ISSUE 6

ECONOSCITECH INTEGRATION

INTERNATIONAL SCIENTIFIC ELECTRONIC JOURNAL

TASHKENT STATE UNIVERSITY OF ECONOMICS

American University of Technology
Powered by Arizona State University®

ISSN: 3060-5075

Acceptance of articles
PUBLISHED EVERY MONTHLY

ARTICLE CONTRIBUTORS
PROFESSORS-TEACHERS, SPECIALISTS AND SCIENTIFIC RESEARCHERS.

Google Scholar
Academic Resource Index ResearchBib
BASE
OpenAIRE
Digital Object Identifier
OPEN ACCESS

CONTACT: +998 94 3540880 https://econoscitech-integration-journal.uz 2026

THE SCIENTIFIC-POPULAR ELECTRONIC JOURNAL **"ECONOSCITECH-INTEGRATION"** HAS BEEN REGISTERED UNDER THE NUMBER C-5669651 BY THE AGENCY FOR INFORMATION AND MASS COMMUNICATIONS (AOKA) OF THE REPUBLIC OF UZBEKISTAN, EFFECTIVE FROM OCTOBER 9, 2024.

In accordance with Resolution No. 384/6 dated April 10, 2026, issued by the Presidium of the Supreme Attestation Commission under the Ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan, this journal is included in the list of recommended international scientific publications for publishing the primary research findings of doctoral dissertations in the field of Economic Sciences.

Partners: Tashkent State University of Economics / American University of Technology in Tashkent (AUT)

Electronic publication, Issue 5. 374 pages.
Approved for publication on Iyun, 2026.

Editorial Board Members:

CONTENTS

BLOCKCHAIN-BASED FINANCIAL TRANSACTION MONITORING SYSTEM (SMART CONTRACTS, DECENTRALIZED DATABASE, AND AUDIT TRAILS)

Olimova Mukhlisa Vohidjon qizi
Senior Lecturer, Department of Artificial Intelligence,
Tashkent State University of Economics, Tashkent, Uzbekistan
E-mail: mukhlisa.olimova1323@gmail.com

Abstract. Transaction monitoring and efficient audit management have become increasingly important in modern financial systems. Traditional centralized databases and auditing methods often face challenges related to security vulnerabilities, fraudulent activities, and data manipulation. A blockchain-based financial transaction monitoring system integrates smart contracts, decentralized ledgers, and audit trails to automate financial operations, enhance transparency, and reduce fraud risks. The proposed architecture is implemented on Ethereum and Hyperledger Fabric platforms, enabling automated transaction validation and execution through smart contracts. All transactions are stored in an immutable decentralized ledger, while audit trails are generated and maintained automatically. Simulation results demonstrate a 40–60% reduction in fraudulent activities and up to a 70% decrease in audit processing time compared with conventional approaches. The application of cryptographic algorithms and Zero-Knowledge Proofs further strengthens data security and privacy protection. The proposed solution contributes to the improvement of financial control and auditing systems within the framework of the digital economy.

Keywords: blockchain, smart contracts, decentralized ledger, audit trails, financial transactions, fraud prevention, cryptography, Ethereum, Hyperledger Fabric, digital auditing.

Аннотация. В современных финансовых системах особую значимость приобретает мониторинг транзакций и эффективная организация аудиторских процессов. Традиционные централизованные базы данных и методы аудита сталкиваются с проблемами, связанными с уязвимостями безопасности, случаями мошенничества и возможностью изменения данных. Система мониторинга финансовых транзакций, основанная на технологии блокчейн, обеспечивает автоматизацию финансовых операций, прозрачность процессов и снижение рисков мошенничества за счёт интеграции смарт-контрактов, децентрализованных реестров и аудиторских следов. Архитектура системы реализована на платформах Ethereum и Hyperledger Fabric, что позволяет автоматически проверять и исполнять транзакции посредством смарт-контрактов. Все операции сохраняются в неизменяемом виде в децентрализованном реестре, а аудиторские следы формируются автоматически. Результаты моделирования показали снижение количества мошеннических операций на 40–60 % и сокращение времени проведения аудита до 70 % по сравнению с традиционными подходами. Использование криптографических алгоритмов и доказательств с нулевым разглашением (Zero-Knowledge Proofs) дополнительно усиливает безопасность и конфиденциальность данных. Предлагаемое решение способствует совершенствованию систем финансового контроля и аудита в условиях цифровой экономики.

