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

Academic Chain: Securing Educational Credentials with Blockchain-Enabled

Zebo Sharipova[1*], Rano Mardonova[2], Azzam Begbutayev[3], Saida Makhkamova[4], I.B. Sapaev[5], Shaxnoza Karimova[6], Khilola Nigmatova[7], and Gulobod Rakhmatova[8]

[1*]Kimyo international university in Tashkent, Uzbekistan. z.sharipova@kiut.uz, https://orcid.org/0000-0003-0547-9180

[2]Associate Professor at the Department of English Language Teaching Methodology, Termez State University, Uzbekistan, ranoinfinity8@gmail.com, mardonovar@tersu.uz, https://orcid.org/0009-0009-9982-4213

[3]PhD., Associate Professor, Department of Informatics and Digital Educational Technologies, Jizzakh State Pedagogical University, Jizzakh, Uzbekistan, azambegbutayev@gmail.com, https://orcid.org/0000-0003-1219-380X

[4]Head of Education Quality Control Department, Tashkent State University of Oriental Studies, Uzbekistan, saida_maxkamova@tsuos.uz, https://orcid.org/0009-0001-3358-7624

[5]Head of the department, Tashkent Institute of Irrigation and Agricultural Mechanization Engineers, National Research University, Tashkent, Uzbekistan. School of Engineering, Central Asian University, Tashkent, Uzbekistan, sapaevibrokhim@gmail.com, https://orcid.org/0000-0003-2365-1554

[6]Lecturer, Tashkent State University of Oriental Studies, Uzbekistan. shahnozasayyid@gmail.com, https://orcid.org/0000-0003-2914-0261

[7]Associate Professor, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan. nigmatovakhilola464@gmail.com, https://orcid.org/0009-0009-3280-6088

[8]Department of Preschool Education, Navoi State University, Uzbekistan. raxmatovagulobod@gmail.com, https://orcid.org/0009-0004-9016-0397

Received: February 06, 2025; Revised: March 18, 2025; Accepted: April 28, 2025; Published: May 30, 2025

Abstract

Blockchain technology presents a novel approach to building and saving trust when tracking data, running transactions, and performing various activities. Some consider it a revolutionary instrument in cryptography and cybersecurity, including use in cryptocurrencies, smart contracts, the Internet of Things, innovative grid governance, healthcare, and supply chain. This project research would closely investigate blockchain security, privacy, and trust problems. It also examines how blockchain technology is used in other related issues and education. At last, the article suggests a blockchain approach for effective and safe student record management.

Keywords: Blockchain, Education, Digital Certificate, Educational Credential, Security, Privacy.

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 2 (May), pp. 374-386.
DOI: *10.58346/JISIS.2025.I2.027*

*Corresponding author: Kimyo international university in Tashkent, Uzbekistan.

1 Introduction

Blockchain provides a new paradigm for data storage, executing transactions, automating tasks, and establishing trust. Its uses range from cryptocurrencies, healthcare, and smart contracts to the Internet of Things (IoT), innovative grid governance, and supply chain management, making it a marvel in cryptography and cybersecurity (Krishnan et al., 2020). This study assesses blockchain implementations to ensure security, privacy, and trust. Further, it investigates the use of blockchain in education and its problems. Finally, it presents a framework based on blockchain technology to manage student academic records securely and reliably (Fraga-Lamas & Fernandez-Carames, 2019).

Blockchain is Bitcoin's underlying technology. It supports Bitcoin's decentralized and distributed ledger, which registers all network participants' data in the transactions. This ledger enables the Bitcoin system to record every transaction in detail, including time, the sender (or spender), and the recipient's addresses, thus eliminating the possibility of double-spending. All data recorded on the Blockchain is encrypted to maintain user privacy (Abdus et al., 2018).

Given that the Blockchain contains all the data on all Bitcoin transactions (Nakamoto, 2008), another definition is a shared ledger. The field of education is turning into the current era. Education and technology are a great fit and have recently become popular. Consequently, instructional technology has spread around the globe like a phenomenon (Raghuvanshi et al., 2021). Still, we cannot talk about the usage of technologies without first addressing the security problem (Dallal, 2024). Ignoring proper protection policies will lead to higher human resource and financial costs with the growing use of digital technologies in education, there has been a lot of research by different scholars recommending specific frameworks, strategies, and policies to guide decision-making on information security policies and protocols. Among the various technologies that are coming up, blockchain is one of the most popular because of its data encryption and data security capabilities (Shamsudinova et al., 2025; Salimitari & Chatterjee, 2018).

