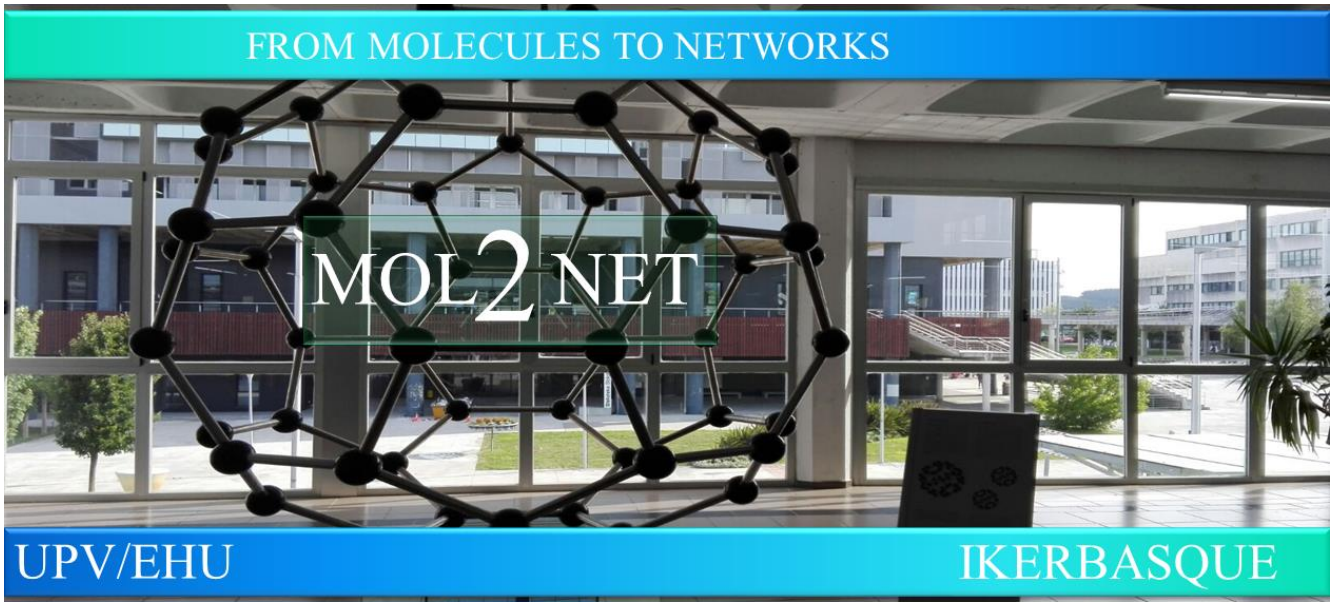
MDPI sciforum

MOL2NET'23, Conference on Molecular, Biomedical, Computational, & Network Science and Engineering, 9th ed.



Blockchain Technology in Healthcare: A Possible Disruption Under the Scope of Privacy

Rabaï Bouderhem[a]

[a] *College of Law, Prince Mohammad Bin Fahd University, P.O. Box 1664, Al Khobar 31952, Saudi Arabia*

Graphical Abstract	**Abstract:** *This paper is based on a research literature review for identifying the challenges posed by the use of blockchain technology in healthcare under the scope of the right to privacy and the protection of personal health information (PHI). The objective of this study is to analyze how research can help healthcare providers implement effective and compliant solutions based on blockchain technology. Many ethical and regulatory challenges are still unsolved such as data privacy, performance, scalability or security. Public authorities – still trying to understand blockchain technology and its benefits – are today in a 'wait and see'*

position: few compulsory regulations cover specifically the use of blockchain technology. As a consequence, actors involved in blockchain technology are facing legal and regulatory uncertainty. Therefore, it is a necessity to adopt specific laws related to the implementation of blockchain technology in healthcare. European Union (EU) law – General Data Protection Regulation (GDPR) and the upcoming EU Data Act – could serve as a law model.

Keywords: Blockchain; data protection; ethics; GDPR; healthcare; privacy.