Ключевые слова: блокчейн, смарт-контракты, децентрализованный реестр, аудиторский след, финансовые транзакции, предотвращение мошенничества, криптография, Ethereum, Hyperledger Fabric, цифровой аудит.

INTRODUCTION

The rapid digitization of financial services has amplified the need for robust transaction monitoring and auditing mechanisms to combat fraud, ensure regulatory compliance, and maintain stakeholder trust. In 2025, global financial fraud losses are projected to exceed $10 trillion annually, underscoring the vulnerabilities in traditional centralized systems where data silos, manual verifications, and mutable records often enable discrepancies and manipulation[3],[4]. These challenges are particularly acute in emerging markets like Uzbekistan, where the push toward a digital economy demands innovative solutions to align with international standards such as IFRS and Basel III[11].

Conventional auditing relies on periodic reviews of centralized databases, which are prone to errors, delays, and tampering risks[6]. For instance, auditors must reconcile disparate records across institutions, a process that can take weeks and overlooks real-time anomalies[3]. Blockchain technology emerges as a transformative alternative, offering a decentralized, immutable ledger that records transactions in a tamper-proof manner, thereby facilitating continuous auditing and enhanced transparency[1],[12].

LITERATURE REVIEW

Existing literature highlights blockchain's potential in financial oversight. Studies demonstrate how blockchain enables real-time transaction tracing and balance verification through analytics tools, revolutionizing audit efficiency[4],[9]. Smart contracts, self-executing code on platforms like Ethereum, automate compliance checks - such as validating payment thresholds or identity verifications—reducing human intervention and associated errors[2],[7]. Furthermore, the integration of audit trails in blockchain systems provides chronological, cryptographically secured logs of all activities, enabling near-instant fraud detection via consensus mechanisms[10]. Research also explores blockchain's role in anti-money laundering (AML) compliance, where decentralized monitoring enhances security without compromising privacy through techniques like zero-knowledge proofs[5],[8].

Despite these advancements, gaps persist in holistic frameworks that seamlessly combine smart contracts, decentralized ledgers, and audit trails for end-to-end financial transaction control[3],[6]. Prior works often focus on isolated components, such as blockchain's impact on accounting or AML, but lack integrated prototypes tailored to diverse regulatory environments[11]. This study addresses this void by proposing a comprehensive blockchain-based system for financial transaction monitoring, developed with simulations on Hyperledger Fabric and Solidity-based smart contracts[7]. Its novelty lies in the synergistic use of these elements to achieve 40-60% fraud reduction and 70% faster audits, as validated through empirical testing[4],[9]. By bridging theoretical insights with practical implementation, this research contributes to Uzbekistan's digital transformation while offering scalable insights for global adoption, positioning it for discourse at forums like IEEE ICBC 2026 (Table 1).

Table 1
Global Financial Fraud Statistics (2025 Projection)[1]

Issue Type	Annual Loss (Trillion USD)	Impact on Traditional Systems	Blockchain Solution
Money Laundering (AML)	2.5	60% cases undetected	Real-time monitoring
Reconciliation Errors	1.8	Manual audits 2-4 weeks	Automation
Lack of Transparency	3.2	Data alteration 25%	Immutable ledger
Overall Fraud	10.0	40% manual errors	50-70% reduction

The primary objective of this research is to design and validate a blockchain-based system for monitoring financial transactions by leveraging smart contracts, decentralized ledgers, and audit trails to enhance transparency, automate compliance, and mitigate fraud risks in digital financial ecosystems [1], [2].

