

Legal View on Blockchain Technologies in Healthcare: A European States Case Study

Ghazi Farouk, Annaba Badji Mokhtar University, Algeria
Tareck Alsamara, Prince Sultan University, Saudi Arabia*

ABSTRACT

This article presents an in-depth study of the legal landscape surrounding blockchain technology in the healthcare sector, with a special focus on case studies from European countries. Analyzing the existing legal framework and regulations, the research highlights the challenges and opportunities associated with the adoption of blockchain in healthcare. The most important research areas are data protection, security, consent, liability, and compliance. Through a comparative analysis of various European countries, the article illuminates the differences in legal approaches and points out possible areas of harmonization. The results clarify the legal aspects that must be addressed to ensure the integration of blockchain technology into healthcare systems, innovation while protecting patients' rights, and compliance with regulatory requirements.

KEYWORDS

Blockchain Technologies, European States, Healthcare, Legal View

INTRODUCTION

Digital transformation has become a prominent subject of public discourse spanning multiple industries. It entails the incorporation and utilization of digital technologies to bring about substantial alterations in organizational workflows, service delivery, and business frameworks. The swift progress of technology has instigated a profound transition towards digitalization, exerting influence on numerous facets of our daily lives. (Kokkinakos et al., 2016; Hassan et al., 2021; Iyamu, 2020; Appio et al., 2021), and several states have adopted huge budgets to transform public utilities into electronic public utilities (Vial, 2021; Sivathanu & Pillai, 2019). Digital transformation refers to the integration of digital technology into all areas of a business, resulting in fundamental changes to how the business operates and delivers value to customers (Matt et al., 2015; Dhali et al., 2022). It is a process of using digital technologies to fundamentally change how an organization functions, delivers value to customers, and achieves success. Digital transformation can involve a wide range of activities, including the adoption of new technologies such as artificial intelligence, the Internet of Things, cloud computing, the development of new business models and processes, and the creation of new products

DOI: 10.4018/IJSKD.333154

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

and services (Kitsios & Kamariotou, 2021; Azar et al., 2023). The goal of digital transformation is to improve efficiency, increase competitiveness, and drive growth by leveraging the power of digital technologies. It requires organizations to rethink their business models and processes and to adapt to new ways of working, which can be challenging. It also requires a culture of continuous learning and innovation, as well as the ability to adapt and change quickly in response to new developments. However, the benefits of digital transformation can be significant, including increased efficiency, agility, and competitiveness, as well as the ability to create new value for customers (Fahed-Sreih & Morin-Delerm, 2012).

Digital transformation in the medical field means relying on digital technology to manage everything related to health services (Kraus et al., 2021). The transformations in this field extend to several areas, including consultation, medical diagnosis (Gopal et al, 2019), treatment (Coile, 2000), rehabilitation services, the drug industry (Finelli & Narasimhan, 2020), and surgical interventions (Hashimoto et al, 2018). These matters require an effective information management system, security, and guarantees of individual privacy for patients. Digital transformation in healthcare refers to the integration of digital technology into all aspects of the healthcare system, including patient care, clinical research, administration, and education. It involves the use of digital tools and technologies, such as electronic health records (Menachemi & Collum, 2011), telemedicine (Hjelm, 2005), and wearable devices, to improve the efficiency, effectiveness, and accessibility of healthcare services (Tang et al., 2022). Also important is the concept of digital transformation in healthcare. Digital transformation in healthcare can improve the quality of care and diminish costs by leveraging the power that computerized innovation can provide. It also involves the re-examination of conventional types of healthcare and the selection of the most up-to-date approaches and innovations to provide care.

Digital transformation in healthcare in health care has many benefits, including:

- Progressive persistent care, with innovations that offer healthcare suppliers assistance in getting and sharing empirical data rapidly and precisely, leading to more proficient care;
- Expanded proficiency, with advanced innovations that can streamline various types of healthcare, such as planning arrangements and the more efficient recording of reserve fund utilization;
- Upgraded collaboration among healthcare providers, including computerized innovations that encourage communication and collaboration among healthcare experts empowering them to share information more successfully (Laurenza et al., 2018);
- Progressed understanding leading to advances such as telemedicine, which can ensure that care reaches patients in distant or underserved locations more rapidly (Ricciardi et al., 2019); and
- Improved provision of healthcare, allowing for more efficient administration and resulting in the greater well-being of patients (Faneela et al., 2023).

Innovations in blockchain technology also offer the possibility of bringing real benefits to the pharmaceutical industry. Blockchain is decentralized and can provide straightforward and secure exchange information (Dubovitskaya et al., 2017). By selectively storing records on a blockchain, healthcare organizations can guarantee that confidential information is secure and can only be accessed by people who are authorized to do so (Paul et al., 2023). Moreover, blockchain technology can be used to encourage the secure exchange of routine information between different healthcare organizations. This leads to superior communication and data sharing between healthcare providers.

Some of the potential benefits of blockchain technology within the pharmaceutical industry include:

- **Enhanced information security:** Blockchain innovation is secure and permanent, making it well-suited for storing sensitive information such as personal records and clinical trial information. This helps in preventing information breaches and unauthorized access to secret data (Liu et al., 2020).

