ZAHRA: JOURNAL OF HEALTH AND MEDICAL RESEARCH e-ISSN: 2808-5396
Vol. 4 No. 2 April 2025, hal., 183-196

BLOCKCHAIN FOR PATIENT DATA SECURITY: POTENTIAL AND CHALLENGES

Loso Judijanto *[1]
IPOSS Jakarta, Indonesia
losojudijantobumn@gmail.com

Arnes Yuli Vandika
Universitas Bandar Lampung
arnes@ieee.org

Lola Yustrisia
Fakultas Hukum Universitas Muhammadiyah Sumatera Barat
yustrisialola@gmail.com

Abstract

The use of blockchain applications in the health sector, in patient data security, promises significant progress in the management and protection of medical information. Database decentralization, which is at the heart of blockchain technology, presents itself as an innovative solution in reducing the risk of cyber attacks and system failures simultaneously, by dividing information into scattered networks. It increases patient information resilience to data loss and identity theft. Another advantage of blockchain is greater transparency and auditability. Any transactions or changes recorded cannot be changed again, ensuring consistent data integrity. This is crucial in a healthcare environment, where errors in patient information can have serious implications for patient care and health outcomes. In addition, the blockchain system allows the use of strong encryption and layered access controls, making patient data much safer from unauthorized access. However, despite the many advantages it offers, there are challenges to overcome in order for this technology to be implemented effectively. Challenges such as system scalability, complex regulatory compliance, and difficulty integrating with existing health information technology systems are major obstacles to blockchain implementation. Concerns about scalability emphasize increased processing time and operating costs as transaction volumes grow. Regulatory compliance often requires extra care and adaptation to strict local regulations relating to personal data and privacy.

Keywords: Blockchain, Patient Data Security, Potential and Challenges.

Introduction

In today's digital age, patient data is a vital asset in the healthcare industry. However, patient data security is often a serious issue given the risk of data leaks that can lead to misuse of information. Information technology in the health sector must be able to protect patient data effectively while facilitating access for authorities.

[1] Correspondence author

Patient data security is a fundamental principle and critical aspect in the healthcare industry, given the very personal and sensitive nature of data. A leak or misuse of patient information can have serious consequences, ranging from violations of individual privacy to negative impacts on health care outcomes. (Patil, H. K., & Seshadri, R. 2014). Furthermore, patient confidence in healthcare facilities and providers can be significantly compromised if their data integrity is not vigilant. This makes patient data security not only an ethical and privacy issue, but also an important component that affects the quality of health care, compliance with standards and regulations, and innovation in healthcare. (Van der Haak et al., 2003). Therefore, ensuring the security of patient data is the primary responsibility of all stakeholders in the health industry, and should be treated with comprehensive and systematic efforts to protect data from all types of cyber and physical threats. (Albisser et al., 2003).

So with that, technology plays an important role in protecting health information. Advances in information and communication technology have provided a variety of tools and systems to secure data, ranging from data encryption to two-factor authentication systems, all designed to enhance health information security. (Taitsman et al., 2013). Applications like Electronic Health Records (EHR) use advanced technology to not only store patient data but also protect it from unauthorized access. (Seymour et al., 2012). Blockchain technology, for example, offers revolutionary potential by making records unchangeable and completely transparent without compromising the confidentiality of patient data. Cyber security is also a crucial aspect, where solutions like firewalls, anti-viruses, and intrusion detection systems, proactively protect patient data from cyber attacks. This is where Blockchain technology offers potential solutions thanks to its ability to provide distributed, immutable, and transparent databases. (Rahardja, U. 2022).

Blockchain, originally developed as a technology behind digital currencies like Bitcoin, is now gaining attention as a solution to a variety of security issues, including in the health sector. Blockchain applications in the health sector are expected to offer a way to store patient data that is secure and easily accessible by authorities without fear of being altered or stolen. However, the application of blockchain in the healthcare industry is not without challenges. From a technical point of view, issues such as scalability, interoperability, and development costs are becoming stumbling blocks, while regulatory, there is a need for clarity about compliance with data privacy regulations such as GDPR in Europe or HIPAA in the United States. (Whitaker, A. 2019).

