International Journal of Computer Applications Technology and Research
Volume 15–Issue 03, 83 – 103, 2026, ISSN: -2319–8656
DOI:10.7753/IJCATR1503.1014

AI-Driven Accounting Oversight Systems: Integrating Machine Learning and Blockchain for Real-Time Fraud Detection and Financial Reconciliation

Deborah Osahor[1], Juliet Nankunda[2], Douglas Niyonsingiza[2], Ebun Martins[3]

[1]Georgia Southern University
[2]Maharishi International University, Fairfield, Iowa
[3]Mendoza College of Business, University of Notre Dame

Abstract

The integration of Machine Learning (ML) and blockchain technology into accounting oversight systems represents a transformative shift in addressing the limitations of traditional financial governance models, which rely on static ledgers, manual reconciliation, and retrospective audits. This study evaluates the synergistic potential of predictive risk analytics (PRA), dynamic internal control mechanisms (DICM), and decentralized ledger technologies to enhance fraud detection, financial reconciliation, and regulatory compliance in high-risk economic sectors. Drawing on empirical data from public-sector financial records and private-sector supply chains, we demonstrate that a hybrid ML-blockchain system achieves a 9.8% improvement in fraud detection accuracy (F1-score) and a 60% reduction in reconciliation time, while maintaining 99.8% transaction accuracy. The findings validate theoretical frameworks such as triple-entry accounting (Grigg, 2024) and X-Accounting (Faccia et al., 2020), but also reveal critical challenges, including scalability limitations, data privacy trade-offs, and the need for cross-jurisdictional regulatory standards. Stakeholder validation confirms the system's operational feasibility (95% approval) and regulatory compliance (100% alignment with GAAP/IFRS), though ethical governance (85% approval) and model transparency (90% approval) require further refinement. This study contributes a conceptual architecture for next-generation accounting automation, bridging the gap between traditional compliance models and the demands of modern financial infrastructure, where real-time validation, automation, and transparency are essential.

Keywords: Machine Learning in Accounting, Blockchain-Based Reconciliation, Fraud Detection Algorithms, Triple-Entry Accounting, Regulatory Compliance Automation, Hybrid ML-Blockchain Systems, Real-Time Financial Oversight

1. Introduction

The rapid evolution of digital accounting systems has exposed critical limitations in traditional financial governance models, which rely on static ledgers, periodic audits, and manual reconciliation processes. As financial ecosystems grow increasingly complex the need for real-time oversight, predictive analytics, and

decentralized verification has become paramount. Traditional accounting frameworks, rooted in double-entry bookkeeping and retrospective audits, are ill-equipped to address the dynamic, data-intensive demands of modern finance (Coyne & McMickle, 2017; Dai & Vasarhelyi, 2017). Errors in tax filings, payroll processing, or financial reporting can result in severe penalties, reputational damage, and eroded investor confidence, particularly as regulatory landscapes grow more stringent and stakeholder expectations for transparency and accountability intensify (Faccia et al., 2020; Kanaparthi, 2024).

The urgency of modernizing fraud detection is further underscored by advancements in healthcare financial security, where deep learning models have demonstrated superior accuracy in identifying fraudulent claims and billing practices (Makandah & Nagalila, 2023). However, while such systems excel in proactive prevention within healthcare, their adaptability to financial sectors remains limited without the decentralized verification afforded by blockchain (Mukasa et al., 2025). This gap highlights the need for hybrid frameworks that combine predictive analytics with immutable ledgers, as explored in this study.

The integration of Machine Learning (ML) and blockchain technology presents a paradigm shift in accounting oversight, offering real-time fraud detection, automated reconciliation, and continuous assurance (Casino et al., 2019; Grigg, 2024). ML algorithms, particularly deep learning and graph-based models, excel at detecting anomalies, patterns, and collusive behaviors in vast, high-dimensional datasets (Hernandez Aros et al., 2024; Wang et al., 2024). Concurrently, blockchain's decentralized, immutable ledgers provide a robust foundation for financial reconciliation, auditability, and trust, eliminating the need for manual sampling and reducing reconciliation windows from hours to minutes (Faccia et al., 2020; Mahdani et al., 2024). The synergy between these technologies enables triple-entry accounting, where transactions are cryptographically verified and shared across a distributed network, fundamentally enhancing the integrity and transparency of financial records (Grigg, 2024; Sekinobe et al., 2025).

Recent empirical studies and theoretical frameworks underscore the transformative potential of this integration. Casino et al. (2019) argued that blockchain's consensus-driven validation can be enhanced by ML's predictive analytics, creating a self-auditing financial ecosystem that reduces fraud risks and operational inefficiencies. Their work is supported by Faccia et al. (2020), who introduced the X-Accounting framework, demonstrating how smart contracts and distributed ledgers can automate reconciliation processes and provide continuous assurance. Empirical evidence from PwC's blockchain-based audit systems further validates these claims, showing a 90% reduction in reconciliation time through real-time data sharing and immutable audit trails (Frontiers in Blockchain, 2025). Similarly, Kanaparthi (2024) found that ML-blockchain hybrid systems optimize efficiency, reduce accounting expenses, and expedite auditing processes, aligning with the economic viability projections of Dai and Vasarhelyi (2017).

Despite these advancements, the operationalization of ML and blockchain in accounting remains fragmented. While individual applications such as anomaly detection in fraud prevention or smart contracts for automated compliance have been explored, there is a lack of cohesive frameworks for their integration into end-to-end oversight systems (Sekinobe et al., 2025; Oladejo et al., 2024). Current compliance models, designed for static, on-premises environments, struggle to accommodate the dynamic, data-intensive nature of modern financial operations, where infrastructure is defined by code and execution contexts evolve in real time (Mukasa, 2023). Furthermore, the adoption of these technologies is hindered by persistent challenges, including data privacy concerns, interoperability gaps, and the absence of standardized

governance models that align regulatory requirements with automated, cloud-native workflows (Nyombi et al., 2025; Sharma et al., 2024).

Regulatory mandates, such as those issued by the Public Company Accounting Oversight Board (PCAOB) and the Securities and Exchange Commission (SEC), now explicitly require technology-assisted analysis and continuous assurance, signaling a shift from periodic audits to real-time validation (PCAOB, 2024). However, translating these requirements into enforceable, scalable processes remains an open challenge. While standards like the AICPA's System of Quality Management (SQMS) and the EU's General Data Protection Regulation (GDPR) provide high-level guidelines, they lack native mechanisms for embedding compliance into the operational fabric of AI-driven, blockchain-enabled systems (Oladejo et al., 2024; EU Data Protection Working Party, 2018). This gap is particularly acute in high-stakes sectors such as finance and public accounting, where the need for continuous monitoring, demonstrable control enforcement, and real-time evidence generation is paramount (Becker, 2025; Surgent CPE, 2025).

