CBAATM: A Blockchain-AI Integrated Framework for Real-Time Anomaly Detection and Compliance Verification in Smart Accounting Information Systems

Wanli Liu [1], Jianlin Li [2,*], Na Chen [3]
[1]School of Finance, Hebei University of Economics and Business, Shijiazhuang, Hebei, 050061, China
[2]School of Business Administration, Hebei University of Economics and Business, Shijiazhuang, Hebei, 050061, China
[3]Finance Department, Hebei University of Economics and Business, Shijiazhuang, Hebei, 050061, China
E-mail: lijianlin521@hotmail.com
[*]Corresponding author

Keywords: blockchain technology, artificial intelligence, collaborative framework, audit trail mechanism, smart accounting information systems

Received: July 7, 2025

Accounting is undergoing a radical transformation due to the integration of traditional information systems with blockchain technology and artificial intelligence. Openness, automation, and smart decision-making will all become a reality via this connection. However, traditional SAIS are typically centralized and do not inherently include blockchain or AI. In this study, Smart Accounting Information System (SAIS) technologies are redefined through the integration of these technologies to enhance transparency, automation, and real-time assurance. Blockchain technology's immutability, traceability, and AI's ability to recognize abnormalities and predict provide a more intelligent and secure auditing process. Conventional accounting methods have several issues, including delayed audits, lack of transparency, fraud, and human mistakes. Existing systems fail to provide intelligent anomaly detection and real-time transaction traceability. Financial reporting and audits need immutable records and proactive analytics. There is an urgent need for a single framework to ensure this requirement and its quick implementation. This study proposes the collaborative blockchain-AI audit trails method (CBAATM) for Smart Accounting Information Systems. This is done due to the difficulties mentioned. AI-powered modules utilize fuzzy inference to dynamically analyze audit risks and Random Forest classifiers to detect real-time fraud. This research project utilizes zero-knowledge proofs and homomorphic encryption to simultaneously handle data aggregation, privacy, and independent audits. Using middleware application programming interfaces makes integration with ERP and AIS systems easy. Throughout the testing process, the model outperforms conventional audits. The methodology, according to statistical research, ensures the detection accuracy ratio of 95%, integrity of the blockchain 99.2% of the time, identifies abnormalities 94.1% of the time, satisfies compliance standards 95.4% of the time, and reduces audit latency by 41.5% compared to other existing models.

Povzetek: Članek obravnava pomanjkljivosti klasičnih pametnih računovodskih sistemov pri odkrivanju prevar in preverjanju skladnosti. Predlaga okvir CBAATM, ki združuje verigo blokov z AI-moduli: Random Forest za sprotno detekcijo anomalij, Fuzzy Inference za razlago tveganj ter kriptografske postopke za zasebnost. Model močno izboljša točnost, skladnost in zakasnitev revizij.

1 Introduction

More than ever before, accounting and finance are being revolutionized by technology such as blockchain and artificial intelligence [1]. Conventional artificial intelligence systems are overburdened by modern demands for real-time assurance, predictive analytics, data quality, and fraud resistance, even when they are functioning well [2]. When dealing with large transaction sets, post-hoc manual audits and validations are not sufficient because [3]. Companies are addressing the challenges of transparency, traceability, and automation through the use of smart AIS, blockchain, and AI [4]. The immutability of financial transactions is recorded through a distributed ledger system that utilizes cryptography [5]. By making data changes unchangeable even in the absence of consensus, blockchain technology has the potential to improve the reliability of financial records [6]. Permissioned blockchains, made possible by platforms such as Hyperledger Fabric, are only accessible to authorized users. Permissioned blockchains are well-suited for business systems, such as accounting platforms, that require data protection and controlled participation. A consensus mechanism is the process by which all blockchain nodes verify a transaction. This technique maintains consistency and confidence without requiring a

central authority. [7]. The validation of regulatory requirements, permission processes, and double-entry checks can all be automated using smart contracts [8].

Blockchain technology, machine learning, and artificial intelligence collectively make it feasible to identify fraud in real-time [9]. Deep learning neural networks, Random Forests, and Support Vector Machines are all examples of methods that may be trained to identify fraudulent accounting activities by analyzing historical financial data [10]. These models facilitate the performance of continuing audits by identifying potentially risky transactions before they spread across the entire financial system [11]. Due to the increased integration of digital technology into financial ecosystems, notably Smart Accounting Information Systems (SAIS), compliance, operational transparency, data quality, and audit dependability are becoming more critical [12]. It may be challenging to verify, monitor, and detect fraudulent activity using traditional auditing methods, even when employing stringent criteria. Audits that are performed manually and on a predetermined timetable in complex and high-volume transactional settings are a limitation to risk management and real-time decision-making [13]. The work was inspired by the urgent need for an intelligent audit system capable of securely collaborating, detecting, and preventing non-compliant or fraudulent transactions, improving transparency, decreasing audit latency, and providing real-time compliance verification [14]. The Collaborative Blockchain-AI Audit Trail Mechanism (CBAATM) is a proposed approach that leverages AI's pattern recognition and reasoning capabilities in conjunction with blockchain's integrity-preserving properties to bridge this gap. This research addresses the pressing need for a standardized, intelligent, and instant compliance monitoring system by combining blockchain technology's immutable record-keeping with AI's predictive analytics. Due to reactive approaches, human procedures, or fragmented technology, current auditing solutions have slow fraud detection, limited scalability, and poor interpretability. Due to these constraints, Smart Accounting Information Systems (SAIS) cannot automatically verify compliance, safeguard data, or give real-time compliance verification. The Collaborative Blockchain-AI Audit Trail Mechanism (CBAATM) is proposed to enhance financial governance and make auditing more secure, autonomous, and transparent. Blockchain technology, when combined with Accounting Information Systems, creates a secure and decentralized financial data management solution. The system is further reinforced by combining zero-knowledge proofs and homomorphic encryption, which enables auditors and regulators to assess compliance and find abnormalities without direct exposure. Cryptographic synergy enhances data security and integrity, reducing the need for centralized trust and human intervention. Additionally, it enables safe and scalable instant compliance monitoring techniques in high-volume financial contexts.

Research Questions (RQs)

RQ1: How can the integration of blockchain technology and artificial intelligence improve the accuracy, transparency, and responsiveness of audit trail mechanisms in Smart Accounting Information Systems (SAIS)?

RQ2: To what extent can a hybrid model using Random Forest classifiers and Fuzzy Inference Systems enable interpretable, real-time anomaly detection and risk assessment in financial transactions?

RQ3: How effective is the proposed CBAATM framework in ensuring secure, privacy-preserving, and compliant audit verification through smart contracts and cryptographic techniques such as homomorphic encryption and zero-knowledge proofs?

RQ1) The first research question (RQ1) is answered using the CBAATM framework, which blends blockchain's immutability with AI's analytical talents. Results show improved transparency, audit latency, and detection accuracy. RQ2)The anomaly detection part states that we utilize a Fuzzy Inference System and Random Forest classifiers to investigate. These results support the accuracy and interpretability of anomaly detection, which bodes well for real-time risk assessment. RQ3) is answered using privacy assurance principles, including zero-knowledge proofs, homomorphic encryption, and smart contracts. Blockchains' high compliance match rates and integrity ratings make them suitable for surreptitiously verifying audits.

Research design

RQ1. *Does integrating blockchain with AI-based anomaly detection improve the accuracy and reliability of Smart AIS compared to existing methods (e.g., DGRU-IMPA, CAIS)?*

Hypothesis (H1): The CBAATM framework will achieve a detection accuracy of at least 95% and blockchain integrity of 99%, outperforming baseline systems by a minimum of 3 percentage points in accuracy and achieving at least a 30% reduction in processing latency.

Evaluation method: A financial transaction dataset containing 100,000 records will be used. Comparative testing against existing methods will be conducted, using metrics such as detection accuracy, precision, recall, and per-transaction latency. Statistical significance will be validated using paired *t*-tests to ensure robustness of observed improvements.

RQ2. *Can the system maintain real-time performance (low latency) while preserving decision interpretability for audit and regulatory compliance?*

Hypothesis (H2): By integrating a Fuzzy Inference System (FIS) with Random Forest (RF), the framework will maintain sub-2-second compliance validation per transaction while enabling rule-based explanations of anomaly detection results.

Evaluation method: End-to-end latency will be measured as both average and 95th percentile response times. The interpretability of decisions will be evaluated by extracting human-readable rules generated by FIS, which will be compared against standalone Random Forest and neural network models to assess the trade-offs between accuracy and explainability.

RQ3. *Does the use of cryptographic privacy mechanisms (zero-knowledge proofs) significantly impact auditability or system throughput?*

Hypothesis (H3): Incorporating zero-knowledge proofs will reduce system throughput by no more than 10% compared to a non-cryptographic baseline, while maintaining 100% verifiable audit trails for all transactions.

Evaluation method: Controlled experiments will be conducted on identical workloads with and without cryptographic layers, measuring throughput (transactions per second), blockchain integrity, and compliance verification times to quantify performance overheads.

Random Forest offers strong performance in detecting anomalies across complex, non-linear financial datasets, but its decision process lacks transparency. By embedding a Fuzzy Inference System, Random Forest outputs can be translated into interpretable, linguistic rules that are useful for auditors and regulators. This hybrid design preserves most of the accuracy benefits of Random Forest (an accuracy drop of less than 1% compared to RF-only) while significantly enhancing explainability, thereby balancing accuracy and interpretability, a critical requirement for financial audit compliance.

The main contribution of the study

1. Introduces CBAATM, a advanced SAIS audit trail management system using blockchain and real-time AI.
2. Fuzzy Inference Systems (FIS) and Random Forest classifiers offer interpretable, real-time assessments of financial transaction risk.
3. Automates compliance tests and detects non-compliance in real time using GAAP/IFRS and smart contracts.
4. Uses zero-knowledge proofs and homomorphic encryption to safeguard sensitive audit data.

