

The Role of Blockchain Technology Transformation in Preventing and Detecting Financial Fraud as an Anti-Fraud System Revolution in Indonesia

Muhammad Syukeri¹, Faridah², M. Yulian Ma'mun³, Faqih El Wafa⁴

^{1,2,3,4} Universitas Islam Negeri Antasari Banjarmasin, Indonesia

e-mail: syukeri411@gmail.com¹, faridah@uin-antasari.ac.id², yulianmamun@uin-antasari.ac.id³, faqihelwafa@uin-antasari.ac.id⁴

Abstrak

Tingginya eskalasi kasus fraud keuangan di Indonesia, yang secara sistematis mengeksploitasi kerentanan pada sistem pencatatan sentralistik konvensional, telah menjadi masalah utama yang mengancam stabilitas ekonomi nasional. Sistem pengawasan tradisional terbukti sangat rentan terhadap manipulasi karena bergantung pada otoritas tunggal dan lemahnya integritas pihak ketiga. Merespons urgensi tersebut, penelitian ini bertujuan untuk menganalisis secara mendalam peran transformasi teknologi blockchain dalam mencegah dan mendeteksi kecurangan finansial sebagai revolusi sistem anti-fraud nasional. Metode yang digunakan dalam penelitian ini adalah kualitatif melalui pendekatan Systematic Literature Review (SLR) yang berpedoman ketat pada protokol PRISMA guna meminimalkan bias subjektif. Data utama penelitian diekstraksi secara sistematis dari 19 artikel jurnal internasional bereputasi tinggi (Q1-Q3) yang terindeks dalam basis data Scopus, dengan rentang publikasi terkini antara 2020 hingga 2024. Kesimpulan penelitian ini menegaskan bahwa blockchain sangat efektif dalam menutup celah manipulasi melalui desentralisasi jaringan, transparansi absolut, dan ketakterubahan data (immutability) yang divalidasi oleh otomatisasi kontrak cerdas (smart contracts). Meskipun secara arsitektural terbukti sangat superior sebagai sistem pertahanan masa depan, kesimpulan kajian juga menggarisbawahi bahwa implementasi blockchain di Indonesia masih dihadapkan pada tantangan yang kompleks. Hambatan utama tersebut mencakup belum matangnya kesiapan regulasi dan hukum, tingginya biaya adaptasi infrastruktur operasional, serta keterbatasan skalabilitas jaringan. Oleh karena itu, kolaborasi lintas sektor sangat diperlukan untuk merancang kerangka adopsi yang terukur.

Kata Kunci: Teknologi Blockchain; Penipuan Keuangan; Sistem Anti Penipuan

Abstract

The escalating incidence of financial fraud in Indonesia, which systematically exploits critical vulnerabilities inherent in conventional centralized record-keeping systems, has become the core threat to national economic stability. Traditional oversight mechanisms have proven highly susceptible to manipulation due to their heavy reliance on single-authority control and the weak integrity of third parties. Responding to this urgency, this study aims to comprehensively analyze the role of blockchain technology transformation in preventing and detecting financial fraud as a revolutionary breakthrough in the national anti-fraud system. The method employed in this research is qualitative, using a Systematic Literature Review (SLR) approach strictly guided by the PRISMA protocol to minimize subjective bias. The primary research data were systematically extracted from 19 highly reputable international journal articles (Q1-Q3) indexed in the Scopus database, featuring recent publications spanning from 2020 to 2024. The research concludes that blockchain is exceptionally effective at permanently eliminating manipulation loopholes through network decentralization, absolute transparency, and data

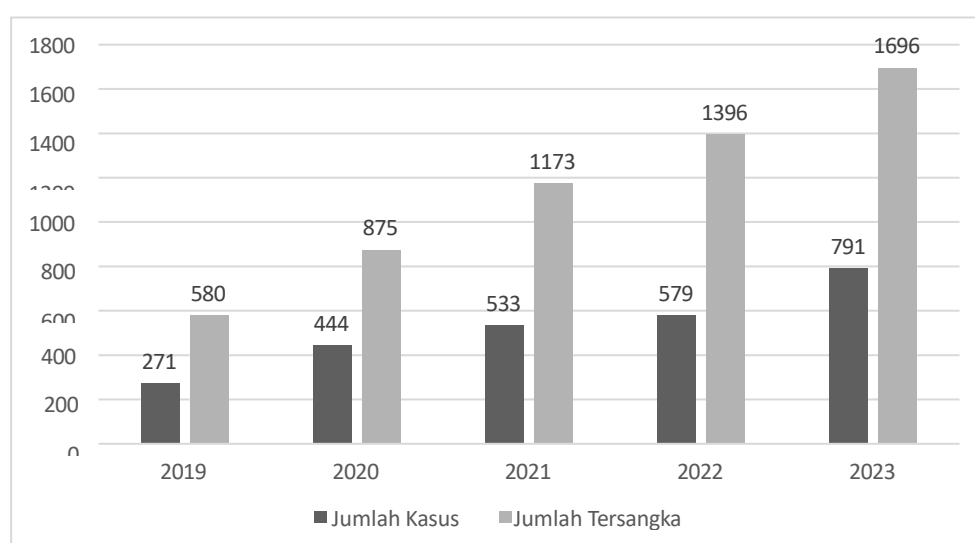
immutability, all validated by smart contract automation. Although architecturally proven to be vastly superior as a future defense system, the study's conclusion also highlights that implementing blockchain in Indonesia still faces complex challenges. These primary barriers include the immaturity of legal and regulatory readiness, the high costs of adapting operational infrastructure, and the limitations of network scalability. Therefore, cross-sectoral collaboration is urgently required to establish a measured adoption framework.

Keywords: Blockchain Technology; Financial Fraud; Anti-Fraud System

INTRODUCTION

The phenomenon of financial fraud in Indonesia has currently reached a highly alarming level and has become a serious threat to national economic stability. Financial fraud cases, particularly corruption and asset misappropriation, continue to show a massive upward trend each year (Anandya & Ramdhana, 2024). According to a report by the Association of Certified Fraud Examiners (ACFE), Indonesia ranks fourth in the Asia-Pacific region for substantial financial losses from asset misappropriation and financial statement fraud (Association of Certified Fraud Examiners, 2022). This reality is exacerbated by data findings from the Corruption Eradication Commission (*Komisi Pemberantasan Korupsi* or KPK) and Indonesia Corruption Watch (ICW) in 2023, which recorded state losses amounting to trillions of rupiah due to various mega financial scandals in major corporations such as ASABRI, Jiwasraya, and the tin commodity trading case. Furthermore, these fraudulent practices not only violate positive law but also strongly contradict ethical principles and fundamental values in the financial system that prioritize transparency, fairness, and the strict prohibition of manipulative asset acquisition. This empirical evidence demonstrates that current supervisory mechanisms and internal control systems across various financial institutions and government agencies have not effectively stemmed the tide of financial confidentiality crimes. Thus, this reality shows that the weaknesses of centralized recording systems and traditional oversight remain the primary loopholes that financial perpetrators in Indonesia continuously exploit. To provide a clearer empirical visualization regarding the massive escalation of these crimes, Chart 1 illustrates the statistical trends of corruption in Indonesia.

Chart 1. Corruption Trends Over the Past Five Years (2019–2023)



Source: Anandya & Ramdhana (2024)

Various academic literatures and existing theoretical foundations for fraud prevention have yet to fully provide fundamental solutions to the vulnerabilities to manipulation within the financial system. Theoretically, the causal factors of fraud are frequently analyzed using the Fraud Hexagon Theory, which encompasses the elements of stimulus (pressure), opportunity, rationalization, capability, arrogance, and collusion (Shonhadji & Irwandi, 2024). Although this theory can map the behavior of perpetrators, conventional anti-fraud strategies built on this framework, such as implementing whistleblowing systems, tightening internal audits, and monitoring surveillance cameras, still have structural weaknesses because they rely on centralized databases. Traditional centralized accounting recording systems grant full authority to a single central authority, making them highly vulnerable to hacking, internal collusion, and undetected data modifications (Vasquez, 2021). Recent literature indicates that dependence on third-party verification involving human elements inadvertently magnifies the opportunity and collusion elements within the fraud theory itself. Prior studies have not comprehensively integrated distributed ledger technology solutions to effectively close loopholes for data manipulation. Prevention approaches that focus solely on bureaucratic reform and penal sanctions often fail to counter the escalating sophistication of digital-era financial crimes. The literature gap regarding the adoption of decentralized technology in developing countries also poses a significant weakness in financial security studies. It is the failure of conventional literature and theories to address the root causes of database manipulation that necessitates a new, more advanced, and decentralized technological approach.