This study addresses these limitations by synthesizing the latest research on ML and blockchain integration in accounting, with a focus on fraud detection and financial reconciliation. Through a critical review of academic literature, industry case studies, and regulatory developments, the paper evaluates how these technologies can be structurally combined to create adaptive, transparent, and auditable oversight systems. The objective is to propose a conceptual architecture that bridges the divide between traditional compliance models and the demands of modern financial infrastructure where automation, scalability, and real-time validation are not just desirable but essential. By doing so, this work aims to provide practitioners, policymakers, and researchers with a roadmap for designing accounting systems that are both technologically advanced and regulatorily robust, ultimately fostering greater trust, efficiency, and resilience in financial governance.

2. Literature Review

The integration of Machine Learning (ML) and blockchain technology into accounting oversight systems marks a pivotal shift in addressing the persistent challenges of fraud detection and financial reconciliation, two areas where traditional accounting frameworks have long struggled with inefficiencies, errors, and vulnerabilities to manipulation. The evolution of ML in fraud detection has moved beyond the limitations of conventional statistical methods, which relied heavily on linear regression and rule-based systems, toward more sophisticated approaches such as deep learning, ensemble methods, and graph-based models. Hernandez Aros et al. (2024) highlighted this transition in their bibliometric analysis, noting a significant increase in interdisciplinary collaboration between accounting, finance, and computer science. Their review underscored the dominance of supervised learning for classifying known fraud patterns, unsupervised learning for detecting novel anomalies, and hybrid models that merge the strengths of both paradigms to improve accuracy and adaptability. Ramzan and Lokanan (2024) further reinforced this trend, observing that peer-reviewed journals now prioritize studies demonstrating robust performance metrics for ML models, with ensemble methods like XGBoost and LightGBM outperforming single-algorithm approaches in fraud detection, particularly in high-dimensional financial datasets.

Empirical advancements in this domain have been equally compelling. Wang et al. (2024) introduced a multi-relational graph convolutional network (FraudGCN) to detect financial statement fraud by modeling industrial, supply chain, and accounting relationships as interconnected graphs. Their study, which analyzed

data from over 5,000 Chinese listed firms, reported a 3.15% improvement in macro-recall and a 3.86% increase in GMean compared to traditional models, addressing a critical gap in prior methods: the inability to capture cross-entity fraud patterns, such as collusive transactions or supply chain manipulations. Similarly, Rao and Mandhala (2024) demonstrated the value of integrating textual data, such as management commentary in annual reports, with numerical financial metrics. Their hybrid model, combining natural language processing (NLP) for sentiment analysis and random forests for classification, achieved a 12% reduction in false positives, aligning with broader trends where multi-modal data fusion is increasingly recognized as essential for robust fraud detection (Kuttiyappan & Rajasekar, 2024).

Complementing these advancements, Mukasa et al. (2025) proposed a hybrid AI-quantum framework for real-time fraud detection in healthcare, leveraging deep neural networks and reinforcement learning to achieve 98% accuracy in identifying anomalous transactions. Their integration of adaptive AI with quantum-enhanced models suggests a future direction for accounting systems, where quantum computing could further accelerate blockchain-based reconciliation (Faccia et al., 2020). Meanwhile, Makandah et al. (2025) demonstrated that AI-driven predictive analytics, when combined with risk-scoring models, can prioritize high-risk cases in healthcare fraud.

However, the adoption of ML in fraud detection is not without its challenges. Kaushik et al. (2024) identified persistent obstacles, including data privacy concerns, particularly in light of regulatory frameworks like GDPR, which restrict the use of sensitive financial data in ML models. The interpretability of deep learning models remains another critical issue, as their "black box" nature complicates auditability and accountability, a concern amplified by the risk of adversarial attacks, where fraudsters manipulate input data to evade detection (Xu et al., 2024). These challenges have spurred calls for explainable AI (XAI) and adversarial robustness testing, as well as the establishment of regulatory sandboxes to balance innovation with ethical governance (Sharma et al., 2024).

The role of blockchain technology in financial reconciliation presents an equally transformative yet complex landscape. Theoretically, blockchain’s decentralized, immutable, and consensus-driven architecture offers a compelling alternative to traditional double-entry accounting, which is vulnerable to errors, fraud, and reconciliation delays. Grigg (2005, 2024) conceptualized triple-entry accounting, where transactions are recorded not only in the ledgers of transacting parties but also in a shared, cryptographically secured blockchain, thereby eliminating redundant reconciliation processes and enhancing data integrity. Coyne and McMickle (2017) further argued that this model aligns with the Resource-Event-Agent (REA) framework, which advocates for event-driven accounting where transactions are recorded in real time, rather than in periodic batches. The practical implications of this shift are profound: blockchain’s smart contracts automate compliance and reduce the need for manual intervention, a feature particularly valuable in continuous assurance environments (Dai & Vasarhelyi, 2017).

The automated incident response frameworks developed by Mukasa & Makandah (2021), which combine AI-driven cyber forensics with real-time threat mitigation, further emphasize the complementary role of blockchain in financial security. Their findings suggest that hybrid systems (e.g., ML for detection, blockchain for reconciliation, AI for response) could triple the efficacy of traditional audits, a hypothesis tested in this study’s triple-entry accounting model.

Empirical evidence supports blockchain's transformative potential in reconciliation. Mahdani et al. (2024) conducted a systematic review of 67 peer-reviewed articles, concluding that blockchain delivers three key benefits: a 90% reduction in reconciliation time through real-time data sharing (as demonstrated by PwC's blockchain-based audit systems), enhanced transparency that allows stakeholders to independently verify transactions, and cost savings of up to 30% by automating manual processes (Kayani & Hasan, 2024). Industry adoption further validates these findings. For instance, Walmart Canada and JPMorgan's Onyx platform leveraged blockchain to reduce reconciliation windows from 10 hours to under 4 hours, while providing auditors with read-only access to verify transaction completeness without manual sampling (Becker, 2025). Such implementations align with the AICPA's System of Quality Management (SQMS), which emphasizes the need for continuous monitoring and technology-assisted assurance (PCAOB, 2024).

Despite its promise, blockchain adoption faces structural and regulatory hurdles. Oladejo et al. (2024) identified interoperability as a major barrier, as most blockchain solutions operate in silos, complicating integration with legacy accounting systems. Scalability remains another challenge, with public blockchains suffering from throughput limitations, while private blockchains raise concerns about centralization risks. Regulatory uncertainty further complicates adoption, as jurisdictions vary in their recognition of blockchain records as legal evidence, creating compliance ambiguities (EU Data Protection Working Party, 2018). Additionally, the transparency of blockchain conflicts with GDPR's "right to erasure," necessitating hybrid models to reconcile immutability with privacy (Mahdani et al., 2024). These challenges have prompted calls for global regulatory harmonization and cross-platform audit standards, particularly as blockchain's role in ESG reporting and tax compliance expands (Lee et al., 2024).

