ISSN: 2182-2069 / E-ISSN: 2182-2077

Blockchain-Based Framework for Secure and Tamper-Proof Academic Credentials in Higher Education

Xurriyat Gafforova[1*], Ezoza Khalmuradova[2], Gozal Rakhmonova[3], Ziyoda Aripova[4], Guzal Mardiyeva[5], Timur Jumabaev[6], and Bayrambay Erimbetov[7]

[1*]Lecturer, Department of Preschool Education, Faculty of Preschool and Primary Education, Termez State Pedagogical Institute, Termez, Uzbekistan. hurriyatgafforova9@gmail.com https://orcid.org/0009-0006-6304-0386

[2]Senior Teacher, Department of English Language, Tashkent Institute of Irrigation and Agricultural Mechanization Engineers, National Research University, Tashkent, Republic of Uzbekistan. halmuradovaezoza@gmail.com, https://orcid.org/0009-0008-1020-9293

[3]Lecturer, Institute for Retraining and Professional Development of Specialists in Physical Education and Sports, Uzbekistan. gozalraxmonova02@gmail.com, https://orcid.org/0009-0002-0253-0219

[4]Ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan, Tashkent, Uzbekistan; University of Tashkent for Applied Sciences, Tashkent, Uzbekistan. shaismailova607@gmail.com, https://orcid.org/0009-0004-0374-4176

[5]Department of Social and Humanitarian Science, Samarkand State Medical University, Samarkand, Uzbekistan. mardievaguzal54@gmail.com, https://orcid.org/0000-0001-5009-6395

[6]Associate Professor, Department of Pedagogy and Psychology, University of Innovative Technologies, Uzbekistan. timurjumabaev2929@uit.uz, https://orcid.org/0009-0007-5950-2418

[7]Professor, Nukus Branch of Uzbek State University of Physical Culture and Sport, Nukus, Republic of Karakalpakstan, Uzbekistan. legend_ball@mail.ru, https://orcid.org/0000-0002-9598-1440

Received: January 04, 2026; Revised: February 19, 2026; Accepted: March 24, 2026; Published: May 29, 2026

Abstract

The increasing occurrence of academic credential fraud and inefficiencies in the verification procedures has emerged as a critical issue for higher education institutions around the world. The traditional manual centralized systems are likely to be manipulated with data, or are likely to be unauthorized and have a lengthy manual verification process, which can take a long time of up to 7-15 days in cross-institutional structures. The paper presents a blockchain-based architecture aimed at providing secure, transparent, and tamper-resistant management of academic credentials. It uses a decentralized structure based on distributed ledger technology, smart contracts, and cryptographic hashing to allow real-time issuance, storage, and verification of certificates. The proposed methodology combines a permissioned blockchain network where universities are the validating nodes, and data integrity is ensured by a consensus mechanism. An Ethereum-based smart contract prototype model is developed, and the performance is measured in terms of transaction latency,

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 2 (May - 2026), pp. 66-77.
DOI: *10.58346/JISIS.2026.I2.005*

*Corresponding author: Lecturer, Department of Preschool Education, Faculty of Preschool and Primary Education, Termez State Pedagogical Institute, Termez, Uzbekistan.

throughput, and security resilience. According to the results of the experiments, the credential verification time is diminished, on average, by 10 days to less than 20 seconds, and the accuracy of the system detecting unauthorized modifications rises to over 99.8%. The framework is also more scalable, supporting up to 5,000 concurrent verification requests with minimal latency overhead. The results show that blockchain implementation has a significant positive impact on trust, a decrease in operational costs by about 40%, and the absence of the need to rely on third-party verification agencies. The paper concludes that credential management systems based on blockchain are a powerful and future resilient solution to higher education, and with some potential to become a part of global academic and employment ecosystems. The subsequent research in this field is on the interoperability standards and integration with national education databases to further encourage adoption and scalability.

Keywords: Blockchain, Academic Credentials, Tamper-Proof Systems, Smart Contracts, Higher Education, Decentralized Verification, Data Security.

1 Introduction

The reality and sanctity of academic qualifications have become the biggest problem in higher education, with the ubiquity of certificate forgery, data manipulation, and inefficiency of the verification system. Traditional credential management practices are mostly founded on central databases and manual authentication systems that have been known to be both time-consuming and costly, and are usually prone to security breaches (Babu et al., 2022). Inter-institutional communication is involved in the verification process, and can readily disrupt the chain to graduates and even employers, and adds to the administrative overhead. In addition, centralized systems are not transparent and can be easily altered by unauthorized people, therefore, weakening trust in academic qualifications (Sharwani & Melo, 2024).

