

Blockchain and the General Data Protection Regulation: Healthcare Data Processing

Paola Perchinunno[1](✉), Antonella Massari[1], Samuela L'Abbate[1], and Corrado Crocetta[2]

[1] Department of Economics, Management and Business Law, University of Bari "Aldo Moro", Bari, Italy
{paola.perchinunno,antonella.massari,samuela.labbate}@uniba.it
[2] Department of Humanities Research and Innovation, University of Bari "Aldo Moro", Bari, Italy
corrado.crocetta@uniba.it

Abstract. The General Data Protection Regulation (GDPR) of the European Union became binding in May 2018. The objective of the GDPR is essentially twofold. On the one hand, it seeks to facilitate the free movement of personal data between the various EU Member States, and, on the other hand, it establishes a framework for the protection of fundamental rights, based on the right to data protection as set out in Article 8 of the Charter of Fundamental Rights. The European Parliament has declared that the Blockchain must be considered a "tool that strengthens the autonomy of citizens by giving them the opportunity to control their data and decide which ones to share in the register, as well as the ability to choose who can see such data", thus favoring the transparency of transactions. Blockchain (or distributed register technology – DLT) technologies and their potential for the European Union's digital single market have been widely discussed in recent years. It has been argued that blockchain technologies could be a suitable tool to achieve some of the goals of GDPR. Blockchains can be designed to allow data sharing, and improve transparency on data access. This study analyzes the relationship between blockchain and GDPR, to highlight existing problems and study possible solutions in relation to the processing of health data.

Keywords: General Data Protection Regulation · Blockchain technologies · transparency · health data

1 Introduction

Data relating to health are a particular type of personal data characterized by being "related to the physical or mental health of a natural person, including the provision of health care services, which reveal information relating to his state of health". They

The contribution is the result of joint reflections by the authors, with the following contributions attributed to C. Crocetta (Chapters 1 and 5); to A. Massari (Chapter 2), to P. Perchinunno (Chapter 4) and to S. L'Abbate (Chapter 3).

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
O. Gervasi et al. (Eds.): ICCSA 2023 Workshops, LNCS 14106, pp. 377–388, 2023.
https://doi.org/10.1007/978-3-031-37111-0_27

are included in the broader category of data subject to special treatment and enhanced protection, as they are able to reveal very intimate details of the person.

The General Data Protection Regulation (GDPR) of the European Union was created with the aim of harmonizing the regulation on the protection of personal data within the European Union, and of developing the European Digital Single Market, fueling citizens' trust in the use of digital services.

The European Parliament has declared that the Blockchain must be considered a "tool that strengthens the autonomy of citizens by giving them the opportunity to control their data and decide which ones to share in the register, as well as the ability to choose who can see such data", thus favoring the transparency of transactions.

Blockchain techniques, if properly designed, share the same objectives with the GDPR: to create an environment in which data security is guaranteed and to give subjects control over them [1]. Blockchain has numerous benefits such as decentralization, persistence, anonymity, and auditability [2]. Blockchain, originally developed to support the cryptocurrency ecosystem, has recently been used in various other fields to achieve extraordinary levels of security [3]. Similarly, the healthcare sector has started integrating blockchain into various aspects of this digital age. Its features such as micro-transactions, decentralized exchanges, consensus mechanisms, and smart contracts allow for securing the privacy of the health data of patients who are key stakeholders in the healthcare domain [4].

Blockchain applications in the healthcare sector generally require more stringent authentication, interoperability, and record sharing requirements, due to exacting legal requirements [5].

This study analyzes the relationship between blockchain and GDPR, to highlight existing problems and study possible solutions in relation to the processing of health data.

2 The General Data Protection Regulation (GDPR)

2.1 Introduction

The General Data Protection Regulation (GDPR) of the European Union was published in the European Official Journal on 4 May 2016, it entered into force on 24 May 2016, but its implementation took place two years later, starting from 25 May 2018. Since it is a regulation, it does not need to be transposed by the States of the Union and is implemented in the same way in all States without margins of freedom in adaptation.