Based on the literature gap and the urgency of the problem in the field, this study primarily aims to explore in depth the role of cutting-edge technology in combating financial crimes. More specifically, the objective of this research is to examine how blockchain technology can be effectively implemented to prevent and detect financial fraud within agencies and corporations in Indonesia (Ahmed & Alabi, 2024). This research is also intended to unpack the mechanisms of decentralization, transparency, and immutability inherent in blockchain as an anti-fraud system revolution that ensures database security. Furthermore, this study aims to comprehensively identify various technical operational challenges, data protection regulatory hurdles, and network scalability issues that may arise during the adoption process of blockchain as a distributed ledger in the national financial and banking sectors (Tan-Vo et al., 2024). Furthermore, this research intends to evaluate the effectiveness of using complementary instruments, such as smart contracts, to automate transaction verification, a process that has historically been vulnerable to manual manipulation by internal parties. Through this series of objectives, this scientific paper is expected to bridge the academic knowledge gap regarding the integration of cutting-edge cybersecurity systems with modern investigative audit instruments, thereby providing valuable new literature for both academia and industry practitioners. The analytical results from all these research objectives are ultimately projected to offer strategic recommendations for policymakers in designing an advanced and trustworthy financial infrastructure.

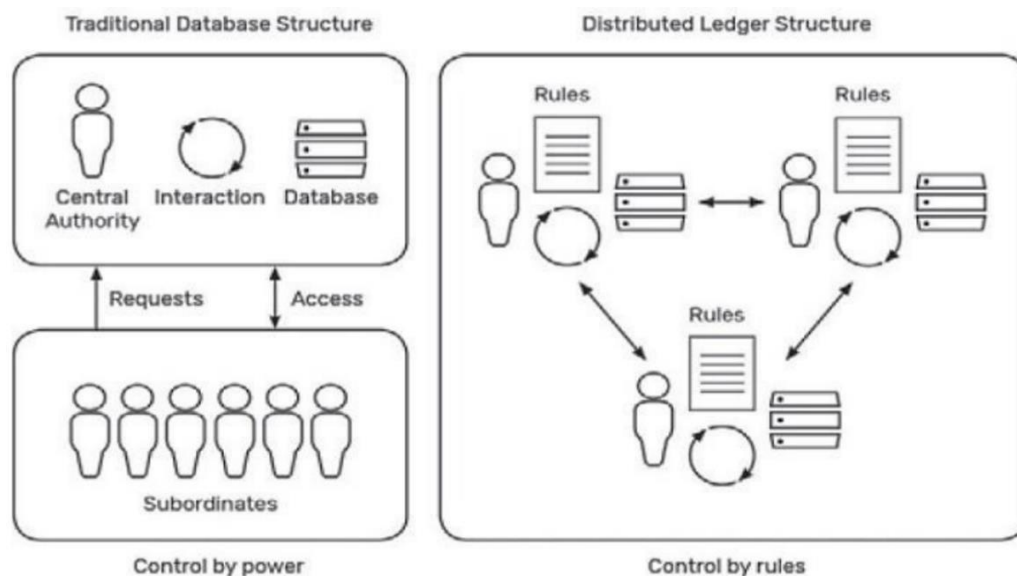
Given the escalating national financial losses and the formulated innovative objectives, this research is of very high urgency. It must be implemented immediately to safeguard the integrity of the economy. The fundamental argument of this paper is that blockchain technology is hypothesized to be capable of permanently closing opportunities for fraud through cryptographic consensus that eliminates single points of control over databases (Pranto et al., 2022). The importance of this research lies in the fact that legal approaches and bureaucratic reforms thus far remain insufficient without the support of advanced digital architecture transformation. The implementation of a distributed ledger system is believed to create an indelible audit trail, thereby making it exceedingly difficult for internal individuals with malicious intent to conceal traces of fictitious transactions (Mapa Mudiyansele et al., 2023). If this research is not conducted, Indonesia is predicted to continue to suffer budget leakages that will burden the economy in the long term due to weaknesses in the recording system. This study is crucial because its findings will provide academic evidence that investing in the

restructuring of financial technology architecture is far more efficient than enduring annual losses due to weak early detection methods. The central hypothesis in this scientific work is that adopting blockchain will radically reduce fraud rates by shifting the paradigm from centralization to decentralization, which is claimed to be significantly more transparent. Thus, the urgency of this research lies in its potential to provide a revolutionary technical framework for protecting state assets and restoring public trust in the integrity of the national financial system.

LITERATURE REVIEW

Conceptually, blockchain technology is a decentralized digital ledger system widely distributed across a network of computers, without the control of a single central authority (Bashir, 2023). This distributed database system operates by collecting and processing data or transaction records into a series of blocks tightly interconnected through high-level cryptographic protection. Whenever new information or transaction data is added, all users or nodes in the network must reach a mutual agreement, known as consensus, before the data is validated. Once this majority approval process is achieved, the new data block will be encrypted using a unique hashing algorithm and chronologically linked to the previous block, forming a permanent chain of blocks (Maulani et al., 2023). The primary characteristics that distinguish this technology from traditional database recording systems rest on three pillars: decentralization, transparency, and immutability (Zainuddin, 2023). Through these pillars, the entire history of validated transactions cannot be unilaterally manipulated, altered, or deleted by any party without being detected by all members of the computer network. Thus, blockchain technology provides a highly robust infrastructure for a digital recording ecosystem that is transparent, independently verifiable, and highly immune to hacking and forgery attempts. The fundamental architectural differences between the vulnerabilities of a traditional centralized database and the robust framework of a distributed ledger are visually depicted in Figure 1

Figure 1. Differences Between Traditional Databases and Distributed Ledgers

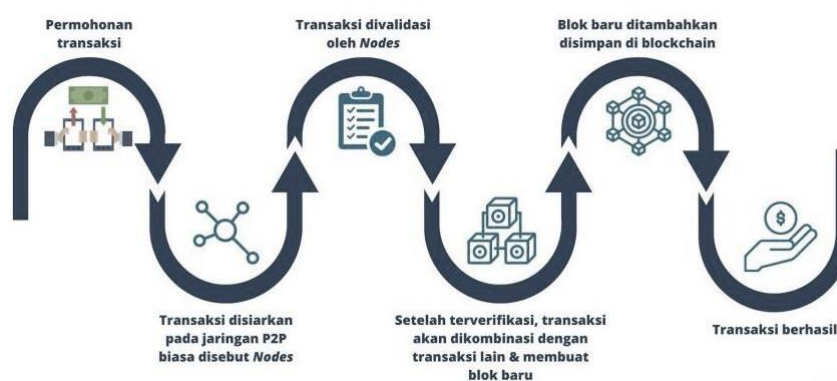


Source: Vasquez (2021)

In its various forms, blockchain technology is categorized into several network architectures based on the level of accessibility and the consensus control systems they employ. The first category is public blockchain, a type of network that is entirely open and

permissionless, thereby allowing anyone to participate in writing, reading, and validating transaction data (Warburg et al., 2019). Conversely, there is the private blockchain category, which grants exclusive full control rights to a single owner or authority to regulate network accessibility, typically implemented for the internal needs of an organization requiring strict data privacy. Beyond these two extreme forms, other classifications include permissioned blockchains, or consortium blockchains, where network operations are restricted to a group of trusted, pre-selected, and approved entities or nodes, such as a collaborative network among banking institutions. Furthermore, technological advancements have also led to the emergence of semi-private blockchain architectures, which combine a private infrastructure for managing sensitive internal data with a public infrastructure to facilitate external participation requiring limited data transparency (Bashir, 2023). This diverse categorization of distributed database infrastructures ultimately provides comprehensive structural flexibility, enabling various agencies to adopt the decentralized model most suitable to their respective security needs, operational privacy, and regulatory compliance. Further technical elaboration on the chronological transaction flow and the consensus mechanism within the *blockchain* network is shown in Figure 2.

Figure 2. How Blockchain Works



Source: Sigit (2022)

The concept of financial fraud is defined as an illegal, deceptive act carried out in a highly calculated and intentional manner, using manipulative ingenuity to unlawfully obtain unilateral benefits. The Association of Certified Fraud Examiners (ACFE) elaborates on the definition of this crime as a form of exploitation involving the intentional misuse of occupational positions, authority, or resources belonging to an organization to enrich oneself or a specific group (Association of Certified Fraud Examiners, 2022). From a legal perspective, fraudulent acts encompass all forms of obscured information, intentional negligence, and the concealment of material facts in an operational report with the malicious intent to mislead interested parties. This phenomenon of financial deviance does not rely solely on the physical misappropriation of assets but also involves the systemic manipulation of data confidentiality to evade payment obligations or to illegally secure an advantageous position (Arianto et al., 2023). Further literature reviews highlight that these exploitative acts are heavily influenced by the psychological rationalization of the perpetrators, where they often attempt to justify the unlawful actions to maintain self-image or to meet the demands of financial pressures that cannot be resolved legally. In essence, financial fraud is a fundamental betrayal of the values of integrity, operational transparency, and good institutional governance, which directly injures public trust and destroys entities.