1. Introduction

Blockchain is a relatively new technology based on decentralization which could potentially [1] disrupt and provide significant improvements to the handling of health data and rethink the healthcare industry [2] with disruptive solutions [3] and new ways to access and own healthcare data [4]. Short-term effects could be a simplification of healthcare back-office services and better supply chain traceability [5]. Blockchain technology is built on transparency and decentralization. Blockchain technology in healthcare promises to provide consistency; also, decentralized networks are ownable and append-only [6]. Users and participants in a blockchain cannot modify preexisting data which improves significantly traceability and facilitates audit [7]. Blockchain technology allows healthcare providers to control data and decide on who can access it [8] although many challenges [9] seem insoluble today. Indeed, data breaches, high costs from both a medical and administrative perspective, malpractice and negligence, management issues are intrinsic limitations to healthcare systems. Blockchain technology can offer real value for the healthcare industry by solving some of these challenges especially fraud, 'compliance' [10], 'interoperability' [11], and data protection [12], and also enable new models focused on a patient centered-approach [13]. However, new regulations have to be adopted at both national and international level for addressing adequately all concerns raised by the use of blockchain technology in healthcare.

2. The deployment of blockchain technology in healthcare: limitations due to unsolved challenges

Blockchain's usefulness can be overstated [14]. As noted by Agbo et al. [15], '*Healthcare is one industry in which blockchain is expected to have significant impacts. Research in this area is relatively new but growing rapidly; so, health informatics researchers and practitioners are always struggling to keep pace with research progress in this area*.' Deployment of blockchain technology in health is still in its infancy [16] as many challenges (see Table 1 below) are to be solved. Blockchain is facing issues relating to big data volume as a blockchain has to be constantly replicated [17]. As noted by Taloba et al. [18], '*managing large amounts of data, including findings and images of each individual, increases human effort and increases protection risks*.' Also, according to Bansod et al. [19], '[T]*he Blockchain solutions are subject to certain limitations like scalability, response times, security threats and privacy issues which affect user identity, confidentiality and transparency on the ledger*.' In addition, OECD [20] pointed out that '*storing personal health data 'on chain' and thus, by definition, visible to other network participants, is a data privacy infringement. Rights under the EU General Data Protection Regulation, particularly the right to erasure, are incompatible with the immutability of blocks in a chain*.' In its Recommendation [21], the OECD Council on

Health Data Governance considers that the use of blockchain technology in healthcare should be done following four fundamental elements: '*fitness of the technology for the use to which it will be applied; alignment with laws and regulations; incremental adoption to allow time for evaluation; and a training and communications plan'*. The scalability [22] and performance of blockchain systems, especially for large-scale and complex applications is a major concern and challenge to tackle. Blockchain systems face some trade-offs between security, decentralization, and efficiency. For example, increasing the number of nodes in the network may enhance security [23] and resilience, but also increase latency and resource consumption. Similarly, using more complex encryption or consensus algorithms may improve security and reliability, but also reduce throughput and speed. Therefore, organizations using blockchain technology need to carefully evaluate their requirements and expectations for their applications, as well as to explore alternative or complementary solutions, such as off-chain processing, sidechains, sharding [24], or layer 2 protocols.

Table 1. Challenges posed by blockchain technology in healthcare

Main challenges posed by blockchain technology
1. Data privacy
2. Data collection and storage
3. Data quality and accuracy
4. Scalability
5. Performance/efficiency
6. Health equity
7. Access to technology in developing countries
8. Lack of regulations at both national and international level
9. Ability to control third parties' access to personal health data
10. Security
11. Speed/Latency/resource consumption
12. Decentralization

3. Blockchain technology in healthcare: the insoluble dilemma of privacy

There are several laws and regulations around the world that aim to protect the privacy of health data. One of the most important regulations is the EU GDPR [25] which has been adopted by European authorities in 2016 with an entry into force in 2018. Under the GDPR, data privacy is now a fundamental human right; also, service providers cannot collect and process data without legal basis. The GDPR enshrines health data as a specific category of information which requires adequate consideration and protection. This regulation has inspired new laws in many other countries and US states. In the US, at both federal and state level, new regulations govern the privacy, security, and exchange of healthcare information. As an illustration, the Children's Online Privacy Protection Act (COPPA) [26] governs data collection about minors. Another example is the California Consumer Privacy Act (CCPA) of 2018 which regulates how service providers can collect and process consumers' data. Such laws grant individuals certain rights over their personal data: the objective is to give more control to users or consumers with the possibility to request modification, rectification or suppression of personal data, or to object or withdraw consent for processing their data. However, these rights may conflict with some of the features of blockchain technology, such as immutability, transparency, pseudonymity, or cross-border data transfer. Therefore, organizations using blockchain technology need to carefully assess the legal implications and risks of their applications, as well as to adopt appropriate mitigation strategies, such as anonymization, encryption,

