International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 11 – Issue 01 || Jan - Feb 2026 || PP. 01-12

Enhancing Transparency and Trust in Auditing through Blockchain-Powered Smart Contracts

Millicent Boadi[1], Rahmayanti Cahyaningtyas[2], Silas Twum[3], Agus Widarson
[1]*Master Student, Department of Accounting, Universitas Pendidikan Indonesia*
[2]*Master Student, Department of Accounting, Universitas Pendidikan Indonesia*
[3]*Master Student, Department of Management, Universitas Pendidikan Indonesia*
[4]*Lecturer (Ph.D.), Department of Accounting, Universitas Pendidikan Indonesia*

Abstract: Background: The increasing complexity of corporate transactions and the growing reliance on digital financial systems have heightened concerns about audit reliability and data integrity. Traditional auditing approaches, which are often retrospective and manual, are increasingly vulnerable to fraud, manipulation, and information asymmetry. Blockchain-powered smart contracts are emerging as a transformative technology to strengthen audit transparency, reduce human intervention, and enhance stakeholder trust.
Purpose: This research aims to analyze how blockchain-based smart contracts can enhance transparency and trust in audit processes, as well as identify key challenges associated with their implementation. The study explores the relevance of smart contracts in modern auditing, their operational role in strengthening audit assurance, and the barriers that must be addressed to build trust in automated audit systems.
Methodology: This study adopts a Systematic Literature Review (SLR) approach by examining peer-reviewed articles published between 2018 and 2025. A total of 44 relevant studies were selected and analyzed through thematic content analysis to synthesize insights related to technological mechanisms, transparency outcomes, and implementation challenges.
Expected Outcome: The findings are expected to provide a comprehensive understanding of how smart contracts can support real-time auditing, automate compliance procedures, and create tamper-proof audit trails, thereby enhancing audit reliability and stakeholder trust.
Conclusion: This research contributes to the emerging discourse on technology-enabled auditing by demonstrating that blockchain-powered smart contracts have significant potential to strengthen audit transparency and integrity. However, successful adoption requires addressing code vulnerabilities, cost adoption, and skill readiness among auditors. Coordinated efforts from practitioners, regulators, and academic communities are essential to ensure secure and effective implementation of automated audit systems.
Key Words: Blockchain; Smart Contracts; Auditing; Transparency; Audit Technology

1. Introduction

Conventional financial auditing and reporting systems, which have long been the main foundation of corporate accountability, are now under critical scrutiny due to their vulnerability to information distortion and manipulation. Traditional mechanisms that rely heavily on data centralization and manual verification processes have proven to have significant weaknesses in terms of human error, information engineering, and fraudulent practices (Ajayi-Nifise et al,. 2024). This vulnerability is not hypothetical, but is reflected in various large-scale audit failures throughout history. The Enron scandal and the collapse of Arthur Andersen are classic examples that confirm how weak fraud detection in traditional audit systems can undermine public trust and market stability (Roszkowska 2020).

Manipulation and fraud that slip through traditional audit processes have been shown to cause significant financial losses on a global scale. According to the Association of Certified Fraud Examiners (ACFE), organizations worldwide lose approximately 5% of their annual revenue to fraud, a figure equivalent to global losses of more than $4.7 trillion (Alagha & Ozcelik, 2025). These losses are not merely incidental, but systemic failures. In the procurement sector alone, an area that should be closely monitored by audits, compliance failures have resulted in financial penalties exceeding $4.3 billion globally between 2016 and 2020 (Celestin 2021). In developing countries, the impact is even more severe, where more than 20% of public funds are estimated to be misallocated due to fraudulent practices (Celestin, 2021). Traditional auditing systems, which are often manual, time-consuming, and costly, coupled with the lack of real-time verification, create an environment where fraudulent activities can go undetected for long periods of time (Alagha & Ozcelik, 2025). These massive financial losses, both in the private and public sectors, directly undermine stakeholder confidence and demonstrate that the current system is no longer adequate to maintain integrity.

The root of this systemic vulnerability lies in two fundamental weaknesses of traditional audit architecture: reliance on human trust and retrospective processes. Conventional systems operate on a centralized

model, where trust is placed in intermediaries such as banks, administrators, and audit firms to validate and maintain data integrity (Adewale et al., 2022). This trust is subjective and prone to bias, error, or even deliberate collusion, as demonstrated by historical audit failures (Roszkowska, 2021). This problem is exacerbated by the slow and retrospective nature of the traditional audit process. Traditional financial audits often rely on periodic reporting, such as quarterly or annual reports (Adewale et al., 2022). This inherent delaythe time lag between when a transaction occurs and when it is audited creates a significant window of opportunity for fraudsters. Absence of real-time verification (Alagha & Ozcelik, 2025) allows fraudulent activities, such as those seen in the Wirecard and Luckin Coffee scandals, to go undetected for a long time, accumulating huge losses before they are finally uncovered (Alagha & Ozcelik, 2025).

Given these long-standing weaknesses, blockchain-powered smart contracts have emerged as a promising technological response. Early literature highlights the potential of blockchain to create immutable audit trails and automate compliance procedures, while smart contracts introduce system-enforced execution of audit rules (Lombardi et al., 2022; Roszkowska, 2020; Ajayi-Nifise et al., 2024). However, despite this growing interest, the existing body of research remains fragmented and largely conceptual. Studies tend to examine individual components such as blockchain immutability, smart contract automation, or audit efficiency in isolation, without providing an integrated understanding of how these mechanisms collectively enhance transparency and trust within real audit environments. Furthermore, empirical evidence is scarce, leaving unanswered questions about how smart contracts operate in practice, how they interact with enterprise systems, and how they address persistent challenges such as information asymmetry, fraud concealment, and delayed detection. Equally important, the literature has not sufficiently examined the practical barriers that inhibit implementation, including code vulnerabilities, cost burdens, regulatory uncertainty, and significant skill gaps among auditors. This fragmented research landscape creates a critical gap that must be addressed through a systematic and comprehensive review.

Therefore, this study fills that gap by synthesizing existing knowledge on the relevance, application, and challenges of blockchain-based smart contracts in auditing, and by offering an integrated understanding of how these technologies can realistically enhance transparency and trust in the financial statement audit process.

