The current issue dan full text archive of this journal is available at
https://e-journal.unair.ac.id/jraba/index
Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 10 No. 1 (2025) 36-51 ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

COMBATTING FRAUD IN STATE-OWNED ENTERPRISES USING BLOCKCHAIN AND IOT TECHNOLOGIES

Muhammad Syahrudin[1*]
Sani Susanto[2]

ABSTRACT

Fraud in strategic sectors such as energy and finance, particularly within state-owned enterprises, remains a critical challenge to national economic integrity. Despite increased state revenues, the incidence of fraud continues to rise, highlighting the urgent need for robust technological interventions. This study aims to explore how Blockchain and Internet of Things (IoT) technologies have been utilized in anti-fraud systems over the past decade. Employing a Systematic Literature Review (SLR) approach guided by the PRISMA framework and conducted using the Watase Uake platform, this study analyzed 69 articles indexed in Scopus from 2015 to 2025. The analysis revealed a significant rise in research activity on this topic since 2019, peaking in 2022. The findings indicate that Blockchain's decentralization and immutability, combined with IoT's real-time monitoring capabilities, create a synergistic effect in enhancing fraud detection and prevention mechanisms. Empirical examples, such as fuel distribution frau d in Pertamina, illustrate how these technologies can reduce information asymmetry and improve audit quality. This study contributes to the literature by offering an integrated framework for leveraging emerging technologies in building transparent, secure, and efficient anti-fraud systems.

Keyword: *blockchain; iot; anti-fraud systems;state-owned enterprises; fraud prevention*

ARTICLE INFO

***Article History*:**

Received: 28 April 2025

Accepted: 1 July 2025

Available online: 31 July 2025

ABSTRAK

Penipuan di sektor strategis seperti energi dan keuangan, terutama di perusahaan milik negara, tetap menjadi tantangan kritis bagi integritas ekonomi nasional. Meskipun pendapatan negara meningkat, insiden penipuan terus meningkat, menyoroti kebutuhan mendesak akan intervensi teknologi yang kuat. Studi ini bertujuan untuk mengeksplorasi bagaimana teknologi Blockchain dan Internet of Things (IoT) telah digunakan dalam sistem anti-penipuan selama dekade terakhir. Menggunakan pendekatan Systematic Literature Review (SLR) yang dipandu oleh kerangka kerja PRISMA dan dilakukan melalui platform Watase Uake, studi ini menganalisis 69 artikel yang terindeks di Scopus dari tahun 2015 hingga 2025. Analisis menunjukkan peningkatan signifikan dalam aktivitas penelitian pada topik ini sejak 2019, dengan puncaknya pada 2022. Temuan menunjukkan bahwa desentralisasi dan ketidakubahannya Blockchain, dikombinasikan dengan kemampuan pemantauan real-time IoT, menciptakan efek sinergis dalam meningkatkan mekanisme deteksi dan pencegahan penipuan. Contoh empiris, seperti penipuan distribusi bahan bakar di Pertamina, menunjukkan bagaimana teknologi ini dapat mengurangi asimetri informasi dan meningkatkan kualitas audit. Studi ini berkontribusi pada literatur dengan menawarkan kerangka kerja terintegrasi untuk memanfaatkan teknologi emergensi dalam membangun sistem anti-penipuan yang transparan, aman, dan efisien. Kata kunci: blockchain, IoT, deteksi penipuan, sistem audit.

Kata kunci: blockchain, IoT, deteksi penipuan, sistem audit

Introduction

Managing strategic sectors such as energy, transport, finance and telecommunications, state-owned companies play an important role in the national economy. Non-tax state revenue (PNBP) from state-owned companies reached 354.2 trillion during the period 2020 to 2023 while the largest tax revenue of SOEs was contributed by PT Pertamina with a value of IDR 25.7 trillion (Kemenkeu, 2024).

The amount of state revenue is also accompanied by an increase in fraud cases that occur. Fraud includes all kinds of ways that can be used by a person or

[1] Corresponden Author : [1]Students of economics doctoral program, Parahyangan University, Jl Ciumbeleuit No. 94, Bandung, Email: syahrudin.ssh@gmail.com

[2] Second Author : [2]Industrial Engineering Study Program, Parahyangan University, Jl Ciumbeleuit No. 94, Bandung Email : ssusanto@unpar.ac.id

DOI: https://doi.org/10.20473/jraba.v10i1.72239

group of people to benefit from other parties by using false representations (Vousinas, 2019). Three fraud schemes in business include asset misappropriation, corruption, and financial statement fraud (Syahrudin, 2024). Based on data from the Komisi Pemberantasan Korupsi (KPK), cases of corruption crimes that occurred within 10 years increased drastically from 5 cases in 2015 to 38 cases in 2024 as presented in the graph below:

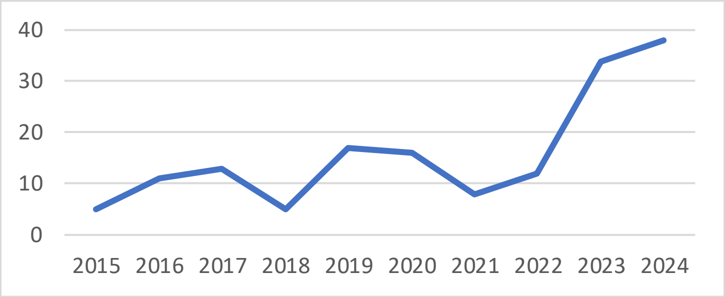


Figure 1 The development of corruption cases in BUMN
Source: KPK (2025)

The biggest disadvantage of corruption is that it leads to inefficient businesses and avoids the most productive use of technology, capital, and talent for society (Tuanakotta, 2019). A corruption case that occurred at Pertamina was revealed in 2025 in the governance of Pertamina's crude oil and refinery products that occurred from 2018 to 2023, the case is estimated to result in state losses of IDR 193.7 trillion. The Attorney General's Office named nine suspects in the case, including six Pertamina employees and three private companies allegedly involved in actions that harmed the state, such as procurement of crude oil that did not meet standards and price manipulation (cnnindonesia.com).