This work aims to study the current status of blockchain applications in education by conducting a comprehensive bibliographic review. In this regard, the paper organizes existing strategies and provides a comprehensive literature overview. The purpose is to draw attention to the critical areas of implementation and investigate the possibilities of further implementation of blockchain technology in education. The emphasis is on three main areas: educational tools based on blockchain, the value proposition of blockchain for academic institutions, and the problems of using this technology in education (Kiruthika et al., 2019).

One common problem in education is verifying official documents, which is often tedious and time-consuming. These documents include government records, financial records, proof of transactions, and academic certificates. Students greatly value academic qualifications. However, the absence of an issuance policy that allows for transparent and systematic verification of credentials has rendered the copious manufacture and circulation of fake certificates too easy. Notable forgeries that compromise social trust can be easily presented as legitimate documents.

This research analyzes the possible uses of blockchain technology in education, particularly regarding data security and confidentiality (Kondori & Peashdad, 2015). It proposes a blockchain-based system intended to immutably record and manage student academic credentials to control access to definitive stored documents. This system would protect students from fraudulent representation and allow dependable verification over time (Khan et al., 2020).

This paper is organized as follows: In Section II, I review literature of blockchain technology in education; Section III describes the methods used in this research; In Section IV, I analyze practical examples of blockchain technology in education; In Section V, I present a baseline strategy for verification of digital records; and In Section VI, I summarize the main findings of the research and propose recommendations for future studies.

2 Background

2.1 Hashing

Hashing is a technique that modifies input information through a cryptographic method into a unique string of text, like a digital fingerprint. Sometimes, hashing is contrasted with encryption; however, it provides message integrity and confidentiality in addition to encryption safeguards when sent to intended recipients (Shuaib et al., 2020). It ensures the original data remains secure from unauthorized changes (Shuaib et al., 2021). Apart from these uses, hashing also helps structure and file data in tables within a database. Hash functions like MD5 and SHA-1 can produce fixed-length outputs irrespective of the input data size. Often, such outputs are referred to as digital signatures or digital checksums. Such functions are one-way algorithms, meaning getting the initial data back from the hash value cannot be done (Bokhari et al., 2014) and (Bokhari & Alam, 2013).

2.2 Blockchain Technology

Blockchain can be viewed as an advanced form of digital innovation first invented for Bitcoin by Sakaoshi Nakamoto (Nakamoto, 2008; Gorkhali et al., 2020). Even if its main aim was to allow secure financial transactions, blockchain extends beyond that to any processes that require data to be stored in a transparent, decentralized, and immutable system (Imam et al., 2021). Blockchain technology may be understood as a chain of data blocks containing information, together with the cryptographic hash of the prior block, which links them together (Krishnaiah & Dayanand Lal, 2025). This forms the foundational distributed ledger technology (DLT) structure within a P2P decentralized network. The new blocks are created and validated according to specific rules of consensus, which all participants must agree upon. Data added into the chain becomes immutable, rendering the system trustless and censorship resistant, guaranteeing the accuracy and truth of the information (Aamir et al., 2020).

2.3 Types of Blockchain

In broad terms, blockchain architectures are subdivided into public and private types, plus there are consortium and hybrid blockchains (Caldarelli & Ellul, 2021). All types of blockchains presume the existence of a network of nodes that preserve the shared ledger in a secure and synchronized way. Each node can validate transactions, spread messages, and create new blocks (Quasim et al., 2020).

2.3.1 Public Blockchain

Public blockchains are an open, decentralized network accessible to anyone with internet connectivity (Siddiqui et al., 2020). Users can participate in the network by viewing transaction history, validating blocks through consensus-based methods like proof-of-work, and even actively participating as miners (Dann et al., 2020). Bitcoin and Litecoin are well-known examples of such public blockchains. With proper user compliance with safety measures, these systems have transparent, secure information and high trustworthiness (Siddiqui et al., 2020).

2.3.2 Private Blockchain

Private blockchains work within a network setting that contains an invasive access control mechanism. Authorized participants are the only individuals who have access to the network. Typically, these blockchains are employed by firms internally for organizational purposes (Gonczol et al., 2020). All rights, grants, validation of actions, and visibility of actions performed are done through a central controller. As with public blockchains, private blockchains have a structure and functionality that operates on the same fundamental principles (Samad et al., 2017). However, they impose limitations regarding access and participation defined by a particular organization or a consortium. Permissioned blockchains are helpful in digital identity verification, supply chain tracking, e-voting, and managing financial assets.