- **Increased efficiency:** Blockchain innovation can help streamline different categories within the pharmaceutical industry, such as following clinical trial information and the clearing administrative endorsements. This could lead to retrieving reserve funds and improving effectiveness (Omar et al., 2021).
- **Improved secrecy:** Blockchain innovation can assist in advancing security by enabling the more accurate tracking of drugs from the point of manufacture to the point of use. This will ensure that patients are receiving the best prescription when taking a drug as intended.

Blockchain innovation has the potential to bring critical benefits to the pharmaceutical industry, including better supply chain efficiency, improved information security, expanded proficiency, and comprehensive security. Blockchain innovation contributes to the pharmaceutical industry through applications that provide a much better and safer system (Schöner et al., 2017; Zakari et al., 2022; Haq & Esuka, 2018).

RELATED WORKS

A comprehensive examination of the legal aspects surrounding blockchain technology in healthcare reveals significant insights and concerns. In their study, McGhin et al. ([2019]), highlight the existence of legal debates about data and smart contracts in the utilization of this technology. Similarly, Bayle et al. (2018) raise important legal considerations associated with these technologies. Additionally, Hasselgren et al. ([Year]), shed light on the privacy issues that arise when implementing blockchain technology in healthcare. Pashkov et al. (2019) highlights how blockchain technology can play a crucial role in identifying counterfeit and low-quality pharmaceutical products, thus contributing to the safety and well-being of patients. By examining the legal aspects associated with the adoption of blockchain in the pharmaceutical sector, Pashkov emphasizes the importance of protecting patients' rights and interests. Riva (2020) concluded that blockchain's disruptive influence on the digital landscape is undeniable, offering to address both patient rights and privacy concerns. While it can enhance security, it may also compromise data protection rights, such as the right to be forgotten, due to general data protection regulation (GDPR) loopholes. This study proposes transitioning from public, distributed blockchains to centralized, privately managed sidechains, entrusted to certified third parties based on legitimate interest. This approach aligns blockchain technology with data protection regulations while preserving its utility. It underscores the enduring relevance of legal frameworks in the digital age and merits further exploration for practical and economic applications.

These studies collectively emphasize the significance of addressing legal and privacy concerns when incorporating blockchain in healthcare systems. Our study aims to examine the legal perspectives surrounding the utilization of blockchain technologies in healthcare within European states. Through a comprehensive case study approach, it seeks to analyze the existing legal framework, regulatory challenges, and potential benefits of blockchain adoption in healthcare, ultimately contributing to a deeper understanding of the legal landscape and its implications for the future of healthcare innovation in Europe.

METHODOLOGY

This article examines the practical applications of blockchain technology in healthcare. This study takes a two-pronged approach, focusing on legal considerations related to blockchain adoption and providing a comparative analysis of the legal frameworks governing the implementation of blockchain in the provision of healthcare services within the European Union (EU).

The first approach focuses on thoroughly investigating the legal implications associated with the integration of blockchain technology in healthcare. The objective is to identify potential challenges and opportunities and assess the capacity of existing legal frameworks to effectively integrate this new technology. The second approach involves a comprehensive comparative study of legal systems within the EU. This analysis distinguishes between national laws that are specific to each country and laws that apply across the EU. By exploring these two types of legal frameworks, this study aims to provide insight into the legal hurdles and potential benefits specific to the implementation of blockchain technology in healthcare within the EU.

Finally, this article aims to contribute to the understanding of the legal dynamics surrounding the integration of blockchain in the healthcare sector, especially in the context of the EU. Through the scientific method and comprehensive analysis, this study reveals the legal challenges and opportunities arising from the implementation of blockchain technology in healthcare, providing valuable insights for EU policymakers, practitioners, and researchers in this field.

RESULTS AND DISCUSSION

The Importance of Blockchain Technology in Healthcare During the COVID-19 Pandemic

It is a mistake to disregard the widespread impact of COVID-19 on the healthcare frameworks of all nations, since the pandemic drastically complicated the provision of healthcare. Computerized innovation was one of the leading means of overcoming the numerous hardships caused by the widespread effects of the pandemic. Blockchain innovation has the potential to bring many benefits to the healthcare industry in the battle against COVID-19. It can be utilized to encourage the effective monitoring of people who have had contact with somebody who has tested positive for COVID-19 (Marbough et al., 2020). Moreover, it can be utilized to maintain the accuracy and traceability of the supply chain for COVID-19 immunizations and other fundamental restorative supplies, making it possible to guarantee that they are distributed impartially and effectively (Rotbi et al., 2021). Blockchain innovation can also be utilized to track and oversee clinical trial information for COVID-19 immunizations and medications, ensuring the accuracy and consistency of clinical trial results (Sharma et al, 2020). It can also be utilized to store and oversee electronic health records related to COVID-19, enabling secure yet efficient access to vital data. In these ways, blockchain innovation has the potential to bring significant benefits to the healthcare industry in the battle against COVID-19, including improved supply chain administration, improved follow-up, and more efficient clinical trial administration (Alam et al., 2021).

