Magna Scientia Advanced Research and Reviews

eISSN: 2582-9394

Cross Ref DOI: 10.30574/msarr

Journal homepage: https://magnascientiapub.com/journals/msarr/

(REVIEW ARTICLE)

Check for updates

Blockchain-integrated accounting information systems in critical financial infrastructure: A comprehensive review of cybersecurity frameworks and internal control innovation

Ifeyinwa Perpetual Nwinyi [1,*], Christian Kofi Amoakoh [2] and Matthew Oman-Amoako [3]

[1] *University of Delaware, USA.*
[2] *Deloitte and Touche Llp, | Houston, TX, USA.*
[3] *Department of Business Administration, Accra Institute of Technology, Ghana.*

Magna Scientia Advanced Research and Reviews, 2026, 17(01), 221-231

Publication history: Received on 14 April 2026; revised on 25 May 2026; accepted on 27 May 2026

Article DOI: https://doi.org/10.30574/msarr.2026.17.1.0092

Abstract

This review is a synthesis of the published empirical and conceptual literature on integrating blockchain technology into the accounting information systems of critical financial infrastructure between 2020 and 2025. It looks at the interaction between distributed ledger architectures and existing cybersecurity frameworks, such as the National Institute of Standards and Technology Cybersecurity Framework, International Organization for Standardization / International Electrotechnical Commission (ISO/IEC 27001), the Control Objectives for Information and Related Technologies framework (COBIT), and Zero Trust principles, and how blockchain can links be used to achieve internal control innovation with smart contracts, continuous auditing, and automated assuranceThis research study has discovered that there is indeed a consistency of high data accuracy, and efficiency in sharing information and high reliability of audit trails in cases where blockchain is suitably incorporated. Nevertheless, operationalization of governance, legacy system interoperability, privacy-preserving assurance, and large-scale empirical validation of the work seem to be areas of persistent gaps in the literature, as well. To solve these problems, the paper comes up with an integrative assurance framework, which combines blockchain technical elements with cybersecurity controls, internal control goals, and audit evidence specifications. The review has added value in explaining the pathways of transformation of controls from manual to self-enforcing systems and also providing implication to financial institution, regulator and the auditing practice. It ends with setting a priority direction on longitudinal research matters, multi-stakeholder experimentation of governance, and standardization activities that were essential to enable dependable, auditable accounting systems in blockchains.

Keywords: Blockchain; Accounting Information System; Cybersecurity Frameworks; Internal Controls; Smart Contracts; Audit Assurance

1. Introduction

The digital transformation in the last few years has been a fast-paced process among financial institutions, payment networks, and accounting processes due to the growth of cloud services, real-time data integration, and experimentation with distributed ledger technologies (Gietzmann and Grossetti, 2021). According to existing literature, there is an increasing interest in cloud-based blockchain accounting services and an integrated Internet of Things (IoT) blockchain reporting architecture with its focus on automation, transparency, and the potential of continuous reporting (Nofel et al., 2024; Brakye and Yeboah, 2026). These changes are altering the way in which accounting data is created, distributed, and provided with assurance and are also changing the scope of responsibility between system designers, users, and auditors (Pflueger et al., 2024). This change is supported by empirical data, with controlled experiments

* Corresponding author: Ifeyinwa Perpetual Nwinyi

showing quantifiable benefits in performance and quality of data collection when enterprise accounting information sharing is achieved using blockchain-based smart contract systems, such as an increase in efficiency and accuracy in reporting compared to conventional systems (Jiang, 2024).

Along with such technological advancements, the traditional accounting information systems and internal control architectures remain under consistent vulnerabilities, with most of them being compounded by the digital transformation (Fullana and Ruiz, 2021). Audit and information systems studies also highlight current concerns about data reliability, security of cloud-based accounting records, and poor performance of current audit strategies when accounting information moves to infrastructures with decentralization or hybridization (Oyeyemi et al., 2025). Blockchain-designed systems are meant to address these drawbacks with documentation that cannot be tampered with and automated verification systems, but as past reviews have noted, operations and governance risks have not been eliminated, and this comes with privacy trade-offs, scale limitations, and regulatory uncertainty that make them unacceptable in the mainstream (Nartey et al., 2026; Lombardi et al., 2022).

Simultaneously, blockchain integration in financial systems has evolved in terms of proofs of concept, pilot applications, and experimental blockchain deployments within corporate accounting information sharing, cloud-based recognition processes, and auditor-centered blockchain-as-a-service platforms (Dashkevich et al., 2020). Recent contributions describe integrated systems that combine IoT technologies, blockchain ledgers, and structured reporting taxonomies to enable automated journal entry generation and standardized financial outputs, signaling a broader movement toward instrumented, ledger-backed reporting pipelines (Brakye and Yeboah, 2026). Simultaneously, the literature review on auditing cloud-based blockchain accounting settings describes the development of novel assurance models, and blockchain-cloud hybrid architectures, such as BCPaaS and BCIaaS, present new challenges to auditors of verifying cryptographic evidence, assessing cloud control environments, and bridging disordered records with known assurance models (Appelbaum and Nehmer, 2020).

Despite the structural benefits that blockchain and associated technologies could provide in relation to data integrity and providing continuous assurance, there exist severe cybersecurity threats and internal control vulnerabilities in both traditional accounting systems and newly developed blockchain-based designs. Among the risks are insecure cloud setups, unaddressed governance, and interoperability vulnerabilities that can add new attack surfaces or vulnerabilities related to operational aspects (Nartey et al., 2026; Fullana and Ruiz, 2021; Lin and Padliansyah, 2025). The responses to these challenges by regulators and setting standards have been patchy, and organizations and auditors lack widely available cybersecurity and internal control models that are more specifically designed to operate within blockchain-integrated accounting information systems within the critical financial infrastructure (Vincent and Barkhi, 2021; Lombardi et al., 2022). The review is based on the integration of empirical and conceptual articles published between 2020 and 2025 to investigate cybersecurity vulnerabilities and internal control innovation in accounting information systems with blocks and traditional accounting information systems.

