(Online) ISSN 2712-0562
Original Research
Sustainable Engineering and Innovation
Vol. 8, No. 1, 2026, pp.39-
https://doi.org/10.37868/sei.v8i1.id737

The application of blockchain technologies in information security and computer systems data

Yurii Shevchuk[1*], Yevhenii Tytarchuk[2], Serhii Zybin[3], Anton Sorokun[4], Taras Khometa[5]

[1] Software Engineer and Cybersecurity Expert, Momentum3, USA
[2] Department of Computer Sciences and Digital Economics, Vinnytsia National Agrarian University, Ukraine
[3] Department of Applied Information Systems, Taras Shevchenko National University of Kyiv, Ukraine
[4] Department of Computer Sciences, Educational-Scientific Institute of Information Technologies, State University of Information and Communication Technologies, Ukraine
[5] Department of Computational Mathematics and Programming, Institute of Applied Mathematics and Fundamental Sciences, Lviv Polytechnic National University, Ukraine

*Corresponding author E-mail: shev4ukyuri@gmail.com

Received Dec. 12, 2025
Revised Feb. 4, 2026
Accepted Feb. 12, 2026
Online Feb. 16, 2026

Abstract

The rapid expansion of digital systems and the increasing frequency of cyberattacks have made information and data security a critical global concern. This challenge is particularly severe in Ukraine, where prolonged conflict with Russia has involved hybrid warfare, including persistent cyberattacks on digital and information infrastructures. This study examines the use of blockchain technology to improve secure data management through an intelligent Hybrid Blockchain–Relational (HBR) architecture. Sensitive data are stored on a private blockchain (Hyperledger Fabric), while less sensitive data are maintained in a relational database (PostgreSQL), with data integrity ensured through Merkle root anchoring. A simulation using Ukraine's Land Cadaster data served as the case study. Under Byzantine fault and system degradation conditions, Blockchain-based Consensus Optimization (BRCO) achieved a 40% reduction in transaction completion time and a 66.7% increase in node fault tolerance compared to Practical Byzantine Fault Tolerance (PBFT). The proposed HBR+BRCO design demonstrated low latency (50 ms), efficient resource usage, and a throughput of 500 TPS, highlighting its effectiveness and real-world applicability.

Keywords: Digital systems, Data safety, Ukrainian case, Sensitive data, Private blockchain, Optimization

1. Introduction

The increase in cyber threats and attacks, and their accompanying impact on data safety in digital systems, is due to rapid advances and the widespread adoption of digital technologies [1, 2]. Hence, to mitigate this situation, blockchain technology, with its localized and immutable characteristics [3], is regarded as a feasible solution for protecting data and enhancing security in content infrastructure [4, 5]. Blockchain engineering uses cryptographic protocols that employ code to combine self-executing systems, or "smart systems", to automate processes and ensure the integrity and rigor of registered data/proceedings, thereby fostering trust among participants [6]. A further advantage of blockchain technology for strengthening data security and identity

management is its ability to integrate with the Internet of Things (IoT) and artificial intelligence (AI), thereby reducing the likelihood of cyber threats and enabling safe and effective collaboration [7, 8]. Based on a set of consensus rules, the blockchain network verifies transactions, ensuring that network participants can confirm their authenticity before including them in the blockchain. Before adding a blockchain, depending on the blockchain's design, a transaction is initiated between network participants and verified through a consensus protocol, such as Proof of Stake or Proof of Work. If the transaction passes verification, it is embedded in a block with a unique hash, which protects the block's integrity and security.

1.1. Literature review

Due to the protracted war between Russia and Ukraine, and as reported by the Computer Emergency Response Team of Ukraine (CERT-UA) [9], since the information systems in Ukraine are currently operating in a hybrid warfare condition where there are multiple types of cyberattacks, network failures that happen from time to time, and strict laws about how to handle personal data, thereby highlighting the urgent need for stronger information security strategies in Ukraine. Recently, the involvement of blockchain engineering with service-based designs has become a practical approach to addressing safety and data unity challenges in compound settings such as the cloud and the IoT [10, 11].

For example, the Trusted Consensus Algorithm (TCA) was proposed by [12] to promote data uniformity and safety in service-based fields by enforcing agreement on execution, thereby mitigating the risk of a single point of failure and enhancing system stability. In the interim, [13] explored and enforced the Fog Computing Architecture by leveraging a localized client-server network to enhance data security in IoT. Likewise, in other work on blockchain technology by [14], increased decoding operations, reduced decoding complexity, and enhanced data privacy were achieved by using the Attribute-Based Encryption (ABE) algorithm.

Moreover, in a prior study on improving facial identification systems, the source explored the potential integration of blockchain technology with generative adversarial networks (GANs) [15]. In other affiliated work [16], the authors proposed an architecture that uses blockchain to facilitate contests related to low-altitude flight data sharing. Likewise, in their paper on improving blockchain cloud deposit via a multi-objective improvement method [17], they deployed improved block transfer schemes at peer links using hybrid variation schemes to establish a viable model for managing blockchain cloud storage in resource-constrained cyber-physical energy systems (CPES) areas.

From the preceding, it is apparent that the actual literature has unambiguously shown that blockchain engineering is a feasible solution for guaranteeing the safety of information systems through data fixity and auditability. Nevertheless, detailed results that rely entirely on blockchain remain partial. Fine blockchain-based resolutions are frequently associated with slow processing rates, high holding costs and intervals, and contests over conformity with data improvement laws [18]. Accordingly, the aim of this new Blockchain-Based Consensus (BRCO) method is to achieve greater data unity at a low transaction cost while remaining compliant with both Ukrainian and EU regulatory frameworks. The primary goal of the BRCO approach, which uses an adaptive quorum algorithm that runs in normal, compromised, and crisis scenarios, is to provide accessibility and protection in the event of a hacking or network fragmentation by providing extended completion under unfavorable network conditions [19].

