UDC 004.056:004.75
IRSTI 20.23.17

https://doi.org/10.55452/1998-6688-2026-23-3-267-281

[1]Sakhipov A.A.,
PhD, Assistant Professor, ORCID ID: 0000-0003-1045-4199,
e-mail: aivar.sakhipov@astanait.edu.kz
[1*]Fedenko A.D.,
MSc, Teacher, ORCID ID: 0009-0000-2290-6995,
*e-mail: a.fedenko@astanait.edu.kz

[1]Astana IT University, Astana, Kazakhstan

ENSURING DATA INTEGRITY OF EXAMINATION RESULTS USING PERMISSIONED DISTRIBUTED LEDGER TECHNOLOGY

Abstract

The increasing use of centralised Student Information Systems (SIS) as part of the digitalisation of higher education has led to these systems being used despite the risk of unauthorised alteration of student data due to reliance of data entry and administration on one administrative trust domain. This paper presents the design and experimental validation of a Distributed Ledger Technology (DLT) architecture to provide verifiable integrity of examination results. The proposed architecture is based on a combination of an SQL-based SIS and a Hyperledger Fabric Blockchain via a secure middleware layer. Examination records in the SIS are converted to a cryptographic hash commitment and stored on an immutable ledger. Experimental validation was carried out by deploying a Hyperledger Fabric Network in a containerized environment and testing it using Hyperledger Caliper at workload levels up to 120,000 transactions. Key performance metrics were throughput, commit latency, ability to detect violations of data integrity and storage characteristics of the ledger. The proposed architecture achieved throughput of 728 transactions/second and maximum throughput of 842 transactions/second with average commit latency less than 2.0 seconds. Tampering tests were performed to verify the architecture's ability to detect unauthorised changes and it successfully detected all unauthorised changes with average detection time of 19.8ms. Analysis of storage requirements showed that the ledger grew linearly and would require less than 5.68 GB over ten years. The results demonstrate that the proposed architecture eliminates the single point of failure in centralized systems and provides scalable, cryptographically verifiable academic record integrity.

Keywords: distributed ledger technology, blockchain, data integrity, information security, Hyperledger Fabric, student information systems, academic records.

Received April 6, 2026; revised June 29, 2026; accepted August 24, 2026.

Introduction

Relatively recent large-scale digitalization of the field of higher education has resulted in the almost complete adoption of both Student Information Systems (SIS) and Learning Management Systems (LMS) in the use of centralized Relational Database Management Systems (RDBMS) for storing and managing student records. For purposes of this research, data integrity (DI) is defined as the property that once an academic record has been submitted by an authorized party, it will not be possible to alter the record without being detected; whereas, the term "verifiability" defines the capability of an unaffiliated third-party to independently verify through cryptography the validity of a submitted record without trusting the submitting entity. Although the reliability, scalability, and efficiency of centralized RDBMS architectures are well-documented, the fact that these systems can only function within a single administrative trust domain means that they are vulnerable to various forms of threats from privileged insiders including but not limited to, direct tampering with the

databases, modification of audit logs [1, 2]. These architectural limitations create an inherent risk to the overall integrity of the system, as unauthorized modifications made directly to the database could result in no evidence of such alterations remaining which would be subject to cryptographic proof [3, 4].

In this respect, existing limitations are especially concerning when it comes to managing results from examinations – because in this case, students' academic records represent the main evidence that support the issue of their qualifications as well as the employers who wish to verify those qualifications. Access control systems, transaction logging, and database replication mechanisms that exist within SISs (e.g., schools' student information systems) can protect against unauthorized use of these systems; however, they cannot provide the same level of mathematical guarantee regarding the immutability of these records using cryptography [5, 6]. Other studies have demonstrated how blockchain-based access control systems can be used to secure the private and integrity of an individual's academic record through the use of cryptography to verify academic credentials [7]. Therefore, despite the existence of such technologies, the institutional trust in students' academic records remains dependent upon central authority controls rather than the mathematically verifiable integrity of those records [8]. Studies have demonstrated that permissioned blockchain networks have greatly enhanced the level of data integrity and trust associated with them as opposed to traditional centralized database systems [9].

Distributed Ledger Technologies (DLTs) are emerging as an immutable, append-only and consensually validated data storage technology using cryptography to create a secure data infrastructure for recording data across multiple independent nodes [10, 11]. The literature has shown that Hyperledger Fabric's permissioned consensus model provides robust data integrity assurances and dependable transaction validation models [12]. For this study, DLT will be operationally defined as a permissioned decentralized system where data integrity is maintained via cryptographic hash functions, digital signatures and consensus protocols instead of by central authorities [13]. The vast majority of prior research into the application of educational blockchains have focused on the issuing of digital diplomas and the validation of credentials using public blockchain architectures [14]. Various implementations utilizing Hyperledger Fabric have illustrated the ability to securely and resistively manage academic credentials using decentralized verification models [15]. Other research has shown that blockchain-based examination monitoring and credentialing systems can increase academic integrity and build trust in digital assessment environments [16]. Although this demonstrates the practicality of validating credentials in a decentralized manner it does not show how to maintain the integrity of the examination records created during the academic lifecycle. Additionally, public blockchain architectures are subject to a number of limitations including privacy compliance issues, throughput limitations and unregulated participation from external networks limiting their use within academic institutions requiring the use of sensitive student data [5, 17].

This highlights a significant research need: the lack of experimentally verified architectures which can ensure the continuous, privacy-preserving, institutionally-controlled, and cryptographically-verifiable integrity protection of examination results at the point of generation in SIS environments of universities. In particular, current solutions are unable to generate a method of creating an unalterable record of examination results (a record anchored to a public immutable ledger) in near-real-time while meeting all of the necessary parameters of institutional access control, privacy, and scalability.

The objective of this paper is to create, develop, and experimentally test a permissioned DLT architecture which will ensure the cryptographically-verifiable integrity of examination results created by university information systems [18]. The architecture uses a Hyperledger Fabric-based permissioned blockchain and an existing SQL-based SIS via a secure API middleware layer. The architecture utilizes SHA-256 cryptographic hashing, X.509-based digital identity management, and multi-endorsed smart contracts to create immutable integrity-proof records of examinations without storing any personally identifiable information on chain.

The key scientific contribution of this research is the experimental validation of a hybrid SIS-DLT architecture for deterministic detection of unauthorized modifications using cryptographic integrity verification. Results suggest that integrating permissioned blockchain with an academic database substantially reduces the single-point-of-failure risk present in centralised architectures while maintaining operational performance sufficient for university-scale workloads.