In addition, the use of Artificial Intelligence (AI) in security threat monitoring and detection enables real-time risk identification and mitigation. Technologies such as machine learning can analyze patterns and behaviour in traffic data that indicate potential interference or attack, allowing health institutions to take action before data leaks occur. (Jordan, M. I., & Mitchell, T. M. 2015). Similarly, the use of cloud technology in data storage offers scalability and flexibility, while providing strong data security protection through strict encryption and access policies. The success of the use of

technology in protecting health information depends heavily on the implementation of effective security policies and cybersecurity awareness among health stakeholders. (Anggeriana, H., Kom, S., & Kom, M. 2011).

From the background that has been outlined, there are some key issues to be addressed in this study, among them: the potential of Blockchain Technology, Challenges in Implementation, and Regulatory and Privacy Issues.

Identifying and exploring these issues is vital to understanding how blockchain technology can be safely and effectively integrated into health data management. The research aims to explore further the potential and challenges faced so that it can broaden the understanding and possibly provide useful recommendations for the implementation of this technology in the future.

Research Method

The method of literature research is a systematic approach to studying various written sources in order to gain an in-depth understanding of a subject. This process involves the search, collection, and analysis of literature relevant to research issues. (Champe & Kleist, 2003; Tharenou et al., 2007). In this method, researchers use relevant keywords to search for references through a variety of databases and information sources, which can include books, journal articles, conference proceedings, and other electronic documents. The use of reliable and relevant sources is critical in promoting the validity of research. (Basrowi, 2008).

In addition, literature studies focus not only on data collection, but also on understanding and interpreting information to produce a synthesis of new knowledge or a unique perspective on a research topic (Zed, 2004). Through literature analysis and Synthesis, researchers can identify gaps in existing knowledge, learn about the latest trends and developments, and direct research to relevant new questions. The primary objective of literary research methods is to build a strong theoretical foundation for research, ensure academic integrity, and determine the future direction of research. (Sugiyono, 2010; Ferdinand, 2014).

Result and Discussion

Blockchain Theory

Blockchain is a distributed and decentralized data storage technology. At the core of the blockchain, there is a 'block' concept that holds a set of transactions, and each of these blocks is connected to each other in a 'chain' using the principle of cryptography. (Ateniese et al., 2017). The unique thing about the blockchain is its blindness, where once a block of information is added, it is very difficult to change or delete. Each newly added block must be verified by a number of nodes (computers or servers that are part of the network) through a process called consensus, which ensures that all information within the network remains consistent and correct. (Aggarwal, S., & Kumar, N. 2021).

The basic principles of blockchain are based on transparency, decentralization, and security. Decentralization eliminates the need for third parties or central authorities to manage and verify transactions, increasing resistance to attack and manipulation. Security is accompanied by the use of complex cryptographic algorithms to ensure that each transaction is authentic and non-falsifiable. (Larrier, J. H. 2021). In addition, each network user or blockchain participant has a complete copy of the entire blockchain, which is updated in real time, ensuring transparency and unlimited access to the history of transactions that have been made. This allows an auditable and reliable track recording system without requiring trust between parties involved in the transaction. (Panda et al., 2020).

Blockchain technology was first introduced in 2008 in a whitepaper written by someone (or group) under the nickname Satoshi Nakamoto. This white paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" displays the design of a fully decentralized digital money system, requiring no central bank or single authority. It was designed to create a digital currency now known as Bitcoin. Blockchain becomes the core component that allows Bitcoin to function as a distributed network, relying on decentralized and encrypted big books to record transactions securely. Initially, blockchain and Bitcoin were often considered synonyms, but over time, the concept of blockchain has evolved far beyond initial applications in digital currencies. (Larrier, J. H. 2021).