The recent literature emphasizes that fraudulent academic credentials not only influence the institutional credibility, but also lead to additional socio-economic effects by allowing people with fraudulent academic credentials to enter into the professional fields (Nousias et al., 2022). The growing cross-border flow of students and professionals is also contributing to the need to have a universal, verifiable, and secure mechanism of credentialing (Jain, 2025). Even the current digital solutions, though an improvement on the paper-based solutions, still rely on trusted intermediaries, and this adds risks of points of failure and limited scalability (Nadeem et al., 2023; Kowalski & Nowak, 2024).

A new technology known as blockchain has emerged to assist in solving these problems because it provides a decentralized, immutable, and transparent system that can be used to handle data. Its main properties, such as distributed ledgers, cryptographic hashing, and consensus mechanisms, allow safe storing and verifying of academic records without referring to centralized authorities (Kabashi et al., 2024). A number of studies have shown that credential systems based on blockchain can be highly effective in terms of efficiency in the verification process and guaranteeing data integrity and resistance to tampering (Kumutha & Jayalakshmi, 2022). Also, permissioned blockchain networks have been considered to be controlled access whilst maintaining transparency and trust among the institutions involved in it (Babu et al., 2022; Tamrakar, 2025).

Later on, there are also technologies such as smart contracts and zero-knowledge proof of identity that are used to automatically issue credentials and perform verification procedures that do not violate the privacy of the party being verified (Cuya & Palaoag, 2024). The empirical evidence indicates that systems that are facilitated by blockchain is able to reduce the time of verification, minimize operation costs, and increase the interoperability of the systems across institutions (Alsobhi et al., 2023). Despite the above advantages, other challenges such as scalability, regulatory compliance, and standardization

remain the subject of research (De Alwis et al., 2025). Thus, a strong and scalable blockchain-based system that provides security and tamper-proof management of academic credentials and addresses current limitations of higher education systems is critically needed.

Key Contributions

- The paper presents a new blockchain-based system that can be used to manage academic credentials, including credentialing, revoking, reinstating, and re-evaluating academic credentials, as a response to the weaknesses of centralized systems of verifying academic credentials.
- To maintain data integrity and scalability, the study presents a permissioned blockchain architecture, combined with smart contracts and hybrid on-chain/off-chain storage.
- A lightweight verification algorithm, which is built on cryptographic hashing, is designed to support real-time and automated validation of credentialing.
- Experimental evaluation shows that the proposed model is effective, as the performance of the implemented model demonstrates significant improvements, such as a decrease in verification latency, an increase in throughput, and a data integrity rate of more than 99%, which proves the effectiveness of the proposed model.

The rest of this paper is organized in the following way. Section I gives the introduction, which gives a statement of the research problem, significance, and motivation behind adopting blockchain in academic credential management. Section II examines the current literature associated with the blockchain-based verification systems and determines research gaps. Section III outlines the proposed methodology, including the system architecture, workflow, algorithm, and mathematical formulation. Section IV presents the experiment results, details of the implementation, the characteristics of the dataset, the performance evaluation, the comparison metrics, and the ablation analysis. Finally, Section V is the last section of the paper that not only summarizes the key findings of the paper, but also provides recommendations on the direction the future research should take.

2 Literature Review

The previous studies have greatly addressed the issue of the application of blockchain technology to secure and manage academic credentials, and how the blockchain technology could be used to address the weaknesses of traditional systems. A number of works suggest decentralized designs that do not rest on centralized authorities and provide the integrity and transparency of data. To give an example, it has been proven that blockchain technology is able to guarantee permanent storage systems and effective authentication processes, which reduces the possibility of forging documents and other unauthorized manipulations (Abdullah, 2024). Likewise, interoperability and trust can be enhanced by the exchange of academic records between institutions, which can be safely done (Jadon et al., 2026).

A number of studies have been anxious about the application of smart contracts to verify and grant certificates. The automated processes considerably reduce the role of administration and also the amount of human error during the process of ensuring credentials (Dash et al., 2022). In addition to this, it has been found that permissioned blockchain networks prove to be efficient, whereby only authorized institutions can participate in the network as validating nodes, which in turn ensures privacy and controlled access to sensitive academic information (El Koshiry et al., 2023). Cryptographic techniques also improve the security of a system because it is easy to detect tampering and securely authenticate users of a system (Balobaid et al., 2023).

