Information Technology Studies Journal (ITECH)
Vol 1 (1) 2024 : 22-40

Utilization of Blockchain Technology to Improve Security and Transparency of Information Systems

Pemanfaatan Teknologi Blockchain untuk Meningkatkan Keamanan dan Transparansi Sistem Informasi

Tb. M. Adrie Admira, Panji Rahman
STMIK Jakarta STI&K, Universitas Islam Riau
*adrie.admira@gmail.com, panjirahman88@gmail.com

**Corresponding Author*

ABSTRACT
The integration of Blockchain technology with artificial intelligence (AI) and the Internet of Things (IoT) has become a major focus in efforts to increase the security and transparency of information systems. This research aims to investigate findings related to the use of Blockchain technology to increase the security and transparency of information systems through integration with artificial intelligence and the Internet of Things. The research method used is a systematic literature review that investigates various related research articles in scientific databases. The discussion results show that this integration offers innovative solutions to improve data security, access control, and privacy protection in various application domains. The implications of this research highlight the importance of considering the challenges and practical implications of adopting this integration, as well as identifying trends and future research directions in this domain.
Keywords: Blockchain, artificial intelligence, Internet of Things, information system security, transparency.

ABSTRAK
Integrasi teknologi Blockchain dengan kecerdasan buatan (AI) dan Internet of Things (IoT) telah menjadi fokus utama dalam upaya meningkatkan keamanan dan transparansi sistem informasi. Penelitian ini bertujuan untuk menyelidiki temuan terkait penggunaan teknologi Blockchain untuk meningkatkan keamanan dan transparansi sistem informasi melalui integrasi dengan kecerdasan buatan dan Internet of Things. Metode penelitian yang digunakan adalah tinjauan literatur sistematis yang menyelidiki berbagai artikel penelitian terkait dalam basis data ilmiah. Hasil pembahasan menunjukkan bahwa integrasi ini menawarkan solusi inovatif untuk meningkatkan keamanan data, akses kontrol, dan perlindungan privasi dalam berbagai domain aplikasi. Implikasi penelitian ini menyoroti pentingnya mempertimbangkan tantangan dan implikasi praktis dalam mengadopsi integrasi ini, serta mengidentifikasi tren dan arah penelitian masa depan dalam domain ini.
Kata Kunci: Blockchain, kecerdasan buatan, Internet of Things, keamanan sistem informasi, transparansi.

1. Introduction

The utilization of blockchain technology has gained significant attention due to its potential to enhance security and transparency in various information systems. Blockchain, as a distributed database, offers a secure and transparent way of storing and managing digital information (Hidayati et al., 2023). It has been recognized for its ability to improve traceability performance by providing full security and transparency in supply chain management (Hidayati et al., 2023). Furthermore, blockchain has been proposed as a solution to bring security and transparency to e-voting systems, offering advantages over traditional technologies (Singh et al., 2022). In the context of agri-food traceability, blockchain has the potential to enhance

information transparency and security in food chains, addressing key benefits and challenges in practical operations and system infrastructure (Feng et al., 2020).

Moreover, the implementation of blockchain technology in sectors such as aquaculture and connected autonomous vehicles (CAVs) has been explored to provide more security and transparency in transactions and activities (Iermakova et al., 2022; Dargahi et al., 2021). Additionally, blockchain has been investigated for its potential to improve security and privacy in medical systems, offering decentralized and secure storage for patient information (Wu et al., 2021). In the realm of e-government, blockchain has been proposed as an underlying technology to address security issues, reliability, and service customization in government information sharing (Walde & Yadav, 2022).

The potential of blockchain technology extends to smart mobility data markets, transport and logistics, and demand response programs, where it offers a multi-layered framework, addressing challenges such as scalability, integration of legacy systems, and inter-organizational change management (López & Farooq, 2020; Koh et al., 2020; Li et al., 2023). Furthermore, blockchain has been identified as a tool to enhance data security in IoT-based healthcare applications, customer relationship management, and Internet-of-Things (IoT) based healthcare applications (Rubaeah et al., 2023; Idian et al., 2023; Alqahtani & Algarni, 2023).

In the context of IoT-based healthcare applications, blockchain has been proposed to create alerts important to authenticated healthcare providers in a secure and private manner (Dwivedi et al., 2019). Additionally, blockchain has been explored for securing connected and autonomous vehicles, addressing security criteria such as fake requests, compromise of smart devices, and alteration in stored user ratings (Rathee et al., 2019). Furthermore, the impact of blockchain on customer relationship management (CRM) has been studied, suggesting an extended CRM based on blockchain capabilities to enhance customer experience and establish a trusted technology environment (Ghazaleh & Zabadi, 2021).

In summary, the utilization of blockchain technology has been explored across various domains to improve security and transparency in information systems, supply chains, e-voting systems, healthcare, and customer relationship management, among others. Its potential to address security challenges, enhance transparency, and provide decentralized and secure storage makes it a promising technology for a wide range of applications.

Utilizing blockchain technology can significantly enhance the security and transparency of information systems across various domains. Blockchain's ability to encrypt and distribute data over a network has been shown to improve information security, privacy, and transparency (Walde & Yadav, 2022). In the context of customer relationship management (CRM), the use of blockchain has been found to enhance customer information transparency, security, and accuracy, ultimately leading to improved customer experience and value maximization (Idian et al., 2023). Furthermore, blockchain technology has been applied to improve agri-food traceability, contributing to sustainable traceability management and enhancing information security and transparency in the agri-food industry (Feng et al., 2020).

In the realm of e-government, blockchain technology has been identified as a tool to increase transparency, prevent fraud, and foster citizen confidence by encrypting and distributing data over the network (Walde & Yadav, 2022). Additionally, the integration of blockchain with connected and autonomous vehicles has been shown to improve data security, ownership, trust, transparency, and auditability (Dargahi et al., 2021). Moreover, blockchain technology has been recognized for its potential to enhance traceability performance and provide full security and transparency in the distribution system design of halal beef supply chains (Hidayati et al., 2023).

In the healthcare sector, blockchain technology has been leveraged for data management operations, improving data security, integrity, access control, and privacy in IoT-based health systems (Rubaeah et al., 2023). Furthermore, blockchain has been found to

significantly improve transparency, openness, and customer participation in demand response programs, contributing to enhanced information system security and transparency (Li et al., 2023). In the transport and logistics domain, blockchain's designed security and consensus systems, along with traceability and transparency, have been acknowledged as foundational elements for improving communication and information systems (Koh et al., 2020).

In the context of securing patient information in medical systems, blockchain technology has been utilized to protect private information and effectively realize anti-theft control of private information, thereby enhancing the security and privacy of patient information (Wu et al., 2021). Additionally, the implementation of blockchain technology in the aquaculture sector has been associated with the potential to root out corruption and provide transparency for records and bookkeeping, contributing to improved information system security and transparency (Iermakova et al., 2022).

In the field of e-voting systems, blockchain technology has been proposed as a means to bring security and transparency to large-scale polls, offering advantages over other technologies and approaches to system design (Singh et al., 2022). Furthermore, blockchain has been recognized for its potential to render the transaction of information more secure and transparent in the context of smart mobility data markets (López & Farooq, 2020).

The integration of Blockchain technology with artificial intelligence (AI) and the Internet of Things (IoT) holds the potential to enhance the security and transparency of information systems. Blockchain technology offers decentralized and transparent transaction management (Francisco & Swanson, 2018). It provides a secure and immutable ledger, ensuring the integrity and reliability of data (Ahmad et al., 2023). However, challenges exist in integrating Blockchain with AI and IoT, such as scalability and consensus mechanisms (Cao et al., 2019; Rozman et al., 2022). The security of transactions, especially in e-commerce and financial activities, is crucial, and Blockchain's adoption can drive sustainability and security in start-ups (Sharma et al., 2023; Sreenivasan & Suresh, 2023). Furthermore, the adoption of Blockchain in accounting and auditing is transforming these fields, emphasizing the importance of this technology (Ponte & Bednárová, 2019; Perera & Abeygunasekera, 2022). The potential of Blockchain in various sectors, including healthcare and higher education, is also evident (Elghoul, 2021; Edastama et al., 2021). However, the adoption of Blockchain faces obstacles, including the need for effective construction schemes and addressing challenges in distributed consensus (Qin et al., 2020; Cao et al., 2019). The literature also highlights the need for further research to address limitations and emerging themes in Blockchain technology (Hughes et al., 2019; (Ahmad et al., 2023; . The potential of Blockchain in addressing the transparency and traceability challenges, especially in the context of the COVID-19 pandemic, is also recognized (Ahmad et al., 2023). The research gap in understanding the integration of Blockchain with AI and IoT to strengthen security and transparency in information systems is evident, and this literature review aims to contribute new insights to bridge this gap.