The evolution of blockchain began to diversify as developers and researchers realized the wider potential of this technology beyond just cryptocurrencies. Ethereum, launched in 2015 by Vitalik Buterin and his team, is a significant example of the next stage of evolution, often referred to as blockchain 2.0. The platform introduces the concept of smart contracts, which allows the programming of business logic directly into the blockchain, which means transactions can be processed automatically when certain requirements are met. It opens up a wide range of opportunities, ranging from the creation of decentralized autonomous organizations (DAOs), tokenization of assets, to the development of a decentralised application. (dApps). With the emergence of Ethereum and similar platforms, blockchain has evolved from a system that merely records financial transactions into a distributed computing infrastructure that can transform industries and aspects of modern life. (Aggarwal, S., & Kumar, N. 2021).

Conclusions from the history and evolution of blockchain technology show how the concept originally developed to support the digital currency Bitcoin has evolved into a technological infrastructure that has a wide and diverse potential of influence. Starting with the work of Satoshi Nakamoto in 2008, blockchain was presented as a solution to the problem of trust in digital transactions without the need for a central authority. Further evolution, especially with the introduction of Ethereum and the concept of smart contracts, has expanded blockchain applications to a variety of sectors beyond cryptocurrency, including banking, supply chains, health, and more. With its nature of transparency, decentralization, and high security, blockchain offers

a new paradigm in the way we record, verify, and transfer assets and information, promising a technological revolution that can change the way economic systems work, data management, and social interaction in the future.

Blockchain's Potential in Patient Data Security

Transparency and Data Integrity

Transparency and data integrity are two important principles underlying a variety of information technologies, including blockchain. Transparency in the context of blockchain refers to the ability of each participant in the network to have access to the same transaction information, enabling verification and audit by all relevant parties. (Moore et al., 2007). It is very different from traditional systems where information is usually held and controlled by a centralized authority, making information more vulnerable to manipulation. In the blockchain, since every block of transactions is approved through consensus and locked cryptographically into the chain, the transparency of the data can be guaranteed, ensuring that no single entity can control or modify the data unilaterally. (Truong et al., 2019).

On the other hand, data integrity in the blockchain is guaranteed by the underlying structural design and cryptography. Any transaction added to the blockchain must be verified by the network through a process called mining or PoS consensus, depending on the specific mechanism of the blockchain. Once the transaction is verified, it is encrypted and cannot be changed or deleted, ensuring long-term data integrity (Moors, A. 2019). Furthermore, since each transaction block contains the hash (encrypted unique identification) of the previous block, any attempt to manipulate data will be easily detected, as it will require the alteration of the entire next blocks in the chain. These two principles, transparency and data integrity, collaborate in providing explicit security and trust in the blockchain system, making it an attractive solution for a variety of applications that require unchangeable data recording. (Geisler et al., 2021).

Controlled Access to Data

Safe patient data access mechanisms are one of the crucial applications of blockchain in the healthcare industry. The use of blockchain gives the ability to create a decentralized electronic medical record system, where data integrity, privacy, and accessibility can be managed more effectively. (Drexl, J. 2018). In a blockchain-based system, patient data can be stored in a block that is encrypted and distributed across the network, rather than in a central database. This minimizes the risk of data leaks and unauthorized access that is often a concern in traditional data storage systems. Any new transaction or medical record added to the blockchain must be verified through a network consensus to ensure the authenticity and accuracy of the data.

(Bertino et al., 2011). Patients can have a 'private key' that acts as an access mechanism, allowing only them or an authorized entity, such as a particular doctor or hospital, to access the relevant information. (Vayena, E., & Blasimme, A. 2017).

Furthermore, the implementation of smart contracts on the blockchain can facilitate consensus management and permission to access patient data automatically and transparently. Smart contracts can be programmed to ensure that data can only be accessed by parties who have obtained explicit consent from the patient, and only for specific purposes. This gives patients greater control over their information, while ensuring that compliance with data privacy regulations, such as the HIPAA (Health Insurance Portability and Accountability Act) in the United States or the GDPR (General Data Protection Regulation) in Europe, is met. (Act, A. 2023; Hoofnagle et al., 2019). Thus, blockchain offers a promising framework for creating a safer and more efficient health system, where trust and transparency form the basis of interaction between patients and healthcare providers.