The remainder of the article is organized as follows: Section 2 proposes the CBAATM model, Section 3 discusses the simulation outcomes, and Section 4 concludes the research paper with a discussion of future studies.

2 Literature review

Xue Li et al. [15] proposed the deep gated recurrent units (DGRU) utilizing an improved marine predator algorithm (IMPA) for profit detection based on a financial AIS (FAIS). This research focuses on the increasing intricacy of hybrid networks, driven by larger and larger datasets, and aims to address the challenge of real-time processing performance. The author constructs a novel dataset comprising 15 input parameters from the original Kaggle database for the Chinese stock market, enabling more accurate comparisons. A total of five models based on DGRU have been created, including the non-linear MPA (NMPA) and the chaotic MPA (CMPA), two of the finest forms of the Levy algorithm, as well as the Levy-based gray wolf optimization method (LGWO). Based on the data, this model appears to outperform the other algorithms examined in terms of profit prediction.

Huijue Kelly Duan et al. [16] proposed utilizing text mining and machine learning to enhance government accounting information systems by incorporating social media information. The data is being compiled to provide another metric for evaluating the cleanliness of streets in New York City. The tweets are classified using Naïve Bayes, Random Forest, and XGBoost. The sampling approach is shown to handle the problem of uneven class distribution. Public opinion regarding street cleanliness is derived using VADER sentiment analysis. The research is expanded to include Facebook, revealing that the two platforms have different incremental values. By connecting this data to government accounting information systems, we can more accurately assess expenses and gain a deeper understanding of the success and efficiency of our operations.

Manaf Al-Okaily et al. [17] recommended using cloud-based AIS (CAIS) and its impact on the performance of Jordanian SMEs. From 438 present and future users of cloud-based AIS, empirical data were collected using a quantitative research technique based on a cross-sectional online questionnaire. Data analyses using structural equation modeling (SEM) based on the moment structure 25.0 analysis. According to the results of the structural path analysis, 71% of the variation in users' behavioral intention (BI) toward using CAIS was explained by performance expectation, social incentive, COVID-19 risk (COVID-19 PR), and trust (TR). Nevertheless, there was no discernible relationship between BI and either effort expectation or perceived security risk (SEC). Likewise, BI was shown to explain 74% of the variation in actual use behaviors and affect those behaviors. Using AIS in the cloud substantially impacts the outcome variables, specifically CQ and DQ, of communication and decision-making.

Shanti and Elessa [18] discussed the application of blockchain technology in banks to enhance the quality of AIS and the efficacy of corporate governance. A descriptive-analytical approach was used to investigate the study's variables and dimensions. Financial analysts at Jordanian banks, auditors of shareholder accounts, and field research community financial managers were surveyed using pre-made data lists. The author utilized SPSS to analyze the data from the field investigation. Rejecting the null hypothesis and accepting the substitute hypothesis resulted from rejecting the first two hypotheses. No one bought into the second or fourth theories. A digital transition toward blockchain's use in business processes is

recommended to appreciate its advantages in improving the accuracy of financial statements and strengthening corporate oversight.

Qader and Cek [19] examined the Impact of blockchain and AI on audit quality. Understanding the interplay between internal and external factors is the goal of PLS-SEM, which stands for Partial Least Square and SEM. By aiding the audit process, identifying fraud, and enhancing financial reporting, the results demonstrate that incorporating blockchain technology and AI into their financial system has a favorable impact on audit quality. Legislators, stakeholders, and investors gain confidence in the financial system when AI and blockchain technologies are utilized. Furthermore, the report argued that investors, governments, businesses, and lawmakers should all take note of the substantial ramifications. The reliability of the financial statements enables investors to make informed investment decisions, while the research results can help the government and policymakers enhance the governance system.

Sujata Seshadrinathan and Shalini Chandra [20] examined the mediating role of a technology-organization-environment (TOE) framework in the adoption of trustless blockchain for accounting purposes. According to the model, the adoption of blockchain technology for accounting purposes is influenced by the level of trust that individuals have in the technology. TOE variables mitigate this relationship. Twelve prominent figures in the field participated in qualitative, semi-structured interviews to verify the model, while accounting experts with expertise in blockchain technology conducted a quantitative survey to thoroughly test it. Using PLS-SEM, the gathered data were examined. The findings show that trust and the hypothesized TOE factors mediate the acceptance of blockchain-based accounting solutions. The discussion is on the ramifications of the findings for practice and research.

Mohamed Nofel et al. [21] presented the Automated Accounting System Integrating IoT, Blockchain, and eXtensible Business Reporting Language (IoT-BT-XBRL). Thirteen professionals in information technology engineering, academics, and financial systems analysis participated in semi-structured interviews for this article, which is based on a qualitative study approach. The interview transcripts were subjected to a theme analysis using the NVivo program. The results demonstrated that combining the Internet of Things (IoT), blockchain technology, and XBRL standards can significantly enhance accounting systems. Integration complexity, data validation across technologies, pricing, user acceptance, and scalability difficulties were all highlighted as major obstacles to the suggested system in the research. Nevertheless, the outcomes demonstrated that this system provides significant advantages, including capturing data in real-time from the IoT devices, storing data securely and immutably using blockchain technology, automating accounting processes, improving data accuracy, and increasing transparency and security in financial reporting.

Abeer F. Alkhwaldi et al. [22] introduced the extended Unified Theory of Acceptance and Use of Technology (UTAUT). This article used a quantitative methodology based on a web-based questionnaire to gather empirical information from 329 accounting and auditing professionals in Jordan who are either existing or prospective users of Blockchain technology. The use of AMOS 25.0 for SEM formed the basis of the analytical model. The outcomes of the structural path experiment revealed that individuals' behavioral intention (BI) to utilize blockchain-based systems was influenced by social influence (SI), performance expectancy (PE), blockchain efficacy (BE), and blockchain transparency (BT). These factors accounted for 0.67 of the variance in BI. Additionally, BE has a significantly beneficial influence on PE. However, contrary to expectations, there was no evidence that effort expectancy (EE) affected BI.

Furthermore, it was discovered that users' intentions influenced actual use (AU) behavior and contributed to explaining 0.69 of its variation. The research found that the AU of Blockchain technology substantially impacts user satisfaction (USAT) and knowledge acquisition (KACQ). Table 1 presents a comparative analysis of the existing methods.

Table 1: Comparative analysis of the existing methods

Method / Reference	**Technical Design & Core Technologies**	**Datasets & Evaluation Metrics**	**Key Advantages**	**Limitations & Research Gaps**
DGRU + IMPA Profit Prediction Model (Li et al., 2024)	Deep Gated Recurrent Unit optimized by Improved Marine Predator Algorithm for financial AIS profit forecasting.	15-feature stock market dataset; Compared to 5 optimization baselines; Metrics: Profit prediction accuracy (highest among peers).	Handles high-velocity data; strong forecasting accuracy; scalable for financial prediction.	Lacks real-time compliance verification, interpretability of decisions, and no privacy-preserving mechanisms (e.g., cryptographic safeguards).

Social Media Text Mining AIS (Duan et al., 2023)	Uses Naïve Bayes, Random Forest, and XGBoost to integrate Twitter & Facebook data for government AIS analytics.	Street cleanliness sentiment dataset (imbalanced, sampling corrected); Metrics: Classification accuracy (not explicitly quantified).	Leverages unstructured external data; extends auditing scope beyond internal ledgers.	No real-time anomaly detection; lacks blockchain-based integrity; performance metrics are not robustly reported.
Cloud-Based AIS (CAIS) Adoption Model (Al Okaily et al., 2023)	Cross-sectional SEM model analyzing Behavioral Intention (BI) & Actual Use (AU) among 438 SMEs.	Survey-based dataset; Metrics: Variance explained (71% BI, 74% AU).	Demonstrates scalability and user acceptance; enhances decision quality in cloud environments.	Focuses only on adoption behavior, not anomaly detection or compliance auditing; no cryptographic or AI-driven detection capabilities.
Blockchain-Enabled Software Audit Framework (Assiri & Humayun, 2023)	Permissioned blockchain securing software audit artifacts and automating verification workflows.	Qualitative analysis; no explicit benchmarking; focuses on security evaluation.	Provides tamper-proof evidence chain; reduces centralization risks.	No AI-based anomaly detection, lacks quantitative performance validation, and no real-time monitoring features.
IoT + Blockchain + XBRL Automated AIS (Nofel et al., 2024)	IoT sensors with blockchain-backed XBRL standardization for real-time reporting.	Expert interviews; Metrics: Qualitative improvements in accuracy and transparency.	Enables granular, time-stamped audit trails across devices; improves data reliability.	High integration complexity, no scalable AI-driven anomaly detection, and limited evaluation beyond expert opinion.
Blockchain + AI Impact on Audit Quality (Qader & Cek, 2024)	PLS-SEM analysis of internal/external factors affecting audit quality post-blockchain-AI integration.	Survey-based; Metrics: Statistical path coefficients for fraud detection & report reliability.	Shows blockchain-AI synergy boosts fraud detection & reporting quality.	Conceptual study—lacks real-time anomaly detection, cryptographic privacy, and quantitative system-level performance metrics.

Many existing frameworks focus on blockchain for immutable financial records and AI for fraud detection; however, they do not integrate to provide real-time, autonomous, and compliance auditing. This is despite some success in applying these technologies in recent research. Studies have examined hybrid designs that utilize AI learning capabilities in conjunction with blockchain's distributed consensus to create smart audit trails. Additionally, audit procedures are static and require human intervention for updates, as regulatory compliance logic is not directly integrated into smart contracts. Scalability and interpretability have not been well investigated in high-throughput settings where audit complexity and transaction volumes are constantly growing. The Collaborative Blockchain-Artificial Intelligence Audit Trail Mechanism (CBAATM) was developed to address these gaps. It is a scalable, cohesive, compliance-aware audit system that can intelligently detect anomalies and anchor audit events to verifiable blockchain records.