The research analyzes the impact of the fundamental blockchain properties, such as immutability, level of consensus, and decentralization, on the accounting, control, and assurance needs and replenishes the deficiencies in the current cybersecurity frameworks and knowledge areas (Kazan and Kocamis, 2023). The value of this review is that it summarizes cross-disciplinary evidence on vulnerabilities to the system and adoption outcomes, critically analyzes assurance implications that exist for auditors and internal control designers, and develops an integrative research and practice agenda concerned with secure, auditable, and scalable blockchain-based accounting information system architecture (Lombardi et al., 2022; Pflueger et al., 2024).

2. Conceptual Foundations: Accounting Information Systems and Blockchain in Critical Financial Infrastructure

Transaction capture, reconciliation, reporting, and control involving banks, clearinghouses, and payment networks are supported by accounting information systems (AIS). Another convergence area in AIS throughout the blockchain age is a process where transactions, control policies, and assurance processes are aligned (Fullana and Ruiz, 2021). Rather than functioning as isolated processing platforms, contemporary AIS are reconceptualized as integrated socio-technical ecosystems that combine IoT-enabled data capture, distributed ledgers for tamper-evident storage, and standardized reporting formats to enable automated disclosure and real-time journal posting across the transaction lifecycle (Nofel et al., 2024; Inghirami, 2020).

In terms of control and assurance, AIS in a critical financial infrastructure should meet layered requirements, such as detection of unauthorized data modification, non-repudiation of transactions, settlement records completeness and timeliness, and verifiability of internal and external audits (Appelbaum and Nehmer, 2020). Yet the traditional

transactional cycles have structural vulnerabilities that include falsification of order, timing effects, and unregistered transactions, and a lack of reconciliation that deters the integrity of operations and reliability of financial reporting (Fullana and Ruiz, 2021). These weaknesses are enhanced because accounting information is moving over to decentralised and hybrid systems.

Blockchain technologies are associated with such architectural characteristics as immutable append-only ledgers, distributed replication, and consensus mechanisms that create canonical transaction histories that directly serve core accounting needs of provenance, integrity, and auditability (Fullana and Ruiz, 2021). The responsibilities of control are also reallocated in the accounting and assurance fields due to immutability and cryptographic block linking, creating tamper-evident records, decentralization transfers trust to centralized intermediaries to protocol-based validation, and the essence of redistribution of roles in the accounting and assurance systems (Appelbaum and Nehmer, 2020; Fullana and Ruiz, 2021). The design options of consensus: proof-of-work, proof-of-stake, or permissioned impact the performance, energy usage, governance systems, and appropriateness to high-throughput settlement systems (Fullana and Ruiz, 2021). In the financial sector, blockchain-based applications encompass the inter-enterprise sharing of accounting information, recognition workflow in the cloud, and hybrid blockchain-cloud audit services (Jiang, 2024). Empirically, it has been shown that data accuracy, the efficiency of information sharing, and the trustworthiness of reporting have become measurably better when validation is automated and the business rules are applied to the boundaries of transactions with the help of smart contracts (Jiang, 2024; Siregar and Hisyam, 2025).

Theoretically, an AIS based on blockchain can be aligned with immutable transaction records, as well as straightforward accounting statements of existence, completeness, and traceability. However, this is conditional upon the sound development of smart contracts and oracle integration to make sure that off-ledger economic events are properly recorded on-chain (Lin and Padliansyah, 2025; Nofel et al., 2024). Blockchain architectures would be able to improve financial statement claims by keeping cryptographic evidence and enabling machine-verifiable transaction history that reduces the amount of work performed in reconciliation (Appelbaum and Nehmer, 2020). Simultaneously, the implementation of blockchain puts additional assurance and regulation requirements. Internal control designers and auditors need to address node governance designs, smart contract integrity, consensus finality, and cybersecurity posture of cloud-based service providers to blockchain infrastructures (Appelbaum and Nehmer, 2020; Wu et al., 2025).

Even though a distributed verification mechanism has a chance of enhancing auditability (Nofel et al., 2024), the integration challenges can be addressed by, but are not limited to, IoT data verification, interoperability of legacy systems, scalability, and adoption by users (Lin and Padliansyah, 2025; Inghirami, 2020). Studies on internal auditing and continuous assurance indicate that the immutability provided by blockchains and in-built smart contract logic can lessen the workload on routine audits and that constant monitoring can be provided by ensuring that the control logic is embedded in transaction execution (Wu et al., 2025). Nonetheless, risk is not removed by the adoption of blockchain. The new control responsibilities crop up in the fields of node security, oracle reliability, cryptographic key management, and smart contract governance and need to be carefully designed to avoid risk displacement instead of risk mitigation (Fullana and Ruiz, 2021; Siregar and Hisyam, 2025). Combined, AIS in critical financial infrastructure needs to be perceived as socio-technical systems where control design, governance processes, consensus, oracle organization, and assurance practices are developed in conjunction with distributed ledger architectures (Fullana and Ruiz, 2021; Lin and Padliansyah, 2025). The technical affordances of blockchain are similar to objectives of accounting integrity and continuous assurance, though they will be translated into effective internal control and cybersecurity regimes only with the active design of governance, the reliance of cryptography, scalability of the system architecture, and the ability of auditors and control designers to upgrade to the cryptographic evidence models (Appelbaum and Nehmer, 2020; Wu et al., 2025).