2. Research Methods

In the Research Methods section, the steps taken to conduct this systematic literature review are explained in detail. First, relevant articles are collected from recommended international databases, such as Scopus, IEEE Xplore, ACM Digital Library, and so on. The selection of keywords used in this search was carried out carefully, taking into account key concepts related to the research topic, such as "Blockchain technology", "Artificial Intelligence integration", "Internet of Things", "Security", and "Transparency" . This search yielded a number of relevant articles, which were then analyzed to meet specific inclusion and exclusion criteria. Inclusion criteria involved articles that were directly related to the integration of Blockchain technology with artificial intelligence or the Internet of Things in the context of increasing the security and transparency of information systems. Meanwhile, articles that are irrelevant, duplicate, or do not meet certain quality standards will be excluded from the review.

The PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method was used as the main guide in guiding this literature review process. This approach helps ensure that all relevant steps in preparing a systematic literature review are carried out systematically and transparently, from the identification stage to article inclusion, analysis, and presentation of results accurately and consistently. Thus, the steps described in this Research Methods section ensure that the literature review is conducted with a robust and reliable methodology.

3. Results and Discussion

3.1. Integration of Blockchain Technology with Artificial Intelligence in Information Systems

3.1.1. Findings related to the use of Blockchain to improve information system security through artificial intelligence.

To improve information system security through artificial intelligence, the integration of blockchain technology has shown promising potential. Blockchain ensures data security and zero-trust adherence, enhancing access management and user authentication (Wang et al., 2023). It acts as a trusted third party, improving the security of data sharing and reducing computational overhead in the Internet of Vehicles (Zhang et al., 2022). Additionally, blockchain is expected to enhance business activity effectiveness and data security (Indrawati & Firdaus, 2022). Its potential uses in enterprise security systems have been explored, particularly in safeguarding against cybercrime (Maesaroh et al., 2022). Blockchain offers an innovative approach to storing information, executing transactions, and establishing trust in an open environment (Zhang et al., 2019). Furthermore, it aids in data access control, solving data-level security sharing problems and enhancing data security in blockchain systems (Xu et al., 2022). The technology is also utilized to optimize system authentication services, enhancing the security of e-commerce and e-voting systems (Riadi et al., 2021).

Moreover, blockchain has been shown to improve economic efficiency, security, and decentralization in administration, contributing to the overall security of information systems (Myeong & Jung, 2019). Its application in hybrid intrusion detection systems has demonstrated improved performance (Khonde & Ulagamuthalvi, 2022). Additionally, blockchain has attracted research in cryptography, adding a security layer to storage systems and enhancing data security and privacy levels (Alkhliwi, 2022). Furthermore, it has the potential to address current securities settlement issues, such as costly reconciliation and difficult cross-border securities settlement (Bauvars, 2021). In the healthcare sector, blockchain has become an effective tool for safeguarding sensitive information, contributing to the security of information systems (Sultana et al., 2020). In summary, the integration of blockchain technology has the potential to significantly enhance information system security through artificial intelligence, offering innovative solutions for data security, access control, and privacy protection.

The integration of Blockchain technology with artificial intelligence (AI) has garnered significant attention in recent literature due to its potential to enhance the security of information systems. Blockchain's decentralized nature and high security features make it a robust foundation for ensuring data integrity and validity in information systems (Shinde et al., 2021). The integration with AI further amplifies this security potential by enabling early detection of security threats through sophisticated data analysis and machine learning (Zhang et al., 2021). This combination increases the resilience of information systems against complex security threats and cyber risks.

The literature also highlights the innovative applications of Blockchain technology in various domains, such as sharing economy, healthcare, and financial fields. For instance, Blockchain technology has been utilized to improve the efficiency of securities products in the securities trading system and ensure the information security of individuals and securities companies (Zhong, 2022). In the healthcare sector, Blockchain has been explored for organizing

medical records and empowering their secure propagation (Srivastava et al., 2022). Additionally, the financial field has seen the integration of Blockchain with distributed cloud storage, big data analysis, and artificial intelligence to enhance data security and service provision (Zhao & Meng, 2019).

Furthermore, the literature emphasizes the potential of Blockchain and AI integration in addressing challenges in various domains, including supply chain management, IoT frameworks for sustainable cities, and electronic health record management. The integration of Blockchain with IoT has been identified as a means to provide a high degree of trust and security, particularly in healthcare asset management (Nazir et al., 2022). Moreover, the use of AI-based trustworthy architecture, leveraging Blockchain characteristics such as smart contracts and trust oracles, has been proposed to enhance the security and reliability of cryptocurrency systems (Shahbazi & Byun, 2022).

Overall, the literature underscores the significance of integrating Blockchain and AI to bolster the security of information systems across diverse domains, offering innovative solutions to address complex security challenges and enhance data integrity and validity.

3.1.2. Findings related to the use of Blockchain to increase the transparency of information systems through artificial intelligence.

To enhance the transparency of information systems through artificial intelligence, the integration of blockchain technology has been explored in various domains. Blockchain has been found to address issues related to information integrity, transparency, and traceability. For instance, in the agri-food industry, blockchain-based traceability management has positively impacted food sustainability (Feng et al., 2020). Similarly, in the energy sector, blockchain has been shown to ensure the authenticity of certificates, increase system transparency, and reduce transactional costs (Khatoon et al., 2019). Furthermore, in the context of supply chain management, blockchain technology has been utilized to enhance transparency and traceability, thereby improving the overall efficiency of the supply chain (Koh et al., 2020; Zhao & Zhao, 2022; Surasak et al., 2019). Additionally, the application of blockchain in areas such as voting systems, aquaculture, and product lifecycle information sharing has demonstrated its potential to improve transparency and accountability ("BLOCKCHAIN BASED E-VOTING SYSTEM", 2023; Iermakova et al., 2022; Hayrutdinov et al., 2020).

Moreover, the combination of blockchain with artificial intelligence has been proposed to enhance the transparency and reliability of accounting information systems (Zhang & Zhu, 2022; Yu et al., 2018). This integration has the potential to suppress accounting fraud and ensure the security and scalability of the blockchain system (Zhang & Zhu, 2022; Li & Li, 2022). Furthermore, the use of blockchain in financial accounting has been associated with increased transparency and permanence, which can potentially reduce the probability and cost of false disclosures (Yu et al., 2018). Additionally, the feasibility of combining blockchain with information management systems has been explored, indicating the potential for enhancing transparency in personnel big data management systems (Chen et al., 2019). Overall, the findings from various studies suggest that the integration of blockchain with artificial intelligence has the potential to significantly enhance the transparency of information systems across diverse domains, including supply chain management, financial accounting, and food traceability.

The integration of Blockchain technology with artificial intelligence (AI) has been a subject of significant research interest in recent years. The potential of this integration lies in the ability of Blockchain to enhance transparency and verifiability of data, while AI extends these benefits by enabling more intelligent analysis of the available information. This combination offers effective mechanisms for verifying and validating information, as well as providing greater visibility into the overall flow and use of data (Zhang et al., 2021). Blockchain

technology, with its decentralized and transparent nature, serves as a strong foundation for facilitating the storage and exchange of publicly verifiable data (Tan & Low, 2019). The use of Blockchain in AI-based systems provides a security blanket, addressing the vulnerabilities of current Blockchain technology (Shinde et al., 2021). Furthermore, the integration of Blockchain and AI has been shown to be beneficial in establishing a secure and distributed resource-sharing environment, while AI technology addresses the problems of uncertainty, time variation, and complexity in wireless systems (Zhang et al., 2021).