In recent years, fraud and corruption have posed significant challenges for state-owned enterprises (SOEs), with cases like those at Pertamina resulting in massive financial losses for the country. While fraud prevention measures have been explored in various industries, few studies have focused on the integration of emerging technologies, such as blockchain and the Internet of Things (IoT), to combat fraud within SOEs. This research aims to fill this gap by examining the potential of combining blockchain and IoT technologies to create more effective, transparent, and accountable anti-fraud systems for SOEs.

The case shows how important it is to improve transparency and accountability in the management of state-owned companies such as Pertamina and how important strict supervision is to prevent corruption in the future. To improve such transparency, efficiency and accountability, technologies such as Blockchain and Internet of Things (IoT) can be utilised in the business processes of state-owned companies in the current era of digitalisation.

Blockchain is a decentralised database technology that allows data to be stored and transmitted securely within a business network. The chain consists of interconnected blocks that store data. Each block contains a record of transactions that cannot be altered except by network consensus. This ensures that the data in the system remains secure and visible. (Šarac et al., 2021). Blockchain has many

DOI: https://doi.org/10.20473/jraba.v10i1.72239

advantages, one of which is its ability to eliminate third-party intermediaries in transactions which increases efficiency and reduces costs. In addition, because it is decentralised and transparent, blockchain is resistant to fraud and manipulation.

The Internet of Things allows various devices to connect and communicate automatically to perform certain activities, such as searching, processing, and transmitting information. This enables better control and automation in various aspects of daily life, such as energy management, security systems, and health monitoring. Internet of Things (IoT) networks are capable of transforming any device through existing network infrastructure by empowering physical resources into intelligent entities. IoT networks aim to develop complex information systems with efficient sensor data acquisition and data exchange through Artificial Intelligence, Machine Learning, cloud, and bigdata networks (Yazdinejad et al., 2023). The application of these two technologies can be used in preventing fraud, if blockchain is used to record transaction data and the Internet of Things is used to monitor BBM physically, an anti-fraud system will be formed which is very difficult to manipulate.

In Pertamina's fraud case, only internal parties know whether the distribution and quality of fuel has been manipulated, Pertamina Patra Niaga has carried out information concealment and signal manipulation which causes the public and authorities to be unaware of illegal fuel mixing, this causes information asymmetry between management, regulators, and the public. To reduce this information asymmetry, Signalling Theory plays a role in explaining how a party (signaler) provides information or signals to other parties (Hughes, 1986). Signal Theory in this case suggests that public and regulatory confidence in the national fuel system may be compromised when signals from the company are unreliable.

Research related to the use of technology, especially blockchain and IoT in helping prevent and detect fraud as a reference in this study is research conducted by Munir et al., (2019), Singh et al., (2020), Yazdinejad et al., (2023), Ashfaq et al., (2022), Shen et al., (2023), Areen Chic & Fardian Bilqisthi (2024), Esfandiari (2022), Elommal & Manita (2022), Sadjadi et al., (2020).

Existing literature has explored fraud prevention in general terms, often using traditional methods like internal auditing and financial control mechanisms. However, there is limited research on applying blockchain, a decentralized, transparent technology, alongside IoT's real-time monitoring capabilities within state-owned enterprises. This research introduces a novel approach by developing a framework that integrates these two technologies into a cohesive system designed to reduce fraud and corruption in SOEs.

The objective of this study is to demonstrate how blockchain and IoT can be leveraged to not only detect and prevent fraudulent activities but also to foster a culture of transparency and accountability within SOEs. By exploring this innovative approach, this research seeks to contribute to the growing body of knowledge in both the fields of technology and anti-fraud systems, offering practical solutions that have yet to be explored in prior studies.

The formulation of the problems of this study are (1) The amount of state revenue is also accompanied by an increase in fraud cases that occur, (2) Cases of corruption crimes that occurred within 10 years increased drastically from 5 cases

DOI: https://doi.org/10.20473/jraba.v10i1.72239

that occurred in 2015 increased sharply to 38 cases in 2024, (3) Cases of corruption that occurred at Pertamina were revealed in 2025 in the governance of Pertamina's crude oil and refinery products that occurred from 2018 to 2023, the case is estimated to result in state losses of IDR 193.7 trillion, (4) To increase transparency, efficiency and accountability, technologies such as Blockchain and Internet of Things (IoT) can be utilised in the business processes of state-owned companies in the current digitalisation era, (5) Pertamina Patra Niaga has carried out information concealment and signal manipulation which causes the public and authorities to be unaware of illegal fuel blending, this causes information asymmetry between management, regulators, and the public, (6) Signal Theory in this case shows that public and regulator trust in the national fuel system can be disrupted when signals from companies cannot be trusted.

Literature review

Signalling Theory

Signaling Theory, originally developed by Spence (1973), explains how parties with more information send signals to others in conditions of information asymmetry. This theory helps explain how unreliable disclosures can mislead stakeholders, especially when organizations manipulate or withhold data (Hughes, 1986). While prior studies have applied signaling theory to financial reporting or investment decisions, its integration in the context of technological fraud detection remains underexplored. In the case of SOEs like Pertamina, signals related to fuel quality and volume are obscured through manipulated reporting, illustrating how ineffective traditional signals can be without technological verification. This research critiques the assumption that signals alone are sufficient arguing that trust must now be built through verifiable, immutable technologies such as blockchain.

Blockchain

Blockchain offers a decentralized and tamper-proof method for recording transactions. Numerous studies, including Šarac et al., (2021) and Faccia et al., 2022), highlight blockchain's potential to improve transparency and accountability in audit processes. Faccia et al., (2022), for example, argue that permissioned blockchain systems can enable a shift toward fully open innovation in auditing, thereby reducing market concentration and conflicts of interest. However, these discussions often assume a frictionless transition and neglect contextual challenges such as institutional readiness, technological infrastructure, and regulatory maturity, which are critical in sectors like state-owned enterprises (SOEs).

