FABA
Finance, Accounting and Business Analysis
ISSN: 2603-5324

Finance, Accounting and Business Analysis
Volume 8 Issue 1, 2026
http://faba.bg/
ISSN 2603-5324
DOI: https://doi.org/10.37075/FABA.2026.1.06
Check for updates

Blockchain Applications in Occupational Fraud Prevention: A Structured Literature Review

Praise Mutoko[1*], **Ephraim Monde Faku**[2]

Tshwane University of Technology, Pretoria, South Africa[1]
Tshwane University of Technology, Soshanguve, South Africa[2]
* Corresponding author

Info Articles

History Article:
Submitted 23 September 2025
Revised 12 April 2026
Accepted 8 May 2026

Keywords:
Occupational Fraud; Blockchain Technology; Auditing; Company Finance; Financial Enterprises

JEL: M4, O3, G3

Abstract

Purpose: The purpose of this study is to examine how blockchain technology can mitigate occupational fraud in financial service enterprises within emerging markets, with a particular focus on mid-sized institutions in South Africa.

Design/Methodology/Approach: A systematic literature review was conducted using Scopus and ScienceDirect databases. Peer-reviewed articles published between 2016 and 2025 were selected through predefined inclusion and exclusion criteria. The review followed PRISMA 2020 guidelines, and thematic analysis was applied to synthesise findings from 36 studies.

Findings: The review revealed that weak internal controls continue to drive occupational fraud, especially corruption, asset misappropriation, and financial statement fraud. Blockchain offers advantages such as real-time auditability and improved transaction traceability. However, regulatory uncertainty, integration costs, and heightened cybersecurity requirements remain barriers to widespread adoption.

Practical Implications: The findings suggest that blockchain can complement existing fraud risk management systems by enhancing organisational transparency, accountability, and operational resilience. Financial service providers in emerging markets can benefit from integrating blockchain within context-specific regulatory and technological frameworks.

Originality/Value: This study contributes to the growing body of knowledge on blockchain and fraud prevention by focusing on its applicability to financial institutions in emerging economies. In this context, empirical research remains limited.

Paper Type: Research Paper

* Address Correspondence:
E-mail: praisemutoko84@gmail.com[1]
FakuEM@tut.ac.za[2]

INTRODUCTION

Occupational fraud is a significant problem across financial service organisations worldwide, including in emerging economies such as South Africa. Occupational fraud refers to fraudulent acts by insiders or employees within an organisation, including the misappropriation of assets, corrupt practices, and account manipulation (Association of Certified Fraud Examiners(ACFE) 2022). These unethical behaviours not only reduce the operating effectiveness of financial firms but also lower investor confidence, hindering sustainable growth and economic progress (PwC 2022). The current extended abstract provides detailed reviews of the available literature that examines the drivers, characteristics, and consequences of occupational fraud in financial services firms, particularly in South Africa. In addition, this article discusses the role that blockchain technology can play as an agent in changing the design of fraud prevention practices in such organisations. Accordingly, this study is guided by the following research question: What is the role of blockchain technology in disrupting occupational fraud in financial service enterprises?. Blockchain technology can serve as an agent that changes how fraud-prevention practices are designed within such organisations. Accordingly, this study is guided by the following research question: What is the role of blockchain technology in disrupting occupational fraud in financial service enterprises?

LITERATURE REVIEW

A review of the current literature includes numerous studies on occupational fraud in financial institutions, which highlight issues such as asset misappropriation, corruption, and fraudulent financial reporting. The literature indicates that internal control flaws, a lack of effective corporate governance structures, and a poor understanding of fraud risks are significant determinants of fraudulent acts (Alagha and Özçelik 2025; Byeon et al. 2025). Moreover, resource shortages, coupled with the volatile nature of financial markets, often make traditional, resource-intensive anti-fraud initiatives such as audits and regulatory announcements less effective against the ever-changing nature of fraud (ACFE 2022).

The lack of effective deterrents promotes an environment of impunity, which in turn leads to the spread of fraudulent schemes and undermines trust in the sector (Singh et al. 2025). In this assessment, the Fraud Triangle model is used, which outlines three key factors leading to occupational fraud: pressure, opportunity, and rationalisation (Cressey 1953). The model is used as a basis for considering how weaknesses in organisational structure, ineffective governance arrangements, and unhelpful regulatory climates create an environment in which fraudulent activity is prone to occur.

Understanding financial services

Financial services businesses are essential to the world economy. They offer crucial financial management systems and products, such as banking, insurance, investments, and financial technologies (fintech). These businesses facilitate everything from small-scale financial infrastructure, such as stock markets and international payments, to larger-scale operations, such as savings and loans. Because of their significance, they are intricately linked to trust, development, and economic stability.

Definitions of financial services enterprises appear neither uniform nor fully articulated. In South Africa, several studies extend conventional SME classifications. Fatoki (2014) defines medium-sized financial enterprises by employee count (2–50 employees). Koppeschaar (2012) uses an IFRS for SMEs framework, while Stainbank (2010) grounds the definition in corporate legal reforms. Other South African studies omit explicit criteria.

Internationally, variations emerge in sector-specific practice. Mwega (2011) categorises banks as small, medium, or large based on size and competitiveness, and Pearce and Helms (2001) define financial services associations as shareholder-based entities operating at a community level. Beck and Cull (2014) offer broader perspectives, with no detailed criteria, leaving definitions implicit.

Collectively, the studies indicate that definitions rely on general SME frameworks, supplemented in some cases by sector-specific adjustments, rather than on clear financial thresholds or uniform size criteria. For this study, Medium-sized financial services companies will use the definition by Fatoki (2014), which is a range of 2-50 people.

Financial services firms are frequently targets of fraud, embezzlement, and cybercrime due to their significance. The stakes are enormous not only for the businesses but also for the people and economies that rely on them. They are, therefore, a crucial area of study for security and fraud prevention.

According to recent studies, blockchain technology can be used to detect fraudulent activity and improve the security of financial transactions. For instance, Sen et al. (2024) solve a fundamental problem in fraud prevention by introducing a blockchain-based federated learning system that identifies fake data in financial contexts. Khan et al. (2025) propose a blockchain forensic approach that enhances traceability and

evidence preservation in financial organisations, with a focus on preventing loan scams through blockchain technology.

Recent research indicates that blockchain technology can be applied to enhance the security of financial transactions and identify fraudulent conduct. For example, Nair and Rao (2025) introduce a blockchain-based federated learning system that detects fraudulent data in financial contexts, thereby resolving a key issue in fraud prevention. Vasudevan et al. (2025), who focus on financial crime investigations involving embezzlement, suggest a blockchain forensic technique that enhances traceability and evidence preservation in financial institutions.

Occupational Fraud in Financial Services

Occupational fraud is defined as the misuse of one's role within an organisation for personal gain through the deliberate misapplication of resources or assets. This continues to evolve in complexity as financial systems become more digitised (Association of Certified Fraud Examiners 2022). For this study, the focus will be on Corruption, Asset Misappropriation, and Financial Statement Fraud.