2.3.3 Consortium (Federated) Blockchain

A consortium blockchain or federated blockchain is one where governance is vested in a pre-selected set of institutions as opposed to a single entity. This form achieves a balance between the degree of decentralization and central supervision (Casino et al., 2019). The network can only be accessed by vetted participants, making it ideal for partnerships like alliances in the banking sector, governmental consortia for sharing data, and closed consortia for industries. The controlled access increases participant trust while safeguarding privacy and operational efficiency.

2.3.4 Hybrid Blockchain

Hybrid blockchains incorporate public and private system components, allowing restricted access to blockchain information. Certain log portions can be accessible while confidential information is kept private. Such a configuration assists organizations in controlling their data privacy while utilizing the open nature of public blockchains. Hybrid models allow interfacing with internal and external systems and thus provide the flexibility needed for various scenarios.

2.4 Blockchain Features

The application of blockchain technology goes beyond cryptocurrency endeavors; its fundamental attributes have prompted its adoption in various other verticals (Shuaib et al., 2021):

- Information Security: The blockchain acts as a digital safeguard, protecting data from unauthorized modification or removal, which is known as tampering.
- No Third-Party Control: The lack of a single authoritative point mitigates control over blockchain and reduces the possibility of compromise or silence.
- Control Enhancement: Greater encryption and consensus approach substantially secure a system from unauthorized changes.
- Consensus procedures: Changes or alterations to a blockchain's underlying data are subject to multi-signature confirmation and the approval of requisitely determined block-based participants.

Transaction Speed: Settlement of transactions is instantaneous with no delays as opposed to traditional methods.

3 Application Areas for Blockchain

Blockchain technology has changed considerably and now extends far beyond its application in cryptocurrencies. While many blockchain networks continue to fulfill financial activities, their versatility has allowed them to be adopted in various non-financial areas. Researchers frequently divide blockchain applications into two categories: economic and non-financial or based on distinct versions of blockchain technology.

3.1 Financial Applications

Blockchain is transforming asset management and transaction processing, making significant inroads into the financial sector. It is used for services including company operations, distributed prediction markets, financial settlements, and digital asset trading. Integrating blockchain with real-world applications now depends critically on marketplace systems (PMS), which serve as sources of validated external data oracles. Blockchain's openness and decentralization help build confidence and efficiency in financial activities, so it is a useful instrument for institutions and investors. Blockchain is projected to be especially important in determining the resilience and sustainability of the worldwide financial ecosystem as it develops (Abou Jaoude & Saade, 2019).

3.2 Governance

Governments have kept extensive databases for decades to handle data on businesses and residents. Many of these conventional systems can be evolved using blockchain. Blockchain-enabled solutions are perfect for enhancing public service efficiency and fighting corruption since they provide automation, openness, and tamper-resistance. Blockchain can streamline procedures, including identity verification, tax records, land registration, and welfare disbursement, by allowing dispersed management of public records. Blockchain can be a safe backbone linking infrastructure elements in physical, social, and industrial spheres in the framework of smart cities (Shuaib et al., 2021; Alam et al., 2019). Blockchain governance seeks to keep legal and institutional legitimacy while replicating state-level capability in a distributed manner. More citizen-centric governance models with simplified, reliable, and safe operations follow.

4 Blockchain in Education

Blockchain Uses for Education

Blockchain technology could greatly aid educational systems' operational efficiency and transparency due to secure record-keeping, authenticated credentials, and support for decentralized learning models. A general framework for applying blockchain technology in the academic setting is provided in Figure 1. In this paragraph, I discuss the most relevant use cases and the advantages and drawbacks of using blockchain technology in education.

Online Education

Online or distant learning mostly depends on digital infrastructure to provide materials and evaluate students. Concerning authenticity and security, blockchain presents a strong answer to typical problems. It guarantees that academic credits are consistently issued and helps to create tamper-proof learning records, eliminating the reliance on outside validation.

Student Records

Academic transcripts have traditionally been time-consuming and prone to mistakes. Manual validation of every entry blocks access to verified data. Blockchain lets educational institutions automatically store and validate course materials, certifications, and student achievements, enabling stakeholders to quickly access verified data (Liu et al., 2020).

Diplomas and Certificates

Blockchain storage and secure issuing of academic credentials, including diplomas and certificates, are possible. This stops the dissemination of false degrees and removes the necessity for outside confirmation. However, blockchain technologies do have limits in throughput and latency, which now prohibit major deployment (Averin et al., 2020).