3. Cybersecurity Frameworks and Blockchain-Specific Security Models in Blockchain-Integrated Accounting Information Systems

3.1. Conventional Frameworks and Their Adaptation to Decentralized Architectures

The deployment of blockchain technology into accounting information systems needs to be adjusted to current cybersecurity frameworks to maintain the primary control goals, while allowing the decentralized architecture of the system design. Instead of introducing completely new frameworks, researchers always suggest the adjustment of common governance and risk management standards to blockchain situations since they offer familiar control frameworks that can facilitate auditability and regulatory legitimacy (Kazan and Kocamis, 2023). The research studies on blockchain-based accounting systems present cybersecurity controls on the existing assurance paradigms, thus supporting professional practice continuity (Appelbaum and Nehmer, 2020; Nofel et al., 2024; Wu et al., 2025). NIST Cybersecurity Framework is commonly utilized as a structuring taxonomy in blockchain-based accounting systems. Its

operations, including identifying, protecting, detecting, responding, and recovering, are implemented as risk management lifecycle models to manage risk in cloud and hybrid blockchain settings (Appelbaum and Nehmer, 2020; Nofel et al., 2024). Instead of redefining the goals Cybersecurity researchers reinterpret the NIST categories to cover the realities of distributed ledger to expand response and recovery to cover chain-level forensics, governance-based rollback, and consensus-layer containment infrastructure (Appelbaum and Nehmer, 2020; Nofel et al., 2024). The ISO/IEC 27001 is positioned as a governance overlay on blockchain implementations in particular, when cloud-hosted services and third-party providers are taken into consideration. Its systematic risk evaluation and the ongoing process of improvement aid major administration, access control, and service provider oversight (Fullana and Ruiz, 2021). Nonetheless, extensions are suggested to deal with consensus operation, oracle validation policy, and secure lifecycles of smart contract development (Lin and Padliansyah, 2025; Wu et al., 2025).

On the same note, COBIT can still be at the center of aligning blockchain initiatives to enterprise IT governance and audit requirements. It is used to formalize consortium governance structures, including node admission, onboarding/offboarding processes, operator responsibilities, and service-level obligations in permissioned environments (Appelbaum and Nehmer, 2020; Fullana and Ruiz, 2021; Nofel et al., 2024). These frameworks are further complemented by zero trust principles since they enable the operationalization of explicit verification, least-privilege access, cryptographic identity, keys on hardware, and the policies of transaction-level endorsement in the distributed environment (Wu et al., 2025). Empirical studies indicate that blockchain-based AIS are still being tested by auditors according to traditional IT control lenses, accuracy of input, access control, integrity of the interface, and reliability of off-chain data (Lin and Padliansyah, 2025; Fullana and Ruiz, 2021). Nonetheless, direct one-to-one mapping of traditional controls to blockchain systems is not enough. Shared control environments, distributed key custody, consensus-based trust models, and cross-organizational governance challenge centralized assumptions embedded in traditional frameworks (Lin and Padliansyah, 2025; Wu et al., 2025).

Adaptation, in its turn, requires the redefining of the control objectives, making some of the controls to be transferred to protocol design and consortium governance systems, whereas the responsibility of off-chain artifacts is explicit (Lin and Padliansyah, 2025; Wu et al., 2025). The Standard information security models are generally under-specialized regarding distributed custody, threshold signatures, key rotation, cryptographic survivability, and identity governance schemes needed in long-term accounting records (Daoud and Serag, 2022; Caldarelli, 2025; Inghirami, 2020). Subsequently, the key to successful cybersecurity in blockchain-integrated AIS is not in substituting the existing standards but rather in re-engineering their implementation to capture distributed trust, shared control ownership, and protocol-level governance.

3.2. Blockchain-Specific Security Risks, Governance Problems, and Convergence Gaps

The accounting systems with blockchain integration fundamentally change the trust models by substituting the centralized control with the protocol-based consensus and cryptographic validation (Appelbaum and Nehmer, 2020). Even though the bounds of algorithmic trust are put in place with the assistance of smart contracts and consensus algorithms, oracles and off-chain interfaces continue to depend on human and organizational control, which forms a tenacious vulnerability of assurance (Albizri and Appelbaum, 2021; Nofel et al., 2024).

Consensus design brings in different risk profiles. Permissionless systems have threats of majority control and strategic manipulation, and scalable variants have alternative fault assumptions and exposure to bribery (Siregar and Hisyam, 2025). These risks have a direct impact on ledger finality in cases where accounting events are based on confirmed transactions (Appelbaum and Nehmer, 2020). Oracles, wallets, and enterprise integrations introduce additional attack surfaces; interface compromise can undermine accounting integrity even when ledger immutability remains intact (Sheldon, 2021). The presence of smart contract defects increases this exposure, and formal verification, rigorous development practices, and other mechanisms by governance are required to correct it (Lin and Padliansyah, 2025; Wu et al., 2025). Off-chain storage dependencies also confirm that immutability by itself is not conclusive, as it fails to fix vulnerabilities in assurance unless there is cryptographic verification, reconciliation controls, and explicit validation in the audit layer (Francati et al., 2021; Banaeian Far et al., 2024; Sarwar et al., 2021; Sheldon, 2021).