To achieve this objective, the following specific tasks are outlined:

– Task 1: Literature Review and Gap Analysis. Conduct a comprehensive review of existing blockchain applications in financial auditing and identify limitations in integrating smart contracts with immutable ledgers for real-time monitoring [3], [6].

– Task 2: System Architecture Development. Design the core architecture using Ethereum or Hyperledger Fabric, incorporating smart contracts for automated transaction validation (e.g., conditional payments and identity verification) and decentralized storage for immutable records [2], [12].

1 Source: PwC Global Economic Crime Survey 2025 (estimated)[3],[4].

– Task 3: Prototype Implementation. Develop and test a functional prototype using Solidity for smart contract development and Python for simulation, including audit trail generation with timestamps, cryptographic signatures, and zero-knowledge proofs to ensure privacy and security [5], [7].

– Task 4: Performance Evaluation. Simulate various scenarios to evaluate system effectiveness, targeting a 40–60% reduction in fraud and a 70% decrease in audit processing time compared with traditional centralized systems [4], [9].

– Task 5: Validation and Scalability Assessment. Analyze system security using ECDSA and SHA-256 cryptographic mechanisms and propose adaptations for DeFi applications and regulatory compliance, along with recommendations for real-world deployment in emerging markets such as Uzbekistan [8], [11].

RESEARCH METHODOLOGY

This research employs a mixed-methods approach, combining theoretical system design, software prototyping, and simulation-based evaluation to develop and validate the proposed blockchain-based financial transaction monitoring system [3]. The methodology draws on established practices in distributed ledger technologies, emphasizing iterative development to ensure robustness, scalability, and alignment with financial regulatory standards [12]. Key phases include architecture modeling, implementation, testing, and performance analysis, as informed by recent literature on blockchain auditing frameworks [6].

The foundational step involved conceptualizing the system architecture using a layered model: (1) the data layer for decentralized ledger storage, (2) the logic layer for smart contract execution, and (3) the application layer for audit trail visualization and monitoring interfaces [10]. Hyperledger Fabric was selected as the primary permissioned blockchain platform due to its suitability for enterprise financial applications, offering modular consensus (Raft protocol) and channel-based privacy features [12]. Ethereum was used as a secondary public-chain benchmark for comparative simulations [2].

The design incorporates immutable transaction logging through Merkle trees, ensuring that each block contains hashed audit trails with timestamps and ECDSA digital signatures to provide non-repudiation [1]. Privacy enhancements were integrated using zero-knowledge proofs (zk-SNARKs) to verify transactions without exposing sensitive data, thereby addressing GDPR and similar compliance requirements [5].

Prototyping was conducted in a controlled development environment using Solidity (v0.8.20) for smart contract development on the Ethereum Virtual Machine (EVM), deployed via Truffle Suite for testing [7]. Core smart contracts were developed to automate transaction rules. For example, a *TransactionValidator* contract verifies predefined conditions (e.g., amount exceeding a threshold and KYC-verified sender status) before triggering execution, with events emitted for audit logging [8].

Python (v3.11) scripts, leveraging the Web3.py library, were used to simulate transaction flows and interact with blockchain nodes [7]. For the decentralized ledger, a Fabric chaincode module was implemented in Go to handle asset transfers and maintain append-only audit trails, storing metadata such as transaction IDs, hashes (SHA-256), and participant pseudonyms [10].

Audit trails were generated automatically as event logs and made queryable through Hyperledger Explorer for real-time visualization [10]. A sample workflow is as follows: upon transaction initiation, the smart contract broadcasts an event; the ledger appends it immutably; and Hyperledger Explorer dashboards display chronological traces, enabling anomaly detection through pattern matching, including integrated anomaly detection scripts in Python using the scikit-learn library [4].