Corruption

Fraud in financial services continues to undermine institutional integrity, with corruption among the most prevalent forms of occupational fraud. As defined by the ACFE (2022), corruption involves employees abusing their positions of trust for personal gain, typically through bribery, conflicts of interest, or embezzlement. Okewale et al. (2025) emphasise that corruption is deeply embedded in operational systems, particularly within financial services institutions, and therefore necessitates context-specific internal control mechanisms. Similarly, Byeon et al. (2025) argue that integrating governance, risk management, and compliance (GRC) systems supported by high-quality internal audits and strong leadership can significantly enhance the detection and prevention of corruption within state-owned enterprises.

Alagha and Özçelik (2025) extend the conversation to insider fraud in the UK policing system, revealing that corruption and asset misappropriation remain dominant due to systemic oversight weaknesses. In the South African context, the Financial Intelligence Centre (2024) and the National Money Laundering Risk Assessment (2024) highlight ongoing risks, including the misuse of shell companies and illicit financial flows, which disproportionately affect SMEs. These challenges are compounded by limited access to affordable finance (Zarpala and Casino 2021) and persistent energy infrastructure issues, which, according to Kroon et al. (2021), create regulatory blind spots and foster environments conducive to corruption.

Asset Misappropriation

Asset misappropriation is widely recognised as the most common form of occupational fraud globally, involving schemes where employees steal or misuse an organisation's resources for personal benefit (ACFE 2022). The Association of Certified Fraud Examiners reports that this category accounts for 86% of occupational fraud cases worldwide. However, it typically results in lower financial losses per incident than corruption or financial statement fraud. Nonetheless, its frequency makes it a critical concern, particularly in emerging economies such as South Africa.

This type of fraud includes a range of activities such as payroll fraud, cash theft, billing schemes, skimming, inventory theft, and expense report falsification (Wells 2017). In South Africa, independent audits by leading professional services firms such as PwC, Deloitte, EY, and KPMG have highlighted that medium-sized financial enterprises remain vulnerable to these schemes. The challenges are often linked to inadequate internal controls, insufficient segregation of duties, and governance weaknesses, which create opportunities for occupational fraud to flourish (PwC 2022).

Multiple studies have highlighted the structural and behavioural drivers of asset misappropriation and have identified poor internal controls, collusion, lack of oversight, and weak ethical cultures as major contributors. In South Africa, high unemployment, poverty, and social inequality. This is compounded by lax enforcement and delayed prosecution, which reduce deterrence and increase vulnerability to internal fraud (Transparency International 2025: Ziorklui, Nwachukwu, and Okafor 2024).

Globally, asset misappropriation is not limited to poorly governed sectors. Zhang et al. (2025) note that even in highly regulated environments, small and medium-sized enterprises (SMEs) often fall victim due to informal processes and over-reliance on trust. Similarly, Khan et al. (2021) stress that in local government contexts, without tailored internal control systems, such fraud remains difficult to detect and prevent

Despite these developments, a significant challenge persists in the uneven application of anti-fraud measures. Under-resourced entities, such as non-profits and SMEs, often lack skilled personnel, robust audit systems, or sufficient donor support to implement effective fraud mitigation strategies. This leaves them exposed to long-term undetected losses, with broader implications for economic stability and organisational sustainability.

Financial Statement Fraud

Though less common than other types of fraud, financial statement fraud (FSF) causes the highest financial losses, with median losses nearing $1 million and typical durations extending to 18–24 months (ACFE 2022). FSF involves intentional misrepresentation to mislead stakeholders and is particularly prevalent in finance and operations departments (Mongwe and Malan 2020). Its impact on investor confidence and corporate sustainability has led to growing academic interest.

Research highlights motivations such as meeting financial targets and personal gain, often underpinned by Cressey's (1953) Fraud Triangle: pressure, opportunity, and rationalisation. This framework remains relevant across contexts (Homer 2020). South African studies, such as those by Mongwe and Malan (2020), emphasise additional contextual drivers, such as weak oversight and structural gaps in governance.

The consequences of FSF include financial collapse, reputational damage, and erosion of market trust, as seen in cases like Enron, WorldCom, and Steinhoff (Mongwe and Malan 2020). Traditional controls, such as audits and segregation of duties, are proving insufficient against complex fraud schemes. Thus, attention has shifted toward machine learning (ML) techniques, such as artificial neural networks, support vector machines, and autoencoders, which can identify anomalous patterns in financial data (Mongwe and Malan 2020).

Global studies continue to explore the broader determinants of financial statement fraud. For example Ding, Huang and Wang (2022) find that greater gender diversity in leadership correlates with lower incidence of financial statement fraud. Indiraswari, Subekti and Rosidi (2025) link financial distress with a higher risk of FSF, while ACFE (2022) highlights that although FSF occurs less frequently than other types of occupational fraud, the financial losses it causes can be significantly larger. Shanikat and Aldabbas (2025) further confirm that strong corporate governance practices play a critical role in reducing fraud risk, especially in emerging markets. While AI-driven tools show promise in fraud detection, their success in South Africa hinges on contextual adaptation, and research must prioritise accessible, interpretable systems compatible with local constraints to bridge the gap between innovation and real-world application (Sreenu and Verma 2024).

Theoretical Framework

Source: (Fraud Conference News 2026)
Figure 1. The Fraud Triangle

Recent research has deepened our understanding of occupational fraud by exploring its root causes, the environments in which it thrives, and strategies to prevent it. A cornerstone in this field is Cressey's Fraud Triangle, which explains fraud as arising when pressure, opportunity, and rationalisation come together. However, Tickner et al. (2021) challenge the model's practical value, arguing that while it is helpful as a basic framework, its simplicity may fall short in capturing the complex dynamics of real-world fraud cases.

Studies have also shown that cultural and contextual factors significantly shape how occupational fraud manifests. Chung et al. (2021), drawing on Hofstede's cultural dimensions, reveal that national culture influences both the likelihood and impact of fraud. Their work suggests that any effective fraud prevention strategy must take cultural norms and values into account. In a related study, Darsono et al. (2024) explore how the COVID-19 pandemic intensified fraud risks in the Financial Services sector, showing that factors

such as pressure, opportunity, rationalisation, and capability interacted in new ways, particularly by enabling asset misappropriation.

Organisational context plays a key role. Bruwer and Petersen (2022) examine South African SMMEs and find that perceptions of fraud risk are closely tied to management practices and financial stability. Their research underscores the role of leadership awareness in building fraud-resistant organisations. Similarly, Bakar et al. (2023) report that in Malaysian SMMEs, strong internal controls, an ethical corporate culture, and fraud awareness significantly reduce the likelihood of occupational fraud, supporting the idea that governance and ethical leadership are vital in limiting opportunities for fraud.

METHODS

This research utilised a systematic literature review (SLR) methodology to investigate how the adoption of sustainable technologies influences business growth and long-term sustainability in emerging markets. To maintain a clear and rigorous review process, the study followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, which offer a standardised framework for ensuring transparency, consistency, and completeness in reporting systematic review findings (Page et al. 2021; Sarkis-Onofre et al. 2021).