Cryptography key control and node security become common control points of critical concern. Weak key custody can negate on-chain protections, and permissioned environments shift risk toward insider governance and membership management vulnerabilities (Fraga et al., 2024). The studies are oriented to the hardware-based key storage, key signature, and identity control, and role-based authorizations as the core accounting safeguards (Lin and Padliansyah, 2025). Cryptographic agility is also pertinent in long-term financial records as it is needed to maintain verifiability in changing algorithms (Siregar and Hisyam, 2025). In the absence of a combination of cryptographic protection and governance and assurance controls, blockchain implementation is likely to increase instead of reducing cybersecurity

risks (Caldarelli, 2020; Fullana and Ruiz, 2021; Freiman, 2025). The other challenges are governance and change control. The immutable records and autonomous smart contracts need systematic upgrade mechanisms such as multi-signature control as well as emergency mechanisms, which are not well defined in the baseline standards. Identity based on blockchain keys cannot be used with centralized revocation models, and distributed custody (including threshold signatures and multi-party computation) is not a well-researched concept in more traditional designs (Lin and Padliansyah, 2025; Nofel et al., 2024). On-chain transparency enhances auditability, but opaque off-chain inputs and privacy-preserving designs complicate evidence collection without robust oracle governance (Wu et al., 2025). The issue of cross-jurisdiction node distribution also makes it difficult to comply with regulations, audit authorities, and forensic investigations.

In the literature, there is a point of convergence in terms of basing blockchain governance on existing risk management frameworks, including ISO, COBIT, and NIST (Appelbaum and Nehmer, 2020; Fullana and Ruiz, 2021). Immutable ledgers are consistent with the evidentiary integrity criteria, yet input controls, oracle dependability, and user controls need to be explicitly defined (Wu et al., 2025). However, all major gaps remain in the missing key custody frameworks, unmeasured consensus-level guarantees, undeveloped smart contract lifecycle management, and undefined liability of autonomous accounting logic (Appelbaum and Nehmer, 2020; Lin and Padliansyah, 2025; Siregar and Hisyam, 2025; Wu et al., 2025). Recent research suggests hybrid control architectures of both legacy standards and protocol-level controls (e.g., threshold signature, multisource oracle architecture, consortium agreement, service level commitments) (Lin and Padliansyah, 2025). Zero Trust integrations also incorporate identity and node management protection (Nofel et al., 2024). Nevertheless, empirical validation is not complete, and longitudinal studies are needed to measure control effectiveness and come up with blockchain-oriented extensions of existing cybersecurity guidelines (Wu et al., 2025). Decentralization reinforces auditability, but governance, key management, consensus assurance, and oracle controls have to be carefully designed in order to maintain accountability instead of diffusing it (Appelbaum and Nehmer, 2020; Lin and Padliansyah, 2025; Nofel et al., 2024; Wu et al., 2025).

4. Internal Control Innovation and Automation in Blockchain-Integrated Accounting Systems

4.1. Structural Limitations of Traditional Internal Control and the Emergence of Automated Control Logic

Blockchain-enabled change reveals weaknesses of the traditional system of internal control, especially when it is used to distribute high-frequency digital transactions. The conceptual validity of the principles of COSO is still intact, but literature frequently reports an inconsistency between centralized and periodic control models when contrasted with a decentralized and non-modifiable ledger environment (Fullana and Ruiz, 2021; Nofel et al., 2024). When evidence is continuously being created and settled by the exchange of cryptographically verified transactions that are replicated between nodes, such a reliance on centralized documentation (which involves human approval) and audit processes is strained (Fullana and Ruiz, 2021; Nofel et al., 2024).

Some of the weaknesses in the legacy transactional cycles documented are manipulation of the order, transactions not documented, changes in the timing of the entries, late deliveries, and unresolved gaps in the reconciliation, even with the formal control procedures in place. The 100-firm randomized field study reports that the accuracy of data and the effectiveness of information sharing have increased by 19.8 percent and 25.7 percent, respectively, with the adoption of smart contract mechanisms, which suggests that decision-makers allowed material inefficiencies and delays in the previous controls (Jiang, 2024). These results are consistent with internal-control design studies in the sales and purchasing cycles, showing that they are structured as they improve validation logic at transaction boundaries (Lin and Padliansyah, 2025).

Integrated IoT-blockchain accounting architectures also indicate the technical capability of automation and pinpoint integration complexity, data validation issues, and scalability challenges that undermine manual reconciliation models (Nofel et al., 2024). Audit studies also indicate that distributed and cloud-hosted books shift the focus of assurance work from walkthrough-based examination to cryptographic control analysis, platform administration examination, and system composition examination (Fullana and Ruiz, 2021). Taken together, the literature finds that control paradigms based on human supervision and periodic inspection offer insufficient coverage of the code-mediated environments and generate sustained gaps in detection, but also open up possibilities of architectural control redefinition (Nofel et al., 2024; Vincent and Barkhi, 2021).

Smart contracts are the fundamental tool that enabled this redesign. They shift the control operations of a manual and detective nature into preventive and automated logic within executable ledger code (Fullana and Ruiz, 2021). By encoding authorization rules, validation conditions, and state transitions within deterministic protocols, smart contracts reduce reliance on post hoc reconciliation while producing tamper-evident audit trails (Nofel et al., 2024;

Fullana and Ruiz, 2021). Smart contracts are used in sales and purchasing scenarios to fully or partially replace manual checkpoints with self-executable points of regulation through validation over authorized nodes, including order validation, payment authorization, goods receipt validation, and three-way matching (Lin and Padliansyah, 2025). This transformation logic is supported with the help of empirical evidence. The results of controlled experimentation claim a 25.7 percentage point enhancement in the efficiency of information sharing, a 19.8 percentage point rise in data accuracy, and a 13.6 percentage point decrease in the cost of information sharing, as well as a quantifiable decrease in the reconciliation effort (Jiang, 2024). These advantages are, however, conditional. There are limitations to effectiveness due to integration complexity, risks in sensor-to-ledger validation, and barriers to user adoption (Nofel et al., 2024). In addition, smart contracts pose new reliance on oracle dependability, code correctness, and administration supervision; thus, control risk is moved rather than removed, unless it is handled expressly (Lin and Padliansyah, 2025).