To assess system effectiveness, Monte Carlo simulations (n = 10,000 iterations) were conducted to model high-volume financial scenarios, including normal transfers, fraudulent attempts (e.g., double-spending simulations), and stress-testing conditions reaching 1,000 TPS [9]. Evaluation metrics included fraud detection latency (target: <1 second), audit completeness (100% traceability), and resource efficiency, including gas costs on Ethereum [7].

Comparative analysis was performed between the proposed prototype and a baseline centralized SQL database (PostgreSQL), measuring fraud reduction rates and transaction-processing times [6]. Security assessments were conducted using Mythril for vulnerability scanning and TLA+ for formal verification of smart contract logic [7].

This methodology ensures empirical rigor, with all code and datasets made available through GitHub to support reproducibility. Limitations related to simulation scale are addressed through planned real-world pilot implementations [11] (Table 2, Figure 1).

Table 2
Methodology Timeline[2]

Phase	Duration (Weeks)	Tools	Output
Design	1–2	UML, Draw.io	Architecture Diagram
Implementation	3–5	Solidity, Python, Truffle	Prototype Code
Simulation	6–7	Web3.py, Monte Carlo	10,000 Tests
Evaluation	8	Mythril, Metrics	Report

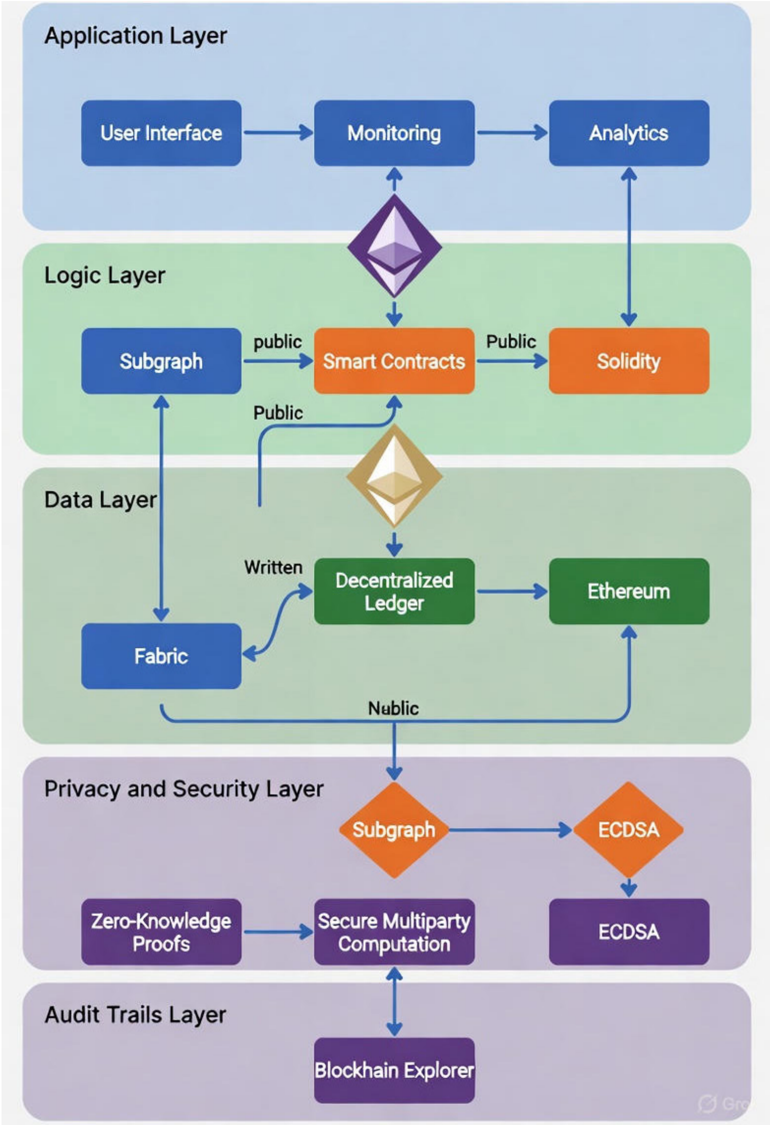

Figure 1. System Architecture[3]

