International Journal of Social and Education (INJOSEDU) e-ISSN: 3047-6151
Vol. 2 No. 2 March 2025, hal., 666-681

USE OF BLOCKCHAIN TECHNOLOGY IN DATA DISTRIBUTION SYSTEM SECURITY

Nur Hakim*
Akademi Maritim Pembangunan Jakarta, Indonesia
E-mail: nurhakimboy5@gmail.com

Asri Ady Bakri
Universitas Muslim, Indonesia
E-mail: asriady.bakri@umi.ac.id

Farid Wahyudi
Universitas Islam Raden Rahmat, Indonesia
E-mail: faridstifler@gmail.com

Abstract

In the current digital era, data security is a major concern in various industrial sectors. Blockchain, as the data distribution technology underlying cryptocurrencies such as Bitcoin, has shown significant potential in addressing various data security issues. This literature research aims to comprehensively examine the use of blockchain technology in improving the security of data distribution systems. Through a systematic review method, this research collects and analyzes various studies, articles and reports related to the use of blockchain in the context of data security. The literature review results show that blockchain offers several key security features, such as decentralization, resistance to manipulation, anonymity, and transparency, which can prevent cyberattacks and protect data integrity. However, this research also identifies challenges faced in blockchain implementation, including issues of scalability, energy efficiency, and compatibility with existing data systems. This research suggests that the development of hybrid solutions that combine blockchain elements with traditional data distribution technologies can provide a balance between security and efficiency. Additionally, cooperation between developers, industry, and regulators is critical to creating standards and frameworks that support widespread blockchain adoption. Thus, this research provides a balanced view of the potential and challenges of using blockchain in the security of data distribution systems, as well as suggesting directions for further research and development in this area.

Keywords: Blockchain, Data Security, Data Distribution Systems, Decentralization, Cyber Risk Management

INTRODUCTION

In the ever-growing digital era, data security has become one of the main priorities in information management. Many technologies exist to answer this challenge, but special attention is currently focused on the use of blockchain in improving the security of data distribution systems. Blockchain technology, widely known through the popularity of digital currencies such as Bitcoin, brings significant innovation in the way data is stored, verified, and distributed (Gu & Sundaram, 2023).

The basic concept of blockchain is a distributed and immutable digital ledger, where digital records or blocks of data are connected to each other using cryptography. This creates a very secure blockchain, because any change to one of the blocks requires revalidation of the entire chain (Wang, 2022). In the context of data distribution system security, this technology offers transparency, integrity, and resistance to attacks or data manipulation.

The use of blockchain in a data distribution system allows various entities to share access to a secure database without the need for trust or intermediaries. This means each entity can independently verify the validity of the data, ensuring the accuracy of the information distributed (Wu et al., 2023). In other words, blockchain eliminates the risk of data leakage or incompatibility, which is often a problem in traditional data distribution systems.

Another advantage of blockchain is its ability to give users greater control over their data. In many systems, users often do not know how their data is used or distributed (Setiawan & Alamsyah, 2023). With blockchain, every data transaction is recorded transparently, giving users the ability to track and audit their data independently. This not only improves data security, but also increases trust between users and service providers.

The use of blockchain in the security of data distribution systems is still a developing area, with many opportunities and challenges that have not yet been fully explored. However, its potential to change the digital security landscape cannot be underestimated. With the ever-increasing volume of data created and distributed every day, blockchain offers a solution that may become the new standard in maintaining the integrity and security of information in the future (Karmakar et al., 2022).

As the adoption of digital technology accelerates in various sectors, there is an urgent need to develop data security systems that are not only effective but also efficient and easy to adapt. Blockchain, with its decentralized characteristics, meets these needs by providing a solution that

reduces dependence on central servers that are vulnerable to cyber attacks. With its distributive design, blockchain ensures that data is not centralized in one location, reducing the risk of data loss due to hacker attacks or system failures. This directly increases the resilience of the data distribution system against external and internal threats (Chander, 2022).