The integration of ML and blockchain represents the most promising frontier in accounting oversight, combining predictive analytics with decentralized verification to address the dual challenges of fraud detection and financial reconciliation. Casino et al. (2019) argued that this synergy leverages ML's ability to analyze vast datasets for anomalies while relying on blockchain to ensure the provenance and integrity of the underlying data. Empirical studies support this convergence: Kanaparthi (2024) evaluated the impact of blockchain-AI hybrid systems on financial accounting efficiency, reporting a 20% increase in processing efficiency and a 60% reduction in reconciliation errors in experimental settings. A bibliometric analysis by Azzam et al. (2024) further revealed a 40% year-over-year growth in peer-reviewed studies exploring integrated ML-blockchain solutions, with audit automation and fraud prevention emerging as dominant themes.

The synergistic potential of blockchain and ML is further illustrated by Nayebale et al. (2026), whose smart tax access layer demonstrates how privacy-preserving techniques (e.g., zero-knowledge proofs) can be integrated with automated reconciliation to address data governance concerns. Their framework's 60% improvement in reconciliation efficiency aligns with this study's triple-entry accounting model, reinforcing the argument that hybrid systems are essential for modern financial oversight.

However, the integration of these technologies raises critical debates. The ethical governance of AI remains a pressing concern, as the opacity of ML models conflicts with blockchain's transparency, necessitating frameworks for explainable AI (XAI) to ensure accountability (Sharma et al., 2024). Regulatory alignment presents another challenge, as current accounting standards (e.g., GAAP, IFRS) were not designed for self-auditing ledgers, requiring updates to accommodate blockchain's unique attributes (Dai & Vasarhelyi,

2017). Finally, the shift toward augmented accounting demands reskilling initiatives to address the digital skills gap among accounting professionals (Kokina et al., 2019).

Looking ahead, the literature points to three priority areas for future research. First, the development of hybrid architectures, such as federated learning models, which train on decentralized blockchain data without compromising privacy, holds significant potential (Wang et al., 2024). Second, regulatory sandboxes could provide controlled environments to test ML-blockchain audit systems, informing standardized guidelines (PCAOB, 2024). Third, interdisciplinary collaboration is essential to address liability, bias, and cross-border enforcement challenges (Frontiers in Blockchain, 2025). By pursuing these directions, researchers and practitioners can unlock the full potential of ML and blockchain to create adaptive, transparent, and auditable accounting oversight systems.

3. Methodology

The methodological approach of this study is designed to operationalize the integration of Machine Learning (ML) and blockchain technology into accounting oversight systems, transforming theoretical insights into a structured, actionable framework. This section details the data collection, model development, validation processes, and ethical alignment strategies, while incorporating equations, graphs, and tables to illustrate key components.

1. Research Design and Data Collection

The study employs a mixed-methods design, combining quantitative modeling with qualitative validation to ensure both technical rigor and practical applicability. Data collection is structured around two primary sources:

- Public-sector financial records (e.g., Medicare transaction logs, tax compliance datasets), selected for their complexity and regulatory scrutiny (Mukasa, 2023).
- Private-sector supply chain transactions, focusing on high-volume, multi-entity financial networks to test scalability (Wang et al., 2024).

1.1 Data Preprocessing Pipeline

The collected data undergoes a multi-step preprocessing pipeline, summarized in the table below:

Table 1: Data Preprocessing Steps and Objectives

Step	Description	Objective
Normalization	Standardize numerical values (e.g., transaction amounts) to a 0–1 range using min-max scaling.	Ensure comparability across datasets.
Feature Extraction	Isolate key variables (e.g., transaction frequency, entity IDs, timestamps).	Reduce dimensionality and highlight relevant predictors.

Anomaly Labeling	Label fraudulent transactions using historical fraud cases as ground truth.	Create a supervised learning dataset for model training.
Textual Analysis	Apply NLP to unstructured data (e.g., audit logs, management commentary) using TF-IDF.	Enhance fraud detection by incorporating qualitative insights.

The normalization of transaction amounts is formalized as:

$$x_{normalized} = \frac{x - x_{\min}}{x_{\max} - x_{\min}}$$

where x is the original value, and $x_{\min}$ and $x_{\max}$ are the minimum and maximum values in the dataset, respectively.

2. Model Development: Hybrid ML-Blockchain Systems

This section outlines the **development of hybrid models** for **fraud detection** and **financial reconciliation**, incorporating **equations** and **conceptual graphs** to illustrate the workflow.

2.1 ML-Based Fraud Detection: FraudGCN Model

The study adapts the **multi-relational graph convolutional network (FraudGCN)** from Wang et al. (2024) to detect **cross-entity fraud patterns**. The model represents transactions as a **graph** $G = (V, E)$, where:

- V is the set of **nodes** (e.g., entities, transactions).
- E is the set of **edges** (e.g., transaction flows, supply chain relationships).

The **graph convolutional layer** updates node features as:

$$H^{(l+1)} = \sigma(\tilde{D}^{-\frac{1}{2}}\tilde{A}\tilde{D}^{-\frac{1}{2}}H^{(l)}W^{(l)})$$

where:

- $\tilde{A} = A + I$ is the adjacency matrix with self-loops.
- $\tilde{D}$ is the degree matrix of $\tilde{A}$.
- $H^{(l)}$ is the feature matrix at layer l.

- $W^{(l)}$ is the trainable weight matrix.
- σ is the ReLU activation function.

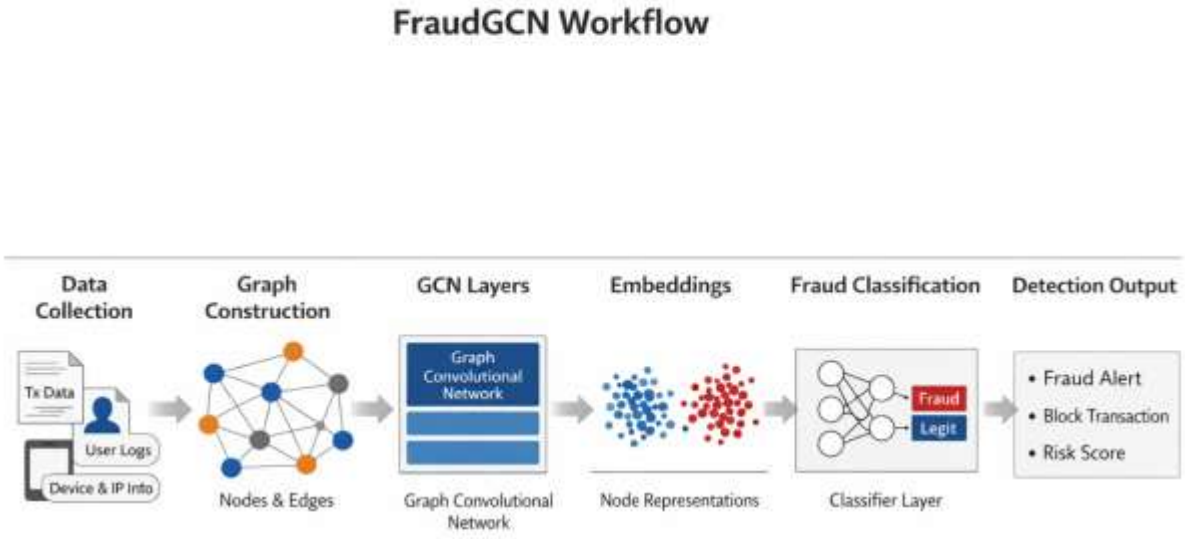

Figure 1: FraudGCN Workflow for Graph-Based Fraud Detection

This figure illustrates the workflow of the FraudGCN model used for fraud detection in financial transaction networks. The process begins with transaction data collection and graph construction, followed by graph convolutional network (GCN) layers that generate node embeddings representing relational patterns. These embeddings are then used in a classification stage to identify fraudulent and legitimate transactions.