With this regulation, the European Commission aims to strengthen the protection of personal data of citizens of the European Union and residents, both inside and outside the borders, giving back to citizens the control of their personal data, simplifying the regulatory environment that affects international affairs, unifying and making internal privacy legislation homogeneous.

2.2 Aims and Purposes

The GDPR regulates the processing of personal data of natural persons only and therefore the identification data of subjects with legal personality are excluded from the application of the code.

First, the Regulation provides a definition of "data" or "any information relating to an identified or identifiable natural person (defined as an interested party). The data, therefore, are all the information strictly related to the person. They go beyond the name and surname, including genetic, biometric data and data relating to the health of a natural person.

Furthermore, the GDPR precisely identifies the role and duties of the subjects involved in the protection of personal data, consisting - in addition to the interested party - in the data controller and data processor. In particular:

- the interested party is the physical subject to whom the data refer;
- the data controller is the key figure (natural or legal person, public authority, service or other body that determines the purposes and means of processing) in terms of data protection, because it is this subject to whom the data subject addresses to assert one's rights recognized by the regulation;
- the data controller is the person (natural or legal) who processes the data, responding directly to the owner.

2.3 Relevant Aspects for the Purposes of Health Data Processing

Let's analyze in detail the main articles of the GDPR that may be of interest for the purposes of processing and tracking health data.

Pursuant to art. 2, paragraph 1 of the GDPR:

- *This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.*

The GDPR applies accordingly to any processing of personal data which takes place in whole or in part by automated means, as well as to processing of personal data which is not automated but forms part of, or is intended to form part of, a filing system.

Personal data processing is defined as 'any operation or set of operations which is performed on personal data or sets of personal data [1].

With regards to blockchains, this very broad definition of what counts as data processing implies that the analysis of personal data, its ongoing retention and any further processing constitutes processing of personal data within the meaning of Article 4(2), of the GDPR:

- *Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval,*

consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Article 3 of the GDPR also provides that:

– *This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*

This implies that where a natural or legal person qualified as a controller or a processor under the GDPR is established in the EU and processes personal data (via blockchain or other means), the European data protection framework applies to such processing. Some data.

The core of the GDPR is the protection of people's data, in other words the individuals to whom that data belongs. In a very synthetic way, this is what the GDPR introduces on the subject in art. 12 and following. Users can:

– *ask and get answers on the use that a company will make of its data and to ask for compensation if these questions do not have clear, concise and timely answers;*
– *know how personal data will be used at the time of their collection/request and know how long they will be kept;*
– *access personal data that are processed/processed by those who have requested consent;*
– *rectify and modify your personal data;*
– *request (and obtain) the cancellation of your personal data when they are no longer necessary for the purposes for which they were collected;*
– *limit the processing of your data (when they are inaccurate, when they were collected illegally or not following legal procedures).*

3 Blockchain Techniques

3.1 Definition of Blockchain

The concept of blockchain was explained by a 2008 paper called Satoshi Nakamoto [6]. Any overview of blockchain technology must commence with the observation that there is not one 'blockchain technology'. Rather, blockchains (or Distributed Ledger Technology – DLT) are better seen as a class of technologies operating on a spectrum that present different technical and governance structures.

DLT is better understood as an inventive combination of existing mechanisms. Indeed, nearly all its technical components originated in academic research from the 1980s and 1990s.

The Blockchain is a technology that "can define a framework of transparency, reduce corruption, detect tax evasion, allow the traceability of illicit payments, facilitate anti-money laundering policies and identify the misappropriation of assets" because it is able to memorize all transactions in blocks connected to each other in chronological order to ensure data integrity. The pillars of this technology are, therefore, the immutability and transparency of data.

The Blockchain, literally "chain of blocks", is a digital register structured as a chain of blocks, concatenated in chronological order, capable of storing data records more commonly called "transactions". The integrity of the blocks is guaranteed using cryptography and one or more transactions can be associated with a block. Furthermore, each block contains a hash pointer linking it to the previous one and a timestamp.