Additionally, the consensus mechanism in blockchain ensures that any changes or additions to data must be approved by the majority of participants in the network. This mechanism significantly reduces the possibility of data manipulation, as any attempt at unauthorized changes will be easily detected by other participants. In the context of using this technology in data distribution, this means that each entity involved can trust the accuracy and authenticity of the information without the need for time- and resource-consuming manual verification (Erica et al., 2024).

The implementation of blockchain in data distribution also allows the creation of smart contracts, which are programs that automatically execute, control, or document events and actions according to the terms of the agreement. Smart contracts can be an important instrument in ensuring transparency and compliance in data transactions, providing further assurance of system reliability and integrity (Feng et al., 2023).

However, despite the great potential that blockchain has, there are still several challenges that need to be overcome for its wider implementation in data security. There are problems related to scalability, energy consumption, and the need for clear standardization and regulations (Tenge & Okello, 2022). Despite these challenges, active efforts from the technology, business, and regulatory communities are being taken to overcome these obstacles and enable a more seamless integration of blockchain into existing data security systems.

In the coming years, it is expected that advances in blockchain technology will continue to pave the way for more secure, transparent, and efficient data security solutions. Along with these steps, sensitivity to privacy and information security is expected to be an impetus for wider adoption of blockchain, not only as a means to strengthen security but also as a marker for a new era in secure and trusted data management and distribution.

RESEARCH METHOD

The study in this research is qualitative with literature. The literature study research method is a research approach that involves the analysis and synthesis of information from various literature sources that are relevant to a

particular research topic. Documents taken from literature research are journals, books and references related to the discussion you want to research (Earley, M.A. 2014; Snyder, H. 2019).

RESULT AND DISCUSSION

Characteristics of Blockchain Technology that Support Data Security

Blockchain technology has revolutionized the way we view data security and distribution in the digital era. Its unique characteristics provide various features that support data security, making this technology a potential solution to overcome various security challenges faced by today's information systems (Kuchipudi et al., 2024).

One of the main characteristics of blockchain that supports data security is its decentralized nature. In contrast to traditional data storage models that use a central server, blockchain stores data in a distributed manner across various nodes or points in the network. This means there is no single point of failure that an attacker could exploit to take over or damage the entire system. By disseminating data widely, blockchain increases resilience to cyberattacks, fraud, and system failures (Swathi et al., 2022).

Encryption is another important aspect of blockchain that strengthens data security. Every transaction or block of data added to the blockchain is encrypted using advanced cryptographic algorithms. User identities are protected using private and public keys, ensuring that only the data owner can access and carry out transactions with them. This encryption technique provides an additional layer of security that maintains the integrity and confidentiality of data, making it very difficult for unauthorized parties to change or access information without permission (Saah et al., 2023).

Then, the transparency and auditability provided by blockchain is another factor that increases data security. Although individual transactions are protected and anonymous, the entire transaction history is visible to all participants in the network. Each new block must be verified by a number of participants through a consensus process before being added to the chain, ensuring that all transactions are valid and accurate (Masroor et al., 2024). This characteristic allows for independent verification without compromising privacy, offering robust security guarantees against data manipulation.

Finally, the use of smart contracts in blockchain adds another layer of security protection. Smart contracts are protocols that execute agreements automatically when conditions are met, without the need for third party intervention. This minimizes the risk of fraud and human error, as the contract

will only execute if all conditions are met and confirmed by the network. The implementation of smart contracts in blockchain not only increases efficiency in transactions but also provides greater certainty in the accuracy and accountability of transactions, strengthening data security fundamentals (Sujan & Suresh, 2022).

Widespread adoption of blockchain technology may still be in its infancy for many industries, but its potential in changing the data security paradigm is clear to see. The emergence of blockchain-based solutions offers new hope in the fight against hacking, data loss and increasingly sophisticated forms of cyberattacks (Bai et al., 2023). By providing a system that is more resistant to external attacks and internal errors, blockchain brings a breath of fresh air into the world of digital data security.

In addition, blockchain's inherent characteristics eliminate the need for third parties in transaction verification, not only cutting costs and reducing transaction times but also significantly increasing security. Eliminating third parties means reducing potential weak points in the security system, an important step considering that many large data leaks occur through third parties whose security is not as tight as the primary entity (Samanta et al., 2023).