Search Strategy

This study conducted a comprehensive literature search across Scopus and ScienceDirect, chosen for their comprehensive indexing of high-quality, peer-reviewed literature across multidisciplinary fields relevant to this study, including technology, finance, and business. The Boolean queries that were implemented, respectively, were:

Blockchain AND Fraud AND Financial AND Service AND NOT Health AND NOT Cryptocurrency AND NOT AI AND NOT Supply Chain

Blockchain AND Technology AND Financial Services NOT Supply Chain NOT Cryptocurrency NOT Healthcare

The Boolean NOT was used in the research to refine and specify the kinds of research most suitable for the current study, having observed that the most common areas of research were blockchain within the supply chain and the cryptocurrency space. The time frame was restricted from **2016 to 2025**, reflecting Scopus's availability from 2016 onward and the marking period when blockchain began gaining traction beyond cryptocurrencies and was increasingly explored in business and finance contexts. Diagram 1 below summarises the search:

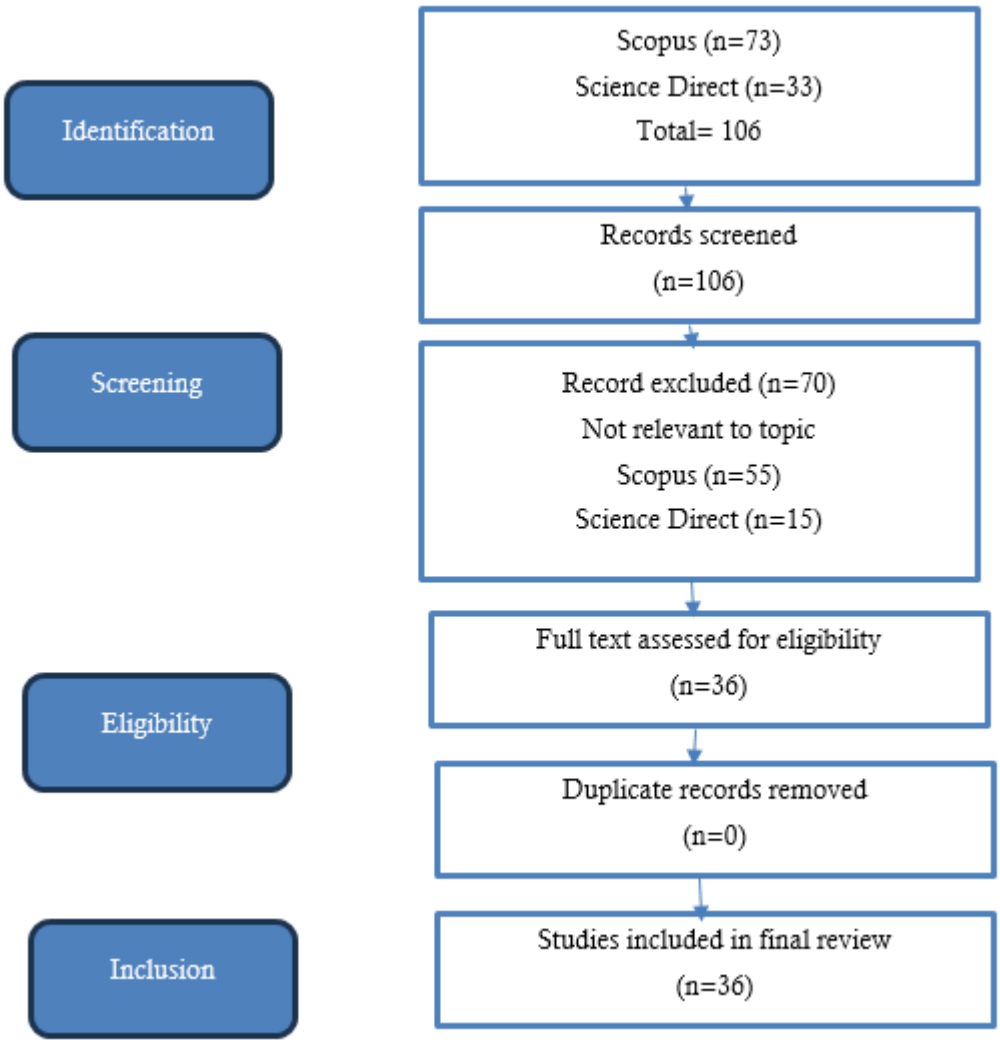

Figure 2. Search Strategy Diagram

Eligibility Criteria

To maintain methodological rigour and thematic focus, this review included a mixture of empirical and conceptual peer-reviewed studies relevant to blockchain applications in occupational fraud prevention. The following criteria were applied:

Inclusion:

• Peer-reviewed systematic, narrative, or integrative reviews addressing blockchain, fraud detection/prevention, and business/enterprise applications.
• Empirical studies (e.g., case studies, experiments);
• Conceptual, editorial, or opinion pieces;
• Indexed in Scopus and Science Direct
• Published in English between 2016 and 2025.

Exclusion:

• Grey literature (e.g., white papers, blogs);
• Studies not addressing the intersection of blockchain, fraud, and business;
• Duplicate records or papers with inaccessible full text.

Study Selection and PRISMA Flow

The initial queries returned 106 records. After removing duplicates, titles, and abstracts underwent screening, resulting in 36 full-text reviews. Ultimately, 36 articles met the inclusion criteria. This process follows the four-stage PRISMA flow: Identification, Screening, Eligibility, and Inclusion.

Data Extraction and Synthesis

Data were extracted into a structured matrix covering author(s), year, review type, blockchain

application, fraud focus, business context, methodology, and key findings. The data synthesis adopted thematic analysis to identify patterns, research gaps, and practical implications for financial services enterprises.

Risk of Bias and Quality Assessment

In alignment with PRISMA 2020 recommendations (Page et al., 2021), this review assessed potential bias and methodological quality across the included studies. However, given that the review exclusively included secondary research, namely, systematic, narrative, and integrative literature reviews. Formal critical appraisal tools such as AMSTAR 2 or ROBIS were not systematically applied.

To mitigate bias, the review applied a series of safeguards. First, inclusion was limited to peer-reviewed articles indexed in Scopus and ScienceDirect, databases known for their comprehensive and quality-controlled indexing (Singh et al. 2020). This ensured that only studies with a minimum standard of academic rigour were evaluated. Second, grey literature, opinion pieces, and conceptual papers were excluded to minimise subjectivity and unsupported assertions.

While formal scoring was not conducted, articles were screened for methodological transparency, the depth of analysis, and relevance to the core themes of blockchain and occupational fraud. Similar to the approach recommended by Sarkis-Onofre et al. (2021), the clarity of the review objectives informed the thematic synthesis, the use of structured data collection or synthesis frameworks, and the relevance to fraud prevention in financial service enterprises.

Nevertheless, this approach does not eliminate all sources of bias. Publication bias may still exist, particularly in favour of reviews reporting successful blockchain implementations. Additionally, language restrictions (English-only) and database limitations could lead to the exclusion of regionally significant literature, particularly from non-English speaking emerging markets (Visser et al. 2020).

Future reviews should consider applying structured critical appraisal tools to increase transparency and facilitate reproducibility. Moreover, integrating empirical studies could provide deeper insights into the effectiveness of real-world blockchain implementations in fraud prevention.