Materials and methods

The system was designed as a hybrid integrity assurance architecture integrating a centralized SIS with a permissioned DLT network implemented using Hyperledger Fabric v2.5 [10, 19]. The SIS, implemented on PostgreSQL v15, functioned as the authoritative data source for academic records, while the blockchain layer served as an independent, append-only integrity verification layer maintaining cryptographic commitments to examination results. Transaction mediation, identity authentication, and integrity commitment generation were performed by an API gateway implemented in Node.js, which isolated the operational database from direct blockchain interaction and enforced strict access control [20, 21]. The overall system architecture and trust boundaries are illustrated in Figure 1.

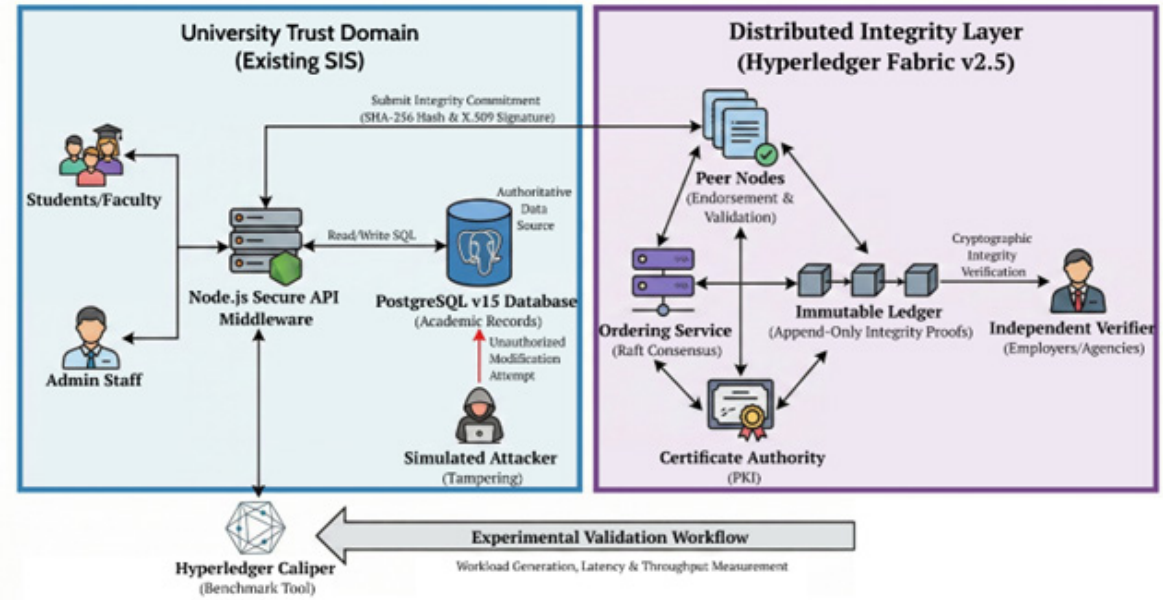

Figure 1 – Hybrid SIS–DLT integrity verification architecture and validation workflow

The integrity model was formally defined as a state consistency verification problem between two independent storage domains: a mutable operational database and an immutable distributed ledger. Let denote the SIS database state at time , and denote the ledger state representing the sequence of committed integrity proofs; integrity preservation is satisfied if and only if every committed academic record in corresponds to a unique, previously committed ledger state entry and no ledger entry can be modified, removed, or reordered. Integrity verification was carried out as a deterministic state reconciliation (reconciliation is a process for identifying discrepancies) where SIS data records are converted to canonical form, hashed with SHA-256 and compared to ledger commitments that were indexed with composite identifiers [2, 14]. Due to the pre-image resistance and collision resistance characteristics of SHA-256, any changes made to SIS records after the ledger has been committed would result in a detectable divergence of states. The complete integrity commitment and verification workflow is illustrated in Figure 2.

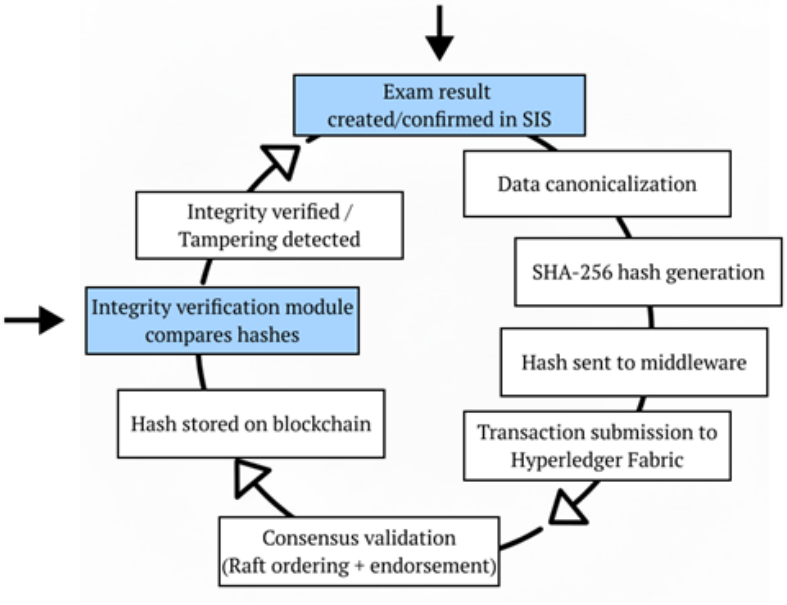

Figure 2 – Continuous integrity verification workflow
and blockchain hash anchoring process

The blockchain network was deployed as a permissioned consortium with authenticated peer nodes representing independent trust domains and coordinated using the Raft consensus protocol [22, 23]. Each transaction required cryptographic authentication via X.509 certificates issued by the Hyperledger Fabric Certificate Authority and validation through smart contract logic enforcing endorsement policies [24]. The smart contract implemented deterministic state transition rules ensuring that only valid, authenticated, and consensus-endorsed integrity commitments could be appended to the ledger. This architecture eliminated the single point of failure characteristic of centralized systems and ensured that no single administrative entity could unilaterally modify committed integrity proofs.