In many developing countries, SOEs still operate with legacy systems and low data integrity, making blockchain implementation far more complex than suggested. Furthermore, while blockchain ensures transparency, its effectiveness is significantly limited without integration with real-time verification tools such as IoT. This research therefore positions blockchain not as a standalone innovation, but as a component in a synergistic technological ecosystem for fraud detection and prevention.

Internet of Things (IoT)

IoT facilitates real-time monitoring of physical assets. Studies like Yazdinejad et al., (2023) and Singh et al., (2020) emphasize IoT's role in anomaly

DOI: https://doi.org/10.20473/jraba.v10i1.72239

detection across supply chains. However, these applications often lack an audit trail to verify whether the data transmitted by sensors are reliable and tamper-proof. This study critiques the common overreliance on IoT data without validating its authenticity an issue that can be resolved when IoT data are recorded within a blockchain ledger. Thus, rather than viewing IoT and blockchain separately, this study examines how their integration forms a complementary antifraud framework**.**

AntiFraud Systems

Fraud encompasses any means by which an individual or group of individuals can gain an advantage over another party by using false representations (Vousinas, 2019). Anti-fraud Systems are a set of policies, procedures, and mechanisms designed to prevent, detect, and respond to fraud within an organisation. The purpose of an anti-fraud system is to detect, prevent, and respond to fraud with advanced technology (Pratama Adiwijaya & Sukma Maulana, 2023).

Synthesis and Gap

Prior literature typically analyzes blockchain and IoT in isolation or within ideal scenarios. This research fills the gap by evaluating how both technologies interact within anti-fraud systems, especially in complex environments like SOEs with systemic corruption issues. Furthermore, unlike prior studies that are either conceptual or single-case focused, this paper uses a structured SLR approach to map, critique, and synthesize decade-long developments in anti-fraud technology adoption. By doing so, it offers a critical framework for integrating digital signals into fraud prevention systems that are both verifiable and adaptive.

Research Methode

This study employs a qualitative research design with a Systematic Literature Review (SLR) approach to explore the development and application of blockchain and Internet of Things (IoT) technologies in anti-fraud systems over the past decade. The SLR was conducted by referring to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework to ensure transparency and replicability in article selection (Hariningsih et al., 2024). Data collection was carried out using the Watase Uake platform, an integrated bibliometric and literature review tool that facilitates collaboration, article screening, keyword mapping, and meta-analysis.

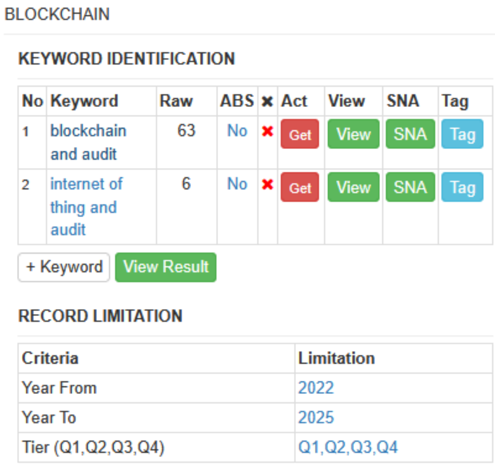
The data source was the Scopus database, chosen for its comprehensive coverage of peer-reviewed journals. The search was conducted using the query string blockchain and internet of things and fraud, applied across the fields of title, abstract, and keywords. Additional filters were applied to limit the results to articles published between 2015 and 2025, written in English, and indexed in Q1 to Q4 journals according to SCImago Journal Rank (SJR). This initial search resulted in 69 articles, which were then refined through the stages of identification, screening, eligibility, and inclusion. After applying relevance criteria and removing duplicates, 7 article**s** were selected for full review and analysis.

For data analysis, the study relied on tools provided by Watase Uake to generate visualizations such as keyword co-occurrence maps, PRISMA flow diagrams, and cluster classifications (Wahyudi, 2024). The analysis also involved manual thematic coding to extract key concepts and trends, particularly regarding

DOI: https://doi.org/10.20473/jraba.v10i1.72239

the integration of blockchain and IoT in fraud prevention. Descriptive statistics such as publication frequency and topic trends were employed, while no inferential statistical testing was used, as the primary goal of this study is to conduct a qualitative synthesis rather than hypothesis testing. This method allows a structured evaluation of the existing literature and provides a foundation for future empirical research in technology-based anti-fraud systems.

The following is an image of the keyword identification and record limitation criteria desired by the researcher:



BLOCKCHAIN

KEYWORD IDENTIFICATION

No	Keyword	Raw	ABS	✖	Act	View	SNA	Tag
1	blockchain and audit	63	No	✖	Get	View	SNA	Tag
2	internet of thing and audit	6	No	✖	Get	View	SNA	Tag

+ Keyword | View Result

RECORD LIMITATION

Criteria	Limitation
Year From	2022
Year To	2025
Tier (Q1,Q2,Q3,Q4)	Q1,Q2,Q3,Q4

Figure 2 keyword identification and record limitation
Source: Generated byWatase (2025)

The flowchart of the results of the article selection process in SLR in Watase processing is as follows:

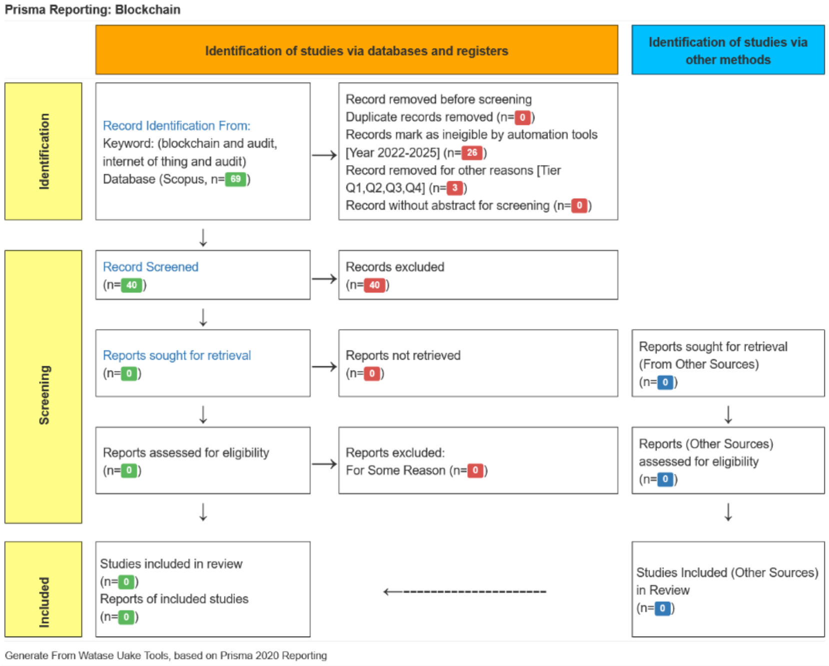

Prisma Reporting: Blockchain
Identification of studies via databases and registers
Identification of studies via other methods
Identification
Record Identification From:
Keyword: (blockchain and audit, internet of thing and audit)
Database (Scopus, n=69)
Record removed before screening
Duplicate records removed (n=0)
Records mark as ineigible by automation tools [Year 2022-2025] (n=26)
Record removed for other reasons [Tier Q1,Q2,Q3,Q4] (n=3)
Record without abstract for screening (n=0)
Screening
Record Screened (n=40)
Records excluded (n=40)
Reports sought for retrieval (n=0)
Reports not retrieved (n=0)
Reports sought for retrieval (From Other Sources) (n=0)
Reports assessed for eligibility (n=0)
Reports excluded: For Some Reason (n=0)
Reports (Other Sources) assessed for eligibility (n=0)
Included
Studies included in review (n=0)
Reports of included studies (n=0)
Studies Included (Other Sources) in Review (n=0)
Generate From Watase Uake Tools, based on Prisma 2020 Reporting

Figure 3 Prisma Reporting

Source: Generated byWatase (2025)

The results of the identification process above resulted in 69 articles that will be further processed through several stages such as identification, screening and inclusion. In SLR research, a Request Question (RQ) is made to prioritise the research review. The following is the Research Question in this study:

Table 1 Research Question

RQ	Description
RQ1	What are the research trends in blockchain, IoT and Fraud based on journal publication year?
RQ2	How are blockchain and IoT applied in Anti-Fraud Systems?

Source: processed by the researcher

Result and Discussion

Results

The selection criteria emphasized studies that (1) explicitly integrated both blockchain and IoT, (2) focused on fraud detection or audit quality, and (3) presented either empirical implementation or framework-based approaches relevant to anti-fraud systems. Articles discussing only one technology or lacking relevance to fraud were excluded to ensure the thematic coherence of the review.

A total of 69 articles were initially identified through the search process using the keywords blockchain, IoT and fraud within Scopus-indexed journals (Q1–Q4) from 2015 to 2025. After undergoing PRISMA-based screening stages including identification, duplication removal, abstract screening, and eligibility checks only 7 articles were selected for full inclusion. The articles are as follows:

Table 2 Article selection results

No	Article	*Jurnal Rank*	Resume
1	A blockchain-based audit approach for encrypted data in federated learning (Sun et al., 2022)	*Q1*	This research suggests a blockchain-based quality audit method for encrypted federated learning data. To avoid third-party access, gradient collection and aggregation are performed on two different blockchains. To ensure the accuracy of the model, custom votes are added and removed after aggregation, while the homomorphic BCP algorithm is used to protect the gradients.
2	Influence of blockchain and artificial intelligence on audit quality: Evidence from Turkey (Qader & Cek, 2024)	*Q1*	This study investigates how blockchain technology and artificial intelligence (AI) affect the quality of audits conducted by Turkish firms. The study collected primary data from 300 participants using a randomised method, and PLS-SEM was used to evaluate correlations between variables. The results show that the application of blockchain and AI in the financial system improves audit quality, especially in terms of speeding up the audit process and discovering fraud, which will ultimately result in better financial reporting. In addition, these technologies increase regulators‘, stakeholders’, and investors‘ confidence in businesses’ financial statements. This study has great benefits for investors, governments, companies, and policymakers. The accuracy of financial reports helps investors make decisions, and governments and policymakers can improve governance mechanisms.

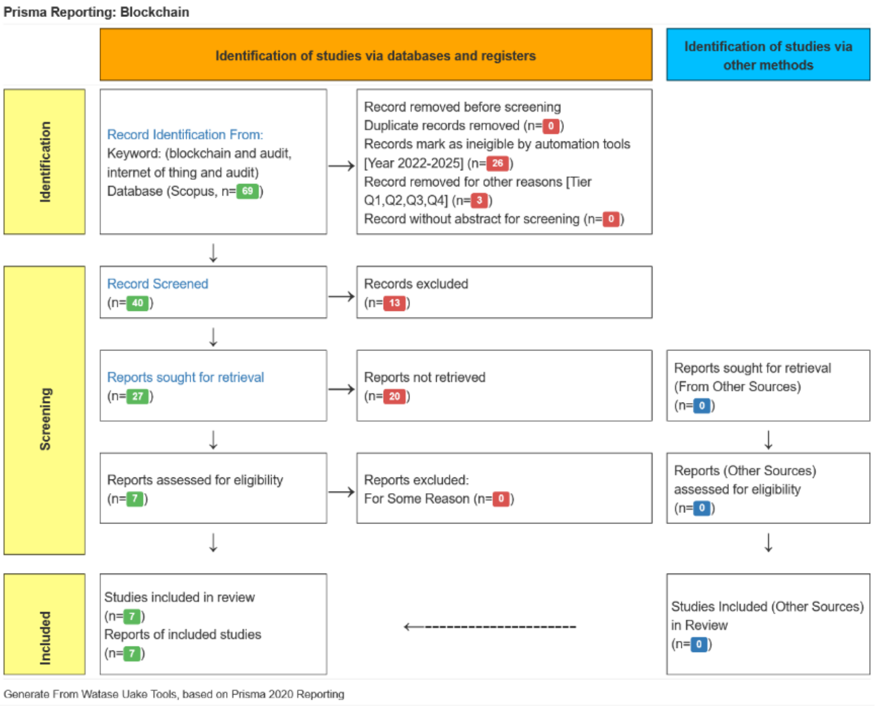
DOI: https://doi.org/10.20473/jraba.v10i1.72239