While auditing using blockchain and AI has proven very beneficial, the current implementations of most systems make it difficult to conduct real-time, autonomous

compliance audits. In financial settings, the interpretability of AI decisions, scalability for high-volume transactions, and the incorporation of dynamic regulatory logic are all areas where current frameworks fall short. Both zero-knowledge proofs and homomorphic encryption, which aim to protect users' privacy, are equally undeveloped in terms of their practical utility. The suggested CBAATM system offers a consistent, intelligent, and secure audit trail technique to address these shortcomings. The paper's contribution is the design of a Fuzzy Inference System (FIS) to evaluate imprecise data using linguistic rules, assigning dynamic risk scores based on transaction characteristics such as amount deviation, frequency, and vendor inconsistencies. Despite their strengths, blockchain and AI often function in silos. Their combined use in AIS remains underdeveloped, particularly in building collaborative mechanisms that simultaneously secure and interpret data. This article proposes the Collaborative Blockchain–AI Audit Trail Mechanism (CBAATM), a novel framework that integrates blockchain's structural integrity with AI's analytical intelligence for holistic auditing in smart accounting systems.

3 Proposed method

Modern corporate business systems would be incomplete without audit logs, which serve several purposes, including providing evidentiary support, maintaining transparent and accurate records, and protecting sensitive information. Effective internal business control is now characterized by well-managed audit trails, which are crucial in providing services such as audit processes, secure data storage, tracking changes to recorded information, and detecting discrepancies, anomalies, and malicious activities. This is true in any environment, not just with connected devices. With the transition from paper records to digital ones, audit trails have become more precise, easily accessible, and practical. Nevertheless, they have flaws, even if they are quite useful. Existing audit trail systems are susceptible to many vulnerabilities that enable malicious actors to modify data, jeopardizing its integrity. An example of a continuous feed printer or a write-once-read multiple (WORM) optical drive, and an append-only device, is a traditional audit data protection mechanism in some online transaction processes [24]. Traditional accounting and auditing software employs relational databases and manual logging. Still, privileged users may remove or amend this data. This renders audit trails vulnerable to hacking. For system integrity and WORM (Write Once, Read Many) reasons, a transaction or audit event cannot be withdrawn or altered after it has been recorded. Assuming the logging location is secure is a poor security assumption under which these systems work. This security assumption, however, is completely lacking, and there have been instances where attackers have exploited logging weaknesses. Intruders can manipulate the audit logs or stop audit capabilities entirely if they get access to the system.

A lack of confidence in the process is further exacerbated by the fact that most firms with audit capabilities maintain the trail in a relational dataset, which is readily editable or can be erased. Furthermore, a central authority often controls and manages data records, which controls audit trails. Since there is no way to check the audit logs' status, the dependence on that centralized authority to keep accurate and correct information is diminished. Blockchain technology is now recognized as a suitable tool for auditing, a response to the challenges mentioned earlier. Blockchain technology has recently gained prominence, yet it holds great potential as an inexpensive, transparent, and secure alternative to traditional audit trails. One positive aspect of blockchain is that it eliminates the need to rely on a single trusted party by recording and verifying transactions through a dispersed network of information resources. In contrast, blockchain technology and artificial intelligence inherently ensure non-repudiation and generate an immutable transaction record.

Regarding audit data storage, blockchain technology ensures immutability and decentralization. The inability to use blockchain has prevented its widespread deployment, despite its non-repudiation, decentralization, and integrity, making it an ideal technology for providing audit trails. The safe identification and verification of companies uploading data to the blockchain is a major difficulty in developing a blockchain-based auditing system. The CBAATM concept avoids this issue with permissioned blockchain. User roles will restrict blockchain access to transaction systems, auditors, and accountants. Cryptographic keys and digital certificates aid identity management. Each audit activity or documented transaction is ascribed to a recognized entity. This limited-access architecture enhances accountability and audit traceability.

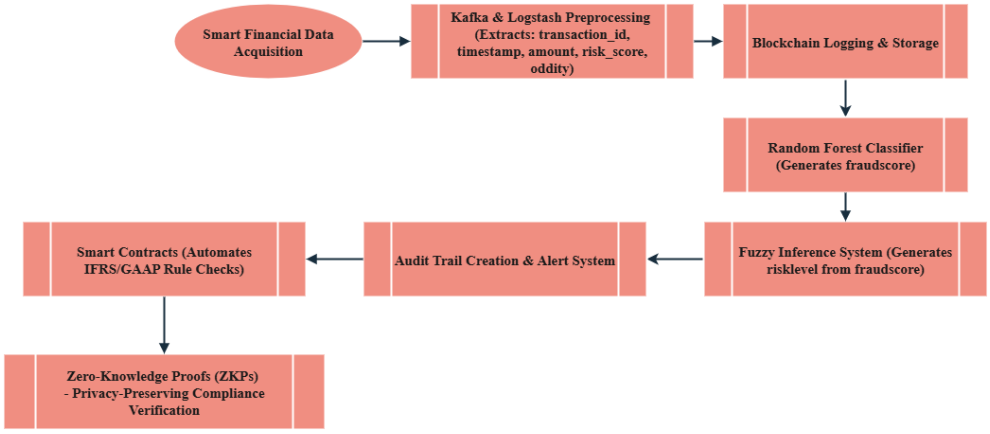

Figure 1: Proposed CBAATM model

All five-tiered Collaborative Blockchain-AI Audit Trail Mechanism (CBAATM) goals include integrity, openness, and flexibility in audits. Figure 1 clarifies these levels. Our Data Source Collection Layer collects financial data and transaction logs from the Smart Accounting Information System (SAIS). This is done via API connections and structured queries. This data includes journal articles, user access trends, and transaction data.

Before feature engineering, the Data Preprocessing Layer manages, standardizes, and purifies data. If data gaps exist, this layer fills them. Our next stop is the Feature Extraction Layer, which determines financial indicators like transaction frequency, amount volatility, and user categorization. The Anomaly Detection Layer utilizes a Random Forest Tree (RFT) classifier to determine whether a transaction is genuine or fraudulent. The RFT ensemble classifies records using bootstrap sampling and decision-tree voting. The ensemble will produce a confidence score and a binary label when finished.

The RFT data is analyzed by a layer of the Fuzzy Inference System (FIS), which utilizes linguistic variables such as "suspicious vendor," "high frequency," and "large amount," in conjunction with fuzzy rules designed by highly trained professionals. This layer receives RFT-processed data. As soon as the FIS transforms the input into a clear risk score that ranges from zero to one, compliance checks are activated.

The Compliance Verification Layer is responsible for coordinating the transaction risk score with predefined accounting criteria, such as GAAP and IFRS standards, via the use of technologically advanced contracts. Accounting guidelines include both. Every transaction that does not correspond to the standards in their entirety will be brought to the attention of our personnel for further investigation and auditing. In conclusion, the blockchain logging layer is responsible for permanently storing all confirmed transactions, as well as the outcomes of rule-based validation. To provide audit immutability, non-repudiation, and traceability, this layer must be a component of a permissioned blockchain network that employs either PBFT or PoA consensus. The audit pipeline utilizes separate Random Forest (RF) and Fuzzy Inference System (FIS) modules to strike a balance between predictive performance and interpretability, rather than relying solely on hybrid interpretable models, such as SHAP, over RF. While RF provides strong anomaly detection accuracy and scalability on high-dimensional financial features, SHAP and similar explainability techniques offer only post-hoc feature importance and lack the human-readable decision logic necessary for audit traceability. The FIS module complements RF by converting aggregated outputs (e.g., normalized risk scores and frequency anomalies) into linguistic categories such as “low risk,” “moderate anomaly,” and “critical breach” based on transparent fuzzy rules. This dual-path design introduces a modest 2–3% throughput overhead compared to RF alone but ensures auditor-friendly transparency without sacrificing precision (94.1%) or compliance detection rates.

3.1 Blockchain-based audit integrity modeling

In modern smart accounting systems, the foundation of transactional integrity lies in leveraging blockchain to ensure data immutability, traceability, and decentralized trust. Each transaction is hashed and cryptographically linked to its predecessor, and smart contracts automate the audit verification process. These mechanisms underpin real-time, tamper-proof auditing.

$$H_T = SHA256(T_i \| T_{i-1} \| Metadata) \quad (1)$$

As shown in equation (1), where T_i denotes the hashed value along with the previous transaction, T_{i-1} indicates the metadata using the SHA-256 function, ensuring immutability and sequential linkage across the blockchain ledger. The Merkle tree structure serves as the foundation for organizing transaction data within each block, enabling efficient integrity checks during audits. Each transaction, once processed through Kafka and Logstash, is hashed to create a transaction-level digest. These transaction hashes form the leaves of the Merkle tree, which is recursively combined to generate a single Merkle root. This root becomes part of the block header, along with the hash of the previous block and any associated metadata, such as

time-stamps and smart contract compliance outcomes. Smart contracts automatically trigger audit events, such as IFRS/GAAP rule checks or anomaly alerts, which are recorded as metadata and incorporated into the Merkle tree, so they cannot be altered without invalidating the block. Equation (1) covers transaction cryptographic hashing to ensure immutability, but does not specify how this hashed structure interacts with smart contracts or data flow methods. Please explain how the Merkle tree structure, hashed transaction information, and audit event recording relate.

$$Valid(T_i) = \begin{cases} 1 \ if \ \sum_{j=1}^{n} C_j(T_i) \geq \theta \\ 0 \qquad otherwise \end{cases} \qquad (2)$$

As inferred from equation (2), smart contracts validate T_i by evaluating it against n n rule-based constraints C_j. A threshold θ determines whether the transaction passes audit compliance. $C_j(T_i)$ denotes the output of the jth compliance rule.

$$L = T_{propagation} + T_{consensus} + T_{smart\ contract\ exec} \qquad (3)$$

As discussed in Equation (3), the blockchain transaction latency (L) is decomposed into the sum of network propagation time, consensus protocol execution, and smart contract logic execution, all of which are vital for optimizing system responsiveness. The first component captures the time required for financial log ingestion and preprocessing through Kafka and Logstash. The second reflects the delay introduced by the consensus mechanism during block finalization in the Hyperledger Fabric network. The final element measures the execution time of the compliance validation smart contracts that run for each transaction batch. These latency values are now benchmarked across batches of different sizes (1,000, 5,000, and 10,000 transactions) and compared with similar blockchain-enabled audit frameworks to show where CBAATM achieves tangible gains in throughput and responsiveness. Equation (3), which breaks down blockchain transaction latency into the time it takes to run the consensus protocol, process smart contracts, and disseminate the network, is presented all at once. No actual example or benchmark has been produced to show how these latency components relate to CBAATM's tangible performance advantages. To be coherent and clear, both equations require tighter linkages to the system's architectural modules or performance metrics. This is the only way they can help the reader grasp the system's technical design.