governance frameworks, or technical solutions. Data privacy is certainly the biggest challenge when implementing blockchain technology in healthcare [27]. One of the most important features of blockchain is related to security and decentralization. However, this may raise concerns about data protection and confidentiality for patients. Medical secret necessitates constant protection and privacy [28]. In the absence of specific laws and regulations, blockchain technology in healthcare may face insoluble issues as key data protection regulations are applicable. In the US, both federal and state privacy and security laws could limit the deployment of blockchain technology to the health care sector especially the Health Insurance Portability and Accountability Act (HIPAA) 1996 [29], the Health Information Technology for Economic and Clinical Health Act [30] and their regulations, including the privacy and security rule (HIPAA), as well as under international privacy and security laws, particularly the GDPR. The HIPAA 1996 aims to protect health data privacy and ensure its security [31]. On the one hand, the HIPAA Privacy Rule introduced federal standards related to the protection of PHI; on the other hand, the HIPAA Security Rule created federal standards applicable to the protection, processing and storing of digital data. Compliance with the GDPR is an incredible challenge for service providers and has to be taken into consideration when implementing blockchain technology in healthcare [32]. Both HIPAA and GDPR aim to protect the privacy of individuals' health information. Here, a balance is necessary to be observed as service providers need to process data and allow for adequate treatment and healthcare. Healthcare professionals have to handle the correct amount of health data when providing treatment or medication. However, there are differences in their scope, applicability, and enforcement mechanisms. It is important for organizations handling health data to be aware of and comply with the relevant regulations in their jurisdiction.

The World Health Organization (WHO) Regional Office for Europe released a guidance document for European countries on how they can improve their respective legal frameworks and arsenals to ensure adequate protection for health data [33]. In this guidance document, the WHO Regional Office for Europe stresses out the importance of patients' data privacy. The guidance document develops a '*useful set of principles for data protection and privacy in health systems which applies to all forms of telemedicine and mobile health (mHealth)*' [34]. As stated, the main issue is to ensure the confidentiality of health data and compliance with key regulations such as the GDPR.

4. How can we ensure data protection with blockchain technology?

Data privacy is a major concern in the digital age. However, blockchain technology offers some potential solutions to ensure data privacy (see Table 2 below).

Table 2. Potential solutions to ensure health data privacy

Potential solutions to ensure health data privacy
1. Using encryption and hashing techniques to protect the data from unauthorized access and modification
2. Using decentralized and distributed networks to store and share the data
3. Using smart contracts and decentralized identity mechanisms to control the data access and usage
4. Educate healthcare personnel
5. Conduct routine risk assessment
6. Restrict access to data
7. Implement role-based access
8. Two-factor authentication

9. Security awareness training

Education and training is an absolute necessity as most data breaches are attributable to human errors [35]. Risk assessment on a daily basis should also be a requirement [36] as it will help identify intrinsic limitations. Healthcare providers need to limit and restrict access to patients' PHI access to certified personnel [37]. Authentication processes such as two-factor authentication should become the norm in the field of healthcare. Healthcare providers should implement role-based access control systems [38]; employees should only have access to a specific assigned system-level.

The HIPAA [39] regulates health data and ensures its security and confidentiality. All data collected, processed and shared in the US must be protected and secured at all times [40]. Data privacy could be achieved through the adoption of international standards for the use of blockchain technology in healthcare for instance [41]. Compliance with health data privacy requires built-on security features, and additional guarantees that the network is safe as well as third party applications. Transparency [42] is another key aspect as users should know who can access their data, whether it is a third party or the healthcare provider itself. The US legal framework applicable to health data and its handling presents a few legal voids as blockchain technology has still to be regulated. HIPAA only targets specifically health data and not the technology used to process data.

EU law can serve as a guidance as it offers a detailed legal framework applicable to privacy and data protection. Indeed, the GDPR [43] is an essential regulation which imposes stringent obligations on service providers handling data in a broad manner [44]. Moreover, the European Union Commission recently made a proposal [45] for a EU Data Act for adequate regulation of data specifically processed, stored or shared by service providers, including healthcare providers. In June 2023, the Council presidency and the European parliament came to a consensus and adopted the EU Data Act as a provisional agreement [46]. The EU Data Act will harmonize rules relating to a fair access to data and its use by public and private actors.

5. Conclusions

As noted by Singh et al. [47], '*[T]he existing privacy-preserving mechanisms are not sufficient for full proof security of healthcare data*.' Blockchain technology has the potential to improve existing healthcare systems but many challenges need to be addressed by all stakeholders involved in the process. Researchers and companies need to develop adequate solutions complying with data protections laws such as the GDPR. As discussed, EU law could inspire states and international organizations such as the WHO to adopt new guidelines in the field of blockchain technology for more legal security and predictability.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.
Data Availability Statement: Publicly available data.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management, 15(1), 70-83; Taherdoost, H. The Role of Blockchain in Medical Data Sharing. *Cryptography* **2023**, *7*, 36. https://doi.org/10.3390/cryptography7030036.
2. Merlo, V., Pio, G., Giusto, F., & Bilancia, M. (2022). On the exploitation of the blockchain technology in the healthcare sector: A systematic review. *Expert Systems with Applications*, 118897.

