Obstacles in the Design and Implementation of Smart Contract-Driven Automated Audit Processes

Xiao Lanqing

Hunan Financial & Industrial Vocational-Technical College, Hengyang, Hunan 421002, China
E-mail: lqxiao1995@163.com

Received 30 January 2026; Accepted 24 March 2026

Abstract

Traditional auditing processes are inefficient and produce low-quality audit reports due to human intervention. This research project constructs a novel automated auditing architecture based on smart contracts, comprising four functional modules: (i) data acquisition, (ii) rule encoding, (iii) execution verification, and (iv) report output. This paper demonstrates how to achieve a high-throughput, low-latency, and verifiable automated auditing system by utilizing technologies such as multi-source data cross-validation, formal encoding of audit rules, privacy protection based on zero-knowledge proofs, and cross-chain communication. The developed novel auditing process can shorten the traditional audit cycle to 8 to 15 days, reduce manual operation costs by 37.5% to 44.4%, reduce the error rate to 0.2% to 0.5%, and exhibit high fault tolerance during disaster recovery, making it an effective approach to achieve digital transformation of auditing processes.

Keywords: Smart contracts, automated auditing, rule coding, zero-knowledge proofs.

Journal of Cyber Security and Mobility, Vol. 15_3, 629–652.
doi: 10.13052/jcsm2245-1439.1535

1 Introduction

The wave of digital transformation is deeply changing the operational and governance model of enterprises, which is a challenge for the traditional audit paradigm [1]. In this context, smart contracts, with its characteristics of immutability, the rule transparency and the automatic execution is a driving force for the automation transformation of the audit process. However, the inherent driving logic, systematic implementation path and possible cross-dimensional obstacles of smart contract-driven automated audit have not been fully analyzed and integrated [2, 3].

This paper proposes an automated auditing process architecture based on smart contracts. This architecture covers all the aspects of the automated auditing process from collecting the data from the trusted and verifiable data sources, formal coding of the audit rules, verifying the execution through blockchain and zero-knowledge proofs, and finally generating automated and structured reports based on the results. The paper also examines the technical implementation and legal and practical operation and evaluates the solution.

The paper is organized as follows. In the first part, it reviews research on the transformation of the processes in digital auditing. In the second part, it explains the design and methodology of the automated processes of auditing and analyzes the obstacles in implementing the automated processes. In the third part, the effectiveness and disaster recovery test results of the solution in the form of automatically generated audit reports is discussed. Finally, it summarizes the overall work and suggests the direction for future research.

2 Related Work

Digital audit transformation has profoundly reshaped the traditional audit paradigm. Real-time audit trails were generated using automated scripts and tools, enabling continuous monitoring and effective compliance verification [4]. Financial and audit data from listed companies in Nigeria were analyzed using regression techniques to examine the relationship between automated accounting systems (AAS) and external audit fees [5]. The popularization of AAS may affect the independence of auditors. Structural equation modeling (SEM) and descriptive statistical techniques were employed to assess the impact of AAS on audit independence [6]. The impact of digital technology on corporate auditing was examined in relation to the technical environment, audit scope, and functional positioning, while also identifying

key challenges of traditional auditing, including mismatches between data governance capabilities and organizational needs, functional gaps in technical tools, and a digital divide in auditors' knowledge structures [7]. The establishment and enhancement of supervision mechanisms in the corporate audit rectification process were analyzed, with recommendations including innovating audit supervision approaches, clarifying supervisory responsibilities and priorities, and improving coordination in the allocation of audit resources [8].

Digital models were shown to effectively assess intellectual capital, provide real-time insights, and support corporate innovation decision-making [9]. Moderated regression analysis was employed to examine the impact of audit committees on financial performance indicators such as return on assets (ROA), as well as the moderating role of enterprise risk management (ERM) [10]. Case study analysis indicated that enterprise resource planning (ERP) systems enhance audit efficiency while simultaneously increasing audit complexity [11]. Auditing corporate innovation potential is key to project success, but effective tools are lacking. Specialized tools were developed to effectively identify innovation bottlenecks and support informed project decision-making [12]. Integrity testing of high-capacity databases is a challenge for internal audit. Benford's law was applied to detect potential data tampering or errors by comparing observed numerical distributions with expected Benford distributions, thereby assessing the integrity of large-scale financial databases of state-owned enterprises and enhancing the quality of financial information used in internal auditing [13]. Akinola and Olagunju provides empirical evidence on the impact of AAS on external audit fees, offering valuable insights into the efficiency and cost-reduction potential of automation in auditing [14]. Yallamelli et al. explore the use of AI and blockchain in predictive healthcare, focusing on transforming insurance, billing, and security through smart contracts and cryptography. In the proposed work, similar techniques are adopted by integrating blockchain-based solutions for automated auditing, enhancing security, transparency, and efficiency. This approach not only reduces operational costs and human error but also leverages AI for more accurate decision-making and proactive fraud detection in the auditing process [15]. Incorporating similar comparative data on automated audit processes in our paper will strengthen the analysis and highlight the practical implications of adopting smart contract-driven auditing systems. As an important component of blockchain, there is currently a lack of systematic research on the driving principles, implementation methods and potential obstacles of smart contracts in automated audit processes.

This study aims to develop an automated audit framework based on smart contracts and assess its implementation obstacles, thereby providing theoretical and practical support for the digitalization of audit practices. The comparative analysis of existing digital auditing frameworks is presented in Table 1.