With a previous block hash contained in the block header, a block has only one parent block. It is worth noting that uncle blocks (children of the block's ancestors) hashes would also be stored in Ethereum blockchain. The first block of a blockchain is called genesis block which has no parent block. We then explain the internals of blockchain in details (see Fig. 1) [7].

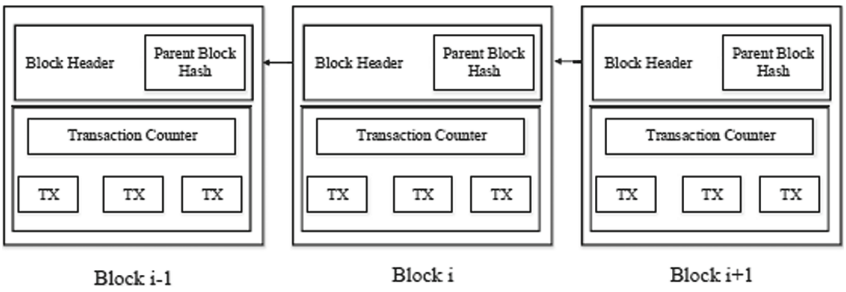

Fig. 1. An example of blockchain which consists of a continuous sequence of blocks [7]

The blockchain is, essentially, an archive divided into different nodes, hierarchically organized: each node can only access certain information and can, if necessary, modify it only by respecting precise and stringent conditions.

In most modern applications and services, the entire system's control lies in the hands of a centralized authority that manages and takes decisions regarding the data being handled [8]. A blockchain enables the decentralization of this control over a network. The blocks are validated using the means of cryptographic hash functions. Each block contains a hashed link to the previous valid block, and this link allows anyone to traverse back through the chain and verify a transaction in the history [9].

The essential components of the blockchain:

- Nodes: are the participants in the blockchain, and are physically made up of the servers of each participant.
- Transaction: consists of data representing the values subject to "exchange" that need to be verified, approved, and archived.
- Block: it is represented by the grouping of a set of transactions that are merged to be verified, approved, and then archived by the participants in the blockchain.
- Ledger: it is the public register in which all transactions carried out in an orderly and sequential manner are "annotated" with the utmost transparency and in an immutable way. The Ledger consists of a set of blocks that are chained together through an encryption function thanks to the use of hashes.
- Hash: a (non-reversible) operation that allows you to map a text and/or numeric string of variable length into a unique and univocal string of a given length. The

Hash uniquely and securely identifies each block. A hash must not allow the text that generated it to be traced back.Nodes or blocks can be of three types:

1. Genesis block/node: it is the hierarchically higher block, from which all the data is made available to the lower blocks;
2. Blocks of the main chain: these are the blocks that are "allowed" to access, use or modify certain information;
3. Orphaned blocks: are blocks that have not been selected for inclusion in a chain.

The data saved on the Blockchain are for this reason considered incorruptible. Each piece of data to be inserted into a block, and consequently each block to become part of a chain, is subjected to a validation process, called mining, in which anyone can participate.

In essence, a blockchain is a shared and synchronized digital database that is maintained by a consensus algorithm and stored on multiple nodes (computers that store a local version of the database).

3.2 Features and Benefits of Blockchain

The main features are:

- Digitization: all transactions are in digital format
- Decentralization: the information contained in the digital register is distributed among multiple nodes (computers that connect to the Blockchain) to ensure computer security so that there is no centralization that the cracker (computer pirate) can exploit to bring down the entire system. The Blockchain also uses public key and private key cryptography;
- Traceability: each element saved in the register is traceable in all its parts and this makes it possible to trace the exact origin and any changes made over time;
- Disintermediation: the individual nodes of the Blockchain certify the distributed information, thus making the presence of central bodies or companies for data certification completely useless;
- Transparency and Verifiability: the contents of the register are visible to all and can be easily consulted and verified. This means that no one can hide or change data without the entire network knowing;
- Immutability of the register: after adding information to the register it is no longer possible to modify it without the consent of the whole network;
- Programmability of transfers: transaction operations can also be programmed over time, so as to be able to wait for certain conditions to occur before proceeding with entry or modification.