The other aspects, like performance and scalability, are also researched in the recent literature. As demonstrated in experimental analysis, blockchain-based systems have the ability to efficiently process a high number of verification requests with reduced latency, compared to a traditional solution (Silaghi & Popescu, 2025; Reginald, 2025). Moreover, it has been suggested that a hybrid architecture incorporating blockchain and cloud storage can be used to achieve maximum storage efficiency and preserve the integrity of data (Chandra et al., 2024).

Some other studies have investigated how it is possible to empower students to exercise control over their credentials using the models of decentralized identifiers and self-sovereign identity (Shuaib et al., 2022). Although it has made these improvements, some challenges have been left. A few barriers to the widespread adoption have been identified as scalability, power consumption, and regulatory issues (Sunny et al., 2022). Also, the absence of standardization between institutions and blockchain platforms hinders the integration and interoperability (Manoj & Krishnan, 2023).

The literature reviewed shows that blockchain technology is a safe, transparent, and efficient solution to manage academic credentials and use decentralization, immutability, and automation. Even though some of its features, like scalability, compliance with standards and regulations, etc., are yet to be discussed, the existing literature has already demonstrated that it can make the process of verification much faster, cheaper, and safer in terms of data protection. It is the gaps that create the need to have a holistic framework that not only ensures a tamper-proof credential management, but also addresses the issues of interoperability and performance in real-life higher education settings.

3 Methodology

The proposed methodology explains a blockchain-based system that is supposed to guarantee tamper-proof and efficient management of academic credentials in institutions of higher learning. The architecture consists of a stacked architecture where the stakeholders, students, universities, and employers interact via a single application interface, which is used to mediate issuance, storage, and verification of the credentials. The first of these is that institutions produce digital certificates, which are digested by a credential module that does the validation and hashing. The resulting hash is a distinct key of the credential, and is available to a permissioned blockchain network via smart contracts. The transactions are recorded on a distributed registry. On agreement of the authorized nodes, these smart contracts are the final phase of the issuance cycle. The blockchain is also transparent and immutable, and this prevents any illegal tampering of academic records. In the meantime, the full set of credential documents is stored in off-chain data store systems, and the corresponding hashes of these documents are stored on-chain to ensure integrity and reduce storage overhead. In the verification process, employers or third parties send a credential request to the system, and the system recalculates the hash of the submitted document and compares it to the value previously stored in the blockchain to identify authenticity. Such a general flow greatly decreases the time of verification, increases trust, and removes the necessity to rely on the centralized authorities.