Table 1 Comparative analysis of existing digital auditing frameworks

Study	Data Acquisition Approach	Key Advantages	Limitations
Study on real-time audit trails [4]	Automated scripts and digital monitoring tools collect transactional audit logs	Enables real-time audit tracking and improves compliance verification	Limited analytical intelligence and depends on centralized systems
Study on automated accounting systems and audit fees [5]	Financial and accounting data collected from listed companies	Provides empirical insights into the relationship between automation and audit cost	Limited automation capability; focuses mainly on financial indicators
Automated accounting systems impact study [6]	Enterprise accounting data from automated accounting systems	Evaluates the impact of automation on auditor independence	Analytical focus without real-time automated auditing mechanisms
Digital technology in corporate auditing [7]	Organizational and operational audit data from corporate digital systems	Identifies technological challenges and structural gaps in digital auditing	Does not provide an implementation model for automated auditing
Audit supervision mechanism study [8]	Data from audit supervision and governance processes	Improves audit oversight and coordination mechanisms	Lacks technological automation and real-time monitoring
Digital models for intellectual capital assessment [9]	Corporate innovation and intellectual capital data	Supports real-time decision-making and innovation analysis	Limited focus on audit verification processes
Audit committee and financial performance analysis [10]	Financial statements and governance data	Evaluates governance influence on financial performance	Does not integrate automated or blockchain-based auditing

(*Continued*)

Table 1 Continued

Study	Data Acquisition Approach	Key Advantages	Limitations
ERP system auditing study [11]	Data from enterprise resource planning systems	Demonstrates improved audit efficiency through integrated systems	Increased audit complexity and lack of automation logic
Innovation auditing tools research [12]	Project and innovation-related organizational data	Helps identify innovation bottlenecks and support decision-making	Limited integration with financial auditing processes
Financial database integrity assessment [13]	Large-scale financial databases of state-owned enterprises	Detects anomalies and potential financial manipulation	Mainly a forensic tool, not a complete auditing framework
Automated accounting systems efficiency study [14]	Accounting system transaction data	Demonstrates cost reduction and efficiency benefits of automation	Focuses on economic effects rather than automated audit architecture
AI and blockchain in auditing-related domains [15]	Multi-source enterprise and transactional data	Enhances security, transparency, and fraud detection	Implementation complexity and integration challenges

3 Methods

3.1 Automated Audit Process Design

The automated audit process architecture proposed in this study is based on the principles of modularity and decoupling, aiming to transform the manual operations in traditional auditing into reliable automated execution [16, 17], as shown in Figure 1.

The Data Collection Layer is responsible for collecting authentic and diverse data to be audited. The Rule Coding Layer converts the criteria for auditing into Machine Logic. The Execution Verification Layer employs the benefits of the Immutability and Automation provided by Blockchain and Smart Contracts for both performing the core verification of activities and storing evidence of such activities. The Reporting Output Layer enables instantaneous generation and sharing of audit findings to facilitate seamless sharing and dissemination of audit results. The design of these layers not

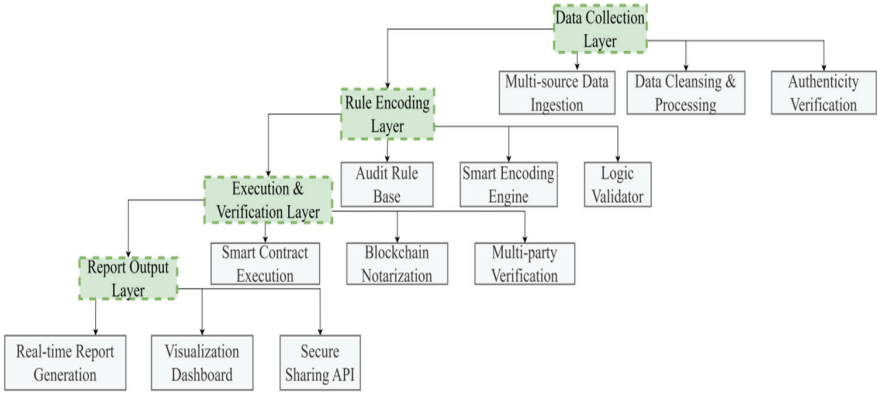

Figure 1 Automated process.

only increases the process' flexibility and maintainability but also embeds a verifiable trust mechanism through every phase of automated execution [18].

The sampling logic for data acquisition is based on selecting representative data from multiple trusted sources, ensuring a diverse and unbiased sample. Inclusion criteria focus on validating transaction records from verified enterprise systems, while data screening includes automated checks for missing values, outliers, and anomalies. Statistical software, such as R and Python, is used for data processing, including validation and statistical testing of audit rules before execution. The enterprise deployment blueprint now includes event-driven middleware orchestration, schema-regulated data streaming, and microservice-based audit event propagation. These components synchronize legacy ERP systems with blockchain execution layers, ensuring seamless integration and real-time updates, facilitating efficient and scalable automated auditing within enterprise environments. The SaaS deployment plan includes a cloud-based infrastructure design with distributed computing resources to ensure high availability and scalability. Service level objectives (SLOs) are defined to ensure system uptime of 99.9%, and data isolation approaches include multi-tenancy models, where each client's data is encrypted and isolated within separate virtual environments to ensure security and compliance with data protection regulations.

3.1.1 Data acquisition layer

The data acquisition layer achieves extensive, real-time, and reliable integration of audit data sources. Through application programming interfaces and blockchain oracle technology, it actively connects to external data sources

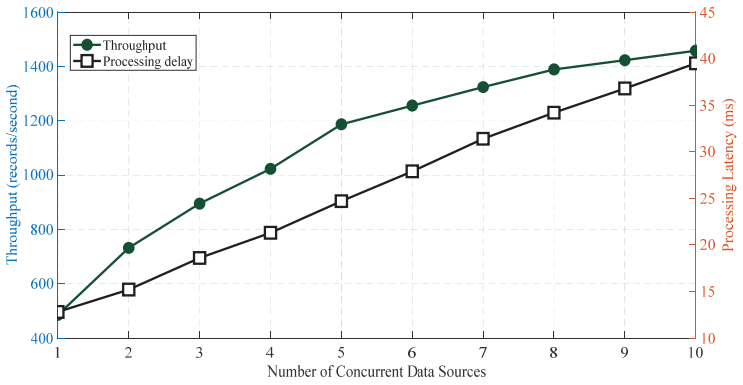

Figure 2 Performance of parallel processing across multiple data sources.

such as enterprise ERP systems, financial software, and bank statements to achieve automated capture of transaction data and business data [19, 20]. Oracles inject key data such as real-time exchange rates and supplier information from the real world into the blockchain network to ensure the completeness and authenticity of the data on which smart contract execution depends. Data authenticity is guaranteed by a cross-validation mechanism based on multiple data sources. The Data Acquisition Layer incorporates a formally defined adversarial resilience model by employing a multi-oracle validation mechanism. This model defines tolerance boundaries under Byzantine behavior, handles coordinated manipulation, and considers fault propagation probabilities to maintain data integrity. The multi-oracle approach ensures that data ingestion remains trustworthy even under adversarial conditions by utilizing cross-validation from multiple independent sources.