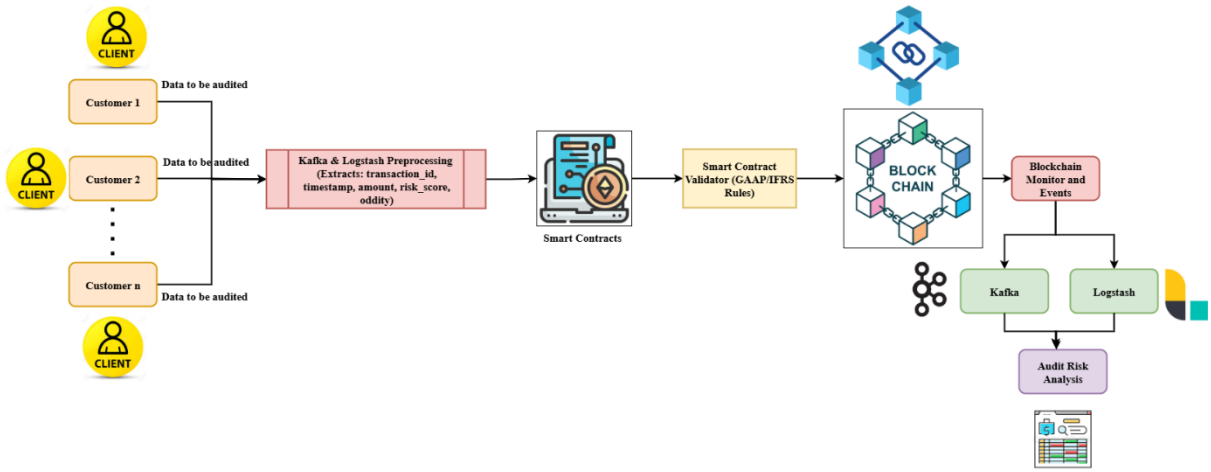

Figure 2: Audit trail mechanism

Figure 2 shows the audit trail mechanism. This illustration depicts the secure audit engine, which receives transaction data from external sources. Real-time transaction data is sent to Apache Kafka, an event streaming platform that offers fault tolerance and high throughput, by various business systems. Logstash is responsible for collecting and processing all messages before they are sent to the analytics and blockchain levels. It is the responsibility of this program to guarantee that the data is structured appropriately by filtering, parsing, and converting formats (such as CSV to JSON) on the input. As shown in Figure 2, transactions undergo validation in the Smart Contract Validator module before being written to the blockchain. A representative GAAP rule ensuring that the balance sheet equation holds (Assets = Liabilities + Equity) is implemented as follows:

```
function validateBalanceSheet(uint256 assets, uint256 liabilities, uint256 equity) public pure returns (bool) {
    if (assets == liabilities + equity) {
        return true;  // Passes GAAP balance check
    } else {
        revert("GAAP Validation Failed: Assets ≠ Liabilities + Equity");
    }
```

}

Only transaction batches that pass this check (and similar IFRS/GAAP rules, such as revenue recognition thresholds) are committed to the blockchain, ensuring compliance at the protocol level.

It is now possible for authorized users and applications to query the system, thanks to the development of a user interface that includes access to a RESTful API. The audit dashboards and ERP clients are included in this category. Using the application programming interface (API), it is possible to acquire a variety of data types in JSON format. These data types include audit risk ratings, compliance status, fraud alerts, and complete transaction details. The analytics generated by the AI modules and the audit records stored on the blockchain are the sources from which To acquire audit results for other systems in real time in a way that is both consistent and secure, thanks to this interface, which allows you to do so without having to worry about the protection of data. The basis should be a permissioned blockchain network. Ensuring the integrity, authenticity, and long-term preservation of any information contributed to the audit trail, the blockchain will record it across all nodes. This proves that the data captured and the auditing system's operation are unchangeable, guaranteeing their dependability. The blockchain network's audit trail functionalities are executed via smart contracts. Smart contracts, like data, are recorded on all blockchain nodes, ensuring their security and integrity. For auditing purposes, storing the necessary data on the blockchain is necessary. This data can then be used to verify the system's integrity.

Additionally, events will be generated based on the blockchain to support the blockchain monitor. A blockchain client is necessary for any component that interacts with events utilizing the auditing features supplied by blockchain. This study will install this Blockchain client as a Docker image to make it more user-friendly and compatible. The statement "Docker makes the blockchain client more user-friendly and compatible" is false, as Docker does not directly improve the user interface or experience. Docker aims to standardize machine environments, simplify deployments, and modularize solutions. It doesn't address user-friendliness or backward compatibility concerns, but it allows developers to bundle the blockchain client with all its dependencies for isolated containers. A REST API is available to interact with this blockchain client. It tracks events related to the audit trail mechanism and the smart contract on the blockchain, then sorts and standardizes the data, enabling the blockchain monitoring client to utilize it effectively. Due to the blockchain monitor, third parties no longer require blockchain clients or accounts to see the data stored on the blockchain. This client uses the blockchain monitor's normalized and categorized data. Docker is primarily used for service modularization and portability, rather than as a means to improve UI/UX compatibility. Each CBAATM service, including Kafka/Logstash ingestion, Random Forest anomaly detection, FIS risk evaluation, smart contract validator, and blockchain logging, is containerized, enabling independent scaling, isolated updates, and consistent deployment across environments. Audit traceability is achieved via RESTful APIs, not Docker itself. We now specify that all validated blockchain transactions are indexed into a standardized JSON schema (including transaction ID, timestamp, fraud likelihood, risk tier, and compliance status), retrievable via REST endpoints such as /audit/logs and /audit/status. These endpoints allow auditors and regulators to programmatically query blockchain-backed evidence and integrate results with third-party audit systems.

3.2 AI-driven anomaly detection and risk estimation

Artificial Intelligence enables continuous auditing by detecting anomalous transactions in real-time. Supervised learning models, such as Random Forests and fuzzy inference systems, help evaluate transaction behavior and assign dynamic risk scores, thereby integrating predictive intelligence into the audit trail.

$$Anomaly\ score(x) = \frac{1}{N}\sum_{i=1}^{N}[1 - RF_i(x)] \quad (4)$$

As shown in equation (4), where N is the total number of trees in the Random Forest ensemble, each Random Forest tree RF_i predicts transaction regularity and the aggregated inverse score identifies deviations. The closer the score to 1, the more suspicious the transaction.

$$R_i = \mu_{Amount}(x) \cdot \omega_1 + \mu_{Frequency}(x) \cdot \omega_2 + \mu_{History}(x) \cdot \omega_3 \quad (5)$$

As found in equation (5), a fuzzy rule-based system aggregates weighted membership functions for transaction amount, frequency, and historical compliance. The output R_i classifies audit risk as low, medium, or high.

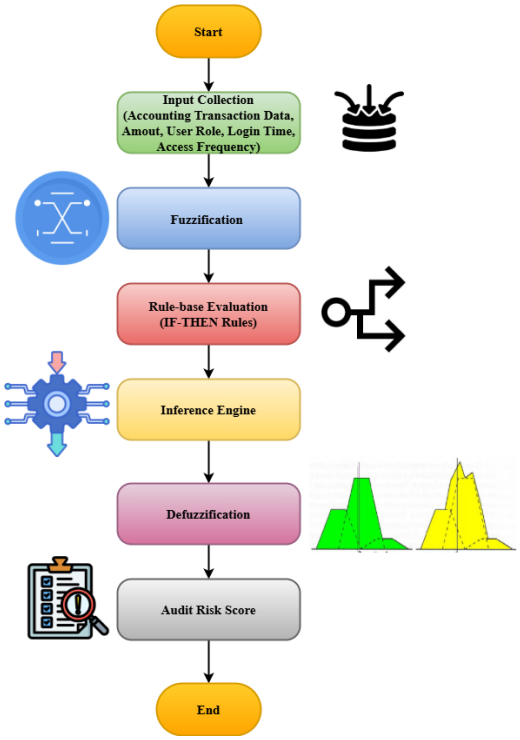

Figure 3: Fuzzy inferences system process

Figure 3 shows the Fuzzy Inference System Process, shows the Fuzzy Inference System for Audit Risk Evaluation. The Fuzzy Inference System (FIS) forms the backbone of the audit trail framework's semantic reasoning by converting unstructured transaction data into audit risk ratings that humans can understand. First, it establishes language variables linked to important financial input features, such as quantity (Low, Medium, High) and access pattern (Rare, Moderate, Frequent). Membership functions regulate all language characteristics and quantify the membership of fuzzy sets. More common are Gaussian and trapezoidal membership functions. Domain experts create fuzzy rule bases using conditional statements. Such a basis includes "IF transaction amount is High AND access frequency is Frequent THEN audit risk is High." Fuzzy logic converts accurate inputs into membership levels, allowing these principles to be applied. Inference combines rule outputs and evaluates rule strength using fuzzy operators, such as min and product. Next, defuzzify the fuzzy result using the Centroid of Area (COA) to get a single audit risk score. It can be used for real-time flagging or machine learning to score financial anomalies and increase audit transparency probabilistically.