RQ1: Why are blockchain-based smart contracts relevant for enhancing the transparency and trust of the financial statement audit process?

RQ2: How are blockchain-based smart contracts applied to improve the transparency and trust of the financial statement audit process?

RQ3: What are the challenges in implementing blockchain-based smart contracts to enhance the transparency and trust of the financial statement audit process?

The main benefit of this research is that it provides clear guidance for academics, practitioners, and regulatory bodies. For academics, this research maps the fragmented research landscape and identifies areas ripe for future empirical research (Schmitz & Leoni, 2019). For practitioners and auditors, this review provides a balanced perspective, highlighting the potential of smart contracts for real-time auditing (Oraby 2025) while identifying security and legal risks that must be mitigated (White et al., 2019). For regulators, this research underscores the urgency of developing new governance frameworks and audit standards (Anis 2023; Cordeiro et al. 2025). By answering the three research questions posed, this systematic literature review contributes to building a solid foundation for the safe, effective, and trustworthy adoption of smart contract technology in the auditing profession.

2. Literature Review and Research Framework

2.1 Literature Review

The evolution of digital systems and past audit failures, most notably the Enron scandal, have underscored the weaknesses of traditional auditing practices, particularly in relation to data manipulation, inefficiency, and lack of transparency (Roszkowska, 2020). In response, a growing body of empirical and conceptual research has begun to explore the intersection of auditing, transparency, and digital technology. Among these technologies, blockchain has emerged as a transformative innovation with the potential to revolutionize both financial reporting and auditing (Adewale, 2022; Ajayi-Nifise, 2024).

Adewale et al. (2022) proposed a conceptual framework emphasizing blockchain's transformative role in promoting accountability, accuracy, and regulatory compliance. Their study highlighted how blockchain's decentralized, immutable, and secure ledger structure provides strong protection against data tampering and manipulation. Similarly, Ajayi-Nifise et al. (2024) identified blockchain as a "catalyst for transparency and integrity" in accounting, noting that each transaction recorded on the blockchain generates a verifiable audit trail, effectively advancing toward a triple-entry accounting model that significantly reduces opportunities for fraud and error.

Beyond passive record-keeping, smart contracts have emerged as key tools for automated execution. Kokogho et al. (2025) examined how smart contracts enable continuous auditing and real-time verification in the fintech industry. Their findings suggest that smart contracts can automate compliance with regulatory standards and, when integrated with advanced analytics such as AI, proactively detect anomalies. This aligns with Roszkowska's (2020) view that smart contracts can address historical audit failures by automating business rules and verification procedures, thereby minimizing human intervention and reducing risks of error and intentional manipulation.

Collectively, these studies reveal a consistent pattern: the integration of blockchain as an immutable ledger and smart contracts as automation engines holds significant theoretical promise for enhancing transparency and trust in auditing. However, as highlighted by Lombardi et al. (2022), the current body of research remains in its nascent stage, dominated by conceptual rather than empirical studies. Lombardi et al. (2022) classified existing literature into three key themes: (1) blockchain as a tool for auditors to save time and prevent fraud, (2) smart contracts as enablers of "Audit 4.0" efficiency, reporting, and transparency, and (3) the role of cryptocurrency and ICOs in shaping corporate governance. The review identified a clear research gapthe lack of robust empirical studies that bridge the divide between theoretical potential and practical implementation of blockchain-powered auditing.

2.2 Theoretical Framework

2.2.1 Agency Theory

Agency Theory, introduced by Jensen and Meckling (1976), explains conflicts between principals (organizations, investors) and agents (management, contractors). Information asymmetry and moral hazards create contractual inefficiencies that traditional auditing attempts to address through independent verification. However, traditional frameworks fail to propose concrete solutions for automating compliance enforcement. This is where smart contracts become transformative. They mitigate agency conflicts by automatically enforcing contractual obligations without requiring human intermediaries. By eliminating principal-agent conflicts through self-executing agreements, smart contracts provide a technological solution to the classic agency problem, building trust through automated, transparent, and objective execution rather than relying solely on human attestation.

2.2.2 Trust Theory

In this article, the trust theory by McKnight & Chervany (2001) serves as the applied theoretical framework to explain the fundamental shift in how audit trust is built. This theory distinguishes between interpersonal trust (Trusting Beliefs; beliefs in the auditor's integrity, benevolence, and competence) and institutional trust (Institution-Based Trust; beliefs in systems and structural assurances). Traditional audits rely heavily on Trusting Beliefs, which are vulnerable to human factors such as collusion, negligence, or fraud. In contrast, blockchain-based smart contracts shift the foundation of trust from individuals to the system itself through the concept of Structural Assurance. Smart contracts function as active structural guarantees; they are auditable, transparent, and automatically enforce compliance and audit procedures in real-time. Combined with blockchain's immutable and decentralized nature, stakeholders can now directly verify the audit process. Thus, trust is no longer rooted in the auditor's reputation but in the mathematical and transparent assurance that the audit process is executed exactly as programmed.

2.3 Conceptual Framework

Smart contracts are essentially computerized transaction protocols that execute terms of a contract, a concept first formalized by Nick Szabo (Andrés and Lorca 2021). They are self-executing digital contracts where the agreement's terms are written directly into lines of code (bodemer 2023; adewale 2022). These programs run in a decentralized manner on a blockchain (Andres and Lorca 2021) and are designed to operate autonomously, verifying their execution conditions and self-activating when necessary (desplebin et al 2021). Their core function is to automatically execute specific actions (bodemer 2023) and enforce the terms of an agreement (bonyuet 2020; celestin 2021) as soon as predefined conditions are met (Adewale, Olorunyomi, and Odonkor 2022; Bodemer 2023).

The primary benefit of blockchain-powered smart contracts is their ability to facilitate automated and tamper-proof agreements (bodemer 2023). By eliminating the need for intermediaries and manual interventions, they can significantly streamline operations, reduce administrative costs, and enhance trust in transactions (bodemer 2023). This automation not only saves time but also considerably reduces the risk of human error (desplebin et al 2021; celestin 2021). This automated enforcement helps ensure transparencyand can mitigate conflicts of interest by executing contractual obligations without bias (celestin 2021).