The manifestation of financial fraud crimes in corporate and governmental environments is generally classified into three main categories that reflect variations in modus operandi and targets of exploitation. The first and most fundamental category is asset misappropriation, which refers to any form of theft or embezzlement of an institution's assets,

whether through direct cash theft or the manipulation of inventory for personal gain. Subsequently, the second category with a massively destructive impact is corruption, wherein individuals abuse their political power or authority through bribery, acceptance of illegal gratuities, economic extortion, and violations of operational conflicts of interest (Association of Certified Fraud Examiners, 2022). The third category of crime focuses on financial statement fraud, which involves the systematic manipulation of accounting records to deceive investors, creditors, or regulatory bodies about a company's financial health. These high-level manipulative practices are frequently manifested as modifying the timing of transaction recording, creating narratives of fictitious revenues, engineering asset valuations to appear higher, and concealing debt liabilities to evade detection by external auditors. This structured categorization clearly demonstrates that financial crime schemes exhibit an extremely broad, complex, and systematic spectrum of manifestations, thus constantly requiring mitigation mechanisms and detection instruments that are designed to be cutting-edge and integrated to address every vulnerability.

An anti-fraud system is a set of strategic control mechanisms, comprehensive oversight procedures, and technological architectures designed by an organization to detect, prevent, and respond to financial fraud threats. Fundamentally, this protection system serves as the primary line of defense, aimed at closing every triggering element of financial crimes, specifically by minimizing opportunities for loopholes and suppressing the rationalization of deviant behavior through strictly integrated supervision. Within a conventional framework, this tracking security system relies heavily on the regular application of internal audits, bureaucratic control policies, rigid separation of duties, and the implementation of anonymous whistleblowing systems to uncover hidden criminal practices (Anandya & Ramdhana, 2024). However, alongside the evolution of cybercrimes and the increasing sophistication of digital transactions, the operational definition of this prevention system has begun to shift radically towards integrating technological intelligence instruments with advanced analytical capabilities and real-time early-warning features. This conceptual transformation of protection emphasizes that asset security can no longer rely solely on manual checks but must use automated data-processing infrastructures capable of eliminating information asymmetry between internal corporate parties and supervisory authorities. Therefore, an ideal fraud mitigation system must be a multi-layered defense ecosystem that is proactive, continuous, and fully adapted to modern digital advancements to ensure the integrity of operational records.

The categorization and manifestation of anti-fraud systems in the modern digital transformation era are tangibly realized through the implementation of various algorithmic detection and prevention tools distributed across all layers of the financial computing architecture. The most revolutionary manifestation of defense technology is the use of smart contracts based on cryptographic programming logic, which automatically execute and verify the payment terms of financial transactions only when all compliance provisions have been fully met (Louati et al., 2024). Another advanced analytical-level manifestation is the application of Federated Learning (FL) computational mechanisms that train artificial intelligence models to detect anomalies without exposing customer data confidentiality across different banking entities (Baabdullah et al., 2024). Additionally, this cyber prevention defense system is implemented through the adoption of Graph Neural Networks (GNNs), which possess deep analytical capabilities to map relationships among complex entities and detect fraud-syndicate patterns that are often invisible to traditional linear audit methods (Wei & Lee, 2024). This series of sophisticated automated detection technologies and decentralized prevention instruments is structurally interconnected and works synergistically to address the weaknesses of past conventional manual mechanisms. Ultimately, all these digital innovation manifestations coalesce into a holistic, robust anti-fraud defense system architecture that is proactive in addressing the escalation of global fraud threats and highly capable of protecting the stability of the entire economic sector infrastructure.

METHOD

The primary focus of this research is the phenomenon of financial manipulation and the defense mechanisms of the accounting system in Indonesia. Specifically, the scope of this research is divided into two main pillars: the exploitation of financial fraud and the architecture of the anti-fraud system itself. In the first pillar, this study highlights various forms, patterns, and mechanisms of financial fraud that visibly continue to occur and evolve within both financial institutions and government agencies in Indonesia. The selection of this object is based on the urgent need to understand the anatomy of financial crimes before formulating a comprehensive mitigation strategy. In the second pillar, the research focuses on evaluating and restructuring the anti-fraud system currently in use in the national financial context. The study of this second object is directed at exploring the extent to which blockchain technology can be technically implemented to address weaknesses in conventional defense systems that remain vulnerable to hacking and manipulation. According to the methodological literature, precisely defining research subjects and objects is crucial because these entities serve as the primary targets for data mining, ensuring that the entire analytical flow remains focused on resolving the core problem (Abdussamad, 2021). Thus, the formulation of these dual research objects is expected to provide a strong analytical foundation for comprehensively measuring the effectiveness of decentralized technology in addressing the complexities of financial data confidentiality crimes holistically.

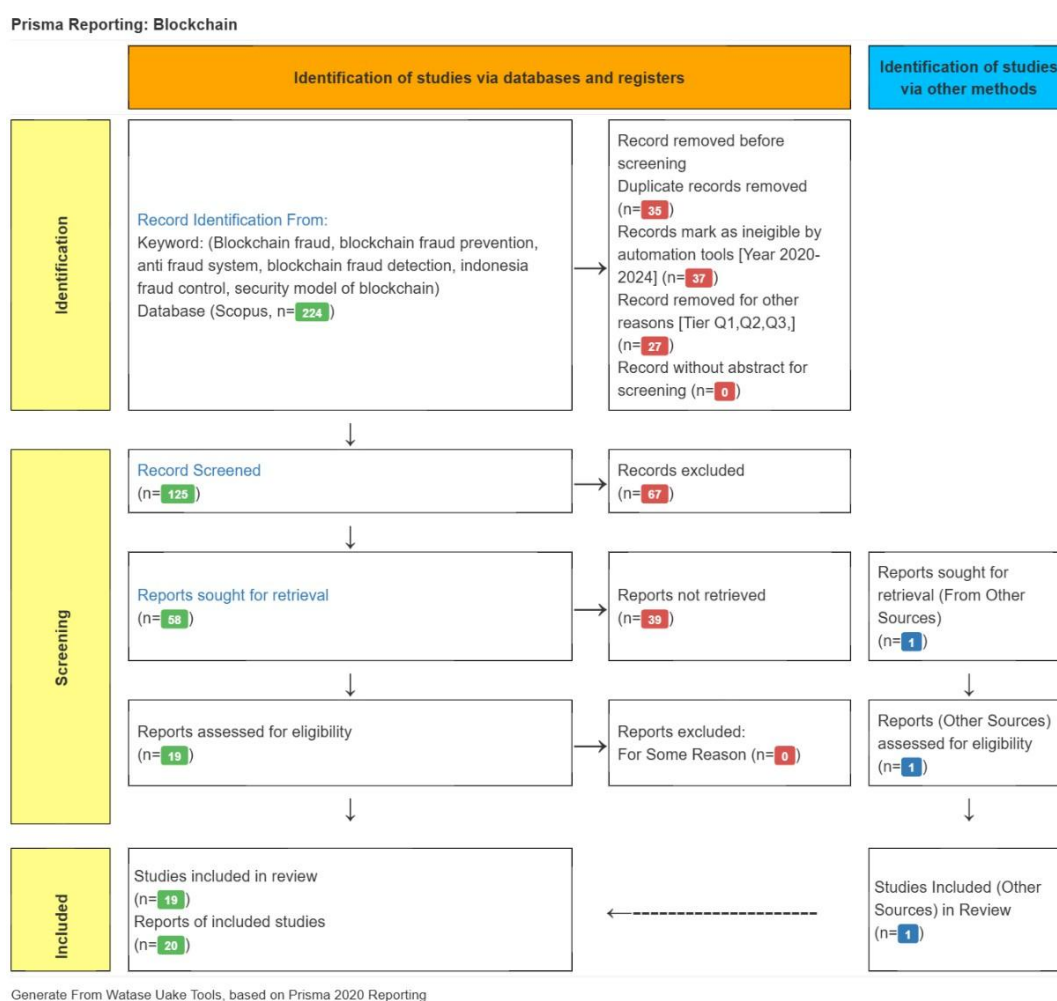
The methodological design of this scientific paper adopts a comprehensive qualitative approach, employing a Systematic Literature Review (SLR). The SLR framework was selected because it provides highly systematic, structured, and transparent procedures for collecting, identifying, and evaluating scientific papers directly relevant to the research topic. In executing this design, the researcher strictly adheres to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) protocol, which helps ensure the validity of the literature screening process and minimizes subjective bias in data synthesis (Page et al., 2021). In line with this approach, the research relies entirely on the utilization of two primary types of data instruments, namely primary data and secondary data, which are collected without involving direct field observation. The primary data instrument in this study comprises internationally published scientific manuscripts that present the latest findings, new theoretical understandings, and conceptual ideas on the use of decentralized technology in financial security systems. Meanwhile, the secondary data instrument is positioned as supporting literature, encompassing conceptual reference books, classical theory studies, and other bibliographic documents that do not originate directly from major research publications, yet still possess informational reliability. The collaboration between the qualitative SLR approach and this measurable data classification ultimately forms a solid methodological foundation for generating highly valid and academically accountable research conclusions.