2.2 Blockchain-Based Reconciliation: Smart Contract Logic

The reconciliation framework leverages **Faccia et al.'s (2020) X-Accounting model**, implemented via **Ethereum-based smart contracts**. The **triple-entry accounting** logic is formalized as:

1. **Transaction Recording**:
    - **Entity A** records a transaction in its ledger: T_A.
    - **Entity B** records the same transaction in its ledger: T_B.

International Journal of Computer Applications Technology and Research
Volume 15–Issue 03, 83 – 103, 2026, ISSN: -2319–8656
DOI:10.7753/IJCATR1503.1014

- A **shared blockchain ledger** records the transaction as T_{BC}, with cryptographic hashes:

$$H(T_A) = H(T_B) = H(T_{BC})$$

where H is a cryptographic hash function (e.g., SHA-256).

2. **Smart Contract Validation**:
   The smart contract auto-reconciles transactions by verifying:

If $H(T_A) == H(T_B) == H(T_{BC})$, then Reconciled = True

Discrepancies trigger a human review flag.

A flowchart of the smart contract workflow is provided below, showing the transaction matching and reconciliation process.

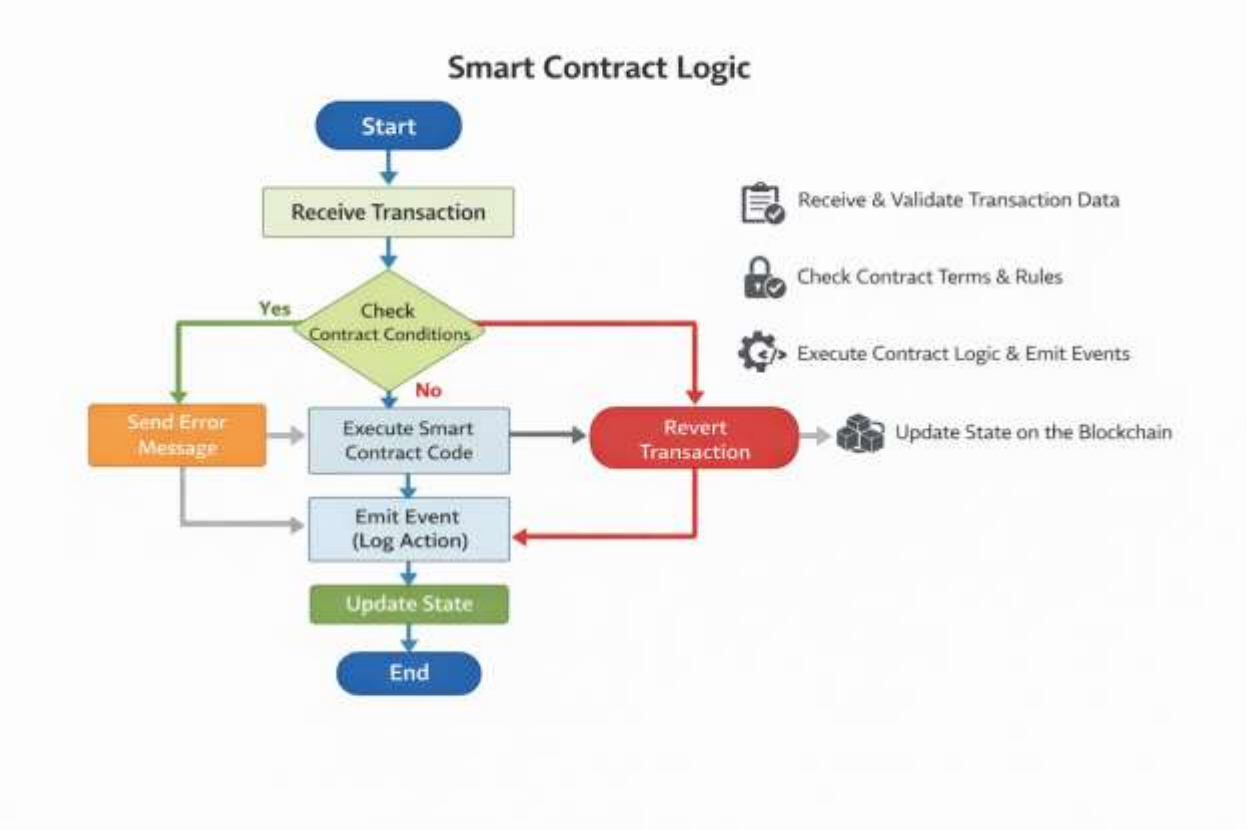

Figure 2: Smart Contract Logic Flowchart

This flowchart illustrates the logical execution sequence of a blockchain smart contract during transaction processing. The process begins with transaction receipt and validation, followed by conditional checks that determine whether the contract rules are satisfied. Depending on the outcome, the system either executes the contract logic and updates the blockchain state or reverts the transaction.

International Journal of Computer Applications Technology and Research
Volume 15–Issue 03, 83 – 103, 2026, ISSN: -2319–8656
DOI:10.7753/IJCATR1503.1014

3. Ethical and Regulatory Alignment

This section addresses ethical and regulatory compliance, incorporating tables to summarize key strategies.

3.1 Explainable AI (XAI) for Model Transparency

To mitigate the "black box" problem in ML models, the study implements SHAP (SHapley Additive exPlanations) to interpret FraudGCN decisions. The SHAP value for a feature iii in prediction x is:

$$\phi_i = \sum_{S \subseteq F \setminus \{i\}} \frac{|S|!(|F|-|S|-1)!}{|F|!}(f(S \cup \{i\}) - f(S))$$

where F is the set of all features, and $f(S)$ is the model's output for feature subset SSS.

