JOURNAL OF DIGITAL LAW AND INNOVATION

(JDLI)

LAW • TECHNOLOGY • INNOVATION • JUSTICE

OPEN ACCESS

ISSN 3093-9364

OUR FIELDS

- Digital law
- Cybersecurity law
- Artificial intelligence and robotics law
- Intellectual property law
- LegalTech and legal innovations
- E-government and digital public services
- Legal aspects of AgroTech and GreenTech
- Smart city and digital governance

OUR INDEXING

- Google Scholar
- Zenodo
- DOI
- OpenAIRE
- Open Access

https://unireview.uz/index.php/jdli

VOLUME 2 | ISSUE 1

Published by UniLex Global

AUGUST 2026

“UNILEX GLOBAL” LLC

Raqamli huquq va innovatsiya jurnali
Journal of Digital Law and Innovation

August, 2026
VOLUME 2, ISSUE 1

EDITORIAL TEAM

UNILEX GLOBAL

ISSN 3093 - 9364

RAQAMLI HUQUQ VA INNOVATSIYA / DIGITAL LAW AND INNOVATION

PROSPECTS FOR USING BLOCKCHAIN TECHNOLOGY TO ENHANCE TRANSPARENCY IN EDUCATIONAL DOCUMENT WORKFLOW

Shaydullayev Ilyos Shukhratovich
1st year student of "Cyber University" State University
Samarov Sherzod Khamraevich
Cyber University State University
Methodologist of the Faculty of Law and Business

ARTICLE INFO

Keywords:
blockchain,
education,
HEMIS,
Merkle tree,
IPFS,
academic records,
digital verification,
cryptographic hash,
consortium blockchain,
cybersecurity.

A B S T R A C T

This article examines the use of blockchain technology to improve transparency in the creation, validation, storage, and verification of diplomas, transcripts, certificates, and other academic records in higher education. While acknowledging the benefits of centralized information systems such as HEMIS, the study identifies structural limitations including a single point of failure, limited independent verification of internal changes, and time-consuming cross-border credential verification. A hybrid architecture combining SHA-256 hashing, Merkle trees, IPFS, and a permissioned consortium blockchain is proposed. Comparative results illustrate differences between centralized and blockchain-based models in terms of integrity assurance, verification time, dependence on a central server, and transaction costs. Percentage estimates are explicitly treated as theoretical scenario values rather than pilot-test results. The study argues that technical deployment must be accompanied by rules on personal-data protection, legal recognition, node governance, and measurable pilot-testing criteria.

UNILEX GLOBAL

ISSN 3093 - 9364

RAQAMLI HUQUQ VA INNOVATSIYA / DIGITAL LAW AND INNOVATION

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ ПОВЫШЕНИЯ ПРОЗРАЧНОСТИ ДОКУМЕНТООБОРОТА В СИСТЕМЕ ОБРАЗОВАНИЯ

ИНФОРМАЦИЯ СТАТЬИ

Ключевые слова:
блокчейн,
образование,
HEMIS,
дерево Меркла,
IPFS,
академические документы,
цифровая верификация,
криптографический хеш,
консорциумный блокчейн,
кибербезопасность.

А Н Н О Т А Т С И Я

В статье анализируются возможности применения технологии блокчейн для повышения прозрачности процессов создания, подтверждения, хранения и проверки дипломов, транскриптов, сертификатов и иных академических документов в высших учебных заведениях. Не отрицая преимуществ централизованных информационных систем типа HEMIS, выделяются такие риски, как единая точка отказа, ограниченные возможности независимой внешней проверки изменений и длительность международной верификации документов. Предлагается гибридная модель, объединяющая хеширование SHA-256, дерево Меркла, IPFS и разрешённый консорциумный блокчейн. Сравнительные результаты показывают различия между централизованной и блокчейн-моделями по целостности данных, скорости проверки, зависимости от центрального сервера и транзакционным расходам. Процентные показатели рассматриваются как теоретические сценарные оценки, а не как результаты пилотного эксперимента. Обосновывается необходимость параллельного решения вопросов защиты персональных данных, юридического признания, управления узлами и разработки критериев пилотного тестирования.

TA’LIM TIZIMIDA HUJJATLAR AYLANMASINI SHAFFOFLASHTIRISHDA BLOKCHEYN TEXNOLOGIYASIDAN FOYDALANISH ISTIQBOLLARI

MAQOLA MA’LUMOTI

Kalit so‘zlar:
blokcheyn, ta’lim,
HEMIS,
Merkle daraxti,
IPFS,
akademik hujjat,
raqamli verifikatsiya,
kripto-xesh,
konsorsium blokcheyni,
kiberxavfsizlik.