The primary and secondary data instrument requirements for this research are sourced exclusively from verified academic literature. For primary data sources, the researcher specifically extracted internationally reputable scientific journal articles officially indexed in the Scopus database. The quality of these primary data sources is strictly maintained by selecting only publications ranked in Quartile 1 (Q1), Quartile 2 (Q2), or Quartile 3 (Q3) and published within the last five years, specifically between 2020 and 2024. The search for these high-standard literature sources was automated using the *Watase UAKE* platform, a web-based application specifically designed to facilitate digital footprint tracing in Systematic Literature Review (SLR)-based research (Kitchenham & Charters, 2007). On the other hand, secondary data sources were obtained from various foundational reference books that thoroughly examine decentralized technology architecture, such as *Basics of Blockchain*, *Beginning Blockchain*, *Mastering Blockchain*, and other relevant publications by experts in cryptography and digital economics. The use of these reference books is crucial for sharpening the theoretical foundation and enriching the comparative synthesis with recent journal findings. Thus, this highly selective and globally database-driven mapping of data sources ensures that

all arguments and discussions constructed in the research possess an exceptionally robust epistemological foundation.

The research execution and data collection techniques in this study were carried out through a series of highly organized, transparently documented literature-screening procedures. The research workflow began with preliminary study stages to map the phenomenon of financial crime, followed by problem formulation, metadata collection and processing, in-depth analysis, and concluded with comprehensive conclusions. During the data collection stage, the researcher conducted a targeted literature search on the *Watase UAKE* platform using strategic keywords, including *blockchain technology*, *fraud control*, *anti-fraud system*, *blockchain prevention*, and *blockchain detection*. To optimize search precision in the Scopus database, this search process also applied advanced Boolean logic operators, such as AND, OR, and NOT, to directionally broaden or narrow the scope of the identification results (Snyder, 2019). All captured literature results were evaluated against the inclusion and exclusion criteria in accordance with the PRISMA protocol, and English-language articles with full-text access on distributed ledgers were accepted. At the same time, non-Scopus articles or those published before 2020 were immediately excluded. Through a reduction process of the 224 initially identified journals, the screening and eligibility stages ultimately selected 19 high-quality journal articles as the primary sample for further review. This series of stringent, systematic data-collection stages is necessary to ensure the internal validity of the research and minimize information anomalies. To ensure strict methodological transparency, the systematic stages of literature identification, screening, and eligibility evaluation based on the PRISMA protocol are structured in Figure 3

Figure 3. PRISMA Diagram



Source: Data analysis results from WATASE UAE

After the entire literature collection stage was completed, the selected data were processed using an in-depth, structured analytical technique. Procedurally, the analytical framework within this systematic literature review methodology began by dissecting the key elements of each selected journal, including identifying the publication year variable, examining the theoretical foundation, evaluating the analytical methods, and extracting the final research results. Following this extraction stage, the researcher applied an interactive model data analysis technique, operationally consisting of four interconnected core processing pillars. The first pillar was comprehensive data collection, in which all relevant information on the application of decentralized technology in anti-fraud systems was compiled into a unified knowledge base. Subsequently, the researcher conducted the data reduction pillar, a critical filtering process to discard irrelevant peripheral information while simultaneously summarizing and restructuring fundamental points to maintain focus on the core formulation of the research problem (Miles et al., 2020). This process was followed by the data display pillar, where the reduced results were classified and visualized as categorization tables, graphs, or systematic textual narratives, thereby facilitating readers' understanding of the correlation patterns between technological variables and cybersecurity. This series of analytical processing culminated in the conclusion-drawing pillar, the final synthesis process in which the researcher evaluated all presented data to formulate a definitive academic answer regarding the effectiveness of blockchain in eradicating financial fraud in Indonesia.

RESULTS

The main finding from this Systematic Literature Review (SLR) is that the first pillar for revolutionizing the anti-fraud system relies entirely on the adoption of Blockchain Technology innovations. Based on 19 reputable Q1-Q3 publications from 2020 to 2024, the research data confirm that blockchain technology dominates cybersecurity discourse as a highly resilient distributed ledger technology. Bibliometric analysis results and mapping using VOSviewer explicitly position blockchain as a central node with the strongest correlations to fraud detection features, smart contracts, privacy and security, and federated learning. Fundamentally, findings from various Scopus journals indicate that this digital infrastructure operates by recording every financial transaction as a series of data blocks, encrypted using highly complex cryptographic hashing algorithms (Jannah et al., 2024). Once a transaction is successfully validated through a consensus approval mechanism by the majority of the computer network (nodes), the data record automatically becomes permanent and impossible to modify unilaterally (Ramesh et al., 2023).

Furthermore, this research data highlights the competitive advantage of blockchain over traditional databases, as its decentralized system eliminates the need for manual third-party verification, which is often slow and vulnerable to compromise. Thus, this data description clearly demonstrates that blockchain architecture is not merely an ordinary transaction-recording tool but rather a high-level security framework that guarantees absolute transparency, data immutability, and digital trail tracking. To reinforce the literature foundation for this analysis, Table 1 summarizes primary studies examining the application of blockchain technology in the financial sector.

Table 1. Journal of Blockchain Applications in the Financial Sector

Author(s)	Title
Tan-Vo, Khoa; Pham, Khanh; Huynh, Phu; Thi, Mong-Thy Nguyen; Ta, Thu-Thuy; Nguyen, Thu; Nguyen-Hoang, Tu-Anh; Dinh, Ngoc-Thanh; Nguyen, Hong-Tri	Optimizing Academic Certificate Management With Blockchain and Machine Learning: A Novel Approach Using Optimistic Rollups and Fraud Detection
Park, Keundug; Youm, Heung-Youl	Proposal of a Service Model for Blockchain-Based Security Tokens
Yakubu Bello Musa; Sabi'u Jamilu; Bhattarakosol Pattarasinee	Blockchain-based privacy and security model for transactional data in large private network
Kapadiya, Khyati; Patel, Usha; Gupta, Rajesh; Alshehri, Mohammad Dahman; Tanwar, Sudeep; Sharma, Gulshan; Bokoro, Pitshou N.	Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: An Analysis, Architecture, and 2022 Future Prospects
Pranto, Tahmid Hasan; Hasib, Kazi Tamzid Akhter Md.; Rahman, Tahsinur; Haque, Akm Bahalul; Islam, A. K. M. Najmul; Rahman, Rashedur M.	Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive-Based Approach
Marjanovic, Jelena; Dalcekovic, Nikola; Sladic, Goran	Blockchain-Based Model For Tracking Compliance With Security Requirements
Tsoulias, Konstantinos; Palaiokrassas, Georgios; Fragkos, Georgios; Litke, Antonios; Varvarigou, Theodora A.	A Graph Model-Based Blockchain Implementation for Increasing Performance and Security in Decentralized Ledger Systems
Islam, Umar; Alshammari, Abdullah; Alzaid, Zaid; Ahmed, Adeel; Abdullah, Saima; Iftikhar, Saman; Bawazeer,	Enhancing Blockchain Security Against Data Tampering: Leveraging Hybrid Model in Multimedia Forensics and Multi-Party

An in-depth explanation of the data findings on Blockchain Technology architecture reveals the underlying mechanism that enables it to eliminate financial data manipulation. The dominance of the blockchain node in the VOSviewer mapping indicates that this technology is not a standalone entity but is dynamically integrated with cutting-edge analytical methods to strengthen the defense layers of the financial system. Its central linkage with smart contracts, for instance, provides a logical explanation for why smart contract protocols will automatically block any payment execution if a transaction fails to meet the compliance parameters rigidly programmed into the network (Xiong et al., 2026). Additionally, the synchronization between decentralized ledgers and federated learning explains how various banking institutions can collaboratively train artificial intelligence models to recognize suspicious transaction patterns without sharing their customers' raw private data (Xiong et al., 2026). This technical explanation underscores that the absence of a single central authority in managing the database is precisely its greatest strength, eliminating the risk of centralized system failure. The multi-layered validation process, performed in real time by all nodes worldwide, ensures that any hacking attempt or the addition of falsified data will be immediately rejected because it will never reach the point of majority consensus. Overall, this data explanation demonstrates that the operability of blockchain-based systems constitutes a multi-layered defense ecosystem, in which every cryptographic code and automation logic works synergistically to protect financial assets from both internal and external threats.