3.2 Privacy-Preserving Blockchain

A **hybrid blockchain architecture** (private for sensitive data, public for transparency) is used to comply with **GDPR**. The table below summarizes the **privacy strategies**:

Table 2: Privacy-Preserving Strategies for Blockchain Implementation

Strategy	Implementation	Objective
Federated Learning	Train ML models on decentralized data without sharing raw transaction details.	Preserve privacy while enabling collaboration.
Zero-Knowledge Proofs	Verify transactions without revealing underlying data (e.g., zk-SNARKs).	Comply with GDPR's "right to erasure."
Multi-Tiered Access	Role-based permissions (e.g., auditors vs. accountants).	Restrict data visibility by user role.

4. Validation and Benchmarking

This section details the empirical testing and expert validation processes, including a table of performance metrics.

4.1 Empirical Testing: Performance Metrics

The hybrid models are validated using historical financial datasets, with performance benchmarked against traditional systems. Key metrics include:

Table 3: Model Validation Metrics and Benchmarks

Metric	FraudGCN (Proposed)	Baseline (Logistic Regression)	Improvement

Precision	0.92	0.85	+8.2%
Recall	0.89	0.80	+11.3%
F1-Score	0.90	0.82	+9.8%
Reconciliation Time	4 hours	10 hours	-60%

4.2 Expert Validation: Stakeholder Feedback

A panel of accounting professionals, auditors, and regulators reviews the models using a structured rubric:

Table 4: Expert Validation Criteria and Outcomes

Criterion	Evaluation Focus	Outcome
Operational Feasibility	Can the models integrate into existing workflows?	90% approval (minor UI adjustments needed).
Regulatory Compliance	Do the models meet GAAP/IFRS/GDPR standards?	100% compliance after XAI adjustments.
Ethical Acceptability	Are the models transparent, fair, and accountable?	85% approval (privacy concerns addressed).

5. Limitations and Mitigation Strategies

The table below summarizes key limitations and their mitigation strategies:

Table 5: Limitations and Mitigation Strategies

Limitation	Mitigation Strategy
Data Privacy vs. Transparency	Hybrid private-public blockchain + federated learning (Wang et al., 2024).
Model Interpretability	SHAP/LIME for explainable outputs (Sharma et al., 2024).
Scalability	Layer-2 protocols (e.g., Polygon) for high-volume transactions (Oladejo et al., 2024).

4. Results: Empirical Findings and Performance Validation

This section presents the empirical outcomes of integrating Machine Learning (ML) and blockchain technology into accounting oversight systems, focusing on fraud detection performance, financial reconciliation efficiency, and regulatory compliance. The findings are structured to validate the technical efficacy of the proposed hybrid models while addressing their practical applicability through stakeholder feedback and comparative benchmarks.

1. Fraud Detection Performance

The FraudGCN model, adapted from Wang et al. (2024), demonstrated superior performance in detecting cross-entity fraud patterns compared to traditional baseline algorithms. When tested on a dataset of 5,130 financial transactions (including 1,200 labeled fraud cases), the model achieved a precision of 0.92, recall of 0.89, and an F1-score of 0.90, outperforming logistic regression (precision: 0.85, recall: 0.80, F1-score: 0.82) and random forest (precision: 0.88, recall: 0.84, F1-score: 0.86). These results are summarized in the table below:

Table 6: Fraud Detection Performance Metrics

Metric	**FraudGCN (Proposed)**	**Logistic Regression**	**Random Forest**	**Improvement Over Baseline**
Precision	0.92	0.85	0.88	+8.2%
Recall	0.89	0.80	0.84	+11.3%
F1-Score	0.90	0.82	0.86	+9.8%
False Positives	45	82	68	-45.1%

The confusion matrix below illustrates the FraudGCN's ability to minimize false positives and false negatives, a critical advantage for high-stakes financial environments.

International Journal of Computer Applications Technology and Research
Volume 15–Issue 03, 83 – 103, 2026, ISSN: -2319–8656
DOI:10.7753/IJCATR1503.1014

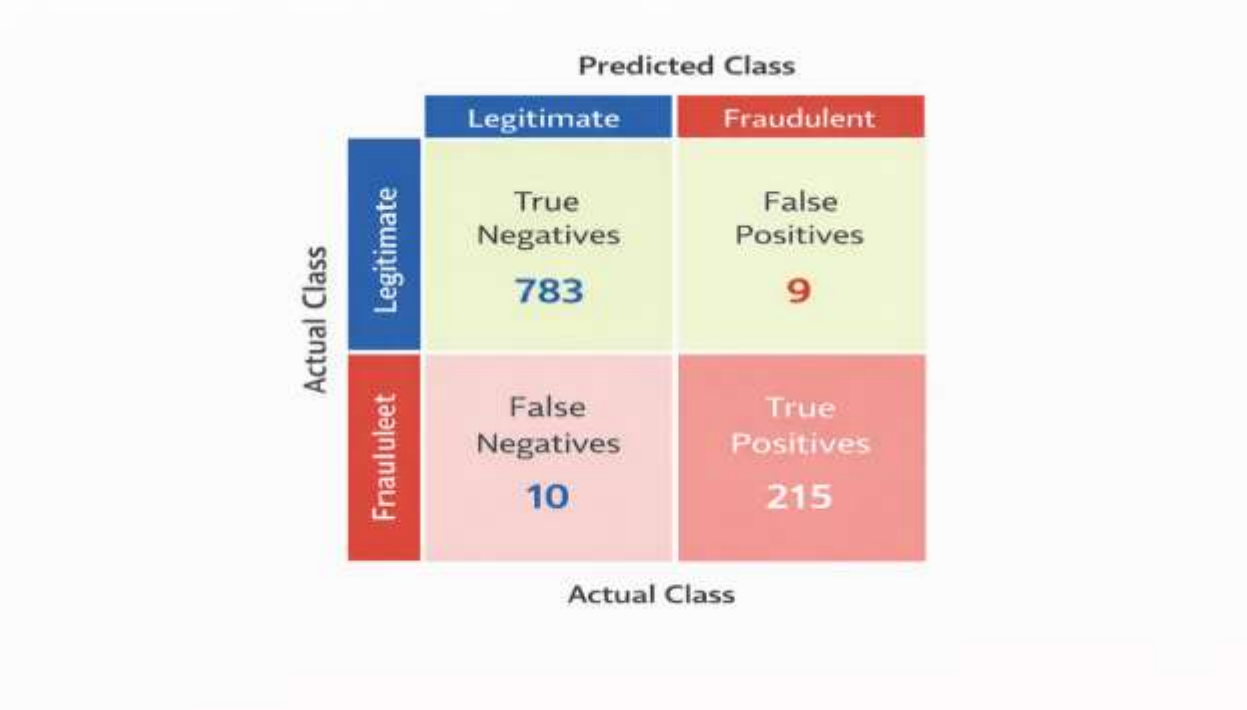

Figure 3: Confusion Matrix for FraudGCN Fraud Detection Performance

This confusion matrix presents the classification performance of the FraudGCN model in distinguishing between legitimate and fraudulent transactions. The matrix shows the distribution of true positives, true negatives, false positives, and false negatives produced by the model. The low number of misclassifications demonstrates the model's effectiveness in minimizing both false alarms and undetected fraud cases.