Experimental validation was performed with the use of a server which is specifically designated for the purposes of evaluating blockchain performance. A total of three peer nodes and one ordering node along with a single certificate authority node were created by deploying each of them as Docker containers on an instance of Ubuntu Server 22.04. To ensure that there would be no hardware-based performance bias and to enable the ability to reproduce results with identical configurations each of the nodes had been allocated equal virtualized hardware (SSD storage; 4 vCPUs; 8 GB RAM). In addition to these configuration specifications, the server environment was designed to represent a real-world institutional implementation of a blockchain solution by utilizing a number of key features such as persistent ledger storage, secure cryptographic identity management and network isolation. Hyperledger Caliper was utilized to generate transactional workloads that simulated the act of submitting and verifying student examination results during realistic academic workload conditions [25]. Key system configuration parameters are listed in Table 1.

Integrity verification effectiveness was measured as the system's ability to detect unauthorized record modification under controlled tampering scenarios. Detection latency, defined as the elapsed time between unauthorized database modification and integrity violation detection, was recorded for each experimental run. System performance was evaluated in terms of transaction throughput, commit latency, and resource utilization under increasing workload intensity. The experimental workflow and integrity verification process are shown in Figure 1.

Table 1 – Experimental system configuration and integrity validation parameters

Parameter	Specification	Function
Blockchain platform	Hyperledger Fabric v2.5	Distributed integrity ledger
Consensus mechanism	Raft	Deterministic transaction ordering
Identity framework	X.509 PKI	Cryptographic authentication
Hash function	SHA-256	Integrity commitment generation
Smart contract runtime	Go chaincode	Integrity validation logic
State database	CouchDB	Ledger state indexing
Operational database	PostgreSQL v15	SIS academic record storage
Middleware	Node.js v20	Transaction mediation
Benchmark tool	Hyperledger Caliper	Performance and integrity testing
Deployment environment	Docker, Ubuntu Server 22.04	Reproducible distributed execution

Results and discussion

The experimental evaluation was conducted to assess the performance, scalability, and integrity enforcement capability of the proposed SIS–DLT architecture under realistic academic workload conditions. A total of 120,000 examination record transactions were generated and submitted to the system over multiple benchmark runs, simulating grade submission patterns typical of midterm and final examination periods. The system demonstrated stable and predictable behavior throughout the experimental period, with no observed transaction failures, ledger inconsistencies, or state divergence under normal operating conditions [11, 22]. These results are consistent with reliable operation under sustained institutional workloads without compromising integrity guarantees.

Transaction throughput, commit latency, and peer node CPU utilization were measured across a range of workload intensities from 50 TPS to 850 TPS to evaluate system scalability and resource efficiency under increasing transactional load. The system achieved a mean sustained throughput of 728 TPS and reached a maximum throughput of 842 TPS before performance saturation occurred due to endorsement validation overhead and ordering service batching constraints [17, 21]. Mean transaction commit latency remained below 0.6 seconds at moderate load levels (≤300 Transactions Per Second, TPS) and increased progressively to 1.97 seconds at peak load, reflecting predictable consensus processing and cryptographic validation overhead [10, 23].

Peer node CPU utilization increased proportionally with transaction throughput, reaching a mean utilization of 63% and a maximum of 71% at peak workload intensity, indicating efficient utilization of available computational resources without exceeding operational capacity limits.

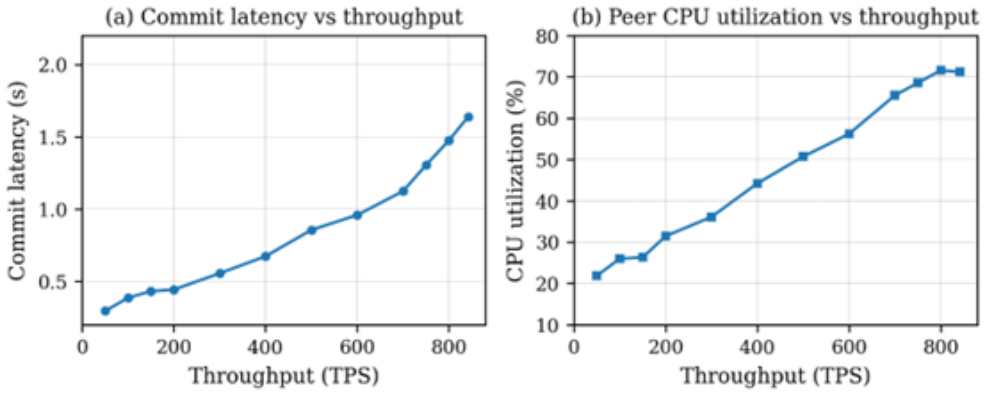

Figure 3 – System performance versus transaction throughput:
(a) commit latency; (b) CPU utilization

The primary reason for the observed latency increases as workload increases is due to the required processes for validating endorsements, i.e., verifying the signatures via cryptography and checking the state consistency among multiple peer nodes. Unlike probabilistic consensus methods (e.g. proof-of-work) utilized by most public blockchains, Raft uses a deterministic method of achieving finality for committed transactions; this means that once a transaction has been finalized it cannot be reversed or forked. The deterministic commit model also provides certainty when validating the integrity of information committed to the ledger; therefore, after an academic record is committed to the ledger, the record will always be verifiably permanent. The measured latency values are still within operational limits since examination result submissions are generally non-latency sensitive and are submitted in batch submissions.

Long duration benchmark testing was performed on the testbed at high transaction rates in order to assess the systems stability when operating under prolonged periods of high workload conditions. Results from these tests showed that the system continued to operate stably for extended periods of time with no indication of resources being exhausted, no memory leaks occurring and no overall degradation in system performance. Average memory usage remained relatively constant at approximately 588MB of memory per peer node during the entire testing period, thus providing supporting evidence of the efficiency of the blockchain execution environment. CPU and Memory usage for each peer node remained temporally consistent during prolonged periods of continuous operation and is shown in Figure 4. As can be seen there is no upward trend in memory usage indicating no memory leaks occurred, and thus the system's ability to execute for extended periods of time was demonstrated.