If critically examined, the technical description and explanation of Blockchain Technology's superiority are highly relevant to addressing the reality of high financial crime rates, which is the core problem of this research. The reality of the research problem indicates that government agencies and large-scale corporations in Indonesia, such as in the ASABRI and Jiwasraya cases, frequently experience asset leakages amounting to trillions of rupiah due to the manipulation of centralized financial reporting systems. Within such fragile traditional systems, rogue internal elements with administrator authority can freely exploit security loopholes to alter audit trails, engage in double spending, or unilaterally disguise the flow of corrupt funds without detection by oversight bodies. The presence of decentralized recording mechanisms from this electronic ledger innovation directly attacks the root of the problem by revoking absolute control from individual hands and transferring it to a completely independent mathematical consensus system (Mahdani & Soufyan, 2026). The absolute transparency offered by the cryptographic blockchain ensures that every fund movement can be openly monitored by all stakeholders in real time, thereby effectively neutralizing the element of opportunity in corporate fraud theory.

Furthermore, data immutability within this computerized network ensures that verified reports are impossible to engineer to retroactively cover up tracks of new fraudulent activities. Thus, this causal relationship asserts that decentralized technology transformation is not merely a theoretical discourse but rather the most appropriate and effective antithesis to dismantling the corrupt ecosystems long rooted in the vulnerabilities of conventional databases. As a more comprehensive architectural comparison, Table 2 outlines the fundamental differences between the vulnerabilities of traditional centralized systems and the advantages of blockchain-based decentralized systems.

Table 2. Differences Between Centralized and Decentralized Systems

Aspect	Centralized System	Decentralized System
Trust	Relies on a single entity or a third party for data management and oversight.	Does not require trust in a third party; trust is automatically established.

Security	Vulnerable to attacks due to possessing a <i>single point of failure</i> .	More resilient against attacks as data is distributed across multiple nodes.
Privacy	Privacy is frequently threatened, including the potential for misuse or the sale of user data.	Privacy is better protected as data is distributed and difficult to access without authorization.
Cost and Time	Requires high costs for infrastructure and maintenance, resulting in slower transaction processes.	Incurs lower costs due to the elimination of intermediaries, resulting in faster transactions.
Transaction Verification	Relies on a single entity to verify transactions, rendering it more susceptible to errors or manipulation.	Verification is easier, faster, and authentic as it utilizes consensus within the network.
Transparency	Transparency is limited because data access is controlled by a central entity.	Transparency is high because data is available across the entire network and can be viewed by all nodes.
System Characteristics	Centralized, vulnerable to data modification or manipulation by authorized parties.	Decentralized and immutable, making it more reliable for permanent data recording.

The second pillar of these research findings focuses on an in-depth analysis of the escalation and spread patterns of Financial Fraud that are detrimental to Indonesia's economy. Based on a review of 19 reputable Q1 to Q3 journals and official audit document data, this research presents statistical evidence showing that financial deviance incidents are an endemic disease that is continuously eroding various strategic sectors. The 2022 ACFE report indicates that an average of five percent of corporate revenue worldwide is lost annually due to manipulative acts, with Indonesia ranking fourth in the Asia-Pacific region, predominantly driven by corruption and asset misappropriation cases. Findings from national corruption statistical literature also recorded a dramatic surge in 2023, with hundreds of financial crime cases ensnaring thousands of suspects and resulting in potential state losses reaching tens of trillions of rupiah. Based on the bibliometric mapping conducted, this financial crime entity has a tightly knit network cluster with issues of cyber hacking, record collusion, and information asymmetry that severely disadvantage external supervisory parties (Igou et al., 2023; Pimentel & Boulianne, 2020). This data indicates that, among numerous organized fraud schemes, financial statement fraud is the most difficult type of deception to detect because it is often disguised by hidden modifications to transaction timing. This empirical description clearly asserts that the crime of fund confidentiality is not just a random anomaly but a systemic, structured cycle that exploits administrative vulnerabilities and loopholes.

Looking further into these findings, the explanation for the rampant phenomenon of Financial Fraud culminates in the fragility of multi-layered supervisory architectures and the high internal motivation of perpetrators across various institutions. The surge in large-scale fraud and corruption cases recorded in national statistical data can be scientifically explained by the Fraud Hexagon theory, in which internal managerial figures often face financial pressures or opportunities that encourage them to act fraudulently without hesitation. Literature reviews reveal that these accounting crimes are growing rapidly because conventional centralized database systems provide an absolute opportunity for authority holders to rationalize their actions without fear of immediate detection by independent auditors (Louati et al., 2024). When an administrator or authorized official has sole access to the operational recording system, they can easily collude with colleagues to modify asset figures, manipulate physical inventory flows, and unilaterally destroy digital evidence before an investigation takes

place. Moreover, economic losses reaching five percent of a commercial entity's total annual revenue explain the massive impact of lacking an automated, real-time, and transparent verification mechanism. The high level of arrogance and technical mastery of rogue bureaucratic elements enables them to silently and continuously breach manual-control barricades. Overall, the explanation of this money-laundering and manipulation phenomenon shows that, no matter how slowly improvements are implemented, outdated architectural loopholes will continue to be exploited by professional corruptors for personal gain.

Connecting the description and explanation of the Financial Fraud escalation reveals a very tight causal relationship with the regulatory deadlocks and technical operational hurdles that have been crucial research problems. The fundamental problem in the field is the powerlessness of administrative legal systems, the application of conventional sanctions, and government bureaucracy in suppressing the rates of mega-scale corruption and investment fraud, as experienced by state-owned entities in Indonesia. Data showing an upward trend in annual criminal acts of fund misappropriation directly correlates with the fact that prevention efforts so far treat symptoms only at the final stage, without daring to revolutionize the recording technology infrastructure behind them. The modus operandi of altering transaction times or creating fictitious corporate revenues can recur continuously solely due to the absence of an open electronic ledger that must be mutually approved by an independent supervisory network (Mohammed et al., 2023). When data records presented by fraud perpetrators cannot be immediately cross-verified by anomaly-tracking machines, audit teams, and law enforcement officials will always remain one step behind cybercriminals' ingenuity. This causal relationship demonstrates that reliance on inspection procedures based solely on employees' trust and moral integrity has proven obsolete, both practically and empirically. Therefore, linking the reality of the fragile centralized database security architecture to the escalation of trillion-rupiah fund thefts further underscores the urgent need to transition to an anti-manipulation security automation system.

The third analytical focus of this Systematic Literature Review examines the operational effectiveness of modern, computationally automated Anti-Fraud Systems that are widely developed in various international journals. Data extracted from 19 reputable scientific papers indicate that most future financial security designs prioritize modernizing intrusion detection supervisory architectures and developing instantaneous automated warning mechanisms. From the existing bibliometric mapping, it is evident that this cyber protection ecosystem is beginning to shift away from the dominance of conventional anonymous reporting regulations by adopting machine learning tools to filter massive volumes of transaction anomalies. Data extraction results demonstrate that integrating artificial intelligence decision-tree methods, such as Random Forest and XGBoost, with encrypted electronic ledgers can achieve financial fraud detection accuracy rates exceeding 90% (Ashfaq et al., 2022). Furthermore, study data from these various applied research studies show that the success of a security framework is no longer measured by how strictly a company's report is audited at each financial year-end, but is determined by the network's computational speed in blocking fraudulent transactions moments before they are permanently recorded on the main server. Several articles also present the development of highly complex computational graph algorithms to hack syndicate fraud network patterns involving multinational manipulations. The description of this data reflects a drastic paradigm shift, in which fund security mechanisms are evolving towards an algorithmic ecosystem entirely controlled by cutting-edge applied science. Further details on the specific literature focusing on integrating these computational instruments for financial crime mitigation can be found in Table 3.