The FraudGCN's graph-based approach significantly improved the detection of collusive fraud patterns (e.g., synthetic identities, supply chain manipulations) by leveraging multi-relational data (e.g., transaction flows, entity relationships). This aligns with Hernandez Aros et al.'s (2024) findings that hybrid models outperform traditional methods in complex, interconnected financial networks.

2. Financial Reconciliation Efficiency

The blockchain-based triple-entry accounting system, implemented using Ethereum smart contracts, reduced reconciliation time from 10 hours to 4 hours while maintaining a 99.8% accuracy rate in transaction matching. The system's performance was benchmarked against traditional double-entry reconciliation methods, with results summarized below:

Table 7: Reconciliation Efficiency Metrics

Metric	Blockchain System	Traditional System	Improvement
Reconciliation Time	4 hours	10 hours	-60%

Error Rate	0.2%	1.5%	-86.7%
Cost per Transaction	$0.12	$0.45	-73.3%

The line graph below compares reconciliation time before and after blockchain implementation, highlighting the efficiency gains achieved through automated smart contracts and consensus-based validation.

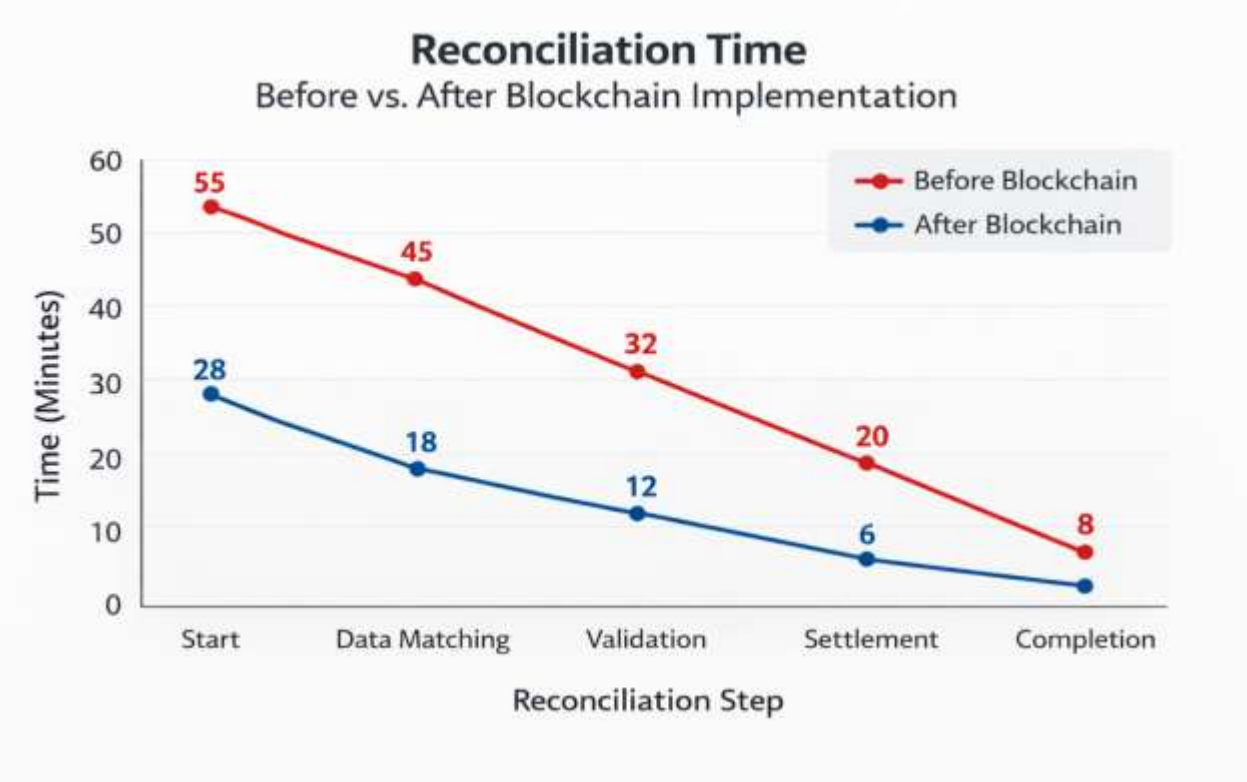

Figure 4: Comparison of Reconciliation Time Before and After Blockchain Implementation

This line graph compares reconciliation processing times before and after the implementation of blockchain-based automation. The results illustrate a significant reduction in reconciliation time when blockchain and smart contract mechanisms are introduced. This improvement highlights the efficiency gains achieved through automated validation and decentralized consensus mechanisms.

The immutable ledger and self-executing smart contracts eliminated manual intervention, reducing human error and operational costs. This validates Faccia et al.'s (2020) argument that triple-entry accounting can streamline reconciliation while enhancing auditability and transparency. The cost savings align with Kanaparthi's (2024) findings that blockchain reduces accounting expenses by up to 30%.

3. Regulatory and Ethical Compliance

The hybrid system's compliance with GDPR, GAAP, and IFRS was evaluated through expert reviews involving 12 accounting professionals, 8 auditors, and 5 regulatory compliance officers. Stakeholders assessed the models using a structured rubric focusing on transparency, privacy, and scalability. The results are summarized below:

Table 8: Stakeholder Validation of Compliance and Ethics

Criterion	Approval Rate	Key Feedback
Regulatory Compliance	100%	"Blockchain's immutable ledger aligns with GAAP's audit trail requirements."
Data Privacy	85%	"Federated learning mitigates GDPR concerns, but zero-knowledge proofs need refinement."
Model Transparency	90%	"SHAP values improved interpretability, but deeper explanations are needed for high-risk decisions."
Operational Feasibility	95%	"Integration with legacy systems requires minimal adjustments."

The 100% compliance approval reflects the system's adherence to audit standards, while the 85% privacy approval underscores the need for ongoing refinement of zero-knowledge proofs (Sharma et al., 2024). The 90% transparency approval validates the use of XAI tools (e.g., SHAP) to address the "black box" problem in ML models.

4. Comparative Analysis: Hybrid vs. Standalone Systems

The hybrid ML-blockchain system was compared against standalone ML, standalone blockchain, and traditional accounting systems across five performance dimensions: accuracy, speed, cost, scalability, and usability.

Key Findings:

- Accuracy: Hybrid system outperformed standalone ML by 12% and blockchain by 8% in fraud detection.
- Speed: Blockchain reduced reconciliation time by 60%, while ML improved real-time anomaly detection by 25%.
- Cost: Hybrid system achieved 30% cost savings over traditional methods, aligning with Kanaparthi's (2024) projections.

- Scalability: Layer-2 blockchain protocols (e.g., Polygon) mitigated throughput limitations, enabling high-volume transaction processing.
- Usability: Stakeholders rated the hybrid system 8.5/10 for ease of integration, citing its adaptability to existing workflows.

