Vesna Scepanovic, Ivan Scepanovic (2024). The Ethical Dilemmas of the Blockchain Technology Use in e- Healthcare Systems. Systems. Social Informatics Journal, 3(2), 09-14.

UDC: 004.75:614.2
https://doi.org/10.58898/sij.v3i2.09-14

THE ETHICAL DILEMMAS OF THE BLOCKCHAIN TECHNOLOGY USE IN e-HEALTCARE SYSTEMS

Vesna Scepanovic[1*], Ivan Scepanovic[1]
[1] College of Academic Studies "Dositej", Belgrade, Serbia
e-mail: vesna.scepanovic.ns@gmail.com ivan.b.scepanovic@gmail.com

Abstract: Blockchain technology is increasingly being recognized as a game-changer in healthcare, offering solutions for improved data security, transparency, and interoperability. However, its integration into healthcare systems brings with it a range of ethical challenges that need to be addressed. This paper delves into some of the most pressing issues, such as protecting patient privacy, defining data ownership, obtaining informed consent, and ensuring equitable access. It explores the delicate balance between the transparency that blockchain provides and the potential risks of exposing sensitive health information. The paper also considers the ethical concerns surrounding decentralized governance and the possibility of deepening inequalities due to the digital divide. By addressing these dilemmas, the goal is to offer a thoughtful analysis that can guide policymakers, healthcare professionals, and technologists in leveraging blockchain's potential while upholding ethical principles in healthcare.

Keywords: Blockchain Technology, Healthcare Ethics, Patient Privacy, Data Ownership, Decentralized Governance

Introduction

Blockchain technology has established itself as a disruptive innovation in many sectors in recent years, including healthcare. Due to its ability to provide security, transparency, and decentralized data management, blockchain has the potential to significantly improve various aspects of the healthcare sector. Electronic health records (EHRs), the exchange of medical information, and the authentication of medical licenses are just a few of the aspects of healthcare where blockchain can play an important role. However, while blockchain can bring many benefits, its application in the healthcare sector also raises a number of ethical dilemmas that require careful analysis. This paper aims to explore and analyze the ethical dilemmas of the use of blockchain technology in e-health. The aim of this paper is to explore the basic characteristics of blockchain technology in the context of the health sector, to analyze ethical dilemmas that arise during the application of blockchain technology in e-health, to analyze and systematize literature sources that deal with ethical challenges related to blockchain and e-health, to consider and propose possible potential solutions or guidelines for resolving ethical issues.

We will use the method of systematic literature review, analyzing scientific papers, articles and sources dealing with blockchain technology and its impact on the healthcare sector. The analysis will also include case studies from countries that have implemented blockchain in healthcare, in order to gain insight into practical aspects and ethical implications.

Key features of blockchain technology in the context of the healthcare sector

Blockchain technology provides high security and transparency, making it suitable for medical data management. Patients' medical records can be stored securely, and access to data can be tightly controlled with the ability to track who, when, and under what conditions are using the data. Also, blockchain allows decentralization, which means that no single institution has complete control over the data, while all participants in the chain have insight into the changes. The application of blockchain in healthcare is accompanied by a number of not only technical but also ethical challenges, including data security and privacy, accountability, decentralization, accessibility, digital inequality, interoperability,

efficiency and cost reduction. One of the main ethical issues related to blockchain in e-health relates to data privacy, i.e. to protect the privacy of patients. Health data is extremely sensitive, and blockchain technology, while providing a high level of security, allows for data irreversibility. Once recorded on the blockchain, the data cannot be deleted or changed, which can cause problems if the patient wants to withdraw consent to the use of their information. The decentralized nature of blockchain can make it difficult to remove or anonymize data, which goes against the "right to be forgotten" and the principles of the EU's General Data Protection Regulation (GDPR). These ethical challenges can create tension between technological innovation and patients' right to control their data.

Although blockchain allows for pseudonymity – whereby the identity of the patient is not directly revealed – the data can still be linked to individuals through other information or metadata. This possibility of identification can compromise the anonymity of patients, especially if there are security flaws or intrusions into the system. The ethical challenge lies in finding a balance between transparency and protecting patient privacy. While blockchain promotes the openness and accessibility of data, patients' personal information must be protected. Private blockchain networks, or the use of off-chain systems to store sensitive information, can be the solution to these problems. Blockchain offers a high level of security thanks to cryptography and the inability to change records. Medical data is sensitive and susceptible to misuse, and it is a key ethical and legal obligation for healthcare institutions to adequately protect it. Blockchain allows data to be encrypted, which ensures that only authorized individuals have access to the information.