Role of Blockchain Technologies in the Prevention of Crime Related to the Drug Industry

Blockchain technology assists the legal authorities in the EU in tracking drug purchasing and monitoring the drug supply chain, to combat the counterfeiting medicine and deviations from legal medicine use. One area that needs to be covered by blockchain technology is drug tracing, to prevent counterfeit drugs from reaching buyers who may not be aware of what they are buying. In addition to managing drug supplies, contracts secured by blockchain technology can help healthcare organizations track expiry dates and contractual obligations of medicines, monitor how exchanges are made, and secure the timely execution of contracts (Musamih et al., 2021). It can also help to improve the transparency and traceability of the pharmaceutical supply chain, enabling companies to track the movement of products from the point of manufacture to the point of sale. This can help to reduce the risk of counterfeiting and fraud, as well as improve the efficiency of the supply chain (Fernando, 2019).

The Cryptographic Benefits for the Management of Healthcare

Medical cryptography has become one of the most important components of healthcare provision, and its use enhances the efficiency of operations in this area (He & Zeadally, 2014, Abdallah et al., 2021). There are different types of cryptographic tokens used in different activities and request functions. Therefore, there are no problems with repetition and misinterpretation in the proper functioning of medical assistance processes using medical cryptography (El Khatib et al., 2021).

The Legal Issue of the Use of Blockchain Related to the Publicity of Patient Records

Management of patient records is the best example of how important the use of blockchain technology has become in health institution management (Kshetri, 2018). Because patients see many different doctors, and because their medical needs change, medical records must be easily transferable between different healthcare organizations to ensure accuracy. Blockchain technology enables healthcare records to be updated quickly and securely (Ivan, 2016).

The Security in Blockchain Technology and Transfer of Patient Medical Record

Blockchain innovation has the potential to be used in the securing and the exchanging of medical records but whatever the application, it is critical to note that the usage of blockchain innovation within the healthcare industry requires careful planning and thought. It is essential to guarantee that suitable security measures are in place to protect information and to guarantee that the new technology operates consistently with existing frameworks and forms. Last but not least, blockchain innovation has the potential to completely ensure the security and availability of medical records and to enable the effective and secure sharing of critical data between healthcare organizations (Engelhardt, 2017; Wang & Wang, 2021; Khater, 2023).

Blockchain frameworks may also grant patients expanded levels of access to and control over their private health data. Requiring confirmation of changes made to archives can guarantee the exactness of records, and this sort of confirmation can give an extra layer of security against both human blunder and purposeful adulteration (Haleem et al, 2021). Protection of health data is vital (Hodge et al., 1999). For this reason: the law of the EU and national laws within the individual states ensure the right to health data security (Hiller et al., 2011). These laws are based on the necessity of ensuring both personal security and the accessibility of health data (Hodge, 2003). If blockchain innovations permit unguarded access to patients' information, this may be a violation of patient's right to health data security. Within the United States, all patients have the right to medical records privacy unless they voluntarily consent to lift the confidentiality of their medical information. The Health Insurance Portability and Accountability Act of 1996 (Theodos & Sittig, 2021) implies that for the patient's medical data to be accessible, the patient's assent must be given. This is usually done by written affirmation of consent. This applies to most healthcare professionals. Privacy rules set out point-by-point guidelines about security and access to data.

In France, the sharing of healthcare information is covered by Article 4 of the Code of Medical Ethics, in which the patient's right to confidentiality is matched by the doctor's duty to ensure that confidentiality. This includes not only the information the doctor has received directly from the patient, but also all related information that he has observed, heard, or understood from whatever source (Régnier & Rouzioux, 1983). In addition, the doctor has a legal obligation related to the patient's health information, as stipulated in Article 7 of the European Code of Medical Ethics, as the doctor is the first to know this information during his contact with the patient, and he is the first to record those results (Frischhut & Werner-Felmayer, 2020). Article 8 prohibits unqualified doctors from participating in databases that might violate the patient's right to privacy and emphasizes that databases should be placed under the responsibility of a specific doctor qualified to deal with a specific patient (Patuzzo & Pulice, 2017). European laws also prohibit the disclosure of medical information related to crimes, to ensure the confidentiality of criminal investigations (Ferguson, 2006), and the interest

of minor children also requires confidentiality in some cases (Uka, 2019). A blockchain system that does not take into account these legal arguments is considered a violation of European laws. For this reason, patient consent is mandatory for blockchain use (Benchoufi et al., 2017).

The Legal Issue in Electronic Health Records and Patient-Generated Data

Patient-generated health data (PGD) is a database related to patients and includes all information related to specific cases, but it is provided by the patients or their relatives, (Shapiro et al, 2012) to bring them together with one goal, which is to overcome the disease or adapt to it (Figueiredo & Chen, 2020). In this case, the patient shares his information with others, which means that there is consent from him to publish and exchange information, and there is no legal breach by any other party towards the patient. However, these databases raise more legal questions about whether the owner of this data is the patient or the electronic service provider (Jim et al., 2020). This even has commercial dimensions (Mikk et al., 2017).