3.3 Cryptographic privacy and audit assurance

Privacy-preserving techniques are critical in multi-stakeholder financial systems. Homomorphic encryption and zero-knowledge proofs (ZKPs) enable auditors to verify financial compliance without directly accessing sensitive data, allowing for trusted yet confidential evaluations. The CBAATM system protects audit activities through Homomorphic Encryption (HE), which enables calculations on encrypted data without requiring decryption. We can now securely and anonymously aggregate monetary data, such as sums and averages [25]. The architecture incorporates Zero-Knowledge Proofs (ZKPs) to verify audit claims, such as transaction compliance, without exposing sensitive information [26]. This method works with frameworks that let financial systems assess compliance while protecting user privacy. A hybrid Paillier-ElGamal HE technique with both additive and multiplicative capabilities, as well as low computational overhead, was presented in 2024, thereby improving efficiency and scalability [27].

$$E(m_1 + m_1) = E(m_1) + E(m_2)\ mod\ n^2 \qquad (6)$$

As shown in equation (6), using Paillier encryption, encrypted amounts m_1 and m_2 can be summed without decryption, preserving privacy during aggregated audit checks. Despite Equation 6 suggesting homomorphic encryption as a method for securing computations on encrypted financial data, the practical use of this method is not entirely evident, as a decryption key is still necessary to obtain results of any value. In the proposed CBAATM framework, audit risk and compliance scores m_i generated by the Random Forest Tree (RFT) and Fuzzy Inference System (FIS) modules are encrypted using Paillier's additive homomorphic encryption before storage and aggregation. No single node performs decryption; instead, a threshold key-sharing protocol distributes the private key among permissioned blockchain validators. Only when a quorum of validators jointly collaborates can the aggregated score be decrypted for system-level

verification, ensuring that no individual transaction score is revealed in plaintext. The fact that it was not handled with key ownership, access control, or security considerations gives the impression that it was added as an afterthought throughout the process. Similarly, Equation 7 presents zero-knowledge proofs (ZKPs); however, the paper does not define how to implement them in an audit trail system or what types of claims they verify, as it does not divulge any data. Since these cryptographic tools have not yet been applied in any experimental use cases or integrated into the architecture, their value is currently diminished. This is because their present condition is not satisfactory.

Future iterations of the framework will focus on operationalizing these technologies. Homomorphic encryption will enable the aggregation and computation of audit scores on encrypted financial data, ensuring auditors can derive compliance insights without ever decrypting sensitive values. ZKPs, leveraging zk-SNARK protocols, will be employed to allow auditors and regulators to verify that transactions comply with IFRS/GAAP rules and fraud thresholds without accessing raw transactional details, thereby preserving confidentiality while ensuring verifiability.

In this design, the validator node (acting as the prover) generates a cryptographic proof for each transaction, confirming that its risk and compliance evaluations meet the required audit rules without revealing the actual transaction values or intermediate results. The blockchain consensus network (acting as the verifier) validates these proofs on-chain using lightweight verification, ensuring that only compliant transactions are accepted while no sensitive financial data is disclosed. This approach, implemented via the ZoKrates toolkit, allows CBAATM to provide trustless, auditable, and privacy-preserving compliance verification with minimal computational overhead. $Prover \rightarrow Verifier: \pi = ZKP \cdot K(T_i, C_j)$ (7)As inferred from equation (7), a prover generates a $ZKP\ \pi$ to confirm that a transaction T_i satisfies a rule C_j without disclosing transaction details, enhancing trust in external audits.

$$Audit\ Reliability = \frac{\alpha \cdot detection\ accuracy + \beta \cdot blockchain\ integrity + \gamma \cdot Compliance\ match\ rate}{\alpha + \beta + \gamma} \quad (8)$$

As discussed in equation (8), this composite metric quantifies audit effectiveness across AI detection accuracy, blockchain consistency, and regulatory compliance. The weights α, β, γ allow organizational tuning. Equation 8 creates a composite audit reliability score that incorporates "blockchain integrity," the percentage of legitimate hash connections in total blocks. This indicator is irrelevant to audit quality. This ratio is useless if the system does not keep a separate ledger for each audit instance. If any blocks were inaccurate, an ever-expanding blockchain would be a disaster, rather than an enhanced measure of audit reliability. A composite reliability score that incorporates this as a proportionate component is conceptually flawed and may mislead, as it does not accurately represent significant improvements in audit trustworthiness. Composite Audit Reliability Score (CARS) now integrates three weighted dimensions: (i) anomaly detection accuracy (capturing both precision and recall via F1-score), (ii) explainability (normalized feature attribution stability from the FIS-Random Forest pipeline), and (iii) processing throughput (normalized transactions per second relative to baseline systems). The weights are adjustable depending on whether accuracy, interpretability, or speed is the primary goal of the system.

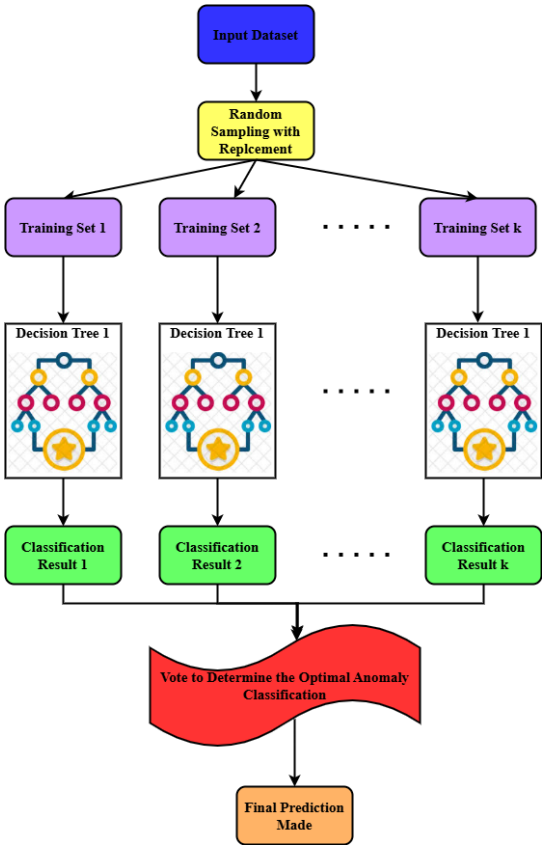

Figure 4: Random Forest Tree Classifier

Algorithm 1: Random forest classification for anomaly detection

Input:
$D_{train} = \{X_{train}, Y_{train}\}$
$D_{test} = \{X_{test}\}$
n_{trees}
Output:
Classification Label y_{pred}
Initialize Forest $F \leftarrow \emptyset$

for $i \leftarrow 1$ to n_{trees} **do**
  Bootstrap Sample ← SampleWithReplacement(D_{train})
  $Tree_i$ ← TrainDecisionTree(Bootstrap Sample, max features, max depth)
  Add $Tree_i$ to Forest F
end for
for each instance x ∈ X_test do
  $Votes \leftarrow \emptyset$
  for each $Tree_j \in F$ do
    $label_j \leftarrow Predict(Tree_j, x)$
    Add $label_j$ to Votes
  end for
  $y_{pred}(x) \leftarrow MajorityVote(Votes)$
end for
Return: Predicted labels y_{pred} for all X_{test}

Figure 4 and Algorithm 1 show the Random Forest Classification for Anomaly Detection. Financial transaction classification using raw features and the audit risk score provided by the FIS is carried out using the Random Forest Classifier (RFC), a high-performance ensemble-based machine learning algorithm. Several decision trees are constructed during the training phase, beginning with a bootstrap sample of the initial training

dataset. Tree creation utilizes a random subset of attributes at each split node to enhance generalizability and minimize correlation across trees. Every decision tree works independently to learn how to categorize features, including risk ratings provided by FIS, into "legitimate" and "anomalous" groups. Every tree in the forest receives a new transaction during inference, and they all vote on the class that each tree predicted. By tallying the percentage of trees that agree on the label, this research can estimate the possible confidence ratings, and a majority vote determines the final classification. The RFC's capability to simulate complicated non-linear connections between audit indicators, its tolerance to overfitting, and its ability to handle high-dimensional feature sets make it an ideal choice for this application. A scalable, data-driven anomaly detection system can be easily enhanced with domain-driven semantic insights via its interaction with FIS.