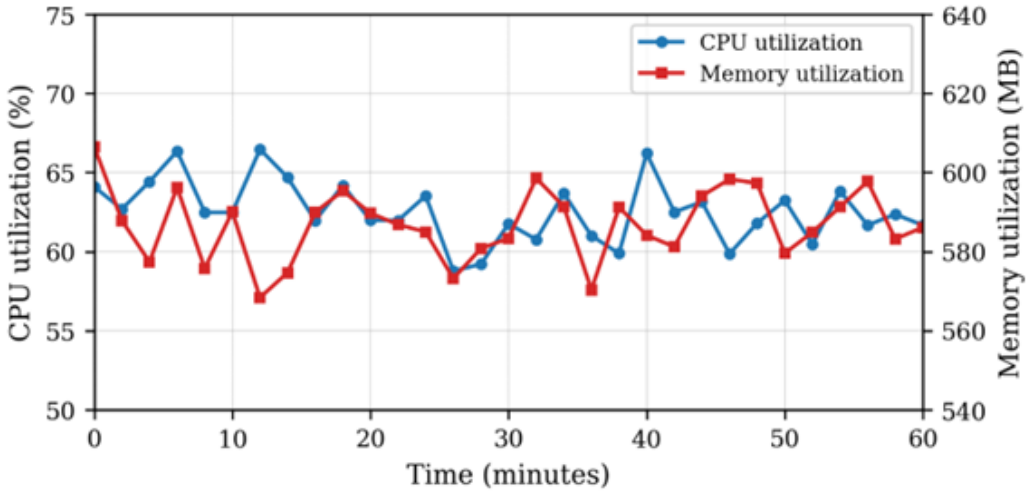

Figure 4 – Peer node CPU and memory utilization over time under sustained workload

These results suggest that the computational overhead associated with cryptographic integrity enforcement may remain within the operational capacity of standard institutional server infrastructure. The ordering service exhibited significantly lower resource utilization compared to peer nodes, confirming that endorsement validation and signature verification represent the dominant computational cost. This finding aligns with the expected performance characteristics of permissioned blockchain architectures, where integrity assurance is enforced through cryptographic verification rather than computational consensus competition. The observed resource utilization indicates that the proposed architecture may be deployable using conventional university virtual infrastructure without requiring specialised hardware.

Integrity protection effectiveness was evaluated using controlled database tampering experiments designed to simulate insider threats and privileged database compromise scenarios [4]. The verification

cycle shown in Figure 2 ensures continuous integrity monitoring independent of database trust assumptions. Unauthorized modifications were performed directly on the SIS PostgreSQL database after ledger commitment, including grade alteration, timestamp modification, record overwriting, and record deletion. Each modification attempt resulted in a detectable integrity violation due to mismatch between the recomputed SIS hash and the immutable ledger commitment. The detection performance results are summarized in Table 2.

Table 2 – Integrity violation detection performance under controlled database tampering scenarios

Attack type	Attempts (n)	Detection rate (%)	Latency (ms) min / mean / max
Grade modification	400	100	11 / 16.8 / 29
Timestamp modification	200	100	12 / 18.9 / 34
Record overwrite	150	100	15 / 22.1 / 41
Record deletion	150	100	17 / 23.4 / 46
Privileged bulk tampering	100	100	19 / 27.5 / 52
Total	1000	100	11 / 19.8 / 52

The system detected all 1,000 attack attempts (100% detection rate), indicating that database integrity was not compromised in any of the controlled tampering scenarios. In addition, the mean detection latency for all attacks was less than 52 ms, indicating that integrity violations were detected close to the time of the attack. The detection latency for these attacks is much better than other common methods of detecting integrity violations using audit logs of database transactions which are dependent upon an administrative control or policy and therefore do not provide a guarantee of integrity.

Additionally, the impact of performing integrity verification as part of the overall SIS system operation was determined and the performance of integrity verification queries were evaluated. The mean integrity verification time for the integrity verification queries was found to be 34 milliseconds. The maximum integrity verification time observed was 61 milliseconds. These results indicate that the integrity verification queries impose low overhead and may therefore be executed continuously without measurable degradation of SIS responsiveness.

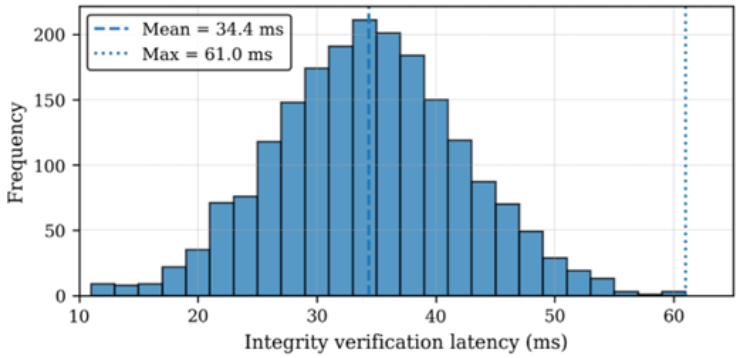

Figure 5 – Integrity verification latency distribution under operational workload

Ledger storage growth analysis indicated that blockchain storage requirements appear manageable and scale approximately linearly with transaction volume. The mean transaction size, including cryptographic signatures and metadata, was measured at 2.41 KB per examination record. Based on this measurement, an institution generating 100,000 examination records per year would produce approximately 241 MB of annual ledger growth. Storage growth projections are presented in Table 3.

Table 3 – Blockchain ledger storage growth and scalability projection under institutional workload

Parameter	50,000 records/year	100,000 records/year	200,000 records/year
Mean transaction size	2.41 KB	2.41 KB	2.41 KB
Mean daily transactions	137	274	548
Mean block size	0.33 MB	0.66 MB	1.32 MB
Blocks generated per year	152	305	610
Annual ledger growth	120 MB	241 MB	482 MB
CouchDB index overhead (~18%)	22 MB	43 MB	87 MB
Total annual storage footprint	142 MB	284 MB	569 MB
5-year cumulative growth	710 MB	1.42 GB	2.84 GB
10-year cumulative growth	1.42 GB	2.84 GB	5.68 GB

As previously mentioned, there were other studies done on the performance of Hyperledger Fabric, where it was shown that the ledger grew at a rate less than 5 GB over multiple years of institutional usage as long as they used off chain data storage and made on-chain commitments to the integrity of their data [26, 27]. By utilizing a hybrid approach where only the commitments for the cryptographic verification of the records are stored on the blockchain and the complete records for all students are kept in the Student Information System (SIS) database, we can significantly reduce the need for storage space for the blockchain while still maintaining the level of cryptographic verifiability needed. Therefore, the proposed model will meet the requirement for the scalability of continuously protecting the integrity of student records without creating any new bottlenecks or constraints in terms of infrastructure.