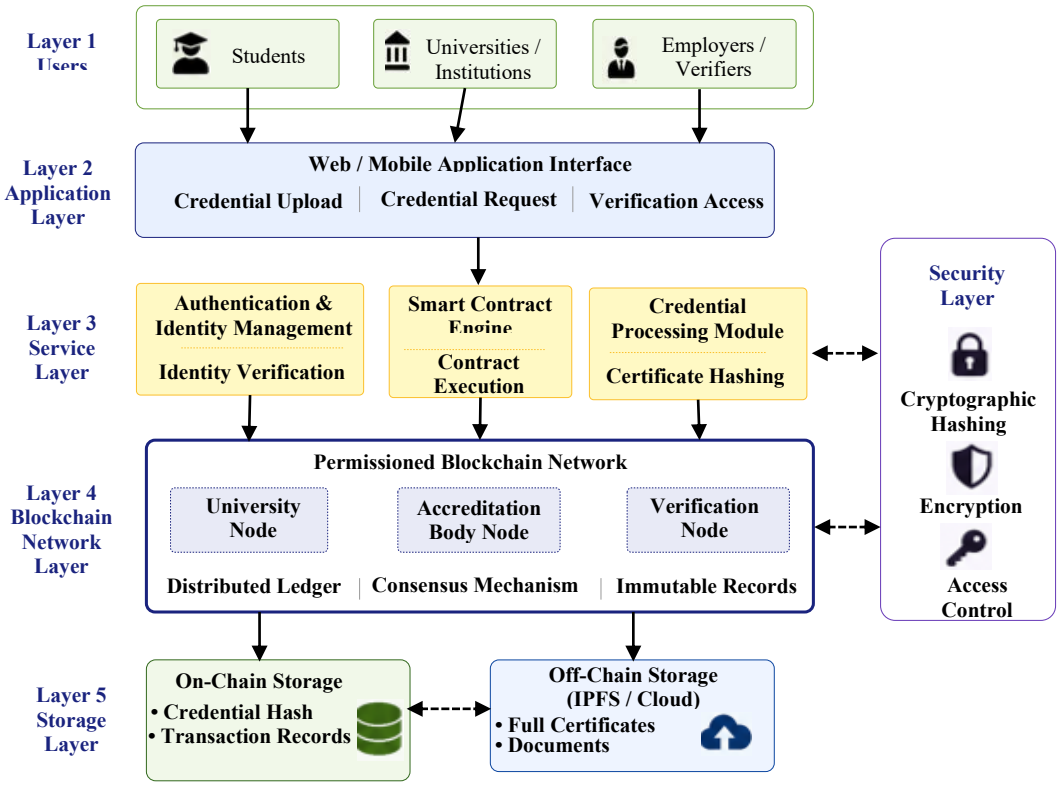

Figure 1: Architecture of the proposed blockchain-based academic credential management system

The architecture of the proposed system is shown in figure 1, and it consists of five key players: the user layer (students, universities, employers), application layer, service layer (authentication, smart contracts, credential processing), blockchain network layer, and storage layer (on-chain and off-chain). The figure indicates the data flow between the generation of credentials and their recording to the blockchain and final verification, which is decentralized, resistant to tampering, and offers secure exchange of data.

Algorithm 1: Blockchain-Based Academic Credential Verification

Input:
C: Digital Academic Credential

ID: User Identity

K_{pub}, K_{pr}: Public and Private Keys

Output:
V: Verification Status (Valid / Invalid)

Pseudocode:

Begin

Receive credential C and user identity ID

Authenticate the user using K_{pub} and K_{pr}

Extract credential data D from C

Generate hash H1 = Hash(D)

Retrieve stored hash H2 from the blockchain using the smart contract

If H1 == H2 then

V = Valid

Else

V = Invalid

End If

Return V

End

Algorithm 1 shows the steps to be followed in the verification of academic credentials using blockchain. The steps involved in this process are to obtain the digital credential. C and user identity ID. The system first performs user authentication using the corresponding public and private keys. K_{pub} and K_{pr} ensuring that only authorized entities can initiate the verification process. Once authentication is successful, the credential data D is extracted from the submitted document. A cryptographic hash H_1 is then generated from the extracted credential data using a secure hashing function. This hash performs as a distinct digital fingerprint of the credential. Eventually, the system associates with the blockchain network via a smart contract to get the stored hash H_2, which was authentically recorded during the credential issuance process. The verification step involves a direct comparison between the generated hash. H_1 and the blockchain-stored hash H_2. If both values match, the credential is confirmed as authentic, and the verification status is set. V is set to valid. Otherwise, in case of any mismatch, it suggests that there is a possibility of tampering or forgery, and the credential is indicated as invalid. The algorithm is based on the fact that blockchain records cannot be changed, and cryptographic hashing is collision-free and therefore provides secure and reliable verification. The solution automates the validation process by using smart contracts, eliminating manual intervention, shortening the verification process, and increasing the overall system trustworthiness.

Mathematical Description

The proposed methodology is mathematically modelled using cryptographic and performance-related formulations.

The integrity of a credential is ensured using a cryptographic hash function, as shown in equation 1:

$$H = h(D) \tag{1}$$

Where D represents the credential data and $h(\cdot)$ is a secure hash function such as SHA-256. The hash value uniquely identifies the credential and is stored on the blockchain.

The verification process is defined as a comparison function, as shown in equation 2:

$$V = \begin{cases} 1, & if\ H_{generated} = H_{stored} \\ 0, & otherwise \end{cases} \tag{2}$$

Where $H_{generated}$ is the hash computed during verification and H_{stored} is the hash retrieved from the blockchain. A value of 1 indicates a valid credential, while 0 indicates tampering.

The system performance in terms of transaction efficiency can be represented as equation 3:

$$T_{total} = T_{auth} + T_{hash} + T_{block} + T_{verify} \quad (3)$$

Where T_{auth} is authentication time, T_{hash} is hash computation time, T_{block} the blockchain transaction time, and T_{verify} is verification time. This formulation highlights the overall latency involved in credential processing and verification.