No	Article	*Jurnal Rank*	Resume
3	A model for CBDC audits based on blockchain technology: Learning from the DCEP (Wang et al., 2022)	*Q1*	The researcher proposed a CDBC (central bank currency) system using blockchain technology and Pederson Commitment that can provide real-time verification of transactions, with an emphasis on comprehensive supervision, privacy-preserving transactions, verifiable audits, and a constant number of CBDCs. The results show that the Central Bank is able to audit 50 Commercial Banks within 1 second and the system operation performance is superior.
4	A Blockchain Architecture for Trusted Sub-Ledger Operations and Financial Audit Using Decentralized Microservices (Fikri et al., 2022)	*Q1*	This research introduces the concept of Trusted Sub-Ledger Operation (TSLO) as a smart contract alternative to improve traceability and validity of accounting data based on asset groupings. TSLO offers a more flexible and adaptive approach to asset management in enterprise accounting and enterprise resource planning (ERP) systems. It is based on the Decentralised Microservices Tree (DMST) and is an extensible E-Bidding form of Triple Entry Accounting (TEA). Instead of using a multi-ledger architecture such as Hyperledger Fabric, which is limited to channels within a single entity, this approach adopts decentralised sub-ledgers with DMST structure for asset-based transactions. In addition, by combining Proof of Authority and Proof of Stake, the system strengthens corporate financial auditing and taxation by applying the principle of 'More stake, more reputation' to maintain transparency and trust.
5	Is Permissioned Blockchain the Key to Support the External Audit Shift to Entirely Open Innovation Paradigm? (Faccia et al., 2022)	*Q1*	This study found that the Semi-Open Innovation method of external auditing is ineffective because it leads to market concentration, conflicts of interest, and even fraud. Therefore, audit authorities should actively support a fully open Open Innovation model to increase transparency, transparency, creativity, collaboration, and fair competition in the audit industry. By emphasising the assumptions necessary for the successful application of technology in auditing, this study offers an alternative perspective. To resolve these issues and ensure the continuity of the transition from Semi-Open to Open Innovation, a permissible blockchain-based audit system is suggested.
6	Enterprise Audits and Blockchain Technology (Dong & Pan, 2023)	*Q2*	Blockchain technology is increasingly commonly used in the audit industry, presenting new challenges to traditional audit methods. This study examines audit cases in Chinese companies using blockchain technology and compares them with blockchain audit cases in Australia through surveys.The results of the study show that the application of new technologies in auditing may increase inherent risk and control risk.This study also offers blockchain audit experience in Australia as a reference for the development of blockchain-based auditing in China, and provides recommendations for dealing with challenges that arise in the modern audit process.
7	A Blockchain-Enabled Framework for Improving the Software Audit Process (Assiri & Humayun, 2023)	*Q2*	Audit logs play a crucial role in this process by recording all system activity and are used as evidence in investigations and to monitor information privacy and security. Auditors are tasked with ensuring the accuracy of business data, verifying regulatory compliance, and identifying potential fraud, malpractice, risks, or inefficiencies. Although various automated tools have been used in auditing, audit fraud is still common. Therefore, this research proposes a blockchain-based framework, SSFTA, to improve the transparency

No	Article	*Jurnal Rank*	Resume
			and effectiveness of software audits. Evaluation through case studies shows that this framework can simplify and improve the transparency of the audit process.

Sources: data processed by researchers (2025)

The process of selecting the articles above has gone through several stages which can be described in the figure below:


Prisma Reporting: Blockchain
Identification of studies via databases and registers
Identification of studies via other methods
Identification
Record Identification From:
Keyword: (blockchain and audit, internet of thing and audit)
Database (Scopus, n=69)
Record removed before screening
Duplicate records removed (n=0)
Records mark as ineigible by automation tools [Year 2022-2025] (n=26)
Record removed for other reasons [Tier Q1,Q2,Q3,Q4] (n=3)
Record without abstract for screening (n=0)
Screening
Record Screened (n=40)
Records excluded (n=13)
Reports sought for retrieval (n=27)
Reports not retrieved (n=20)
Reports sought for retrieval (From Other Sources) (n=0)
Reports assessed for eligibility (n=7)
Reports excluded: For Some Reason (n=0)
Reports (Other Sources) assessed for eligibility (n=0)
Included
Studies included in review (n=7)
Reports of included studies (n=7)
Studies Included (Other Sources) in Review (n=0)

Generate From Watase Uake Tools, based on Prisma 2020 Reporting

Figure 4 Prisma Reporting Result
Source: Generated byWatase (2025)

From these 7 articles, several key themes emerged. First, there is a strong indication that the integration of blockchain and IoT can enhance audit quality, particularly by increasing transparency, automation, and data integrity. For example, Qader & Cek (2024) empirically demonstrated how blockchain and AI improved fraud detection and audit speed in Turkish firms, echoing similar findings by (Assiri & Humayun, 2023), who proposed a blockchain-based software audit framework. Second, Sun et al., (2022) and Wang et al., (2022) focused on enhancing data integrity and auditability using encrypted blockchain models, reinforcing the relevance of blockchain in secure financial environments.