Although the proposed architecture has shown its feasibility as well as advantages regarding security and privacy, it increases the time needed to confirm transactions, i.e., the time for committing transactions when compared to the classical central databases that usually allow a write operation within milliseconds. As indicated above, the blockchain based commit latency of approximately 0.5 – 2.0 seconds includes the computational effort for cryptographic validations and the enforcement of the consensus process (i.e., (1) hash computation and digital signature verification; (2) multi-node endorsement validation; (3) consensus-based ordering of transactions). It has been also reported in other studies that evaluate the performance of the Hyperledger Fabric blockchain framework that similar delay characteristics are present in order to achieve a deterministic finality of the transactions, while the delay times for the commit operation range from 0.4 to 3.0 seconds dependent on the chosen endorsement policy and number of nodes in the network [28, 29]. The results obtained during the experimentation show that these delays do not affect the usability of the application because the submission of examination records is an interactive administrative process rather than a real-time transaction with high latency requirements. From a systems engineering perspective, this delay represents an acceptable tradeoff in order to obtain strong integrity guarantees that cannot be obtained through classical central database architectures.

To contextualise the proposed SIS–DLT architecture, it is necessary to distinguish it from established non-blockchain approaches to database integrity assurance. The principal alternatives applicable to academic information systems include: (i) integrity-coded database schemes, (ii) write-once read-many (WORM) storage solutions, (iii) database-level audit logging, and (iv) hash-based file integrity monitoring. ICDB approaches [30] embed cryptographic integrity codes directly into the relational schema and verify query correctness at retrieval time; however, they rely on a trusted client agent and do not produce a consensus-validated integrity record accessible to external verifiers. WORM solutions prevent post-write modification but are administered by the same entity controlling the source data, placing the trust boundary at the assumed threat actor. Audit log frameworks record modification events within the database layer, where a sufficiently privileged insider can suppress entries prior to detection [31]. The critical distinction of the proposed architecture is that the integrity commitment chain is maintained by independent peer nodes under Byzantine fault-tolerant consensus,

ensuring that no single administrator can modify committed hash records without consensus approval from the remaining peer organizations. A comparative summary is presented in Table 4.

Table 4 – Comparative analysis of database integrity assurance approaches

Property	Proposed SIS–DLT	Integrity Coded DB [30]	WORM Storage	Audit Log Framework [31]
Trust model	Distributed consensus (multi-node)	Trusted client agent	Centralized administrator	Centralized DBMS layer
Insider tamper resistance	Yes – consensus-enforced	Partial – agent-dependent	Partial – admin-dependent	No – logs modifiable
Tamper detection	Cryptographic hash divergence	IC mismatch at query time	Not applicable (prevention only)	Policy-dependent review
Mean detection latency	19.8 ms (this study)	Query execution time	N/A	Post-event review
External verifiability	Yes — auditable within consortium	No	No	No
Single point of trust	Eliminated	Present (ICDB agent)	Present (storage admin)	Present (DBMS layer)
Performance overhead	Moderate (< 2 s commit latency)	Moderate (query verification)	Minimal	Minimal
Cryptographic mechanism	SHA-256 + Merkle tree + X.509	MAC-based integrity codes	Optional hash digest	None by default
Ongoing storage growth	Linear (2.41 KB/ transaction)	Linear (IC + placeholder overhead)	Linear	Linear

The high level of throughput from our experimental testing also illustrates that the proposed architecture could be implemented on an institutional scale, and still achieve performance that would not degrade. The architecture was able to sustain throughputs of over 728 TPS with peak throughputs reaching 842 TPS, both numbers far exceeding normal university SIS environment requirements for the volume of grades submitted during peak times for exams (i.e., 50-100 TPS). The architecture's performance is consistent with previous studies on permissioned blockchain systems that have found that consensus protocols like Raft result in much greater throughput and lower latency than do public blockchain consensus methods [26, 29]. Our measured linear scalability until saturation indicates that this architecture can handle increased institutional size and workloads, along with increased student populations, without impacting its performance. This type of scalability is critical to maintaining the viability of blockchain based systems designed to ensure academic integrity.

There are several limits to this proposed architecture that need to be taken into account when implementing in a real-world deployment scenario. First, blockchains only protect integrity after data has been committed to the blockchain, therefore, organizational controls and multi-party validation processes will continue to be required to prevent incorrect or fraudulent submissions at the time of data entry. Second, the introduction of additional infrastructure for the deployment of blockchain nodes, certificate authority management, and secure cryptography key management, etc., adds to the overall complexity of deploying the architecture versus traditional SIS architectures. Finally, although the Raft consensus protocol offers highly efficient and deterministic transaction ordering, it assumes that all peer nodes involved in the consensus process will be available and that they will not introduce faults in the process; thus, some additional fault tolerance mechanisms may be required to protect against failures in geographically distributed implementations. These limits highlight the importance of designing blockchain integrity assurance with robust institutional governance and operational security frameworks [32].

The Node.js middleware layer represents a trust boundary not fully captured by the blockchain consensus model. The middleware is responsible for SHA-256 hash computation, X.509 transaction signing, and submission to the Fabric peer network. A compromised instance could submit incorrect hash commitments to the ledger without the consensus mechanism detecting the discrepancy, since consensus validates cryptographic structure rather than the semantic relationship between committed hashes and the source database state. In the current implementation, this risk is mitigated through: (i) X.509 identity credentials issued by the Fabric Certificate Authority, providing non-repudiation and enabling post-hoc attribution of anomalous commitments; (ii) deployment within a network-isolated application tier; and (iii) periodic cross-validation by independent peer node operators. Complete elimination of this trust boundary would require in-database hash computation via database-native triggers, which represents a direction for future architectural refinement.

The architecture raises privacy considerations relevant to jurisdictions subject to personal data protection regulations. The proposed system stores only SHA-256 hash commitments on-chain; examination records, student identifiers, and associated metadata remain exclusively within the operational SIS database. This off-chain design is consistent with GDPR data minimization principles and has been validated for academic certification contexts [33]. However, the cryptographic binding between on-chain commitments and database records enables record-level inference if both components are simultaneously compromised. Additionally, the right to erasure under applicable data protection law requires consideration: while off-chain records can be deleted in accordance with institutional retention policies, on-chain hash commitments remain permanently anchored. Institutional deployment should therefore be accompanied by legal assessment of hash-only on-chain entries under applicable data protection law, as regulatory guidance on this classification continues to evolve [33].