Table 3. Journals on the Application of Blockchain in Preventing and Detecting Financial Fraud

Author(s)	Title
Ahmed, Ahmed Abdelmoamen; Alabi, Oluwayemisi O.	Secure and Scalable <i>Blockchain</i> -Based Federated Learning for Cryptocurrency <i>Fraud</i> Detection: A Systematic Review
Mapa Mudiyansele, Chalani; Perera, Pethigamage; Grandhi, Sriamannarayana	A <i>Blockchain</i> -Based Model for the Prevention of Superannuation <i>Fraud</i> : A Study of Australian Super Funds
Baabdullah, Tahani; Alzahrani, Amani; Rawat, Danda B.; Liu, Chunmei	Efficiency of Federated Learning and <i>Blockchain</i> in Preserving Privacy and Enhancing the Performance of Credit Card <i>Fraud</i> Detection (CCFD) Systems
Wei, Sizheng; Lee, Suan	Financial Anti- <i>Fraud</i> Based on Dual-Channel Graph Attention Network
Pranto, Tahmid Hasan; Hasib, Kazi Tamzid Akhter Md.; Rahman, Tahsinur; Haque, Akm Bahalul; Islam, A. K. M. Najmul; Rahman, Rashedur M.	<i>Blockchain</i> and Machine Learning for <i>Fraud</i> Detection: A Privacy-Preserving and Adaptive Incentive-Based Approach
Mohammed, Mohammed A.; Boujelben, Manel; Abid, Mohamed	A Novel Approach for <i>Fraud</i> Detection in <i>Blockchain</i> -Based Healthcare Networks Using Machine Learning
Lyu, Qiuyun; Li, Hao; Zhou, Renjie; Zhang, Jilin; Zhao, Nailiang; Liu, Yan	BCFDPS: A <i>Blockchain</i> -Based Click <i>Fraud</i> Detection and Prevention Scheme for <i>Online</i> Advertising
Bellagarda, Jagger; Abu-Mahfouz, Adnan M.	Connect2NFT: A Web-Based, <i>Blockchain</i> Enabled NFT Application with the Aim of Reducing <i>Fraud</i> and Ensuring Authenticated Social, Non-Human Verified Digital Identity
Ashfaq, Tehreem; Khalid, Rabiya; Yahaya, Adamu Sani; Aslam, Sheraz; Azar, Ahmad Taher; Alsafari, Safa; Hameed, Ibrahim A.	A Machine Learning and <i>Blockchain</i> Based Efficient <i>Fraud</i> Detection Mechanism

Further elaboration of the computational Anti-Fraud System paradigm shift provides a logical explanation for the urgency of enhancing artificial intelligence capabilities to proactively respond to hacking threats without human intervention. The explanation for the high precision rate of predictive algorithms shows that modern cloud computing possesses an extraordinary ability to learn the entire history of financial behavior, identify shifting trends, and block the execution of funds that deviate even slightly from the normal activity patterns of application users (Ahmed & Alabi, 2024; Lyu et al., 2022). The use of collaborative Federated Learning architectures, heavily highlighted in the literature, can be understood as an innovation in which various banking institutions exchange artificial intelligence parameters to thwart fraud without exposing their customers' private details to the public domain. This cross-company protection collaboration mechanism effectively eliminates operational information asymmetry, which criminals have long exploited to smuggle illegal funds through blind supervisory loopholes. Furthermore, the integration of these automated cyber defense instruments provides an economic explanation: deploying software patrols is considered strategically far more profitable than hiring external investigative firms prone to observational errors or even to involvement in recording bribery scandals. Overall, the explanation for utilizing this cryptographically systemized machine intelligence underscores that the foundation of internal

control governance must no longer rely solely on the reliability of supervisory staff but must be anchored in the precision of computational algorithms.

If a comprehensive synthesis is drawn at the end of the data analysis, the correlation between the precise operational capabilities of Anti-Fraud Systems and the resolution of real-world rampant asset breaches reveals the most cutting-edge systematic reconstruction solution. The reality of the crises continuously haunting the stability of the banking sector and the integrity of financial governance in Indonesia today is the sluggishness of manual investigative procedures in tracing a series of document irregularities, which grants perpetrators of corruption crimes lenient time to launder their illicit proceeds. This administrative crime emergency correlates strongly with the absence of a reactive cybersecurity infrastructure holding the authority to instantaneously block accounts exactly when the bounds of electronic transaction fairness parameters have been violated. Through the innovative fusion of artificial intelligence-based automated tracking software and the cryptographic wall resilience of distributed databases, these conventional supervisory loopholes can be eliminated immediately, as machine intervention will replace the role of human authorization validation, which can often be bought or unilaterally compromised (Selvarajan et al., 2023). The empirical evidence in this problem resolution proves that modernizing decentralized audit mechanisms is not merely an aesthetic database accessory but a surgical instrument for legal compliance procedures, ensuring their execution operates with absolute transparency. In conclusion, adapting early detection architectures with autonomous, multi-layered computational security is a necessity—a final defense strategy to fortify the stability of national monetary flows against a spectrum of destruction.

DISCUSSION

A. The Effectiveness of Blockchain Decentralization as an Anti-Fraud System Revolution

A comprehensive analysis of these research findings empirically demonstrates that the transformation of digital architecture through distributed ledger technology is not merely a software update but a radical overhaul of the philosophy of trust within the financial system. The decentralized configuration embedded in the consensus mechanism successfully eliminates absolute dependence on the moral integrity of individuals or entities, which has thus far proven highly vulnerable to exploitation. Analytically, the cryptographic network's success in validating trillions of data points instantaneously demonstrates that the loophole for manipulation can be tightly closed when verification is delegated to mathematical algorithms devoid of subjective interests. Furthermore, the database's ability to maintain information immutability breaks the perpetrators' rationalization cycle, as any attempt to engineer reports will instantly trigger systemic rejection across all supervisory nodes. From a system capability perspective, integrating artificial intelligence into this ecosystem automatically removes information asymmetry barriers that often become a fatal weakness in conventional audit procedures. This analytical reality asserts that the essence of fraud eradication no longer lies in how many punitive regulations are enacted, but rather in how resilient the data storage architecture is in rejecting both external and internal interventions. The analytical conclusion drawn from this series of findings is that the future of national economic stability depends heavily on accelerating the transition to an autonomous recording infrastructure immune to corrupt negotiations.

Upon analyzing the comparative discourse between this study and prior literature, a clear demarcation emerges regarding the superiority of the analytical framework presented. The majority of previous studies tend to be trapped in reactive mitigation approaches centered on post-incident legal sanctions or mere normative compliance evaluations without addressing the root weaknesses of the technological infrastructure (Park & Youm, 2024). In contrast to such conservative views, this research boldly deconstructs the old paradigm by positioning cryptographic technology as a proactive prevention instrument that neutralizes criminal intent

right from the transaction initiation stage. Another comparative advantage lies in this study's ability to marry the theory of financial deviance behavior with high-level computational architecture solutions, an analytical hybridization that is very rarely explored by forensic accounting researchers in developing countries (Li, 2023). While other research focuses solely on the scale of digital currency implementation, this investigation specifically uncovers the utility of distributed ledgers as a state asset-protection ecosystem and a real-time audit instrument. This hybridization proves that resolving money laundering problems can no longer rely on a monodisciplinary approach but demands the integration of financial criminology with cybersecurity software engineering. This discursive positioning ultimately affirms that the research results provide a mitigation roadmap that is far more comprehensive, precise, and measurable than the patchwork solutions conventionally recommended in the academic literature.

Reflecting on the results of these analytical findings, a strong signal emerges that the fundamental objective of this research has been fully achieved in dissecting the solution to the public trust crisis. The research results reflect the reality that transitioning to a decentralized architecture is not merely utopian discourse but a logical imperative capable of fortifying economic integrity against systemic ruin. The success in mapping the specific functions of smart contracts and consensus mechanisms as anti-manipulation instruments serves as a primary indicator that this literature successfully provides concrete answers to the deadlocks of traditional supervisory systems. This reflection also yields immense strategic benefits, as policymakers now possess a robust epistemological foundation to begin a total overhaul of audit regulations that have historically proven obsolete. Moreover, the in-depth identification of various technical hurdles, such as scalability issues and legal framework gaps, reflects the research's objectivity, demonstrating that this study does not intend to glorify technology unquestioningly. The disclosure of these operational obstacles is highly beneficial as an early warning sign for banking institutions and state agencies, enabling them to formulate a technological migration blueprint in a measured, gradual manner. Through this holistic reflection, the essence of the research's usefulness does not stop at contributing to the academic literature; it becomes a strategic guiding document crucial to efforts to salvage trillions of rupiah in national assets in the future. A systematic mapping of the literature highlighting various technical, operational, and regulatory constraints to adopting this technology is presented in Table 4.