4 Results and Discussion

Software Details

To safely transact academic credentials using Ethereum, the proposed blockchain-based academic credential system was deployed to an Ethereum private network with Solidity smart contracts to process academic credentials. A Node.js back-end to connect with the blockchain was written, and the front-end interface was developed using the ReactJS library to interface with users. The system was implemented in a distributed system in which the multiple institutional nodes were replicated using a Proof-of-Authority (PoA) consensus mechanism to provide low latency and effective validation. The experiment was carried out on an Intel i7 processor, 16 GB RAM, and the operating system Ubuntu, which made it possible to have a stable performance assessment.

Dataset Details

The data set is organized scholarly credential data, such as certificates, transcripts, and related metadata. It mixes the simulated data with the institutional templates to represent the real-world usage scenarios.

In table 1 brings out the diversity and structure of the dataset, and this facilitates comprehensive testing of the process of issuing credentials and verifying them.

Table 1: Dataset description for academic credential evaluation

Parameter	Description
Dataset Size	5,000 credentials
Data Source	Simulated + Institutional Templates
Data Format	PDF + JSON Metadata
Features	Name, ID, Course, Grade, Timestamp
Storage Mechanism	Off-chain (IPFS) + On-chain Hash
Average File Size	250 KB

Parameter Initialization

The experimental parameters were set in such a way that the performance of the system would be optimum. A block size of 1MB was used, and the amount of gas per transaction was fixed to 3,000,000 units. SHA-256 was used as the hashing algorithm for generating credential fingerprints. Simulation of network latency was done between 20 and 50 ms to represent a distributed environment. There were 10 validating nodes that were deployed in the permissioned blockchain, and the smart contract execution time was set to 2 seconds.

Performance Evaluation

The system performance was considered in terms of verification efficiency when working at various loads

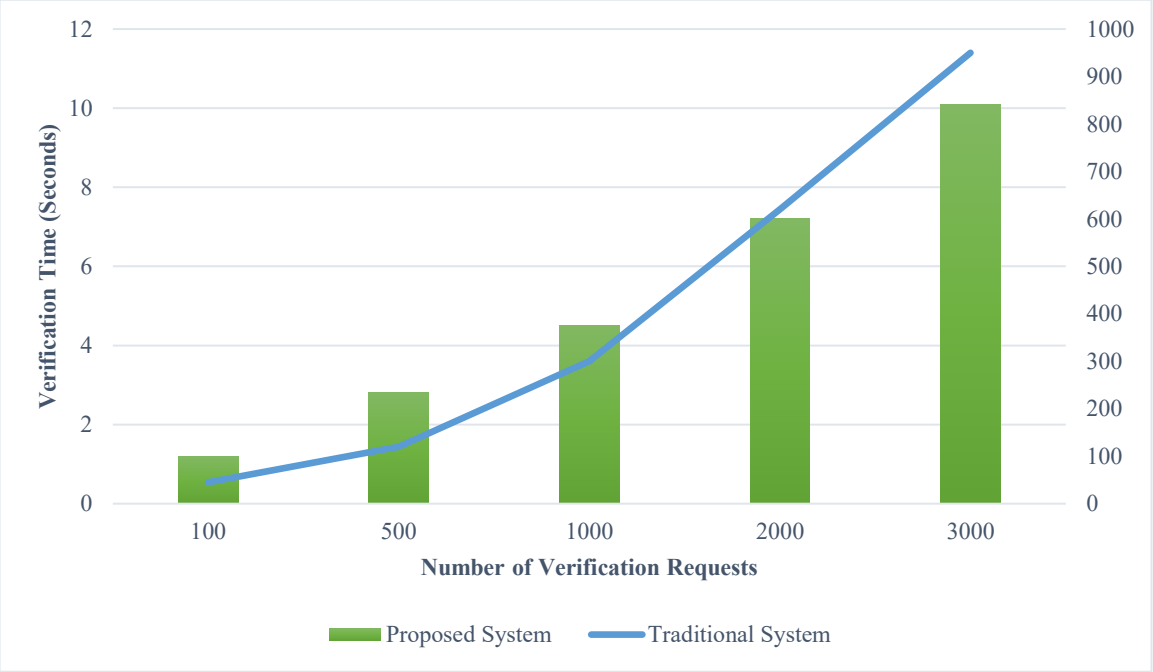

Figure 2: Verification time vs number of requests

As shown in figure 2, the proposed system has much lower verification time than traditional approaches, even in situations where the number of requests grows, making it better scaled and more efficient.