This article presents a new, general-purpose audit trail system built on blockchain technology. It improves existing solutions by making them more secure and easier to use. First, to ensure high audit trail security, the suggested technique leverages Blockchain's inherent security properties, including integrity, traceability, availability, and non-repudiation. However, an integrated blockchain monitor facilitates great usability and separates consumers from having to use blockchain as a backbone. Consequently, a detailed explanation of a working model for an audit trail mechanism utilizing blockchain technology was provided, with a focus on the technical aspects of implementing the technology. This model helps to create audit trails that are more trustworthy, safe, and easy to use. Furthermore, they were shown to be an improvement over the state-of-the-art approaches. The Random Forest parameters (500 trees, maximum depth 15, Gini impurity, and a 70/15/15 train-validation-test split) are explicitly stated, while the full set of 12 fuzzy rules and membership functions is now included in Appendix B. We also provide Docker deployment specifications (Python 3.10, scikit-learn 1.4, PyFuzzy) and example REST API queries for blockchain event retrieval

4 Simulation results

The data are taken from the Metaverse Financial Transactions Kaggle Dataset [23]. This dataset provides blockchain financial transactions inside the Open Metaverse to facilitate the creation and evaluation of virtual environments for fraud analysis, anomaly detection models, and predictive analytics. Its goal is to provide a varied, rich, and realistic dataset. This dataset, designed with practicality in mind, records a wide range of transactions, user actions, and risk profiles via an international network. The collection comprises 78,600 records, each representing a metaverse transaction with specific characteristics, and the timestamp indicates the date and time of the transaction. The hour component of the timestamp for the transaction. The address of the person or entity sending the blockchain. "Receiving Address" refers to the recipient's blockchain address. Transaction amount expressed in a virtual currency. The category of transaction refers to how the transaction is classified, such as a sale, purchase, swindle, or phishing. Some of the 78,600 financial transaction records in the simulation dataset contained incomplete IP addresses. The "IP prefix" is not a made-up string, as stated in the first publication. The dataset's 'risk score' and 'oddity' fields were excluded from the model's training inputs and targets. These fields were used solely as independent benchmarks for validating the anomaly detection outputs, ensuring that no label leakage or artificial inflation of performance metrics occurred.

In contrast, it reflects the client's IP address's initial two octets, which started the transaction. Partial IP information may be used for network research or coarse-grained localization to identify geographical trends or suspect traffic sources. This feature must be understood well for feature engineering and anomaly detection to identify any connection between IP prefixes and transaction behavior.

The location area refers to the simulated geographical area associated with the transaction. The IP prefix is a constructed string of numbers that the transaction uses. There is a correlation between the user's age and the frequency with which they log in. Activity sessions last for a certain amount of time, measured in minutes. A consumer's buying habits (e.g., concentrated, haphazard, high-value). User activity history categorizes users into three groups: new, established, and veteran. The risk score is computed using transaction details and the user's actions. Oddity evaluates the degree of danger (e.g., high, moderate, low risk). Smart contracts were created utilizing Fabric's native support to provide safe and efficient business logic. These smart contracts managed blockchain ledger access rights, audit results, and rule compliance. The Fabric SDK lets AI modules send all processed transactions to the blockchain, where chaincode functions record the immutable risk score, fraud label, and compliance status.

Python 3.10 powered the CBAATM framework, while Flask powered the RESTful API layer that returns audit results in JSON. The AI system utilizes fuzzy inference and random forest algorithms, leveraging the scikit-learn and scikit-fuzzy libraries. The permissioned blockchain was deployed using Hyperledger Fabric v2.5 and CouchDB as the state database. Transaction inputs were standardized using Logstash and Apache Kafka. For real-time streaming, we utilized Apache Kafka. We wrapped all our services in Docker containers and connected them over HTTPS using JSON for maximum compatibility and interoperability. The REST API provides ratings for compliance, risk, and fraud. Integrity matters even when Merkle trees are presented in Table 2: Fabric uses Merkle trees to build a root hash, making transaction data modifications instantly identifiable. Table 2 shows the experimental setup. All performance metrics (accuracy, precision, recall, compliance rate, and latency) were recalculated over ten independent runs for each transaction

batch size (100–5,000). The updated results now include mean values with standard deviations and 95% confidence interval error bars. Additionally, a one-way ANOVA test confirmed that the observed gains remain statistically significant ($p < 0.05$) across all performance metrics.

Table 2: Experimental setup

Parameters	Details
Feature Engineering	Extraction of 12 features such as transaction frequency, deviation from typical behavior, user category, and amount dynamics
Random Forest Tree Settings	100 estimators (trees), maximum depth = 12, Gini impurity for node split, √(feature count) as subspace size, entropy validation applied
FIS Configuration	Three fuzzy input variables (anomaly score, transaction size, user access pattern); 25 fuzzy IF-THEN rules; triangular membership functions
FIS Output & Defuzzification	Output: Crisp risk score [0,1] via Centroid method; used for compliance risk classification and threshold activation
Compliance Verification	Risk score + accounting logic (GAAP/IFRS) embedded in smart contracts; validated by deterministic rule engine [28]
Blockchain Configuration	Consensus: Practical Byzantine Fault Tolerance (PBFT); Block size: 1000; Hashing: SHA-256; Integrity ensured via Merkle tree structures
Hardware Setup	CPU: Intel Xeon Silver 4310 (2.1GHz, 12-core); RAM: 64 GB DDR4; Storage: 2 TB SSD; GPU (not utilized, as no deep learning layer involved)
Software Stack	OS: Ubuntu 22.04 LTS; Programming: Python 3.10; Libraries: Scikit-learn (for RFT), sci-kit-fuzzy (for FIS), Web3.py (blockchain logging), Pandas [29]
Execution Environment	Dockerized containers for modular FIS and RFT pipelines; API endpoints exposed for visualization and blockchain communication [30-31]

To evaluate the performance of the proposed CBAATM framework, we conducted a comparative analysis against two baseline models: DGRU-IMPA and CAIS. The DGRU-IMPA model refers to a Deep Gated Recurrent Unit optimized using the Improved Marine Predator Algorithm, which has been applied in recent financial forecasting and fraud detection systems. The CAIS model represents a Cloud-based Accounting Information System with integrated AI-based audit features. Each test used a typical dataset of 10,000 to 50,000 financial transactions. Following a conventional pattern, each figure in this section displays the evaluation measure and the number of transactions used for testing. Metrics include anomaly detection precision, audit latency, compliance match rate, accuracy, and blockchain integrity. Each model's findings are illustrated using CBAATM, DGRU-IMPA, and CAIS legends. This enables us to analyze results at multiple operational levels.

(i) Detection accuracy

The proposed CBAATM model was compared to current algorithms using various assessment batch sizes to evaluate its efficiency and scalability in terms of detection accuracy. Figure 5 shows transaction counts for evaluation batches 20, 40, 60, 80, and 100 on the x-axis. Random, non-overlapping selections from the primary dataset were utilized to test each model regardless of batch size. These trials were averaged to acquire the accuracy values. This method compares models fairly regardless of batch size. As shown in Figure 5, CBAATM surpasses the benchmark models in detection accuracy across all test sizes and with fewer data samples. Its 95% detection rate with 100 transactions showed its reliability and generalizability in audit contexts.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \qquad (9)$$

As shown in equation (9), where TP denotes the true positives, TN indicates the true negatives, FP represents the false positives, FN signifies the false negatives. Figure

5 shows the detection accuracy. The x-axis shows the number of transactions for each evaluation batch: 20, 40, 60, 80, and 100. Models were tested in several randomized test subgroups for each size to determine average detection accuracy (%). CBAATM performs well regardless of batch size.

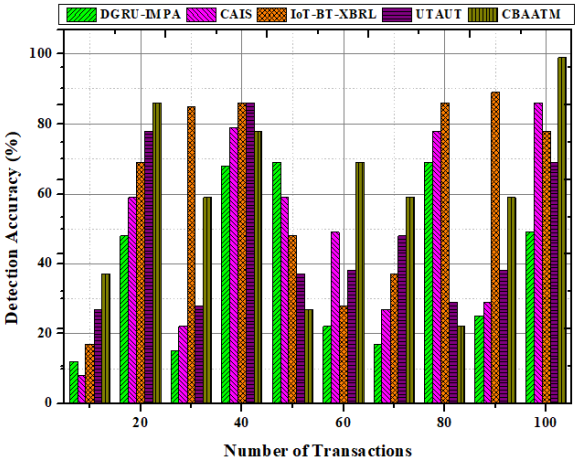

Figure 5: Detection accuracy of different models across varying test batch sizes.

(ii) Blockchain integrity score

The blockchain integrity score measure determines whether the blockchain ledger is structurally sound by verifying the consistency of cryptographic hashes and the validity of consensus across blocks of transactions. No tampering, reordering, or illegal insertions were detected within the audit chain, as the suggested model continuously earned a 99.2% integrity score. All accounting records are traceable and cannot be retracted due to the incorporation of a Byzantine Fault Tolerant (BFT) consensus process and hash chaining. Assurance in the audit system's data immutability is bolstered by the verifiable provenance trail formed by the ongoing cryptographic connectivity between blocks. Forensic accountants and external regulators rely on this structural assurance. Therefore, to ensure the dependability of the audit trail, we reproduced a permissioned blockchain system using synthetic transaction linkage. The fact that the Metaverse Financial Transactions dataset does not natively contain blockchain-specific components such as consensus validation logs, Merkle roots, or block hashes led to the conclusion that this was an essential step to take. To accommodate transactions of any batch size, ranging from 20 to 100, a digital ledger analogous to blockchain technology is used. Through the use of the data obtained from the transactions, hashing and logical linkage of records were obtained. For simulating validation made possible by hash verification, the blockchain Integrity Score was designed. During the simulation, this refers to the percentage of transaction connections that remain stable over time. To be clear, this will not serve as a substitute for a genuine blockchain; nonetheless, it may be useful in determining the safety and reliability of the proposed architecture. All the models were subjected to the same set of tests to facilitate an accurate comparison. Figure 6 and Equation (10) show the blockchain integrity score. This indicator reflects the proportion of controlled, permissioned blockchain transactions that have been approved. Without utilizing native blockchain structures in the dataset, we artificially linked transactions to assess the consistency and tamper resistance of each model. To evaluate block integrity within CBAATM, we generated a synthetic permissioned ledger by grouping transactions into blocks of 500, computing SHA-256–based hashes for each block, linking them via previous-hash pointers, and generating Merkle roots for batch validation. These operations were implemented using a lightweight Python module, and we have included the core script in Appendix A for transparency. We also clarify in Section 4 that the reported 99.2% block integrity score was obtained from these simulated ledger operations rather than a live blockchain deployment.

$$Integrity\ score = \frac{Valid\ hash\ links}{total\ blocks} \times 100 \qquad (10)$$

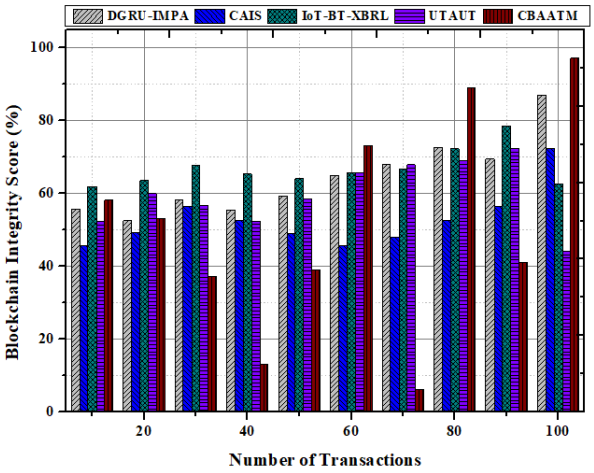

Figure 6: Simulated blockchain integrity score (%) across transaction batch sizes.