Blockchain and IoT Keyword Analysis

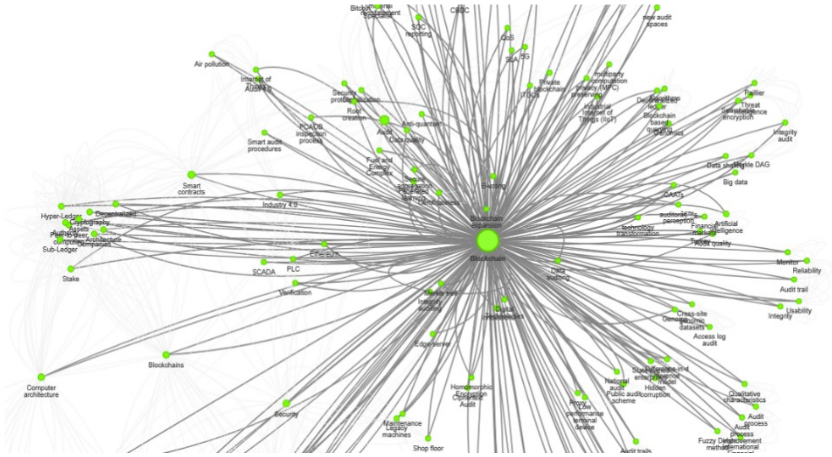


Figure 5 Blockchain and IoT Keyword Analysis
Source: Generated byWatase (2025)

The results of keyword processing by Watase software are obtained as shown in the figure above, which shows that in modern technology, blockchain, Internet of Things, and fraud prevention are interconnected. By combining these three technologies, a system can be created that is more transparent, secure, and efficient to prevent and detect fraud. Some of the nodes that appear to have a strong relationship with the main node include: (1) Blockchain keywords are related to smart contracts, distributed ledgers, hyperledgers, and computer architecture. Smart contracts and distributed ledgers, which ensure transparency and auditability of transactions, can be used to prevent fraud. (2) The keyword IoT (Internet of Things) is related to SCADA, Industry 4.0, and sensor technology. IoT makes it possible to monitor transactions or product distribution in real-time. It can be used in the financial industry or the petrol supply chain. In Industry 4.0, sensors and SCADA demonstrate the role of IoT in detecting anomalies or data irregularities. (3) Keywords Fraud related to audit trail, reliability, access log audit, and risk assessment. Audit trails and blockchain immutability can help reduce the risk of data manipulation. (4) Big Data & AI related buzzwords such as fuzzy classification, machine learning, and predictive analytics are emerging as supporting technologies in fraud prevention. Machine learning and fuzzy classification technologies enable the system to recognise suspicious patterns in transactions. Predictive analytics is used to predict potential fraud based on historical patterns.

Blockchain and IoT Research Trends by Year of Publication

In Figure 6, trend of research with the keywords blockchain, IoT and fraud in Scopus accredited journals began to increase since 2019 with a total of 6 articles with the highest in 2022 with 19 articles although it dropped in 2023. The increase in research on technology that assists the audit process is related to the covid-19

DOI: https://doi.org/10.20473/jraba.v10i1.72239

pandemic which forced a shift from traditional methods to remote auditing. Auditors are increasingly relying on technology to overcome physical access limitations during the pandemic. These technologies enable electronic testing of data, increasing efficiency and effectiveness in detecting anomalies or indications of fraud, and auditors have started using technological solutions to customise their audit procedures during the pandemic. To ensure a smooth audit process, collaboration software, advanced data analysis tools, and virtual communication platforms are part of this.

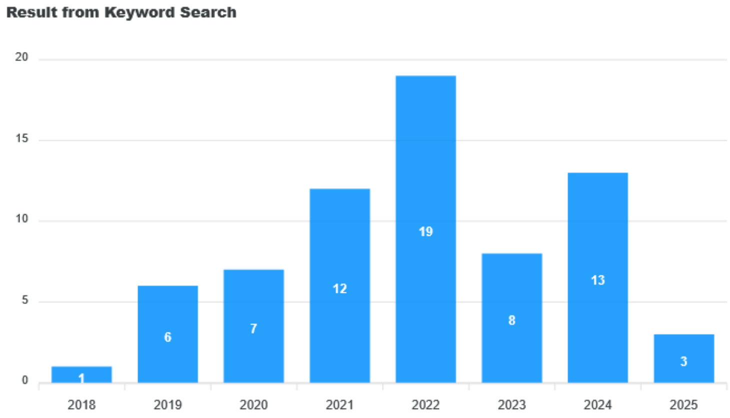


Figure 6 Research Trends by Publication Year

sources: generated by watase (2025)

The Implementation of Blockchain and Iot in Anti-Fraud Systems

The implementation of blockchain and IoT into the Anti-fraud System shows quite positive results. The results show that the application of blockchain and AI in the financial system is able to improve the quality of audits in Turkey, especially in terms of speeding up the audit process and finding fraud. (Qader & Cek, 2024). The results of research conducted by Dong & Pan, (2023) also shows that the application of new technology in auditing can increase inherent risk and control risk.

By providing transparency, immutability, and automation in transactions and data recording, blockchain is one of the powerful tools that can be used to prevent fraud. Combining this technology with smart contracts and IoT, detecting fraud can be done in real-time so that companies, regulators, and the public can more easily monitor and prevent fraud before it occurs. The use of blockchain and the Internet of Things has enabled real-time monitoring, data authenticity, and transparency in the regulatory process (Shen et al., 2023).