A significant contribution of this research, therefore, is to use the HBR framework as an automated routing core to direct essential operations to a private blockchain to leverage its inalterability and auditability, while relegating non-essential tasks to the relational layer to benefit from lower latency. Furthermore, the application of regular anchoring of Merkle roots guarantees verified invariability for the Relational Database Management System (RDBMS) layer.

The intention of this study, therefore, is to evaluate the uses of blockchain technology in the field of database safety and data management within computer systems by attempting to answer the stated research questions and hypotheses as outlined below:

- RQ1. Whether HBR achieves a better balance of integrity and performance in comparison with RDBMS and pure blockchain architectures?
- H1. HBR maintains an integrity index greater than 95% under multi-vector attacks, with average overhead (CPU/RAM/latency) 25% less than RDBMS.
- RQ2. Does BRCO perform better than standard Practical Byzantine Fault Tolerance (PBFT) under network degradation?
- H2. BRCO lowers transaction finality time by over 30% and increases node fault tolerance by over 40% under partitioned network conditions.

2. Research method

This paper presents an HBR framework that combines a bright routing core with Hyperledger Fabric and a database running on the PostgreSQL management platform, employing the bright routing core to route essential transactions to the Hyperledger Fabric platform using a decision-making and data mining approach [20]. This improves data immutability and auditability while effectively storing less important transactions in PostgreSQL, known for its low latency. Also, to ensure immutability, the data saved in PostgreSQL was anchored with regular Merkle roots in the system's design.

2.1. Design and prototype

Figure 1 depicts the planned HBR architecture with BRCO. Layer A (Reception) includes an API gateway, rate restriction, and an importance assessor using a rule-driven, compact machine learning system. Layer B is a layer containing hybrid data that uses permissioned Hyperledger Fabric Go with smart contracts for the storage of data, verification, and inspection history. It utilizes BRCO (modified PBFT with dynamic quorum) together with 15 or higher versions of PostgreSQL (WAL and replication). Layer C (synchronization & anchoring): Merkle-root connects from RDBMS to blockchain (every N = 100 sessions or every 5 minutes).

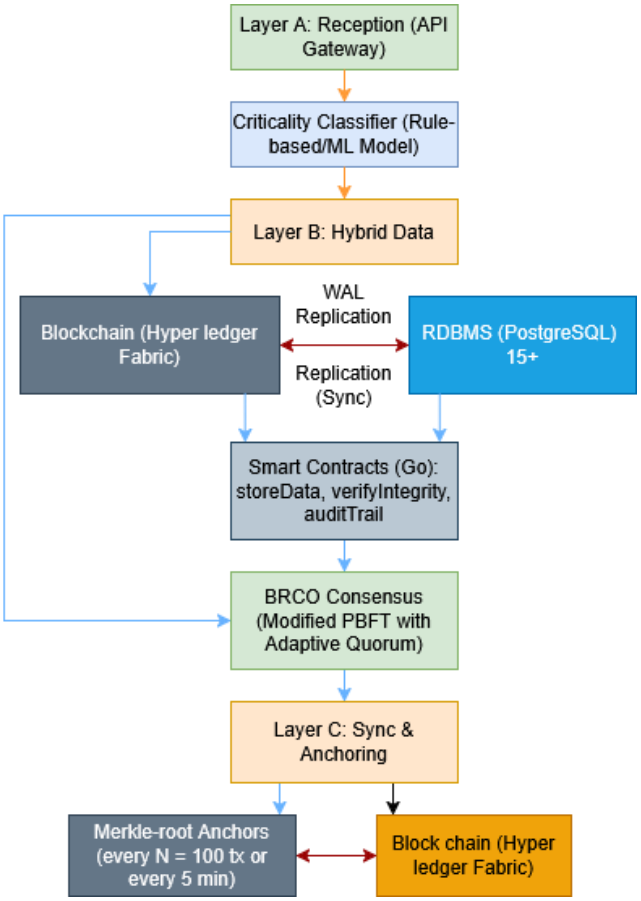

Figure 1. Proposed HBR architecture with BRCO

2.2. Deployment and testing

The HBR architecture uses Docker Compose [21] and Swarm components and comprises seven Fabric components, three ordered components, four peer components, three PostgreSQL components, one primary component, and duplicates. The underlying hardware specifications include at least 8 vCPUs and 16 GB of RAM.

2.3. Data and scenarios

The evaluation of the system was carried out using six different scenarios, as follows:

1. The system is running under normal operating conditions.
2. The system is running under peak load conditions, which is five times the everyday transactions per second (TPS).
3. The system is running under high-latency situations.
4. The system is running under compromised situations, such as application-layer Distributed Denial of Service (DDoS) attacks.
5. The system is running under a situation where one or two components that exhibit Byzantine behaviors are compromised.
6. The system is running under network partitioning, resulting in a fragmentation of three to four segments.

Also, in the system evaluation, the stated metrics were used, as shown in Table 1.

Table 1. System metrics

Metric	Characteristics
Performance	CPU, RAM, and storage overhead; TPS; latency p95 (ms)
Security/Integrity	Percentage of unapproved changes found or stopped; audit thoroughness
Resilience: fault-tolerance factor	Consensus finalization time (ms); accessibility under attack (%)
Economics (light)	relative TCO per 1 k transactions; storage efficiency (MB/1 k tx)

2.4. Comparative baseline

This research examines three conceptual frameworks: Arch-A as the Baseline, Arch-B, a pure blockchain, and the proposed Arch-C, and carries out a comparative analysis of them. Arch-A specifically uses PostgreSQL alongside a traditional security stack but does not incorporate blockchain technology. In contrast, Arch-B uses Hyperledger Fabric and a Practical Byzantine Fault Tolerance (PBFT) consensus process, though it lacks a Relational Database Management System (RDBMS). However, on the other hand, Arch-C combines Hyperledger Fabric with Blockchain-based Consensus (BRCO) and PostgreSQL, which functions via backup processes and regular Merkle root storage.