4.2. Continuous Assurance, Privacy Tensions, and the Logic of Control Transformation

The blockchain architectures enable the transition from periodic, sample-based assurance to continuous or near continuous assurance based on immutable and time-stamped records of transactions (Appelbaum and Nehmer, 2020; Nofel et al., 2024). Since ledger entries are append-only, and programmatic controls are directly embedded within transaction flows, organizations will not need so much reliance on end of period reconciliations and will have to rely on continual monitoring of activities and control results. Audit routines using smart contracts can automatically extract evidence, conduct analytic processes, and generate audit trails on chain, minimizing manual sampling and enhancing independent verification (Nofel et al., 2024; Wu et al., 2025). Sophisticated alerts to anomalies, like duplicated invoices or policy breaches, can also be generated by smart contracts so that auditors and internal surveillance teams become able to respond almost in real-time (Wu et al., 2025). An increased level of transparency presents significant privacy tradeoffs as well. Due to the distributed ledger, sensitive financial data can be exposed outside the context of an organization because the data is replicated in nodes involved in the process, which leads to a threat to confidentiality and regulatory issues. Some level of exposure can be mitigated by permissioned ledgers, role-based access controls, or data minimization strategies, but these strategies do not ensure that the differences in visibility of the network participants are completely removed (Jiang, 2024; Lin and Padliansyah, 2025; Nofel et al., 2024). Despite the reports of the benefits in efficiency and accuracy of data, similar evidence of the long-term protection of privacy across jurisdictions has not been found. Some of the solutions suggested are selective disclosure mechanisms, off-chain storage with on-chain integrity proofs, transaction obfuscation, and sophisticated cryptographic tools such as zero-knowledge proofs. The methods are intended to help strike the right balance between auditability and confidentiality, and empirical confirmation in the accounting situation remains limited. Consequently, the issue of balancing transparency and privacy has been a technical, governance, and policy problem and not a completely solved solution (Fullana and Ruiz, 2021; Lin and Padliansyah, 2025; Nofel et al., 2024).

5. Integrated Governance, Risk, Compliance, and Assurance Framework

Across the literature, governance emerges as the principal convergence point connecting cybersecurity, internal control, compliance, and auditability. Throughout the literature, governance appears to be the fundamental control centre between cybersecurity, inside control, compliance, and auditability. The reason why consortium and permissioned architectures are always preferred is that they formalize the node admission, consensus mechanisms, and upgrade processes in a manner that enables accountability and regulatory compliance (Lin and Padliansyah, 2025; Nwinyi et al., 2026). The empirical relationships between clear governance and access control structures and an enhanced degree of data trustworthiness and information-sharing performance have been identified (Jiang, 2024; Nofel et al., 2024). Enterprise risk management frameworks should thus be able to start factoring blockchain-specific risks instead of treating them as technical anomalies. The risks related to flaws in smart contracts, oracle stability, and scalability constraints must be formally documented in the risk registers, and specific mitigation measures include the use of code inspection, multi-signing governance mechanisms, and hybrid controls over reconciliation (Lin and Padliansyah, 2025; Fullana and Ruiz, 2021). In its turn, auditors have to increase the traditional access and change-control testing with the evaluation of the consensus integrity and the provenance of blockchain-generated evidence (Appelbaum and Nehmer, 2020; Wu et al., 2025). Considerations of compliance are not that mature. Even though smart contracts and permissioned controls can be used to automate contractual or regulatory requirements, the existing regulatory frameworks were designed with centralized assumptions. The immutability, cross-jurisdictional data access, and automated execution will have to be dealt with through legal and policy adjustments (Fullana and Ruiz, 2021; Nofel et al., 2024). Although there is improvement in efficiency and accuracy, which point to indirect benefits in compliance (Jiang, 2024), standardized models of automated regulatory compliance are still under development. The level of auditability is relatively higher. The research on cloud-based blockchain accounting describes why ledger integrity should be evaluated along with the controls of service providers (Appelbaum and Nehmer, 2020). The ongoing auditing studies reveal that the near-real-time assurance cannot be completed without oracle assurance and third-party

attestations (Wu et al., 2025; Fullana and Ruiz, 2021). There should be a holistic assurance method, hence, involving the combination of on-chain evidence and external validation mechanisms. The proposed integrated assurance framework in the literature includes distributed ledgers, smart contracts, oracles, nodes, and interfaces as control-enabling structures, the reliability of which should be validated with the help of the coordinated approach to cybersecurity and internal control examination (Lin and Padliansyah, 2025). The trusted blockchain-based accounting requires the cryptographic key management, secure oracle provisioning, and consensus resilience, which are directly associated with the financial reporting objectives, including authorization, accuracy, completeness, and timeliness (Appelbaum and Nehmer, 2020; Fullana and Ruiz, 2021). Analysis of empirical data shows that in case such mappings are successfully introduced, the data accuracy and reporting efficiency improve measurably (Jiang, 2024; Nofel et al., 2024). However, the ledger cannot be trusted to provide assurance. External and systemic risks also need to be addressed with code audits, governance documentation, and attestations by the service-providers (Appelbaum and Nehmer, 2020; Wu et al., 2025). Significant gaps persist, including the absence of standardized tools to convert ledger activity into control-testable evidence and the lack of empirically validated mappings between major cybersecurity frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, and COBIT and blockchain-specific control implementations (Fullana and Ruiz, 2021; Jiang, 2024).