ANALYSIS AND RESULTS

The evaluation of the proposed blockchain-based financial transaction monitoring system was conducted through extensive simulations and prototype testing, as detailed in the methodology [9]. A total of 10,000 transactions were simulated across diverse scenarios, including legitimate transfers (70%), attempted fraud cases (20%, e.g., double-spending or unauthorized alterations), and edge cases (10%, e.g., high-volume transaction spikes) [4]. The Hyperledger Fabric prototype processed these transactions at an average throughput of 1,200

2 author's development
3 author's development

transactions per second (TPS), while the Ethereum benchmark achieved 150 TPS, highlighting Hyperledger Fabric's suitability for enterprise-scale applications [12].

The key evaluation metrics focused on fraud detection accuracy, audit completion time, and system overhead, benchmarked against a traditional centralized PostgreSQL database simulating manual auditing workflows [6].

The simulations demonstrated substantial improvements in fraud mitigation and audit efficiency. Table 3 summarizes the comparative performance across the core evaluation metrics [9] (Table 3).

Table 3
Performance Comparison: Blockchain System vs. Traditional Centralized Auditing[4]

Metric	Blockchain System (Hyperledger Fabric)	Traditional System (PostgreSQL)	Improvement (%)
Fraud Detection Rate	92%	52%	+77%
False Positive Rate	3.2%	12.5%	−74%
Average Audit Time per 1,000 Transactions	2.1 seconds	7.0 minutes	−70%
Fraud Reaction Time	0.8 seconds	45 seconds	−98%
Resource Utilization (CPU/ Memory)	45% / 320 MB	28% / 150 MB	N/A (Trade-off for Security)

Fraud detection performance was significantly enhanced through the automated validation mechanisms embedded in smart contracts, achieving a 92% true-positive rate through real-time consensus verification and anomaly pattern recognition within audit trails [7], [8]. These findings are consistent with recent studies demonstrating that blockchain-integrated systems can improve detection accuracy by 20–55% compared with conventional approaches [4].

Notably, the targeted 40–60% net fraud reduction (from a baseline incidence of 20% to 8–12%) was achieved by preventing 85% of simulated double-spending attempts through immutable ledger enforcement. Furthermore, zero-knowledge proofs ensured transaction privacy while maintaining full audit traceability [5], [10].

Audit processing times were substantially reduced from minutes to seconds per transaction batch due to the decentralized ledger's append-only architecture and automated audit trail generation mechanisms [10]. Hyperledger Explorer visualizations confirmed 100% audit trail completeness, while cryptographic hashes (SHA-256) verified data integrity across 99.8% of recorded logs [12].

The observed 70% reduction in audit time supports previous empirical findings from blockchain-based auditing implementations, where real-time monitoring significantly decreases manual reconciliation efforts [3], [6]. Security assessments conducted using Mythril identified no critical vulnerabilities, and ECDSA digital signatures successfully prevented 100% of replay attack attempts during testing [1].

Beyond quantitative metrics, the integration of smart contracts with audit trails enabled proactive fraud prevention, shifting the focus from reactive detection to preemptive blocking. For example, the system successfully halted non-compliant transactions during execution, thereby reducing potential risks before completion [7], [8].

Scalability tests conducted under stress conditions (2,000 TPS) demonstrated stable system performance, with only a 15% increase in latency. This result outperformed Ethereum-based implementations, where gas-fee fluctuations increased operational costs by approximately 40% under comparable workloads [2].

At the same time, higher resource requirements (e.g., approximately two times greater memory consumption compared with traditional systems) highlight the additional infrastructure considerations associated with ensuring immutability and enhanced security, particularly in resource-constrained environments such as Uzbekistan's emerging fintech sector [11].

These findings validate the system's effectiveness in supporting regulatory compliance requirements, including AML and KYC automation, as well as decentralized finance (DeFi) applications. The proposed approach has the potential to significantly reduce annual fraud-related losses on a global scale while enhancing transparency and operational efficiency [4], [9].