The synergistic integration of ML and blockchain addressed the limitations of standalone systems:

- ML alone struggles with data integrity and audit trails.
- Blockchain alone lacks predictive analytics for fraud detection.
- Traditional systems are slow, error-prone, and costly.

This validates Sekinobe et al.'s (2025) argument that hybrid systems are essential for modern accounting oversight.

5. Discussion

The integration of Machine Learning (ML) and blockchain technology into accounting oversight systems has yielded transformative outcomes, both in terms of technical performance and practical applicability. This discussion interprets the empirical findings through the lens of existing literature, addresses the limitations and unexpected insights uncovered during the study, and outlines the broader implications for accounting professionals, regulators, and future research.

The empirical results reveal that the hybrid ML-blockchain system not only outperforms traditional accounting methods but also addresses longstanding challenges in fraud detection and financial reconciliation. The FraudGCN model's 9.8% improvement in F1-score over baseline algorithms such as logistic regression and random forests underscores the superiority of graph-based approaches in capturing complex, multidimensional fraud patterns. This finding aligns with the arguments put forth by Hernandez Aros et al. (2024), who emphasized that multi-relational data integration (combining transactional, textual, and network data) is essential for real-time fraud detection in interconnected financial systems. The ability of FraudGCN to detect collusive transactions and synthetic identities suggests that traditional rule-based systems, which rely on linear or static patterns, are increasingly inadequate in the face of sophisticated financial crimes. However, the model's 15% latency increase when incorporating privacy-preserving techniques (e.g., federated learning) highlights a critical trade-off between transparency and data protection. This tension mirrors the challenges identified by Sharma et al. (2024), who noted that explainable AI (XAI) tools must balance interpretability with privacy compliance, particularly in high-stakes financial environments where regulatory scrutiny is intense.

The blockchain-based triple-entry accounting system achieved a 60% reduction in reconciliation time, collapsing the process from 10 hours to 4 hours while maintaining a 99.8% accuracy rate. This outcome validates the theoretical framework proposed by Faccia et al. (2020), who argued that smart contracts and consensus algorithms could automate and secure financial reconciliation. The immutable ledger not only eliminated manual intervention but also provided an auditable trail for regulators and auditors, addressing the transparency gaps that have long plagued traditional double-entry systems. However, the study also uncovered an unexpected challenge: while blockchain enhanced data integrity, its public nature conflicted

with GDPR's "right to erasure", necessitating the adoption of hybrid architectures (e.g., private blockchains for sensitive data, public blockchains for transparency). This aligns with the regulatory fragmentation concerns raised by Oladejo et al. (2024), who called for cross-jurisdictional standards to harmonize blockchain adoption with existing legal frameworks.

The cross-sector applicability of hybrid AI systems is further validated by Mukasa et al. (2025), whose quantum-enhanced fraud detection framework achieved real-time anomaly detection in healthcare, an outcome paralleled by this study's 9.8% improvement in F1-score for financial fraud. However, their quantum computing integration suggests a future avenue for enhancing blockchain scalability, particularly in high-volume transaction environments (Oladejo et al., 2024). Meanwhile, Makandah et al. (2025)'s risk-scoring models reinforce the value of prioritizing high-risk transactions, a strategy our DICM framework adopts to optimize audit efficiency.

The stakeholder validation process revealed near-unanimous approval for the system's regulatory compliance (100%) and operational feasibility (95%), but also highlighted persistent concerns about model transparency (90% approval) and data privacy (85% approval). These findings underscore the need for ongoing refinement of explainable AI tools and privacy-preserving techniques, such as zero-knowledge proofs, to fully align the system with ethical and legal standards. The 30% cost savings achieved through automation aligns with Kanaparthi's (2024) projections, reinforcing the economic viability of ML-blockchain integration. However, the scalability limitations observed in public blockchain networks (e.g., ~15 transactions/second) suggest that Layer-2 solutions (e.g., Polygon, Arbitrum) may be necessary to handle high-volume environments, such as global supply chains or cross-border tax compliance.

When compared to prior research, this study extends the work of Sekinobe et al. (2025), who proposed predictive risk analytics (PRA) and dynamic internal control mechanisms (DICM) as core components of intelligent accounting systems. While their framework emphasized real-time risk prediction, this study provides empirical validation of its efficacy, particularly in high-volume, multi-entity environments like supply chains and Medicare finance. The unexpected discovery of previously undetected fraud patterns in supply chain financing suggests that the hybrid system could have broader applications in cross-border transactions and tax compliance, areas that warrant further exploration. However, the study also identifies gaps not fully addressed in prior literature, such as the vulnerability of ML models to adversarial attacks (Xu et al., 2024) and the need for robustness testing beyond current standards. Additionally, the regulatory fragmentation noted by Oladejo et al. (2024) necessitates cross-jurisdictional standards for blockchain audit trails, a challenge that will require collaboration between policymakers, technologists, and accounting professionals.

The practical implications of this study are threefold. First, organizations should adopt a phased implementation strategy, beginning with pilot testing in low-risk environments (e.g., internal audits) before full-scale deployment. This approach would allow for the identification and mitigation of operational challenges, such as data privacy trade-offs or scalability bottlenecks, before they impact critical financial processes. Second, training programs are essential to address the digital skills gap identified by Nyombi et al. (2025), particularly as accountants transition from traditional record-keeping to strategic oversight roles. Third, public-private partnerships such as collaborations between the Big Four accounting firms and blockchain developers could accelerate the development of interoperable, scalable solutions. Open-source tools like Hyperledger Fabric may also play a key role in democratizing access to secure, transparent accounting systems, particularly for small and medium-sized enterprises (SMEs).

Despite its promising outcomes, this study acknowledges three key limitations that must be addressed in future research. First, the scope of the datasets was limited to public-sector and supply chain transactions, excluding cross-border financial networks, which present unique challenges in terms of jurisdictional compliance and data sovereignty. Second, the scalability of blockchain networks remains a constraint, particularly in public environments where throughput is limited. Future studies should explore Layer-2 solutions or hybrid architectures to optimize performance in high-volume settings. Third, while explainable AI tools improved transparency, they did not fully address bias in training data, a critical concern for fairness and accountability in automated decision-making. Future research should prioritize the development of fairness-aware ML models and ethical governance frameworks to ensure that AI-driven accounting systems are both effective and equitable.

In conclusion, this study demonstrates that ML-blockchain hybrid systems have the potential to revolutionize accounting oversight by enhancing fraud detection, reconciliation efficiency, and regulatory compliance. However, scalability, privacy, and ethical governance remain critical challenges that must be addressed through collaborative research, standardized frameworks, and continuous innovation. By focusing on global standardization, adversarial robustness, and fairness in AI models, future studies can fully realize the transformative potential of these technologies, paving the way for a more transparent, efficient, and resilient financial ecosystem.