6. Implications

6.1. Implications on Financial Institutions and Accounting-Auditing Practice.

To financial institutions, accounting architectures based on blockchain introduce an operational opportunity and complexity of implementation. These benefits indicate that blockchain can be used as an infrastructure enabler to support real-time reconciliation and automated settlement and better provenance of transactions, especially with Internet of Things data capture and standardized reporting outputs. Nevertheless, the literature is always reminded that scalability, interoperability, and data validation in heterogeneous systems are still binding requirements, and implementation should take a gradual approach by adopting permissioned or hybrid ledger systems instead of replacing the entire system (Wu et al., 2025; Fullana and Ruiz, 2021). The success of implementation is determined by organizational change as well as the choice of technology. Research underlines that ledger mechanics cannot be the main reason behind integration problems often, and those problems can be associated with fragmented data schema, weak oracle design, and poor user adoption (Nofel et al., 2024).

There is evidence that the positive effects are achieved only in the case when users follow standardized processes, shared governance schemes, and specific training courses, which proves the significance of cross-functional practice, in terms of cross-functional activity coordination, within operations, compliance, treasury, and information technology functions (Jiang, 2024; Wu et al., 2025). Based on this, literature indicates that it is best to form dedicated distributed-ledger implementation teams, creating a clear sense of ownership of processes that will be supported by smart contracts, and connecting pilot outcomes with performance metrics like exception rates, time to reconcile, and the ability to reduce audit effort (Yeboah et al., 2026). Governance-based blockchain literature also suggests that the successful outcomes of internal control are associated with the alignment of distributed-ledger initiatives with enterprise-wide IT governance systems, such as role distribution based on the COBIT framework, DevOps organizational, and formal responsibility towards protocol upgrades and smart contract lifecycle management systems (Aisyah et al., 2025; Doekhi, 2023).

In the case of accounting and auditing practice, the adoption of blockchain requires reassessment of the assurance models, competency, and the evaluation of evidence. According to Appelbaum and Nehmer (2020), auditors should cease using sample-based and point-in-time testing and adopt continuous or near-continuous assurance based on the immutable ledger records and machine-readable streams of transactions. Empirical test results that depicted enhanced data accuracy and reduced cost of reconciliation suggest that audit effort may be diverted to the control design, exception management, and system saliency evaluation (Jiang, 2024; Fullana and Ruiz, 2021). In the meantime, new audit issues related to smart-contract correctness, oracle reliability, cryptographic key management, or the use of cloud-hosted blockchain services are novel assurance challenges that require increased technical capacity and more dependence on third-party attestations (Appelbaum and Nehmer, 2020; Nofel et al., 2024). The literature also presents the implications for professional standards and education. As indicated by Wu et al. (2025) and Siregar and Hisyam (2025), the existing accounting and auditing standards do not offer much information about the adequacy of evidence, responsibility, and liability on consortium-managed or platform-hosted ledger environments. As a result, the standard-setters are invited to shed light on expectations in terms of smart-contract testing, continued monitoring, and the dependency on assurances by the service-providers. Simultaneously, audit education and continuing professional development should provide training on blockchain architecture, data analytics, and technology risk assessment to get

the practitioners to make informed judgments in automated control settings (Nofel et al., 2024; Nwinyi and Oman-Amoako, 2026).

6.2. Implications for Regulators and Policymakers

To regulators and policymakers, accounting systems linked to blockchain provide both control prospects and regulatory issues. The literature identifies the possibility of using supervisory technology applications to utilize permissioned ledger technology and standardized and machine-readable records to facilitate near real-time monitoring, automated anomaly detection, and enhanced systemic risk analysis (Wu et al., 2025). According to Nofel et al. (2024), standardized reporting output, eXtensible Business Reporting Language (XBRL), created directly based on ledger events, would be able to decrease reporting lag and increase the consistency of data across supervisory regimes, as long as access control and privacy are well-defined. There is also a regulatory technology scholarship that is aimed at blockchain-based supervisory sandboxes and parallel regulatory infrastructure in a bid to experiment with automated oversight, real-time compliance monitoring, and cross-border coordination of distributed financial systems (Daah et al., 2024). Simultaneously, the current regulatory frameworks do not fit distributed ledger architectures very well. The literature highlights that accounting, prudential, and supervisory regulations still presuppose centralized ledgers and periodic reports, where the responsibility of executing smart contracts remains unclear, and the responsibility of data location in the case of crossing jurisdictions and dependability standards for oracles and sensors has not been established yet (Nartey et al., 2026; Siregar and Hisyam, 2025). The models of enforcement should also consider the immutable records and evoke the questions of remediation, the admissibility of evidence, or the necessity of node-level access or periodic attestations of the consortium operators (Appelbaum and Nehmer, 2020). The coordination across borders has become a key issue of concern. In their study, Wu et al. (2025) and Siregar and Hisyam (2025) observe that transnational ledger networks escalate conflicts between data protection, anti-money-laundering, and banking supervision regimes, which has underscored the need to have interoperable technical and legal frameworks, supervision memoranda of understanding, and harmonized standards. The literature thus proposes regulatory sandboxes relating to permissioned ledger ecosystems, issuing minimal standards to test smart-contracts, key management, and oracle governance, and creation of cross-jurisdictional supervisory deals to make sure that innovation does not compromise market integrity and consumer protection.