Update and distribute data in real time

Blockchain has a unique ability to update and distribute patient data in real time and safely, thanks to its decentralized structure and consensus mechanisms. In a blockchain network, when a new transaction or medical record is added, it is immediately encrypted and distributed across nodes in the network. Consensus mechanisms used, such as Proof of Work (PoW) or Proof Of Stake (PoS), ensure that only valid and valid transactions by network participants can be added to the blockchain. (Kaul et al., 2012). This minimizes the risk of data manipulation and allows for rapid and transparent data updates among authorized stakeholders without the need for a mediator or a centralized data center. Thus, doctors and health facilities can have access to the most up-to-date patient information, enabling them to make more informative clinical decisions quickly. (Meunier, S. 2018).

Besides, everything is processed in a secure and encrypted environment, where every transaction is tracked and unchangeable, guaranteeing the accuracy and integrity of the data. This blockchain innovation enables the integration of previously separated and distributed health data across systems into a cohesive chronology, making it easier to manage the patient's health history. This combination of transparency, security, and efficiency transforms the way patient data is shared and managed, paving the way for a more coordinated and patient-oriented health system. (Klinger et al., 2017).

Thus, blockchain’s ability to update and distribute patient data in real time and safely offers a revolution in health data management. By leveraging this technology, the healthcare industry can an unprecedented level of data integrity, ensuring that patient information is protected, accurate, and always accessible by authorized entities. This not only strengthens confidence between patients and healthcare

providers but also improves the quality of healthcare itself, making the use of blockchain an important step towards a smarter and safer healthcare future.

Challenges in Blockchain Implementation

Scalability problem

The adoption of blockchain in health data management has great potential to significantly improve the overall health system performance. With its ability to provide decentralized, secure, and immutable data sources, blockchain simplifies and strengthens the exchange of health information between entities. It minimizes barriers to accessing information that often hampers rapid diagnosis and effective decision-making in medical care. (Koteska et al., 2017). For example, the transition from robust centralized data storage practices to blockchain-based systems allows healthcare facilities to eliminate information siloes, reduce the time and costs associated with the exchange of medical data between healthcare providers, and ultimately, speed up the patient's healing process by ensuring that treatment is given based on the most accurate and up-to-date information. (Meva, D. 2018).

Furthermore, the implementation of blockchain in the health system can increase the level of transparency and accountability, which is an important factor in increasing patient confidence. By giving patients greater control over their own data and the ability to easily verify who accesses their information, blockchain supports a more inclusive and participatory patient care model. This can encourage patients to be more actively involved in their own treatment processes, leading to better health outcomes (Gao et al., 2018). In addition, the reliability and security offered by the blockchain in the storage and exchange of medical data can reduce the incidence of data breaches, which is one of the biggest challenges facing the healthcare industry today, thereby improving operational efficiency and reducing security-related costs. (Memon et al., 2018).

Privacy and Compliance Issues

Blockchain presents an innovative approach to data management and exchange, but also raises significant questions regarding data privacy laws and regulations. Regulations such as the General Data Protection Regulation (GDPR) in the European Union give individuals control over their personal data and demand the right to be forgotten. (Protection, F. D. 2018). On the other hand, the permanent nature of the blockchain, where data once written cannot be altered or deleted, contradicts principles like this. Ensuring that the implementation of blockchain is consistent with the protection of privacy as required by law becomes a challenge (Holotescu, C. 2018).

Therefore, developers and users of blockchain technology in health systems should work carefully to understand and imply local and international legal frameworks, and may need to design applications that support data deletion, such as using references to data stored outside the chain or implementing pruners that proactively delete data on request.

Furthermore, in order to comply with privacy laws, the establishment of blockchain in the health system may require the development of more sophisticated systems capable of dealing with dynamic and complex privacy policies. For example, by leveraging smart contracts, blockchain can automatically enforce privacy regulations by restricting access to patient data based on previously agreed rules. (Akram et al., 2020). However, it requires rigorous system design and an in-depth understanding of data privacy laws. It requires continued dialogue between technology developers, policymakers, and authorities to ensure that blockchain can be implemented in a way that complies with existing regulations, while providing flexibility to accommodate new regulations that may arise as the data and technology privacy landscape changes. (Ahmed et al., 2019).