3. Kucukaltan, B., Kamasak, R., Yalcinkaya, B., & Irani, Z. (2022). Investigating the themes in supply chain finance: the emergence of blockchain as a disruptive technology. *International journal of production research*, 1-20.
4. Singh, S., Sharma, S. K., Mehrotra, P., Bhatt, P., & Kaurav, M. (2022). Blockchain technology for efficient data management in healthcare system: Opportunity, challenges and future perspectives. Materials Today: Proceedings, 62, 5042-5046.
5. Tarun Kumar Agrawal, Vijay Kumar, Rudrajeet Pal, Lichuan Wang, Yan Chen, Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry, Computers & Industrial Engineering, Volume 154, 2021, 107130, ISSN 0360-8352, https://doi.org/10.1016/j.cie.2021.107130.
6. Przytarski, D.; Stach, C.; Gritti, C.; Mitschang, B. Query Processing in Blockchain Systems: Current State and Future Challenges. Future Internet 2022, 14, 1. https://doi.org/10.3390/fi14010001.
7. Zhuang, Y., Zhang, L., Gao, X., Shae, Z. Y., Tsai, J. J., Li, P., & Shyu, C. R. (2022). Re-Engineering a clinical trial management system using blockchain technology: system design, development, and case studies. Journal of Medical Internet Research, 24(6), e36774.
8. Ali, O., Jaradat, A., Ally, M., & Rotabi, S. (2022). Blockchain technology enables healthcare data management and accessibility. Blockchain Technologies for Sustainability, 91-118.
9. Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. *International Journal of Healthcare Management*, *15*(1), 70-83.
10. Roy, R., & Pillai, S. (2022, November). Intelligent Decision Making with Block chain in healthcare industry. In 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC) (pp. 131-135). IEEE.
11. Schmeelk, S., Kanabar, M., Peterson, K., & Pathak, J. (2022). Electronic health records and blockchain interoperability requirements: a scoping review. *JAMIA open*, *5*(3), ooac068.
12. Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: security issues, healthcare applications, challenges and future trends. Electronics, 12(3), 546.
13. Aldamaeen, O., Rashideh, W., & Obidallah, W. J. (2023). Toward Patient-Centric Healthcare Systems: Key Requirements and Framework for Personal Health Records Based on Blockchain Technology. Applied Sciences, 13(13), 7697.
14. Jaiswal, H., Misra, A., & Misra, P. K. Health Record Management System Using Block chain Technologies.
15. Agbo CC, Mahmoud QH, Eklund JM. Blockchain Technology in Healthcare: A Systematic Review. Healthcare (Basel). 2019 Apr 4;7(2):56. doi: 10.3390/healthcare7020056. PMID: 30987333; PMCID: PMC6627742.
16. A. Thakur, A Comprehensive Study of the Trends and Analysis of Distributed Ledger Technology and Blockchain Technology in the Healthcare Industry, Frontiers in Blockchain, VOLUME 5, https://www.frontiersin.org/articles/10.3389/fbloc.2022.844834, DOI=10.3389/fbloc.2022.844834.
17. Alruwaill, M. N., Mohanty, S. P., & Kougianos, E. (2023, June). hChain: Blockchain Based Healthcare Data Sharing with Enhanced Security and Privacy Location-Based-Authentication. In *Proceedings of the Great Lakes Symposium on VLSI 2023* (pp. 97-102).
18. Taloba, A. I., Elhadad, A., Rayan, A., Abd El-Aziz, R. M., Salem, M., Alzahrani, A. A., ... & Park, C. (2023). A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare. *Alexandria Engineering Journal*, *65*, 263-274.
19. Bansod, S., Ragha, L. Challenges in making blockchain privacy compliant for the digital world: some measures. *Sādhanā* **47**, 168 (2022). https://doi.org/10.1007/s12046-022-01931-1.
20. OECD, Report, Opportunities and Challenges of Blockchain Technologies in Health Care, OECD Blockchain Policy Series, December 2020. Available at : https://www.oecd.org/finance/Opportunities-and-Challenges-of-Blockchain-Technologies-in-Health-Care.pdf.
21. OECD, Report, Opportunities and Challenges of Blockchain Technologies in Health Care, OECD Blockchain Policy Series, December 2020. Available at : https://www.oecd.org/finance/Opportunities-and-Challenges-of-Blockchain-Technologies-in-Health-Care.pdf.
22. Salim, M. M., Park, L., & Park, J. H. (2022, October). A Machine Learning based Scalable Blockchain architecture for a secure Healthcare system. In *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)* (pp. 2231-2234). IEEE.
23. Jayabalan, J., & Jeyanthi, N. (2022). Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *Journal of Parallel and Distributed Computing*, *164*, 152-167.
24. Hashim, F., Shuaib, K., & Zaki, N. (2022). Sharding for scalable blockchain networks. *SN Computer Science*, *4*(1), 2.
25. EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504.
26. See https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.
27. Kiania K, Jameii SM, Rahmani AM. Blockchain-based privacy and security preserving in electronic health: a systematic review. Multimed Tools Appl. 2023 Feb 17:1-27. doi: 10.1007/s11042-023-14488-w. Epub ahead of print. PMID: 36811000; PMCID: PMC9936121.
28. Shi S, He D, Li L, Kumar N, Khan MK, Choo KR. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Comput Secur. 2020 Oct;97:101966. doi: 10.1016/j.cose.2020.101966. Epub 2020 Jul 15. PMID: 32834254; PMCID: PMC7362828.