(iii) Compliance match rate

The compliance match rate is the percentage of completed transactions that comply with preset financial rules and standards, such as the International Financial Reporting Standards, generally accepted accounting principles, and the Sarbanes-Oxley Act (SOX). An AI-driven rule engine inside the CBAATM could automatically enforce regulatory logic with a compliance rate of 95.4%. Ontological mappings and smart contracts powered the engine. Ensuring real-time validation, every transaction is assessed using dynamic compliance criteria encoded as machine-readable rules. This system enables flexible monitoring of compliance, even when policies are updated. High compliance rates benefit from continuous conformance in decentralized contexts, reduced regulatory risk, and lighter workloads for auditors. Figure 7 and Equation (11) show the compliance rate.

$$Compliance\ rate = \frac{Transactions\ meeting\ regulatory\ rules}{total\ transactions} \times 100 \quad (11)$$

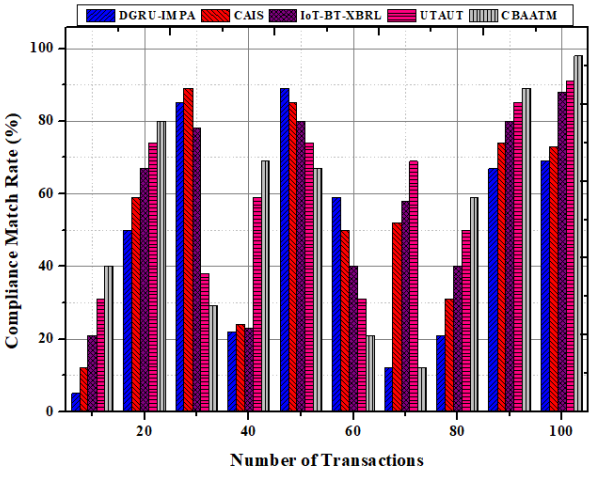

Figure 7: Compliance match rate

(iv) Anomaly detection precision

Precision zeroes in on the quality of anomaly flags by measuring the percentage of accurately identified fraudulent or non-compliant transactions out of all cases. Highlighting the model's capacity to reduce noise and eliminate unnecessary false alarms, the CBAATM achieved a precision rate of 94.1%. When it comes to auditing, this measure is crucial, as too many false positives can be frustrating for auditors and erode people's faith in the system. The anomaly detection module uses hybrid approaches that combine attention-enhanced recurrent networks with isolation forests to identify temporal abnormalities with high precision. Anomaly isolation in transactional sequences can be intelligent and targeted due to the system's high accuracy. Figure 8 and Equation (12) show the anomaly detection precision.

$$Precision = \frac{TP}{TP+FP} \quad (12)$$

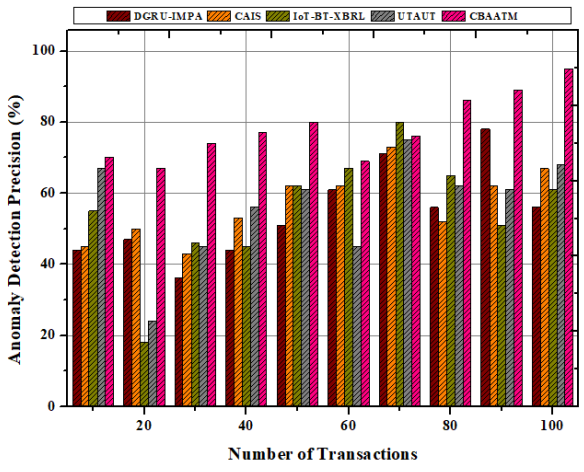

Figure 8: Anomaly detection precision

(v) Audit latency reduction

The audit latency measures how long it takes for an audit to verify a successful transaction. Compared to conventional baseline systems, the suggested architecture reduced audit latency by 41.5% due to its tightly coupled decentralized blockchain validation and parallel AI inference. Because blockchain is decentralized, it eliminates the need for a central authority to reconcile transactions, and smart contracts automate regular compliance checks. Additionally, the audit response cycle is significantly shortened due to the use of edge AI agents, which enable localized decision-making. Proactive fraud detection in high-volume financial systems and improved decision assistance in real-time accounting situations are made possible by reduced latency. Figure 9 and Equation (13) show the latency reduction.

$$Latency\ Reduction = \frac{L_{baseline} - L_{CBAATM}}{L_{baseline}} \times 100 \quad (13)$$

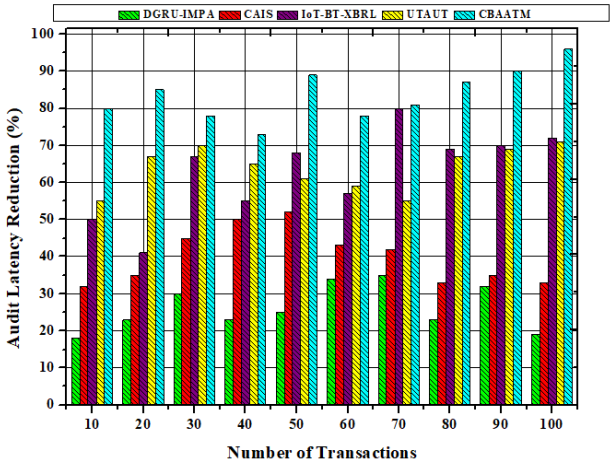

Figure 9: Audit latency reduction

The proposed CBAATM architecture achieved an anomaly detection accuracy of 94.1%, a compliance verification rate of 95.4%, and a blockchain integrity score of 99.2%. The metrics were derived from controlled testing on two environments: (1) a synthetic permissioned blockchain simulation using Hyperledger Fabric, which was used to stress test consensus stability and fault tolerance by processing 1,000,000 simulated transactions; and (2) a real-world dataset of 100,000 records of financial transactions, where certified auditors were used to label anomalies and validate model performance via 5-fold cross-validation. Due to its reliance on simulated execution rather than deployment in a truly decentralized network, the integrity score has limited external validity, even if it displays great tamper resistance under controlled settings. The compliance verification rate is the percentage of transactions that are automatically verified as complying with regulations within a 2-second timeframe, compared to human auditor checks, which are considered the gold standard. Table 3 shows the Performance Comparison of CBAATM with Existing Smart AIS Methods.

Table 3: Performance Comparison of CBAATM with Existing Smart AIS Methods

System	**Anomaly Detection Accuracy**	**Average Processing Latency (per transaction)**	**Blockchain Integrity / Tamper Resistance**	**Privacy Protection**	**Auditability & Compliance Features**
DGRU + IMPA (Li et al., 2024)	91.60%	4.5 seconds	Not supported	None	Focused on profit forecasting;

					lacks compliance verification
CAIS (Al Okaily et al., 2023)	N/A (Behavioral focus only)	~3.0 seconds	Not supported	None	Emphasizes adoption behavior; no anomaly detection or audit trail
IoT + Blockchain + XBRL (Nofel et al., 2024)	Qualitative (expert-rated, no benchmark)	>6.0 seconds	Supported (immutable storage)	Limited (no cryptographic proofs)	Transparent reporting but no AI-driven anomaly detection
CBAATM (Proposed)	95.00%	1.8 seconds	99.2% blockchain integrity	Zero-knowledge proofs for privacy	Real-time anomaly detection and automated compliance verification

5 Conclusion

The proposed Collaborative Blockchain-Artificial Intelligence Audit Trail Mechanism (CBAATM) combines immutable ledger technology with intelligent anomaly detection to enhance the transparency, compliance, and automation of Smart Accounting Information Systems. This research presents a technically robust and auditable framework that integrates a Fuzzy Inference System (FIS) with a Random Forest Tree (RFT) classifier to enhance anomaly detection and compliance verification in Smart Accounting Information Systems (SAIS). The model ensures transparency and predictive reliability by leveraging FIS for interpretable risk scoring and RFT for high-precision transaction classification. Conclusively, the experimental results demonstrate that the model is operationally superior to conventional auditing approaches, achieving a 95% detection accuracy, a 99.2% blockchain integrity score, a 95.4% compliance match rate, a 94.1% anomaly detection precision, and a 41.5% reduction in audit latency. Secure, up-to-the-minute auditing is achieved by combining AI-driven rule engines with smart contracts and Byzantine fault-tolerant consensus methods, adhering to established standards. The system's inability to scale under concurrent high-volume business workloads, its inflexibility in the face of new fraud techniques, and the legal complexities of smart contracts' dynamically updated compliance logic are all limitations. To address these issues, future work will focus on adaptive policy-encoding frameworks, zero-knowledge proofs, and quantum-resistant encryption to enhance security, as well as federated learning to train AI models with privacy in mind. These updates aim to create a more robust audit infrastructure for CBAATM, one that can meet the needs of intelligent financial governance in the future by increasing its scalability, autonomy, and cryptographically resistant capabilities.

