Analysis on the Impact of GDPR in Healthcare-related Blockchain Solutions and Guidelines for Achieving Compliance

Christos Kontzinos
Decision Support Systems Lab
National Technical University of Athens
Athens, Greece
e-mail: ckon@epu.ntua.gr

Ourania Markaki
Decision Support Systems Lab
National Technical University of Athens
Athens, Greece
e-mail: omarkaki@epu.ntua.gr

Panagiotis Kapsalis
Decision Support Systems Lab
National Technical University of Athens
Athens, Greece
e-mail: pkapsalis@epu.ntua.gr

Dimitris Askounis
Decision Support Systems Lab
National Technical University of Athens
Athens, Greece
e-mail: askous@epu.ntua.gr

Spiros Mouzakitis
Decision Support Systems Lab
National Technical University of Athens
Athens, Greece
e-mail: smouzakitis@epu.ntua.gr

Haralampos Karanikas
Datamed S.A.
Athens, Greece
e-mail: h.karanikas@gmail.com

Michael Kontoulis
Decision Support Systems Lab
National Technical University of Athens
Athens, Greece
e-mail: mkontoulis@epu.ntua.gr

Alexandros Christodoulakis
Datamed S.A.
Athens, Greece
e-mail: alexandroschristodoulakis8@gmail.com

Panagiotis Dimitrakopoulos
Datamed S.A.
Athens, Greece
e-mail: pdimitrakopoulos@datamed.gr

Abstract—**Blockchain is an emerging technology that offers decentralised data management capabilities in a distributed ledger. While the initial and main domain of application has been and continues to be that of cryptocurrencies and their use in secure, digital economic transactions, blockchain's inherent properties for security, immutability and transparency make it an excellent solution for various domains that deal with personal or even sensitive data such as the domain of healthcare. At the same time, the radical increase of digitisation in healthcare, as well as automation of processes, robotics, and the rise of medical sensors and devices also led to an unprecedented rise in medical data availability. This fact has brought forth citizen and societal concerns regarding the safety of their medical data and the transparency of data transactions that they engage in, especially given that medical data are sensitive. To address these and other concerns, in the European Union, the European Commission established in 2016 that General Data Protection Regulation (GDPR) to establish user rights concerning their data as well as set out the obligations of an organisation that is responsible for storing, managing and processing said data. Some of the articles of the GDPR, while integral to safeguard a user's rights, are opposite to the technical capabilities of innovative technologies, blockchain being one of them. The scope of this publication is to present blockchain, describe its potential in the healthcare domain, list limitations between blockchain and the GDPR, and finally provide guidelines to reconcile the two, acting as a roadmap for researchers and organisations who are developing blockchain applications in healthcare and other domains.**

Keywords-blockchain; healthcare; GDPR; sensitive data; patient rights.

I. INTRODUCTION

Blockchain is a technology that enables decentralised data management in a distributed ledger [1, 2]. It consists of a number of blocks, which are interconnected and represent a set of transactions [3]. The structure of blockchain involves the distribution of a ledger's blocks in a number of peer-to-peer nodes of a given data infrastructure instead of being stored centrally [4]. Each block, in addition to the data stored in it, contains a cryptographic hash, the hash of the previous block, and the timestamp of its creation. A hash is generated with the help of cryptographic hash functions and is the representation of the block data as it is directly dependant on them. For this reason, it can be used to verify the integrity of data transactions contained in each block. In addition, the hash of each block depends on the hash of the previous block in the chain, which essentially makes the entire blockchain ledger immutable, given that any change to a block will change the hash, not only of that block but of all following

 ISBN: 978-1-61208-763-4

blocks as well. In addition, blockchain is not managed by a central authority, and maintains the integrity of the transaction history in the system through consent algorithms that require some form of network majority to validate and accept a system change. Consequently, blockchain solutions empower the users by providing them not only with the capability to manage and share their data as they see fit but also with voting rights that are important to achieve network consensus.

Blockchain first appeared in 2008 and has become widely known for its use as a public account for cryptocurrencies such as bitcoin and Ethereum. Nevertheless, it can also be used in other domains to create permanent, public, and transparent data management systems [5]. In fact, in recent years, the added value of blockchain has been realised by the research community and various organisations that propose and develop innovative solutions in areas other than cryptocurrencies such as health, education, public administration, and supply chains among others. Regardless of the scope of the application, the general operation of a blockchain can be seen in Figure 1.