Limitations

This study relies on the Scopus and ScienceDirect databases, which, although comprehensive and multidisciplinary, may omit domain-specific or emerging literature indexed in other databases such as IEEE Xplore or Google Scholar. As a result, relevant publications outside Scopus and Science Direct's indexing criteria, particularly in the fields of blockchain engineering or forensic accounting, may have been excluded.

Additionally, only English-language articles were considered, potentially excluding valuable regional studies, especially from non-English-speaking countries that may offer context-specific insights into fraud and blockchain adoption.

A further limitation stems from the decision to include only review articles. While this approach ensures conceptual breadth and synthesised findings, it excludes empirical studies and case-specific implementations that could provide practical insights into real-world fraud detection systems in financial enterprises. This may limit the granularity of insights into operational, technological, or regional implementation challenges.

To mitigate some of these constraints, backwards and forward citation tracking was employed where applicable to identify influential works that might have been missed in the initial search.

RESULTS AND DISCUSSION

The study outlines several key factors that cause occupational fraud in financial institutions, and there are various ways of dealing with the issues as discussed below:

Weak Internal Controls

Many organisations continue to rely on internal audit and control systems that are fragmented or insufficiently integrated into digital transaction environments, limiting their effectiveness in detecting and preventing fraud in a timely manner (Alagha and Özçelik 2025). Prior research emphasises that fraud risk management (FRM) fundamentally depends on the design and enforcement of robust internal control and assurance mechanisms, particularly in technology-driven financial systems (Turker and Bicer 2020; Nathan and Jacobs 2020). In this context, audit trails, continuous monitoring, and system-level accountability mechanisms play a critical role in strengthening organisational oversight and governance (Alagha and Özçelik 2025; Albaroodi and Anbar 2025).

However, as financial transactions become increasingly digital and decentralised, traditional control mechanisms alone are often inadequate. Recent studies show that fraud in blockchain-enabled and fintech environments increasingly manifests through smart contracts, transaction manipulation, and system-level vulnerabilities, which require more advanced, technology-enabled detection approaches (Zarpala and

Casino 2021; Liu et al. 2022; Nikkel 2020). This has shifted FRM from a purely procedural control function toward a more data-driven and forensic-oriented discipline embedded within digital financial infrastructures (Zarpala and Casino 2021; Liu et al. 2022).

Within this evolving landscape, blockchain-based systems are increasingly viewed as a structural enhancement to internal control environments due to their immutability, transparency, and auditability, which strengthen both preventive and detective controls (Turker and Bicer 2020; Nathan and Jacobs 2020). Nevertheless, adoption and effective use of such technologies remain uneven across financial institutions and enterprises, particularly in emerging and developing contexts, where organisational, technical, and governance barriers persist (Neves et al. 2023; Jha and Dangwal 2024). This reinforces the need to view fraud risk management not only as a control function, but as an integrated socio-technical system combining governance, auditing, and digital infrastructure design.

Blockchain As a Disruptive Force

Given the limitations inherent in conventional anti-fraud mechanisms, the literature increasingly positions blockchain technology as a structural departure from traditional control and assurance models in financial systems. Across studies, blockchain-based infrastructures are shown to offer key features such as transparency, immutability, and decentralised verification, which strengthen the reliability, traceability, and auditability of financial records and significantly constrain the possibility of undetected data manipulation (Turker and Bicer 2020; Nathan and Jacobs 2020; Alagha and Özçelik 2025; Singh et al. 2025). These characteristics enhance both the credibility of financial transactions and the integrity of accounting information by embedding verification mechanisms directly into transaction processes (Turker and Bicer 2020; Nathan and Jacobs 2020).

From a fraud risk management perspective, the reviewed literature indicates that the ability of blockchain to provide a permanent, auditable, and shared ledger makes it particularly suitable for addressing problems related to fraudulent misrepresentation, corruption, and asset misappropriation in digital financial environments (Zarpala and Casino 2021; Liu et al. 2022; Vasudevan et al. 2025; Okewale et al. 2025). Several studies further suggest that blockchain should not be viewed as a substitute for governance and internal control systems, but rather as a technological layer that reinforces their effectiveness by embedding accountability and verifiability directly into financial infrastructures (Turker and Bicer 2020; Nathan and Jacobs 2020; Albaroodi and Anbar 2025).

Empirical and design-oriented contributions also illustrate the practical relevance of these arguments. For example, Khan and Ahmad (2025) demonstrate how blockchain can be integrated with Internet of Things technologies in loan-processing environments to reduce document manipulation, identity fraud, and internal interference. Similarly, Vasudevan et al. (2025) and Trivedi (2023) show that blockchain-based frameworks for cheque processing and document verification enhance the integrity of transactional records and reduce opportunities for occupational fraud. Studies focusing on anomaly detection and forensic analysis further indicate that blockchain environments support more effective, technology-enabled fraud detection mechanisms when combined with advanced analytics and monitoring techniques (Liu et al. 2022; Sen et al. 2025; Nikkel 2020; Zarpala and Casino 2021).

More broadly, the literature suggests that as financial systems become increasingly digital and interconnected, fraud risk management must evolve from predominantly procedural control mechanisms toward integrated, technology-enabled, and forensic-oriented architectures embedded within transaction infrastructures (Nikkel 2020; Zarpala and Casino 2021; Liu et al. 2022; Hyvärinen et al. 2017). However, adoption remains uneven, particularly in emerging and developing contexts, where organisational, governance, and capability constraints continue to shape the uptake and effective use of such technologies (Neves et al. 2023; Jha and Dangwal 2024; Byeon et al. 2025).

Benefits and Challenges in Implementing Blockchain Technology for Fraud Prevention

The literature consistently identifies blockchain technology as a potentially transformative tool in the fight against fraud in financial enterprises, particularly in environments where traditional internal control systems are fragmented or insufficiently adapted to digital transactions. At a foundational level, blockchain provides a decentralised, transparent, and immutable ledger that reduces opportunities for data tampering, record manipulation, and unauthorised transaction modification (Turker and Bicer 2020; Nathan and Jacobs 2020; Singh et al. 2025). Through distributed consensus mechanisms and the use of smart contracts, blockchain-based systems can automate transaction execution and embed compliance rules directly into financial processes, thereby reducing reliance on intermediaries and limiting opportunities for internal interference and collusion (Turker and Bicer 2020; Langaliya and Gohil 2021; Xiong and Wan 2023).

From a fraud risk management perspective, the reviewed studies indicate that blockchain's capacity to generate permanent, auditable, and shared transaction records is particularly valuable for addressing fraudulent misrepresentation, asset misappropriation, and financial manipulation in digital environments

(Zarpala and Casino 2021; Liu et al. 2022; Vasudevan et al. 2025; Okewale et al. 2025). Several applied studies demonstrate that blockchain-based systems enhance both preventive and detective controls by strengthening traceability, reducing document tampering, and improving the reliability of transaction evidence (Rajasekaran et al. 2024; Vasudevan et al. 2025; Khan and Ahmad 2025). In addition, research focusing on forensic and analytical applications shows that blockchain infrastructures support more effective post-incident investigation and continuous monitoring through immutable audit trails and technology-enabled anomaly detection mechanisms (Nikkel 2020; Zarpala and Casino 2021; Liu et al. 2022; Sen et al. 2025).