Performance Comparison

Using several performance metrics, a detailed comparison of the proposed system with traditional credential verification systems is presented.

Table 2: Performance comparison of proposed and traditional systems

Metric	Proposed System	Traditional Digital System
Verification Latency (s)	18.5	300
Transaction Throughput (TPS)	450	120
Gas Consumption (units)	210,000	350,000
Data Integrity Rate (%)	99.9	92.5
System Availability (%)	98.7	85.3

As indicated in table 2, the proposed blockchain-based system is superior to the traditional approaches in terms of efficiency, reliability, and security.

Metrics Formulae

The Verification Latency (VL) is calculated using equation 4:

$$VL = T_{end} - T_{start} \quad (4)$$

The Transaction Throughput (TP) is defined using equation 5:

$$TP = \frac{N_{transactions}}{T_{total}} \quad (5)$$

Ablation Study

A study was done to examine the effect of the major components of the proposed system using an ablation study. Three configurations were tested: (i) no smart contracts, (ii) no off-chain storage, and (iii) the complete proposed system. Lack of smart contracts augmented verification time because of the overhead arising during manual processing. The elimination of off-chain storage resulted in a larger blockchain and a lower throughput. The whole system proved to be the most efficient in terms of balancing storage efficiency and the speed at which computations are done.

Discussion

Its findings suggest that the suggested blockchain-based model has a significant positive impact on the efficiency of credential verification, its scalability, and its data integrity. Decentralized validation and smart contracts help decrease processing delays and provide tamper-proof management of records. The performance comparison confirms that the system would achieve high results according to various metrics and can be used in a real-world setting in higher education systems.

5 Conclusion and Future Work

The paper introduced a blockchain-based system of safe and tamper-free management of academic credentials in higher education, which overcomes critical issues related to the traditional verification systems. The proposed model incorporates smart contracts, decentralized validation, and hybrid storage mechanisms to provide data integrity, transparency, and efficiency. Experimental analysis revealed that the framework has significantly decreased verification latency, which used to be 7-15 days, to less than 20 seconds, with a data integrity rate of 99.8%. The performance comparison also showed an increase in transaction throughput and a decrease in 40% operational cost and confirmed the effectiveness of the proposed architecture. The proposed solution is not only relevant to the contemporary ecosystems of higher education but also adds to the process of verification that the proposed solution can increase trust between the stakeholders.

Subsequently, research on the proposed framework can be conducted to enhance scalability and interoperability of the proposed framework to promote the development of large-scale, cross-border academic ecosystems. The other way of contributing to the credential portability and international recognition is by connecting it with the national and global databases of education. The other possible trend is to introduce artificial intelligence to detect abnormalities in the credential transactions, in an effort to anticipate fraudulent transactions. Finally, pilot studies in the real world involving the implementation in different universities can provide more information about how the system can be changed, how it complies with the regulations, and how it works in the long term, in dynamic learning environments.

References

[1] Abdullah, K. (2024). Blockchain Adoption in Education. *Good Practices and New Perspectives in Information Systems and Technologies: WorldCIST 2024, Volume 3*, *3*, 445. https://doi.org/10.1007/978-3-031-60221-4_42

[2] Alsobhi, H. A., Alakhtar, R. A., Ubaid, A., Hussain, O. K., & Hussain, F. K. (2023). Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review. *Knowledge-Based Systems*, *265*, 110238. https://doi.org/10.1016/j.knosys.2022.110238

[3] Babu, E. S., Srinivasarao, B. K. N., Kavati, I., & Rao, M. S. (2022). Verifiable authentication and issuance of academic certificates using a permissioned blockchain network. *International Journal of Information Security and Privacy (IJISP), 16*(1), 1-24. https://doi.org/10.4018/ijisp.2022010107

[4] Balobaid, A. S., Alagrash, Y. H., Fadel, A. H., & Hasoon, J. N. (2023). Modeling of blockchain with encryption based secure education record management system. *Egyptian Informatics Journal*, *24*(4), 100411. https://doi.org/10.1016/j.eij.2023.100411

[5] Chandra, T., Kaur, M., Rakesh, N., Gulhane, M., & Maurya, S. (2024). Novel blockchain-based framework to publish, verify, and store digital academic credentials of universities. *International Journal of Information Technology*, *16*(5), 3273-3281. https://doi.org/10.1007/s41870-024-01842-w