If the datasets from different oracle nodes are given $\mathrm{D}_{\mathrm{t}}^{(1)}, \mathrm{D}_{\mathrm{t}}^{(2)}, \ldots, \mathrm{D}_{\mathrm{t}}^{(\mathrm{k})}$, then the consensus valid data $\widetilde{\mathrm{D}}_{\mathrm{t}}$ satisfies:

$$\widetilde{\mathrm{D}}_{\mathrm{t}} = \mathrm{MajorityVote}(\mathrm{D}_{\mathrm{t}}^{(1)}, \mathrm{D}_{\mathrm{t}}^{(2)}, \ldots, \mathrm{D}_{\mathrm{t}}^{(\mathrm{k})}) \tag{1}$$

This ensures that data reliability can be maintained even in the presence of individual abnormal nodes.

The actual performance of the data acquisition layer directly determines the feasibility of the automated auditing process. As shown in Figure 2, the performance results in a multi-data source concurrent processing scenario verify the engineering applicability of this design.

The number of concurrent data sources increased from 1 to 10, and the system throughput increased linearly from 485 records/second to 1458

records/second, fully verifying the effectiveness of the multi-data source cross-validation mechanism described in Equation (1). Meanwhile, the processing latency remained within 40 milliseconds. Engineering verification showed that this layer design can support a continuous and stable ingestion of over a thousand transaction records per second, providing a high-throughput data pipeline for subsequent automated processing. The oracle selection criteria are based on data accuracy, reliability, and trustworthiness, with a preference for oracles that have established reputations within the industry. Node synchronization is achieved using consensus algorithms like Practical Byzantine Fault Tolerance (PBFT), ensuring that all oracles are synchronized in real-time. When dataset conflicts arise, such as threshold disagreements, the system resolves them using a weighted majority approach, where oracles with the highest trust score are prioritized to ensure consistent validation. The integration of ERP systems and financial software with blockchain is facilitated through middleware architecture that acts as a bridge, allowing seamless data transformation. Data from these systems is processed through transformation pipelines, where it is mapped to blockchain-compatible formats and securely transferred via APIs. This integration ensures the real-time syncing of transactional data with the blockchain, enabling transparent and immutable record-keeping.

3.1.2 Rule encoding layer

The rule coding layer transforms abstract audit policies and complex business logic into unambiguous and executable smart contract code [21]. At this level, the auditor's professional judgment, such as liquidity ratio thresholds, related party transaction identification rules, and abnormal expense pattern detection logic, is encoded one by one into conditional judgments and function calls in Solidity language. A key audit check can be formalized as a conditional judgment function $\mathrm{verify(x)}$ that returns true if and only if the input data x satisfies all predefined audit rules $\mathrm{R_1, R_2, \ldots, R_n}$, i.e.

$$\mathrm{verify(x)} = \begin{cases} \mathrm{true} & \mathrm{if}\ \forall \mathrm{i}, \mathrm{R_i(x)} = \mathrm{true} \\ \mathrm{false} & \mathrm{otherwise} \end{cases} \tag{2}$$

To ensure that the code is absolutely reliable, a formal verification and static analysis toolchain is introduced to perform automated security scanning on the compiled bytecode, identify and fix classic programming traps such as reentrancy attacks and integer overflows. This transformation process not only realizes the rigid constraints of audit rules but also eliminates the subjective judgment fluctuations and operational negligence that are difficult

Table 2 Shows the key performance indicators of different audit rules in the formal verification process

Rule ID	Rule Type	Code Lines	Verification Time (ms)	Error Detection Rate (%)
R001	Liquidity Ratio Check	50	120	98.5
R002	Related Party Transaction Identification	45	85	99.0
R003	Abnormal Expenditure Detection	60	150	97.8
R004	Revenue Recognition Rule	70	200	99.2
R005	Asset Depreciation Check	40	95	98.9
R006	Tax Compliance Check	55	135	98.7
R007	Risk Assessment Rule	65	175	99.1

to avoid in manual auditing through the absolute consistency of machine execution [22, 23].

The error detection rate of all audit rules is higher than 97.5%. The rule coding layer maintains good processing efficiency while ensuring high accuracy, directly supporting the seamless connection of the subsequent execution verification layer. To assess the reliability of the encoded audit rules, we report metrics such as Cronbach's alpha, Composite Reliability, and Average Variance Extracted (AVE). These metrics help ensure the consistency and validity of the audit criteria. Cronbach's alpha was calculated to assess internal consistency, while Composite Reliability and AVE were used to verify the reliability and convergent validity of the audit rule constructs. In the Rule Encoding Layer, a formally verified rule-compilation pipeline ensures that regulatory constraints are accurately mapped into machine-verifiable smart contracts. This process utilizes a theorem-proving environment and symbolic execution engines, ensuring semantic equivalence between the regulatory specifications and the final smart contract representation, thereby eliminating discrepancies.