The Legal Issue of the Use of Blockchain in Health Insurance

Blockchain technology creates a single source of truth to ensure interoperability and accessibility (Thenmozhi et al., 2021). This enables the provision of accurate information to medical providers and insurance companies (Chondrogiannis et al., 2022). It can also detect and protect against fraud through smart contracts powered by blockchain technology (Saldamli et al., 2020; Park & Ryu, 2019). In addition, blockchain technology seems useful for managing administrative operations related to health insurance, through smart insurance contracts, as the creation of smart contracts is very rapid and the financial payment methods are automatic. Furthermore, the cost of financial services is low (Amponsah et al., 2022).

The Problem of the Time and Place of the Smart Contract in the Framework of the Blockchain

A contract is defined as an agreement between two parties to create legal effects that include mutual obligations (Koffman & Macdonald, 2010; Momani, 2020). A smart contract is a contract that is made through smart technologies such as blockchain. It is known as a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein are stored on the blockchain network. Unlike a traditional contract, there is no third party tasked with maintaining the contract, as the smart contract is available and registered with all parties to the network.

Smart contracts are designed to facilitate, verify, and enforce the negotiation or performance of a contract (Raskin, 2016). They can be used in a variety of applications, including financial transactions, supply chain management, and real estate transactions. Smart contracts are often associated with blockchain technology, as they rely on the decentralized and distributed nature of the blockchain to function. Blockchain technology provides a secure and transparent platform for the creation and execution of smart contracts, as it allows for the safe and efficient transfer of data. Finally, the relationship between blockchain technology and smart contracts is such that smart contracts rely on the decentralized and secure nature of the blockchain to function, while blockchain technology provides a platform for the creation and execution of smart contracts.

Furthermore, the time and place of the contract determine the law applicable to any disputes that might be related to it. It may be easy from a technical point of view to determine the time of the smart contract in the frameworks of blockchain technology, but determining the place of the smart contract is impossible (Szczerbowski, 2017), and the place of the contract is mandatory to determine the applicable law. In the case of smart contracts, legislation should establish solutions to this problem within the framework of private international law (Djurovic & Janssen, 2018).

Relationship Between Blockchain and the Right to be Forgotten

The “right to be forgotten” is a concept that alludes to an individual’s right to have their information deleted from the web or other sources (Graux et al., 2012). This right is based on the thought that people ought to have control over their information and the right to choose how it is utilized and shared. This right to be overlooked has been recognized in numerous national laws, including the EU, where it is ensured by the GDPR (Sartor, 2016). In Europe, the Court of Justice of the European Union established the right to be forgotten, saying that, under certain conditions, “the administrator of a search engine is obliged to expel from the search results information relevant to concerned parties.” (*Google Spain v. AEPD*, 2014)

After that decision, European inhabitants could have references alluding to their information removed, given a valid reason (Kropf, 2014). Under the GDPR, people have the right to request the erasure of their individual information under certain circumstances, such as when the information is not essential for the reason for which it was collected or when the person pulls back their assent for the processing of their information. This has important implications for online security and the assurance of the privacy of individual data. It empowers people to have more prominent control over their individual information and to ensure that it isn’t utilized in ways that will be destructive or detrimental to their interests (Voigt & Von dem Bussche, 2017, pp. 9–30).

The relationship between blockchain innovation and such privacy measures can be complex, as blockchain is planned to be a decentralized and unchanging record innovation. This means that once data is stored in the blockchain system, it is extremely difficult to erase or alter. This characteristic of blockchain innovation poses challenges for the execution of the right to be forgotten, because it may be troublesome to eradicate an individual’s personal information from the blockchain (Bayle et al., 2018).

However, the right to be forgotten does not require the total deletion of information from the web or other online stages. There are a few ways in which blockchain innovation can be utilized to bolster the execution of the right to be forgotten, including the utilization of cryptographic methods, such as encryption, to protect the security of individual information, and the utilization of permissioned blockchains to control access to individual information. While the relationship between blockchain innovation and the right to be forgotten can be complex, it is conceivable to utilize blockchain innovation to support the execution of health information security and to allow people more control over their individual data (Bharadwaj, 2021).

The activity of companies in the field of blockchain technology in health care is recent in Europe (Buchanan & Naqvi, 2018), and its activity may develop in the future.

CONCLUSION

The correct utilization of blockchain in healthcare includes numerous legal provisions. Especially critical is persistent assent, which permits patients to exercise their independence and to allow for ongoing choices concerning the collection, utilization, and sharing of their individual information.

Table 1. Laws regulating blockchain and blockchain companies

	Laws regulating Blockchain	Blockchain companies in healthcare
UK	Data Protection Act 2018	Medical chain
France	The GDPR is an EU Data Protection Act (Loi Informatique et Libertés).	Chain Factory French National Health Data System (SNDS)
Germany	The GDPR is an EU Federal Data Protection Act (BDSG).	Medibloc

It guarantees that patients can completely understand the purposes for which their information will be used and select whether to allow the collection and utilization of their information. It can help secure the protection and security of private data by guaranteeing that it is collected, utilized, and shared according to patients' wishes. This is especially critical when it comes to the establishment of EHRs and PGD, which may contain delicate and individual data. Furthermore, patient assent is essential to create confidence and straightforwardness between patients and healthcare suppliers by building up an unequivocal understanding between the two parties. This will greatly improve the relationship between patients and healthcare suppliers and will also improve the quality of care. In numerous nations, persistent assent is required by law to gather, utilize, and share individual information, counting EHRs and PGD.