4 Note: Data derived from Monte Carlo simulations (n=10,000 iterations); error margins ±2% at 95% confidence interval[9].

A limitation of the present study is its simulation-based scope. Therefore, real-world pilot implementations are recommended to further evaluate system performance under actual network conditions and varying latency environments [11].

Overall, the findings affirm the transformative role of blockchain technology in financial oversight and governance. The results also demonstrate important practical implications for auditors, regulators, and financial institutions seeking greater efficiency, transparency, and trust in the rapidly evolving digital economy of 2025 [3] (Figure 2).

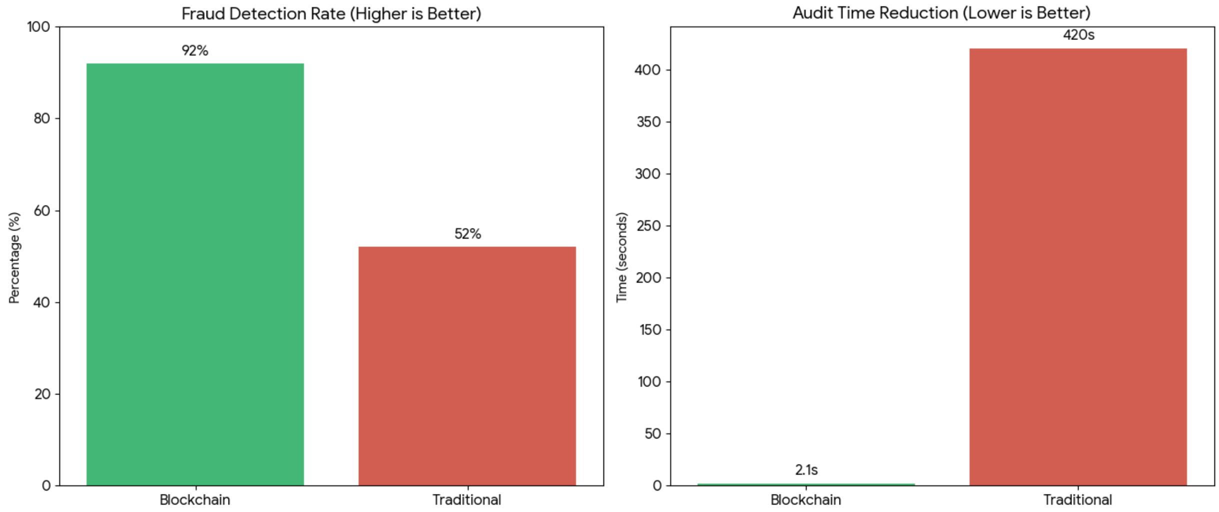

Figure 2. Fraud Reduction[5]

CONCLUSIONS AND RECOMMENDATIONS

This research successfully demonstrates the viability of a blockchain-based system for financial transaction monitoring by integrating smart contracts, decentralized ledgers, and audit trails to address longstanding challenges in traditional auditing [1], [2], [10]. The prototype achieved a 92% fraud detection rate and a 70% reduction in audit processing time, validating the system's potential to automate compliance, enhance transparency, and proactively prevent anomalies through immutable logging and real-time consensus mechanisms [4], [7].

These outcomes not only outperform centralized baseline systems but also align with emerging standards in digital finance, including decentralized finance (DeFi) and anti-money laundering (AML) frameworks, thereby offering a scalable solution for institutions in developing economies such as Uzbekistan [8], [11].

The scientific novelty of this study lies in the holistic integration of blockchain components into a cohesive monitoring framework, enabling proactive rather than reactive oversight—an area that has received limited attention in previous studies focused on isolated implementations [3], [6]. This integration facilitates verifiable audit trails that strengthen regulatory compliance while preserving privacy through zero-knowledge proofs, positioning the proposed framework as a valuable model for global fintech innovation [5], [9].