Digital badges

Blockchain can authenticate non-traditional accomplishments like technical knowledge or language ability outside of degrees. Once confirmed by an approved third party, these abilities can be entered into digital badges on the blockchain. Open Badge Passports and other projects like them best show this micro-credentialing trend.

Examining and Assessing Students

Smart contracts and blockchain can automate student assessments. Teachers can define correct answers and grading standards, while the blockchain can independently assess student entries. Moreover, it can record extracurricular successes, providing a complete picture of student capacity for academic and occupational interests.

Classes and Coursework

Smart contracts included in blockchain systems can automate lesson distribution and course completion validation. Instructors can program assignments into the blockchain, which subsequently guarantees completion. Students can receive points or tokens upon task completion, supporting autonomous, self-paced learning.

Academic publishing and protection of intellectual property

Blockchain fixes problems, including academic publishing transparency, peer review manipulation, and plagiarism. Safely documenting contributions from teachers, researchers, and students can help maintain the provenance of research products and promote repeatability.

Applications for Admission

Traditional admission systems often suffer from data loss or manipulation. Blockchain-based systems offer decentralized, verifiable, safe student data storage that may be shared between universities, enabling worldwide access and simplifying application processes (Bhaskar et al., 2020).

Blockchain's Advantages for Education

- There are several benefits of introducing blockchain technology into educational environments:

- Immutable, chronologically ordered blocks stop manipulation in data integrity.
- Accessibility and Transparency: Academic records are on hand around the clock for review.
- Shortened Verification Time: Companies and organizations may rapidly confirm credentials.
- Blockchain helps people to have faith in the accuracy of instructional data.
- Cost Efficiency: Administrative expenses are lowered by the need for fewer hand validation procedures.

Blockchain technologies thus generate a safe digital infrastructure supporting academic mobility, credential management, and lifetime learning.

Challenges in Educational Blockchain Adoption

Even with its benefits, several blockchain technology implementation challenges exist in education:

- Subjectivity in Evaluation: Human judgment is necessary for evaluating essays or presentations; therefore, smart contracts cannot assess such tasks.
- Immutability Limitations: The blockchain's irreversible nature obstructs updating student records.
- Technical Constraints: The classroom application of consensus algorithms like Proof-of-Work is unrealistic due to the high resource expenditure and low transaction throughput.
- Reliability Issues: Providing students' academic history on a publicly accessible ledger compromises privacy (Nabil et al., 2020).

There is a strong need for adaptable, low-energy-consuming, and privacy-respecting blockchain frameworks for the educational sector.

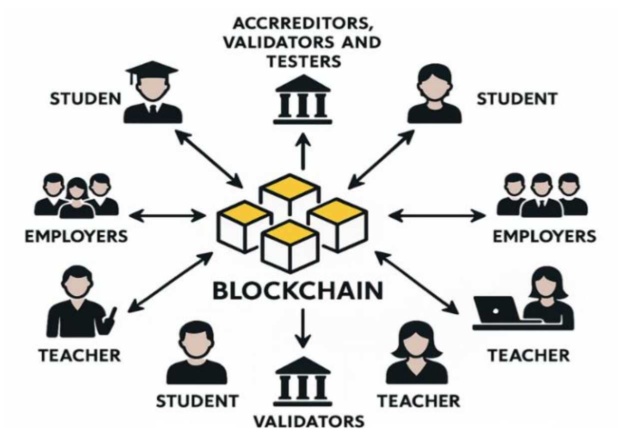

Figure 1: Blockchain in Education

5 Blockchain Technology-Based Systems in Education for Managing Digital Credentials

Digital Credentials and Verification Frameworks

Digital credentials of qualifications might include digital badges and certificates, as they replace traditional credentials issued in Figure 2. Such credentials, which include degrees, course completions, and certifications of competencies, are easier to issue, manage, and verify (Mishra et al., 2021).

Unlike traditional printed certificates, digital certificates indicate sophisticated attributes such as the holder's skills and the issuing authority. An example is the Faculty Development badge, which indicates proficiency in course and curriculum design issued by the Colorado Community College System. Digital formats of documents are more appropriate than the conventional university transcripts for modern hiring processes and credential evaluations, making them faster than instantaneously outdated paper documents (Mahankali & Chaudhary, 2020).