AUTHOR NOTE

The authors are thankful to Governance and Policy Design Research Lab (GPDRL) and Prince Sultan University for providing APC for this publication.

Correspondence regarding this article should be sent to Tareck Alsamara at tareck.alsamara@gmail.com.

REFERENCES

- Abdallah, H. M., Taha, A., & Selim, M. M. (2021). Cloud-based fuzzy keyword search scheme over encrypted documents. [IJSKD]. *International Journal of Sociotechnology and Knowledge Development*, 13(4), 82–100. doi:10.4018/IJSKD.2021100106
- Alam, S., Reegu, F. A., Daud, S. M., & Shuaib, M. (2021). Blockchain-based electronic health record system for efficient Covid-19 pandemic management. Preprints, 2021, 1–5. 10.20944/preprints202104.0771.v1
- Amponsah, A. A., Adekoya, A. F., & Weyori, B. A. (2022). Improving the financial security of national health insurance using cloud-based blockchain technology application. *International Journal of Information Management Data Insights*, 2(1), 100081. doi:10.1016/j.jjime.2022.100081
- Appio, F. P., Frattini, F., Petruzzelli, A. M., & Neirotti, P. (2021). Digital transformation and innovation management: A synthesis of existing research and an agenda for future studies. *Journal of Product Innovation Management*, 38(1), 4–20. doi:10.1111/jpim.12562
- Azar, A. T., Tounsi, M., Fati, S. M., Javed, Y., Amin, S. U., Khan, Z. I., Alsenan, S., & Ganesan, J. (2023). Automated system for colon cancer detection and segmentation based on deep learning techniques. [IJSKD]. *International Journal of Sociotechnology and Knowledge Development*, 15(1), 1–28. doi:10.4018/IJSKD.326629
- Bayle, A., Koscina, M., Manset, D., & Perez-Kempner, O. (2018). When blockchain meets the right to be forgotten: Technology versus law in the healthcare industry. In *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)* (pp. 788–792). IEEE. doi:10.1109/WI.2018.00133
- Benchoufi, M., Porcher, R., & Ravaud, P. (2017). Blockchain protocols in clinical trials: Transparency and traceability of consent [version 5; peer review: 1 approved, 2 approved with reservations, 2 not approved]. *F1000 Research*, 6, 1–66. doi:10.12688/f1000research.10531.1 PMID:29167732
- Bharadwaj, A. (2021). Blockchain and the right to be forgotten. *Nirma University Law Journal*, 11, 35. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/nulj11&div=8&id=&page=>
- Buchanan, B., & Naqvi, N. (2018). Analysis: Building the future of EU: Moving forward with international collaboration on blockchain. *The Journal of The British Blockchain Association*, 1(1), 1–4. <https://researchrepository.napier.ac.uk/Output/1202098>. doi:10.31585/jbba-1-1-(7)2018
- Chondrogiannis, E., Andronikou, V., Karanastasis, E., Litke, A., & Varvarigou, T. (2022). Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations. *Blockchain: Research and Applications*, 3(2), 1–14. doi:10.1016/j.bcr.2021.100049
- Coile, R. C. Jr. (2000). The digital transformation of health care. (Health care meets e-commerce). *Physician Executive*, 26(1), 8–15. <https://link.gale.com/apps/doc/A102340165/AONE?u=anon~87cea9ec&sid=googleScholar&xid=6adbbf66> PMID:10788126
- Dhali, M., Hassan, S., Zuhuda, S., & Bt Ismail, S. F. (2022). Artificial intelligence in health care: Data protection concerns in Malaysia. *International Data Privacy Law*, 12(2), 143–161. doi:10.1093/idpl/ipac005
- Djurovic, M., & Janssen, A. (2018). The formation of blockchain-based smart contracts in the light of contract law. *European Review of Private Law*, 26(6), 753–771. doi:10.54648/ERPL2018053
- Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain. In *AMIA ... annual symposium proceedings / AMIA symposium* (Vol. 2017, pp. 650–659). American Medical Informatics Association., <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5977675/>
- El Khatib, M., Beshwari, F., Beshwari, M., & Beshwari, A. (2021). The impact of blockchain on project management. *ICIC Express Letters*, 15(5), 467–474. doi:10.24507/icicel.15.05.467
- Engelhardt, M. A. (2017). Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. *Technology Innovation Management Review*, 7(10), 22–34. https://www.timreview.ca/sites/default/files/article_PDF/Engelhardt_TIMReview_October2017.pdf. doi:10.22215/timreview/1111
- Fahed-Sreih, J., & Morin-Delerm, S. (2012). A perspective on leadership in small businesses: Is the need for achievement a motive in predicting success? *International Journal of Entrepreneurship*, 16, 1.