The main advantages of systems developed with Blockchain technologies are the possibility of creating a decentralized, shared and immutable archive since, as a rule, its content once written can no longer be modified or eliminated, unless the entire structure.

3.3 Blockchain Technologies for Public Health

Blockchain can also be seen as an agreement convergence algorithm, ensuring that data from books distributed across each node is always present among large nodes. This

ability enables nodes to run anonymously, to have poor connections, or even to involve unreliable operators (see Fig. 2).

Blockchain has many algorithms. We want to apply the health information blockchain using the HyperPORalgorithm, which is an agreement algorithm among public blockchains. The reason for using the Hyper POR algorithm is that these medical data will become a PHR (Personal Health Record) in the future, requiring many TPS (Translations Per Second) if many data are used. This is because many TPS performance data are required to authenticate these blockchains. Therefore, the health information blockchain needs a high-performance consensus algorithm [10].

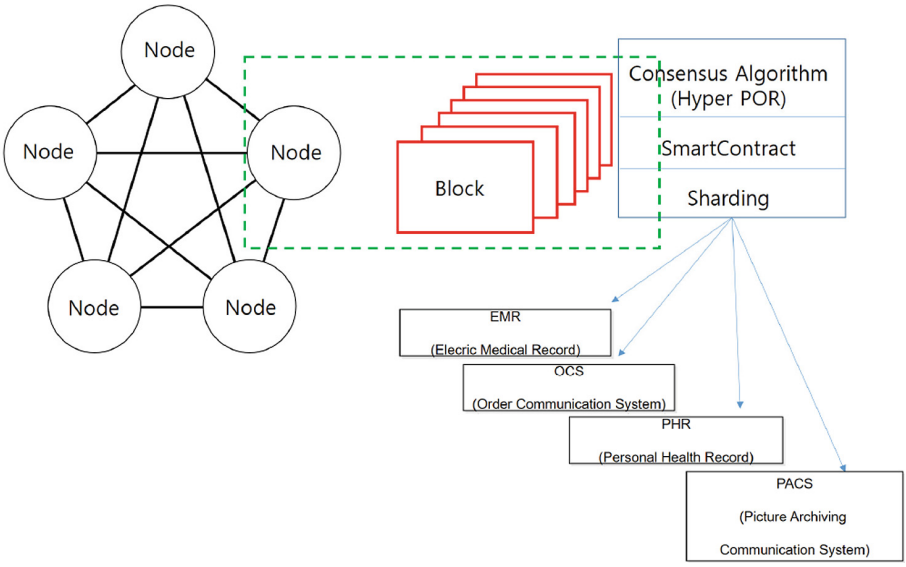

Fig. 2. Blockchain algorithm for healthcare [9]

Different studies suggest the application of blockchain in the health sector mainly for sharing and better management of patient's data, electronic health records (EHR) and, if less frequently, the supply chain management of medical devices and drugs, the management of drug prescriptions, to improve the scientific research and the divulging of scientific knowledge, and for the development of precision medicine [10–16].

Blockchain technology provides numerous benefits to medical researchers, health care providers, and individuals [12,17]. It would serve research as well as personalized medicine to create a single storage location for all health data, track personalized data in real-time and set data access permissions at a granular level [18]. Health researchers need comprehensive data sets to advance understanding of disease, accelerate biomedical discovery, track the development of drugs quickly, and design individual treatment plans based on genetics, lifecycle, and environment [19]. By including patients of different ethnic and socio-economic backgrounds and from different geographic areas, the shared data system of Blockchain would provide a wide range of data set [20, 21]. It provides

perfect information for longitudinal studies because blockchain collects health data over the lifetime of a person [22].