The potential applications of Blockchain and AI integration extend to various domains, such as sustainable cities, healthcare, and finance. For instance, a Blockchain- and AI-enabled smart IoT framework has been proposed for sustainable cities, demonstrating the diverse applications of this integration (Ahmed et al., 2022). Additionally, the integration of Blockchain and AI has been explored in the context of financial decision-making, where Blockchain technology has brought reform to the data industry globally (Gawande & Bakliwal, 2022). Moreover, the potential of AI-powered Blockchain in decentralized secure multiparty computation protocols for the Internet of Vehicles (IoV) has been investigated, highlighting the wide-ranging implications of this integration (Raja et al., 2020).

While the integration of Blockchain and AI offers numerous benefits, it is essential to address challenges such as the efficiency degradation caused by the use of Blockchain technology and the legal implications posed by these technologies (Zhang et al., 2022; Murillo, 2023). Furthermore, the potential for anomaly detection using AI and Blockchain technology has been explored in various domains, including traffic anomaly detection and passenger flow anomaly detection, demonstrating the versatility of this integration (Zhang et al., 2022; Liu et al., 2023). In conclusion, the integration of Blockchain and AI has the potential to revolutionize various sectors by enhancing transparency, security, and data analysis capabilities. However, it is crucial to address challenges and legal implications while leveraging the benefits of this integration.

3.1.3. Challenges faced and potential solutions in the integration of Blockchain technology and artificial intelligence.

To integrate blockchain technology with artificial intelligence (AI), several challenges need to be addressed. The potential solutions to these challenges lie in the convergence of these technologies. The integration of blockchain with AI presents both merits and challenges. The combined advantages of both technologies open new opportunities for various applications (Makridakis & Christodoulou, 2019). However, challenges such as anomaly detection, legal implications, and explainability of AI need to be addressed (Chithanuru & Ramaiah, 2023; Murillo, 2023; Arrieta et al., 2020). The integration of AI into the Internet of Things (IoT), Blockchain, and AR/VR is considered an effective option for addressing challenges related to pandemic outbreaks (Shah et al., 2022). Furthermore, the convergence of blockchain technology and AI drives technological transformation in intelligent and sustainable IoT applications (Ahmed et al., 2022). The integration of blockchain with AI can potentially overcome the challenges of blockchain systems, forming intelligent blockchain systems (Zheng, 2019). However, open research challenges in utilizing blockchain technologies for AI need to be addressed (Salah et al., 2019). Additionally, the scalability challenges of existing blockchain platforms need to be carefully handled through the integration of compression algorithms into blockchain-assisted deep learning solutions (Shafay et al., 2022).

The integration of blockchain and AI also faces challenges related to interoperability, security, privacy, and suitable business models of implementation (Boulos et al., 2018). Moreover, the convergence of blockchain technology with the Internet, AI, and other technologies can enable the life cycle management of asset securitization (Zhong, 2022). The promises of blockchain adoption need to be delivered, and barriers such as scalability, legacy system integration, investment requirements, and inter-organizational change management

need to be addressed (Koh et al., 2020). Innovative technologies such as blockchain and AI have emerged as promising solutions for combating epidemic outbreaks (Nguyen et al., 2020). In the healthcare sector, the potential applications of blockchain technology need to be revealed, and the associated challenges and possible research directions need to be highlighted (Hölbl et al., 2018). The convergence of blockchain and next-generation AI technologies can accelerate biomedical research and enable patients to control and profit from their personal data (Mamoshina et al., 2017). Furthermore, the integration of AI with IoT plays a beneficial role in various fields, including intelligent surveillance applications (Ahmed et al., 2021). The integration of IoT solutions into healthcare systems can significantly increase intelligence, flexibility, and interoperability (Gardasevic et al., 2020). In conclusion, the integration of blockchain technology and AI presents numerous challenges, including anomaly detection, legal implications, scalability, interoperability, and security. Addressing these challenges requires a comprehensive approach that leverages the convergence of these technologies to unlock new opportunities and applications.

3.2. Integration of Blockchain Technology with the Internet of Things (IoT) in Information Systems

3.2.1. Findings related to the use of Blockchain to improve information system security through the Internet of Things (IoT).

Blockchain technology has been increasingly explored as a means to enhance the security of information systems, particularly in the context of the Internet of Things (IoT). The integration of blockchain with IoT aims to address security challenges and improve data integrity. Li et al. (2020) conducted a survey on the security of blockchain systems and highlighted the potential for security enhancement solutions in various blockchain applications, including IoT. Furthermore, Zhang et al. (2022) emphasized the application of blockchain to improve information security, data security, and IoT. The study by Zhang et al. (2019) also underscored the innovative approach of blockchain in storing information and establishing trust in open environments, which is pertinent to IoT security.

Moreover, the use of blockchain as a trusted third party to enhance data security in the IoT was discussed by . (Zhang et al., 2022). Additionally, the systematic review by Ahmed (2022) highlighted the utilization of blockchain characteristics to secure information in IoT. Anand et al. (2022) and Dhanju et al. (2022) both explored the integration of blockchain with IoT to address security challenges, particularly in smart cities, further emphasizing the relevance of blockchain in enhancing IoT security.

Furthermore, Parmar & Shah (2023) focused on the benefits of integrating blockchain with IoT, particularly in lightweight cryptography for data security and integrity. Additionally, Hu et al. (2020) proposed an adaptive dynamic blockchain networking method based on discrete heartbeat signals to improve the security and stability of blockchain technology in IoT applications. Overall, the literature supports the potential of blockchain technology to enhance the security of IoT systems by providing tamper-proof features, securing data sharing, and improving data integrity. The integration of blockchain with IoT offers promising solutions to address security challenges and establish trust in decentralized environments.

The integration of Blockchain technology with the Internet of Things (IoT) has been a subject of significant research and has shown promising results in enhancing information system security. By leveraging the decentralized and tamper-proof nature of Blockchain, along with the extensive connectivity of IoT, a secure ecosystem for managing and securing data from diverse connected devices can be established (Singh et al., 2021). This integration offers robust and verified authentication mechanisms for IoT devices, ensuring that only authorized devices can communicate within the network. Furthermore, Blockchain provides an immutable record of transactions, ensuring the integrity and reliability of data generated by IoT devices, thus

preventing cyber attacks such as data manipulation or breaches in IoT device security (Wazid et al., 2020).

The potential benefits of integrating Blockchain with IoT extend to various application fields, including healthcare, logistics, and smart buildings. For instance, in the healthcare domain, the integration of IoT technology and Blockchain has been explored through systematic literature reviews, demonstrating its potential to enhance data security and management in healthcare-related application areas (Kamangar et al., 2023). Similarly, in the context of smart buildings, Blockchain-enabled reparations in smart buildings' cyber-physical systems have been investigated, highlighting the potential for improved security and resilience in smart building environments (Tiwari & Batra, 2021).

Moreover, the secure access of IoT at scale using Blockchain and smart contracts has been proposed, demonstrating the practical implementation of Blockchain technology, particularly Ethereum, in a large-scale event-based IoT control system (Fotiou et al., 2019). Additionally, the application of Blockchain in IoT data access control has been explored, combining attribute-based encryption and Blockchain to effectively protect the security and privacy of IoT data and enable secure data sharing (Lu et al., 2021).

The literature also emphasizes the importance of addressing the security challenges posed by the increasing number of IoT devices and the explosion of user privacy data. It underscores the critical role of Blockchain in ensuring information security in the IoT environment (Alboraei, 2019; Chen, 2023). In conclusion, the integration of Blockchain technology with the Internet of Things holds great promise in enhancing the security and resilience of information systems across various domains. The findings from the literature underscore the potential of this integration to create a secure and trusted environment for managing and communicating with data from a wide array of IoT devices, thereby contributing significantly to improving information system security.