- Faneela, Khan, M. A., Alsuhibany, S. A., El-Shafai, W., Rehman, M. U., & Ahmad, J. (2023). An immutable framework for smart healthcare using blockchain technology. *Computer Systems Science and Engineering*, 46(1), 165–179. doi:10.32604/csse.2023.035066
- Ferguson, P. R. (2006). The criminal jury in England and Scotland: The confidentiality principle and the investigation of impropriety. *The International Journal of Evidence & Proof*, 10(3), 180–211. doi:10.1350/ijep.2006.10.3.180
- Fernando, E. (2019). Success factor of implementation blockchain technology in pharmaceutical industry: A literature review. In *2019 6th international conference on information technology, computer and electrical engineering (ICITACEE)* (pp. 1–5). IEEE. doi:10.1109/ICITACEE.2019.8904335
- Figueiredo, M. C., & Chen, Y. (2020). Patient-generated health data: Dimensions, challenges, and open questions. *Foundations and Trends® in Human–Computer Interaction*, 13(3), 165–297. 10.1561/11000000080
- Finelli, L. A., & Narasimhan, V. (2020). Leading a digital transformation in the pharmaceutical industry: Reimagining the way we work in global drug development. *Clinical Pharmacology and Therapeutics*, 108(4), 756–761. doi:10.1002/cpt.1850 PMID:32294230
- Frischhut, M., & Werner-Felmayer, G. (2020). A European perspective on medical ethics. *Medicine (Abingdon)*, 48(10), 634–636. doi:10.1016/j.mpmed.2020.07.001
- Gopal, G., Suter-Crazzolaro, C., Toldo, L., & Eberhardt, W. (2019). Digital transformation in healthcare—architectures of present and future information technologies. [CCLM]. *Clinical Chemistry and Laboratory Medicine*, 57(3), 328–335. doi:10.1515/cclm-2018-0658 PMID:30530878
- Graux, H., Ausloos, J., & Valcke, P. (2012). *The right to be forgotten in the internet era*. ICRI research paper. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2174896
- Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*, 2, 130–139. doi:10.1016/j.ijin.2021.09.005
- Haq, I., & Esuka, O. M. (2018). Blockchain technology in the pharmaceutical industry to prevent counterfeit drugs. *International Journal of Computer Applications*, 180(25), 8–12. https://www.researchgate.net/profile/Ijazul-Haq/publication/323872197_Blockchain_Technology_in_Pharmaceutical_Industry_to_Prevent_Counterfeit_Drugs/links/5acc9154a6fdcc8bfc87e5f4/Blockchain-Technology-in-Pharmaceutical-Industry-to-Prevent-Counterfeit-Drugs.pdf. doi:10.5120/ijca2018916579
- Hashimoto, D. A., Rosman, G., Rus, D., & Meireles, O. R. (2018). Artificial intelligence in surgery: Promises and perils. *Annals of Surgery*, 268(1), 70–76. doi:10.1097/SLA.0000000000002693 PMID:29389679
- Hassan, S., Dhali, M., Zaman, F., & Tanveer, M. (2021). Big data and predictive analytics in healthcare in Bangladesh: Regulatory challenges. *Heliyon*, 7(6), 1–12. doi:10.1016/j.heliyon.2021.e07179 PMID:34141936
- He, D., & Zeadally, S. (2014). An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. *IEEE Internet of Things Journal*, 2(1), 72–83. doi:10.1109/JIOT.2014.2360121
- Hiller, J., McMullen, M. S., Chumney, W. M., & Baumer, D. L. (2011). Privacy and security in the implementation of health information technology (electronic health records): US and EU compared. *Boston University Journal of Science & Technology Law*, 17, 1–39. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/jstl17&div=4&id=&page=>
- Hjelm, N. M. (2005). Benefits and drawbacks of telemedicine. *Journal of Telemedicine and Telecare*, 11(2), 60–70. doi:10.1258/1357633053499886 PMID:15829049
- Hodge, J. G. Jr. (2003). Health information privacy and public health. *The Journal of Law, Medicine & Ethics*, 31(4), 663–671. doi:10.1111/j.1748-720X.2003.tb00133.x PMID:14968668
- Hodge, J. G. Jr, Gostin, L. O., & Jacobson, P. D. (1999). Legal issues concerning electronic health information: Privacy, quality, and liability. *Journal of the American Medical Association*, 282(15), 1466–1471. doi:10.1001/jama.282.15.1466 PMID:10535438