Smart contracts have a wide range of applications, particularly in automating and securing processes. In supply chain management, they are used to automate critical events like product registration, quality verification, and ownership transfers (codeiro et al 2025). They are also transforming auditing by enabling smart audit procedures(Bonyuet 2020) and defining frameworks for continuous, automated audit reports (Andres 2021). For instance, a smart contract can be used as an automated control tool (Desplebin, Lux, and Petit 2021), automatically checking for compliance with regulations (adewale 2022; celestin 2021) or matching sales contract provisions to identify erroneous transactions (bonyuet 2020). This automation also applies to procurement, where they can execute supplier payments automatically once delivery conditions are fulfilled (celestin 2021).

The contemporary audit environment faces increasing demands for greater assurance, data transparency, and stakeholder trust (codeiro et al 2025). Traditional audit processes, often criticized for their retrospective nature, sample-based testing, and reliance on siloed client systems, carry inherent risks related to data integrity and potential manipulation (adewale 2022). In response, blockchain technology, particularly smart contracts, has emerged as a disruptive innovation with the fundamental potential to revolutionize audit practices (ajayi-nifise 2024). The relevance of this technology (RQ1) lies in its ability to create a decentralized, immutable, and transparent ledger system (bonyuet 2020; ajayi-nifise 2024). This infrastructure fundamentally enhances transparency and integrity, significantly reducing the likelihood of fraud, errors, and misreporting (adewale 2022; bodemer 2023).

To grasp this potential, it is essential to explore specifically how blockchain-based smart contracts can be integrated into audit processes to enhance transparency and trust (RQ2). Smart contracts are "computerized transaction protocols that execute terms of a contract" (Andres 2021). They function as automated control tools (desplebin et al 2021) that automatically enforce predefined conditions (bodemer 2023). In an audit context, this translates to the automation of compliance checks (adewale 2022), the autonomous analysis of audit evidence (bonyuet 2020), and the creation of a framework for continuous audit reports (Andres 2021). By embedding audit logic and compliance rules directly into the code, smart contracts can facilitate "real-time auditing" (anis 2023; ajayi-nifise 2024), shifting the audit paradigm from periodic verification to continuous, automated assurance.

Nevertheless, the adoption of smart contracts in auditing is not without its hurdles. This implementation introduces a significant set of challenges that must be addressed before trust in these automated systems can be fully realized (RQ3). These challenges span multiple dimensions (anis 2023; adewale 2022). They include technical barriers such as scalability, ensuring the functional correctness of the smart contract code (Andres 2021), and interoperability with legacy systems (adewale 2022). Furthermore, significant organizational and regulatory obstacles exist, including regulatory ambiguities (adewale 2022), the need for new accounting and auditing standards (anis 2023), and addressing the critical "skill gaps" among auditors who must learn to interact with these new technological systems (anis 2023).

To systematically investigate these questions, a conceptual research framework is necessary. The following framework is proposed to map the relationships between the implementation of blockchain-powered smart contracts, the challenges that emerge from this implementation, and their ultimate impact on achieving a transparent and trusted audit process.

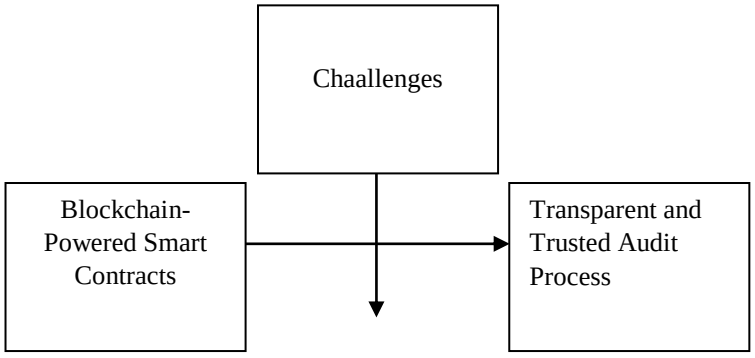

Figure 1: Conceptual Framework Based on Agency Theory and Trust Theory

3. Methodology

3.1 Research Design

This research uses a qualitative approach with a Systematic Literature Review (SLR) design (ajayi-nifise 2024). The SLR method was chosen because it provides a systematic, transparent, and replicable framework to

identify, evaluate, and synthesize all relevant and high-quality research evidence (codeiro et al 2025). This approach is essential for mapping the existing research landscape, understanding current trends, and identifying gaps in the literature (ajayi-nifise 2024). The purpose of this SLR is to comprehensively gather and analyze previous studies to answer the research questions regarding the relevance, application, and challenges of blockchain-powered smart contracts in the audit process.

The data collection process began with a systematic search across various major academic databases and industry report repositories. This initial search identified a total of 200 articles potentially relevant to the research topic. To ensure the novelty and relevance of the findings, the scope of publication was limited to articles published between 2020 and 2025. All 200 of these articles then underwent a rigorous screening process based on predetermined inclusion and exclusion criteria. After a careful eligibility assessment process, 28 articles were confirmed to meet all criteria and were selected for further analysis (codeiro et al 2025).

To extract and synthesize data from the 28 selected articles, this study applied a qualitative content analysis method, specifically through thematic analysis (anis 2023; codeiro et al 2025). Thematic analysis is a systematic method for identifying, analyzing, and reporting patterns (themes) within qualitative data (anis 2023). This process involved in-depth reading and systematic coding of each article to identify recurring concepts, patterns, and insights. The emerging themes were then categorized and linked to build a comprehensive understanding that directly answers the research questions.

3.2 Data Collection Methods

Data for this research was collected through a two-source methodological approach. First, case analyses were conducted on documented incidents of digital corruption or fraud within public sector institutions, with a particular focus on how investigative auditing and cybersecurity measures were applied to detect or prevent such incidents. Sources for this analysis included publicly available audit reports, forensic investigation findings, cybersecurity incident reports, and official publications from anti-corruption agencies and audit institutions.