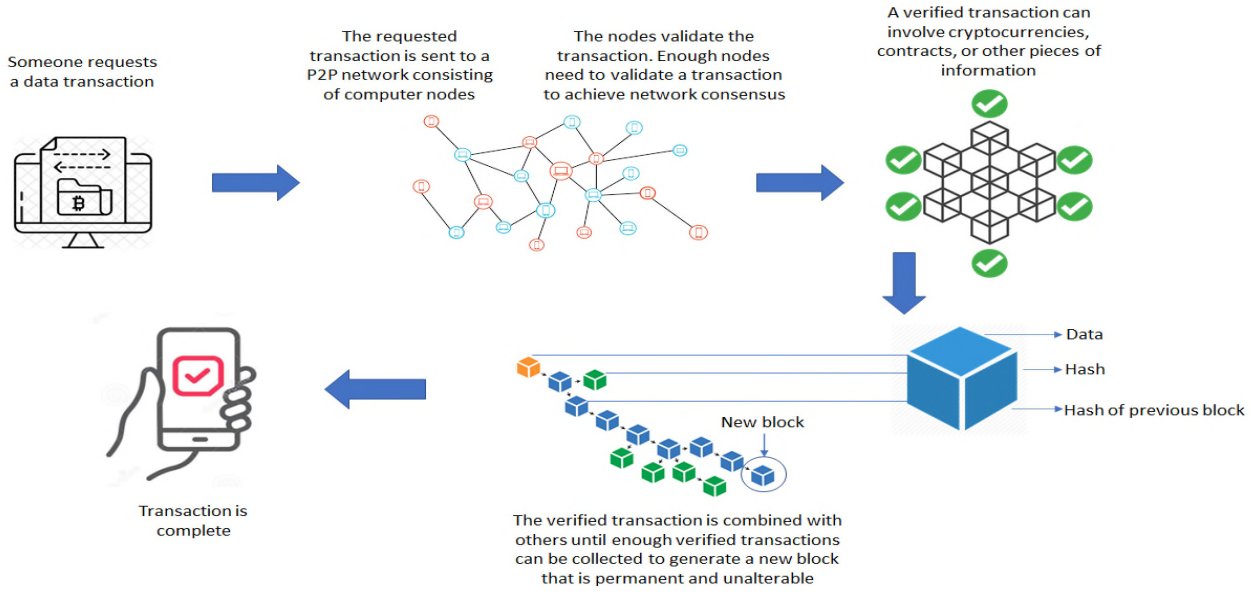

Figure 1. High level operation of a blockchain.

It is widely accepted that blockchain can be an effective and most importantly secure solution in any field involving data transactions. Smart contracts (contracts that can be executed/implemented partially or completely without human interaction) also play a big role not only in providing data protection but also by adding a degree of automation in the management and validation of transactions in the system [6]. Given that in the general case of an open, public blockchain, users have ownership of their data, smart contracts are used to help them define the rights (access, sharing, processing rights etc.) that third party users have on specific pieces of data. Overall, blockchain networks ensure continuous availability, reliability, security, durability, and integrity in a given network or system [4]. The main reason that allows blockchain to have such a wide scope is that at any time, network users can know the system status. To increase security and trust in the network, blockchain includes various mechanisms through which a transaction is secured [4], the main ones being the proof of existence and non-existence (it can be easily verified with certainty if an item exists in the system), the proof of time (when information is stored in the blockchain, the time at which it was added is also stored as part of the transaction's metadata), the proof of order (in case of network congestion, the order in which some requests/transactions were made is stored as well), the proof of authorship (data entries in the blockchain include details of the user who added them) and the proof of ownership (the owner of a specific item is always known).

The main scope of this publication is to present the potential of blockchain for developing secure data management systems in the domain of healthcare, address legal, ethical and societal challenges and obligations and provide guidelines for the development of not only secure but legally compliant blockchain solutions when it comes to managing sensitive medical data.

Section I provides the introduction to the document, explains in short, the operation of a generic blockchain system and describes the scope of the publication. Section II includes a bibliographic research on the potential of blockchain systems in healthcare and describes the current European and national legislations that impact the development of blockchain solutions. Section III lists successful practices and provides guidelines for the development of ethical blockchain systems. Finally, Section IV concludes the document and provides ideas for future work.