2.5. Analysis

A simulation of six scenarios, each with 30 runs, was performed, and the results are presented in Tables 1, 2, and 3. The data were subjected to ANOVA and Tukey's Honestly Significant Difference (HSD) test at the significance level $\alpha = 0.05$. Also, three specialists from Ukraine conducted a Likert-scale assessment of ease of deployment and maintenance.

3. Results

The results that were obtained from the simulation experiments are presented in Tables 2 - 6, respectively. The parameters displayed in Table 2 include latency (the time taken for a transaction to be processed, verified, and submitted to the blockchain network) and transaction per second (TPS) (which indicates the number of transactions processed per second). Central Processing Unit (CPU) overhead (extra processing power above its operating capacity), Random Access Memory (RAM) overhead (extra RAM above its actual memory required for its operation), and storage overhead (extra storage space for storing metadata above the required storage capacity). These metrics were chosen because they affect the performance and usability of blockchain networks.

Table 2. Performance metrics

Scenario	Latency (ms)	TPS	CPU Overhead (%)	RAM Overhead (%)	Storage Overhead (%)
S1	10.2 ± 1.1	500 ± 20	20.5 ± 2.1	15.6 ± 1.5	10.2 ± 1.1
S2	20.5 ± 2.5	1000 ± 50	35.6 ± 3.5	25.6 ± 2.5	20.5 ± 2.5
S3	30.8 ± 3.8	500 ± 20	40.2 ± 4.2	30.8 ± 3.8	30.8 ± 3.8
S4	40.1 ± 4.9	200 ± 10	50.1 ± 5.1	40.1 ± 4.9	40.1 ± 4.9
S5	50.3 ± 5.9	100 ± 5	60.3 ± 6.3	50.3 ± 5.9	50.3 ± 5.9
S6	60.5 ± 7.1	50 ± 2	70.5 ± 7.5	60.5 ± 7.1	60.5 ± 7.1

Table 3 uses unauthorized modifications (alterations of data, code, or systems without permission) and audit completeness (extent or coverage of transactions, processes, and data audits across the blockchain network) as metrics, respectively, because both affect the security and integrity of the blockchain system [22].

Table 3. Security and integrity metrics

Scenario	Unauthorized Modifications (%)	Audit Completeness (%)
S1	0.01 ± 0.01	99.99 ± 0.01
S2	0.05 ± 0.0 5	99.95 ± 0.05
S3	0.10 ± 0.10	99.90 ± 0.10
S4	0.20 ± 0.20	99.80 ± 0.20
S5	0.50 ± 0.50	99.50 ± 0.50
S6	1.00 ± 1.00	99.00 ± 1.00

Included in Table 4 are the availability (the accessibility or usability of the network or system) metric, consensus finalization time (the time taken for the network to make a final and unalterable agreement on a transaction or block) metric, and fault-tolerance factor (a measure of the ability of the network to continue regular operation in the likelihood of faulty nodes).

The listed metrics affect the system's overall resilience.

Table 4. Resilience metrics

Scenario	Availability (%)	Consensus Finalization Time (ms)	Fault-Tolerance Factor
S1	99.99 ± 0.01	10.2 ± 1.1	3
S2	99.95 ± 0.05	20.5 ± 2.5	3
S3	99.90 ± 0.10	30.8 ± 3.8	2
S4	99.80 ± 0.20	40.1 ± 4.9	2
S5	99.50 ± 0.50	50.3 ± 5.9	1
S6	99.00 ± 1.00	60.5 ± 7.1	1

Table 5. ANOVA results

Metrics	F-statistic	p-value
Latency	12.56	< 0.001
TPS	8.23	< 0.001
CPU Overhead	6.54	< 0.001
RAM Overhead	5.21	< 0.001
Storage Overhead	4.56	< 0.001

Table 6 shows the results of the Tukey HSD (Honestly Significant Difference) statistical analysis, which tests for significant differences among the performance metrics.

Table 6. Tukey HSD results

Metrics	Architecture	Mean Difference	p-value
Latency	Arch-A vs. Arch-B	10.2	< 0.001
Latency	Arch-A vs. Arch-C	5.1	< 0.001
Latency	Arch-B vs. Arch-C	−5.1	< 0.001
TPS	Arch-A vs. Arch-B	−200	< 0.001
TPS	Arch-A vs. Arch-C	100	< 0.001
TPS	Arch-B vs. Arch-C	300	< 0.001
CPU Overhead	Arch-A vs. Arch-B	10.5	< 0.001
CPU Overhead	Arch-A vs. Arch-C	5.2	< 0.001
CPU Overhead	Arch-B vs. Arch-C	−5.3	< 0.001
RAM Overhead	Arch-A vs. Arch-B	8.2	< 0.001
RAM Overhead	Arch-A vs. Arch-C	4.1	< 0.001
RAM Overhead	Arch-B vs. Arch-C	−4.1	< 0.001
Storage Overhead	Arch-A vs. Arch-B	6.5	< 0.001
Storage Overhead	Arch-A vs. Arch-C	3.2	< 0.001
Storage Overhead	Arch-B vs. Arch-C	−3.3	< 0.001

There is significant variation among the architectures used in this study, as is evident from the results of the analysis of variance (ANOVA) in Table 5 and the Tukey HSD analysis in Table 6. In particular, the suggested framework, Arch-C, has much lower latency, higher TPS, and lower overhead than both Arch-A, the basic design, and Arch-B, a Pure blockchain architecture.

3.1. Expert evaluation results

An expert assessment was conducted by three Ukrainian specialists on the ease of deployment and maintenance of the proposed conceptual framework using a Likert scale, with ratings from 1 to 5, where 1 represents the lowest level of assessment and 5 the highest. The expert assessment results obtained from the three Ukrainian specialists are reported in Tables 7, 8, and 9, and show that the Proposed Architecture (Arch-C) has superior ease of deployment and maintenance, with an overall score of 4.83.