Second, to complement the case analyses, a Systematic Literature Review (SLR) was performed on both academic and institutional literature. This review gathered peer-reviewed articles, policy papers, and technical reports published between 2020 and 2025 from databases such as Scopus, Science Direct, Emerald Insight, and Google Scholar. The search process employed keywords such as “Smart Contract Audit,” “Blockchain Audit,” and “Trustworthy Audit,” and followed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines to ensure transparency and replicability.

3.3 Data Analysis

The data was analyzed using thematic analysis, which enabled the researcher to identify and interpret recurring patterns and relationships across case studies and literature sources. The process began with familiarization, involving careful reading and coding of the collected data. Next, initial codes were generated based on recurring ideas related to auditing practices.

3.4 Validity and Reliability

To maintain the study’s validity, only credible and authenticated sources such as peer-reviewed journals and reputable institutional publications were utilized. Reliability was strengthened through triangulation between case evidence and insights from the literature. In addition, clear and transparent reporting of data selection and coding procedures ensures that the research remains reproducible and verifiable.

3.5 Scope and Delimitation

The study focused on the emerging adoption of blockchain and smart contract technologies, where challenges related to transparency and trust remain significant. Since the analysis was based on secondary data, the findings provide contextual insights rather than broadly generalizable conclusions across all sectors. Nonetheless, by integrating case evidence with a systematic literature review, this study offers a balanced, evidence-based perspective on how blockchain-powered smart contracts can enhance transparency, accountability, and trust in the auditing process.

4. Findings and Discussion

4.1 Findings

4.1.1 Relevance of Blockchain-Based Smart Contracts for Enhancing Audit Transparency and Trust (RQ1)

The review demonstrates a clear and consistent agreement across the literature that blockchain-powered smart contracts fundamentally address the long-standing vulnerabilities of traditional auditing systems. Conventional audits rely heavily on centralized databases, manual verification, and periodic review cycles, all of which create significant exposure to manipulation, information asymmetry, and retrospective detection of errors or fraud (Busari & Zaynab, 2025). Blockchain’s decentralized, distributed ledger architecture directly addresses these weaknesses by ensuring that data recorded on the ledger is immutable, chronologically ordered, and

cryptographically secured(Antal et al., 2021). Once a transaction is added, it cannot be unilaterally altered or deleted, thereby eliminating the possibility of concealed adjustments or backdated entries that often undermine audit credibility. This structural integrity, repeatedly highlighted by Adewale et al. (2022) and Ajayi-Nifise et al. (2024), lays the foundation for a transparent and tamper-resistant audit environment.

Beyond providing immutable records, the relevance of smart contracts becomes even more significant when viewed through the lens of Trust Theory and Agency Theory**,** which explain why trust failures persist in traditional auditing. Trust Theory posits that stakeholders typically rely on interpersonal trust in the competence, integrity, and professionalism of the auditor(Rawashdeh, 2025). However, past audit failures such as Enron, Wirecard, and Luckin Coffee illustrate the fragility of this model, where auditors can miss, overlook, or even collude in fraudulent reporting. Smart contracts shift the foundation of trust away from personal credibility toward structural assurance, meaning that trust is placed in the system's technical properties rather than in individuals. These contracts execute predefined audit rules automatically, verify compliance conditions in real time, and provide audit evidence continuously, minimizing the need for subjective interpretation or discretionary human judgment.

From the perspective of Agency Theory, traditional audits attempt to reduce information asymmetry between principals (investors, regulators, and owners) and agents (management)(Ajaegbu & Mmayie, 2025). However, because the audit process is periodic, sample-based, and dependent on centralized client systems, managers often retain substantial control over the information environment. Smart contracts directly reduce this information gap by embedding audit logic into decentralized code that all authorized parties can observe. As a result, principals gain direct access to validated, real-time financial data, while managers lose the ability to selectively withhold or manipulate information. This technological enforcement of transparency dramatically strengthens monitoring mechanisms and reduces the classic agency problem of opportunistic managerial behavior.

Moreover, smart contracts enhance audit trust by providing continuous access to audit trails that are verifiable by multiple participants(Assiri & Humayun, 2023). Each transaction, control action, or compliance check is captured permanently on-chain, creating a transparent ecosystem where discrepancies can be quickly detected and traced back to their origin. This reduces reliance on ex-post document examination - a process vulnerable to forgery and reconstruction, and replaces it with automatic, real-time verification(Kasztelnik, 2025). The literature reviewed in the study emphasizes that this shift from retrospective to proactive assurance represents one of the most significant advances in modern auditing.

4.1.2 Application of Smart Contracts in Audit Processes (RQ2)

The SLR reveals that blockchain-powered smart contracts are not merely theoretical innovations but operational tools capable of reshaping audit processes. Their application spans automation, real-time assurance, integration with enterprise systems, and enhancement of fraud detection mechanisms(Bello et al., 2024). Across the reviewed studies and Big 4 case examples, smart contracts emerge as practical infrastructures that embed audit logic directly into organizational transactions. This enables auditors to transition from passive reviewers of historical data to active overseers of continuously validated financial information.

4.1.2.1 Real-Time Auditing and Continuous Assurance

Smart contracts introduce a foundational shift in how auditors collect evidence and evaluate compliance. Traditional auditing relies on retrospective procedures such as periodic testing, sampling, and self-reported client information, all of which expose audits to delays, incompleteness, and manipulation. The literature consistently emphasizes that smart contracts automate these procedures by verifying transactions at the moment they occur, without waiting for periodic reporting cycles (Andres, 2021; Desplebin et al., 2021).

This "always-on" audit environment eliminates reliance on sampling techniques and allows full-population testing, where every transaction is checked against predefined contractual and regulatory rules. As soon as a breach or inconsistency occurs, the system generates an automatic alert or blocks the transaction entirely. This capacity provides auditors with real-time visibility into financial events, drastically reducing detection lags that previously allowed fraud such as that in Wirecard and Luckin Coffeeto remain concealed for extended periods. Consequently, smart contracts transform the audit role from detecting past errors to actively preventing noncompliance in real time.

4.1.2.2 Automated Control Systems

The SLR identifies that smart contracts extend beyond mere verification to become active internal control mechanisms. By encoding organizational policies, financial reporting rules, and regulatory requirements into executable code, smart contracts autonomously enforce compliance without human intervention (Celestin, 2021; Bonyuet, 2020).