However, the literature also highlights a number of significant challenges associated with the adoption of blockchain for fraud prevention in financial enterprises. One recurring concern relates to technical complexity, security vulnerabilities, and infrastructure risks within blockchain-based systems themselves. Albaroodi and Anbar (2025) note that weaknesses in blockchain cloud infrastructure, governance configurations, and access controls can expose organisations to new categories of operational and security risk if not properly managed. Similarly, Hyvarinen et al. (2017) emphasise that while blockchain-enhanced architectures improve fraud detection capabilities, their effectiveness depends heavily on the quality of system integration, data governance, and cybersecurity controls embedded within the broader digital ecosystem.

Beyond technical considerations, organisational and adoption-related barriers also constrain the realisation of blockchain's fraud prevention potential. The literature on digital financial services and fintech adoption suggests that many financial institutions, particularly in emerging and developing contexts, face limitations related to skills, governance capacity, regulatory uncertainty, and implementation readiness (Neves et al. 2023; Jha and Dangwal 2024; Byeon et al. 2025). These constraints contribute to uneven uptake and partial implementations that may weaken the expected control and assurance benefits of blockchain-based systems.

Taken together, the reviewed studies suggest that while blockchain offers substantial advantages for strengthening fraud prevention, detection, and forensic investigation in financial enterprises, its effectiveness is contingent upon complementary investments in governance, cybersecurity, system design, and organisational capability. Blockchain should therefore be viewed not as a standalone solution, but as a component of a broader, integrated fraud risk management and digital control architecture (Nakashima 2018; Bibi et al. 2024; Alagha and Özçelik 2025).

An outlook on the Complex Digital Ecosystem

Fraud risk in modern financial enterprises exists within a complex digital ecosystem rather than as a simple internal control problem. Financial systems increasingly rely on interconnected platforms, automated decision-making, and data-driven infrastructures, which expand both the scale and sophistication of potential fraud (Cosma 2023; Tian 2021; Arenas-Parra 2024).

Advanced technologies are reshaping financial operations. Robo-advisory systems and large-scale data analytics improve efficiency but also create model risk, opacity, and governance challenges (Arenas-Parra 2024; Cosma 2023; Tian 2021; Dar et al. 2024). Digital platforms such as crowdfunding and Islamic social finance expand access while introducing opportunities for misrepresentation, information asymmetry, and regulatory gaps (Ng and Kwok 2017; Jha and Dangwal 2024; Ghosh 2024).

Technological infrastructures are becoming more distributed and interdependent. Cloud computing, federated learning, and edge-based systems change accountability and complicate oversight (Yan et.al 2021; Jannat 2025; Zhang 2024). Emerging risks such as quantum computing and data marketplaces threaten security, transparency, and auditability (Baseri 2024).

These trends show that fraud risk is a systemic, socio-technical challenge. Blockchain, forensic tools, and audits are important but represent only one layer within a broader, digitally transformed financial environment (Tian 2021; Cosma 2023; Arenas-Parra 2024; Jannat 2025).

Discussion

The reviewed literature increasingly frames blockchain-based and digital financial technologies as components of a broader transformation of financial control, governance, and fraud risk management architectures. Across studies, blockchain is not presented as a standalone solution, but rather as part of an integrated socio-technical framework that combines transaction infrastructure, audit mechanisms, governance arrangements, and organisational capability (Turker and Bicer 2020; Nathan and Jacobs 2020; Alagha and Özçelik 2025; Singh et al. 2025). At the same time, the literature emphasises that realising these benefits requires simultaneous attention to system integration, governance design, and regulatory alignment within financial institutions (Albaroodi and Anbar 2025; Byeon et al. 2025).

Although blockchain and fintech technologies are widely discussed as tools for improving transparency, data security, and fraud prevention, evidence from the reviewed studies suggests that adoption

remains uneven and often fragmented, particularly in emerging and developing contexts. Research on digital financial services and fintech adoption highlights persistent barriers related to organisational readiness, regulatory uncertainty, skills constraints, and implementation complexity, which limit large-scale, systemic deployment within financial sectors (Neves et al. 2023; Jha and Dangwal 2024; Ghosh 2024). Consequently, many implementations remain pilot-oriented, experimental, or confined to specific use cases rather than embedded as core components of financial infrastructure (Byeon et al. 2025; Singh et al. 2025).

At the same time, applied and design-oriented studies within the corpus demonstrate that where blockchain is deployed, it is most often in targeted contexts such as document verification, cheque processing, loan administration, and transaction validation, rather than as a fully integrated enterprise-wide control architecture (Vasudevan et al. 2025; Rajasekaran et al. 2024; Khan and Ahmad 2025; Aracil et al. 2025). These applications nevertheless provide important evidence of blockchain's capacity to strengthen auditability, reduce record manipulation, and improve the reliability of transaction evidence within specific operational domains (Turker and Bicer 2020; Nathan and Jacobs 2020; Okewale et al. 2025).

From a theoretical and control perspective, the literature consistently underscores the continuing importance of internal control systems, audit functions, and governance structures as the foundation of fraud risk management, even in technologically advanced environments (Turker and Bicer 2020; Nathan and Jacobs 2020; Alagha and Özçelik 2025). However, as financial processes become increasingly digital and platform-based, traditional procedural controls are shown to be insufficient on their own. Instead, effective fraud risk management is increasingly conceptualised as a combination of governance, auditability, and technology-embedded controls within transaction infrastructures (Zarpala and Casino 2021; Liu et al. 2022; Nikkel 2020).

A growing stream of the reviewed literature further indicates that fraud in digital financial systems is evolving toward more complex, system-level and transaction-level manipulation, requiring more advanced forensic and analytical capabilities. Studies on anomaly detection, smart contract analysis, and blockchain-based forensic models demonstrate that technology-enabled monitoring and investigation mechanisms are becoming central to modern fraud risk management architectures (Zarpala and Casino 2021; Liu et al. 2022; Sen et al. 2025; Nikkel 2020). These developments reinforce the view that fraud prevention and detection are increasingly embedded within digital infrastructures rather than operating solely as ex-post control functions.

Nevertheless, the literature also highlights that technological capability alone does not guarantee improved fraud outcomes. Research on blockchain infrastructure and fintech systems points to ongoing challenges related to cybersecurity, system vulnerabilities, governance weaknesses, and integration risks, which can themselves become sources of new operational and control exposures if not properly managed (Albaroodi and Anbar 2025; Alagha and Özçelik 2025). These concerns further strengthen the argument that blockchain-based fraud prevention must be accompanied by robust governance, risk management, and assurance frameworks rather than being treated as a purely technical upgrade.

The reviewed studies suggest that the evolution of fraud risk management in financial enterprises is best understood as a transition toward integrated digital control architectures in which blockchain, analytics, auditing, and governance mechanisms operate as mutually reinforcing components. While the potential benefits are substantial, the literature consistently cautions that real-world impact depends on organisational readiness, regulatory alignment, and the quality of implementation rather than on the technology itself (Neves et al. 2023; Jha and Dangwal 2024; Byeon et al. 2025; Singh et al. 2025).