This platform can serve as an example for other countries looking to improve efficiency. Sun et al., (2022) suggests a blockchain-based quality audit method for encrypted federated learning data. To avoid third-party access, gradient collection and aggregation are performed on two different blockchains. To ensure the accuracy of the model, custom votes are added and removed after aggregation, while the homomorphic BCP algorithm is used to protect the gradients. Liu et al.,

DOI: https://doi.org/10.20473/jraba.v10i1.72239

(2022) Propose a blockchain expansion-based data integrity system that aims to solve the high cost of blockchain network maintenance and user creation of new blocks caused by the rapid growth of blocks in the existing blockchain technology's data integrity audit scheme.

Reflecting on the Pertamina Patra Niaga case above, through the decentralisation of data recording, blockchain technology allows every entity in the supply chain to access the same data and ensure that no changes are made unilaterally. Therefore, blockchain allows people who want to manipulate data for personal gain to avoid such loopholes. In addition, connected devices such as volume and fuel quality sensors can be monitored and analysed in real-time by the Internet of Things (IoT). IoT sensors can instantly record the amount of fuel dispensed, the location of the transport vehicle, and the quality of the fuel in a blockchain system that enables early detection of suspicious anomalies so that corrections can be made before large-scale fraud occurs.

Most people believe that the combination of Internet of Things (IoT) and blockchain technology can create a more transparent, secure, and efficient anti-fraud system. By applying these two technologies, the risk of fraud can be minimised and public confidence in the distribution system and fuel quality can be increased.

Discussions

While prior studies often explore blockchain or IoT independently, this research shows that their integration forms a more robust anti-fraud system, particularly when real-time IoT sensor data is recorded on immutable blockchain ledgers. This addresses a gap in earlier literature (e.g., Singh et al., 2020; Yazdinejad et al., 2023a) that examined IoT's potential in anomaly detection but lacked consideration for auditability and traceability.

Furthermore, this study critiques the assumptions of ideal implementation in earlier works. For instance, Faccia et al. (2022) suggest permissioned blockchain as a shift toward open innovation in external auditing. However, this review highlights that without real-time verification (IoT), blockchain's transparency may be insufficient in environments like SOEs where internal manipulation is rampant.

Comparing with Esfandiari (2022), who examined blockchain in food supply chains, this study offers a novel insight: in high-corruption contexts such as the Pertamina fuel fraud case, the synergy of IoT and blockchain can reduce information asymmetry by enabling independent verification of distribution volumes, transport locations, and fuel quality—factors critical for fraud detection yet often hidden in traditional reporting systems.

This review also underscores a future research agenda: (1) empirical field trials of integrated blockchain-IoT systems in SOEs, (2) comparative evaluations of different blockchain architectures (e.g., public vs permissioned), and (3) integration of AI/ML to enhance anomaly detection based on real-time sensor input.

Conclusion

DOI: https://doi.org/10.20473/jraba.v10i1.72239

This study examined the role of Blockchain and Internet of Things (IoT) technologies in anti-fraud systems through a systematic literature review of Scopus-indexed articles published between 2015 and 2025. From an initial pool of 69 articles, seven were selected based on strict inclusion criteria focusing on the integration of both technologies in fraud detection and audit applications. The findings show a growing trend in academic research on this topic, especially after 2019, with the COVID-19 pandemic acting as a catalyst for digital transformation in auditing practices.

The key insight from this review is that while Blockchain ensures transparency, immutability, and decentralized data access, its full anti-fraud potential is realized when combined with IoT's real-time monitoring capabilities. Together, these technologies address critical gaps in traditional fraud detection systems, such as information asymmetry, delayed reporting, and manipulation of audit trails. This is particularly relevant for high-risk sectors like state-owned enterprises (SOEs), where legacy systems and weak governance structures prevail.

By integrating both technologies, organizations can build a more resilient and proactive anti-fraud infrastructure. This study contributes theoretically by synthesizing existing fragmented literature and proposing an integrated framework for blockchain-IoT synergy in fraud prevention. Practically, it highlights the urgent need for technological innovation in governance, especially in developing economies where corruption remains systemic.

Future research should focus on real-world implementation trials, performance comparisons across blockchain platforms, and the integration of artificial intelligence to enhance anomaly detection accuracy.

Limitation

This research has several limitations. First, the implementation of Blockchain and IoT in the anti-fraud system is still done on a simulation scale, so the results may be different when applied in a real system with high complexity. Second, limited access to real-time IoT data causes anomaly analysis to not fully reflect field conditions. Third, this research uses one type of blockchain without comparing the effectiveness of various other blockchain platforms. In addition, time and resource constraints also affected the scope and depth of the analysis.

Sugestions

Future research is recommended to conduct direct trials on real systems that use large-scale IoT networks, so that the validity of Blockchain-based anti-fraud applications can be strengthened. In addition, it is necessary to compare various blockchain platforms to find out which one is the most optimal in supporting fraud detection and prevention. Researchers are also advised to integrate AI (Artificial Intelligence) technology to strengthen anomaly analysis of IoT data automatically and more accurately.

Implication

The results of this study provide practical implications for organisations, especially in the financial, logistics, and manufacturing sectors, that the integration of Blockchain and IoT can improve transparency, security, and efficiency in fraud prevention. This research also provides a basis that traditional central server-based

DOI: https://doi.org/10.20473/jraba.v10i1.72239

systems can be strengthened with a decentralised approach to reduce the risk of data manipulation. For academics, this research opens up space for developing further studies on the collaboration of emerging technologies for anti-fraud solutions.

Reference

Areen Chic, S., & Fardian Bilqisthi, M. (2024). Tantangan dan Peluang Blockchain di Era Digital dalam Bidang Keamanan Data dan Transaksi Digital. In Journal of Comprehensive Science (Vol. 3, Issue 11).