Overall, although the potential of blockchain in improving clinical data management and access is promising, there is still considerable scope for adapting this technology to current data privacy regulatory needs and demands. Preparedness to adapt and develop solutions that balance technological capabilities and legal demands will be key to ensuring the role of blockchain in a secure and reliable healthcare system of the future.

Infrastructure Fees and Technologies

The financial implications and technology infrastructure needs are two important aspects in considering the adoption of blockchain technology in the health sector. The cost of blockchain implementation varies significantly, depending on the scale and complexity of the desired system. (Nartey et al., 2021). The initial development of the blockchain system requires huge investments, not only in terms of the necessary hardware and software but also costs for staff training and integration of the system with existing technology. These costs can be a challenge for health facilities operating on a limited budget or for developing countries. (Khan et al., 2021). In addition, the maintenance and updating of the blockchain system to meet the latest security standards and user needs also leads to sustainable costs to be taken into account. Therefore, a comprehensive assessment of ROI (Return on Investment) and cost-benefit analysis are important steps before commitment of funds for blockchain implementation in the health system (Pandey, P., & Litoriya, R. 2020).

From an infrastructure point of view, the need for technology to implement blockchain in healthcare systems is not only limited to servers and adequate data storage capacity, but also includes a need for stable and fast network connectivity. (Bary et al., 2024). In this context, the existing IT infrastructure may need to be

upgraded or completely modified to ensure optimal system performance. This could include strengthening the cybersecurity system, given the critical role of blockchain in the storage and exchange of sensitive medical data. (De Novi et al., 2023). Adaptation to blockchain technology also requires healthcare institutions to have or access adequate technical expertise, both from internal resources and through partnerships with external blockchain solution providers. Since this technology is still new in many regions, finding talent with sufficient expertise can be a challenge in itself. Thus, the implementation of blockchain in the health sector requires mature planning and investment, not only in financial aspects but also in capacity development and supporting technology infrastructure. (Aripin, Z., & Paramarta, V. 2024).

Solution to Challenge

In reaching its full potential in the health sector, blockchain is heading towards perfection through supporting technology innovations that strengthen its capabilities and efficiency. One key area is increased scalability and transaction speed, which is overcome through the development of new, more efficient consensus protocols and techniques like sharding, which divides the blockchain into smaller parts to process transactions in parallel. (Koteska et al., 2017). In addition, the interconnection between the blockchain with artificial intelligence (AI) systems and the Internet of Things (IoT) allows for more sophisticated health data analysis and real-time patient monitoring, resulting in better clinical insights and more personalized treatment. Data security, being a central challenge to the health system, is continuously strengthened through more complex encryption algorithms and the use of technologies such as zero-knowledge proofs to allow transaction verification without revealing sensitive information. (Pandey, P., & Litoriya, R. 2020). Through this evolution, blockchain has not only become more technically suitable for health applications, but also more secure and capable of dealing with strict data privacy needs. This marks a significant step towards wider integration of blockchain within the health ecosystem, leading to improved operational efficiency and quality of patient care. (Politou et al., 2019).

Developing a legal framework that supports the implementation of blockchain in a variety of sectors, including health, finance, and commercial transactions, has become vital to ensuring the adoption of this technology runs effectively and responsibly. It involves creating regulations that can provide legal clarity for the developers and users of blockchain technology, while protecting individual rights and guaranteeing data security. Legislation designed should be flexible enough to accommodate rapid innovation in blockchain technologies, but must also be firm in setting standards for transparency, auditable, and ethical use of data. (Holotescu, V., & Vasiu, R. 2020). Strong monitoring mechanisms are needed to prevent the misuse of technology, including the use of blockchain for illegal activities. A mature legal framework should also address cross-jurisdictional issues, enabling the interoperability of blockchain systems that extend across national borders while

adhering to local regulatory variations. Global initiatives and intergovernmental collaboration will be key to creating consistent legal standards for blockchain, promoting its wider adoption whileining protection for all parties involved (Dorri et al., 2016).