Within procurement processes, smart contracts automatically validate vendor credentials, match purchase orders with delivery records, and authorize payments only when contractual terms are satisfied(Omar et al., 2021). In supply chain auditing, they ensure that inventory flows, production milestones, and logistics data align with corporate records, thereby eliminating opportunities for duplicated invoices or manipulation of cost figures (Olajide et al., 2021). In financial reporting, smart contracts cross-check journal entries, revenue recognition conditions, and transaction timestamps against embedded audit rules (Gupta, 2025).

This automation not only strengthens internal controls but also provides auditors with an evidence trail that is inherently tamper-resistant. Errors or anomalies are not discovered months later during year-end audits; instead, they are identified instantaneously, improving both accuracy and speed of audit procedures. The literature supports the view that automated audit controls are a key building block of "Audit 4.0," where technology takes over routine assurance tasks, freeing auditors to focus on high-level analysis and judgment (Dai, 2017).

4.1.3 Challenges Hindering Implementation of Smart Contract-Based Auditing (RQ3)

Although blockchain-powered smart contracts demonstrate strong potential to enhance transparency and trust in audits, the SLR reveals that their implementation is hindered by substantial technical, organizational, and human-capital challenges. These obstacles threaten the reliability, security, and scalability of automated audit systems and must be resolved before widespread adoption becomes feasible. The challenges are grouped into four major themes.

4.1.3.1 Code Immutability and Vulnerability Risks

One of the foundational strengths of blockchain immutability also becomes a critical limitation when smart contracts are used for auditing. Since deployed smart contracts cannot be modified, corrected, or patched, any coding flaw becomes a permanent part of the system. The article notes that this creates a significant paradox: while immutability ensures trustworthiness by preventing unauthorized alterations, it also locks in logical errors, bugs, or security vulnerabilities that may compromise audit outcomes (Taherdoost, 2023; Setiono & Nasution, 2025).

In auditing contexts, smart contracts often encode complex accounting rules, regulatory provisions, and internal control logic. These rules are sensitive to coding precision, and even minor errors can lead to misinterpretation of audit conditions, false positives/negatives, or failure to detect fraudulent transactions. Redeploying the contract is possible, but the process is costly and introduces additional operational risk, especially when multiple parties rely on the contract for synchronized audit evidence. As a result, immutability introduces a high-stakes environment in which coding accuracy must approach perfection a standard that is difficult to achieve given the interdisciplinary nature of audit logic and programming.

4.1.3.2 Network Security and Node Participation Risks

The effectiveness of blockchain-based auditing depends heavily on the underlying network structure. A blockchain must be sufficiently decentralized, with a large and distributed set of nodes validating transactions. However, as highlighted in the article, low network participation creates a "thin" blockchain that is vulnerable to malicious attacks, allowing attackers to manipulate blockchain data or disrupt transaction verification (Zheng et al., 2024).

For audit processes, this is a critical concern. If the blockchain supporting audit evidence becomes compromised, the entire automated assurance mechanism collapses. The literature shows that a reduction in bookkeeping nodes raises the economic incentive for network attacks, including 51% attacks or node corruption, which can rewrite or halt transaction validation. This contradicts the very essence of blockchain's promised transparency and tamper-resistance.

Furthermore, organizations may hesitate to commit resources to maintain a large network solely for audit purposes, especially when the perceived benefits are uncertain. Thus, low network participation not only threatens system security but also becomes a barrier to building trust among users who depend on the system for reliable audit information.

4.1.3.3 High Cost and Low Adoption Incentives

The article identifies cost-effectiveness as a major determinant of whether auditors and clients adopt blockchain-based smart contract systems. Implementation requires substantial financial investment, including acquiring or developing blockchain platforms, upgrading IT infrastructure, integrating new audit tools, and training audit personnel.

Simulation models (Zheng, 2024) show that when these upfront costs exceed expected benefits, both auditors and clients rationally reject adoption. The decision becomes a strategic one:

- Auditors may see no immediate increase in revenue or efficiency that justifies the investment.
- Audit clients may view the adoption as too disruptive or costly, especially when legacy systems still function adequately.

The SLR also reveals that adoption speeds increase only when costs decrease or when incentives such as regulatory pressure, competitive advantage, or enhanced operational efficiency become more tangible. Without clear financial benefits, organizations hesitate to transition from familiar traditional audit systems to smart-contract-based alternatives.

This cost-benefit mismatch remains a central barrier to large-scale deployment, particularly in developing economies or smaller firms with limited technological budgets.

4.1.3.4 Skill Gaps Among Auditors

The article highlights a critical human-capital challenge: auditors are generally not trained in the technical skills required to validate or evaluate blockchain-based systems. Smart contract auditing requires expertise in coding (e.g., Solidity), cryptography, blockchain architecture, and cybersecurity skills that fall outside the traditional competencies of financial auditors (Popchev, 2021; Roszkowska, 2020).

This creates several problems:

1. Auditors cannot independently verify the correctness of smart contract code, meaning they must rely on external experts or automated tools, which undermines the auditor's assurance function.
2. The automated system becomes a "black box" when auditors lack knowledge of how the code executes audit logic. This paradoxically reduces trust rather than increasing it.
3. Audit firms face difficulties integrating smart contract technology into their work due to limited in-house technical capacity.
4. Universities and professional training bodies have not yet fully incorporated blockchain or smart contract auditing into their curricula, widening the competency gap.

The SLR emphasizes that overcoming this challenge requires interdisciplinary collaboration between auditors, programmers, and legal experts, as well as updated curricula, certification programs, and professional development initiatives. Without these capacity-building efforts, auditors will be unable to effectively oversee or validate automated systems, hindering the trustworthiness of smart contract–based auditing.

Collectively, these challenges illustrate that while smart contracts offer transformative potential, their implementation in auditing requires deep structural adjustments. Technical reliability, cybersecurity, financial feasibility, and human expertise must align before smart contract auditing can be safely and widely adopted. The findings underscore that the future of automated auditing depends not only on technological innovation but also on regulatory updates, organizational readiness, and the development of a new generation of tech-savvy auditors.