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, *22*(19). https://doi.org/10.3390/s22197162

Assiri, M., & Humayun, M. (2023). A Blockchain-Enabled Framework for Improving the Software Audit Process. Applied Sciences (Switzerland), *13*(6). https://doi.org/10.3390/app13063437

Dong, Y., & Pan, H. (2023). Enterprise Audits and Blockchain Technology. *SAGE Open*, *13*(4). https://doi.org/10.1177/21582440231218839

Elommal, N., & Manita, R. (2022). How Blockchain Innovation could affect the Audit Profession: A Qualitative Study. Journal of Innovation Economics & Management. https://doi.org/10.3917/jie.037.0037

Esfandiari, S. (2022). The effect of blockchain technology on supply chain management: its potential to prevent fraud and reduce risks to food safety and its effects on the relationships between supply chain actors in the Mexican food processing industry. *2022* IEEE Technology and Engineering Management Conference (TEMSCON EUROPE*)*, 179–183. https://doi.org/10.1109/TEMSCONEUROPE54743.2022.9801908

Faccia, A., Pandey, V., & Banga, C. (2022). Is Permissioned Blockchain the Key to Support the External Audit Shift to Entirely Open Innovation Paradigm? Journal of Open Innovation: Technology, Market, and Complexity, *8*(2), 85. https://doi.org/10.3390/JOITMC8020085

Fikri, N., Rida, M., Abghour, N., Moussaid, K., Omri, A. El, & Myara, M. (2022). A Blockchain Architecture for Trusted Sub-Ledger Operations and Financial Audit Using Decentralized Microservices. *IEEE Access*, *10*, 90873–90886. https://doi.org/10.1109/ACCESS.2022.3201885

Hariningsih, E., Haryanto, B., Wahyudi, L., & Sugiarto, C. (2024). Ten years of evolving traditional versus non-traditional celebrity endorser study: review and synthesis. Management Review Quarterly. https://doi.org/10.1007/s11301-024-00425-0

Hughes, P. J. (1986). Signalling By Direct Disclosure Under Asymmetric Information. Journal of Accounting and Economics, 8, 119–142.

Kemenkeu. (2024). APBN Kita - *Kinerja dan Fakta*.

Liu, Z., Feng, Y., Ren, L., & Zheng, W. (2022). Data Integrity Audit Scheme Based on Blockchain Expansion Technology. *IEEEAccess*, *10*.

DOI: https://doi.org/10.20473/jraba.v10i1.72239

Munir, M. S., Bajwa, I. S., & Cheema, S. M. (2019). An intelligent and secure smart watering system using fuzzy logic and blockchain. Computers and Electrical Engineering, *77*, 109–119. https://doi.org/10.1016/j.compeleceng.2019.05.006

Pratama Adiwijaya, A., & Sukma Maulana, W. (2023). Analisis Pembuatan Sistem Antifraud Pada Startup Fintech, Khususnya Peer-To-Peer Lending. Jurnal Ilmiah Teknik, *2*(3), 69–76.

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

Sadjadi, E. N., Menhaj, M. B., Zadeh, D. S., & Moshiri, B. (2020). Stability Analysis of Smooth Positive Fuzzy Systems. Canadian Conference on Electrical and Computer Engineering. https://doi.org/10.1109/CCECE47787.2020.9255694

Šarac, M., Pavlović, N., Bacanin, N., Al-Turjman, F., & Adamović, S. (2021). Increasing privacy and security by integrating a Blockchain Secure Interface into an IoT Device Security Gateway Architecture. Energy Reports, 7, 8075–8082. https://doi.org/10.1016/j.egyr.2021.07.078

Shen, L., Zhang, Z., Zhou, Y., & Xu, Y. (2023). Applying Blockchain Technology and the Internet of Things to Improve the Data Reliability for Livestock Insurance. Sensors, *23*(14). https://doi.org/10.3390/s23146290

Singh, S. K., Rathore, S., & Park, J. H. (2020). Block IoT Intelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence. Future Generation Computer Systems, *110*, 721–743. https://doi.org/10.1016/j.future.2019.09.002

Spence, M. (1973). Job Market Signaling. *The Quarterly Journal of Economics*, *87*(3), 355–374.

Sun, Z., Wan, J., Yin, L., Cao, Z., Luo, T., & Wang, B. (2022). A blockchain-based audit approach for encrypted data in federated learning. *Digital* Communications and Networks, *8*(5), 614–624. https://doi.org/10.1016/j.dcan.2022.05.006

Syahrudin, M. (2024). A Systematic Literature Review Of Artificial Intelligence In Detecting Fraud In Health Insurance. Bima Journal: Business, Management and Accounting Journal, *5*(2), 175–188. https://doi.org/10.37638/bima.5.2.175-188

Tuanakotta, T. M. (2019). Akuntansi Forensik & Audit Investigatif (2nd ed.). Salemba Empat.

Vousinas, G. L. (2019). Advancing theory of fraud: the S.C.O.R.E. model. Journal of Financial Crime, *26*(1), 372–381. https://doi.org/10.1108/JFC-12-2017-0128

Wahyudi, L. (2024). *Watase Uake: Research Collaboration Tools*. https://www.watase.web.id

Wang, Y. R., Ma, C. Q., & Ren, Y. S. (2022). A model for CBDC audits based on blockchain technology: Learning from the DCEP. Research in International Business and Finance, *63*. https://doi.org/10.1016/j.ribaf.2022.101781

DOI: https://doi.org/10.20473/jraba.v10i1.72239

Yazdinejad, A., Dehghantanha, A., Parizi, R. M., Srivastava, G., & Karimipour, H. (2023a). Secure Intelligent Fuzzy Blockchain Framework: Effective Threat Detection in IoT Networks. *Computers in Industry*, *144*, 103801. https://doi.org/10.1016/J.COMPIND.2022.103801

Yazdinejad, A., Dehghantanha, A., Parizi, R. M., Srivastava, G., & Karimipour, H. (2023b). Secure Intelligent Fuzzy Blockchain Framework: Effective Threat Detection in IoT Networks. Computers in Industry, *144*, 103801. https://doi.org/https://doi.org/10.1016/j.compind.2022.103801

DOI: https://doi.org/10.20473/jraba.v10i1.72239