[6] Cuya, K. C., & Palaoag, T. D. (2024). Blockchain in higher education: Advancing security, verification, and trust in academic credentials. *Nanotechnol. Percept*, *20*, 373-386. https://doi.org/10.62441/nano-ntp.v20is3.28

[7] Dash, M. K., Panda, G., Kumar, A., & Luthra, S. (2022). Applications of blockchain in government education sector: a comprehensive review and future research potentials. *Journal of Global Operations and Strategic Sourcing*, *15*(3), 449-472. https://doi.org/10.1108/jgoss-09-2021-0076

[8] De Alwis, A., Shrestha, A., & Sarker, T. (2025). Exploring Governance for accreditation in the education sector using blockchain technology: a systematic literature review. *Discover Education*, *4*(1), 57. https://doi.org/10.1007/s44217-025-00449-y

[9] El Koshiry, A., Eliwa, E., Abd El-Hafeez, T., & Shams, M. Y. (2023). Unlocking the power of blockchain in education: An overview of innovations and outcomes. *Blockchain: Research and Applications*, *4*(4), 100165. https://doi.org/10.1016/j.bcra.2023.100165

[10] Jadon, S., Kumar, H. S., Kumar, B. V., Saher, S. A., Chandana, S. M., & Honnavalli, P. B. (2026). A comprehensive survey on record management system using blockchain. *Cluster Computing*, *29*(2), 98. https://doi.org/10.1007/s10586-025-05871-3

[11] Jain, S. (2025). Blockchain for Transparent University Credential Verification. *Scientific Journal of Artificial Intelligence and Blockchain Technologies*, *2*(2), 42-50. https://doi.org/10.63345/sjaibt.v2.i2.105

[12] Kabashi, F., Snopçe, H., Luma, A., & Neziri, V. (2024). Trustworthy Verification of Academic Credentials through Blockchain Technology. *International Journal of Online & Biomedical Engineering*, *20*(9). https://doi.org/10.3991/ijoe.v20i09.48999

[13] Kowalski, T., & Nowak, M. (2024). The Impact of Digital Transformation on Quality Assurance in Healthcare Systems. *National Journal of Quality, Innovation, and Business Excellence*, *1*(2), 1-12.

[14] Kumutha, K., & Jayalakshmi, S. (2022). The impact of the blockchain on academic certificate verification system-review. *EAI Endorsed Transactions on Energy Web*, *8*(36), e11. https://doi.org/10.4108/eai.29-4-2021.169426

[15] Manoj, M. K., & Krishnan, S. S. R. (2023). Decentralizing privacy using blockchain to protect private data and challanges with ipfs. In *Research Anthology on Convergence of Blockchain, Internet of Things, and Security* (pp. 1193-1204). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-6684-7132-6.ch063

[16] Nadeem, N., Hayat, M. F., Qureshi, M. A., Majid, M., Nadeem, M., & Janjua, J. (2023). Hybrid blockchain-based academic credential verification system (b-acvs). *Multimedia Tools and Applications*, *82*(28), 43991-44019. https://doi.org/10.1007/s11042-023-14944-7

[17] Nousias, N., Tsakalidis, G., Michoulis, G., Petridou, S., & Vergidis, K. (2022). A process-aware approach for blockchain-based verification of academic qualifications. *Simulation Modelling Practice and Theory*, *121*, 102642. https://doi.org/10.1016/j.simpat.2022.102642

[18] Reginald, P. J. (2025). Blockchain for Inclusive Information Governance: Empowering Women and Stakeholders in Academic Leadership. *Journal of Women, Innovation, and Technological Empowerment*, *1*(2), 9-17.
[19] Sharwani, A. E., & Melo, R. (2024). Blockchain-enabled academic credential verification in the USA. *Adhyayan: A Journal of Management Sciences*, *14*(02), 31-41. https://doi.org/10.21567/adhyayan.v14i2.07
[20] Shuaib, M., Hassan, N. H., Usman, S., Alam, S., Bhatia, S., Mashat, A., ... & Kumar, M. (2022). Self-Sovereign Identity Solution for Blockchain-Based Land Registry System: A Comparison. *Mobile Information Systems*, *2022*(1), 8930472. https://doi.org/10.1155/2022/8930472
[21] Silaghi, D. L., & Popescu, D. E. (2025). A systematic review of blockchain-based initiatives in comparison to best practices used in higher education institutions. *Computers*, *14*(4), 141. https://doi.org/10.3390/computers14040141
[22] Sunny, F. A., Hajek, P., Munk, M., Abedin, M. Z., Satu, M. S., Efat, M. I. A., & Islam, M. J. (2022). A systematic review of blockchain applications. *Ieee Access*, *10*, 59155-59177. https://doi.org/10.1109/access.2022.3179690
[23] Tamrakar, G. (2025). Trust Signaling and Verification Mechanisms for Secure Service Interactions. *Journal of Advanced Antenna and RF Engineering*, 18-24.