4.1.4 Case-Based Insights from Big 4 Company

4.1.4.1 PricewaterhouseCoopers(PwC): The Intelligent Audit Mechanism

PwC has taken the lead in developing a blockchain-based "networked audit system" that connects with enterprise financial systems in real time using distributed ledger technology (DLT) to enable cross-agency data sharing. For instance, in a supply chain audit, the information of suppliers, logistics providers, and customers is synchronized on the blockchain, allowing auditors to directly verify the authenticity and integrity of transactions, thereby reducing manual reconciliation time by 90% compared to traditional models (PwC, 2017). Moreover, PwC incorporates AI models such as DeepSeek-R1 into its blockchain audit platform to automatically detect unusual transaction patterns. In a 2023 audit of a multinational corporation, the system successfully identified five fictitious cross-border transactions totaling US$12 million, demonstrating the synergistic potential of combining "blockchain + AI" for early risk detection.

4.1.4.2 Ernst and Young (EY): The Blockchain Analyzer

EY has created the "EY Blockchain Analyzer", a tool designed to facilitate pass-through audits of crypto currencies and smart contracts. Its main innovation is the integration of zero-knowledge proof (ZKP) technology, which enables organizations to demonstrate transaction compliance to auditors without disclosing sensitive information. For instance, during the audit of a financial institution's crypto assets, EY used ZKP to confirm the authenticity of its Bitcoin reserves while maintaining customer privacy (EY, 2023). This advancement effectively addresses the tension between blockchain transparency and data confidentiality in enterprises.

4.1.4.3 Deloitte: Private Chain in The Financial Sector

Deloitte has emphasized blockchain-based audits in the financial industry by collaborating with JPMorgan Chase to create Deloitte Chain Finance, a private blockchain platform that automates the processing of letters of credit and trade finance. The system records loan origination and repayment data on-chain in real time, enabling auditors to verify compliance through smart contracts, which reduced a bank's LC audit cycle from 14 days to 2 days and lowered the error rate by 75% (Deloitte, 2021).

4.1.4.4 KPMG: Supply Chain Tracking System in Retail Industry

KPMG developed an innovative contract-based supply chain tracking system using blockchain technology to enhance audit processes in the retail industry. In one case involving a global FMCG brand, the system recorded data on procurement, production, and logistics on-chain, automatically matched inventory and sales information, and enabled auditors to detect a supplier's fraudulent repeated invoicing, helping the company recover around US$8 million in losses (KPMG, 2017).

4.2 Discussion

The findings of this study demonstrate that blockchain-powered smart contracts have the potential to fundamentally transform the audit environment by addressing persistent weaknesses inherent in traditional auditing systems. Through the lens of Agency Theory and Trust Theory, the discussion highlights how immutability, decentralization, and automation reshape the foundations of audit assurance, while also underscoring the barriers that limit widespread adoption.

First, the relevance of blockchain-enabled smart contracts becomes evident when viewed against the structural deficiencies of traditional auditing. Conventional systems rely heavily on human judgment, retrospective procedures, and centralized information repositories, all of which contribute to information asymmetry and vulnerability to manipulation. The findings show that blockchain's decentralized architecture reduces the dominance of individual actors by enabling transparent, tamper-proof audit trails (Ahmad et al., 2021). This supports Trust Theory's concept of structural assurance, where trust is rooted in system reliability rather than the auditor's personal competence or integrity. Smart contracts further deepen this transformation by embedding audit logic directly into the transactional process, thereby reducing the window of opportunity for concealment or misreporting an outcome that aligns with Agency Theory's goal of minimizing opportunistic managerial behavior.

The results also highlight that the application of smart contracts in auditing extends beyond theoretical possibilities. The case analyses from PwC, EY, Deloitte, and KPMG demonstrate that smart-contract-based auditing is already being operationalized in sophisticated contexts such as supply chain audits, crypto asset verification, trade finance, and fraud detection. These real-world examples validate the technological promise identified in the literature and show how automated controls, real-time auditing, and advanced cryptography (e.g., zero-knowledge proofs) enhance the accuracy, speed, and reliability of audit evidence. Smart contracts enable continuous assurance an evolution from periodic, sample-driven audits to full-population, real-time verification indicating a paradigm shift toward Audit 4.0.

However, the findings indicate that the path to adoption is neither linear nor uncomplicated. Several critical challenges hinder the widespread implementation of smart-contract-based auditing. The inherent immutability of blockchain creates a double-edged sword: while it ensures data integrity, it also locks in coding errors that may compromise audit quality (Paik et al., 2019). This raises new forms of audit risk that did not exist in traditional systems. Furthermore, blockchain's security depends heavily on network size and participation. Low node participation creates vulnerabilities that undermine the very trust blockchain is designed to establish. These technical risks signal that the implementation of blockchain requires robust governance mechanisms and secure network structures issues that regulators have not yet fully addressed.

Equally noteworthy are the economic and human-capital constraints. High implementation costs spanning infrastructure investment, system integration, and workforce training deter adoption, particularly for smaller firms or firms in developing economies. The findings reinforce that cost–benefit considerations play a decisive role in determining whether clients and auditors embrace the technology. Even when potential long-term benefits exist, the absence of immediate financial incentives significantly reduces adoption readiness.

The most pronounced barrier, however, is the skill gap among auditors. Smart-contract auditing requires competencies in coding, cryptography, blockchain architecture, and cybersecurity skills not traditionally associated with the accounting profession (Bhatti et al., n.d.). This skills deficit transforms smart contracts into opaque "black boxes," limiting the auditor's ability to validate the correctness of the automated processes. Without bridging this gap, confidence in automated auditing systems may deteriorate rather than strengthen. This finding aligns with broader concerns in the literature that technological disruption in auditing requires substantial re-skilling and interdisciplinary collaboration.

Taken together, these insights indicate that blockchain-based smart contracts are not merely technological innovations but catalysts for a broader paradigm shift in auditing. The technology has the potential to establish a real-time, transparent, and highly reliable audit ecosystem. However, realizing this potential requires addressing fundamental technical, educational, and organizational challenges. Regulatory bodies need to update audit standards to accommodate decentralized and immutable processes, while academic institutions and professional associations must redesign curricula to prepare auditors for the digital era.