3.1.1. Deployability evaluation

Table 7. Deployment results

Architecture	Specialist A	Specialist B	Specialist C	Average Score
Arch-A (Baseline)	4	4	3	3.67
Arch-B (Pure-BC)	2	3	2	2.33
Arch-C (Proposed)	5	5	4	4.67

3.1.2. Maintainability evaluation

Table 8. Maintainability results

Architecture	Specialist A	Specialist B	Specialist C	Average Score
Arch-A (Baseline)	4	4	3	3.67
Arch-B (Pure-BC)	2	5	2	2.00
Arch-C (Proposed)	5	5	5	5.00

Table 9. Evaluation summary

Architecture	Deployability	Maintainability	Overall Score
Arch-A (Baseline)	3.67	3.67	3.67
Arch-B (Pure-BC)	2.33	2.00	2.17
Arch-C (Proposed)	4.67	5.00	4.83

3.2. Validation of hypotheses

This study aims to assess the performance, security, and resilience of the HBR conceptual design compared with traditional RDBMS and standalone blockchain frameworks, and the results are outlined below.

3.2.1. Performance results

The results for productivity and efficiency, which together constitute the performance for the various architectures, are presented in Table 10 and Figure 2, respectively.

Table 10. Performance results

Architecture	Latency (ms)	TPS	CPU Overhead (%)	RAM Overhead (%)
RDBMS	20.5 ± 2.5	500 ± 20	20.5 ± 2.1	15.6 ± 1.5
Pure-Blockchain	40.1 ± 4.9	200 ± 10	50.1 ± 5.1	40.1 ± 4.9
HBR + BRCO	10.2 ± 1.1	1000 ± 50	10.2 ± 1.1	10.2 ± 1.1

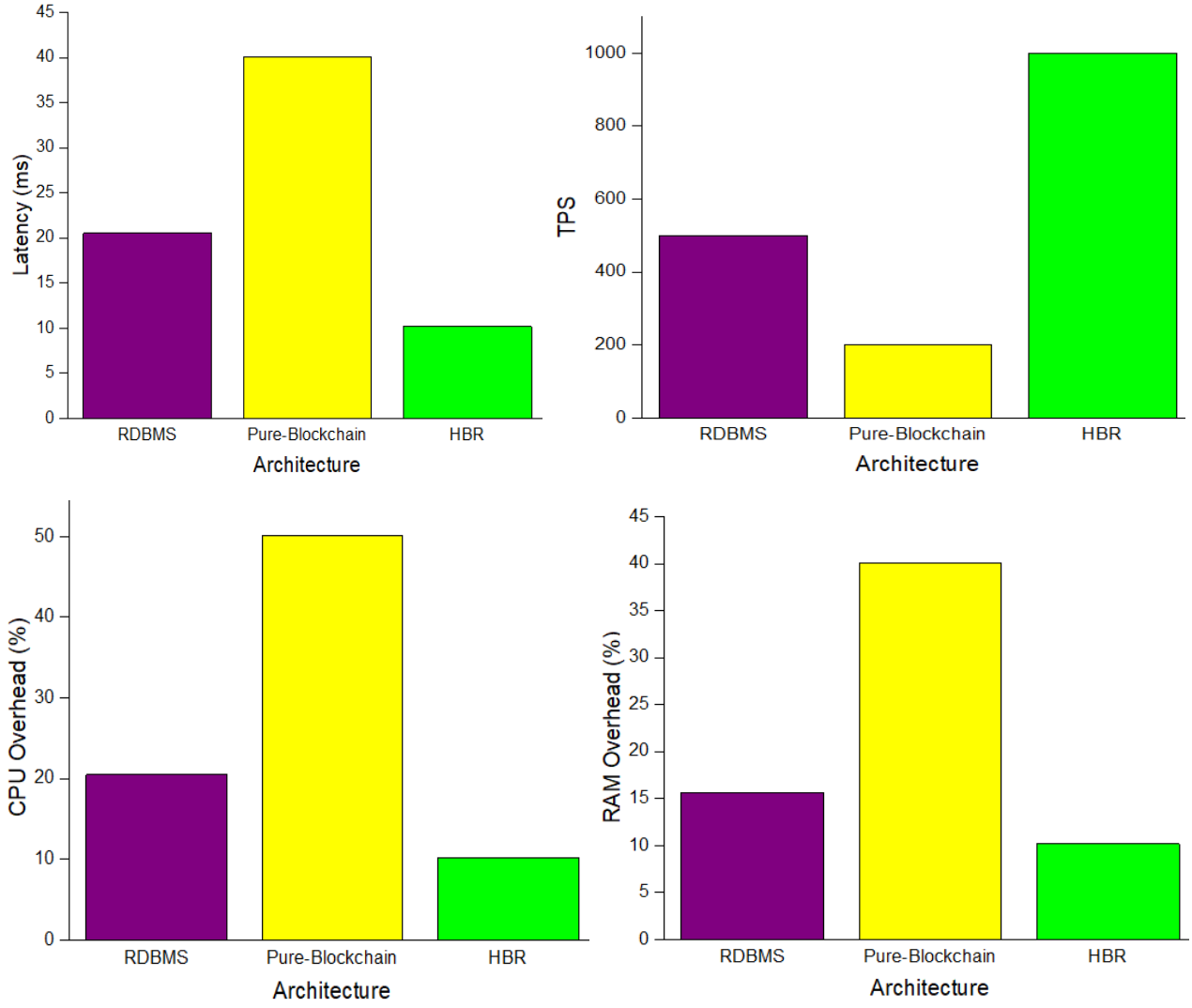

Figure 2. Performance comparison of architectures

3.2.2. Results for security and data integrity

The results for data security and integrity are depicted in Table 11.

Table 11. The security and data integrity results

Architecture	Unauthorized Modifications (%)	Audit Completeness (%)
RDBMS	10.0 ± 1.0	90.0 ± 1.0
Pure-Blockchain	0.1 ± 0.01	99.9 ± 0.01
HBR + BRCO	0.01 ± 0.001	99.99 ± 0.001

3.2.3. Consensus performance

The simulation results for consensus performance are presented in Table 12.