3.2.2. Findings related to the use of Blockchain to increase the transparency of information systems through the Internet of Things (IoT).

Blockchain technology has been increasingly recognized for its potential to enhance the transparency of information systems in the context of the Internet of Things (IoT). The integration of blockchain with IoT systems offers the opportunity to secure and transfer data flow, preserve its integrity, and provide transparent mechanisms for its management (Alzoubi et al., 2023). This is particularly relevant in the industrial sector, where blockchain can enhance the reliability and scalability of IoT systems (Dai et al., 2019). Furthermore, blockchain's decentralized nature provides a useful mechanism for addressing IoT challenges, thereby increasing transparency and accountability (Ramesh et al., 2020). The use of blockchain in IoT can also improve data security, provide data immutability, and enhance data transparency for real-time updates on various processes (Wong et al., 2021). Additionally, blockchain technology has the potential to address security, anonymity, and centralization challenges, thereby enhancing the auditability and transparency of conventional IoT frameworks (Dorri et al., 2022).

Moreover, blockchain offers distinctive characteristics such as transactional privacy, data immutability, and cryptographic transparency, which are essential for ensuring the trustworthiness of IoT systems ("A comprehensive review of significant learning for anomalous transaction detection using a machine learning method in a decentralized blockchain network", 2022). The potential of blockchain to become a key component of many IoT systems is underscored by its ability to offer an unprecedented level of accountability, transparency, and reliability (Voulgaris et al., 2019). Furthermore, the integration of blockchain with IoT can contribute to estimating service quality in industrial IoT monitoring applications, thereby enhancing transparency and accountability in industrial processes (Maiti et al., 2019). The key features of blockchain, including decentralization, openness, and transparency, align with the

requirements of ubiquitous power IoT, further emphasizing its potential in enhancing transparency in IoT applications (Jia et al., 2020). In conclusion, the integration of blockchain with IoT systems holds significant promise for increasing the transparency of information systems. The decentralized and transparent nature of blockchain technology, along with its ability to ensure data integrity and security, makes it a valuable tool for addressing the challenges associated with IoT systems.

3.2.3. Challenges faced and potential solutions in the integration of Blockchain and IoT technology.

The integration of Blockchain and IoT technology presents several challenges, including security, scalability, interoperability, and data management. Ali et al. (2019) and Dai et al. (2019) highlight the potential of blockchain technology in addressing the challenges faced by centralized IoT models. They emphasize the need for decentralized and secure mediums for IoT, which blockchain can provide. Furthermore, Panarello et al. (2018) and Parmar & Shah (2023) discuss the challenges faced by the research community in integrating Blockchain and IoT, emphasizing the need for solutions to ensure smooth integration.

In addition, Ramesh et al. (2020) and Kamangar et al. (2023) identify the challenges in integrating Blockchain and IoT technologies, particularly in the healthcare domain. They emphasize the need for secure integration to support medical delivery drones and address the limitations of IoT and Blockchain technologies. Moreover, Romashkova et al. (2021) propose critical solutions to address integration bottlenecks, such as transitioning from Proof-of-Work to Distributed Proof-of-Stake consensus and leveraging the synergies of blockchain and IoT technology.

Furthermore, Ebrahim et al. (2022) and Mahmood & Dabagh (2023) discuss the role of Blockchain and IoT technologies in addressing security challenges and privacy concerns. They emphasize the potential of blockchain technology to resolve the security problems of IoT systems. Additionally, Singh & Singh (2020) highlight the importance of integrating blockchain with IoT and AI in agriculture and healthcare fields to manage supply chains, traceability of products, and smart contracts.

Overall, the literature emphasizes the challenges in integrating Blockchain and IoT technologies, including security, scalability, and interoperability. However, it also highlights the potential of blockchain technology in addressing these challenges and providing secure and decentralized solutions for IoT applications.

3.3. Comparison and Contrast Between the Integration of Blockchain Technology with Artificial Intelligence and the Internet of Things (IoT)

3.3.1. Comparison of the advantages and disadvantages of Blockchain integration with artificial intelligence and IoT.

The integration of blockchain with artificial intelligence (AI) and the Internet of Things (IoT) offers several advantages and disadvantages. The integration of these technologies aims to enhance security, privacy, and interoperability in various applications. Blockchain 5.0 focuses on integrating AI, IoT, big data, cyber-physical systems, and cloud computing to advance decentralized IoT applications (Ahmed et al., 2022). This integration provides speed for IoT devices and enables real-time transaction visibility through distributed ledgers (Ahmed, 2022). Furthermore, the combination of IoT, AI, and blockchain technology can transform smart agriculture into the Internet of smart agriculture, offering greater control, management, and security in supply-chain networks (Ahmed et al., 2022).

However, integrating IoT and blockchain also presents challenges, such as low throughput, which needs to be addressed to fully realize the potential benefits (Dwivedi et al., 2021). Additionally, security issues, rapid changes in cryptography due to quantum computing, and the rise of AI and evolution methods in the scope of IoT security are trends that require

specific attention (Balogh et al., 2021). Despite these challenges, the integration of leading technologies like IoT, blockchain, big data, edge and cloud computing, robotics, and open-source software has extended the scope of Industry 4.0, benefiting both industry and partners (Hameed et al., 2022).

The integration of IoT with blockchain offers robust solutions to issues related to interoperability, privacy, security, traceability, and reliability of the system (Tahir et al., 2020). Moreover, the integration of blockchain with IoT adds several benefits, including enhanced data preprocessing, analytics approaches, and improved service platforms in healthcare applications (Jamil et al., 2021). With its "security by design," blockchain can help address major security requirements in IoT (Panarello et al., 2018). Furthermore, the emergence of blockchain has fulfilled many security, maintenance, and authentication requirements of IoT systems, making blockchain-based IoT systems increasingly prevalent (Li et al., 2020). In conclusion, the integration of blockchain with AI and IoT presents numerous opportunities for enhancing various applications, particularly in terms of security, privacy, and interoperability. However, it also poses challenges that need to be addressed to fully leverage its potential.

3.3.2. Implications of using both integrations for security and transparency of information systems.

To address the implications of using both integrations for security and transparency of information systems, it is essential to consider the impact on confidentiality, integrity, and non-repudiation, as well as the tension between confidentiality and transparency (Xu et al., 2021). Integrating biometric identification and authentication can protect the availability, confidentiality, and integrity of information, particularly in social security and pension services (Owusu-Oware & Effah, 2022). Furthermore, the intention to bridge subjective norms and attitudes toward information system behavior is crucial, emphasizing the importance of security policy and standards to stimulate integrated behavior impact in accountability and governance (Hartanti et al., 2021).

In the context of transparency, the use of blockchain technology can ensure data integrity, transparency, and traceability in clinical trial data management (de-Melo-Diogo et al., 2021). Additionally, the implementation of integrated information technologies into the management of public funds is crucial to ensure transparency of budgetary processes and procedures at the state and local levels (Melnychuk, 2020). Moreover, the development of an integrated security and safety management system structure is essential to address threats of intrusion into physical, information, and signal spaces in the Industry 4.0 context (Dotsenko et al., 2019).

It is also important to consider the practical implications of these integrations. For instance, the proposed approach for implementing information security in e-Government systems ensures a holistic approach to ensuring confidentiality, integrity, and non-repudiation, allowing e-Government maturity to progress in emerging economies (Ramtohul & Soyjaudah, 2016). Additionally, the influence of transformations of informational economic transparency of an enterprise on external impacts from legal relations parties is a practical implication that needs to be considered (Dmitriev & Novikov, 2019). In conclusion, integrating security and transparency in information systems has significant implications for ensuring confidentiality, integrity, non-repudiation, and transparency. It is crucial to consider the practical implications of these integrations, particularly in e-Government systems, social security and pension services, and clinical trial data management. Furthermore, addressing the tension between confidentiality and transparency is essential to ensure the successful implementation of these integrations.

3.3.3. Identify trends and future research directions in the integration of Blockchain technology with artificial intelligence and IoT.