29. See https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.
30. See https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.
31. Edemekong PF, Annamaraju P, Haydel MJ. Health Insurance Portability and Accountability Act. [Updated 2022 Feb 3]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2023 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK500019/.
32. Rahime Belen-Saglam, Enes Altuncu, Yang Lu, Shujun Li, A systematic literature review of the tension between the GDPR and public blockchain systems, Blockchain: Research and Applications, Volume 4, Issue 2, 2023, 100129, ISSN 2096-7209, https://doi.org/10.1016/j.bcra.2023.100129.
33. World Health Organization. Regional Office for Europe. (2021). The protection of personal data in health information systems-principles and processes for public health. World Health Organization. Regional Office for Europe. https://apps.who.int/iris/handle/10665/341374.
34. Wolvaardt E. Data protection and privacy: an introduction. Community Eye Health. 2022;35(114):21. Epub 2022 Jun 7. PMID: 36035104; PMCID: PMC9412086.
35. Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. Heliyon, 7(3).
36. Khan, F., Kim, J. H., Mathiassen, L., & Moore, R. (2021). Data breach management: an integrated risk model. Information & Management, 58(1), 103392.
37. Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications, 100016.
38. Saha, S., Chowdhury, C., & Neogy, S. (2023). A novel two phase data sensitivity based access control framework for healthcare data. Multimedia Tools and Applications, 1-26.
39. Edemekong PF, Annamaraju P, Haydel MJ. Health Insurance Portability and Accountability Act. [Updated 2022 Feb 3]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2023 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK500019/.
40. Jayanthilladevi, A., Sangeetha, K., & Balamurugan, E. (2020, March). Healthcare biometrics security and regulations: Biometrics data security and regulations governing phi and hipaa act for patient privacy. In 2020 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 244-247). IEEE.
41. Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management, 15(1), 70-83. See also: OECD, December 2020, Policy Brief: Opportunities and Challenges of Blockchain in Healthcare, https://www.oecd.org/finance/Opportunities-and-Challenges-of-Blockchain-Technologies-in-Health-Care.pdf.
42. Kapoor, V., Singh, R., Reddy, R., & Churi, P. (2020, April). Privacy issues in wearable technology: An intrinsic review. In Proceedings of the International Conference on Innovative Computing & Communications (ICICC).
43. EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
44. T. Mulder & M. Tudorica (2019) Privacy policies, cross-border health data and the GDPR, Information & Communications Technology Law, 28:3, 261-274, DOI: 10.1080/13600834.2019.1644068.
45. EU Commission, Press Release, 23 Feb. 2022, Brussels, Data Act: Commission proposes measures for a fair and innovative data economy. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.
46. Council of the EU, Press release, 27 June 2023, Data act: Council and Parliament strike a deal on fair access to and use of data. Available at: https://www.consilium.europa.eu/en/press/press-releases/2023/06/27/data-act-council-and-parliament-strike-a-deal-on-fair-access-to-and-use-of-data/#:~:text=The%20data%20act%20will%20give,objects%2C%20machines%2C%20and%20devices.
47. Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. (2022). A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Generation Computer Systems*, *129*, 380-388. https://doi.org/10.1016/j.future.2021.11.028.