Practical deployment additionally requires consideration of governance factors beyond technical performance. Permissioned blockchain networks require frameworks addressing node membership policies, endorsement policy configuration, channel management, certificate lifecycle, and chaincode versioning procedures. Research on blockchain adoption in higher education identifies governance complexity and regulatory compliance requirements as significant inhibitors that substantially extend practical implementation timelines beyond what technical benchmarks suggest [34]. The overhead of maintaining Hyperledger Fabric infrastructure – including Certificate Authority management, peer software updates, cryptographic key rotation, and ledger backups – represents an administrative burden that must be absorbed by institutional IT governance. These governance considerations do not diminish the integrity assurance value of the architecture but constitute essential contextual factors for decision-makers assessing deployment feasibility and total cost of ownership.

A further limitation is that experimental validation was conducted exclusively within a single-institution SIS deployment context. The reported performance characteristics, tamper detection accuracy, and storage scalability projections reflect this specific environment and should not be extrapolated uncritically to multi-institution consortium configurations. The mean throughput of 728 TPS observed under single-institution conditions may decrease in multi-organization deployments due to increased cross-organizational endorsement latency and inter-peer communication overhead. Research on blockchain adoption in higher education further highlights that consortium deployments introduce additional challenges related to data schema standardization, interoperability with heterogeneous SIS infrastructures, and alignment of institutional governance obligations [34] – none of which were evaluated in this study. Extension to consortium settings is identified as a priority direction for future research.

The practical applicability and scientific significance of the proposed architecture extend beyond examination result protection and support broader academic data integrity assurance scenarios [35, 36]. The system enables (1) deterministic detection of unauthorized academic record modification, (2) elimination of the single point of failure inherent in centralized database architectures, and (3) independent cryptographic verification of academic record authenticity by external entities such as employers and accreditation bodies. These capabilities directly address

longstanding challenges in academic credential verification and digital trust management [37]. From a scientific perspective, this work provides evidence that permissioned DLT may function as a scalable and operationally feasible integrity assurance layer, rather than merely a credential issuance mechanism. The architecture therefore represents a meaningful contribution to the application of distributed ledger technology to securing academic information systems.

Future research should extend the architecture to multi-institution consortium networks for decentralized academic record verification across universities, accreditation agencies, and governmental organizations. Additional directions include automated grading system integration, anomaly detection for suspicious grading patterns, and post-quantum cryptographic mechanisms for long-term security resilience.

Conclusion

This study designed and validated a hybrid SIS-DLT architecture using Hyperledger Fabric for cryptographic integrity verification of examination records. The system achieved 728 TPS mean throughput (842 TPS peak) with commit latency below 2 seconds, and demonstrated 100% detection of unauthorized modifications with detection latency under 52 ms.

The results indicate that integrating permissioned blockchain technology with a centralized academic database substantially reduces the single point of failure risk of administratively-controlled SIS environments by replacing institutionally-anchored trust with cryptographically-enforced integrity commitments validated by independent peer organizations. The hybrid off-chain and on-chain model offers a potentially feasible balance between operational scalability and integrity assurance, with experimental results providing initial support for its applicability to real-world higher education environments under the deployment and governance conditions discussed above. It should be noted, however, that the evaluated architecture represents a single-institution implementation, and that multi-institution consortium deployments would introduce additional technical and governance considerations not captured in the present experimental scope.

Within the experimental parameters evaluated, the proposed system demonstrated scalable and stable performance characteristics consistent with institutional-scale deployment requirements, and the cryptographic commitment model enables independent verification of examination record integrity by authorized parties outside the institutional administrative chain. These findings contribute supporting evidence for permissioned distributed ledger technology in academic data integrity assurance, while the identified limitations – regarding single-institution scope, middleware trust assumptions, governance overhead, and privacy regulatory considerations – provide concrete directions for subsequent research and architectural refinement.

REFERENCES

1 Cardenas-Quispe, M.A., and Pacheco, A. Blockchain ensuring academic integrity with a degree verification prototype. Scientific Reports, 15 (1), 9281 (2025). https://doi.org/10.1038/s41598-025-93913-6

2 Chaudhari, S., and Shirole, M. Blockchain-driven academic learning record management in higher education: A comprehensive review of methodologies, applications, benefits, and challenges. SN Computer Science, 6 (5), 427 (2025). https://doi.org/10.1007/s42979-025-03952-z

3 Sangeetha, A.S., and Shunmugan, S. Privacy-enabled academic certificate authentication and deep learning-based student performance prediction system using Hyperledger blockchain technology. Journal of Parallel and Distributed Computing, 204, 105119 (2025). https://doi.org/10.1016/j.jpdc.2025.105119

4 Khaleelullah, S., Vangapalli, S.T., Gaddam, M., Hanumakonda, V.S., and Gangapuram, U.K.G. Verification of academic records using Hyperledger Fabric and IPFS. Proceedings of the 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN), 210–217 (2023). https://doi.org/10.1109/ICPCSN58827.2023.00040

5 Ajwalia, M., and Shah, P. Performance comparison of permissioned and permissionless blockchain by varying workload transaction. BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 5 (4), 100251 (2025). https://doi.org/10.1016/j.tbench.2025.100251

6 Cheng, H., Lu, J., Xiang, Z., and Song, B. A permissioned blockchain-based platform for education certificate verification. Lecture Notes in Computer Science, 456–471 (2020). https://doi.org/10.1007/978-981-15-9213-3_36

7 Saleh, O.S., Ghazali, O., and Idris, N.B. Enhancing academic certificate privacy with a Hyperledger Fabric blockchain-based access control approach. SN Computer Science, 4 (5), 602 (2023). https://doi.org/10.1007/s42979-023-02060-0

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

9 Kadhum, O.I., and Hamad, A.H. Performance evaluation of multi-organization e-government based on Hyperledger Fabric blockchain platform. Ingénierie des Systèmes d'Information, 28 (2), 499–507 (2023). https://doi.org/10.18280/isi.280227

10 Guggenberger, T., Sedlmeir, J., Fridgen, G., and Luckow, A. An in-depth investigation of the performance characteristics of Hyperledger Fabric. Computers and Industrial Engineering, 173, 108716 (2022). https://doi.org/10.1016/j.cie.2022.108716

11 Khan, M.M., Khan, F.S., Nadeem, M., Khan, T.H., Haider, S., and Daas, D. Scalability and efficiency analysis of Hyperledger Fabric and private Ethereum in smart contract execution. Computers, 14 (4), 132 (2025). https://doi.org/10.3390/computers14040132