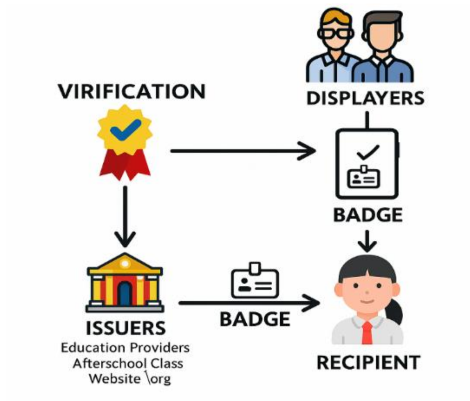

Figure 2: Digital Verification of Academic Records

A. Issues with Digital Certificates

The emergence of counterfeit academic qualifications has risen in parallel with the increasing significance of professional credentials. This problem cuts across all levels of society, from low-level workers to high-profile aspirants and politicians. The distinctly cumbersome vulnerabilities of paper-based and electronic transcripts, including poor sharing capabilities, feeble security, and weak accessibility, only fail the fire. These problems complicate and increase the cost of managing credentials. The issuance and verification of academic credentials through self-secured blockchain technology offer an enticing solution. This increases trust and mitigates administrative delays in credentialing (Liu et al., 2020).

B. Blockchain-Based Framework for Digital Credentials

Verifying academic documents in advanced innovative educational ecosystems can be manual and cumbersome. In this regard, blockchain technology serves as an architectural framework designed for automating and verifying academic credentials. As depicted in Figure. 3, a blockchain-based architecture exists where certain bridges, such as Grades and Qualifying Competencies, are excluded from the teaching module.

If the students exhaust all expected learning activities (substantial modules), a check-based algorithm evaluates eligibility against the degree requirements. Subsequently, it issues a "congratulations" notification with a digital diploma and transcript. Every document is encoded with non-repeating identifiers, such as URIs, enabling graduates to provide tamper-proof documents to verifiable systems external to their institutions, including employers and government bodies. Figure 3 illustrates the management of academic credentials and certificates utilizing blockchain technology. Since blockchain can neither be changed nor altered, strategies for conflicting perpetual refreshment need not be entrusted, and these documents remain unquestioned as they carry no burdens of extra authentication.

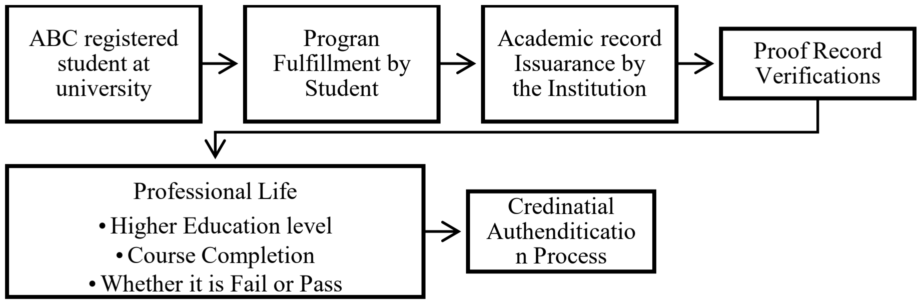

Figure 3: Management of Academic Credentials and Certificates Utilizing Blockchain Technology

A blockchain-based architecture is suggested to guarantee the verifiable and safe maintenance of student academic data (Figure 4 and Figure 5). This system would comprise unchangeable digital documents that one could independently verify. It improves data security and lets students access confirmed credentials even after protracted intervals. Furthermore, the technology precludes the creation of bogus degrees since the blockchain network allows all certifications to be uniquely identified and verified.