6.3. Research Gaps and Future Directions

Although existing studies demonstrate the technical feasibility and localized benefits of blockchain-integrated accounting information systems, the literature remains constrained by limited scale, duration, and diversity of empirical evidence. The existing evidence is based on small qualitative interview studies, design-science artifacts as well as a limited number of controlled experiments which are not enough to draw strong causal conclusions and extrapolate the findings to other industries and jurisdictions. Longitudinal and cross-industry studies are strikingly missing, and it is unclear how the benefits persist, which have unintended effects, and cost and benefit trade-offs in the long-run. Governance-related gaps are equally pronounced, as multi-stakeholder accountability models involving firms, auditors, regulators, and platform providers remain largely conceptual, with limited empirical validation of liability allocation, oracle governance, smart-contract failure remediation, and evidentiary status of ledger records, particularly in cross-jurisdictional contexts. Technical challenges related to interoperability and scalability persist, including integration with legacy enterprise resource planning systems, throughput and latency constraints under accounting workloads, and the absence of harmonized standards for data exchange, audit trails, and machine-readable reporting. Unresolved human-technology tensions, such as lack of skills in accounting professionals, trust and adoption even in the face of quantifiable technical benefits, ethical issues presented by non-erasable records, automated decision making, and long-term retention of data are also brought to focus in the literature. The new areas of research suggested, yet not fully investigated, are privacy-sensitive assurance protocols, the combination of artificial intelligence and blockchain to support continuous auditing and detect anomalies, governance frameworks based on the example of decentralized autonomous organizations, and cryptographic futureproofing of enduring accounting entries. Future research should therefore prioritize large-scale and longitudinal field studies, controlled comparisons with non-blockchain systems, empirically tested governance pilots, standardized mappings between cybersecurity and accounting control frameworks, and cross-disciplinary collaboration to operationalize accountability, auditability, and resilience in blockchain-enabled accounting systems.

7. Conclusion

This review examined existing studies on the implementation of blockchain in accounting information systems by synthesizing governance considerations, technical limitations, empirical evidence, and relationships between technology and humans. Theoretically, the reviewed studies broaden accounting information systems and audit theory by positioning immutable ledgers, smart contracts, and algorithm-mediated controls in more established assurance and

control paradigms and by emphasizing the importance of multi-stakeholders and cross-jurisdictional governance models. In practice, there is an indication that benefits materialize when blockchain projects are well integrated into legacy systems, supported by a well-defined governing structure, and consistent with the existing reporting and assurance processes. In general, an AIS with the support of blockchain should be regarded not as a substitute, but as an augmentative innovation where automation is not a replacement, but rather a complement to professional judgment. It will be based on empirical research, technical standardization, and collaborative rulemaking between firms, auditors, regulators, and policymakers to make progress on reliable, auditable, and scalable implementations.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Aisyah, S. N., Mulyana, R., and Kusumasari, T. F. (2025). Ambidextrous Blockchain Governance to Strengthen BankCo's Digital Transformation through COBIT 2019 Traditional and DevOps. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control.

[2] Albizri, A., and Appelbaum, D. (2021). Trust but verify: The oracle paradox of blockchain smart contracts. Journal of Information Systems, 35(2), 1-16.

[3] Appelbaum, D., and Nehmer, R. A. (2020). Auditing cloud-based blockchain accounting systems. Journal of information systems, 34(2), 5-21.

[4] Banaeian Far, S., Rajabzadeh Asaar, M., and Haghbin, A. (2024). A generic framework for blockchain-assisted on-chain auditing for off-chain storage. International Journal of Information Security, 23(3), 2407-2435.

[5] Caldarelli, G. (2025). Integration of Blockchain in Accounting and ESG Reporting: A Systematic Review from an Oracle-Based Perspective. Journal of Risk and Financial Management, 18(9), 491.

[6] Daah, C., Qureshi, A., Awan, I., and Konur, S. (2024). Enhancing zero trust models in the financial industry through blockchain integration: A proposed framework. Electronics, 13(5), 865.

[7] Daoud, M. M., and Serag, A. A. (2022). A proposed framework for studying the impact of cybersecurity on accounting information to increase trust in the financial reports in the context of industry 4.0: An event, impact and response approach. 61-20 ,(1)42 ,التجارة والتمويل.

[8] Dashkevich, N., Counsell, S., and Destefanis, G. (2020). Blockchain application for central banks: A systematic mapping study. IEEE Access, 8, 139918-139952.

[9] Doekhi, R. J. (2023). The Intercompany Settlement Blockchain: Benefits, Risks, and Internal IT-Controls. Advanced Digital Auditing, 47.

[10] Fraga, C., Abelém, A., Borges, V., Pinheiro, B., and Cordeiro, W. (2024, May). A blockchain-based approach for continuous auditing in it change management. In NOMS 2024-2024 IEEE Network Operations and Management Symposium (pp. 1-4). IEEE.

[11] Francati, D., Ateniese, G., Faye, A., Milazzo, A. M., Perillo, A. M., Schiatti, L., and Giordano, G. (2021, May). Audita: A blockchain-based auditing framework for off-chain storage. In Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing (pp. 5-10).

[12] Freiman, J. W. (2025). BENEFITS OF BLOCKCHAIN AND SMART CONTRACT INTEGRATION IN INTERNAL CONTROL MONITORING AND DATA. Journal of Theoretical Accounting Research, 21(1).

[13] Fullana, O., and Ruiz, J. (2021). Accounting information systems in the blockchain era. International Journal of Intellectual Property Management, 11(1), 63-80.

[14] Gietzmann, M., and Grossetti, F. (2021). Blockchain and other distributed ledger technologies: where is the accounting?. Journal of Accounting and Public Policy, 40(5), 106881.

[15] Hussain, A. A., and Al-Turjman, F. (2021). Artificial intelligence and blockchain: A review. Transactions on emerging telecommunications technologies, 32(9), e4268.

[16] Inghirami, I. E. (2020). Accounting information systems: the scope of blockchain accounting. In Digital Business Transformation: Organizing, Managing and Controlling in the Information Age (pp. 107-120). Cham: Springer International Publishing.