4 Application of the European Data Protection Law (GDPR) to the Blockchain

4.1 Introduction

In recent years, multiple points of tension between blockchain technologies and the GDPR have been identified.

First, the GDPR relies on the basic assumption that there is at least one natural or legal person - the controller - to whom data subjects can turn to enforce their rights under EU data protection law. Data (accountability). Blockchains, however, often seek to achieve decentralization by replacing one unitary actor with many different actors.

Secondly, the GDPR is based on the assumption that data can be modified or deleted where necessary to comply with legal requirements such as Articles 16 and 17 of the GDPR. Blockchains, however, make such data modifications deliberately onerous to ensure data integrity and increase trust in the network (right of the data subject).

Another element of tension between blockchain and GDPR concerns the general principles of data minimization and purpose limitation. While the GDPR requires that personal data processed be kept to a minimum and processed only for purposes specified in advance, these principles can be difficult to apply to blockchain technologies.

Further complexity also relates to the difficulty in determining whether data that was once personal data can be sufficiently anonymized to meet the GDPR's "anonymization" and "pseudonymization".

4.2 Identification of the Data Controller

The first problem that arises concerns the identification of the data controller in the blockchain. The principle of accountability designated by the GDPR is relevant not only in the event of a violation of the law but also in the preventive phase, in which it is up to the owner to choose the "technical and organizational measures" useful for avoiding external tampering.

To identify the data controller in the blockchains, it is necessary to go back to the distinction between private and public. In the former, it would seem easier to identify a data controller, since access is linked to the authorization of certain subjects. Therefore, a sort of centralized government would be replicated that goes well with the prototype designed by the GDPR. The case of permissionless blockchains is different and more complex, where everyone can participate and interact without constraints (peer-to-peer scheme) and it is not possible to find a single control point of the network.

The thesis of those who claim that the data controllers could be the developers of the protocol can easily be overcome: these, in fact, only deal with building a technological infrastructure for other users. According to others, the figure of the data controller would be incorporated by all the nodes of the network: precisely, the node that enters data into the network would incorporate both the user and the data controller, while, if it limits

itself to receiving such data, it would respond only in manager quality. Even this thesis does not remain free from criticisms, mainly concerning the impossibility of fulfilling the principle of accountability in the absence of tools that allow monitoring the use of data.

Finally, some argue that the data controllers are not the nodes, but the users (those who carry out the transactions). In this case, if the user uses the blockchain for personal purposes (not commercial activities) the GDPR under Article 2, paragraph 2, letter c should not apply.

4.3 Rights of the Interested Party

As announced, there are other issues to be examined in the relationship with the blockchain those concerning the founding principles of the Regulation (article 5) and some rights recognized by the interested party.

The first principle is composite since it includes the principles of legality, fairness, and transparency. This assumes that the data controller must have legitimate reasons to collect the data, treating them transparently and without committing illegal activities. If transparency is certainly satisfied in the blockchain, the same cannot be said about the principle of legality, since a user is lawful only when one of the conditions of Article 6 exists. If we take the example of consent, it is natural to ask ourselves who gives consent to the user when it is still uncertain who is the data controller.

Furthermore, they must be "exact, and if necessary, updated" and the owner must implement all suitable measures to promptly modify/cancel the data when this is requested by the interested party. Also in this case, it is not difficult to imagine an incompatibility with the blockchain, given that it is characterized by being a system of adding only, whereby data (even incorrect) remains permanently on all blocks of the chain, without the possibility of modification or cancellation.

The blockchain, by its nature, is destined to grow and cannot regress in any way, and it is precisely the immutability of the data that justifies trust in the network. The non-modifiability of the information is in direct contrast with the data subject's right to rectification and integration. Even if the difficulties in identifying the owner were overcome, this could not in any way modify the block chain. At most, new blocks with adjusted data could be added.

4.4 Data Minimization

The principle of data minimization provides that these are "adequate, relevant and limited" and used only for the stated purposes.