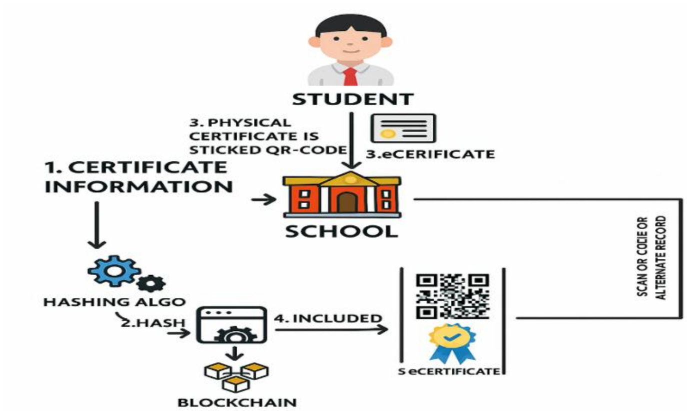

Figure 4: Issuance of a Digital Certificate using Blockchain Technology

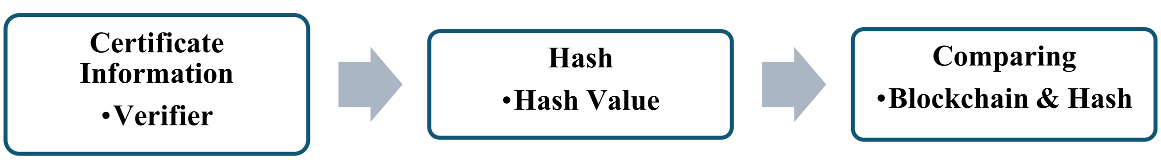

Figure 5: Verification of Digital Certificates Using Blockchain Technology

6 Conclusion and Future Work

Blockchain represents a transformative advancement in the secure management of educational data. Its decentralized architecture enables the creation of immutable academic records, ensuring verifiability and long-term accessibility without reliance on centralized authorities. Implementing blockchain technology into education systems can remarkably improve transparency, decrease credential fraud, and simplify the infrastructural work related to certifying and maintaining academic records. The integration of blockchain technology can address some of the most fundamental issues in the rapidly changing education landscape, including credentialing, data sharing, and trust management. However, successful implementation requires technical readiness, institutional support, stakeholder awareness, and policy adaptation.

Future research should focus on refining blockchain architectures to address scalability, energy efficiency, and privacy concerns. Furthermore, comprehensive studies involving educators, administrators, and policymakers are needed to uncover domain-specific requirements and constraints. Developing accessible educational resources and training programs on blockchain and smart contracts will also equip stakeholders with the necessary knowledge to utilize this technology effectively. With thoughtful integration and continued exploration, blockchain holds the potential to become a foundational pillar in modern educational infrastructure.

References

[1] Aamir, M., Qureshi, R., Khan, F. A., & Huzaifa, M. (2020). Blockchain based academic records verification in smart cities. *Wireless personal communications*, *113*(3), 1397-1406.

[2] Abdus, S., Shadab, A., Mohammed, S., & Ubaidullah, B. M. (2018). Internet of Vehicles (IoV) requirements, attacks and countermeasures. In *5th International Conference on Computing for Sustainable Global Development*. 4037–4040.

[3] Abou Jaoude, J., & Saade, R. G. (2019). Blockchain applications – usage in different domains. *IEEE Access, 7*, 45360–45381. https://doi.org/10.1109/ACCESS.2019.2902501

[4] Alam, S., Shuaib, M., & Samad, A. (2018, November). A collaborative study of intrusion detection and prevention techniques in cloud computing. In *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2018, Volume 1* (pp. 231-240). Singapore: Springer Singapore.

[5] Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-based applications in education: A systematic review. *Applied Sciences, 9*(12), 2400. https://doi.org/10.3390/app9122400

[6] Averin, A., Snegireva, D., & Ladejshchikov, A. (2020, September). Model of a monitoring system for academic performance and the issuance of diplomas using blockchain technology. In *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)* (pp. 88-91). IEEE.

[7] Bhaskar, P., Tiwari, C. K., & Joshi, A. (2021). Blockchain in education management: present and future applications. *Interactive Technology and Smart Education*, *18*(1), 1-17.

[8] Bokhari, M. U., & Alam, S. (2013). BSF-128: a new synchronous stream cipher design. In *Proceeding of international conference on emerging trends in engineering and technology* (pp. 541-545).

[9] Bokhari, M. U., Alam, S., & Hasan, S. H. (2014). A detailed analysis of Grain family of stream ciphers. *International Journal of Computer Network and Information Security, 6*(6), 34-40.

[10] Caldarelli, G., & Ellul, J. (2021). Trusted academic transcripts on the blockchain: A systematic literature review. *Applied Sciences, 11*(4), 1842.

[11] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36*, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

[12] Dallal, H. R. H. A. (2024). Changes to communication infrastructure caused by blockchain technology. *International Academic Journal of Science and Engineering, 11*(1), 25–39. https://doi.org/10.9756/IAJSE/V11I1/IAJSE1105

[13] Dann, D., Peukert, C., Martin, C., Weinhardt, C., & Hawlitschek, F. (2020). Blockchain and Trust in the Platform Economy: The Case of Peer-to-Peer Sharing. In *Wirtschaftsinformatik (Zentrale Tracks)* (pp. 1459-1473).