CONCLUSION

The study emphasises the importance of embracing an integrated strategy to fight occupational fraud in financial institutions. Even though traditional methods, such as internal controls and audits, remain paramount, their limitations in busy, resource-constrained environments justify the integration of advanced technologies. Blockchain, with its transparent and secure nature, is seen as a vital tool for refining fraud detection and prevention techniques. The study provides a foundation for continued investigation into the role of blockchain in the evolving nature of monetary regulation and fraud supervision in financial institutions. Even though traditional methods, such as internal controls and audits, remain paramount, their limitations in busy, resource-constrained environments justify the integration of advanced technologies. Blockchain, with its transparent and secure nature, is seen as a vital tool for refining fraud detection and prevention techniques. The study provides a foundation for continued investigation into the role of blockchain in the evolving nature of monetary regulation and fraud supervision.

Acknowledgments
The authors acknowledge that no additional support outside of the Author Contributions or Funding sections was received for this study.

Funding
The authors declare that no financial support, grants, or external funding were received for the conduct of this research, analysis, or publication of this article.

Data Available Statement
The data utilised in this study were derived from secondary sources, including Scopus and ScienceDirect databases. These datasets are accessible through institutional or individual subscription-based access to the respective platforms.

Conflict of interest
The authors declare that they have no known personal, professional, or financial conflicts of interest that could have influenced the design, execution, analysis, or interpretation of the findings of this study.

AI Tools Statement
AI-based language editing tools were used to improve grammar and clarity. All intellectual content, interpretation, and conclusions are solely the responsibility of the authors.

Author contribution
• Conceptualization: Praise Mutoko. The conceptualization of the study was primarily undertaken by Praise Mutoko, who developed the initial research idea and framework guiding the study.
• Methodology: Praise Mutoko and Ephraim Faku. The research methodology was developed collaboratively by Praise Mutoko and Ephraim Faku, focusing on the design of the approach and structure of the secondary data analysis.
• Validation: Praise Mutoko. Validation of the study findings and analytical consistency was carried out by Praise Mutoko.
• Formal analysis: Ephraim Faku and Praise Mutoko. Formal analysis of the secondary data was conducted jointly by Ephraim Faku and Praise Mutoko.
• Resources: Ephraim Faku
• Writing – original draft: Praise Mutoko. The original draft of the manuscript was prepared by Praise Mutoko.
• Writing – review & editing: Ephraim Faku . The manuscript was reviewed and edited by Ephraim Faku to ensure academic quality and coherence.
• Visualization: Praise Mutoko. Praise Mutoko developed visualization of results and findings.
• Supervision: Ephraim Faku. The research process was supervised by Ephraim Faku, who provided academic guidance throughout the study.
• Project administration: Praise Mutoko. Project administration was managed by Praise Mutoko, including coordination of research activities.

REFERENCES

Alagha, B., and I. Özçelik. 2025. Using Blockchain Technology for Audit Trail. In *Digital Strategy and Governance in Transformative Technologies*, 239–259. Cham: Springer. https://doi.org/10.1201/978100347dangwa7808-14.

Albaroodi, H. A., and M. Anbar. 2025. Security Issues and Weaknesses in Blockchain Cloud Infrastructure: A Review Article. *Journal of Applied Data Sciences,* 6 (1): 155–177.

Arenas-Parra, M., H. Rico-Pérez, and R. Quiroga-García. 2024. The Emerging Field of Robo-Advisors: A Relational Analysis. *Heliyon,* 10: e21543. https://doi.org/10.1016/j.heliyon.2024.e35946.

Aracil, E., L. Fernández-Méndez, and F. J. Fuertes. 2025. Trust and Financial Inclusion: A Literature Review with Reference to the Digital Transformation."*Heliyon,* 11: e25631. https://doi.org/10.1016/j.heliyon.2025.e44128.

Association of Certified Fraud Examiners (ACFE). 2022. *Report to the Nations: 2022 Global Study on Occupational Fraud and Abuse*. Austin, TX: ACFE.

Bakar, A. B. S. A., N. A. B. M. Ghazali, and M. B. Ahmad. 2019. Sustainability Reporting and Board Diversity in Malaysia. *International Journal of Academic Research in Business and Social Sciences,* 9(3): 91–99. https://doi.org/10.6007/ijarbss/v9-i2/5663.

Baseri, Y., V. Chouhan, and A. Hafid. 2024. Navigating Quantum Security Risks in Networked Environments. *Computers & Security,* 132: 103332. https://doi.org/10.1016/j.cose.2024.103883.

Beck, T., and R. Cull. 2014. SME Finance in Africa. *Journal of African Economies,* 23(5): 583–613. https://doi.org/10.1093/jae/eju016.

Bibi, S., H. Zada, and N. Khan. 2024. Governance, ICT and Financial Inclusion. *Heliyon,* 10: e19843. https://doi.org/10.1016/j.heliyon.2024.e33711.

Bruwer, J. P., and A. Petersen. 2022. The Perceptions of South African Small, Medium and Micro Enterprise Management on Occupational Fraud Risk, Economic Sustainability and Key Employee Characteristics. *Journal of Accounting, Finance and Auditing Studies*. https://doi.org/10.32602/jafas.2022.026.

Byeon, H., G. P. Selvi, R. Robert, and S. Agalya. 2025. Blockchain Technology in Financial Services. *AIP Conference Proceedings,* 3306: 030068. https://doi.org/10.1063/5.0275939.

Chung, T., P. N. Sharma, C. C. Lee, and J. Pinto. 2021. National Culture and Occupational Fraud Magnitude: The Moderating Role of Fraud Type. *Journal of Forensic Accounting Research,* 6(1): 406–435. https://doi.org/10.2308/jfar-2020-025.

Cosma, S., G. Rimo, and G. Torluccio. 2023. Knowledge Mapping of Model Risk in Banking. *International Review of Financial Analysis,* 89: 102743. https://doi.org/10.1016/j.irfa.2023.102800.

Cressey, D. R. 1953. *Other People's Money: A Study in the Social Psychology of Embezzlement*. Glencoe, IL: Free Press.

Dar, B. I., N. Badwan, and J. Kumar. 2024. FinTech Innovations and Green Finance. *International Journal of Islamic and Middle Eastern Finance and Management,* 17(4): 1–22. https://doi.org/10.1108/imefm-01-2024-0018.

Darsono, J., A. Hidayat, and S. Nugroho. 2024. Crisis-Driven Fraud Risks. *Journal of Financial Crime,* 31(1): 88–104.

Ding, W., Y. Huang, and S. Wang. 2024. Regulatory and Privacy Risks in Blockchain Finance. *Information Systems Frontiers,* 26(2): 421–438.

Fatoki, O. 2014. The Causes of SME Failure in South Africa. *Mediterranean Journal of Social Sciences,* 5(20): 922–927. https://doi.org/10.5901/mjss.2014.v5n20p922.

Financial Intelligence Centre. 2024. *Strategic Analysis Brief: Corruption and Financial Crime Threats in South Africa's Financial Sector*. Pretoria: FIC.

Ghosh, M. 2024. Financial Inclusion Bibliometric Analysis. *Sustainable Futures,* 6: 100142. https://doi.org/10.1016/j.sftr.2024.100160.

Homer, J. 2020. An Analysis of the Fraud Triangle. *Journal of Forensic and Investigative Accounting,* 12(2): 89–103.