[17] Jiang, L. (2024). The use of blockchain technology in enterprise financial accounting information sharing. Plos one, 19(2), e0298210.

[18] Kazan, G., and Kocamış, T. U. (2023). Assessing the impact of blockchain technology on internal controls within the COSO framework. Journal of Corporate Governance Insurance and Risk Management, 10(1), 1-15.

[19] Le, V. (2024). Integrating blockchain and machine learning for continuous auditing: challenges and strategies.

[20] Lin, Y. C., Padliansyah, R., and Wu, P. P. (2025). The Adoption of Blockchain Technology on Company's Internal Control System in Sales and Purchasing Cycle. Journal of Emerging Technologies in Accounting, 22(1), 65-83.

[21] Lombardi, R., de Villiers, C., Moscariello, N., and Pizzo, M. (2022). The disruption of blockchain in auditing–a systematic literature review and an agenda for future research. Accounting, Auditing and Accountability Journal, 35(7), 1534-1565.

[22] Mökander, J., Morley, J., Taddeo, M., and Floridi, L. (2021). Ethics-based auditing of automated decision-making systems: Nature, scope, and limitations. Science and Engineering Ethics, 27(4), 44.

[23] Nofel, M., Marzouk, M., Elbardan, H., Saleh, R., and Mogahed, A. (2024). From sensors to standardized financial reports: A proposed automated accounting system integrating IoT, Blockchain, and XBRL. Journal of Risk and Financial Management, 17(10), 445.

[24] Nwinyi, I. P., and Oman-Amoako, M. (2026). AI-driven business analytics frameworks for government financial management: Advancing accountability and transparency in U.S. federal programs. EPRA International Journal of Economics, Business and Management Studies. https://doi.org/10.36713/epra26112

[25]

[26] Oyeyemi, D. O., Okosieme, O. O., Idowu-Kunlere, O., Julius, E. A., and Nwinyi, I. P. (2025). Explainable AI for credit risk assessment: Integrating machine learning with business analytics. IOSR Journal of Economics and Finance, 16(5), 63–72. https://doi.org/10.9790/5933-1605016372

[27] Nwinyi, I. P., Amoakoh, C. K., Twum, P. G., and Yeboah, M. M. (2026). Small business financial compliance analytics: Reducing regulatory burden while maintaining oversight through data-driven solutions. International Journal for Multidisciplinary Research, 8(1).

[28] Nartey, O. L., Agyei, E., Anim, B., and Yeboah, M. M. (2026). AI and blockchain in forensic auditing: A review of tools for investigating financial crimes in the U.S. International Journal for Multidisciplinary Research, 8(1). https://doi.org/10.36948/ijfmr.2026.v08i01.63239

[29] Nartey, O. L., Aryeetey, S., Apaflo, D. A., and Yeboah, M. M. (2026). AI and blockchain in financial auditing: A systematic review of fraud detection techniques and their impact on investor confidence in U.S. market. EPRA International Journal of Research and Development (IJRD), 11(3). https://doi.org/10.36713/epra2016

[30] Brakye, K., and Yeboah, M. M. (2026). Technology-driven risk governance in U.S. financial reporting: The role of cybersecurity disclosure and regulatory technology in strengthening capital market transparency. Sarcouncil Journal of Engineering and Computer Sciences, 5(4). https://doi.org/10.5281/zenodo.19654718

[31]

[32] Pflueger, D., Kornberger, M., and Mouritsen, J. (2024). What is blockchain accounting? A critical examination in relation to organizing, governance, and trust. European Accounting Review, 33(4), 1139-1164.

[33] Samiolo, R., Spence, C., and Toh, D. (2024). Auditor judgment in the fourth industrial revolution. Contemporary accounting research, 41(1), 498-528.

[34] Sarwar, M. I., Iqbal, M. W., Alyas, T., Namoun, A., Alrehaili, A., Tufail, A., and Tabassum, N. (2021). Data vaults for blockchain-empowered accounting information systems. Ieee Access, 9, 117306-117324.

[35] Sheldon, M. D. (2021). Auditing the blockchain oracle problem. Journal of Information Systems, 35(1), 121-133.

[36] Siregar, Y., and Hisyam, M. (2025). The blockchain integration in cloud accounting for financial statement recognition. Jurnal Ilmiah Akuntansi Kesatuan, 13(4), 655-666.

[37] Stein Smith, S. (2024). Audit Implications of AI and Blockchain. In Blockchain, Artificial Intelligence, and Financial Services: Applications for Finance and Accounting Professionals, including the Cryptoasset Ecosystem (pp. 179-192). Cham: Springer Nature Switzerland.

[38] Tyma, B., Dhillon, R., Sivabalan, P., and Wieder, B. (2022). Understanding accountability in blockchain systems. Accounting, Auditing and Accountability Journal, 35(7), 1625-1655.

[39] Vincent, N. E., and Barkhi, R. (2021). Evaluating blockchain using COSO. Current Issues in Auditing, 15(1), A57-A71.

[40] Wang, S., Tu, X., Chai, H., Sun, Q., Wu, J., Cai, H., and Wang, F. Y. (2020). Blockchain-powered parallel fintech regulatory sandbox based on the ACP approach. IFAC-PapersOnLine, 53(5), 863-867.

[41] Wu, H. P., Liu, Z. H., Dong, H. Y., Lu, Y., and Xu, L. D. (2025). Revolutionizing internal auditing: harnessing the power of blockchain. Enterprise Information Systems, 19(1-2), 2448003.

[42] Yeboah, M. M., Agyei, E., Anim, B., Nwinyi, P., and Nartey, O. L. (2026): AI in financial auditing: Addressing U.S. audit failures and strengthening PCAOB/SEC compliance.