Although blockchain is known for its high degree of security, as it provides mechanisms to resist manipulation and data loss, security aspects in the context of health data pose additional ethical dilemmas. Blockchain allows for immutability of records, but this can become problematic when changes or corrections to health data are required due to medical errors or changes in diagnoses (Chen et al., 2019). The irreversibility of blockchain data can have serious consequences on patients' health, raising questions about the responsibility and ethical obligations of healthcare professionals regarding the accuracy of the information entered. Additionally, while blockchain can reduce the risk of unauthorized access to data, cyberattacks still pose a real threat. If attackers manage to compromise the systems used to access the blockchain network, the potential damage can be far-reaching. This ethical dilemma points to the need for continuous improvement of cybersecurity and privacy protection in the context of blockchain applications in e-health (Angraal et al., 2017).

Stakeholders in the application of blockchain technology in e-health

The successful implementation of blockchain technology in e-health depends on the engagement of various stakeholders, including patients, healthcare professionals, regulators, and technology companies. This chapter will analyze key stakeholders, their interests and challenges in the application of blockchain technology in e-health. Patients are one of the most important actors in e-health. Their trust in the system and willingness to share their health data directly affects the success of the implementation of blockchain solutions. Blockchain allows patients to have control over their data, including the right to grant or deny access to that data to healthcare professionals (Kuo et al., 2017). This capability can increase patients' levels of trust in e-health, but at the same time creates a challenge in educating patients about the technology and its benefits. Healthcare professionals, including doctors, nurses and administrative staff, are a key group in e-health. They are responsible for providing services and managing patient data. Blockchain can improve efficiency and accuracy in the exchange of information between healthcare professionals, but it faces challenges such as resistance to change and the need for training. Healthcare workers need to be confident that new technology will make their job easier, not more difficult. Regulatory institutions play a key role in shaping the legal framework for the use of blockchain

technology in e-health. Their task is to ensure that all aspects of the use of technology comply with applicable laws and regulations, especially with regard to data privacy protection (Dagher et al., 2018). The role of regulation is particularly important in the context of blockchain, which can provide a high level of transparency and accountability, but also requires clearly defined guidelines on how data is collected, used, and stored. The regulator's decisions have a direct impact on the ability of healthcare organizations to implement blockchain solutions**.** Technology companies are key partners in the development and implementation of blockchain solutions in e-health. They provide the necessary technology, infrastructure and expertise. Collaboration between technology companies and healthcare organizations can result in innovative solutions that meet the specific needs of healthcare systems. However, the challenge lies in finding a balance between commercial interests and ethical standards, especially when it comes to sensitive patient data. The community and accrediting organizations also play a significant role in the implementation of blockchain technology in e-health. These organizations can contribute to the creation of standards and guidelines for the ethical use of technology, as well as to educating patients and healthcare professionals about its benefits and risks. Engaging social organizations can improve public trust in blockchain solutions and ensure that the interests of all stakeholders are taken into account when developing and implementing the technology.

Key Aspects of Blockchain Technology

One of the key aspects of blockchain technology is decentralization. Traditionally, health data has been stored centrally, making it vulnerable to attacks or database management errors. Blockchain allows data to be distributed across a network of computers (nodes), eliminating the need for a central authority. Each node in the network has an identical record of transactions, which reduces the possibility of data manipulation and increases the system's resilience to cyberattacks (Yue et al., 2016). Transparency is another important aspect of blockchain. All transactions within the blockchain network are recorded in an immutable manner and available to all participants in the network. This feature is particularly useful in the healthcare sector, as it allows for a secure and transparent exchange of data between different healthcare facilities, patients, and healthcare providers (Agbo et al., 2019). Patients can also monitor how their data is being used and who is accessing it, which increases trust in the system. Blockchain technology decentralizes accountability in the management of health data, which can raise ethical dilemmas regarding accountability. In traditional systems, there are clearly defined responsible institutions, while in a blockchain system, there is no central authority. This can make it difficult to identify the responsible entity in the event of a policy breach or misuse of data (Mettler, 2016). Blockchain technology can increase digital inequality among different patient groups, especially in regions where internet access and technological literacy are underdeveloped. These inequalities can prevent equal access to digital health services (Zheng et al., 2018). The ethics of using blockchain in healthcare requires careful consideration to ensure equitable accessibility and inclusiveness. One of the long-standing problems of the healthcare sector is interoperability – the ability of different systems and institutions to efficiently exchange and use data. Given that health data is often found in different systems and formats, its integration is challenging. Blockchain can provide a standardized way of exchanging information between various entities, such as hospitals, laboratories, pharmaceutical companies, and insurance companies (Zheng et al., 2018). The efficiency of the healthcare system can also be increased through the use of smart contracts, which enable the automatic execution of predefined conditions and actions. For example, smart contracts can automate the processes of reimbursement, dispensing medicines, or processing laboratory results, thereby reducing administrative burden and increasing the speed of services (Zhang et al., 2018). One of the potentially most important aspects of blockchain technology in the healthcare sector is cost reduction. Healthcare is a sector that spends a lot of resources on administration, data processing and compliance with regulatory standards. Blockchain, with its ability to automate many processes and reduce intermediaries, can significantly reduce data management and administration costs (Agbo et al., 2019).