Table 4. Journal Analysis of the Challenges and Barriers Faced in the Implementation of *Blockchain* in the Accounting Sector

Author(s)	Title
Louati, Hassen; Louati, Ali; Almekhlafi, Abdulla; ElSaka, Maha; Alharbi, Meshal; Kariri, Elham; Altherwy, Youssef N.	Adopting Artificial Intelligence to Strengthen Legal Safeguards in <i>Blockchain</i> Smart Contracts: A Strategy to Mitigate <i>Fraud</i> and Enhance Digital Transaction Security
Marjanovic, Jelena; Dalcekovic, Nikola; Sladic, Goran	<i>Blockchain</i> -based model for tracking compliance with security requirements
Li, Jia	Dynamic financial and monetary security risk assessment based on information service security assessment model and <i>blockchain</i>
Selvarajan, Shitharth; Srivastava, Gautam; Khadidos, Alaa O.; Khadidos, Adil O.; Baza, Mohamed; Alshehri, Ali; Lin, Jerry Chun-We	An artificial intelligence lightweight <i>blockchain</i> security model for security and privacy in IIoT system
Yakubu Bello Musa, Sabi'u Jamilu, Bhattarakosol Pattarasinee	<i>Blockchain</i> -based privacy and security model for transactional data in large <i>private</i> network

Lyu, Qiuyun; Li, Hao; Zhou, Renjie;
Zhang, Jilin; Zhao, Nailiang; Liu, YanBCFDPS: A *Blockchain*-Based Click *Fraud*
Detection and Prevention Scheme for *Online*
Advertising

B. Strategic Implications, Causality Rationale, and Implementation Roadmap

Delving further into the implications, the results of this analytical investigation have significant structural consequences for the governance of financial institutions and the national supervisory architecture. The most crucial implication of proving the effectiveness of decentralized ledgers is the revolutionary demand that banking institutions and financial audit boards fundamentally restructure their standard operating procedures for auditing. These research findings implicitly force the banking ecosystem to abandon sluggish historical reporting methods and transition entirely to real-time validation mechanisms authorized by computational consensus. Other practical implications target lawmakers, where the legalization of digital assets and the legal recognition of smart contract validity must be enacted immediately to comprehensively umbrella digital transformation (Mapa Mudiyansele et al., 2023; Marjanović et al., 2023). Without progressive adjustments to regulatory frameworks, the prowess of these security algorithms will be rendered futile as they lack binding jurisdictional power in courts. In addition, these findings also have implications for overhauling accounting and finance education curricula, which are now required to integrate data science and cryptographic engineering disciplines to produce an adaptive generation of investigative auditors. Macroscopically, the successful implementation of this research's recommendations will directly lead to a drastic improvement in the national anti-corruption perception index, which in turn will restore the foreign investment climate and solidify the foundation of macroeconomic resilience against recession threats stemming from banking liquidity breaches.

Analyzing the causal rationale behind the highly effective performance of this technology reveals that the root cause lies in the mathematical construction of cryptography, which absolutely rejects human compromise. Research results indicate that the near-perfect security level is due to the decentralized architecture, which distributes the burden of trust across thousands of independent computers, thereby eliminating the single point of failure that has long been a prime target for hackers (Mohammed et al., 2023). The inability of perpetrators to manipulate financial reports arises because any attempt to alter a single data point requires them to hack the entire chain of blocks before a new block is created—a computational challenge that is theoretically impossible to accomplish without controlling the majority of global computing power. The high precision in detecting anomalies is also attributed to the network's integration with federated machine learning methods, which constantly update their algorithmic knowledge base based on billions of cross-jurisdictional transaction patterns unceasingly (Baabdullah et al., 2024). The combination of the strict programming logic of smart contracts and the absence of emotional intervention in the verification process neutralizes the psychological instruments that corruptors frequently use to pressure subordinates or bribe auditors. In essence, the reason the results of this decentralization-based exploitation are so superior at eradicating potential for fraud is that the system radically transfers decision-making authority from fallible human entities to mathematical algorithms that are entirely blind to material seductions.

Based on the crystallized understanding of all these causality analyses and implications, there is a series of urgent strategic actions that must be absolutely executed immediately by stakeholders. The most crucial first step is initiating cross-sectoral collaboration among Bank Indonesia, the Financial Services Authority (*Otoritas Jasa Keuangan*), and the Ministry of Communication and Information Technology to draft a standardized national distributed ledger architecture blueprint (Ahmed & Alabi, 2024). The government must immediately establish a national banking consortium to launch a pilot project to implement a semi-private cryptographic network dedicated to monitoring the flow of social assistance funds

and state capital injections. The subsequent crucial action is the massive allocation of specialized budgets by the banking sector to upgrade cloud computing infrastructure and build high-level data centers to address transaction scalability challenges. In the legislative domain, the House of Representatives (*Dewan Perwakilan Rakyat*) must prioritize the formulation of consensus-based electronic data protection legislation that provides a definitive legal umbrella for the validity of smart contracts as legitimate evidence in court. At the institutional managerial level, the boards of directors of public companies are obligated to immediately organize large-scale digital transition training programs to prepare competent accounting human resources capable of operating forensic algorithms. This series of tactical and continuous actions is not merely a theoretical recommendation but an execution roadmap that must be implemented immediately if this nation genuinely intends to break the entrenched chain of corporate fraud.

CONCLUSION

Unveiling the vulnerabilities that have long shrouded the national economic infrastructure, this research convincingly demonstrates that heavy reliance on centralized supervisory systems is a systematic form of financial suicide. The traditional database architecture is, in reality, nothing more than a fragile safe, the keys to which are voluntarily handed over to white-collar predators. The emergence of distributed ledger technology stands out as a brutal revolution that strips away the weaknesses of conventional audit procedures, empirically proving that trillion-rupiah financial statement manipulation can be suffocated from the very first second a transaction is initiated. Decentralized mathematical cryptography successfully destroys the hegemony of corrupt internal individuals by creating a consensus chain that is completely impenetrable and non-negotiable by any entity. The manifestation of these radical findings constitutes a monumental contribution by theoretically deconstructing the classic fraud hexagon paradigm through cutting-edge technological determinism, in which the immutability of programming code eliminates criminal opportunity and rationalization. On a practical level, this study materializes tangibly as a state asset-rescue blueprint, providing precise navigational guidelines for monetary authorities to design high-level, multi-layered cyber defense infrastructures. Furthermore, it grants robust academic legitimacy for national banking leaders to justify massive investments in adopting smart contracts and federated machine learning. Ultimately, this paradigm shift transforms decentralized technology into a primary foundation for institutional treasury governance, guaranteeing absolute transparency and thereby directly restoring the dignity and credibility of the national economic system.

Behind the glamour of the conceptual revolution on offer, this academic exploration consciously and objectively acknowledges a series of scope limitations that open the gates wide to far more massive future explorations. The foremost limitation in the execution of this systematic literature review is the lack of direct empirical simulation trials assessing the reliability of decentralized networks when applied to actual central ministry agencies or local banking institutions. The research focus, which is concentrated on international-scale secondary literature analysis, has not been fully capable of measuring and mapping the level of cultural resistance within the Indonesian government bureaucracy if this system of absolute transparency is subsequently enforced in full. Therefore, this series of limitations inherently outlines a highly stimulating roadmap for opening up opportunities for subsequent research development based on field experimental methodologies. Cross-disciplinary scientists and academic practitioners in the future are strongly encouraged to begin designing national-scale empirical studies focused entirely on testing the performance of anomaly detection algorithms using samples of real Indonesian Rupiah transaction data. Further analytical exploration is urgently needed to design a comprehensive legislative framework that bridges the sharp gap between the positive law of the Indonesian judiciary and the geographically borderless jurisdiction of smart contracts. Through this continuous relay of academic research, the noble aspiration to establish an indestructible pillar of the financial defense system will soon evolve from a mere academic utopia on paper into a reality of genuine security civilization.