12 Lohachab, A., Garg, S., Kang, B.H., and Amin, M.B. Performance evaluation of Hyperledger Fabric-enabled framework for pervasive peer-to-peer energy trading in smart cyber–physical systems. Future Generation Computer Systems, 118, 392–416 (2021). https://doi.org/10.1016/j.future.2021.01.023

13 Berrios Moya, J.A., Ayoade, J., and Uddin, M.A. A zero-knowledge proof-enabled blockchain-based academic record verification system. Sensors, 25 (11), 3450 (2025). https://doi.org/10.3390/s25113450

14 Xu, Y. Development of blockchain-based academic credential verification system. Open Access Library Journal, 11 (9), 1–20 (2024). https://doi.org/10.4236/oalib.1112130

15 Pulmano, C.E., Estuar, M.R.J.E., De Leon, M.M., Tan, H.C.L., Co, N.A.S., and Tamayo, L.P.V. Towards the development of a blockchain-based decentralized digital credential system using Hyperledger Fabric for participatory governance. Procedia Computer Science, 219, 99–106 (2023). https://doi.org/10.1016/j.procs.2023.01.269

16 Sakhipov A. Beyond face recognition: A multi-layered approach to academic integrity in online exams / A. Sakhipov, I. Omirzak, A. Fedenko // Electronic Journal of e-Learning. – 2025. – № 23(1). – P. 81–95. https://doi.org/10.34190/ejel.23.1.3896.

17 Thakkar, P., Nathan, S., and Viswanathan, B. Performance benchmarking and optimizing Hyperledger Fabric blockchain platform. Proceedings of the IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), 264–276 (2018). https://doi.org/10.1109/MASCOTS.2018.00034

18 Panwar, A., Sugandh, U., Jain, A., Jain, V., Kumar Dubey, A.K., Majumdar, S., and Mallik, S. Enhancing trust and transparency in education using blockchain: A Hyperledger Fabric-based framework. Artificial Intelligence and Applications (2025). https://doi.org/10.47852/bonviewAIA52026268

19 Dreyer, J., Fischer, M., and Tönjes, R. Performance analysis of Hyperledger Fabric 2.0 blockchain platform. Proceedings of the Workshop on Cloud Continuum Services for Smart IoT Systems, 32–38 (2020). https://doi.org/10.1145/3417310.3431398

20 Das, S.R., Zaman, N., Asirvatham, D., Ashfaq, F., Masud, M., and Shorfuzzaman, M. Empirical performance analysis of Hyperledger Fabric. SSRN Electronic Journal (2025). https://doi.org/10.2139/ssrn.5127328

21 Sadath, M.L., Mehrotra, D., and Kumar, A. Scalability performance analysis of blockchain using hierarchical model in healthcare. Blockchain in Healthcare Today, 7 (1) (2024). https://doi.org/10.30953/bhty.v7.295

22 Nasir, Q., Qasse, I.A., Abu Talib, M., and Nassif, A.B. Performance analysis of Hyperledger Fabric platforms. Security and Communication Networks, 2018, 1–14 (2018). https://doi.org/10.1155/2018/3976093

23 Enare Abang, J., Takruri, H., Al-Zaidi, R., and Al-Khalidi, M. Latency performance modelling in Hyperledger Fabric blockchain: Challenges and directions with an IoT perspective. Internet of Things, 26, 101217 (2024). https://doi.org/10.1016/j.iot.2024.101217

24 Khan, D., Jung, L.T., Hashmani, M.A., and Cheong, M.K. Empirical performance analysis of Hyperledger LTS for small and medium enterprises. Sensors, 22 (3), 915 (2022). https://doi.org/10.3390/s22030915

25 Zulkarnain, M.M., Ramli, N., and Nordin, A.N. Performance benchmarking of Hyperledger Fabric on heterogeneous hardware for IoT applications. IIUM Engineering Journal, 26 (3), 156–170 (2025). https://doi.org/10.31436/iiumej.v26i3.3610

26 Honar Pajooh, H., Rashid, M.A., Alam, F., and Demidenko, S. Experimental performance analysis of a scalable distributed Hyperledger Fabric for a large-scale IoT testbed. Sensors, 22 (13), 4868 (2022). https://doi.org/10.3390/s22134868

27 Lu, N., Zhang, Y., Shi, W., Kumari, S., and Choo, K.K.R. A secure and scalable data integrity auditing scheme based on Hyperledger Fabric. Computers and Security, 92, 101741 (2020). https://doi.org/10.1016/j.cose.2020.101741

28 Honar Pajooh, H., Rashid, M., Alam, F., and Demidenko, S. Hyperledger Fabric blockchain for securing the edge Internet of Things. Sensors, 21 (2), 359 (2021). https://doi.org/10.3390/s21020359

29 Jung, S., Yoo, Y., Yang, G., and Yoo, C. Prediction of permissioned blockchain performance for resource scaling configurations. ICT Express, 10 (6), 1253–1258 (2024). https://doi.org/10.1016/j.icte.2024.09.003

30 Yeh, J.-H., Arifin, M.M., Shen, N., Karki, U., Xie, Y., and Nanjundarao, A. Integrity coded databases – protecting data integrity for outsourced databases. Computers & Security, 136, 103569 (2024). https://doi.org/10.1016/j.cose.2023.103569

31 Deep, G., Sidhu, J., and Mohana, R. Insider threat prevention in distributed database as a service cloud environment. Computers & Industrial Engineering, 169, 108278 (2022). https://doi.org/10.1016/j.cie.2022.108278

32 Psarra, E., Apostolou, D., Verginadis, Y., Patiniotakis, I., and Mentzas, G. Permissioned blockchain network for proactive access control to electronic health records. BMC Medical Informatics and Decision Making, 24 (1), 303 (2024). https://doi.org/10.1186/s12911-024-02708-8

33 Gómez Vieites, A., Delgado-von-Eitzen, C., and Estévez Garcia, D. GDPR-compliant academic certification via blockchain: legal and technical validation of the GAVIN Project. Applied Sciences, 15 (16), 9191 (2025). https://doi.org/10.3390/app15169191

34 Pathak, B., Alakkad, M.F., and Kumar, V. Institutional environment and the use of blockchain technology: exploring the context and conditions of using blockchain in higher education institutions. Higher Education Quarterly, 79 (3), e70034 (2025). https://doi.org/10.1111/hequ.70034