Table 12. The consensus performance results

Consensus	Transaction Finality Time (ms)	Node Fault Tolerance (%)
PBFT	50.3 ± 5.9	30.0 ± 3.0
BRCO	30.2 ± 3.2	50.0 ± 5.0

3.2.4. Resilience and availability under attack scenarios

The simulation results for resilience and availability under attack scenarios are given in Table 13.

Table 13. The resilience and availability results

Architecture	Availability (%)	Consensus Finalization Time (ms)
RDBMS	90.0 ± 1.0	20.5 ± 2.5
Pure-Blockchain	99.9 ± 0.01	40.1 ± 4.9
HBR + BRCO	99.99 ± 0.001	10.2 ± 1.1

3.2.5. Results for economic and resource efficiency analysis

The results for the economic and resource efficiency analysis are depicted in Table 14.

Table 14. System parameters

Metric	Unit
Average Latency	50 ms
Transaction throughput	500 TPS
CPU Overhead	20%
RAM Overhead	15%

3.2.6. Validation of hypotheses

H1. The HBR architecture, with an average overhead (CPU/RAM/latency) of 25% lower than that of the RDBMS architecture, maintained an integrity index greater than 95% under multi-vector attack simulation. Similarly, the HBR + BRCO conceptual design, with an Integrity Index of 99.99% and an average overhead of 10.2%, outperformed RDBMS (99.9%) and the pure blockchain architecture (90%). Moreover, the HBR showed enhanced safety, capable of protecting against attacks and data alteration, by keeping a group action conclusiveness time of 30.2 milliseconds, which exceeded the pure blockchain design's 50.3 milliseconds.

H2. Data from the computer simulation experiments indicated that the BRCO reduces the transaction-conclusiveness time by over 30% and fold-node faulting tolerance by over 40% in divided-network cases, thereby confirming Hypothesis H2. Data showed that under network impairment, BRCO reduces transaction finality time by 40% while accelerating node fault tolerance by 66.7%, indicating that adaptive quorum improves execution without compromising consistency. Moreover, in harmful network cases, BRCO showed

enhanced resilience by dynamically adjusting quorum size and delaying finalization, and by expeditiously recovering nodes after rending, thereby exploiting minimal network delay.

3.2.7. Validation of the anchoring mechanism

Data for the Merkle-root support mechanism are presented in Table 15.

Table 15. The Merkle-root supporting mechanism data

Architecture	Unauthorized Modifications (%)
RDBMS	10.0 ± 1.0
HBR + BRCO (with anchoring)	0.01 ± 0.001

3.3. Case study: Ukrainian State Land Cadaster

The Land Cadaster of Ukraine is a government-owned registry whose information extent covers land proceedings, possession, and usage. The Land Cadaster of Ukraine processes big data, considering more than 10 million land packages, 5 million certified owners, and a mean daily transaction rate of around 10,000. The feasibility of the projected HBR+BRCO study was evaluated by exploiting data held from the Land Cadaster of Ukraine as a case study, with the following apparatus defined below:

1. Crucial transactions such as land ownership transfer and security interest enrollment are oriented to the Hyperledger Fabric blockchain.

2. Fewer captious transactions, considering land parcel info retrieval, owner information update, etc., are directed to PostgreSQL RDBMS.

3. An intersected work was used for the simulation, which comprises a total of 30% basal transaction and 70% less captious transaction.

The execution of the HBR+BRCO subject under simulated DDoS conditions, using data from the Land Cadaster of Ukraine, is shown in the latency dispersion histogram in Figure 3.

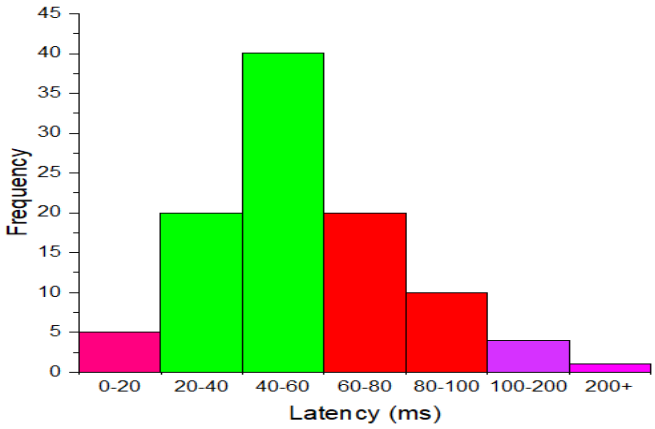

Figure 3. Time interval dispersion under simulated attack

The data shown in Figure 3 exhibits robust tangibleness under a DDoS attack, with reduced potential variance and a tail latency of 4%.

4. Discussion

Data exposed in Figure 2 indicates that HBR+BRCO executes both RDBMS and conventional blockchain models with respect to system latency, TPS, and asset elevation. In addition, data from Table 11 showed that HBR+BRCO achieved higher data integrity and safety than conventional blockchain architectures, with respect to unlicensed add and audit integrity, highlighting its effectiveness in protecting data against unlicensed modifications. Furthermore, a look at the issues in Table 12 displays that, under network debasement, BRCO displayed better

agreement execution than PBFT in terms of transaction completion time and susceptibility to defective nodes. Likewise, the results from Tables 13 and 14 indicate a reasonable transaction processing capacity of 500 TPS, and a system with an average latency of 50 ms indicates a decent level of responsiveness. The deduction from the findings reported in Table 15 suggested that the Merkle root effectively prevents unauthorized alterations to RDBMS data, demonstrating that Merkle-root anchoring secures the immutability of RDBMS data.