The integration of blockchain technology with artificial intelligence (AI) and the Internet of Things (IoT) has garnered significant attention in recent years. Several research studies have explored the potential of this integration and have identified future research directions in this domain. Abdelmaboud et al. (2022) provide a comprehensive taxonomy, recent advances, challenges, and future research directions for the integration of blockchain with IoT applications. They offer a roadmap for the future and identify research trends for blockchain technology as a baseline for its adoption and integration into IoT systems. Memon et al. (2019) present a detailed survey on the integration of blockchain in IoT, highlighting existing and expected issues of both technologies, and outlining future research directions. They provide valuable insights into the challenges and opportunities in this integration. Nazir et al. (2022) emphasize the paramount importance of integrating blockchain with IoT, AI, Edge and Cloud Computing, and 5G technologies in an increasingly connected society. This highlights the potential for further research in exploring the integration of these technologies. Ramesh et al. (2020) study the effectiveness of combining blockchain for IoT in different applications, focusing on a Blockchain-enabled Intelligent IoT framework with Artificial Intelligence. This study provides insights into the potential applications and benefits of integrating these technologies. Bothra et al. (2021) conduct a systematic survey on the integration of IoT and blockchain, studying current trends in the usage of blockchain in IoT systems. This survey offers valuable insights into the current landscape and future research directions in this area.

In conclusion, the integration of blockchain technology with AI and IoT presents numerous opportunities and challenges. Future research directions in this domain include addressing scalability and throughput issues, exploring security enhancements, and leveraging the potential of these integrated technologies in various applications.

4. Conclusion

From the results of the discussions carried out, it can be concluded that the integration of Blockchain technology with artificial intelligence (AI) and the Internet of Things (IoT) has great potential to increase the security and transparency of information systems. The use of Blockchain technology in the context of artificial intelligence has shown promising potential in improving the security of information systems. Blockchain is able to ensure data security and trustless compliance, improving access management and user authentication. In addition, the integration of Blockchain with artificial intelligence also makes a significant contribution in increasing the transparency of information systems by ensuring the integrity and authenticity of data, as well as providing a transparent mechanism for data management.

However, there are challenges that need to be overcome in this integration. Some of the main challenges include managing large-scale data, security issues, and interoperability. Solutions to these challenges can be found through the convergence of Blockchain technology, artificial intelligence, and IoT. Concrete steps such as changing consensus from Proof-of-Work to Distributed Proof-of-Stake, as well as leveraging synergies between blockchain and IoT technology, can help overcome some of these obstacles.

The implications of using this integration for the security and transparency of information systems are very important to consider. Using these two integrations can bring significant benefits in improving data security, integrity and transparency. However, it is also necessary to pay attention to the practical implications, including in the implementation of e-Government systems, social security and pension services, and clinical trial data management. In addition, it is also important to identify trends and future research directions in the integration of Blockchain technology with artificial intelligence and IoT. Future research could focus on addressing specific challenges, such as increasing scalability and throughput, as

well as exploring the potential applications of these integrated technologies in various domains.

Thus, the integration of Blockchain technology with artificial intelligence and IoT has great potential to change the security and transparency landscape of information systems. However, the challenges and implications of using this integration must be well understood to ensure its success in practical implementation and future research.

5. References

Abdelmaboud, A., Ahmed, A., Abaker, M., Eisa, T., Albasheer, H., Ghorashi, S., … & Karim, F. (2022). Blockchain for iot applications: taxonomy, platforms, recent advances, challenges and future research directions. Electronics, 11(4), 630. https://doi.org/10.3390/electronics11040630

Ahmad, R., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., & Omar, M. (2023). Blockchain and covid-19 pandemic: applications and challenges.. https://doi.org/10.36227/techrxiv.12936572

Ahmed, I., Anisetti, M., & Jeon, G. (2021). An iot‐based human detection system for complex industrial environment with deep learning architectures and transfer learning. International Journal of Intelligent Systems, 37(12), 10249-10267. https://doi.org/10.1002/int.22472

Ahmed, I., Zhang, Y., Jeon, G., Lin, W., Khosravi, M., & Qi, L. (2022). A blockchain‐ and artificial intelligence‐enabled smart iot framework for sustainable city. International Journal of Intelligent Systems, 37(9), 6493-6507. https://doi.org/10.1002/int.22852

Ahmed, M. (2022). Integration of blockchain with the internet of things: a systematic review.. https://doi.org/10.14293/s2199-1006.1.sor-.ppgvo0b.v1

Ahmed, R., Hemdan, E., El-Shafai, W., Ahmed, Z., El-Rabaie, E., & El-Samie, F. (2022). Climate‐smart agriculture using intelligent techniques, blockchain and internet of things: concepts, challenges, and opportunities. Transactions on Emerging Telecommunications Technologies, 33(11). https://doi.org/10.1002/ett.4607

Alboraei, A. (2019). Privacy-aware decentralized and scalable access control management for iot

Ali, M., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. (2019). Applications of blockchains in the internet of things: a comprehensive survey. Ieee Communications Surveys & Tutorials, 21(2), 1676-1717. https://doi.org/10.1109/comst.2018.2886932

Alkhliwi, S. (2022). An efficient dynamic access control and security sharing scheme using blockchain. International Journal of Advanced and Applied Sciences, 9(8), 28-40. https://doi.org/10.21833/ijaas.2022.08.004

Alqahtani, A. and Algarni, A. (2023). A survey on blockchain technology concepts, applications and security. International Journal of Advanced Computer Science and Applications, 14(2). https://doi.org/10.14569/ijacsa.2023.0140296

Alzoubi, A., Saadeddin, T., & Dmour, M. (2023). An ethereum private network for data management in blockchain of things ecosystem. International Journal of Online and Biomedical Engineering (Ijoe), 19(01), 38-58. https://doi.org/10.3991/ijoe.v19i01.35261

Anand, M., Sabharwal, M., & S, V. (2022). Alleviating data storage challenge through virtualization of blockchain embedded with internet of things. Indian Journal of Computer Science and Engineering, 13(2), 312-323. https://doi.org/10.21817/indjcse/2022/v13i2/221302005

Arrieta, A., Díaz-Rodríguez, N., Ser, J., Bennetot, A., Tabik, S., Barbado, A., … & Herrera, F. (2020). Explainable artificial intelligence (xai): concepts, taxonomies, opportunities and challenges toward responsible ai. Information Fusion, 58, 82-115. https://doi.org/10.1016/j.inffus.2019.12.012

Balogh, S., Gallo, O., Ploszek, R., Špaček, P., & Zajac, P. (2021). Iot security challenges: cloud and blockchain, postquantum cryptography, and evolutionary techniques. Electronics, 10(21), 2647. https://doi.org/10.3390/electronics10212647

Bauvars, J. (2021). Applicability of blockchain technology in securities settlement. Complex Systems Informatics and Modeling Quarterly, (28), 34-58. https://doi.org/10.7250/csimq.2021-28.03

Bothra, P., Karmakar, R., Bhattacharya, S., & De, S. (2021). How can applications of blockchain and artificial intelligence improve performance of internet of things? -- a survey.. https://doi.org/10.48550/arxiv.2111.14018

Boulos, M., Wilson, J., & Clauson, K. (2018). Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. International Journal of Health Geographics, 17(1). https://doi.org/10.1186/s12942-018-0144-x

Cao, B., Li, Y., Zhang, L., Long, Z., Mumtaz, S., Zhou, Z., … & Peng, M. (2019). When internet of things meets blockchain: challenges in distributed consensus. Ieee Network, 33(6), 133-139. https://doi.org/10.1109/mnet.2019.1900002

Chen, C. (2023). Research on internet of things information security based on blockchain.. https://doi.org/10.1117/12.3010663

Chithanuru, V. and Ramaiah, M. (2023). An anomaly detection on blockchain infrastructure using artificial intelligence techniques: challenges and future directions – a review. Concurrency and Computation Practice and Experience, 35(22). https://doi.org/10.1002/cpe.7724

