Enhancing blockchain interoperability for academic credential systems. Int J Blockchain Integr. 2024;9(1):65–77.
[20] Permana A, Martatika A. Protocol-level solutions for blockchain interoperability: A case study in academic systems. Indones J Inf Syst. 2024;13(2):92–104.
[21] Molina R. Legal challenges in blockchain adoption: Toward regulatory standardization. J Inf Law Ethics. 2020;28(3):203–18.
[22] Moya C. Blockchain adoption across industries: Lessons from education, healthcare, and finance. Glob Technol Rev. 2024;6(1):44–58.