Increasing awareness and knowledge about blockchain among health professionals is a critical step in optimizing the use of this technology in the health sector. Comprehensive and up-to-date education on the basic principles of blockchain, potential benefits, and the challenges of its application can strengthen the ability of these professionals to evaluate, adopt, and integrate blockchain solutions into their health practices. (Zafar et al., 2022). This increased awareness not only promotes more effective implementation thanks to a good understanding of the potential of technology but also helps in formulating policies and procedures that support the safe and ethical use of data. (Ismail, L., & Materwala, H. 2019). With in-depth knowledge, health professionals can be important intermediaries in educating patients about the benefits and limitations of this system, strengthening the relationship of trust between healthcare providers and patients. Furthermore, adequate blockchain literacy among these supports better cross-disciplinary collaboration in developing innovative solutions that focus on the patient, improving the quality of care and the efficiency of the overall health system. (Zafar et al., 2022).

Thus, the development of blockchain technology in the health sector, a supportive legal framework, and increased awareness among health professionals show that blockchain offers revolutionary potential to improve efficiency, transparency, and security in health data management. However, the full realization of this potential requires not only technical progress, but also the development of a solid legal framework that can support innovation, whileining the protection of individual rights and privacy. Moreover, efforts to raise awareness and knowledge about these technologies among health professionals are essential to ensuring successful adoption and effective integration of blockchain into the health system. With synergies between technological innovation, supportive regulation, and good education, blockchain has the potential to transform the health sector, leading to better care and more efficient and accessible health systems for all.

Conclusion

The use of blockchain technology in improving patient data security promises a revolution in health information governance, offering untouched potential for securing and facilitating access to health data. The key characteristics of blockchain, such as decentralization, transparency, and resilience to change, provide a solid foundation for addressing the problems that exist in traditional health data management systems. Decentralization eliminates single point of failure, strengthens data against cyber attacks and system damage. Blockchain also supports unchangeable and transparent

recording, enabling better audits and ensuring data integrity, which is crucial in managing health information.

However, this technology is not without challenges. One of the biggest challenges is scalability; with the increasing number of transactions and data stored in the system, blockchain can become slow and expensive to operate. This raises questions about the sustainability and operational efficiency of blockchain-based solutions on a large scale. Furthermore, the issue of regulatory compliance also stands as a major obstacle, due to differences in data protection standards across regions that can make it difficult to implement blockchain on widespread and fragmented health systems.

Integration with existing health information technology systems also shows significant challenges. Many health systems operate on outdated or highly specialized IT infrastructure, which makes the installation and integration of blockchain solutions a complex and expensive process. As a result, despite its huge potential, the practical adoption of blockchain in health data security faces significant technical and economic obstacles.

Assessing overall, while blockchain offers a potential revolutionary solution to some of the long-standing issues in patient data management and security, the full realization of this potential requires careful navigation towards technical, regulatory, and operational challenges. The success of blockchain implementation in the health sector will depend heavily on cooperation between technology developers, health service providers, governments, and regulators, as well as on the development of solutions that are not only technically sophisticated but also seamlessly integrated into complex and varied health ecosystems.

References

Act, A. (2023). Health insurance portability and accountability act. Public Law.

Aggarwal, S., & Kumar, N. (2021). History of blockchain-blockchain 1.0: Currency. In Advances in Computers (Vol. 121, pp. 147-169). Elsevier.

Ahmed, M., Elahi, I., Abrar, M., Aslam, U., Khalid, I., & Habib, M. A. (2019, July). Understanding blockchain: platforms, applications and implementation challenges. In Proceedings of the 3rd International Conference on Future Networks and Distributed Systems (pp. 1-8).

Akram, S. V., Malik, P. K., Singh, R., Anita, G., & Tanwar, S. (2020). Adoption of blockchain technology in various realms: Opportunities and challenges. Security and Privacy, 3(5), e109.

Albisser, A. M., Albisser, J. B., & Parker, L. (2003). Patient confidentiality, data security, and provider liabilities in diabetes management. Diabetes Technology & Therapeutics, 5(4), 631-640.

Anggeriana, H., Kom, S., & Kom, M. (2011). Cloud Computing. Jurnal Teknik Informatika, 1.