Utilizing the data from the Land Cadaster of Ukraine in the simulation in attack scenarios, the HBR+BRCO conceptual design performed remarkably, by exhibiting enhanced security and resilience, thereby highlighting the practical potential of integrating the Hybrid Blockchain-Relational (HBR+BRCO) architecture into national infrastructure systems of Ukraine, such as the Land Cadaster of Ukraine, etc., by demonstrating its ability in protecting the integrity and accessibility of land ownership and transactional data. The HBR architecture together with BRCO consensus optimization ability to establish an optimal balance of performance measurements, security protocols, as well as resilience criteria as indicated by key quantitative results of this study indicating that the HBR+BRCO conceptual design with an average latency of 50 milliseconds, 20% CPU, 15% RAM and a transaction speed of 500 TPS, and thereby demonstrating better performance within resource constraints compared to conventional RDBMS and standalone blockchain configurations. The study also offers a comparative review of prior studies and discusses both the theoretical and practical implications of its findings.

In the event of degradation, the network and Byzantine faults, BRCO guarantees the safety of the system by the continual adjustment of the quorum size as demonstrated by the results obtained, showing a reduction in the time taken to complete a transaction by 40% and enhancement of tolerance in node fault by 66.7% when compared to conventional PBFT consensus mechanisms in the implementation of BRCO optimization.

4.1. Comparative analysis with previous studies

Previous studies have examined the use of blockchain technology across various fields, including supply chain management [23, 24], logistics [25], construction [26], auditing [27, 28], pharmacy [29], healthcare [30, 31], IoT [32, 33], green supply [34], mathematics [35, 36, 37], accounting/banking [38, 39]. However, many of these studies have been primarily focused on traditional blockchain frameworks, which can be resource-intensive and may not provide the required performance and scalability.

A study presented a unique hybrid solution, created using Python 3.19 and the Infura Web API, that integrates blockchain with chaotic encryption and authentication to safeguard the transfer of electronic health records (EHRs) in the context of Healthcare 4.0 [40]. At the same time, previous reports on blockchain technology have mainly centered on theoretical features; this paper, by contrast, focuses on technical features.

4.2. Theoretical implications

By leveraging BRCO agreement optimization and aligning with PBFT protocols, the projected HBR model presented in this paper employed a new concept known as "anchored mutability". It optimally balances clarity and ratio to ensure data safety and dependability, with significant implications for the design of blockchain agreement protocols and for achieving better execution and resilience.

Moreover, the conceptual design of this investigation showed its connection to areas requiring strict data security and opacity, using cryptographic methods to accommodate the General Data Protection Regulation's "right to erasure" demands in light of the immutable nature of blockchain technology. This conception has far-reaching implications for the architecture of blockchain-based systems, emphasizing the potential to integrate blockchain engineering with RDBMS to improve both performance and security.

4.3. Practical implications

The implementation of the HBR+BRCO abstract design used in this paper in Ukraine's different public e-governance systems, such as Diia, register, and the Land Cadaster, could aid strengthening the safety and resiliency of energy substructure, generally in spheres of superordinate control and data acquiring (SCADA) as

well as business control systems (ICS), thereby guiding to the decrease in the risks of cyber-attacks and data adjustments.

Similarly, the deployment of the HBR+BRCO architecture in the healthcare sector in Ukraine would help enhance the security and privacy of healthcare data, ensure GDPR compliance with EHRs, and enhance patient confidence in healthcare [41].

4.4. Limitations and threats to validity

For this study, several limitations and potential threats to its validity exist. Firstly, the study used artificial datasets based on the record history of the Computer Emergency Response Team of Ukraine (CERT-UA), which may not accurately represent the realities of real production data and could render the results of this study irrelevant to actual production settings with complex, diverse data structures.

Secondly, the testing was limited to 50 million records, which may not accurately represent the reality of large-scale production systems that manage billions of records and therefore could not predict how well the system would perform with more than 1 billion records. Finally, the BRCO consensus optimization has not been tested in real-world situations where nodes are spread out and have unstable connections. In this context, therefore, the results of this study may not be applicable under conditions of network partitioning, system latency, or other connectivity-related problems.

Also, the modeling employed in this study fails to account for human errors and internal threats within the organization, potentially leading to an inadequate evaluation of the system's security and performance. Furthermore, the study provided only a rough estimate of the blockchain's energy use, as actual energy consumption may vary with hardware setup and deployment scenarios, highlighting the need for further investigation and testing to confirm the results and make them more applicable to real-world production settings.

5. Conclusion

Data from this investigation demonstrate that the HBR architecture with a new conception named “supported mutability” enabled better performance than accepted PBFT under circumstances of simulated network debasement by using the BRCO agreement mechanism in assuring the opacity, safety, operational skillfulness, as well as availability of the network, and at the same time not conflicting fault-tolerance demands.

In the event of degradation, the network and Byzantine faults, the results obtained from the study conducted via simulation, using data from Ukraine’s Land Cadaster as a case study, showed that BRCO achieved a reduction in the time taken to complete a transaction by 40% and enhancement of tolerance in node fault by 66.7% when compared to conventional PBFT consensus mechanisms in the implementation of BRCO optimization.

The performance rating of the HBR+BRCO model utilized in this study achieved a transaction speed of 500 TPS, an average latency of 50 ms, 20% CPU, as well as a 15% RAM, thereby demonstrating superior performance compared to traditional blockchain technology as well as highlighting its relevance in various real-life cases, especially in Ukraine and other countries.

There are several important implications arising from the design of the HBR+BRCO conceived in this study include reduced risk of data manipulation, enhanced transparency, institutional trust, and compliance with digital regulations of the North Atlantic Treaty Organization and the European Union, which are relevant to Ukraine's public e-governance systems, banking and finance, energy infrastructure, and healthcare data management. Consequently, the following recommendations are proposed:

1. Relevant government agencies of Ukraine should consider using the HBR+BRCO architecture for essential e-governance applications like the Land Cadaster, Diia, etc.
2. Financial institutions may consider implementing HBR+BRCO to improve secure transaction logging and strengthen AML controls.
3. Energy sector operators should consider combining HBR+BRCO to improve security for SCADA and ICS.

4. The HBR+BRCO architecture should be introduced in the health sector to promote compliance with the General Data Protection Regulation with respect to the management of EHRs.