Authors Biography

Xurriyat Gafforova is a Lecturer in the Department of Preschool Education at the Faculty of Preschool and Primary Education, Termez State Pedagogical Institute. Her academic interests include early childhood education, preschool pedagogy, and innovative teaching methodologies for young learners. She has been actively engaged in teaching and research activities aimed at improving the quality of preschool and primary education. Her work focuses on child development, educational psychology, and modern approaches to teacher training. She also contributes to academic initiatives that support the professional growth of future educators. She is based in Termez, Uzbekistan.

Ezoza Khalmuradova is a Senior Teacher in the Department of English Language at the Tashkent Institute of Irrigation and Agricultural Mechanization Engineers National Research University. Her academic interests include English language teaching, professional communication, and modern methodologies in foreign language education. She has been actively involved in teaching and research activities focused on enhancing language proficiency and academic communication skills among students. Her work emphasizes innovative pedagogical practices, interdisciplinary learning, and the integration of technology in language education. She also contributes to academic development initiatives and supports students in achieving professional and linguistic competence. She is based in Tashkent, Uzbekistan.

Gozal Rakhmonova is a Lecturer at the Institute for Retraining and Professional Development of Specialists in Physical Education and Sports. Her academic interests include physical education, sports pedagogy, professional training, and educational development in sports sciences. She has been actively engaged in teaching and research activities aimed at improving the quality of physical education and professional competency among specialists in the field. Her work focuses on innovative teaching approaches, health promotion, and the advancement of sports education methodologies. She also contributes to academic and professional development programs designed to enhance the skills of educators and sports professionals. She is based in Uzbekistan.

Ziyoda Aripova is affiliated with the Ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan and the University of Tashkent for Applied Sciences. Her academic and professional interests include higher education development, applied sciences, educational innovation, and interdisciplinary research. She has been actively involved in initiatives aimed at advancing academic quality, scientific research, and innovation in higher education institutions. Her work focuses on promoting modern educational practices, research collaboration, and professional development in applied sciences. She also contributes to policy-oriented and academic projects that support the growth of higher education and scientific advancement in Uzbekistan. She is based in Tashkent, Uzbekistan.

Guzal Mardiyeva is affiliated with the Department of Social and Humanitarian Science at Samarkand State Medical University. Her academic interests include social sciences, гуманitarian studies, medical education, and interdisciplinary research in higher education. She has been actively involved in teaching and scholarly activities aimed at enhancing the integration of social and humanitarian perspectives in medical education. Her work focuses on educational development, communication, ethics, and the promotion of student-centered learning approaches. She also contributes to academic research initiatives and professional development programs within the university community. She is based in Samarkand, Uzbekistan.

Timur Jumabaev is an Associate Professor in the Department of Pedagogy and Psychology at the University of Innovative Technologies. His academic interests include pedagogy, educational psychology, innovative teaching methodologies, and student development in higher education. He has been actively engaged in teaching, research, and academic initiatives focused on improving educational quality and modern learning practices. His work emphasizes interdisciplinary approaches, psychological aspects of learning, and the integration of innovative technologies in education. He also contributes to mentoring students and supporting professional development in the fields of pedagogy and psychology. He is based in Uzbekistan.

Bayrambay Erimbetov is a Professor at the Nukus branch of Uzbek State University of Physical Culture and Sports. His academic interests include physical education, sports sciences, athletic training, and the development of sports pedagogy in higher education. He has extensive experience in teaching, research, and academic leadership related to physical culture and sports education. His scholarly work focuses on improving training methodologies, promoting healthy lifestyles, and advancing professional education in sports sciences. He is also actively involved in mentoring students and supporting research initiatives in the field of physical education and sports. He is based in Nukus, Karakalpakstan, Uzbekistan.