Aripin, Z., & Paramarta, V. (2024, February). BETWEEN INNOVATION AND CHALLENGES: UTILIZATION OF BLOCKCHAIN AND CLOUD PLATFORMS IN

THE TRANSFORMATION OF BANKING SERVICES IN THE DIGITAL ERA. In Journal of Jabar Economic Society Networking Forum (Vol. 1, No. 3, pp. 1-16).
Ateniese, G., Magri, B., Venturi, D., & Andrade, E. (2017, April). Redactable blockchain–or–rewriting history in bitcoin and friends. In 2017 IEEE European symposium on security and privacy (EuroS&P) (pp. 111-126). IEEE.
Bary, T. A. A. A. A., Elomda, B. M., & Hassan, H. A. (2024). Multiple Layer Public Blockchain Approach for Internet of Things (IoT) Systems (January 2024). IEEE Access.
Basrowi, S. (2008). Memahami penelitian kualitatif. Jakarta: Rineka Cipta, 12(1), 128–215.
Bertino, E., Ghinita, G., & Kamra, A. (2011). Access control for databases: Concepts and systems. Foundations and Trends® in Databases, 3(1–2), 1-148.
Champe, J., & Kleist, D. M. (2003). Live supervision: A review of the research. The Family Journal, 11(3), 268–275.
De Novi, G., Sofia, N., Vasiliu-Feltes, I., Zang, C. Y., & Ricotta, F. (2023). Blockchain Technology Predictions 2024: Transformations in Healthcare, Patient Identity, and Public Health. Blockchain in Healthcare Today, 6.
Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187.
Drexl, J. (2018). Data access and control in the era of connected devices. Report for BEUC.
Ferdinand, A. (2014). Metode Penelitian Manajemen: Pedoman Penelitian untuk Penulisan Skripsi Tesis dan Desrtasi Ilmu Manajemen.
Gao, W., Hatcher, W. G., & Yu, W. (2018, July). A survey of blockchain: Techniques, applications, and challenges. In 2018 27th international conference on computer communication and networks (ICCCN) (pp. 1-11). IEEE.
Geisler, S., Vidal, M. E., Cappiello, C., Lóscio, B. F., Gal, A., Jarke, M., ... & Rehof, J. (2021). Knowledge-driven data ecosystems toward data transparency. ACM Journal of Data and Information Quality (JDIQ), 14(1), 1-12.
Holotescu, C. (2018). Understanding blockchain opportunities and challenges. In Conference proceedings of» eLearning and Software for Education «(eLSE) (Vol. 14, No. 04, pp. 275-283). Carol I National Defence University Publishing House.
Holotescu, V., & Vasiu, R. (2020). Challenges and emerging solutions for public blockchains. BRAIN. Broad Research in Artificial Intelligence and Neuroscience, 11(1), 58-83.
Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. Information & Communications Technology Law, 28(1), 65-98.
Ismail, L., & Materwala, H. (2019). A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. Symmetry, 11(10), 1198.
Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. Science, 349(6245), 255-260.
Kaul, S., Yates, R., & Gruteser, M. (2012, March). Real-time status: How often should one update?. In 2012 Proceedings IEEE INFOCOM (pp. 2731-2735). IEEE.
Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic literature review of challenges in blockchain scalability. Applied Sciences, 11(20), 9372.