- Ivan, D. (2016, September 26–27). *Moving toward a blockchain-based method for the secure storage of patient records* [Paper presentation]. ONC/NIST Use of Blockchain for Healthcare and Research Workshop, Gaithersburg, MA, United States. https://www.truevaluemetrics.org/DBpdfs/Technology/Blockchain/9-16-drew_ivan_20160804_blockchain_for_healthcare_final.pdf
- Iyamu, T. (2020). Examining e-government enabling of e-health service through the lens of structuration theory. [IJSKD]. *International Journal of Sociotechnology and Knowledge Development*, 12(3), 26–40. doi:10.4018/IJSKD.2020070102
- Jim, H. S., Hoogland, A. I., Brownstein, N. C., Barata, A., Dicker, A. P., Knoop, H., Gonzalez, B. D., Perkins, R., Rollinson, D., Gilbert, S. M., Nanda, R., Berglund, A., Mitchell, R., & Johnstone, P. A. S. (2020). Innovations in research and clinical care using patient-generated health data. *CA: a Cancer Journal for Clinicians*, 70(3), 182–199. doi:10.3322/caac.21608 PMID:32311776
- Khater, M. H. (2023). International perspective on securing cyberspace against terrorist acts. [IJSKD]. *International Journal of Sociotechnology and Knowledge Development*, 15(1), 1–11. doi:10.4018/IJSKD.318706
- Kitsios, F., & Kamariotou, M. (2021). Artificial intelligence and business strategy towards digital transformation: A research agenda. *Sustainability (Basel)*, 13(4), 2025. doi:10.3390/su13042025
- Koffman, L., & Macdonald, E. (2010). *The law of contract*. Oxford University Press. doi:10.1093/he/9780199570201.001.0001
- Kokkinakos, P., Markaki, O., Koussouris, S., & Psarras, J. (2016). Digital transformation: Is public sector following the enterprise 2.0 paradigm? In A. Chugunov, R. Bolgov, Y. Kabanov, G. Kampis, & M. Wimmer (Eds.), *Digital Transformation and Global Society. DTGS 2016. Communications in Computer and Information Science* (Vol. 674, pp. 96–105). Springer. doi:10.1007/978-3-319-49700-6_11
- Kraus, S., Schiavone, F., Pluzhnikova, A., & Invernizzi, A. C. (2021). Digital transformation in healthcare: Analyzing the current state-of-research. *Journal of Business Research*, 123, 557–567. doi:10.1016/j.jbusres.2020.10.030
- Kropf, J. W. (2014). Google Spain SL v. Agencia Española de Protección de Datos (AEPD). *The American Journal of International Law*, 108(3), 502–509. doi:10.5305/amerjintelaw.108.3.0502
- Kshetri, N. (2018). Blockchain and electronic healthcare records [cybertrust]. *Computer*, 51(12), 59–63. doi:10.1109/MC.2018.2880021
- Laurenza, E., Quintano, M., Schiavone, F., & Vrontis, D. (2018). The effect of digital technologies adoption in healthcare industry: A case-based analysis. *Business Process Management Journal*, 24(6), 1364–1386. doi:10.1108/BPMJ-04-2017-0084
- Liu, H., Crespo, R. G., & Martínez, O. S. (2020). Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts. *Health Care*, 8(3), 1–17. PMID:32751325
- Marbough, D., Abbasi, T., Maasmi, F., Omar, I. A., Debe, M. S., Salah, K., Jayaraman, R., & Ellahham, S. (2020). Blockchain for COVID-19: Review, opportunities, and a trusted tracking system. *Arabian Journal for Science and Engineering*, 45(12), 9895–9911. doi:10.1007/s13369-020-04950-4 PMID:33072472
- Matt, C., Hess, T., & Benlian, A. (2015). Digital transformation strategies. *Business & Information Systems Engineering*, 57(5), 339–343. doi:10.1007/s12599-015-0401-5
- McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, 135, 62–75. doi:10.1016/j.jnca.2019.02.027
- Menachemi, N., & Collum, T. H. (2011). Benefits and drawbacks of electronic health record systems. *Risk Management and Healthcare Policy*, 4, 47–55. doi:10.2147/RMHP.S12985 PMID:22312227
- Mikk, K. A., Sleeper, H. A., & Topol, E. J. (2017). The pathway to patient data ownership and better health. *Journal of the American Medical Association*, 318(15), 1433–1434. doi:10.1001/jama.2017.12145 PMID:28973063
- Momani, A. M. (2020). The unified theory of acceptance and use of technology: A new approach in technology acceptance. [IJSKD]. *International Journal of Sociotechnology and Knowledge Development*, 12(3), 79–98. doi:10.4018/IJSKD.2020070105