In order to be lawful, and therefore permitted, the processing of "personal data" must be limited only to data that is indispensable, pertinent and limited to what is necessary for the pursuit of the purposes for which they are collected and processed. The reference to the purposes of the collection makes it necessary, from time to time, to ascertain what is the purpose that the Data Controller sets for himself when requesting personal data from the interested parties, since the consent of the latter is, precisely, linked to this sole purpose, and use for different purposes would be excessive and irrelevant.

A collection of data is excessive when it is excessive, exaggerated in numerical terms, too vast with respect to the intention of the person collecting the information; it is irrelevant when it is not linked to the objective to be achieved, it does not serve the pre-established purpose, in summary, it is superfluous.

Only by taking the purpose into consideration is it therefore possible to establish whether the collected data comply with the conditions of lawfulness pursuant to Art. 6 of the GDPR (i.e. if they respect specific, explicit and legitimate purposes), and if their collection is strictly necessary to achieve the set purpose.

4.5 Anonymization and Pseudonymization of Data

Data can be considered anonymous when people are no longer identifiable. However, it should be remembered that a person does not have to be named to be identifiable. In fact, there is a lot of other information that allows an individual to be linked to his personal data and therefore allows him to be identified.

The GDPR, however, does not prescribe any particular technique for anonymization; it is therefore up to individual data controllers to ensure that any anonymization process chosen is robust enough.

On the contrary, it provides that "personal data subjected to pseudonymization, which could be attributed to a natural person through the use of additional information, should be considered as information about an identifiable natural person". Pseudonymization is thus defined as "the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is kept separately and subject to technical measures and organizational arrangements designed to ensure that such personal data are not attributed to an identified or identifiable natural person".

The subtle difference between anonymization and pseudonymization has made determining suitable techniques difficult in practice, as demonstrated by several examples of incomplete or incorrectly conducted anonymization processes which ultimately led to the re-identification of individuals.

5 Conclusions

The paper has given a brief overview of how the blockchain system works and the different layers present in the design.

From the analysis just conducted, it has been highlighted that the blockchain is a technology, by definition, incapable of forgetting and resistant to censorship thanks to its widespread data archiving model. It is precisely these characteristics that have determined its rise in recent years, combined with its profound versatility, which makes it suitable for use in many fields.

In recent years we have also seen growing attention toward other needs, equally important and closely connected to the advance of innovation. The protection of personal data is in fact a European (and national) priority even prior to the creation of Nakamoto, which led to the emergence of problems on the applicability of European legislation to

this technological infrastructure and determined the need to find coordination between this and the current regulatory model.

Although some aspects and some rights recognized by the Regulation are not easy to implement, it is clear that there is room for maneuvering to make the blockchain compliant with the requests of the GDPR. Moreover, it must not be forgotten that this regulation and the blockchain have the potential to provide the data subject/user with greater control over their data.

The challenge that awaits us in the coming years concerns the need to find a balance between two European and national needs: to support innovation without forcing it into an inflexible regulatory framework and at the same time guarantee the protection of personal data, including in the face of the advance of new technologies.

In conclusion, it cannot be said that this technology is absolutely incompatible with current data protection legislation, but rather that the use made of it so far has been difficult to coordinate in some cases and for some aspects. However, as already stated, given the enormous potential that exists in the blockchain field, we hope that the legislator will work in this direction.