Klinger, B. A. R. T. Ł. O. M. I. E. J., & Szczepański, J. A. C. E. K. (2017). Blockchain-history, features and main areas of application. Man in Cyberspace, (1), 11-27.
Koteska, B., Karafiloski, E., & Mishev, A. (2017, September). Blockchain implementation quality challenges: a literature. In SQAMIA 2017: 6th workshop of software quality, analysis, monitoring, improvement, and applications (Vol. 11, p. 2017).
Koteska, B., Karafiloski, E., & Mishev, A. (2017, September). Blockchain implementation quality challenges: a literature. In SQAMIA 2017: 6th workshop of software quality, analysis, monitoring, improvement, and applications (Vol. 11, p. 2017).
Larrier, J. H. (2021). A brief history of blockchain. Transforming Scholarly Publishing With Blockchain Technologies and AI, 85-100.
Memon, M., Hussain, S. S., Bajwa, U. A., & Ikhlas, A. (2018, August). Blockchain beyond bitcoin: Blockchain technology challenges and real-world applications. In 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE) (pp. 29-34). IEEE.
Meunier, S. (2018). Blockchain 101: what is blockchain and how does this revolutionary technology work?. In Transforming climate finance and green investment with Blockchains (pp. 23-34). Academic Press.
Meva, D. (2018). Issues and challenges with blockchain: a survey. International Journal of Computer Sciences and Engineering, 6(12), 488-491.
Moore, N., Juillet, Y., & Bertoye, P. H. (2007). Integrity of scientific data: transparency of clinical trial data. Therapie, 62(3), 211-216.
Moors, A. (2019). The trouble with transparency: Reconnecting ethics, integrity, epistemology, and power. Ethnography, 20(2), 149-169.
Nartey, C., Tchao, E. T., Gadze, J. D., Keelson, E., Klogo, G. S., Kommey, B., & Diawuo, K. (2021). On blockchain and IoT integration platforms: current implementation challenges and future perspectives. Wireless Communications and Mobile Computing, 2021, 1-25.
Panda, S. K., Elngar, A. A., Balas, V. E., & Kayed, M. (Eds.). (2020). Bitcoin and blockchain: History and current applications. CRC Press.
Pandey, P., & Litoriya, R. (2020). Implementing healthcare services on a large scale: challenges and remedies based on blockchain technology. Health Policy and Technology, 9(1), 69-78.
Pandey, P., & Litoriya, R. (2020). Implementing healthcare services on a large scale: challenges and remedies based on blockchain technology. Health Policy and Technology, 9(1), 69-78.
Patil, H. K., & Seshadri, R. (2014, June). Big data security and privacy issues in healthcare. In *2014 IEEE international congress on big data* (pp. 762-765). IEEE.
Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. IEEE Transactions on Emerging Topics in Computing, 9(4), 1972-1986.
Protection, F. D. (2018). General data protection regulation (GDPR).
Rahardja, U. (2022). Skema Catatan Kesehatan menggunakan Teknologi Blockchain dalam Pendidikan. Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi, 1(1), 29-37.
Seymour, T., Frantsvog, D., & Graeber, T. (2012). Electronic health records (EHR). American Journal of Health Sciences (AJHS), 3(3), 201-210.

Sugiyono, S. (2010). Metode penelitian kuantitatif dan kualitatif dan R&D. Alfabeta Bandung.
Taitsman, J. K., Grimm, C. M., & Agrawal, S. (2013). Protecting patient privacy and data security. New England Journal of Medicine, 368(11), 977-979.
Tharenou, P., Donohue, R., & Cooper, B. (2007). Management research methods. Cambridge University Press.
Truong, D. D., Nguyen-Van, T., Nguyen, Q. B., Huy, N. H., Tran, T. A., Le, N. Q., & Nguyen-An, K. (2019, November). Blockchain-based open data: An approach for resolving data integrity and transparency. In International Conference on Future Data and Security Engineering (pp. 526-541). Cham: Springer International Publishing.
Van der Haak, M., Wolff, A. C., Brandner, R., Drings, P., Wannenmacher, M., & Wetter, T. (2003). Data security and protection in cross-institutional electronic patient records. International journal of medical informatics, 70(2-3), 117-130.
Vayena, E., & Blasimme, A. (2017). Biomedical big data: new models of control over access, use and governance. Journal of bioethical inquiry, 14, 501-513.
Whitaker, A. (2019). Art and blockchain: A primer, history, and taxonomy of blockchain use cases in the arts. Artivate, 8(2), 21-46.
Zafar, S., Bhatti, K. M., Shabbir, M., Hashmat, F., & Akbar, A. H. (2022). Integration of blockchain and Internet of Things: Challenges and solutions. Annals of Telecommunications, 77(1), 13-32.
Zed, M. (2004). Metode peneletian kepustakaan. Yayasan Obor Indonesia.