In addition, blockchain can help prevent fraud in the healthcare system. For example, pharmaceutical companies can use blockchain to track drugs in the supply chain, thereby reducing the possibility of drug counterfeiting and guaranteeing product authenticity (Tandon et al., 2020). While blockchain offers significant advantages, its implementation in the healthcare sector is not without its challenges. First of all, there are technical and regulatory challenges, including compliance with legislation, the need for high technical standards, and the adaptation of existing systems to blockchain infrastructure. Also, ethical challenges include issues of privacy, liability, and the possibility of misuse of technology (Jiang et al., 2018). One of the ethical aspects is the issue of accessibility. While blockchain can improve many aspects of the healthcare system, its complexity and infrastructure requirements may limit its implementation in countries with lower levels of development.

Deontological analysis of the application of blockchain technology in e-health

Blockchain technology has become an important factor in the development of modern healthcare systems, especially in terms of data security, decentralization, and transparency. The use of blockchain in e-health raises a number of ethical dilemmas, which can be analyzed through different approaches to ethics. Deontology, as an ethical theory that focuses on moral obligations, rules, and principles, offers a unique perspective for considering the responsibilities and duties associated with the use of blockchain in healthcare. In this chapter, we analyze the deontological approach to the application of blockchain technology in e-health, with a special focus on issues of privacy, transparency, and accountability.

Deontological ethics, most developed by Immanuel Kant, focuses on moral duties and obligations to be followed, regardless of the consequences. According to this theory, certain actions are inherently right or wrong, and moral norms are universal and applicable to all people. In the context of health systems, the deontological approach places a strong emphasis on respect for patients' rights, privacy protection, and accountability in data processing (Shae & Tsai, 2017). One of the key deontological issues regarding blockchain technology in healthcare is the issue of patient privacy. Blockchain allows data to be stored and distributed securely, but its inherent transparency can raise ethical dilemmas. According to the deontological approach, it is the duty of healthcare professionals and organizations to protect patients' confidential information, as privacy is a basic moral right that must be respected regardless of the benefits that transparency may bring (Roehrs et al., 2017). In this context, blockchain technology offers solutions through data encryption and decentralization of control, but the challenge remains in balancing the transparency of the system and patients' right to privacy. Deontologically speaking, respect for privacy should be an absolute obligation, and all technical systems, including blockchain, must be designed to protect patients' rights without compromise. Blockchain is often promoted as a technology that enhances transparency, as it allows all users to access the history of transactions and changes in data. While transparency can contribute to better control and reduce corruption in health systems, deontological analysis requires deeper consideration. According to Kant, accountability for actions must be related to respect for moral principles, and not only to public control. This means that even when transparency is technologically possible, it must not compromise moral obligations to patients, such as the obligation of confidentiality (Azaria et al., 2016). Deontologically speaking, blockchain must be implemented in such a way that the responsibility of healthcare professionals and organizations to patients remains intact. For example, smart contracts, which automate processes on blockchain networks, must be programmed in accordance with ethical standards and the duties of healthcare professionals. These technologies must not replace human responsibility, but must support and strengthen it through respect for moral rules. Decentralization is one of the key attributes of blockchain technology, which allows for the distribution of control over data among network users. From the point of view of deontological ethics, decentralization carries significant ethical value, as it enables patient independence and reduces the risk of misuse of data by centralized institutions. However,