35 Dias, P., Gonçalves, H., Silva, F., Duque, J., Martins, J., and Godinho, A. Blockchain technologies: A scrutiny into Hyperledger Fabric for higher educational institutions. Procedia Computer Science, 237, 213–220 (2024). https://doi.org/10.1016/j.procs.2024.05.098

36 Jaafar, R.A., and Alsaad, S.N. Enhancing educational certificate verification with blockchain and IPFS: A decentralized approach using Hyperledger Fabric. TEM Journal, 2385–2395 (2023). https://doi.org/10.18421/TEM124-51

37 Silaghi, D.L., and Popescu, D.E. A systematic review of blockchain-based initiatives in comparison to best practices used in higher education institutions. Computers, 14 (4), 141 (2025). https://doi.org/10.3390/computers14040141

[1]Сахипов А.А.,
PhD, ассистент профессор, ORCID ID: 0000-0003-1045-4199,
e-mail: aivar.sakhipov@astanait.edu.kz
[1*]Феденко А.Д.,
магистр, оқытушы, ORCID ID: 0009-0000-2290-6995,
*e-mail: a.fedenko@astanait.edu.kz

[1]Astana IT University, Astana, Kazakhstan

ТАРАТЫЛҒАН ТІЗІЛІМ ТЕХНОЛОГИЯСЫН ПАЙДАЛАНУ АРҚЫЛЫ ЕМТИХАН НӘТИЖЕЛЕРІ ДЕРЕКТЕРІНІҢ ТҰТАСТЫҒЫН ҚАМТАМАСЫЗ ЕТУ

Аңдатпа

Жоғары білім беруді цифрландыру аясында орталықтандырылған студенттік ақпараттық жүйелердің (Student Information Systems, SIS) кең қолданылуы студент деректерінің рұқсатсыз өзгертілу қаупін арттырады, себебі барлық деректер енгізу мен басқару бір әкімшілік сенім доменіне тәуелді. Мақалада емтихан нәтижелерінің криптографиялық тексерілетін тұтастығын қамтамасыз етуге арналатын таратылған тізілім технологиясы (Distributed Ledger Technology, DLT) архитектурасының жобалануы және эксперименттік тексеруі ұсынылған. Ұсынылған архитектура SQL-негізіндегі SIS және Hyperledger Fabric блокчейн жүйесін қауіпсіз middleware қабаты арқылы біріктіруге негізделген. SIS жүйесіндегі емтихан жазбалары криптографиялық hash-commitment түріне түрлендіріліп, өзгермейтін ledger-де сақталады. Эксперименттік тексеру контейнерленген ортада нақты Hyperledger Fabric желісін орналастыру және Hyperledger Caliper көмегімен 120,000 транзакцияға дейінгі жүктеме кезінде тестілеу арқылы жүргізілді. Негізгі көрсеткіштер өткізу қабілеті, бекіту кідірісі, деректер тұтастығының бұзылуын анықтау мүмкіндігі және тізілімді сақтау сипаттамалары болды. Архитектура 728 транзакция/секунд өткізу қабілетін және 842 транзакция/секунд максималды өткізу қабілетін көрсетті, ал орташа бекіту кідірісі 2.0 секундтан аз болды. Рұқсатсыз қол сұғуды анықтау тесттері барлық рұқсатсыз өзгерістерді орташа 19.8 мс уақытта анықтағанын көрсетті. Сақтау талдауы тізілімнің сызықты өсетінін және он жыл ішінде 5.68 ГБ-тан аз орын қажет ететінін көрсетті. Нәтижелер ұсынылған архитектура орталықтандырылған жүйелерге тән бірыңғай істен шығу нүктесі мәселесін жоятынын және академиялық жазбалардың масштабталатын, криптографиялық тексерілетін тұтастығын қамтамасыз ететінін дәлелдейді.

Түйін сөздер: таратылған тізілім технологиясы, блокчейн, деректер тұтастығы, ақпараттық қауіпсіздік, Hyperledger Fabric, студенттік ақпараттық жүйелер, академиялық жазбалар

[1]Сахипов А.А.,
PhD, ассистент профессор, ORCID ID: 0000-0003-1045-4199,
e-mail: aivar.sakhipov@astanait.edu.kz
[1*]Феденко А.Д.,
магистр, преподаватель, ORCID ID: 0009-0000-2290-6995,
*e-mail: a.fedenko@astanait.edu.kz
1Astana IT University, Astana, Kazakhstan

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ДАННЫХ РЕЗУЛЬТАТОВ ЭКЗАМЕНОВ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННОГО РЕЕСТРА

Аннотация

Расширенное использование централизованных студенческих информационных систем (Student Information Systems, SIS) в условиях цифровизации высшего образования увеличивает риск несанкционированного изменения данных студентов, поскольку ввод и управление данными зависят от одного административного доверенного домена. В данной работе представлена разработка и экспериментальная проверка архитектуры технологии распределенного реестра (Distributed Ledger Technology, DLT), предназначенной для обеспечения криптографически проверяемой целостности экзаменационных результатов. Предложенная

архитектура основана на интеграции SQL-ориентированной SIS и блокчейн-системы Hyperledger Fabric через защищенный middleware-слой. Экзаменационные записи SIS преобразуются в криптографическое hash-commitment и сохраняются в неизменяемом ledger. Экспериментальная проверка проводилась путем развертывания реальной сети Hyperledger Fabric в контейнеризированной среде и тестирования с использованием Hyperledger Caliper при нагрузке до 120,000 транзакций. Основными показателями были пропускная способность, задержка фиксации, способность обнаружения нарушений целостности данных и характеристики хранения реестра. Архитектура достигла пропускной способности 728 транзакций/секунду и максимальной пропускной способности 842 транзакции/секунду при средней задержке фиксации менее 2.0 секунд. Тесты на несанкционированное вмешательство показали успешное обнаружение всех несанкционированных изменений со средним временем обнаружения 19.8 мс. Анализ хранения показал линейный рост реестра и потребность менее 5.68 ГБ за десять лет. Результаты демонстрируют, что предложенная архитектура устраняет единую точку отказа, присущую централизованным системам, и обеспечивает масштабируемую криптографически проверяемую целостность академических записей.

Ключевые слова: технология распределенного реестра, блокчейн, целостность данных, информационная безопасность, Hyperledger Fabric, студенческие информационные системы, академические записи.