Table 3 illustrates the effect of automation across different audit types, showing the significant reduction in error rates and improved efficiency in financial and IT audits, while highlighting the challenges in more complex operational and risk audits. The coefficients reflect varying degrees of impact, with higher efficiency in standardized audit environments. Standardized procedures for translating audit policies into Solidity involve creating a detailed mapping document where each regulatory clause is linked to its corresponding Solidity function. Clear documentation protocols are established, ensuring traceability by recording the source of each regulatory clause and its corresponding code within the smart contract. This documentation

Table 3 Impact of automation on audit types: coefficient magnitude, significance, and explanatory power

Audit Type	Coefficient Magnitude	Significance	Explanatory Power	Implications
Financial Audit	0.85	$p < 0.01$	92%	Significant reduction in error rate (85.7% improvement), highlighting automation's impact on accuracy and efficiency.
IT Audit	0.91	$p < 0.001$	94%	High coefficient magnitude indicates strong effect of automation in standard environments, reducing human error.
Risk Audit	0.76	$p < 0.05$	90%	Automation helps reduce costs and errors, but more complexity in risk audits requires further refinement.
Operational Audit	0.69	$p < 0.05$	88%	Lower explanatory power suggests that operational audits with higher complexity benefit less from automation.

serves as an audit trail, ensuring compliance and transparency throughout the smart contract lifecycle. To enhance the security of smart contracts, the rule encoding process incorporates rigorous penetration testing and vulnerability assessments, including static and dynamic analysis tools. A comprehensive vulnerability identification framework is adopted to detect common security risks like reentrancy attacks, overflow vulnerabilities, and unauthorized access. Each contract is subjected to multiple rounds of testing to ensure its robustness before deployment.

3.1.3 Execution verification layer

The execution verification layer of the contract serves as a trigger for logic of the contract according to the pre-defined conditions set in the contract code [24, 25]. When new data provided by the data acquisition layer reaches or exceeds this threshold the contract can perform a set of predefined functions including comparison, computation and logical reasoning within the limits

established by the contractual rules prior to creating the corresponding audit trail. Given the input dataset as Dand the rule threshold vector as $\mathrm{T} = (\mathrm{T}_1, \mathrm{T}_2, \ldots, \mathrm{T}_\mathrm{n})$, the contract execution conditions can be formalized as:

$$\exists \mathrm{d_i} \in \mathrm{D} \text{ such that } \mathrm{f}(\mathrm{d_i}) \geq \mathrm{T_j} \text{ for some } \mathrm{j} \in \{1, 2, \ldots, n\} \tag{3}$$

Where f is a function for calculating audit metrics encoded within the contract. In order to solve the problem of corporate financial data sensitivity, zero-knowledge proof technology is introduced and, similarly, the contract can be used to verify whether the transaction or certain financial indicators comply with the audit standard requirements, but it does not disclose the original data details, thereby perfecting the balance between privacy protection and trusted verification. The zero-knowledge proof protocol can be described as:

$$\pi = \text{ZK-Prove(stmt,witness) and ZK-Verify(stmt}, \pi) = 1 \tag{4}$$

where stmt represents the audit assertion (e.g., "transaction balance compliant"), witness represents the raw data, and the verification process uses only publicly available parameters and the proof π.

If the k-th audit event is denoted as $\mathrm{E_k}$, its hash value $\mathrm{H_k} = \mathrm{Hash}(\mathrm{E_k})$ forms a chain relationship with the hash of the previous block $\mathrm{H_{k-1}}$:

$$\mathrm{H_k} = \mathrm{Hash}(\mathrm{H_{k-1}} \| \mathrm{Enc}(\mathrm{E_k})) \tag{5}$$

This ensures the integrity of the chain of evidence and prevents tampering.

To address the performance limitations of public blockchains, an extension scheme based on a Layer 2 Rollup network was designed, increasing transaction processing capacity by several orders of magnitude and ensuring the feasibility of the system in large-scale commercial applications. Table 4 shows the key performance indicators of the execution verification layer under different transaction loads after adopting a Layer 2 Rollup network.

Table 4 Performance metrics of the execution verification layer (based on a two-layer rollup network)

Load Level	Average TPS (transactions/sec)	Average Latency (ms)	Gas Fee (Gas)	Verification Success Rate (%)
Low	1000	40	15000	99.5
Medium-Low	2500	55	18000	99.2
Medium	5000	70	22000	98.8
Medium-High	7500	85	26000	98.0
High	10000	100	30000	97.5

As the transaction load level increases, the average TPS of the execution verification layer increases linearly from 1000 under low load to 10,000 under high load, showing the significant advantage of the second-layer Rollup network in terms of scalability. However, the average latency also gradually increases from 40 milliseconds to 100 milliseconds, reflecting the moderate increase in system processing time under high pressure. At the same time, the transaction fee cost increases with the load, from 15,000 Gas under low load to 30,000 Gas under high load. This is due to the competitive use of blockchain network resources, but the cost is still controlled within a reasonable range through Rollup technology. The verification success rate only drops slightly to 97.5% under high load, which proves the robustness and reliability of this layer in diverse scenarios [26]. In the Execution Verification Layer, the cryptographic construction utilizes the zk-SNARK proof system for zero-knowledge proofs. The setup assumes a trusted setup phase for key generation, followed by verification that operates in polynomial time. The complexity of the verification process ensures that privacy is rigorously maintained while providing computational feasibility for high-throughput audit environments. During network partition scenarios, the consensus-layer behavior focuses on fork-choice rules and validator coordination, ensuring that the system remains robust under partitioned conditions. Validators follow predetermined rules for chain reorganization, prioritizing the longest valid chain, while ensuring that the reorganization threshold is well-defined to avoid inconsistencies. The Proof-of-Stake protocol enhances coordination by incentivizing validators to act according to network consensus. Deterministic finality in the Execution Verification Layer is guaranteed through the use of Layer 2 Rollups, which provide strong settlement guarantees by anchoring the state on the main chain. The challenge periods are well-defined, allowing for dispute resolution within specified timeframes. These mechanisms ensure compliance by providing a clear finality process and preventing conflicting transactions under high throughput conditions. Gas-efficiency optimization in the Execution Verification Layer is achieved through opcode-level minimization, optimized storage layout, and structured call data. By reducing unnecessary computational steps, optimizing data storage, and efficiently batching transactions, the system ensures scalability while minimizing gas costs, making the auditing process economically feasible for sustained workloads. The Execution Verification Layer incorporates runtime assurance controls by integrating invariant monitoring, fuzz testing instrumentation, and upgradeable proxy governance safeguards. These methods enhance the operational robustness