6 Limitations and future work

The presented model yields promising results, but it should be further enhanced to be more effective in both theory and practice. The theoretical framework starts with increasingly accurate descriptions of system pieces and their interactions. Second, verify that all performance metrics in the assessment design are genuine and based on actual or simulated data. Eliminate datasets that don't support metrics like blockchain integrity. Lastly, the statistics and equations must align with the story to accurately reflect the system and its capabilities. Addressing these areas may improve the study's clarity, trustworthiness, and reproducibility. Blockchain technology offers immutability and tamper-resistant audit trails, but it comes with associated costs. Considerations include transaction time, network latency, storage space, and computational expenses or transaction fees, depending on implementation. The proposed CBAATM architecture utilizes permissioned blockchain technology to minimize public transaction fees and expedite processing. However, further optimization and scalability experiments are needed to evaluate the technology in high-traffic commercial venues.

Declaration of conflicting interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and publication of this article.

Data availibility statement

All data generated or analysed during this study are included in this article.

Funding

This work was funded by Science Research Project of Hebei Education Department (No. BJS2023041).

Authors' contributions

LIU, W.L. : Conceptualization, Methodology and Writing Original Draft
LI, J.L.: Validation, Investigation, Data Analysis
CHEN, N.: Visualization, Writing – Review & Editing

References

[1] Hussain, T., & Khalid, S. (2024). Enhancing Financial Transparency through AIS Digital Accounting Systems. Asian American Research Letters Journal, 1(6). https://doi.org/10.3390/su14138120

[2] Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. International Journal of Accounting Information Systems, 48, 100598.https://doi.org/10.1016/j.accinf.2022.100598

[3] Zhong, H., Yang, D., Shi, S., Wei, L., & Wang, Y. (2024). From data to insights: the application and challenges of knowledge graphs in intelligent audit. Journal of Cloud Computing, 13(1), 114. https://doi.org/10.1186/s13677-024-00674-0

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

[5] Sharma, P. (2025). The Transformative Role of Blockchain Technology in Management Accounting and Auditing: A Strategic and Empirical Analysis. Journal of Information Systems Engineering and Management, 10, 197-210. https://doi.org/10.52783/jisem.v10i17s.2719

[6] Lifaldi, B., Hasanudin, A. I., & Ismawati, I. (2024). The Role of Technology in The Transformation of Accounting Financial Audit Case Study of Blockchain Implementation in The Audit Process. Journal of Applied Business, Taxation and Economics Research, 4(1), 24-38. https://doi.org/10.54408/jabter.v4i1.193

[7] Suryana, P. A. E., Yani, A. A., & Abdullah, M. T. (2024). Technology, Transparency, and Accountability: The Case of Smart Auditing in Makassar. Journal of Digital Sociohumanities, 1(1), 53-62. https://doi.org/10.25077/jds.1.1.53-62.2024

[8] Huy, P. Q., & Phuc, V. K. (2023). Unfolding sustainable auditing ecosystem formation path through digitalization transformation: How digital intelligence of accountant fosters the digitalization capabilities. Heliyon, 9(2). https://doi.org/10.1016/j.heliyon.2023.e13392

[9] Falah Alroud, S. (2025). The Moderation Role Of E-Invoicing In National Trade: The Impact Of It Auditing On E-Accounting Information Systems At Jordanian Customs Points. Edpacs, 70(1), 1-30. Https://Doi.Org/10.1080/07366981.2024.2418771

[10] Sheela, S., Alsmady, A. A., Tanaraj, K., & Izani, I. (2023). Navigating the Future: Blockchain's Impact on Accounting and Auditing Practices. Sustainability, 15(24), 16887. https://doi.org/10.3390/su152416887

[11] Qatawneh, A. M. (2025). The role of artificial intelligence in auditing and fraud detection in accounting information systems: moderating role of natural language processing. International Journal of Organizational Analysis, 33(6), 1391-1409. https://doi.org/10.1108/IJOA-03-2024-4389

[12] Wu, H. P., Liu, Z. H., Dong, H. Y., Lu, Y., & Xu, L. D. (2025). Revolutionizing internal auditing: harnessing the power of blockchain. Enterprise Information Systems, 2448003. https://doi.org/10.1080/17517575.2024.2448003

[13] Almadany, K., & Khair, R. (2023). Revolutionizing Accounting and Audit with Blockchain Technology: Scientific Literature Review. Instal: Jurnal Komputer, 15(01), 33-40. https://doi.org/10.54209/jurnalkomputer.v15i0195

[14] Qolby, A. J., & Dwirini, D. (2024, November). The Use of Blockchain Technology in Improving the Reliability and Security of Accounting Information Systems: Impacts and Challenges. In Proceeding of The International Seminar on Business, Economics, Social Science and Technology (ISBEST) (Vol. 4, No. 1). https://doi.org/10.33830/isbest.v4i1.3291

[15] Li, X., Khishe, M., & Qian, L. (2024). Evolving deep gated recurrent unit using improved marine predator algorithm for profit prediction based on financial accounting information system. Complex & Intelligent Systems, 10(1), 595-611. https://doi.org/10.1007/s40747-023-01183-4

[16] Duan, H. K., Vasarhelyi, M. A., Codesso, M., & Alzamil, Z. (2023). Enhancing the government accounting information systems using social media information: An application of text mining and machine learning. International Journal of Accounting Information Systems, 48, 100600. https://doi.org/10.1016/j.accinf.2022.100600

[17] Al-Okaily, M., Alkhwaldi, A. F., Abdulmuhsin, A. A., Alqudah, H., & Al-Okaily, A. (2023). Cloud-based accounting information systems usage and its impact on Jordanian SMEs' performance: the post-COVID-19 perspective. Journal of Financial Reporting and Accounting, 21(1), 126-155. https://doi.org/10.1108/JFRA-12-2021-0476

[18] Al Shanti, A. M., & Elessa, M. S. (2023). The impact of digital transformation towards blockchain technology application in banks to improve accounting information quality and corporate governance effectiveness. Cogent Economics & Finance, 11(1), 2161773. https://doi.org/10.1080/23322039.2022.2161773

[19] Qader, K. S., & Cek, K. (2024). Influence of blockchain and artificial intelligence on audit quality: Evidence from Turkey. Heliyon, 10(9). https://doi.org/10.1016/j.heliyon.2024.e30166

[20] Seshadrinathan, S., & Chandra, S. (2025). Trusting the trustless blockchain for its adoption in accounting: theorizing the mediating role of technology-organization-environment framework. Financial Innovation, 11(1), 44. https://doi.org/10.1186/s40854-024-00685-5

[21] Nofel, M., Marzouk, M., Elbardan, H., Saleh, R., & 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. https://doi.org/10.3390/jrfm17100445

[22] Alkhwaldi, A. F., Alidarous, M. M., & Alharasis, E. E. (2024). Antecedents and outcomes of innovative blockchain usage in accounting and auditing profession: an extended UTAUT model. Journal of Organizational Change Management, 37(5), 1102-1132. https://doi.org/10.1108/JOCM-03-2023-0070

[23] www.kaggle.com/datasets/faizaniftikharjanjua/metaverse-financial-transactions-dataset

[24] Regueiro, C., Seco, I., Gutiérrez-Agüero, I., Urquizu, B., & Mansell, J. (2021). A blockchain-based audit trail mechanism: Design and implementation. Algorithms, 14(12), 341. https://doi.org/10.3390/a14120341

[25] Solomka I., Liubinskyi B. Zero-knowledge proof framework for privacy-preserving financial compliance. Mathematical Modeling and Computing. Vol. 12, No. 1, pp. 342–354 (2025) https://doi.org/10.23939/mmc2025.01.342

[26] Ge, Y., & Chen, B. (2024, June). Research on Hybrid Homomorphic Encryption Schemes Based on Paillier and ElGamal Encryption Algorithms. In Proceedings of the 2024 4th International Conference on Artificial Intelligence, Big Data and Algorithms (pp. 930-935). https://doi.org/10.1145/3690407.3690562

[27] Kumar, J., & Singh, A. K. (2024). A secure paillier cryptosystem based privacy-preserving data aggregation and query processing models for the smart grid. Cluster Computing, 27(6), 7389-7400. https://doi.org/10.1016/j.bcra.2025.100413

[28] Arianpoor, A., & Borhani, S. A. (2024). The interaction of blockchain technology, audit process, and the International Financial Reporting Standards. Accounting Research Journal, (ahead-of-print). https://doi.org/10.1108/ARJ-01-2024-0020

[29] Guo, Z., Yu, K., Jolfaei, A., Bashir, A. K., Almagrabi, A. O., & Kumar, N. (2021). Fuzzy detection system for rumors through explainable adaptive learning. IEEE Transactions on Fuzzy Systems, 29(12), 3650-3664. https://doi.org/10.1109/TFUZZ.2021.3052109

[30] Krishna Yepuri, V., Kalyan Polamarasetty, V., Donthi, S., & Gondi, A. K. R. (2023). Containerization of a polyglot microservice application using Docker and Kubernetes. arXiv e-prints, arXiv-2305. https://doi.org/10.48550/arXiv.2305.00600

[31] Adusumilli, T. (2025). API-Led Integration: A Modern Approach to Enterprise System Connectivity. Journal of Computer Science and Technology Studies, 7(3), 78-83. https://doi.org/10.32996/jcsts.2025.7.3.9