Further development of blockchain technology also focuses on scalability and sustainability, two aspects that will help enhance its usefulness as a data security tool. For example, advances such as blockchain technology are eco-friendly and scalable consensus mechanism solutions are designed to address challenges such as high energy consumption and low transaction speeds. These innovations not only help overcome technical limitations but also strengthen blockchain's position as a secure, reliable, and sustainable technology (Lakshmaiah et al., 2023).

Finally, the application of blockchain in sectors other than finance such as healthcare, education, and government governance shows the broader potential of this technology in securing sensitive data. In healthcare, for example, blockchain can ensure the integrity and privacy of patient data while facilitating the secure exchange of information between institutions (Heister & Yuthas, 2022). In an educational context, blockchain can be used to verify diplomas and academic records, offering a transparent and immutable solution for validating academic achievements.

In essence, blockchain characteristics such as decentralization, encryption, transparency, and the use of smart contracts promise significant improvements in data security. As its adoption continues to grow, we will

likely see broader and more innovative use of this technology, not only as a security tool but also as the foundation of many new digital applications and services in the future (Soni et al., 2023).

Blockchain Use Cases in Various Sectors for Secure Data Distribution

In the healthcare sector, blockchain has great potential for distributing secure data and ensuring information integrity. Patient medical information is highly sensitive and requires the highest level of privacy and compliance with regulations such as HIPAA in the United States. Blockchain can be used to store electronic health records in a decentralized manner, reducing the risk of data leaks often associated with centralized storage. Patients can have greater control over their own data by providing selective access to different healthcare providers (Halkiopoulos et al., 2023). By using this technology, transactions between hospitals, laboratories, insurance companies and patients can occur more efficiently and safely, because every health record update will automatically be validated and recorded in the blockchain.

The education sector can also benefit from blockchain in distributing and authenticating academic and professional data. Transcripts and diplomas stored in a blockchain can be accessed by interested parties such as academic institutions or potential employers, without the risk of document forgery (Gopal & Omeleze-Baror, 2024). This allows for a faster and more transparent verification process, thereby increasing individual academic and professional mobility. Furthermore, by using smart contracts, universities can automatically issue credits or certificates that students have successfully completed, eliminating the need for administrative intervention and reducing the costs and time involved.

Turning to the supply chain sector, the use of blockchain can increase the visibility and traceability of products moving from the factory to the hands of consumers. Each stage in the supply chain can be recorded on the blockchain, offering immutable proof of the product's origin, journey and handling. This is especially important in industries such as food and pharmaceuticals, where product authenticity and freshness can be a health issue (Kumar & Sharma, 2024). For example, blockchain can be used to monitor the distribution of medicines, ensuring that the medicines that reach patients are genuine and meet required storage standards. This reduces the risk of contamination, product substitution and fraud, while increasing consumer confidence in the brands and products they purchase.

In the financial sector, blockchain has demonstrated its potential to revolutionize the way transactions are conducted, reducing fraud and increasing transparency. This technology enables secure peer-to-peer transactions without the need for intermediaries, such as banks or other financial institutions. This can reduce transaction costs and speed up cross-border payment processing. In addition, by using blockchain, financial institutions can simplify KYC (Know Your Customer) and AML (Anti-Money Laundering) processes, ensuring compliance with regulations more efficiently. Real-time distributed ledgers make it easier to track assets and payments, reducing the possibility of fraud and ensuring data integrity (Goel et al., 2024).

In the energy industry, blockchain implementation can create transparency and efficiency in energy distribution. With the emergence of decentralized energy grid models, blockchain supports peer-to-peer energy transactions, allowing households to sell excess energy generated from renewable sources such as solar panels directly to their neighbors without the need for intermediaries. This can reduce energy expenditure and increase the use of renewable energy sources. Blockchain can also be used to validate and record energy transactions automatically, encouraging the creation of more accurate and transparent billing systems (Ramasamy & Khan, 2024).