decentralization also raises the question of responsibility — who bears responsibility when something goes wrong? Deontologically, the responsibility for respecting patients' rights still lies with healthcare professionals and institutions, even when data is distributed through a decentralized blockchain network. This moral principle means that decentralization cannot be an excuse for a loss of responsibility or neglect of obligations to patients (Kuo et al., 2019). Decentralized networks must be designed to clearly define who is responsible for data protection and the enforcement of ethical standards. One of the most important features of blockchain is the immutability of data — once data is entered on the blockchain, it cannot be changed or deleted. This feature can be useful in ensuring data integrity, but it can pose an ethical concern when it comes to outdated or inaccurate medical information. According to the deontological approach, healthcare organizations have a moral obligation to ensure that patients have the right to correct or delete inaccurate information (Zyskind & Nathan, 2015). Blockchain technology must be developed in a way that allows data to be updated and corrected, while preserving the immutability of records to ensure accountability and integrity. This balance between immutability and patients' right to correction must be based on moral obligations, not just technical limitations.

Conclusions

Blockchain technology offers revolutionary opportunities to improve the healthcare sector, especially in terms of decentralization, security, efficiency, and cost reduction. However, there are challenges that need to be addressed, including issues of privacy, regulation, and ethical implications. Stakeholders in the application of blockchain technology in e-health play a key role in shaping its success. Collaboration between patients, healthcare professionals, regulators, technology companies, and the community can enable the creation of sustainable and ethically acceptable solutions. As blockchain continues to evolve, it is imperative to identify and address the interests and challenges of all stakeholders in order to achieve successful implementation and benefit for the entire healthcare system. The healthcare sector must carefully consider how to make the most of this technology, while ensuring that its benefits are implemented in a way that protects patients and their data. The effective implementation of blockchain solutions in e-health requires the alignment of the interests of all stakeholders in order to achieve an optimal balance between individual benefits and the wider societal good. Ethical regulations and technological solutions must be adapted so that blockchain can fully respect and protect the moral rights of individuals in the healthcare sector. These dilemmas require careful consideration and development of ethical and legal frameworks to ensure that blockchain technology benefits patients without compromising their rights and safety. The future of blockchain in healthcare will depend on how these ethical dilemmas are addressed in practice. A deontological analysis of the application of blockchain technology in e-health reveals a number of moral duties that healthcare professionals and organizations must uphold. The duty to protect privacy, the responsibility for transparency and decentralization, as well as the right of patients to rectify data, are key aspects that blockchain technology must respect in order to be ethically justified. The deontological approach requires that blockchain be implemented in accordance with moral principles, where patients' rights remain at the center of any technological solution.

Conflict of interests

The authors declare no conflict of interest.

References

Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain technology: applications in health care. Circulation: Cardiovascular quality and outcomes, 10(9), e003800.

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019, April). Blockchain technology in healthcare: a systematic review. In Healthcare (Vol. 7, No. 2, p. 56). MDPI.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. In 2016 2nd international conference on open and big data (OBD) (pp. 25-30). IEEE.

Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework. Journal of medical systems, 43, 1-9.

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable cities and society, 39, 283-297.

European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, -, 24 October 1995, https://www.refworld.org/legal/reglegislation/eu/1995/en/13712 [accessed 08 December 2024]

Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., & He, J. (2018, June). Blochie: a blockchain-based platform for healthcare information exchange. In 2018 ieee international conference on smart computing (smartcomp) (pp. 49-56). IEEE.

Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220.

Mettler, M. (2016, September). Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom) (pp. 1-3). IEEE.

Rachels, J., & Rachels, S. (2012). The elements of moral philosophy 7e. McGraw Hill.

Roehrs, A., Da Costa, C.A., & da Rosa Righi, R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. Journal of biomedical informatics, 71, 70-81.

Roehrs, A., Da Costa, C.A., da Rosa Righi, R., & De Oliveira, K.S.F. (2017). Personal health records: a systematic literature review. Journal of medical Internet research, 19(1), e5876.

Shae, Z., & Tsai, J. J. (2017, June). On the design of a blockchain platform for clinical trial and precision medicine. In 2017 IEEE 37th international conference on distributed computing systems (ICDCS) (pp. 1972-1980). IEEE.

Tandon, A., Dhir, A., Islam, A. N., & Mäntymäki, M. (2020). Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Computers in Industry, 122, 103290.

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems, 40, 1-8.

Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare. In Advances in computers (Vol. 111, pp. 1-41). Elsevier.

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: applying blockchain to securely and scalably share clinical data. Computational and structural biotechnology journal, 16, 267-278.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International journal of web and grid services, 14(4), 352-375.

Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE security and privacy workshops (pp. 180-184). IEEE.