REFERENCES

- Abdussamad, Z. (2021). *Metode Penelitian Kualitatif*. Syakir Media Press.
- Ahmed, A. A., & Alabi, O. O. (2024). Secure And Scalable Blockchain-Based Federated Learning For Cryptocurrency Fraud Detection: A Systematic Review. *Ieee Access*, 12, 102219–102241. <https://doi.org/10.1109/Access.2024.3429205>
- Anandya, D., & Ramdhana, K. (2024). Laporan Hasil Pemantauan Tren Korupsi Tahun 2023.
- Arianto, B., Dinata, R. O., Ridhawati, R., Indarto, S. L., Syahrir, D. K., Rukmana, A. Y., Faisol, I. A., Yusran, M., & Andaningsih, I. R. (2023). *Akuntansi Forensik* (D. P. Sari, Ed.). Getpress Indonesia.
- Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A Machine Learning And Blockchain Based Efficient Fraud Detection Mechanism. *Sensors* 2022, Vol. 22, Page 7162, 22(19), 7162. <https://doi.org/10.3390/S22197162>
- Association Of Certified Fraud Examiners. (2022). Report To Members 2022.
- Baabdullah, T., Alzahrani, A., Rawat, D. B., & Liu, C. (2024). Efficiency Of Federated Learning And Blockchain In Preserving Privacy And Enhancing The Performance Of Credit Card Fraud Detection (Ccfd) Systems. *Future Internet* 2024, Vol. 16, Page 196, 16(6), 196. <https://doi.org/10.3390/Fi16060196>
- Bashir, I. (2023). *Mastering Blockchain : Inner Workings Of Blockchain, From Cryptography And Decentralized Identities, To Defi, Nfts And Web3*. Packt Publishing.
- Igou, A., Power, D. J., Brosnan, S., & Heavin, C. (2023). Digital Futures For Accountants. *Journal Of Emerging Technologies In Accounting*, 20(1), 39–57. <https://doi.org/10.2308/Jeta-2020-088>
- Jannah, R., Sari, M. P., Utaminingsih, N. S., & Alirastra Budiantoro, R. (2024). A Bibliometric Analysis Of Artificial Intelligence And Blockchain Technology In Fraud Prevention And Detection. *Akuisisi : Jurnal Akuntansi*, 20(1), 96–115. <https://doi.org/10.24127/Akuisisi.V20i1.2193>
- Kitchenham, B., & Charters, S. (2007). Guidelines For Performing Systematic Literature Reviews In Software Engineering. Technical Report, Ebse Technical Report Ebse-2007-01.
- Li, J. (2023). Dynamic Financial And Monetary Security Risk Assessment Based On Information Service Security Assessment Model And Blockchain. *Scientific Reports* 2023 13:1, 13(1), 18707-. <https://doi.org/10.1038/S41598-023-45977-5>
- Louati, H., Louati, A., Almekhlafi, A., Elsaka, M., Alharbi, M., Kariri, E., & Altherwy, Y. N. (2024). Adopting Artificial Intelligence To Strengthen Legal Safeguards In Blockchain Smart Contracts: A Strategy To Mitigate Fraud And Enhance Digital Transaction Security. *Journal Of Theoretical And Applied Electronic Commerce Research* 2024, Vol. 19, Pages 2139-2156, 19(3), 2139–2156. <https://doi.org/10.3390/Jtaer19030104>
- Lyu, Q., Li, H., Zhou, R., Zhang, J., Zhao, N., & Liu, Y. (2022). Bcfdps: A Blockchain-Based Click Fraud Detection And Prevention Scheme For Online Advertising. *Security And Communication Networks*, 2022(1), 3043489. <https://doi.org/10.1155/2022/3043489>
- Mahdani, R., & Soufyan, D. A. (2026). Blockchain And Ai In Combating Financial Corruption: A Systematic Literature Review. *Journal Of Central Banking Law And Institutions*, 5(1), 125–152. <https://doi.org/10.21098/Jcli.V5i1.412>
- Mapa Mudiyansele, C., Perera, P., & Grandhi, S. (2023). A Blockchain-Based Model For The Prevention Of Superannuation Fraud: A Study Of Australian Super Funds. *Applied Sciences* 2023, Vol. 13, Page 9949, 13(17), 9949. <https://doi.org/10.3390/App13179949>
- Marjanović, J., Dalčević, N., & Sladić, G. (2023). Blockchain-Based Model For Tracking Compliance With Security Requirements. *Computer Science And Information Systems*, 20(1), 359–380. <https://doi.org/10.2298/Csis210923060m>

- Maulani, I. E., Herdianto, T., Syawaludin, D. F., & Laksana, M. O. (2023). Penerapan Teknologi Blockchain Pada Sistem Keamanan Informasi. *Jurnal Sosial Teknologi*, 3(2), 99–102. <https://doi.org/10.59188/Journalsostech.V3i2.634>
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2020). *Qualitative Data Analysis* (4th Ed.). Sage Publication.
- Mohammed, M. A., Boujelben, M., & Abid, M. (2023). A Novel Approach For Fraud Detection In Blockchain-Based Healthcare Networks Using Machine Learning. *Future Internet* 2023, Vol. 15, Page 250, 15(8), 250. <https://doi.org/10.3390/Fi15080250>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The Prisma 2020 Statement: An Updated Guideline For Reporting Systematic Reviews. *Bmj*, 372. <https://doi.org/10.1136/Bmj.N71>
- Park, K., & Youm, H. Y. (2024). Proposal Of A Service Model For Blockchain-Based Security Tokens. *Big Data And Cognitive Computing* 2024, Vol. 8, Page 30, 8(3), 30. <https://doi.org/10.3390/Bdcc8030030>
- Pimentel, E., & Boulianne, E. (2020). Blockchain In Accounting Research And Practice: Current Trends And Future Opportunities. *Accounting Perspectives*, 19(4), 325–361. <https://doi.org/10.1111/1911-3838.12239>
- Pranto, T. H., Hasib, K. T. A. M., Rahman, T., Haque, A. B., Islam, A. K. M. N., & Rahman, R. M. (2022). Blockchain And Machine Learning For Fraud Detection: A Privacy-Preserving And Adaptive Incentive Based Approach. *Ieee Access*, 10, 87115–87134. <https://doi.org/10.1109/Access.2022.3198956>
- Ramesh, A., Eeswaran, M., Roslan, F. F., & Arumugam, D. (2023). Effectiveness Of Blockchain Technology In Preventing Financial Fraud: A Study Among Public Listed Companies In Malaysia. *Electronic Journal Of Business And Management*, 8(S2), 1–19. <https://doi.org/10.65136/Ejbm.V8is2.196>
- Selvarajan, S., Srivastava, G., Khadidos, A. O., Khadidos, A. O., Baza, M., Alshehri, A., & Lin, J. C. W. (2023). An Artificial Intelligence Lightweight Blockchain Security Model For Security And Privacy In Iot Systems. *Journal Of Cloud Computing* 2023 12:1, 12(1), 38-. <https://doi.org/10.1186/S13677-023-00412-Y>
- Shonhadji, N., & Irwandi, S. A. (2024). Fraud Prevention In The Indonesian Banking Sector Using Anti-Fraud Strategy. *Banks And Bank Systems*, 19(1), 12–23. [https://doi.org/10.21511/Bbs.19\(1\).2024.02](https://doi.org/10.21511/Bbs.19(1).2024.02)
- Sigit, R. (2022). Apa Itu Blockchain: Sejarah, Cara Kerja, Kelebihan Dan Kekurangan. https://www.cryptomedia.id/cryptopedia/mengenal-blockchain/#Cara_Kerja_Blockchain
- Snyder, H. (2019). Literature Review As A Research Methodology: An Overview And Guidelines. *Journal Of Business Research*, 104, 333–339. <https://doi.org/10.1016/J.Jbusres.2019.07.039>
- Tan-Vo, K., Pham, K., Huynh, P., Thi, M. T. N., Ta, T. T., Nguyen, T., Nguyen-Hoang, T. A., Dinh, N. T., & Nguyen, H. T. (2024). Optimizing Academic Certificate Management With Blockchain And Machine Learning: A Novel Approach Using Optimistic Rollups And Fraud Detection. *Ieee Access*, 12, 168135–168159. <https://doi.org/10.1109/Access.2024.3486029>
- Vasquez, G. (2021). An Introduction To Blockchain - The Cpa Journal. *The Cpa Journal*. <https://www.cpajournal.com/2021/08/18/An-Introduction-To-Blockchain/>
- Warburg, Bettina., Wagner, Bill., & Serres, Tom. (2019). *Basics Of Blockchain: A Guide For Building Literacy In The Economics, Technology, And Business Of Blockchain*. Animal Ventures.

- Wei, S., & Lee, S. (2024). Financial Anti-Fraud Based On Dual-Channel Graph Attention Network. *Journal Of Theoretical And Applied Electronic Commerce Research* 2024, Vol. 19, Pages 297-314, 19(1), 297–314. <https://doi.org/10.3390/jtaer19010016>
- Xiong, W., Hu, Y., & Wan, D. (2026). A Blockchain-Based Smart Contract Framework For Fraud-Resistant Financial Product Advisory. *Peerj Computer Science*, 12(4), E3834. <https://doi.org/10.7717/Peerj-Cs.3834/Supp-4>
- Zainuddin, M. A. (2023). *Pengenalan Dan Implementasi Teknologi Blockchain Pada Web 3.0*. Deepublish.