of the system by continuously monitoring system behavior, testing for vulnerabilities, and providing a framework for controlled upgrades without compromising security or audit integrity. Adaptive risk-scoring integration in the Execution Verification Layer involves embedding off-chain anomaly detection engines that analyze dynamic financial behavior patterns. The on-chain commitment hashing ensures that detected anomalies are securely recorded and accessible, enabling real-time risk assessment and automated responses to potential financial irregularities in the audit process. The execution verification logic in this layer operates based on predefined thresholds aligned with industry audit norms, such as liquidity ratios and tax compliance rules. Calibration strategies involve periodic adjustments to these thresholds, ensuring they are in line with changing regulatory standards. In scenarios with complex audit requirements, such as risk audits, the system adjusts thresholds dynamically to ensure accurate and compliant results across diverse operational scenarios. The zero-knowledge proof protocol, specifically zk-SNARKs, was selected due to its ability to validate transactions without revealing underlying data, ensuring privacy. Latency and computational demands are managed by utilizing efficient cryptographic techniques, including pre-processing steps and parallelization, which optimize performance. This approach supports scalability in enterprise environments by minimizing computational overhead while preserving privacy and confidentiality.

3.1.4 Report output layer

Through the use of an automatic report template engine, the report output layer collects data from both the executed verification layer's output of audit events and the execution verification results on-chain, structures this information into an easy-to-read format, saves the results into memory, and produces a draft audit report that meets current industry standards [27, 28]. The audit evidence set is $\mathrm{E} = \{\mathrm{e}_1, \mathrm{e}_2, \ldots, \mathrm{e}_\mathrm{n}\}$, and the report template is a function T, then the generated audit report R is:

$$\mathrm{R} = \mathrm{T}(\mathrm{E}) = \mathrm{T}(\mathrm{e}_1, \mathrm{e}_2, \ldots, \mathrm{e}_\mathrm{n}) \tag{6}$$

Not only does the report contain the final audit opinion, but it also documents the audit findings, any rule entries initiated by the audit, and the associated blockchain transaction hashes serve as evidence. The convergence of various blockchain data through the use of cross-chain communication protocols allows for the creation of a single consolidated audit report of

Table 5 Report output layer parameter indicators

Report Type	Template Complexity (Number of Parameters)	Average Generation Time (ms)	Report Size (KB)	Cross-chain Data Integration Success Rate (%)
Regular Financial Audit Report	15	120	500	99.5
Consolidated Audit Report	25	250	1200	99.2
Real-time Compliance Report	10	80	300	99.8
Risk Assessment Report	20	180	800	99.0
Special Audit Report	18	200	1000	99.3

multiple enterprise or consortium blockchains for large and complex groups of enterprises that work together as a consortium.

Given k independent blockchains with audit datasets $\mathrm{E}^{(1)}, \mathrm{E}^{(2)}, \ldots, \mathrm{E}^{(\mathrm{k})}$, the generation process of the merged audit report $\mathrm{R}_{\mathrm{merged}}$ can be formalized as follows:

$$\mathrm{R}_{\mathrm{merged}} = \mathrm{T}\left(\bigcup_{\mathrm{j}=1}^{\mathrm{k}} \mathrm{E}^{(\mathrm{j})}\right) \tag{7}$$

The cross-chain communication protocol ensures the verifiable extraction and secure transmission of data $\mathrm{E}^{(\mathrm{j})}$ across different chains.

Table 5 shows the key parameter indicators of the report output layer under different report types, reflecting its core performance and reliability characteristics.

Based on tabular data, the report output layer demonstrates efficient generation capabilities and stable cross-chain integration performance across different report types. The cross-chain interoperability protocol relies on light-client bridges to ensure secure and efficient communication between different blockchain systems. Trust assumptions are defined based on the validation of proof of data via relay verification, while the attack surface is minimized by using hash-locked transfer schemes to prevent unauthorized access and data manipulation between chains.

3.2 Multidimensional Implementation Barriers

Based on the audit process design, the substantial bottlenecks it may encounter in three dimensions are examined: technical implementation, legal compliance, and industry acceptance. These obstacles together constitute the challenges that prevent it from being transformed from an ideal architecture into a standard operating procedure.

3.2.1 Technical barriers

Even after formal verification, smart contracts still possess inherent security vulnerabilities. Smart contracts contain complex business logic, which may contain flaws that can be maliciously exploited, leading to financial losses and/or incorrect conclusions in signature audits. Secondly, public blockchain technology and its related infrastructure often face scalability bottlenecks. Therefore, due to the limited transaction processing speed, transaction confirmation delays, and increased costs during network congestion, it has limitations in supporting enterprise-level real-time auditing. Finally, regarding data standardization and system integration, many information systems across different enterprises use different data formats and interface specifications. Therefore, to achieve smooth and accurate integration with blockchain, relevant entities need to invest time and resources in data format cleanup and interface specification adaptation.

3.2.2 Legal and compliance barriers

Another significant barrier to realize the full potential of Blockchain technology is the uncertainty related to the legal and compliance aspects. The current worldwide standards for auditing and regulations of Financial Services are primarily based on a centralized approach, thus raising doubts about the viability of automated audit processes (especially with regard to the underlying smart contract logic) in terms of compliance with existing Professional Standards. Approval from the regulatory authorities is therefore a requirement for any form of audit process to be carried out. In the case of an audit failure, the definition of legal obligations in respect of smart contract developers, deployers and the audited entity may present an entirely new challenge for the courts. Additionally, while Blockchain-based evidence cannot be altered, there is no universally accepted judicial precedent regarding the legal value of Blockchain-based evidence and there may be significant challenges in relation to its probative value before the courts, including in a cross-border context.