A N N O T A T S I Y A

Maqolada oliy ta’lim muassasalarida diplom, transkript, sertifikat va boshqa akademik hujjatlarning yaratilishi, tasdiqlanishi, saqlanishi va tekshirilishini blokcheyn texnologiyasi yordamida shaffoflashtirish imkoniyatlari tahlil qilinadi. O‘zbekistondagi HEMIS kabi markazlashgan axborot tizimlarining afzalliklari inkor etilmagan holda, yagona nosozlik nuqtasi, ichki o‘zgartirishlarni tashqi tomon tomonidan mustaqil tekshirishning cheklanganligi va xalqaro verifikatsiyaning vaqt talab qilishi kabi muammolar ajratib ko‘rsatiladi. Tadqiqotda SHA-256 xesh-funksiyasi, Merkle daraxti, IPFS va ruxsatga asoslangan konsorsium blokcheynini birlashtiruvchi gibrid model taklif etiladi. Qiyosiy natijalar markazlashgan va

blokcheyn asosidagi modellarning yaxlitlik, tekshiruv tezligi, serverga bog‘liqlik va tranzaksiya xarajatlari bo‘yicha farqlarini ko‘rsatadi. Keltirilgan foizli ko‘rsatkichlar pilot sinov natijasi emas, balki nazariy ssenariy baholari ekanligi alohida qayd etiladi. Yakunda texnik arxitektura bilan bir qatorda shaxsiy ma’lumotlarni himoya qilish, yuridik tan olish, tugunlarni boshqarish va pilot sinov mezonlarini belgilash zarurligi asoslanadi.

INTRODUCTION

Digital transformation has penetrated almost all stages of higher education management. The transition of student registries, assessment results, transcripts, and diploma data into electronic form has accelerated document circulation, reduced dependence on paper, and centralized management data. However, digitalization itself does not automatically guarantee the immutability, external verifiability, and long-term reliability of documents. In particular, when an academic document is verified by another university, employer, or foreign organization, the dependence of the verification process on a central operator becomes a significant problem.

Although centralized systems such as HEMIS are effective for operational management, from an architectural perspective, storing data within a limited cluster of servers creates the risk of a single point of failure. Abuse of administrator privileges, cyberattacks, misconfiguration, or technical disruptions may affect data availability and integrity. Furthermore, an external verifier cannot independently confirm through cryptographic means that a record in the central database has remained unchanged.

Blockchain technology attracts attention at precisely this point not as an alternative, but as an additional layer of trust. The idea of a distributed ledger proposed by Nakamoto [1] was subsequently studied in the field of education for the verification of academic records, reputation, and credential management [2, 3]. The main value of blockchain in education lies not in placing the document itself on a public network, but in recording its cryptographic fingerprint together with a timestamp in an immutable ledger and enabling independent verification by a third party.

Therefore, the aim of the study is not to replace HEMIS, but to develop a scientific and technical model for integrating an external verification layer based on hash functions, Merkle trees, IPFS, and a consortium blockchain into the existing centralized management system. The research question is formulated as follows: how can the integrity and independent verifiability of academic documents be strengthened through blockchain while preserving the operational convenience of a centralized educational information system?

MATERIALS AND METHODS

The study was based on conceptual architecture analysis, the comparative method, and scenario-based risk assessment. No empirical pilot test was conducted. Therefore, the percentages and reductions in time presented in the results are estimated indicators based on similar architectures, the characteristics of cryptographic operations, and the logical model of the proposed workflow.

At the first stage, the lifecycle of an academic document was identified: document creation, validation, storage, updating, presentation, and verification by a third party. At the second stage, the trust points and vulnerabilities in the centralized model were identified, and the way in which they are redistributed in the blockchain-based model was analyzed. At the third stage, a hybrid architecture consisting of the SHA-256 hash function, a Merkle tree, IPFS, and a permissioned consortium blockchain was developed. At the fourth stage, the model was compared according to the criteria of integrity, verification speed, dependence on the central server, scalability, privacy, and cost.

A cryptographic hash function generates a fixed-length digital fingerprint from the content of a document. Even a minor change in the document produces a different hash value; in practice, it is impossible to reconstruct the original document from the hash. This characteristic makes it possible to verify only the integrity of the document without placing the document itself on the blockchain.

Instead of recording a large number of documents as separate transactions, the use of a Merkle tree is proposed. The hashes of individual documents are combined in pairs to generate a single Merkle root. A verifier checks whether a particular document belongs to this

root using a Merkle proof. This approach makes it possible to verify thousands of documents using a single root hash.

Storing large PDF files and attachments directly on the blockchain is not appropriate from economic and privacy perspectives. Therefore, it is proposed that the file itself be stored in IPFS or a controlled distributed storage layer, while the blockchain stores the CID, Merkle root, timestamp, and digital signature of the authorized organization. Avoiding the direct recording of open personal identifiers on the blockchain is adopted as a privacy principle.

RESULTS

The analysis indicates that blockchain should operate as an external verification layer while HEMIS continues performing routine academic administration. This separation preserves institutional efficiency and simultaneously provides immutable cryptographic evidence for third-party verification.