The entertainment and media sectors can leverage blockchain to provide a fairer and more transparent content distribution model. In the music industry, for example, blockchain could facilitate direct royalty payments to artists and content creators every time their work is played, reducing the need for record labels and distributors as middlemen. It can also improve the user experience by enabling direct access to content through smart contracts, which provide rules-based permissions without bypassing traditional DRM (Digital Rights Management) systems that often hinder and slow down the access process. Thus, blockchain offers a way to distribute revenue more fairly while ensuring copyright and secure distribution of content in the entertainment sector (Shafeeq & Fischer, 2023).

Barriers and Disadvantages of Using Blockchain in Data Security Aspects

Although blockchain is considered a promising technology for improving data security, there are several obstacles and drawbacks that need to be considered. One of the biggest drawbacks of using blockchain in data security is the issue of scalability. Conventional blockchains such as Bitcoin can process transactions at relatively low speeds compared to traditional payment systems such as Visa or PayPal (Sehrawat, 2024). This is due to consensus

mechanisms such as proof-of-work that ensure security and decentralization but require a lot of time and computing power. These throughput limitations may limit blockchain's ability to be widely adopted in applications that require processing large volumes of data and at high speed.

In addition to scalability issues, interoperability is also an important challenge. Because there are many different blockchain chains and no established standards, it is difficult to move or access information across blockchain platforms. This means that information on one blockchain may be incompatible with another, which can limit data exchange and collaboration between sectors or organizations. This fragmented data distribution can complicate system integration and limit cross-platform innovation (Peterson & Wendt, 2023).

Security is the main attraction of blockchain, but it is not without its drawbacks. One of the security risks that exists in blockchain is the potential for a 51% attack. If an attacker manages to control more than 50% of the blockchain network's computing power, he can manipulate or revise transactions and prevent the confirmation of new transactions. While the risk of this type of attack may be small for large blockchains with very widespread and large networks, smaller, less decentralized blockchains could be potentially vulnerable to this type of manipulation (Mahasree et al., 2022).

Finally, privacy concerns emerge as one of the drawbacks of blockchain, especially due to the transparent nature of decentralized ledgers. Although transactions on the blockchain are pseudonymous, the entire transaction is open to the public and traceable, meaning that users' privacy could be compromised if the identity associated with their blockchain address is discovered (Kashevarova & Kulikova, 2024). Additionally, these technologies still have to address how to manage and protect personal data in compliance with increasingly stringent privacy regulations such as Europe's General Data Protection Regulation (GDPR), which demands a right to be forgotten that may be incompatible with the permanent and unchangeable nature of blockchain .

Despite these challenges, industry and researchers continue to seek solutions to overcome the barriers and shortcomings that exist in using blockchain for data security. One approach being explored is the development of new consensus algorithms that are more efficient and minimize power usage without sacrificing security and decentralization (Hooda et al., 2024). For example, proof-of-stake and other variants are being tested as alternatives to the energy-intensive and slow proof-of-work. Additionally, technologies

such as sharding and layer 2 networks are being developed to increase blockchain scalability, allowing for faster processing and validation of transactions while maintaining the principle of decentralization.

On the interoperability side, blockchain projects are now focusing more on creating standards that allow different chains to communicate efficiently with each other. Cross-chain protocols and blockchain bridges have been designed to simplify the exchange of information and assets between different blockchain platforms, thereby unlocking the potential for a truly interconnected blockchain ecosystem. This move will not only strengthen the use cases for blockchain technology in various industries but also pave the way for new innovations that can leverage data across networks (Kaur & Lnu, 2022).

To address security risks such as 51% attacks, proposed solutions include the use of sidechains to distribute computing power more evenly and reduce the concentration of power on a small group of participants. The use of more sophisticated smart contracts and multi-signature validation mechanisms can also improve transaction security. Furthermore, the development of new cryptographic techniques, such as zero-knowledge proofs, offers a way to increase user privacy by enabling transaction verification without the need to disclose sensitive information to third parties (Kuye, 2024).