3.2.3 Practical and operational obstacles

At the practical level, there are many challenges to implement this solution, such as a lack of talent and economic constraints. One of the most important is the lack of qualified professionals, i.e. those with expertise in current auditing and certification methodologies and who can design and implement smart contracts based on blockchain technology which are necessary for introducing this 'code is law' automated approach. Furthermore, traditional

institutions, especially auditors who have been using subjective judgement and sampling methods for a period of time, are not inclined to accept and utilize this new automated model, which likely continue to impede adoption among users and industry stakeholders. Additionally, corporate executives may only be hesitant about adopting the new technology until they have a full understanding of how it works and alternative methods to ensure blockchain data privacy. Finally, the first costs of implementation of this new approach are not cheap, from selection of technology to the development of the system, deployment and integration with the legacy system, and its return on investment requires long-term practical validation.

3.2.4 Discussion of coping strategies

The smart contract development to do list must incorporate formal verification and multilayer security auditing as part of a mandatorily employed process as these two processes ensure a unified level of compliance that all smart contracts comply with. To permit the block chains to lessen their overall performance impediments by using the application of modular architecture and utilizing Layer 2 solutions for more scaling. From a legal perspective, a proactive approach can be to work with the different regulatory agencies to ensure that the legalities of a blockchain solution can be established through a regulatory sandbox within which innovative blockchain applications can be entertaining and also creating specific laws pertaining to the legal liability of smart contract breaches or misrepresentations. To address real-world problems, an extensive training program needs to be collaboratively defined between universities and industries in order to educate the next-generation talent between various fields implicated in developing blockchain infrastructure and solutions. Piloting a small number of high visibility use cases in situations where tangible benefits are obvious, like supply chain finance, can generate awareness in the industry, and show how blockchain technologies can create value. A simultaneous effort to create SaaS-based services delivered through cloud-based technologies can lower the initial cost threshold and technical burdens that are associated with implementation of a blockchain solution.

4 Results and Discussion

4.1 Effectiveness of the Plan

Five typical scenarios – financial audit, compliance audit, risk audit, operational audit, and IT audit – were selected as the test environment. By

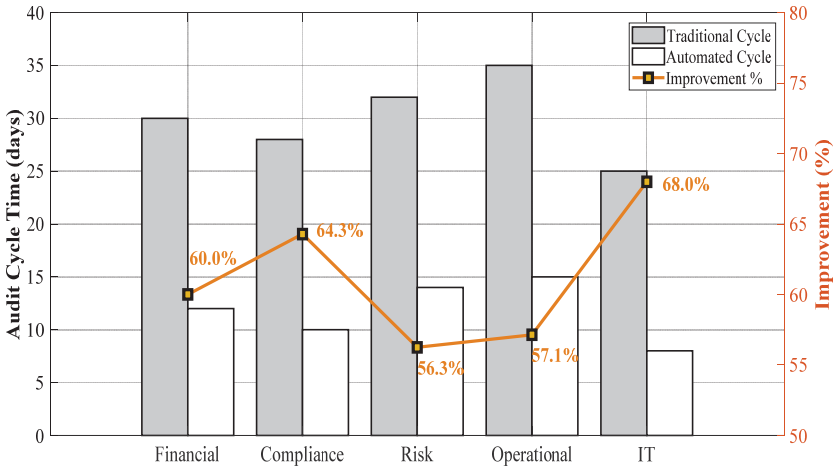

Figure 3 Audit cycle.

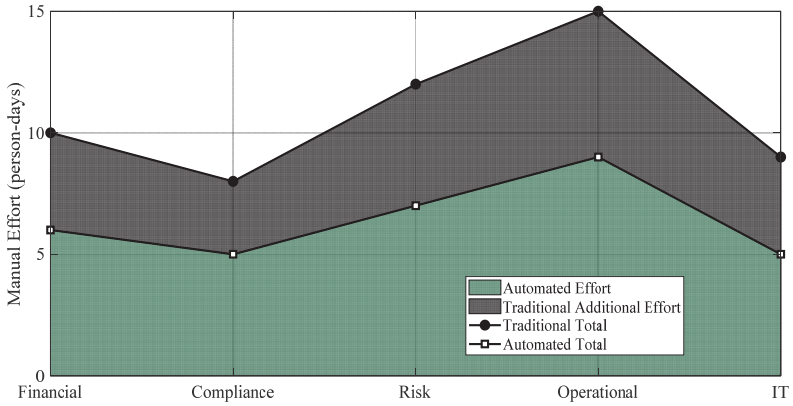

Figure 4 Cost distribution.

simulating real business data flow, comparative data were collected between traditional audit (which is centered on manual operation and relies on sampling inspection and post-event review) and automated audit.

The results are shown in Figures 3, 4, and 5.

The results analysis shows that, in all five cases, the implementation of automated auditing significantly reduced the total time required for completion of audit. Under traditional methods, on average, an audit took 25 to 35 days to complete. With automated auditing, the average time took 8 to 15 days. The improvement was most significant in the area of IT auditing,

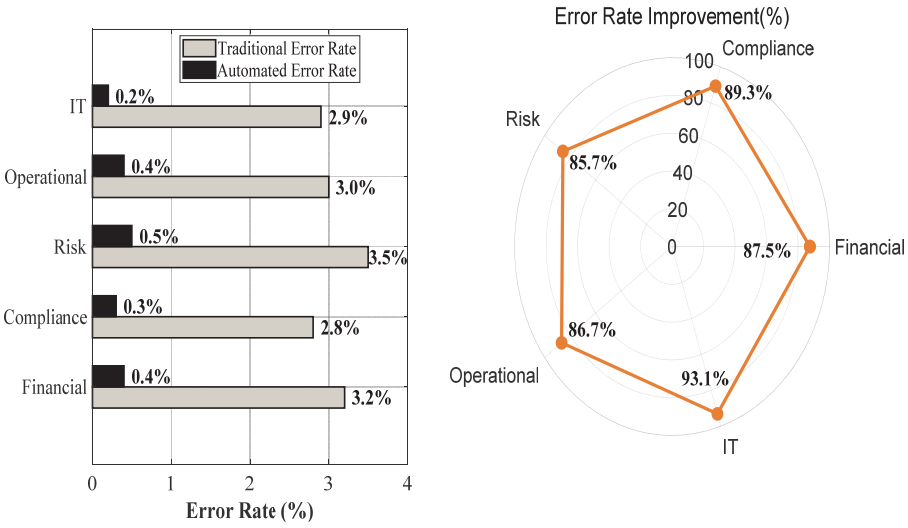

Figure 5 Audit results: error rate comparison (left) and improvement rate (right).