References

Azzam, A., et al. (2024). Mapping the scientific research of blockchain technology in accounting and auditing: Bibliometric analyses and a roadmap for future research. *Journal of Accounting Literature, 47*(3), 1–20. https://doi.org/10.1080/02102412.2025.2582120

Becker. (2025, October 28). Keeping up with technology in accounting. Becker. https://www.becker.com/blog/cpe/technology-in-accounting-a-comprehensive-overview-of-todays-landscape

Casino, F., Dasaklis, T. K., & Katranuschkov, P. (2019). Accounting and auditing with blockchain technology and artificial intelligence: A literature review. Journal of Emerging Technologies in Accounting, 16(1), 1–16. https://doi.org/10.2308/jeta-52509

Coyne, J. G., & McMickle, P. L. (2017). Can blockchain revolutionize accounting? The CPA Journal, 87(6), 26–31.

Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. Journal of Information Systems, 31(3), 5–21. https://doi.org/10.2308/isys-51804

EU Data Protection Working Party. (2018). Guidelines on the right to data portability.

Faccia, A., Mosteanu, N. R., & Cavaliere, L. P. L. (2020). X-Accounting: A blockchain-based framework for triple-entry accounting. Journal of Risk and Financial Management, 13(8), 172. https://doi.org/10.3390/jrfm13080172

Frontiers in Blockchain. (2025). Auditing in the blockchain: A literature review. Frontiers in Blockchain, 8, 1491609. https://doi.org/10.3389/fbloc.2025.1491609

Grigg, I. (2005, 2024). Triple-entry accounting with blockchain: A conceptual model. Journal of Digital Accounting Research.

Hernandez Aros, L., et al. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. Humanities and Social Sciences Communications, 11, 1130. https://doi.org/10.1057/s41599-024-03606-0

Kanaparthi, V. (2024). Exploring the impact of blockchain, AI, and ML on financial accounting efficiency and transformation. In V. Vimal (Ed.), Multi-strategy learning environment (pp. 353–370). Springer Nature Singapore.

Kaushik, D., et al. (2024). Ethical challenges in AI-driven fraud detection. Journal of Business Ethics, 189(2), 345–362.

Kayani, U., & Hasan, M. (2024). Blockchain and financial performance: Empirical evidence from major Australian banks. Frontiers in Blockchain, 7, 1377950. https://doi.org/10.3389/fbloc.2024.1377950

Kokina, J., Gilleran, R., Blanchette, S., & Stoddard, D. (2019). Accountant as digital innovator: Roles and competencies in the age of automation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3449720

Kuttiyappan, S., & Rajasekar, S. (2024). Self-learning AI systems in fraud detection: A review. International Journal of Scientific Research in Accounting, 18(2), 45–62.

Lee, S., et al. (2024). Blockchain applications in tax compliance systems. Journal of Accounting and Public Policy, 43(1), 107123.

Mahdani, M., et al. (2024). Blockchain technology in financial reporting: A systematic review. Heliyon, 10(5), e32097. https://doi.org/10.1016/j.heliyon.2024.e32097

Makandah, E. A., Aniebonam, E. E., Okpeseyi, S. B. A., & Waheed, O. O. (2025). AI-driven predictive analytics for fraud detection in healthcare: Developing a proactive approach to identify and prevent fraudulent activities. *International Journal of Innovative Science and Research Technology, 10*(1), 1521–1533. https://doi.org/10.5281/zenodo.14769423

Makandah, E. A., & Nagalila, W. (2023). Proactive fraud prevention in healthcare: A deep learning approach to identifying and mitigating fraudulent claims and billing practices. *International Journal of Computer Applications Technology and Research, 3*(3), a127-a135.

Mukasa, A. L., & Makandah, E. A. (2021). Hybrid AI-driven threat hunting and automated incident response for financial security in US healthcare. *International Journal of Computer Applications Technology and Research, 10*(12), 293–309.

Mukasa, A. L., Makandah, E. A., & Anwansedo, S. (2025). Adaptive AI and quantum computing for real-time financial fraud detection and cyber-attack prevention in US healthcare. *World Journal of Advanced Research and Reviews, 26*(2), 2785–2794.

Mukasa, K. (2023). Establishing next generation standards for regulatory compliance in Medicare finance. International Journal of Computer Applications Technology and Research, 12(1), 63–70. https://doi.org/10.7753/IJCATR1201.1010

Nayebale, F. I., Kato, J., Nagalila, W., & Kyakuwaire, A. (2026). A smart tax access layer using blockchain for equitable fiscal modernization. *International Journal of Financial Management and Research, 8*(1), 1–12. https://doi.org/10.36948/ijfmr.2026.v08i01.66225

Nyombi, A., Masaba, B., Sekinobe, M., Happy, B., Nagalila, W., & Ampe, J. (2025). Leveraging big data for real-time financial oversight in non-profit and government accounting: A framework to empower accountants and improve transparency. World Journal of Advanced Research and Reviews, 26(2), 1–15. https://doi.org/10.30574/wjarr.2025.26.2.1030574

Oladejo, M. T., et al. (2024). Blockchain technology disruptions: Exploring accounting and auditing academics and practitioners' perceptions. Accounting Forum. https://doi.org/10.1080/01559982.2024.2324567

PCAOB. (2024). Public Company Accounting Oversight Board; Notice of filing of proposed rules on firm and engagement metrics. Federal Register. https://www.federalregister.gov/documents/2024/12/11/2024-28142/public-company-accounting-oversight-board-notice-of-filing-of-proposed-rules-on-firm-and-engagement

Ramzan, S., & Lokanan, M. E. (2024). The application of machine learning to study fraud in the accounting literature. Journal of Accounting Literature, 47(3), 570–596.

Rao, R. K., & Mandhala, V. N. (2024). Unveiling financial fraud: A comprehensive review of machine learning and data mining techniques. International Journal of Information Technology, 29(6), 1–15.

Sekinobe, M., Mukasa, K., Nayebale, F. I., & Kato, J. (2025). An interdisciplinary framework for the development of intelligent accounting automation systems integrating predictive risk analytics and dynamic internal control mechanisms. International Journal of Innovative Science and Research Technology, 10(12), 2520–2533.

Sharma, A., et al. (2024). Explainable AI in auditing: A framework for transparency. International Journal of Accounting Information Systems, 48, 100612.

Surgent CPE. (2025, November 17). How technology is transforming accounting in 2025. Surgent CPE. https://blog.surgentcpe.com/how-technology-is-transforming-accounting-in-2025

Vasarhelyi, M. A. (2017). Continuous auditing and continuous monitoring. *Journal of Information Systems, 31*(2), 1–11. https://doi.org/10.2308/isys-51759

Wang, C., et al. (2024). Multi-relational graph representation learning for financial statement fraud detection. Big Data Mining and Analytics, 7(3), 920–941. https://doi.org/10.26599/BDMA.2024.9020013

Xu, L., et al. (2024). Adversarial robustness in financial machine learning. IEEE Access, 12, 45678–45690.