Regarding privacy, solutions such as homomorphic encryption and the use of private blockchains or hybrid blockchains may offer a balance between transparency and privacy. By ensuring that sensitive data can remain encrypted even while it is being processed, blockchain can comply with privacy regulations while still offering security and transparency. Regulations and policies designed specifically for blockchain technology are also being discussed as a way to ensure that data privacy and security needs are met without hindering technological innovation (Du et al., 2022).

Overall, although there are still obstacles and shortcomings in using blockchain for data security, ongoing efforts in research and development show the potential to overcome these challenges. With innovative and collaborative solutions, the future of blockchain in the aspect of data security looks increasingly promising.

CONCLUSION

The use of blockchain technology in the security of data distribution systems promises significant improvements in terms of transparency, integrity

and non-repudiation. By its decentralized nature, blockchain reduces central points of weakness, reducing the risk of cyberattacks and data manipulation. Consensus algorithms, such as proof-of-work or proof-of-stake, ensure that only valid transactions can be added to the chain, adding an additional layer of security. Challenges such as scalability, energy efficiency, and interoperability still need to be overcome to maximize blockchain's potential. Efforts to develop new consensus algorithms, sharding, second-layer networks, and interoperability solutions are being explored to overcome these obstacles. Additionally, improved security mechanisms through more advanced smart contracts and new cryptographic techniques such as zero-knowledge proofs offer better user privacy without compromising transaction security. In the context of regulation and standardization, it is important for developers and regulators to work together to create frameworks that support the use of blockchain while addressing data privacy and security concerns. The use of homomorphic encryption and a hybrid blockchain model offers a middle ground between transparency and personal data protection. In conclusion, blockchain technology has tremendous potential in improving the security of data distribution systems, although there are obstacles and challenges that must be overcome. Through continued innovation and collaboration between industry and regulators, blockchain can change the data security landscape by offering solutions that are more secure, decentralized, and resistant to manipulation.

REFERENCES

Bai, Y., Liu, Y., & Deng, X. (2023). Research on the System of Blockchain Data Sharing and Early-warning Decision for Public Health Emergency. *2023 International Conference on Blockchain Technology and Information Security (ICBCTIS)*, *32*(Query date: 2024-09-08 19:16:29), 54–59. https://doi.org/10.1109/icbctis59921.2023.00015

Chander, B. (2022). Deep Dive Into Blockchain Technology: Characteristics, Security and Privacy Issues, Challenges, and Future Research Directions. *Smart City Infrastructure*, *Query date: 2024-09-08 19:16:29*, 1–32. https://doi.org/10.1002/9781119785569.ch1

Du, Y., Miao, S., Tong, Z., Lemieux, V., & Wang, Z. (2022). Blockchain-Empowered Mobile Edge Intelligence, Machine Learning and Secure Data Sharing. *Blockchain Potential in AI*, *Query date: 2024-09-08 19:22:57*. https://doi.org/10.5772/intechopen.96618

Earley, M. A. (2014). A synthesis of the literature on research methods education. Teaching in Higher Education, 19(3), 242-253.

Erica, A., Wulandari, S., & Widayanti, R. (2024). Data Security Transformation: The Significant Role of Blockchain Technology. *Blockchain Frontier Technology*, *3*(2), 107–112. https://doi.org/10.34306/bfront.v3i2.466

Feng, Y., Zhao, J., Chen, T., & Yu, Y. (2023). Blockchain-based ciphertext access control for data sharing using key encapsulation mechanism. *2023 International Conference on Blockchain Technology and Information Security (ICBCTIS)*, *29*(Query date: 2024-09-08 19:16:29), 46–53. https://doi.org/10.1109/icbctis59921.2023.00014

Goel, S., Sawant, S., & Rudra, B. (2024). Secure Decentralized Carpooling Application Using Blockchain and Zero Knowledge Proof. *Proceedings of the 9th International Conference on Internet of Things, Big Data and Security*, *Query date: 2024-09-08 19:22:57*, 260–267. https://doi.org/10.5220/0012701400003705