Dai, H., Zheng, Z., & Zhang, Y. (2019). Blockchain for internet of things: a survey. Ieee Internet of Things Journal, 6(5), 8076-8094. https://doi.org/10.1109/jiot.2019.2920987

Dai, H., Zheng, Z., & Zhang, Y. (2019). Blockchain for internet of things: a survey. Ieee Internet of Things Journal, 6(5), 8076-8094. https://doi.org/10.1109/jiot.2019.2920987

Dargahi, T., Ahmadvand, H., Alraja, M., & Yu, C. (2021). Integration of blockchain with connected and autonomous vehicles: vision and challenge. Journal of Data and Information Quality, 14(1), 1-10. https://doi.org/10.1145/3460003

Dargahi, T., Ahmadvand, H., Alraja, M., & Yu, C. (2021). Integration of blockchain with connected and autonomous vehicles: vision and challenge. Journal of Data and Information Quality, 14(1), 1-10. https://doi.org/10.1145/3460003

de-Melo-Diogo, M., Tavares, J., & Luís, Â. (2021). Data security in clinical trials using blockchain technology., 250-268. https://doi.org/10.4018/978-1-7998-7363-1.ch010

Dhanju, G., Tyagi, S., Kumar, A., Asthana, I., & Taluja, A. (2022). Review on smart city iot security using blockchain. IJEAST, 7(6), 436-441. https://doi.org/10.33564/ijeast.2022.v07i06.053

Dmitriev, O. and Novikov, S. (2019). Optimizing the economic information transparency level of high-tech enterprises in the post-industrial globalized economy. International Journal of Economics and Business Administration, VII(Issue 3), 25-56. https://doi.org/10.35808/ijeba/306

Dmitriev, O. and Novikov, S. (2019). Optimizing the economic information transparency level of high-tech enterprises in the post-industrial globalized economy. International Journal of Economics and Business Administration, VII(Issue 3), 25-56. https://doi.org/10.35808/ijeba/306

Dorri, A., Roulin, C., Pal, S., Baalbaki, S., Jurdak, R., & Kanhere, S. (2022). Device identification in blockchain-based internet of things.. https://doi.org/10.48550/arxiv.2202.09603

Dotsenko, S., Illiashenko, O., Kamenskyi, S., & Kharchenko, V. (2019). Integrated security management system for enterprises in industry 4.0. Information & Security an International Journal, 43(3), 294-304. https://doi.org/10.11610/isij.4322

Dwivedi, A., Malina, L., Dzurenda, P., & Srivastava, G. (2019). Optimized blockchain model for internet of things based healthcare applications.. https://doi.org/10.1109/tsp.2019.8769060

Dwivedi, A., Singh, R., Kaushik, K., Mukkamala, R., & Alnumay, W. (2021). Blockchain and artificial intelligence for 5g‐enabled internet of things: challenges, opportunities, and solutions. Transactions on Emerging Telecommunications Technologies, 35(4). https://doi.org/10.1002/ett.4329

Ebrahim, M., Hafid, A., & Elie, E. (2022). Blockchain as privacy and security solution for smart environments: a survey.. https://doi.org/10.48550/arxiv.2203.08901

Edastama, P., Purnama, S., Widayanti, R., Meria, L., & Rivelino, D. (2021). Potential blockchain technology in higher education learning innovations in era 4.0. Blockchain Frontier Technology, 1(01), 104-113. https://doi.org/10.34306/bfront.v1i01.18

Elghoul, M. (2021). A review of leveraging blockchain based framework landscape in healthcare systems. International Journal of Intelligent Computing and Information Sciences, 0(0), 1-13. https://doi.org/10.21608/ijicis.2021.75531.1095

environment. Journal of King Abdulaziz University-Computing and Information Technology Sciences, 8(1), 71-84. https://doi.org/10.4197/comp.8-1.7

Feng, H., Wang, X., Duan, Y., Zhang, J., & Zhang, X. (2020). Applying blockchain technology to improve agri-food traceability: a review of development methods, benefits and challenges. Journal of Cleaner Production, 260, 121031. https://doi.org/10.1016/j.jclepro.2020.121031

Fotiou, N., Pittaras, I., Siris, V., Voulgaris, S., & Polyzos, G. (2019). Secure iot access at scale using blockchains and smart contracts.. https://doi.org/10.1109/wowmom.2019.8793047

Francisco, K. and Swanson, D. (2018). The supply chain has no clothes: technology adoption of blockchain for supply chain transparency. Logistics, 2(1), 2. https://doi.org/10.3390/logistics2010002

Gardasevic, G., Katzis, K., Bajic, D., & Berbakov, L. (2020). Emerging wireless sensor networks and internet of things technologies—foundations of smart healthcare. Sensors, 20(13), 3619. https://doi.org/10.3390/s20133619

Gawande, N. and Bakliwal, A. (2022). Application of artificial intelligence in blockchain technology: a perspective of financial decision making. Prayukti – Journal of Management Applications, 02(01), 26-31. https://doi.org/10.52814/pjma.2022.2104

Ghazaleh, M. and Zabadi, A. (2021). Blockchain (bc) upending customer experience: promoting a new customer relationship management (crm) structure using blockchain technology (bct). Journal of Management and Sustainability, 11(1), 203. https://doi.org/10.5539/jms.v11n1p203

Hameed, K., Barika, M., Garg, S., Amin, M., & Kang, B. (2022). A taxonomy study on securing blockchain-based industrial applications: an overview, application perspectives, requirements, attacks, countermeasures, and open issues. Journal of Industrial Information Integration, 26, 100312. https://doi.org/10.1016/j.jii.2021.100312

Hartanti, B., Romadon, A., Anisah, N., & Utomo, L. (2021). Information systems behavior on system security in the perspective of “theory of reasoned action”.. https://doi.org/10.2991/assehr.k.210413.001

Hidayati, J., Vamelia, R., Hammami, J., & Endri, E. (2023). Transparent distribution system design of halal beef supply chain. Uncertain Supply Chain Management, 11(1), 31-40. https://doi.org/10.5267/j.uscm.2022.12.003

Hölbl, M., Kompara, M., Kamišalić, A., & Zlatolas, L. (2018). A systematic review of the use of blockchain in healthcare. Symmetry, 10(10), 470. https://doi.org/10.3390/sym10100470

Hu, X., Su, Y., & Guo, R. (2020). Iot adaptive dynamic blockchain networking method based on discrete heartbeat signals. Sensors, 20(22), 6503. https://doi.org/10.3390/s20226503

Hughes, D., Dwivedi, Y., Misra, S., Rana, N., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: applications, benefits, limitations, emerging research themes and research agenda. International Journal of Information Management, 49, 114-129. https://doi.org/10.1016/j.ijinfomgt.2019.02.005

Idian, M., Hassan, M., & Terzungwe, A. (2023). Artificial intelligence, blockchain, machine learning, and customer relationship management. Bincang Sains Dan Teknologi, 2(01), 16-20. https://doi.org/10.56741/bst.v2i01.276

Iermakova, O., Sedikova, I., & Dashian, A. (2022). Prospects of implementation of blockchain technology into aquaculture sector of ukraine. Economics Ecology Socium, 6(2), 29-37. https://doi.org/10.31520/2616-7107/2022.6.2-3

Iermakova, O., Sedikova, I., & Dashian, A. (2022). Prospects of implementation of blockchain technology into aquaculture sector of ukraine. Economics Ecology Socium, 6(2), 29-37. https://doi.org/10.31520/2616-7107/2022.6.2-3

Indrawati, I. and Firdaus, N. (2022). Blockchain acceptance analysis using the utaut2 model. Trikonomika, 21(2), 77-83. https://doi.org/10.23969/trikonomika.v21i2.5031

Jamil, F., Qayyum, F., Alhelaly, S., Javed, F., & Muthanna, A. (2021). Intelligent microservice based on blockchain for healthcare applications. Computers Materials & Continua, 69(2), 2513-2530. https://doi.org/10.32604/cmc.2021.018809