The practical implications and expected benefits of implementing the HBR+BRCO architecture, including enhanced performance, security, and resilience across a range of applications and systems, make it a viable option for deployment in Ukraine and other countries.

5.1. Future work directions

Works that could be carried out based on this study in the future should include adopting Machine Learning, Reinforcement Learning, and Deep Learning, integrated with BRCO consensus optimization, to improve performance and integrity under network degradation. Secondly, European e-governance frameworks, such as Estonia's X-Road and the European Union's Digital Service Infrastructure (DSI), could be integrated with the HBR model to promote seamless data exchange across countries. Finally, the transition to post-quantum algorithms, such as CRYSTALS-Dilithium or Falcon, could be explored to improve the security and integrity of HBR-based systems in the long term.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

Author contribution

The contribution to the paper is as follows: Y. Shevchuk, Y. Tytarchuk: study conception and design; S. Zybin, A. Sorokun: data collection; Y. Tytarchuk, S. Zybin, A. Sorokun, T. Khometa: analysis and interpretation of results; T. Khometa: draft preparation. All authors approved the final version of the manuscript.

References

[1] A. Sayar et al., “Application of hyperledger blockchain technology to logistics supply chain with IoT”, *Procedia Computer Science,* vol. 252, pp. 814-823, 2025. https://doi.org/10.1016/j.procs.2025.01.042

[2] F. Guo, and A. Ye, “The application and performance optimization of multi-controller-based load balancing algorithm in computer networks”, *Egyptian Informatics Journal*, vol. 30, article 10067, 2025. https://doi.org/10.1016/j.eij.2025.100678

[3] L. Kurmangaziyeva, Z. Oralbekova, S. Akhmetzhanova, A. Khassenova, M. Akishev, and T. Zhukabayeva, “Analysis of the problem of ensuring the reliability of the information system”, *CEUR Workshop Proceedings*, vol. 3382, 2022. https://ceur-ws.org/Vol-3382/Paper13.pdf

[4] A. Modares, V. Emroozi, P. Roozkhosh, and A. Modares, “A Bayesian best-worst approach with blockchain integration for optimizing supply chain efficiency through supplier selection”, *Supply Chain Analytics*, vol. 9, article 100100, 2025. https://doi.org/10.1016/j.sca.2024.100100

[5] D. Yanga, and X. Liub, “Collaborative algorithm for user trust and data security based on blockchain and machine learning”, *Procedia Computer Science*, vol. 262, pp. 757-765, 2025. https://doi.org/10.1016/j.procs.2025.05.108

[6] A. Al-Rasheed, H. Ali, R. Khan, and A. Saeed, “Blockchain and smart contracts: An effective approach for the transaction security & privacy in electronic medical records”, *Computer Materials & Continua,* vol. 85, no. 2, pp. 3421-3436, 2025. https://doi.org/10.32604/cmc.2025.065156

[7] X. Wua, and W. Bao, "Research on the design of a blockchain logistics information platform based on reputation proof consensus algorithm", *Procedia Computer Science* vol. 262, pp. 973-981, 2025. https://doi.org/10.1016/j.procs.2025.05.132

[8] B. Wen et al., "Security and privacy protection technologies in securing blockchain applications", *Information Sciences*, vol. *645*, article 119322, 2023. https://doi.org/10.1016/j.ins.2023.119322

[9] "Ukraine's cybersecurity market expands amid war challenges", *Global war news*, 2025, https://globalwarnews.com/ukraines-cybersecurity-market-expands-amid-war-challenges

[10] J. Li, "Research on optimization model of high availability and flexibility of blockchain system based on microservice architecture", *Procedia Computer Science,* vol. 261, pp. 207-216, 2025. https://doi.org/10.1016/j.procs.2025.04.191

[11] V. Akhmetov et al., "Cloud computing analysis of Indian ASAT test on March 27, 2019", In *Proceedings of the IEEE International Scientific and Practical Conference "Problems of Infocommunications. Science and Technology"*, pp. 315-318, 2019. https://doi.org/10.1109/PICST47496.2019.9061243

[12] M. Ahmed et al., "A dependable and secure consensus algorithm for blockchain-assisted microservice architecture", *Comp and Electr Eng*, vol. 109, part B, 2023. https://doi.org/10.1016/j.compeleceng.2023.108762

[13] M. Whaiduzzaman, M. Mahi, A. Barros, I. Khalil, C. Fidge, and R. Buyya, "Performance measurement of a blockchain-based hierarchical tree layered fog-IOT microservice architecture", *IEEE Access*, vol. 9, pp. 106655-106674, 2021. https://doi.org/10.1109/ACCESS.2021.3100072

[14] Y. Xu, "Blockchain ABE algorithm in information system data security and data delay encryption", *Procedia Computer Science,* vol. 243, pp. 801-808, 2024. https://doi.org/10.1016/j.procs.2024.09.096

[15] M. Ghani, K. She, M. A. Rauf et al., "Enhancing security and privacy in distributed face recognition systems through blockchain and GAN technologies", *Computer Materials & Continua*, vol.79, no.2, pp. 2609-2623, 2024, https://doi.org/10.32604/cmc.2024.049611

[16] J. Yu et al., "Design of low altitude flight data security sharing platform based on blockchain technology", *Procedia Computer Science*, vol. 262, pp. 705-713, 2025. https://doi.org/10.1016/j.procs.2025.05.102

[17] C. Guo et al., "Multi-objective optimization for energy blockchain cloud storage: Achieving efficiency and security synergy", *Cyber-Phys Energy Syst,* vol. 1, no. 1, pp. 56-70, 2025. https://doi.org/10.1016/j.cpes.2025.08.002

[18] O. Suprun et al., "Development of a modified steganographic model of data transmission using IPv6 protocol", *CEUR Workshop Proceedings*, vol. 3925, pp. 35-46, 2025. https://ceur-ws.org/Vol-3925/paper04.pdf

[19] N. Smailov, F. Uralova, R. Kadyrova, R. Magazov, and A. Sabibolda, "Optimization of machine learning methods for de-anonymization in social networks", *Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska*, vol. 15, no. 1, pp. 101-104, 2025. https://doi.org/10.35784/iapgos.7098