[14] Fraga-Lamas, P., & Fernandez-Carames, T. M. (2019). A review on blockchain technologies for an advanced and cyber-resilient automotive industry. *IEEE Access, 7*, 17578–17598. https://doi.org/10.1109/ACCESS.2019.2895302

[15] Gonczol, P., Katsikouli, P., Herskind, L., & Dragoni, N. (2020). Blockchain implementations and use cases for supply chains – a survey. *IEEE Access, 8*, 11856–11871. https://doi.org/10.1109/ACCESS.2020.2964880

[16] Gorkhali, A., Li, L., & Shrestha, A. (2020). Blockchain: A literature review. *Journal of Management Analytics, 7*(3), 321–343. https://doi.org/10.1080/23270012.2020.1801529

[17] Imam, I. T., Arafat, Y., Alam, K. S., & Shahriyar, S. A. (2021, February). DOC-BLOCK: A blockchain based authentication system for digital documents. In *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)* (pp. 1262-1267). IEEE.

[18] Khan, M. A., Quasim, M. T., Algarni, F., & Alharthi, A. (2020). *Decentralized Internet of Things: A blockchain perspective* (Vol. 71). Springer Nature.

[19] Kiruthika, J., Poovizhi, V., Kiruthika, P., Madura, E., & Narmatha, P. (2019). Blockchain-based unforgeable license. *International Journal of Communication and Computer Technologies, 7*(2), 4–7. http://dx.doi.org/10.31838/ijccts/07.02.02

[20] Kondori, M. A. P., & Peashdad, M. H. (2015). Analysis of challenges and solutions in cloud computing security. *International Academic Journal of Innovative Research*, *2*(1), 20-30.

[21] Krishnaiah, P. N. S., & Dayanand Lal, N. (2025). Classification of lung diseases using a federated proximal term-based two-layer LSTM with federated learning and blockchain. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 16*(1), 269–288. https://doi.org/10.58346/JOWUA.2025.I1.017

[22] Krishnan, V. G., Krishnan, T. N., Karim, S. S., Yuvarajan, G., & Priya, M. R. (2020). Cyber Security in Data Mining to Data Driven Security. *International Journal of Advances in Engineering and Emerging Technology*, *11*(1), 71-76.

[23] Liu, L., Han, M., Zhou, Y., Parizi, R. M., & Korayem, M. (2020). Blockchain-based certification for education, employment, and skill with incentive mechanism. In *Blockchain cybersecurity, trust and privacy* (pp. 269-290). Cham: Springer International Publishing.

[24] Mahankali, S., & Chaudhary, S. (2020). Blockchain in education: a comprehensive approach–utility, use cases, and implementation in a university. In *Blockchain technology applications in education* (pp. 267-293). IGI global.

[25] Mishra, R. A., Kalla, A., Braeken, A., & Liyanage, M. (2021). Privacy protected blockchain-based architecture and implementation for sharing of students' credentials. *Information Processing & Management, 58*(3), 102512.

[26] Nabil, A., Nafil, K., & Mounir, F. (2020, April). Blockchain Security and Privacy in Education: A Systematic Mapping Study. In *World Conference on Information Systems and Technologies* (pp. 253-262). Cham: Springer International Publishing.

[27] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

[28] Quasim, M. T., Radwan, A. A. E., Alshmrani, G. M. M., & Meraj, M. (2020). A blockchain framework for secure electronic health records in healthcare industry. In *2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*. 605–609.

[29] Raghuvanshi, A., Singh, U. K., Shuaib, M., & Alam, S. (2021). WITHDRAWN: An investigation of various applications and related security challenges of Internet of Things. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.01.821

[30] Salimitari, M., & Chatterjee, M. (2018). A survey on consensus protocols in blockchain for IoT networks.

[31] Samad, A., Alam, S., Mohammed, S., & Bhukhari, M. (2018, March). Internet of vehicles (IoV) requirements, attacks and countermeasures. In *Proceedings of 12th INDIACom; INDIACom-*

2018; 5th international conference on "computing for sustainable global development" IEEE conference, New Delhi (pp. 1-4).

[32] Samad, A., Shuaib, M., & Beg, M. R. (2017). Monitoring of military base station using flooding and ACO technique: An efficient approach. *International Journal of Computer Network and Information Security, 9*(12), 36–44. https://doi.org/10.5815/ijcnis.2017.12.05

[33] Shamsudinova, I., Karimov, N., Umarova, M., Mustafaqulova, D., Almuratova, G., Qodirov, S., Istamova, D., & Matniyoz, S. (2025). Educational disparities in the digital era and the impact of information access on learning achievements. *Indian Journal of Information Sources and Services, 15*(1), 6–11. https://doi.org/10.51983/ijiss-2025.IJISS.15.1.02

[34] Shuaib, M., Alam, S., & Daud, S. M. (2020, December). Improving the authenticity of real estate land transaction data using blockchain-based security scheme. In *International Conference on Advances in Cyber Security* (pp. 3-10). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-33-6835-4_1

[35] Shuaib, M., Alam, S., Alam, S. M., & Nasir, M. S. (2021). WITHDRAWN: Compliance with HIPAA and GDPR in electronic health record. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.03.059

[36] Shuaib, M., Alam, S., Mohd, S., & Ahmad, S. (2020). Blockchain-based initiatives in social security sector. In *Proceedings of the EAI 2nd International Conference on ICT for Digital, Smart, and Sustainable Development (ICIDSSD)* (p. 8).