Jia, C., Ding, H., Zhang, C., & Zhang, X. (2020). Management and security analysis of blockchain shard storage for monitoring data on the state of smart substations. European Journal of Electrical Engineering, 22(2), 105-110. https://doi.org/10.18280/ejee.220203

Kamangar, Z., Memon, R., Memon, G., & Kamangar, U. (2023). Integration of internet of things and blockchain technology in healthcare domain: a systematic literature review. International Journal of Communication Systems, 36(16). https://doi.org/10.1002/dac.5582

Khonde, S. and Ulagamuthalvi, V. (2022). Hybrid intrusion detection system using blockchain framework. Eurasip Journal on Wireless Communications and Networking, 2022(1). https://doi.org/10.1186/s13638-022-02089-4

Koh, S., Dolgui, A., & Sarkis, J. (2020). Blockchain in transport and logistics – paradigms and transitions. International Journal of Production Research, 58(7), 2054-2062. https://doi.org/10.1080/00207543.2020.1736428

Li, B., Banimenia, I., Liu, C., Hou, Z., & Zhao, J. (2023). Incentive‐based demand response program with self‐reported baseline supported by blockchain technology. Iet Smart Grid, 6(2), 205-218. https://doi.org/10.1049/stg2.12100

Li, G., Dong, M., Yang, L., Ota, K., Wu, J., & Li, J. (2020). Preserving edge knowledge sharing among iot services: a blockchain-based approach. Ieee Transactions on Emerging Topics in Computational Intelligence, 4(5), 653-665. https://doi.org/10.1109/tetci.2019.2952587

Li, X., Jiang, P., Chen, T., Wang, L., & Wen, Q. (2020). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841-853. https://doi.org/10.1016/j.future.2017.08.020

Liu, B., Ma, X., Tan, E., & Ma, Z. (2023). Passenger flow anomaly detection in urban rail transit networks with graph convolution network–informer and gaussian bayes models. Philosophical Transactions of the Royal Society a Mathematical Physical and Engineering Sciences, 381(2254). https://doi.org/10.1098/rsta.2022.0253

López, D. and Farooq, B. (2020). A multi-layered blockchain framework for smart mobility data-markets. Transportation Research Part C Emerging Technologies, 111, 588-615. https://doi.org/10.1016/j.trc.2020.01.002

Lu, X., Fu, S., Jiang, C., & Liò, P. (2021). A fine-grained iot data access control scheme combining attribute-based encryption and blockchain. Security and Communication Networks, 2021, 1-13. https://doi.org/10.1155/2021/5308206

Maesaroh, S., Permana, H., Febrianaga, P., & Pardosi, R. (2022). Blockchain technology in the future of enterprise security system from cybercrime. Blockchain Frontier Technology, 2(1), 1-8. https://doi.org/10.34306/bfront.v2i1.88

Mahmood, M. and Dabagh, N. (2023). Blockchain technology and internet of things: review, challenge and security concern. International Journal of Electrical and Computer Engineering (Ijece), 13(1), 718. https://doi.org/10.11591/ijece.v13i1.pp718-735

Maiti, A., Raza, A., Kang, B., & Hardy, L. (2019). Estimating service quality in industrial internet-of-things monitoring applications with blockchain. Ieee Access, 7, 155489-155503. https://doi.org/10.1109/access.2019.2948269

Makridakis, S. and Christodoulou, K. (2019). Blockchain: current challenges and future prospects/applications. Future Internet, 11(12), 258. https://doi.org/10.3390/fi11120258

Mamoshina, P., Ojomoko, L., Yanovich, Y., Ostrovski, A., Botezatu, A., Prikhodko, P., … & Zhavoronkov, A. (2017). Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. Oncotarget, 9(5), 5665-5690. https://doi.org/10.18632/oncotarget.22345

Melnychuk, N. (2020). Analyzing the conceptual bases of development of the integrated information-analytical system «transparent budget» in ukraine. Business Inform, 1(504), 330-336. https://doi.org/10.32983/2222-4459-2020-1-330-336

Memon, R., Li, J., Nazeer, M., Khan, A., & Ahmed, J. (2019). Dualfog-iot: additional fog layer for solving blockchain integration problem in internet of things. Ieee Access, 7, 169073-169093. https://doi.org/10.1109/access.2019.2952472

Murillo, A. (2023). Artificial intelligence and blockchain: debate around legal challenges.. https://doi.org/10.5772/intechopen.106998

Myeong, S. and Jung, Y. (2019). Administrative reforms in the fourth industrial revolution: the case of blockchain use. Sustainability, 11(14), 3971. https://doi.org/10.3390/su11143971

Nazir, S., Kaleem, M., Hamdoun, H., Alzubi, J., & Tianfield, H. (2022). Blockchain of things for healthcare asset management., 181-198. https://doi.org/10.1049/pbhe038e_ch10

Nguyen, D., Ding, M., Pathirana, P., & Seneviratne, A. (2020). Blockchain and ai-based solutions to combat coronavirus (covid-19)-like epidemics: a survey.. https://doi.org/10.36227/techrxiv.12121962

Owusu-Oware, E. and Effah, J. (2022). Biometric system for protecting information and improving service delivery: the case of a developing country's social security and pension organisation. Information Development, 40(1), 61-74. https://doi.org/10.1177/02666669221085709

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and iot integration: a systematic survey. Sensors, 18(8), 2575. https://doi.org/10.3390/s18082575

Parmar, M. and Shah, P. (2023). Internet of things-blockchain lightweight cryptography to data security and integrity for intelligent application. International Journal of Electrical and Computer Engineering (Ijece), 13(4), 4422. https://doi.org/10.11591/ijece.v13i4.pp4422-4431

Perera, P. and Abeygunasekera, A. (2022). Blockchain adoption in accounting and auditing: a qualitative inquiry in sri lanka. Colombo Business Journal International Journal of Theory and Practice, 13(1), 57-87. https://doi.org/10.4038/cbj.v13i1.89

Ponte, E. and Bednárová, M. (2019). Blockchain and its implications for accounting and auditing. Meditari Accountancy Research, 27(5), 725-740. https://doi.org/10.1108/medar-11-2018-0406

Qin, C., Guo, B., Shen, Y., Tao, L., Yun, Z., & Zhang, Z. (2020). A secure and effective construction scheme for blockchain networks. Security and Communication Networks, 2020, 1-20. https://doi.org/10.1155/2020/8881881

Raja, G., Manaswini, Y., Vivekanandan, G., Sampath, H., Dev, K., & Bashir, A. (2020). Ai-powered blockchain - a decentralized secure multiparty computation protocol for iov.. https://doi.org/10.1109/infocomwkshps50562.2020.9162866

Ramesh, S., Patan, R., Prasath, R., Al-Turjman, F., Ramachandran, M., & Mostarda, L. (2020). Survival study on blockchain based 6g-enabled mobile edge computation for iot automation. Ieee Access, 8, 143453-143463. https://doi.org/10.1109/access.2020.3013946

Ramtohul, A. and Soyjaudah, K. (2016). Information security governance for e-services in southern african developing countries e-government projects. Journal of Science and

Technology Policy Management, 7(1), 26-42. https://doi.org/10.1108/jstpm-04-2014-0014

Ramtohul, A. and Soyjaudah, K. (2016). Information security governance for e-services in southern african developing countries e-government projects. Journal of Science and Technology Policy Management, 7(1), 26-42. https://doi.org/10.1108/jstpm-04-2014-0014

Rathee, G., Sharma, A., Iqbal, R., Aloqaily, M., Jaglan, N., & Kumar, R. (2019). A blockchain framework for securing connected and autonomous vehicles. Sensors, 19(14), 3165. https://doi.org/10.3390/s19143165

Riadi, I., Herman, H., & Ifani, A. (2021). Optimization of system authentication services using blockchain technology. Kinetik Game Technology Information System Computer Network Computing Electronics and Control. https://doi.org/10.22219/kinetik.v6i4.1325

Romashkova, I., Komarov, M., & Ometov, A. (2021). Demystifying blockchain technology for resource-constrained iot devices: parameters, challenges and future perspective. Ieee Access, 9, 129264-129277. https://doi.org/10.1109/access.2021.3112228