Hyvärinen, H., M. Risius, and G. Friis. 2017. Blockchain-Based Approach to Public Sector Fraud. *Business & Information Systems Engineering,* 59(6): 441–456. https://doi.org/10.1007/s12599-017-0502-4.

Indiraswari, S. D., B. Subroto, R. Rosidi, and I. Subekti. 2025. Corporate Governance and Financial Statement Fraud: Evidence on the Moderating Influence of Financial Distress. *Problems and Perspectives in Management,* 23(2): 785. https://doi.org/10.21511/ppm.23(2).2025.57.

Jannat, S. 2025. Crowdfunding Dilemmas in Bangladesh SMEs. *International Journal of Innovation Science,* 17(2): 1–18. https://doi.org/10.1108/ijis-03-2024-0066.

Jha, S., and R. C. Dangwal. 2024. FinTech Services and Financial Inclusion. *Journal of Science and Technology Policy Management,* 15(2): 211–230. https://doi.org/10.1108/jstpm-03-2023-0034.

Khan, A. H. J., and S. A. Ahmad. 2025. IoTBlockFin. *Journal of Intelligent Systems and Internet of Things,* 14(1): 209–220. https://doi.org/10.54216/jisiot.140116.

Koppeschaar, Z. 2012. IFRS for SMEs. *Southern African Journal of Entrepreneurship and Small Business Management,* 5(1): 54–68. https://doi.org/10.4102/sajesbm.v5i1.27.

Kroon, N., M. C. Alves, and I. Martins. 2021. Emerging Technologies and Accountants' Skills. *Journal of Open Innovation,* 7 (3): 163. https://doi.org/10.3390/joitmc7030163.

Kumar, A., H. Pavana Kumari, P. A. M. Auxilia, and P. O. Bhoir. 2023. Implementation of Blockchain in Finance. In *ICACITE 2023 Proceedings*, 1102–1106. https://doi.org/10.1109/icacite57410.2023.10182951.

Langaliya, V., and J. A. Gohil. 2021. Smart Contract Applications. *International Journal on Recent and Innovation Trends in Computing and Communication,* 9(9): 16–26. https://doi.org/10.17762/ijritcc.v9i9.5489.

Liu, L., W.-T. Tsai, M. Z. A. Bhuiyan, H. Peng, and M. Liu. 2022. "Blockchain-Enabled Fraud Discovery." *Future Generation Computer Systems* 128: 158–166. https://doi.org/10.1016/j.future.2021.08.023.

Mongwe, A., and D. Malan. 2020. Machine Learning and Fraud Detection in South Africa. *South African Journal of Accounting Research,* 34(1): 45–68. https://doi.org/10.18489/sacj.v32i1.777.

Mwega, F. M. 2011. Structural Shifts in Kenya's Financial Institutions. *African Development Review,* 23(1): 105–123. https://doi.org/10.1111/j.1467-8268.2010.00271.x.

Nair, A. J., and A. S. Rao. 2025. Quantifying the Fiscal Ramifications of Big Data Integration in Service Organisations. In *AI and the Revival of Big Data*, 239–258. https://doi.org/10.4018/979-8-3693-8472-5.ch011.

Nathan, J., and B. Jacobs. 2020. Blockchain Consortium Networks. *Journal of Corporate Accounting and Finance,* 31(2): 29–33. https://doi.org/10.1002/jcaf.22428.

National Treasury. 2024. *National Money Laundering and Terror Financing Risk Assessment Report: South Africa*. Pretoria: Republic of South Africa.

Neves, C., T. Oliveira, and L. Gutman. 2023. Adoption of Digital Financial Services. *International Journal of Information Management Data Insights,* 3: 100146. https://doi.org/10.1016/j.jjimei.2023.100201.

Ng, A. W., and B. K. B. Kwok. 2017. FinTech and Cybersecurity. *Journal of Financial Regulation and Compliance,* 25(4): 368–384. https://doi.org/10.1108/jfrc-01-2017-0013.

Nikkel, B. 2020. FinTech Forensics. *Forensic Science International: Digital Investigation,* 33: 300939. https://doi.org/10.1016/j.fsidi.2020.200908.

Okewale, K., O. Akinhanmi, I. Idowu, O. Jasanya, and O. E. Peter. 2025. Blockchain Efficiency in Financial Security. *NIPES Journal of Science and Technology Research,* 7(1): 1378–1383. https://doi.org/10.37933/nipes/7.4.2025.si159.

Page, M. J., J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, and D. Moher. 2021. The PRISMA 2020 Statement. *BMJ* 372: n71. https://doi.org/10.1016/j.jclinepi.2021.02.003.

Pearce, D., and B. Helms. 2001. *Financial Services Associations: The Story So Far*. Washington, DC: Consultative Group to Assist the Poorest. https://doi.org/10.1596/12843.

PricewaterhouseCoopers (PwC). 2022. *Global Economic Crime and Fraud Survey 2022*. London: PwC.

Rajasekaran, A. S., J. Haribabu, G. V. Ramnjaneyulu, T. Sivakumar, A. Mohanarathinam, and T. Velmurugan. 2024. Blockchain-Based Document Verification Scheme for Enhanced Security and Fraud Control. In *Proceedings of the International Conference on Emerging Research in Computational Science (ICERCS)*, 1–5. https://doi.org/10.1109/icercs63125.2024.10895236.

Sarkis-Onofre, R., F. Catalá-López, E. Aromataris, and C. Lockwood. 2021. How to Properly Use the PRISMA Statement. *Systematic Reviews,* 10(1): 117. https://doi.org/10.1186/s13643-021-01671-z.

Shanikat, M., and M. M. Aldabbas. 2025. Perception of Corporate Governance Factors in Mitigating Financial Statement Fraud in Emerging Markets. *Journal of Risk and Financial Management,* 18(8): 430. https://doi.org/10.3390/jrfm18080430.

Sen, A. C., P. Kumar, M. J. Dave, A. Kalra, and M. Goyal. 2025. Machine Learning-Driven Anomaly Detection. In *Communications in Computer and Information Science*, 2382: 143–157. https://doi.org/10.1007/978-3-031-86069-0_12.

Singh, M., K. Srivastava, K. R. P. Vittala, and A. K. Tyagi. 2025. Blockchain in Modern Banking. In *Establishing AI Specific Cloud Computing Infrastructure*, 331–358. Cham: Springer. https://doi.org/10.4018/979-8-3693-9694-0.ch016.

Singh, S., S. Singh, and T. Kajla. 2023. Checking the Effectiveness of Blockchain Application in Fraud Detection with a Systematic Literature Review Approach. https://doi.org/10.1108/978-1-80455-566-820231003.

Sreenu, N., and S. S. Verma. 2024. Digital Financial Inclusion in India. *Transnational Corporations Review,* 16(4): 1–20. https://doi.org/10.1016/j.tncr.2024.200091.

Stainbank, L. J. 2010. Due Process in Adopting IFRS for SMEs in South Africa. *Meditari Accountancy Research,* 18(2): 1–20. https://doi.org/10.1108/10222529201000010.