as the audit cycle is now reduced from 25 days to 8 days (improvement of 68%). Financial auditing and risk auditing cycles were reduced by 60% and 56.3%, respectively. Operational auditing, which has the greatest level of complexity, was the only case showing only a 57.1% rate of improvement, lower than the other cases. The rate of improvement of various automated processes showed different trends, and this indicated that the complexity of business audits was different and the degree of improvement brought about by automation also varied. IT auditing suffered the most because of the high level of standardization of IT data; and while operational auditing suffered the least because there is complexity in dealing with unstructured data. This suggests that smart contract-driven automated auditing processes work primarily in highly standardized environments and, in relatively unstructured business processes, there is a need for more detailed rules to work.

By comparing the cost of labor, automation is a great way to reduce the cost of the audit processes since traditional auditing takes 8 to 15 working days to complete, while the automated processes take only 5 to 9 days, which is a cost reduction of 37% to 44%. Due to high standardization of IT system software and hardware, the cost saving is about 44.4%, a huge contrast with the reliance on professional judgment in financial and operational audits. Although operational audits provide cost savings by about 40%, the absolute cost of labor is the highest for the audits, which means that companies should

work with human resource to maximize efficiency while automating these processes to reduce complexity. Further analysis shows that smart contract auditing is very effective in reducing repetitive audit tasks, but it still requires human supervision and judgement when using the system.

The automated audit of error rate control analysis shows a significant improvement in the reduction of error from an average of 2.8% to as high as 3.5% (in the traditional model) down to as low as 0.2% to as high as 0.5%, which is 85.7% to 93.1% improvement. Figure 5 (right) shows where the distribution of the improvement rates are different looking at IT versus Risk Audit: IT Auditing had the highest rate of improvement for the period at 93.1% and the lowest improvement of the 85.7% for Risk Audit. Figure 5 (left) shows the difference between the traditional model and the automated model, while Figure 5 (right) presents a more multi-dimensional view of the type of improvement in different scenarios. The analysis shows that through the standardization of execution, smart contract essentially eliminates human error, but Risk Auditing still has relatively high error rates because of the complexity of its rules, thus indicating that high complexity scenarios need more thorough formal verification and test coverage.

4.2 Disaster Recovery Testing

Five independent test scenarios were designed: single-node failure, multi-node failure, data breach attack, network partition, and hardware storage failure. During each scenario simulation, fault injection was carried out, and the results were evaluated by recording the mean recovery time, data integrity percentage, and system availability percentage. Each scenario was repeated 10 times, and the average of all measurements was taken. Test results are shown in the Table 6.

Due to its high reliability, the automated audit process performed exceptionally well in disaster recovery simulation tests. It achieved the fastest

Table 6 Key indicators for disaster recovery testing

Test Scenario	Average Recovery Time (ms)	Data Integrity (%)	System Availability (%)
Single-Node Failure	500	100.0	99.9
Multi-Node Failure	2000	99.5	99.0
Data Breach Attack	1000	98.0	98.5
Network Partition	1500	99.8	99.2
Hardware Storage Failure	3000	97.5	97.0

recovery speed and best results (no data loss) in the case of a single-node failure. However, the longest recovery time occurred when physical replacement of hardware components was required due to storage media failure. The test results confirm that the current automated audit process design can support continuous auditing of users and prevent business interruptions.

5 Conclusion

This paper provides a framework for an automated auditing solution powered by smart contracts. By employing a modular design to integrate several different methods of data verification, along with coding auditing rules as well as using zero-knowledge proof mechanisms, the paper have created a more efficient process that lowers overhead costs and reduces the chance of human error to less than 0.5%. Disaster recovery testing shows the durability of this solution; however, more research is needed in order to create a more adaptable method for dealing with complex and unstructured business environments. Future studies should concentrate on developing an adaptive rule engine capable of accommodating varying degrees of subjective judgment in auditing; investigating how AI can work in concert with smart contracts to create better outcomes; and establishing standards for cross-chain auditing and technologies associated with digital transformation of the entire audit domain. Zero-Knowledge Proofs offer significant scalability by ensuring privacy-preserving verification while supporting high transaction volumes. Their contextual adaptability across various audit scenarios makes them a robust solution for diverse industries, enhancing the overall effectiveness of automated auditing systems. The adaptive rule engine will incorporate subjective judgment modeling by embedding off-chain machine learning models that analyze contextual business factors, such as market conditions and financial behavior. This will allow the deterministic smart contract logic to adjust its behavior based on dynamic inputs, enabling it to handle complex audit scenarios and ensuring more accurate and adaptable decision-making in automated audits.

Declarations

Funding

Authors did not receive any funding.

Conflicts of Interests

Authors do not have any conflicts.

Data Availability Statement

The data generated and analyzed during the current study are available from the author Xiao Lanqing upon reasonable request but are not yet publicly available due to ongoing research.

Code availability

Not applicable.

Authors' Contributions

Xiao Lanqing is responsible for designing the framework, analyzing the performance, validating the results, and writing the article.

References

[1] Mustika I G. *Audit quality in state-owned enterprises: Audit costs, rotation, and company size*, Jurnal Ecoment Global, 2025, Vol. 10, No. 2, pp. 152–165.

[2] Zhang K. *Application of computer-aided audit systems and innovation research of enterprise financial audit under the background of big data*. Advances in Engineering Technology Research, 2023, Vol. 5, No. 1, p. 484.