Gopal, J., & Omeleze-Baror, S. (2024). Using Blockchain to Secure Digital Identity and Privacy Across Digital Sectors. *International Conference on Cyber Warfare and Security*, *19*(1), 519–526. https://doi.org/10.34190/iccws.19.1.2041

Gu, Y., & Sundaram, S. M. (2023). Financial Technology Security Risk Management and Control Based on Big Data and Blockchain Technology. *2023 International Conference on Data Science and Network Security (ICDSNS)*, *2*(Query date: 2024-09-08 19:16:29), 1–5. https://doi.org/10.1109/icdsns58469.2023.10245206

Halkiopoulos, C., Antonopoulou, H., & Kostopoulos, N. (2023). Utilizing Blockchain Technology in Various Applications to Secure Data Flows. A Comprehensive Analysis. *Technium: Romanian Journal of Applied Sciences and Technology*, *11*(Query date: 2024-09-08 19:22:57), 44–55. https://doi.org/10.47577/technium.v11i.9132

Heister, S., & Yuthas, K. (2022). How Blockchain and AI Enable Personal Data Privacy and Support Cybersecurity. *Blockchain Potential in AI*, *Query date: 2024-09-08 19:16:29*. https://doi.org/10.5772/intechopen.96999

Hooda, A., Hooda, A., & Yadav, D. (2024). *Integrating Blockchain with Big Data for Secure Data Sharing: A Comprehensive Methodology*. *Query date: 2024-09-08 19:22:57*. https://doi.org/10.21203/rs.3.rs-5005857/v1

Karmakar, A., Ghosh, P., Banerjee, P. S., & De. (2022). E-Healthcare data security using blockchain technology. *Blockchain Technology in E-Healthcare Management*, *Query date: 2024-09-08 19:16:29*, 127–145. https://doi.org/10.1049/pbhe048e_ch5

Kashevarova, N. A., & Kulikova, M. E. (2024). Integration of blockchain and artificial intelligence as a mechanism for modernisation of various economic sectors. *Vestnik Universiteta*, *5*, 54–67. https://doi.org/10.26425/1816-4277-2024-5-54-67

Kaur, M., & Lnu, N. (2022). Ethereum, Hyperledger and CordaA Side-by-Side Comparison of Capabilities and Constraints for Developing Various

Business Case Uses. *The Auditor's Guide to Blockchain Technology*, *Query date: 2024-09-08 19:22:57*, 105–126. https://doi.org/10.1201/9781003211723-7

Kuchipudi, R., Murthy, T. S., Palamakula, R. B., & Sureddi, R. M. K. (2024). Security Aspects of Blockchain Technology. *Blockchain-Based Cyber Security*, *Query date: 2024-09-08 19:16:29*, 128–139. https://doi.org/10.1201/9781003389576-8

Kumar, R., & Sharma, R. (2024). *Secure and Efficient IoT Data Exchange: A Multilayer Authentication System with Blockchain*. *Query date: 2024-09-08 19:22:57*. https://doi.org/10.22541/au.171668819.94496032/v1

Kuye, A. (2024). *Decentralized Data Ownership and Secure Access Control in Web3: Leveraging Blockchain Technology to Enhance Data Privacy and Improve Healthcare Efficiency*. *Query date: 2024-09-08 19:22:57*. https://doi.org/10.2139/ssrn.4886316

Lakshmaiah, D., Rao, L. K., Rao, R. Y., Narayana, I. S., & Sneha, A. (2023). Hyper Ledger Fabric Blockchain for Data Security in IoT Devices. *Blockchain Technology for IoT and Wireless Communications*, *Query date: 2024-09-08 19:16:29*, 19–33. https://doi.org/10.1201/9781003269991-3

Mahasree, M., Puviarasan, N., & Aruna, P. (2022). Interpolation-based reversible data hiding with blockchain for secure e-healthcare systems. *Blockchain Applications for Healthcare Informatics*, *Query date: 2024-09-08 19:22:57*, 373–400. https://doi.org/10.1016/b978-0-323-90615-9.00005-0