Rozman, N., Corn, M., Škulj, G., Diaci, J., & Podržaj, P. (2022). Scalability solutions in blockchain-supported manufacturing: a survey. Strojniški Vestnik – Journal of Mechanical Engineering, 68(10), 585-609. https://doi.org/10.5545/sv-jme.2022.355

Rubaeah, S., Mangkunegara, I., & Purwono, P. (2023). Review of internet of things (iot) and blockchain in healthcare: chronic disease detection and data security. JAHIR, 1(1), 16-20. https://doi.org/10.59247/jahir.v1i1.15

Salah, K., Rehman, M., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for ai: review and open research challenges. Ieee Access, 7, 10127-10149. https://doi.org/10.1109/access.2018.2890507

Shafay, M., Ahmad, R., Yaqoob, I., Jayaraman, R., & Omar, M. (2022). Blockchain for deep learning: review and open challenges. Cluster Computing, 26(1), 197-221. https://doi.org/10.1007/s10586-022-03582-7

Shah, I., Doshi, C., Patel, M., Tanwar, S., Hong, W., & Sharma, R. (2022). A comprehensive review of the technological solutions to analyse the effects of pandemic outbreak on human lives. Medicina, 58(2), 311. https://doi.org/10.3390/medicina58020311

Shahbazi, Z. and Byun, Y. (2022). Analysis of the security and reliability of cryptocurrency systems using knowledge discovery and machine learning methods. Sensors, 22(23), 9083. https://doi.org/10.3390/s22239083

Sharma, P., Bhatia, V., & Prakash, S. (2023). Securing optical networks using quantum-secured blockchain: an overview. Sensors, 23(3), 1228. https://doi.org/10.3390/s23031228

Shinde, R., Patil, S., Kotecha, K., & Ruikar, K. (2021). Blockchain for securing ai applications and open innovations. Journal of Open Innovation Technology Market and Complexity, 7(3), 189. https://doi.org/10.3390/joitmc7030189

Shinde, R., Patil, S., Kotecha, K., & Ruikar, K. (2021). Blockchain for securing ai applications and open innovations. Journal of Open Innovation Technology Market and Complexity, 7(3), 189. https://doi.org/10.3390/joitmc7030189

Singh, P. and Singh, N. (2020). Blockchain with iot and ai. International Journal of Applied Evolutionary Computation, 11(4), 13-27. https://doi.org/10.4018/ijaec.2020100102

Singh, S., Hosen, A., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed iot network. Ieee Access, 9, 13938-13959. https://doi.org/10.1109/access.2021.3051602

Singh, S., Wable, S., & Kharose, P. (2022). A review of e-voting system based on blockchain technology. International Journal of New Practices in Management and Engineering, 10(04), 09-13. https://doi.org/10.17762/ijnpme.v10i04.125

Sreenivasan, A. and Suresh, M. (2023). Start-up sustainability: does blockchain adoption drives sustainability in start-ups? a systematic literature reviews. Management Research Review, 47(3), 390-405. https://doi.org/10.1108/mrr-07-2022-0519

Srivastava, S., Pant, M., Jauhar, S., & Nagar, A. (2022). Analyzing the prospects of blockchain in healthcare industry. Computational and Mathematical Methods in Medicine, 2022, 1-24. https://doi.org/10.1155/2022/3727389

Sultana, M., Hossain, A., Laila, F., Taher, K., & Islam, M. (2020). Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. BMC Medical Informatics and Decision Making, 20(1). https://doi.org/10.1186/s12911-020-01275-y

Tahir, M., Sardaraz, M., Muhammad, S., & Khan, M. (2020). A lightweight authentication and authorization framework for blockchain-enabled iot network in health-informatics. Sustainability, 12(17), 6960. https://doi.org/10.3390/su12176960

Tan, B. and Low, K. (2019). Blockchain as the database engine in the accounting system. Australian Accounting Review, 29(2), 312-318. https://doi.org/10.1111/auar.12278

Tiwari, A. and Batra, U. (2021). Blockchain enabled reparations in smart buildings cyber physical system. Defence Science Journal, 71(4), 491-498. https://doi.org/10.14429/dsj.71.16454

Voulgaris, S., Fotiou, N., Siris, V., Polyzos, G., Jaatinen, M., & Oikonomidis, Y. (2019). Blockchain technology for intelligent environments. Future Internet, 11(10), 213. https://doi.org/10.3390/fi11100213

Walde, R. and Yadav, A. (2022). Blockchain technology for e-government. International Journal for Research in Applied Science and Engineering Technology, 10(8), 1698-1703. https://doi.org/10.22214/ijraset.2022.46487

Wang, J., Xiong, N., Alfarraj, O., Tolba, A., & Ren, Y. (2023). S-bds: an effective blockchain-based data storage scheme in zero-trust iot. Acm Transactions on Internet Technology, 23(3), 1-23. https://doi.org/10.1145/3511902

Wazid, M., Das, A., Shetty, S., & Jo, M. (2020). A tutorial and future research for building a blockchain-based secure communication scheme for internet of intelligent things. Ieee Access, 8, 88700-88716. https://doi.org/10.1109/access.2020.2992467

Wong, P., Sinha, S., & Chui, C. (2021). Blockchain in manufacturing quality control: a computer simulation study. Plos One, 16(3), e0247925. https://doi.org/10.1371/journal.pone.0247925

Wu, H., Dwivedi, A., & Srivastava, G. (2021). Security and privacy of patient information in medical systems based on blockchain technology. Acm Transactions on Multimedia Computing Communications and Applications, 17(2s), 1-17. https://doi.org/10.1145/3408321

Xu, P., Lee, J., Barth, J., & Richey, R. (2021). Blockchain as supply chain technology: considering transparency and security. International Journal of Physical Distribution & Logistics Management, 51(3), 305-324. https://doi.org/10.1108/ijpdlm-08-2019-0234

Xu, Z., Zhang, S., Han, H., Dong, X., Zhang, Z., Wang, H., … & Tian, W. (2022). Blockchain-aided searchable encryption-based two-way attribute access control research. Security and Communication Networks, 2022, 1-13. https://doi.org/10.1155/2022/2410455

Zhang, H., Zhao, S., Liu, R., Wang, W., Hong, Y., & Hu, R. (2022). Automatic traffic anomaly detection on the road network with spatial-temporal graph neural network representation learning. Wireless Communications and Mobile Computing, 2022, 1-12. https://doi.org/10.1155/2022/4222827

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. Acm Computing Surveys, 52(3), 1-34. https://doi.org/10.1145/3316481

Zhang, X., Xue, M., & Miao, X. (2022). A consensus algorithm based on risk assessment model for permissioned blockchain. Wireless Communications and Mobile Computing, 2022, 1-21. https://doi.org/10.1155/2022/8698009

Zhang, Y., Geng, H., Su, L., & Lu, L. (2022). A blockchain-based efficient data integrity verification scheme in multi-cloud storage. Ieee Access, 10, 105920-105929. https://doi.org/10.1109/access.2022.3211391

Zhang, Z., Song, X., Liu, L., Yin, J., Wang, Y., & Lan, D. (2021). Recent advances in blockchain and artificial intelligence integration: feasibility analysis, research issues, applications, challenges, and future work. Security and Communication Networks, 2021, 1-15. https://doi.org/10.1155/2021/9991535

Zhang, Z., Yang, M., Su, R., & Wen, J. (2022). Blockchain-based data sharing scheme for internet of vehicles.. https://doi.org/10.1117/12.2662710

Zhao, C. and Meng, X. (2019). Research on innovation and development of blockchain technology in financial field.. https://doi.org/10.2991/icpcs-19.2019.93

Zheng, Z. (2019). Blockchain intelligence: when blockchain meets artificial intelligence.. https://doi.org/10.48550/arxiv.1912.06485

Zhong, B. (2022). The research on innovative application of blockchain technology in sharing economy., 68-79. https://doi.org/10.2991/978-94-6463-030-5_9