- Musamih, A., Salah, K., Jayaraman, R., Arshad, J., Debe, M., Al-Hammadi, Y., & Ellahham, S. (2021). A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE Access : Practical Innovations, Open Solutions*, 9, 9728–9743. doi:10.1109/ACCESS.2021.3049920
- Omar, I. A., Jayaraman, R., Salah, K., Yaqoob, I., & Ellahham, S. (2021). Applications of blockchain technology in clinical trials: Review and open challenges. *Arabian Journal for Science and Engineering*, 46(4), 3001–3015. doi:10.1007/s13369-020-04989-3
- Park, D., & Ryu, D. (2019). Blockchain in health insurance: Sharing medical information and preventing insurance fraud. *Korean Journal of Financial Studies*, 48(4), 417–447. doi:10.26845/KJFS.2019.08.48.4.417
- Pashkov, V., & Soloviov, O. (2019). Legal implementation of blockchain technology in pharmacy. *SHS web of conferences*, 68, 01027.
- Patuzzo, S., & Pulice, E. (2017). Towards a European code of medical ethics: Ethical and legal issues. *Journal of Medical Ethics*, 43(1), 41–46. doi:10.1136/medethics-2015-102963 PMID:27974420
- Paul, M., Maglaras, L., Ferrag, M. A., & AlMomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express*, 9(4), 571–588. doi:10.1016/j.icte.2023.02.007
- Raskin, M. (2016). The law and legality of smart contracts. *Georgetown Law Technology Review*, 1, 305. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/gtltr1&div=32&id=&page=>
- Régnier, F., & Rouzioux, J. M. (1983). Report from France: Contemporary aspects of medical ethics in France. *Journal of Medical Ethics*, 9(3), 170–174. doi:10.1136/jme.9.3.170 PMID:6352945
- Ricciardi, W., Pita Barros, P., Bourek, A., Brouwer, W., Kelsey, T., Lehtonen, L., Anastasy, C., Barros, P., Barry, M., Bourek, A., Brouwer, W., De Maeseneer, J., Kringos, D., Lehtonen, L., McKee, M., Murauskiene, L., Nuti, S., Ricciardi, W., Siciliani, L., & Wild, C. (2019). How to govern the digital transformation of health services. *European Journal of Public Health*, 29(Suppl. 3), 7–12. doi:10.1093/eurpub/ckz165 PMID:31738442
- Riva, G. M. (2020). What happens in blockchain stays in blockchain. A legal solution to conflicts between digital ledgers and privacy rights. *Frontiers in Blockchain*, 3, 36. doi:10.3389/fbloc.2020.00036
- Rotbi, M. F., Motahhir, S., & Ghzizal, A. E. (2021). Blockchain technology for a safe and transparent COVID-19 vaccination. *Journal of ICT Standardization*, 10(2), 125–144. doi:10.13052/jicts2245-800X.1022
- Saldamli, G., Reddy, V., Bojja, K. S., Gururaja, M. K., Doddaveerappa, Y., & Tawalbeh, L. (2020). Health care insurance fraud detection using blockchain. In *2020 seventh international conference on software defined systems (SDS)* (pp. 145–152). IEEE. doi:10.1109/SDS49854.2020.9143900
- Sartor, G. (2016). The right to be forgotten: Balancing interests in the flux of time. *International Journal of Law and Information Technology*, 24(1), 72–98. doi:10.1093/ijlit/eav017
- Schöner, M. M., Kourouklis, D., Sandner, P., Gonzalez, E., & Förster, J. (2017). *Blockchain technology in the pharmaceutical industry*. Frankfurt School Blockchain Center. http://explore-ip.com/2017_Blockchain-Technology-in-the-Pharmaceutical-Industry.pdf
- Shapiro, M., Johnston, D., Wald, J., & Mon, D. (2012). *Patient-generated health data* [White paper]. RTI International. <https://www.rti.org/sites/default/files/resources/patientgeneratedhealthdata.pdf>
- Sharma, A., Bahl, S., Bagha, A. K., Javaid, M., Shukla, D. K., & Haleem, A. (2020). Blockchain technology and its applications to combat COVID-19 pandemic. *Research on Biomedical Engineering*, 38(1), 173–180. doi:10.1007/s42600-020-00106-3
- Sivathanu, B., & Pillai, R. (2019). Leveraging technology for talent management: Foresight for organizational performance. [IJSKD]. *International Journal of Sociotechnology and Knowledge Development*, 11(2), 16–30. doi:10.4018/IJSKD.2019040102
- Szczerbowski, J. J. (2017). Place of smart contracts in civil law. A few comments on form and interpretation. In *Proceedings of the 12th annual international scientific conference NEW TRENDS*, 333–338. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3095933

- Tang, X., Zhu, L., Shen, M., Peng, J., Kang, J., Niyato, D., & El-Latif, A. A. A. (2022). Secure and trusted collaborative learning based on blockchain for artificial intelligence of things. *IEEE Wireless Communications*, 29(3), 14–22. doi:10.1109/MWC.003.2100598
- Thenmozhi, M., Dhanalakshmi, R., Geetha, S., & Valli, R. (2021). WITHDRAWN: Implementing blockchain technologies for health insurance claim processing in hospitals. *Materials Today: Proceedings*, 1–20. doi:10.1016/j.matpr.2021.02.776
- Theodos, K., & Sittig, S. (2021). Health information privacy laws in the digital age: HIPAA doesn't apply. *Perspectives in Health Information Management*, 18(Winter), 1–10. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7883355/> PMID:33633522
- Uka, M. (2019). The right of the defendant for public hearing and the role of media in this publicity. *Acta Universitatis Danubius. Juridica*, 15(1), 214–228. <https://www.cceol.com/search/article-detail?id=799553>
- Vial, G. (2021). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), 118–144. doi:10.1016/j.jsis.2019.01.003
- Voigt, P., & Von dem Bussche, A. (2017). *The EU general data protection regulation (GDPR): A practical guide* (1st ed.). Springer International Publishing. doi:10.1007/978-3-319-57959-7
- Wang, S., & Wang, H. (2021). A sociotechnical systems analysis of knowledge management for cybersecurity. [IJSKD]. *International Journal of Sociotechnology and Knowledge Development*, 13(3), 77–94. doi:10.4018/IJSKD.2021070105
- Zakari, N., Al-Razgan, M., Alsaadi, A., Alshareef, H., Al saigh, H., Alashaikh, L., Alharbi, M., Alomar, R., & Alotaibi, S. (2022). Blockchain technology in the pharmaceutical industry: A systematic review. *PeerJ. Computer Science*, 8, 1–26. doi:10.7717/peerj-cs.840 PMID:35634106