[3] Han Shaozhen, Li Liaoning, Zhang Hanshi, Pan Ying, *Impact of internet transformation on enterprise audit fees*. Scientific Research Management, 2025, Vol. 46, No. 5, pp. 172–181.

[4] Varanasi S R. *HIPAA-as-code: Automated audit trails in AWS SageMaker pipelines*. European Journal of Engineering and Technology Research, 2025, Vol. 10, No. 5, pp. 23–26.

[5] Akinola A O, Olagunju A. *Automated accounting systems and external audit fees: Evidence from Nigeria*, KIU Interdisciplinary Journal of Humanities and Social Sciences, 2023, Vol. 4, No. 1, pp. 55–81.

[6] Akinola A O, Oladejo A O, Oluwakayode E F, et al. *Effect of automated accounting systems on audit independence: Evidence from Southwest*

Nigeria. Eurasian Journal of Management & Social Sciences, 2024, Vol. 5, No. 1, pp. 1–27.

[7] Zhou Xiaoli, *Innovative paths of enterprise audit work models under digital transformation*. China E-commerce, 2025, Vol. 26, No. 16, pp. 85–88.

[8] Zhong Rao, *Strategies for establishing and improving supervision mechanisms in enterprise audit rectification*. Vitality, 2025, Vol. 43, No. 14, pp. 121–123.

[9] Zaytsev A, Dmitriev N, Bunkovsky D, et al. *Audit of intellectual capital at an industrial enterprise: Open data digital model*. International Journal of Technology, 2022, Vol. 13, No. 7, pp. 1473–1483.

[10] Shatnawi S A, Marei A, Hanefah M M, et al. *Effect of audit committee on financial performance with enterprise risk management as a moderator.* Journal of Management Information & Decision Sciences, 2022, Vol. 25, No. 2, pp. 1–10.

[11] Salur M N, Kattar W K. *Impact of enterprise resource planning on audit in emerging technologies*. Ekonomi Maliye İşletme Dergisi, 2021, Vol. 4, No. 2, pp. 115–123.

[12] Dmitriev N, Zaytsev A, Faizullin R, et al. *Instrumental apparatus of innovative potential audit in project implementation*. International Journal of Technology, 2022, Vol. 13, No. 7, pp. 1484–1494.

[13] Morales H R, Porporato M, Epelbaum N. *Benford's law for integrity testing of high-volume databases: A state-owned enterprise case*. Journal of Economics, Finance and Administrative Science, 2022, Vol. 27, No. 53, pp. 154–174.

[14] Akinola A O, Olagunju A. 2023. *Automated accounting system and external audit fees: Empirical evidence from Nigeria*. KIU Interdisciplinary Journal of Humanities and Social Sciences, *4*(1), pp. 55–81.

[15] Yallamelli A R G, Ganesan T, Devarajan M V, Mamidala V, Yalla R M K, Sambas A. 2023. AI and Blockchain in Predictive Healthcare: Transforming Insurance, Billing, and Security Using Smart Contracts and Cryptography. *International Journal of Information Technology and Computer Engineering*, *11*(2), pp. 46–61.

[16] Lei S. *Application of big data in enterprise audit from a full coverage perspective*. Academic Journal of Business & Management, 2023, Vol. 5, No. 20, pp. 153–157.

[17] Gharrafi M, Mahouat N, Mohammed K, et al. *Role of corporate governance and internal audit in fraud prevention in Moroccan public*

enterprises. Pakistan Journal of Criminology, 2024, Vol. 16, No. 4, pp. 781–796.

[18] Hansa E, Ridaryanto P. *Differences in ERM and internal audit effectiveness before and during COVID-19*. Indonesian Interdisciplinary Journal of Sharia Economics, 2024, Vol. 7, No. 1, pp. 1907–1930.

[19] Su Aiping, *Audit strategies of state-owned enterprises under comprehensive reform*. Market Weekly, 2025, Vol. 38, No. 20, pp. 143–146.

[20] Jaber T A, Shah S M, Johari J, et al. *Impact of internal audit on enterprise risk management effectiveness*. International Journal of Academic Research in Accounting, Finance and Management Sciences, 2024, Vol. 14, No. 1, pp. 14–31.

[21] Jassem S. *Influence of internal audit functions on enterprise risk management in the transportation industry*. International Journal of Business Excellence, 2022, Vol. 26, No. 2, pp. 196–223.

[22] Zhang Senwei, *Enterprise audit risks and information-based audit strategies*. Chief Financial Officer, 2025, Vol. 21, No. 15, pp. 174–176.

[23] Bukhari T T, Oladimeji O, Etim E D, et al. *Automated control monitoring as a standard for continuous audit readiness*. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2021, Vol. 7, No. 3, pp. 711–735.

[24] Ghafoor Z, Ahmed I, Hassan A. *Audit committee characteristics, ERM, and stock price synchronicity*. Managerial Auditing Journal, 2022, Vol. 37, No. 1, pp. 69–101.

[25] Navasardyan A A, Nuretdinov I G. *Environmental audit of enterprises as a tool for environmental safety*. Izvestiya of Samara Scientific Center of the Russian Academy of Sciences, 2021, Vol. 23, No. 1, pp. 126–130.

[26] Hosayni S R, Ganji H R, Eskandari G, et al. *Effects of ERM and audit committee characteristics on firm reputation*. Empirical Research in Accounting, 2021, Vol. 11, No. 2, pp. 99–136.

[27] Fernhaber S A. *Actively engaging with social entrepreneurs: The social enterprise audit*. Entrepreneurship Education and Pedagogy, 2022, Vol. 5, No. 2, pp. 192–207.

[28] Li Y. 2025. *Application Mode of Blockchain Technology in User Data Sovereignty and Privacy Protection*. Journal of Cyber Security and Mobility, *14*(5), pp.1199–1220.

Biography

Xiao Lanqing (1995 -), female, Han ethnicity, from Hengyang, Hunan Province, is a lecturer with a master's degree. Her main research field is business administration.