References

1. European Parliament Report on Blockchain: a Forward-Looking Trade Policy (AB-0407/2018), 27 November 2018. Para 14. http://www.europarl.europa.eu/doceo/document/A-8-2018-0407_EN.html
2. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., Wang, H.: Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. **14**, 352–375 (2018)
3. Yaeger, K., Martini, M., Rasouli, J., Costa, A.: Emerging blockchain technology solutions for modern healthcare infrastructure. J. Sci. Innov. Med. **2**, 1–7 (2019). https://doi.org/10.29024/jsim.7
4. Kumar R, Arjunaditya, Singh D, Srinivasan K, Hu Y-C.: AI-powered blockchain technology for public health: a contemporary review, open challenges, and future research directions. Healthcare **11**(1), 81 (2023). https://doi.org/10.3390/healthcare11010081
5. McGhin, T., Choo, K.K.R., Liu, C.Z., He, D.: Blockchain in healthcare applications: research challenges and opportunities. J. Netw. Comput. Appl. **135**, 62–75 (2019)
6. Macdonald, M., Liu-Thorrold, L., Julien, R.: The blockchain: a comparison of platforms and their uses beyond bitcoin; COMS4507-Adv; Computer and Network Security, Queensland, Australia (2017). [Google Scholar]
7. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: architecture, consensus, and future trends. In: Proceedingso of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, 25–30 June 2017, pp. 557–564 (2017). https://doi.org/10.1109/BigDataCongress.2017.85
8. Bodkhe, U., et al.: Blockchain for industry 4.0: a comprehensive review. IEEE Access **8**, 79764–79800 (2020). https://doi.org/10.1109/ACCESS.2020.2988579
9. Nofer, M., Gomber, P., Hinz, O., Schiereck, D.: Blockchain. Bus. Inf. Syst. Eng. **59**(3), 183–187 (2017). https://doi.org/10.1007/s12599-017-0467-3
10. Kim, S.-K., Huh, J.-H.: Artificial neural network blockchain techniques for healthcare system: focusing on the personal health records. Electronics **9**, 763 (2020). https://doi.org/10.3390/electronics9050763
11. Fusco, A., Dicuonzo, G., Dell'Atti, V., Tatullo, M.: Blockchain in healthcare: insights on COVID-19. Int. J. Environ. Res. Public Health **17**(19), 7167 (2020). https://doi.org/10.3390/ijerph17197167.PMID:33007951;PMCID:PMC7579329

12. Kuo, T.T., Kim, H.E., Ohno-Machado, L.: Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inform. Assoc. **24**, 1211–1220 (2017). https://doi.org/10.1093/jamia/ocx068
13. Khatoon, A.: A blockchain-based smart contract system for healthcare management. Electronics **9**, 94 (2020). https://doi.org/10.3390/electronics9010094
14. Hoolbl, M., Kompara, M., Kamissalic, A., Zlatolas, L.N.: A systematic review of the use of blockchain in healthcare. Symmetry. **10**, 470 (2018). https://doi.org/10.3390/sym10100470
15. Clauson, K.A., Breeden, E.A., Davidson, C., Mackey, T.K.: Leveraging blockchain technology to enhance supply chain management in healthcare: an exploration of challenges and opportunities in the health supply chain. Blockchain Healthc. Today **1**, 1–12 (2018)
16. Mackey, T.K., et al.: 'Fit-for-purpose?'—Challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Med. **17**, 68 (2019). https://doi.org/10.1186/s12916-019-1296-7
17. Carson, B., Romanelli, G., Walsh, P., Zhumaev, A.: Blockchain Beyond the Hype: What Is the Strategic Business Value. McKinsey & Company (2018). https://www.mckinsey.com/business-functions/mckinsey-digital/ourinsights/blockchain-beyond-the-hype-what-is-the-strategic-business-value. Accessed 31 Dec 2019
18. Randall, D., Goel, P., Abujamra, R.: Blockchain applications and use cases in health information technology. J. Health Med. Inform. **8**, 2 (2017)
19. Kshetri, N.: Blockchain and electronic healthcare records. Computer **51**, 59–63 (2018)
20. Brennan, B.: Blockchain HIE overview: a framework for healthcare interoperability. Telehealth Med. Today **2**, 3 (2017)
21. Radanović, I., Likić, R.: Opportunities for use of blockchain technology in medicine. Appl. Health Econ. Health Policy **16**, 583–590 (2018)
22. Dimitrov, D.V.: Blockchain applications for healthcare data management. Healthc. Inform. Res. **25**, 51–56 (2019)