Table 1. Comparative evaluation of centralized and blockchain-based educational document management

Indicator	Centralized model	Hybrid blockchain model	Expected outcome
Single point of failure	High	Low	Improved resilience
External verification	Institution-dependent	Merkle proof	Independent audit
International validation	Days or weeks	Seconds or minutes	Faster verification
Server dependence	Continuous	Reduced	Lower infrastructure load
Privacy	Central access control	Off-chain storage + hash	Privacy by design

The comparative assessment demonstrates that blockchain significantly improves document integrity and verification transparency while avoiding unnecessary storage of personal data on-chain. The proposed architecture therefore balances scalability, privacy, and institutional governance.

Table 2. Proposed pilot evaluation indicators

Indicator	Measurement	Expected direction
Verification time	Submission to confirmation	Reduction
Integrity detection	Modified hash + Merkle proof	100% detection
Scalability	1k–100k documents	Logarithmic verification
Privacy	On-chain audit	No personal data stored
Fault tolerance	Node outage simulation	Service continuity

DISCUSSION

The findings demonstrate that the value of blockchain in education does not lie in the idea of "moving all data to a decentralized network." On the contrary, preserving the existing HEMIS infrastructure and adding an external verifiability layer is an institutionally less disruptive and technically more realistic approach. This position makes it possible to evaluate blockchain not as an end in itself, but as a tool for solving a specific trust problem.

The international circulation of educational documents constitutes one of the strongest practical foundations for this model. When a graduate submits a diploma to a foreign university or employer, verification may no longer depend on the response speed of the central operator. A cryptographic proof confirms that the document was entered into the ledger by an authorized issuer at a particular time. However, this mechanism does not automatically eliminate processes such as apostille, recognition of qualifications, or the legal equivalence of the content of a document; it primarily performs the function of verifying authenticity and integrity.

Privacy requires particular caution. Recording a person's full name, passport information, grades, or other personal data in an immutable ledger in an open form may subsequently create legal problems associated with their correction or deletion. Therefore, in the proposed model, personal data are stored off-chain, while only minimal cryptographic

evidence is retained in the on-chain layer. This architecture reconciles technical efficiency with the principle of data minimization.

Legal recognition is no less important than technical architecture. The institutions of electronic documents and electronic signatures provide a basis for ensuring the legal validity of digital documents [4]; however, the evidentiary status of a record in a consortium blockchain, the authority of node operators, the procedure for correcting an erroneous record, ledger governance, and the boundaries of liability require separate regulatory clarity. A technically immutable record does not legally mean an "error-free record"; incorrect information can also be recorded immutably. Therefore, a legal model for issuer authentication and corrective transactions is necessary.

From an economic perspective, the advantages of blockchain are not automatic either. The energy and transaction costs of public Proof-of-Work networks may be unsuitable for a public education system. If a permissioned consortium network uses a PBFT-type consensus mechanism or other energy-efficient mechanisms, costs and governance may be more sustainable. In this case, the main costs may arise not from the blockchain itself, but from integration, node infrastructure, cybersecurity, key management, and staff training.

The main limitation of the study is the absence of an empirical pilot. Therefore, at the next stage, it would be appropriate to organize a limited pilot within a single university, for example, by combining a set of certificates or transcripts issued during one semester into a Merkle tree and recording them on consortium nodes. If the pilot results are measured according to the criteria presented in Table 2, theoretical assumptions can be replaced with actual indicators.

CONCLUSION

The study demonstrated that the most justified application of blockchain technology in educational document workflow is to strengthen document integrity and independent verification. Instead of completely replacing centralized systems such as HEMIS, the creation of an additional trust layer consisting of SHA-256, a Merkle tree, IPFS, and a permissioned consortium blockchain was assessed as a relatively realistic model that can be implemented gradually under the conditions of Uzbekistan.

In the proposed model, the document itself is not placed on the blockchain. The document remains in a controlled off-chain storage system, while its hash, Merkle root, timestamp, and minimal information confirming the issuer are stored on the blockchain. This approach creates a balance between scalability, privacy, and verifiability.

Before practical implementation, three areas must be addressed in parallel: first, verification speed, cost, and fault tolerance must be measured through pilot technical tests; second, standards for node governance, key protection, and cybersecurity must be established; and third, a clear legal mechanism must be developed concerning the legal status of blockchain records, correction procedures, and personal data protection. Only then can blockchain become not merely another technological slogan in the digitalization of education, but a verifiable and legally reliable element of infrastructure.

REFERENCES

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
2. Grech, A., & Camilleri, A. F. (2017). Blockchain in Education. European Commission.
3. Sharples, M., & Domingue, J. (2016). The Blockchain and Kudos.
4. Legislation of the Republic of Uzbekistan on Electronic Documents and Digital Signatures.
5. Official HEMIS documentation and higher education information system guidelines.