In summary, the discussion reaffirms that smart contracts offer a transformative pathway toward continuous, transparent, and trustworthy auditing, yet their practical realization depends on coordinated efforts across the auditing profession, regulatory institutions, and academia. Without such alignment, the promise of blockchain-enabled auditing will remain partially fulfilled, with adoption occurring unevenly across industries and jurisdictions.

5 Implications

The findings of this study carry important implications for practice, policy, and future research in the auditing profession. For practitioners, the emergence of blockchain-powered smart contracts requires a fundamental redesign of audit procedures toward continuous, real-time assurance rather than periodic, sample-based verification. Audit firms must invest in technological capacity building by training auditors in blockchain architecture, cryptography, smart contract logic, and cybersecurity, while fostering stronger collaboration between auditors, software engineers, and IT specialists to ensure that the audit logic embedded in smart contracts accurately reflects regulatory and accounting requirements. From a policy perspective, regulators must update existing auditing standards to address issues unique to smart contracts and blockchain systems, including guidelines for validating on-chain audit evidence, assessing automated controls, and clarifying legal liabilities associated with immutability, coding errors, and system failure. Policymakers also need to provide clearer frameworks for data privacy, error correction mechanisms, and cybersecurity requirements tailored to decentralized audit systems, while creating economic incentives that support organizations transitioning to blockchain-enabled assurance. For future research, the study highlights the need for empirical evidence that tests the real-world effectiveness and cost-benefit dynamics of smart contract auditing, as current literature remains mostly conceptual. Further studies should explore how auditors interact with automated systems, how trust is formed between humans and blockchain-based processes, and how skill gaps influence audit quality. Developing standardized frameworks, tools, and protocols for evaluating smart contract reliability and auditability remains essential, as does investigating regulatory readiness across jurisdictions to understand how global audit ecosystems can adapt to this technological shift. Collectively, these implications emphasize that the successful adoption of smart-contract-enabled auditing depends on coordinated progress across professional practice, regulatory reform, and interdisciplinary research.

6 Conclusion

This study confirms that blockchain-based smart contracts hold substantial potential in enhancing transparency and trust within audit environments. With their immutable and decentralized nature and ability to execute rules automatically, this technology enables real-time auditing and reduces dependence on manual verification processes that are prone to error and manipulation (Adewale et al., 2022; Ajayi-Nifise et al., 2024). Smart contracts can also function as automated control tools that ensure compliance and continuously generate audit evidence without direct auditor intervention (Desplebin et al., 2021; Rozario & Vasarhelyi, 2018).

However, the findings also highlight significant challenges in implementing this technology. Code vulnerabilities and logical errors within smart contracts remain leading threats to system reliability (He et al., 2020; Chaliasos et al., 2024). In addition, the current legal and regulatory ecosystem is not yet fully equipped to accommodate the decentralized and immutable characteristics of blockchain, creating ambiguity regarding liability and mechanisms for error correction (Ellul et al., 2020). Skill gaps among auditors in understanding blockchain technology also present a major barrier to adoption (Anis, 2023).

Therefore, collaborative efforts among regulators, practitioners, and academics are necessary to develop technology-enabled audit standards, clearer legal frameworks, and professional training programs. The implementation of smart contracts in auditing represents not only a technological shift but also a paradigm shift toward a more automated, transparent, and digitally-verified audit ecosystem (Bonyuet, 2020; Cordeiro et al., 2025). If these challenges are properly addressed, smart contract adoption has the potential to drive the evolution toward continuous and trustworthy auditing in the digital era.

Reference

[1]. Adewale, Titilope Tosin, Titilayo Deborah Olorunyomi, and Theodore Narku Odonkor. 2022. "Blockchain-Enhanced Financial Transparency: A Conceptual Approach to Reporting and Compliance." *International Journal of Frontiers in Science and Technology Research* 2(1): 024–045. doi:10.53294/ijfstr.2022.2.1.0027.

[2]. Ajaegbu, E. E., & Mmayie, S. (2025). Resolving Principal Agent Conflicts: Revisiting Agency Theory Through the Lens of Internal Audit. *International Journal of Innovative Science and Research Technology*, *10*, 1050–1059.

[3]. Ajayi-Nifise, Adeola Olusola, Titilola Falaiye, Odeyemi Olubusola, Andrew Ifesinachi Daraojimba, and Noluthando Zamanjomane Mhlongo. 2024. "Blockchain In U.S. Accounting: A Review: Assessing Its Transformative Potential For Enhancing Transparency And Integrity." *Finance & Accounting Research Journal* 6(2):159–82. doi:10.51594/farj.v6i2.786.

[4]. Alagha, Bilal, and Ilker Ozcelik. 2025. "BEATS: Practical Audit Trail in Blockchain Systems." *IEEE Access* 13:109657–69. doi:10.1109/ACCESS.2025.3582722.

[5]. Andrés, Javier De, and Pedro Lorca. 2021. "On the Impact of Smart Contracts on Auditing." *The International Journal of Digital Accounting Research* 155–81. doi:10.4192/1577-8517-v21_6. DOI: 10.4192/1577-8517-v21_6

[6]. Anis, Ahmed. 2023. "Blockchain in Accounting and Auditing: Unveiling Challenges and Unleashing Opportunities for Digital Transformation in Egypt." *Journal of Humanities and Applied Social Sciences* 5(4):359–80. doi:10.1108/JHASS-06-2023-0072.

[7]. Antal, C., Cioara, T., Anghel, I., Antal, M., & Salomie, I. (2021). Distributed ledger technology review and decentralized applications development guidelines. *Future Internet*, *13*(3), 62. https://doi.org/10.3390/fi13030062

[8]. Assiri, M., & Humayun, M. (2023). A blockchain-enabled framework for improving the software audit process. *Applied Sciences*, *13*(6), 3437. https://doi.org/10.3390/app13063437

[9]. Bello, H. O., Idemudia, C., & Iyelolu, T. V. (2024). Integrating machine learning and blockchain: Conceptual frameworks for real-time fraud detection and prevention. *World Journal of Advanced Research and Reviews*, *23*(1), 56–68. https://doi.org/10.30574/wjarr.2024.23.1.1985

[10]. Bhatti, A., Mutlib, A., Waheed, A., Tasleem, I., & Khan, A. (n.d.). The Future Of Chartered Accountancy Integrating Ai And Block-Chain Into Financial Auditing.: https://doi.org/10.5281/zenodo.15280815

[11]. Bodemer, Oliver. 2023. "Transforming the Insurance Industry with Blockchain and Smart Contracts: Enhancing Efficiency, Transparency, and Trust."