[37] Siddiqui, S. T., Ahmad, R., Shuaib, M., & Alam, S. (2020). Blockchain security threats, attacks and countermeasures. In *Ambient Communications and Computer Systems: RACCCS 2019* (pp. 51-62). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-15-1518-7_5

[38] Siddiqui, S. T., Alam, S., Ahmad, R., & Shuaib, M. (2020). Security threats, attacks, and possible countermeasures in internet of things. In *Advances in data and information sciences: Proceedings of ICDIS 2019* (pp. 35-46). Singapore: Springer Singapore.

Authors Biography

Zebo Sharipova, Head of Management & Marketing at Kimyo International University in Tashkent. Her expertise lies in blockchain applications in education and academic administration. She advocates for secure verification of educational credentials using digital platforms. Zebo is involved in initiatives enhancing institutional transparency via technology. She actively participates in projects connecting management systems with IT. Her current work focuses on blockchain-enabled frameworks for academic trust.

Rano Mardonova, Associate Professor in English Language Teaching at Termez State University. Her academic focus includes modern pedagogy, blended learning, and methodology. She explores language education supported by blockchain and secure platforms. Rano emphasizes cross-disciplinary teaching methods for digital-age learners. Her recent projects involve digital integration in teacher training modules. She contributes to innovative language frameworks for hybrid classrooms.

Dr. Azzam Begbutayev, PhD, Associate Professor, Department of Informatics and Digital Educational Technologies, Jizzakh State Pedagogical University, Uzbekistan. He specializes in digital transformation in education, educational data security, and blockchain applications. His research explores the integration of decentralized technologies into academic verification systems. Dr. Begbutayev focuses on enhancing transparency and trust in credential management through blockchain. He actively contributes to projects on secure digital infrastructure in higher education institutions. His work supports innovation in e-governance and academic record authentication.

Saida Makhkamova, Head of Education Quality Control at TSU of Oriental Studies, Tashkent. She specializes in academic governance, quality assurance, and digital audits. Saida promotes the use of secure technology in university assessment systems. Her work includes aligning academic performance with digital verification tools. She supports AI-driven dashboards for institutional monitoring. Saida Makhkamova, Head of Education Quality Control at TSU of Oriental Studies, Tashkent. She specializes in academic governance, quality assurance, and digital audits. Saida promotes the use of secure technology in university assessment systems. Her work includes aligning academic performance with digital verification tools. She supports AI-driven dashboards for institutional monitoring. Her current research explores tech-enhanced quality frameworks in HEIs. Her current research explores tech-enhanced quality frameworks in HEIs.

I.B. Sapaev, Department Head of Physics & Chemistry at TIIAME NRU, Tashkent. Also affiliated with Alfraganus University and Central Asian University. His work spans material science, digital education systems, and smart classrooms. Sapaev supports cross-institutional research in AI-driven academic security. He is involved in multidisciplinary projects integrating hardware with pedagogy. His research aims at bridging core sciences and digital infrastructure.

Shaxnoza Karimova, PhD, Lecturer at Tashkent State University of Oriental Studies. Her work connects philology with digital content development for education. She studies language acquisition through technology-supported instruction. Her focus includes cybersecurity aspects in educational platforms. Shaxnoza supports AI-assisted learning tools for multilingual instruction. She is involved in international collaborations in linguistics and digital education.

Khilola Nigmatova, Associate Professor, Foreign Languages, TUIT. She works on foreign language teaching in ICT and economics contexts. Her research includes tech-enhanced learning environments and security. She explores language access using IoT and AI-based classroom models. Khilola also contributes to digital pedagogy in multilingual ecosystems. Her recent work involves secure smart classroom integration

Gulobod Rakhmatova, Faculty in Preschool Education at Navoi State University.She explores early childhood learning via digital and mobile platforms. Her work aligns with the secure integration of EdTech in early education. Gulobod supports projects on gamified and sensor-based learning. She focuses on safe digital literacy for preschoolers.