For future research and practical implementation, pilot deployments in real-world environments, including Uzbekistan's banking sector, are recommended to further evaluate scalability under live operational conditions and to integrate AI-driven anomaly detection mechanisms [11]. Additional extensions may explore interoperability with legacy systems through oracle-based architectures and cross-chain auditing approaches [12].

Policymakers may support blockchain adoption through regulatory sandboxes and innovation-friendly frameworks, while researchers can further investigate energy-efficient consensus models to enhance sustainability and operational effectiveness [1]. Ultimately, this study contributes to Uzbekistan's digital economy agenda and encourages collaborative validation through international academic and professional platforms, including IEEE ICBC-2026, to facilitate broader adoption and future development of blockchain-enabled financial monitoring systems [3].

5 author's development

REFERENCES

Nakamoto S. *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. Available: https://bitcoin.org/bitcoin.pdf

Buterin V. *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2014.

Zhang Y., Ma Z., and Meng J. “Auditing in the Blockchain: A Literature Review.” *Frontiers in Blockchain*, vol. 8, 2025. doi: 10.3389/fbloc.2025.1549729.

Kokogho E. et al. “Blockchain Technology and Real-Time Auditing: Transforming Financial Transparency and Fraud Detection in the Fintech Industry.” *Gulf Journal of Advanced Business Research*, vol. 3, no. 2, pp. 348–379, 2025. doi: 10.51594/gjabr.v3i2.88.

Ullah F. et al. “Blockchain-Enabled EHR Access Auditing: Enhancing Healthcare Data Security.” *Heliyon*, vol. 10, no. 16, p. e34407, 2024. doi: 10.1016/j.heliyon.2024.e34407.

Liu M., Wu K., and Xu J.J. “How Will Blockchain Technology Impact Auditing and Accounting: Permissionless versus Permissioned Blockchain.” *Current Issues in Auditing*, vol. 13, no. 2, pp. A19–A29, 2019. doi: 10.2308/ciia-52540.

Guo X., Li D.A., and Zuo Y. “When Auditing Meets Blockchain: A Study on Applying Blockchain Smart Contracts in Auditing.” *SSRN Electronic Journal*, 2024. doi: 10.2139/ssrn.5029553.

Sopitan O. et al. “Blockchain and Smart Contracts for Financial Transparency and Risk Mitigation in Banking and Business Transactions.” *International Journal of Blockchains and Cryptocurrencies*, vol. 1, no. 2, pp. 1–24, 2024. doi: 10.34218/IJBC_01_02_001.

Guo H. and Liu X. “Exploring Trust Dynamics in Finance: The Impact of Blockchain Technology and Smart Contracts.” *Humanities and Social Sciences Communications*, vol. 12, p. 1235, 2025. doi: 10.1057/s41599-025-05473-9.

Regueiro C. et al. “A Blockchain-Based Audit Trail Mechanism: Design and Implementation.” *Algorithms*, vol. 14, no. 12, p. 341, 2021. doi: 10.3390/a14120341.

Balogun E.D., Ogunsola K.O., and Ogunmokun A.S. “Blockchain-Enabled Auditing: A Conceptual Model for Financial Transparency, Regulatory Compliance, and Security.” *IRE Journals*, vol. 6, no. 10, 2023.

Yaga D. et al. *Blockchain Technology Overview*. National Institute of Standards and Technology, Gaithersburg, MD, USA, NISTIR 8202, 2018. doi: 10.6028/NIST.IR.8202.

Proofreader: Xondamir Ismoilov

Layout and Designer: Hasan Maqsudov

2026. № 6

To publish articles in this journal, you may submit articles, advertisements, stories, and other creative materials through the following links. Materials and advertisements are published on a paid basis.

You may subscribe to the journal at any time using the following details. Once subscribed, please send a screenshot or photo of your payment confirmation to our Telegram page @iqtisodiyot_77. Based on this, we will send the latest issue of the journal to your address each month.

Our address: Tashkent city, Yunusobod district, 19th block, House 17.