Tian, X., J. S. He, and M. Han. 2021. "Data-Driven Approaches in FinTech. *Information Discovery and Delivery,* 49(2): 113–126. https://doi.org/10.1108/idd-06-2020-0062.

Tickner, P., and M. Button. 2021. Deconstructing the Origins of Cressey's Fraud Triangle." *Journal of Financial Crime*, 28(3): 722–731. https://doi.org/10.1108/jfc-10-2020-0204.

Transparency International. 2025. *South Africa Country Profile*. Berlin: Transparency International.

Trivedi, S. 2023. Blockchain Framework for Insurance. *International Journal of Innovation and Technology Management,* 20(6): 2350034. https://doi.org/10.1142/s0219877023500347.

Turker, I., and A. A. Bicer. 2020. Blockchain in Auditing and Assurance. In *Contributions to Management Science*, 457–471. Cham: Springer. https://doi.org/10.1007/978-3-030-29739-8_22.

Vasudevan, A., M. Thayanithi, A. Pandiyarajan, N. Raja, and A. Kumar. 2025. ChequeGuard Framework. *International Journal of Interactive Mobile Technologies,* 19(14): 108–120. https://doi.org/10.3991/ijim.v19i14.56869.

Wells, J. T. 2017. *Corporate Fraud Handbook: Prevention and Detection*. 5th ed. Hoboken, NJ: Wiley.

Xiong, W., and D. Wan. 2023. Financial Investment Trust Mechanism Based on Smart Contract. *PLOS ONE* 18 (7): e0287706. https://doi.org/10.1371/journal.pone.0287706.

Yan, M., R. Filieri, and M. Gorton. 2021. "Continuance Intention of Online Technologies." *International Journal of Information Management,* 58: 102296. https://doi.org/10.1016/j.ijinfomgt.2021.102315.

Zarpala, L., and F. Casino. 2021. Blockchain-Based Forensic Model. *Digital Finance,* 3 (3–4): 301–332. https://doi.org/10.1007/s42521-021-00035-5.

Zhang, J., Q. Wu, and Q. Fan. 2024. Joint Resource Allocation in Federated Edge Learning. *Computers, Materials and Continua,* 78(1): 1–25. https://doi.org/10.32604/cmc.2024.057006.

Ziorklui, S. Q., C. Nwachukwu, and T. Okafor. 2024. Internal Controls and Fraud Prevention. *Journal of Financial Crime,* 31(2): 455–472. https://doi.org/10.51594/farj.v6i7.1322

Appendix

Summary of Reviewed Literature

No.	Author(s) & Year	Title	Journal/ Source	Main Theme	Methodology	Key Contribution
1	Okewale et al. (2025)	Blockchain efficiency in financial security	NIPES Journal	Blockchain security	Empirical	Improves transaction security
2	Alagha and Özçelik (2025)	Blockchain for audit trails	Digital Strategy & Governance	Auditing	Conceptual	Immutable audit trails
3	Byeon et al. (2025)	Blockchain in financial services	AIP Conf. Proc.	Financial services	Review	Opportunities and risks
4	Singh et al. (2025)	Blockchain in modern banking	Book chapter	Banking	Conceptual	DLT impact on banking
5	Nair and Rao (2025)	Big data & malfeasance	AI & Big Data	Fraud mitigation	Analytical	Reduces financial misconduct
6	Khan and Ahmad (2025)	IoTBlockFin loan model	J. Intelligent Systems & IoT	Loan fraud	System design	Prevents loan scams
7	Sen et al. (2025)	ML anomaly detection	CCIS	Fraud detection	ML model	Detects anomalies
8	Vasudevan et al. (2025)	ChequeGuard framework	IJIMT	Cheque fraud	Framework	Prevents fake cheques
9	Albaroodi & Anbar (2025)	Blockchain cloud security	J. Applied Data Sciences	Security	Review	Identifies vulnerabilities
10	Zarpala and Casino (2021)	Blockchain forensic model	Digital Finance	Financial crime	Case model	Supports investigations
11	Liu et al. (2022)	Smart contract fraud detection	FGCS	Ethereum fraud	Analytics	Detects abnormal contracts
12	Hyvärinen et al. (2017)	Blockchain against public fraud	BISE	Public sector	Conceptual	Anti-fraud framework
13	Langaliya and Gohil (2021)	Smart contract applications	IJRI Trends CC	Smart contracts	Comparative	Evaluates use cases
14	Xiong and Wan (2023)	Investment trust via contracts	PLOS One	Investments	Model	Trust mechanism
15	Kumar et al. (2023)	Blockchain in finance	ICACITE	Finance systems	Experimental	Implementation evidence
16	Trivedi (2023)	Blockchain for insurance	IJITM	Insurance	Framework	Improves processes
17	Turker and Bicer (2020)	Blockchain in auditing	Mgmt Science	Auditing	Conceptual	Assurance guidance
18	Nathan and Jacobs (2020)	Consortium blockchains	JCAF	Governance	Case analysis	Improves trust
19	Neves et	Digital	IJIM Data	FinTech	Meta-analysis	Identifies

No.	Author(s) & Year	Title	Journal/ Source	Main Theme	Methodology	Key Contribution
	al. (2023)	finance adoption	Insights	adoption		barriers
20	Dar et al. (2024)	FinTech & green finance	IJ Islamic & ME Finance	Sustainability	Bibliometric	Maps research
21	Ng and Kwok (2017)	FinTech & cybersecurity	JFRC	Cybersecurity	Conceptual	Early risk insights
22	Kroon et al. (2021)	Tech impact on accountants	JOI	Professional skills	SLR	Skill transformation
23	Jannat (2025)	SME crowdfunding barriers	IJ Innovation Science	SMEs	Qualitative	Identifies obstacles
24	Nikkel (2020)	FinTech forensics	FSI Digital Investigation	Forensics	Review	Digital evidence methods
25	Yan et al. (2021)	Technology continuance	IJIM	User behaviour	SLR	Explains adoption
26	Aracil et al. (2025)	Trust & inclusion	Heliyon	Financial inclusion	Review	Trust as driver
27	Sreenu and Verma (2024)	Digital inclusion India	TCR	Economic growth	Empirical	Growth impact
28	Bibi et al. (2024)	Governance & inclusion	Heliyon	Governance	Quantitative	Moderating role
29	Ghosh (2024)	Inclusion bibliometrics	Sustainable Futures	Inclusion	Bibliometric	Future trends
30	Jha and Dangwal (2024)	FinTech & inclusion	JSTPM	Policy	SLR	Synthesises evidence
31	Arenas-Parra et al. (2024)	Robo-advisors	Heliyon	AI finance	Relational	Maps field
32	Nakashima (2018)	FinTech, IoT & credit	IATSS Research	Credit systems	Conceptual	Mobility-based credit
33	Baseri et al. (2024)	Quantum-safe security	Computers & Security	Cybersecurity	Technical review	Post-quantum risks
34	Tian et al. (2021)	Data-driven FinTech	IDD	FinTech analytics	Survey	Model overview
35	Cosma et al. (2023)	Model risk banking	IRFA	Banking risk	Knowledge mapping	Risk mapping
36	Zhang et al. (2024)	Federated edge learning	CMC	Distributed learning	Survey	Resource allocation