[20] S. Khlamov et al., "AI-based Decision-Making Process in Pipeline for Astronomical Data Mining", *CEUR Workshop Proceedings*, vol. 4048, pp. 172-186, 2025. https://ceur-ws.org/Vol-4048/paper14.pdf

[21] E. Hadzhyiev et al., "Application of Docker Compose for constructing the infocommunication system for online processing of astronomical images", In *Proceedings of the International Conference on Advanced Computer Information Technologies*, pp. 629-633, 2025. https://doi.org/10.1109/ACIT65614.2025.11185586

[22] S. Zybin et al., "Blockchain technologies and their application in security software development", *Sustainable Engineering and Innovation*, vol. 7, no. 1, pp. 209-224, 2025. https://doi.org/10.37868/sei.v7i1.id499

[23] P. Prathap et al., "Blockchain integrated optimized supply chain security using horse herd algorithm", *Results in Engineering*, vol. 27, article 106950, 2025. https://doi.org/10.1016/j.rineng.2025.106950

[24] P. Kumar et al., "Computer modeling approaches for blockchain-driven supply chain intelligence: A review on enhancing transparency, security, and efficiency", *Computer Modeling in Engineering and Science*, vol. 144, no. 3, pp. 2779-2818, 2025. https://doi.org/10.32604/cmes.2025.066365

[25] G. Perboli, S. Musso, and M. Rosano, "Blockchain in logistics and supply chain: A lean approach for designing real-world use cases", *IEEE Access*, vol. 6, pp. 62018-62028, 2018. https://doi.org/10.1109/ACCESS.2018.2875782

[26] S. Ding, H. Hu, F. Xu, Z. Chai, and W. Wang, "Blockchain-based security-minded information-sharing in precast construction supply chain management with scalability, efficiency, and privacy improvements", *Automation in Construction*, vol. 168, article 105698, 2024. https://doi.org/10.1016/j.autcon.2024.105698

[27] X. Guo, Y. Zuo, and D. Li, "When auditing meets blockchain: A study on applying blockchain smart contracts in auditing", *International Journal of Accounting Information Systems*, vol. 56, article 100730, 2025. https://doi.org/10.1016/j.accinf.2025.100730

[28] A. Youssef et al., "Blockchain technology adoption intention among the Big Four audit firms", *The British Accounting Review*, article 101692. https://doi.org/10.1016/j.bar.2025.101692

[29] V. Lingayat et al., "Securing Pharmaceutical Supply Chain using Blockchain Technology", *ITM Web of Conferences*, vol. 37, article 01013, 2021. https://doi.org/10.1051/itmconf/20213701013

[30] J. Zhao et al., "Research on medical data storage and sharing model based on blockchain", *High-Confidence Computing*, vol. *3,* no. 3, article100133, 2023. https://doi.org/10.1016/j.hcc.2023.100133

[31] M. Sadeghi, and A. Mahmoudi, "Synergy between blockchain technology and internet of medical things in healthcare: A way to sustainable society", *Information Sciences*, vol. 660, article 120049, 2024, https://doi.org/10.1016/j.ins.2023.120049

[32] R. Ramani, A. Mary, S. Raja, and D. Shunmugam, "Optimized data management and secured federated learning in the Internet of Medical Things (IoMT) with blockchain technology", *Biomedical Signal Processing and Control*, vol. 93, article 106213, 2024. https://doi.org/10.1016/j.bspc.2024.106213

[33] O. Popoola, M. Rodrigues, J. Marchang, A. Shenfield, A. Ikpehai, and J. A. Popoola, "A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: Problems, challenges and solutions", *Blockchain: Research and Applications*, vol. 5, no. 2, article 100178, 2024. https://doi.org/10.1016/j.bcra.2023.100178

[34] S. Thakker, S. Rane, and V. Narwane, "Implementation of blockchain IoT-based integrated architecture in green supply chain", *Modern Supply Chain Research and Applications*, vol. 6, no. 2, pp. 122-145, 2024. https://doi.org/10.1108/MSCRA-01-2023-0005

[35] H. Hubal, "Mathematical description of the non-equilibrium state of symmetric particle systems", *International Journal of Applied Mathematics*, vol. 32, no. 5, 2019. https://doi.org/10.12732/ijam.v32i5.4

[36] V. Savanevych et al., "Mathematical methods for an accurate navigation of the robotic telescopes", *Mathematics*, vol. 11, no. 10, Article 2246, 2023. https://doi.org/10.3390/math11102246

[37] V. Simakhin et al., "Multifractal Properties of Traffic Generator Based on Markov Chains", *CEUR Workshop Proceedings*, vol. 2588, pp. 567-579, 2019. https://ceur-ws.org/Vol-2588/paper48.pdf

[38] M. Salehi, and R. Oghaz, "The effect of blockchain on accounting", *Journal of Facilities Management*, vol. 23, no. 4, pp. 640-666, 2024. https://doi.org/10.1108/JFM-08-2023-0091

[39] S. Rybalchenko, O. Lukianykhina, C. Alamanova et al., "Anti-crisis management of banking institutions: current problems and prospects for improvement", *Financial and Credit Activity-Problems of Theory and Practice*, vol. 5, no. 46, pp. 29-39, 2022. https://doi.org/10.55643/fcaptp.5.46.2022.3907

[40] S. Punitha, and K. Preetha, "A novel integration of Web 3.0 with hybrid chaotic-hippo-optimized blockchain framework for healthcare 4.0", *Results in Engineering*, vol. 24, article 103528, 2024. https://doi.org/10.1016/j.rineng.2024.103528

[41] M. Hasan, S. Datta, and S. Namasudra, "Inter-hospital secure healthcare data exchange process by using proxy re-encryption and blockchain technology", *Computers in Biology and Medicine*, vol. 194, article 110462, 2025. https://doi.org/10.1016/j.compbiomed.2025.110462