[12]. Bonyuet, Derrick. 2020. "Overview and Impact of Blockchain on Auditing." *The International Journal of Digital Accounting Research* 31–43. doi:10.4192/1577-8517-v20_2.

[13]. Busari, M., & Zaynab, S. (2025). *Decentralized Ledgers and Corporate Finance Transformation: A Comparative Study of Traditional and Blockchain-Based Reconciliation Systems*.

[14]. Celestin, Mbonigaba. 2021. "How Smart Contracts Are Transforming Legal Compliance In Procurement Transactions." doi:10.5281/ZENODO.15057002.

[15]. Chaliasos, Stefanos, Marcos Antonios Charalambous, Liyi Zhou, Rafaila Galanopoulou, Arthur Gervais, Dimitris Mitropoulos, and Benjamin Livshits. 2024. "Smart Contract and DeFi Security Tools: Do They Meet the Needs of Practitioners?" Pp. 1–13 in *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*. Lisbon Portugal: ACM.

[16]. Chen, Haiwen, Huan Zhou, Jiaping Yu, Kui Wu, Fang Liu, Tongqing Zhou, and Zhiping Cai. 2021. "Trusted Audit with Untrusted Auditors: A Decentralized Data Integrity Crowdauditing Approach Based on Blockchain." *International Journal of Intelligent Systems* 36(11):6213–39. doi:10.1002/int.22548.

[17]. Cordeiro, Manuela, Joao Carlos Amaro Ferreira, Luis Elvas, and Vitor Fernandes. 2025. "Blockchain-Powered Traceability in the Wine Industry: Enhancing Transparency and Consumer Trust." *Blockchain: Research and Applications* 100405. doi:10.1016/j.bcra.2025.100405.

[18]. Dai, J. (2017). *Three essays on audit technology: audit 4.0, blockchain, and audit app*. Rutgers University-Graduate School-Newark.

[19]. Desplebin, Olivier, Gulliver Lux, and Nicolas Petit. 2021. "To Be or Not to Be: Blockchain and the Future of Accounting and Auditing*." *Accounting Perspectives* 20(4):743–69. doi:10.1111/1911-3838.12265.

[20]. Ellul, Joshua, Jonathan Galea, Max Ganado, Stephen Mccarthy, and Gordon J. Pace. 2020. "Regulating Blockchain, DLT and Smart Contracts: A Technology Regulator's Perspective." *ERA Forum* 21(2):209–20. doi:10.1007/s12027-020-00617-7.

[21]. Fahdil, Husam Nawfal, Hayder Mohammed Hassan, Adel Subhe, and Abdulrazzaq Tuama Hawas. 2024. "Blockchain Technology in Accounting Transforming Financial Reporting and Auditing." *Journal of Ecohumanism* 3(5):216–33. doi:10.62754/joe.v3i5.3903.

[22]. Gupta, S. (2025). *AI, Blockchain, And Autonomous Innovation*.

[23]. Kasztelnik, K. (2025). Blockchain Technology and Smart Contracts for Fraud Detection and Deterrence in Cryptocurrency Markets. *Journal of Forensic Accounting Research*, *10*(1), 102–128.

[24]. Kokogho, Eseoghene, Obianuju Clement Onwuzulike, Bamidele Michael Omowole, Chikezie Paul-Mikki Ewim, and Mary Oyenike Adeyanju. 2025. "Blockchain Technology and Real-Time Auditing: Transforming Financial Transparency and Fraud Detection in the Fintech Industry." *Gulf Journal of Advance Business Research* 3(2):348–79. doi:10.51594/gjabr.v3i2.88.

[25]. Olajide, J. O., Otokiti, B. O., Nwani, S., Ogunmokun, A. S., Adekunle, B. I., & Efekpogua, J. (2021). Building an IFRS-Driven Internal Audit Model for Manufacturing and Logistics Operations. *IRE Journals*, *5*(2), 261–263.

[26]. Omar, I. A., Jayaraman, R., Debe, M. S., Salah, K., Yaqoob, I., & Omar, M. (2021). Automating procurement contracts in the healthcare supply chain using blockchain smart contracts. *IEEE Access*, *9*, 37397–37409.

[27]. Oraby, Salah Ahmed. 2025. "The Impact of Blockchain Technology on Accounting and Auditing Functions: Evidence from Saudi Arabia." *Pakistan Journal of Life and Social Sciences (PJLSS)* 23(1). doi:10.57239/PJLSS-2025-23.1.0026.

[28]. Paik, H.-Y., Xu, X., Bandara, H. M. N. D., Lee, S. U., & Lo, S. K. (2019). Analysis of data management in blockchain-based systems: From architecture to governance. *Ieee Access*, *7*, 186091–186107.

[29]. Rawashdeh, A. (2025). Bridging the trust gap in financial reporting: the impact of blockchain technology and smart contracts. *Journal of Financial Reporting and Accounting*, *23*(2), 660–679.

[30]. Roszkowska, Paulina. 2020. "Fintech in Financial Reporting and Audit for Fraud Prevention and Safeguarding Equity Investments." *Journal of Accounting & Organizational Change* 17(2):164–96. doi:10.1108/JAOC-09-2019-0098.

[31]. Rozario, Andrea M., and Miklos A. Vasarhelyi. 2018. "Auditing with Smart Contracts." *The International Journal of Digital Accounting Research* 1–27. doi:10.4192/1577-8517-v18_1.

[32]. Setiono, Aris, and M. Irsan Nasution. 2025. "Smart Audit Contracts." *2nd International Conference on Islamic Community Studies (ICICS)*.