Masroor, F., Gopalakrishnan, A., & Goveas, N. (2024). Securing Patient Data in IoT Devices: A Blockchain-NFT Approach for Privacy, Security, and Authentication. *Proceedings of the 21st International Conference on Security and Cryptography*, *Query date: 2024-09-08 19:16:29*. https://doi.org/10.5220/0012764800003767

Peterson, J., & Wendt, C. (2023). *Messaging Use Cases and Extensions for Secure Telephone Identity Revisited (STIR)*. *Query date: 2024-09-08 19:22:57*. https://doi.org/10.17487/rfc9475

Ramasamy, L. K., & Khan, F. (2024). Secure and Transparent Educational Data Record-Keeping with Blockchain. *Blockchain for Global Education*, *Query date: 2024-09-08 19:22:57*, 147–164. https://doi.org/10.1007/978-3-031-52123-2_8

Saah, A. E. N., Yee, J.-J., & Choi, J. (2023). *Securing the construction workers' data security and privacy with blockchain technology*. *Query date: 2024-09-08 19:16:29*. https://doi.org/10.20944/preprints202310.1179.v1

Samanta, R., Biswas, A., Bandyopadhyay, A., & Mandal, G. (2023). IoE and Blockchain Convergence for Enhanced Security. *Blockchain Technology for IoE*, *Query date: 2024-09-08 19:16:29*, 45–64. https://doi.org/10.1201/9781003366010-4

Sehrawat, K. D. S. (2024). Revolutionizing Public Health: A Blockchain—Based System for Secure Genetic and Medical Data Management. *International Journal of Science and Research (IJSR)*, *13*(1), 661–664. https://doi.org/10.21275/sr24109114954

Setiawan, I. P. S., & Alamsyah, A. (2023). Enhancing Security, Privacy, and Traceability in Indonesia's National Health Insurance Claims Process using Blockchain Technology. *2023 International Conference on Artificial Intelligence, Blockchain, Cloud Computing, and Data Analytics (ICoABCD)*, *26*(Query date: 2024-09-08 19:16:29), 77–82. https://doi.org/10.1109/icoabcd59879.2023.10390967

Shafeeq, S., & Fischer, M. (2023). SEBDA: A Secure and Efficient Blockchain Based Data Aggregation Scheme. *Proceedings of the 20th International Conference on Security and Cryptography*, *Query date: 2024-09-08 19:22:57*, 369–376. https://doi.org/10.5220/0012077900003555

Snyder, H. (2019¬). Literature review as a research methodology: An overview and guidelines. Journal of business research, 104, 333-339.

Soni, G., Chandrawanshi, K., Verma, R., & Saraswat, D. (2023). High Data Priority Endorsement and Profile Overhaul Using Blockchain against Remapping Attack in MANET-IoT. *Blockchain Technology for IoE*, *Query date: 2024-09-08 19:16:29*, 159–190. https://doi.org/10.1201/9781003366010-10

Sujan, R., & Suresh, k. (2022). Securing Distributed Data Mechanism Based On Blockchain Technology. *2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS)*, *46*(Query date: 2024-09-08 19:16:29), 1–6. https://doi.org/10.1109/ic3sis54991.2022.9885536

Swathi, B. H., Anusha, K. S., Gagana, S., & Lin, H. (2022). Security and privacy of smart grid data and management using blockchain technology. *Blockchain Technology for Smart Grids: Implementation, Management and Security*, *Query date: 2024-09-08 19:16:29*, 165–192. https://doi.org/10.1049/pbpo211e_ch7

Tenge, H., & Okello, M. (2022). Blockchain Technology. *The Auditor's Guide to Blockchain Technology*, *Query date: 2024-09-08 19:16:29*, 1–16. https://doi.org/10.1201/9781003211723-1

Wang, L. (2022). Financial risk analysis system and supervision based on big data and blockchain technology. *SECURITY AND PRIVACY*, *6*(2). https://doi.org/10.1002/spy2.224

Wu, J., Jiang, H., & Chen, J. (2023). *Enterprise data security storage integrating blockchain and artificial intelligence technology in investment risk management*. *Query date: 2024-09-08 19:16:29*. https://doi.org/10.21203/rs.3.rs-2589697/v1