 ISBN: 978-1-61208-763-4

II. BLOCKCHAIN IN HEALTH AND GDPR COMPLIANCE

A. *Blockchain in Healthcare*

Blockchain is an emerging technology that can be applied in various domains. In healthcare, blockchain's inherent properties for security, immutability, decentralisation, and transparency can help reengineer many everyday processes for both patients and healthcare practitioners, as well as develop and implement more innovative and effective ICT healthcare systems. Blockchain can initially be used as a database, given that in traditional medical/hospital systems, efficient and secure data management comes with high installation and maintenance costs to ensure data safety when it comes to sensitive medical data. This fact can also result in ineffective communication and coordination among systems of different healthcare providers (lack of trust when it comes to data sharing), leading to patients having their medical data split among various ICT platforms in fragmented form. Blockchain significantly reduces these problems by ensuring data integrity and maintainability across all devices and systems connected to the network, since every data transaction leaves a digital trail, thus ensuring visibility of actions, while also reducing the possibility of system malfunction, due to the fact that there is no central point of failure. In other words, in a blockchain network, the creation of a new block of data (which represents a specific number of data transactions) must follow specific rules, usually hardcoded in the system and governed by smart contracts and must also achieve system consensus to be included in the ledger. Blockchain makes users responsible for their data, by also allowing them to define the access rights of third parties to it. Giving control of the data back to the patients and the users of the network and not only to healthcare organisations, ensures their correct use (existence of greater transparency and increased security). As such, blockchain systems are more secure against attacks and eavesdropping, so cases of malicious use are virtually impossible [7].

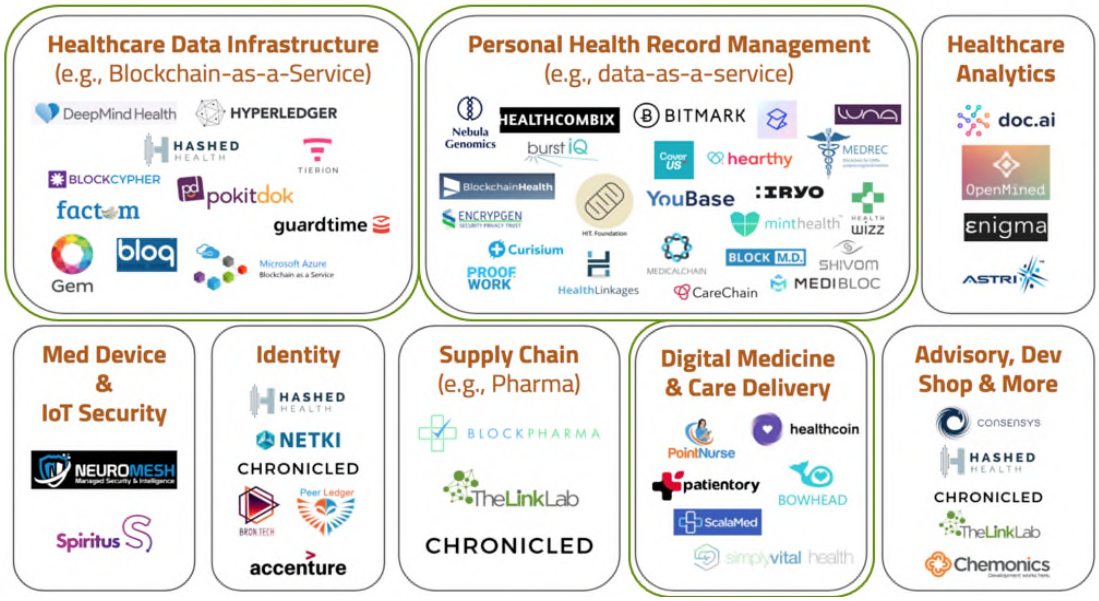

Figure 2. Blockchain Projects and Initiatives in Healthcare [11].

In modern healthcare, the prevailing standard for health data management is the Electronic Health Record or EHR, which represents the amalgamation of health and medical data concerning a patient in digital form. Nevertheless, the low degree of digitisation in the sector, in combination with the increased costs for the adoption of EHR systems hinders their widespread use and implementation in more medical processes. It is considered that the introduction of EHRs in blockchain-based medical platforms could increase overall data interoperability in the domain, and improve communication and coordination among heterogeneous healthcare providers, in addition to reducing costs for managing security and data governance issues [8]. Blockchain offers a robust infrastructure and an additional level of security that can be implemented with no extra cost, compared to traditional systems. This allows the development of value-adding applications and services on top of the blockchain ledger that can in turn facilitate mass analyses of medical data, freeform queries on a patient's data, personalisation of a patient's profile, notifications etc. In traditional systems, such applications usually operate in the isolated ICT environment of each respective healthcare provider to minimise security risks, while analysis of patients' data requires their informed consent. Such issues are minimised when patients have control over their data and decide who can have access to them and for what purpose. Moreover, every action that requires blockchain data leaves a digital trail, thus increasing overall transparency and trust in the system and its stakeholders. Another innovative concept when it comes to blockchain in healthcare, includes the use of cryptocurrencies (peer-to-peer decentralised electronic form of money, which is based on cryptographic principles

 ISBN: 978-1-61208-763-4

to ensure network security and authenticate transactions) [9] to facilitate economic transactions in the network. Companies, such as Bowhead Health, have developed such platforms, where users can make their data available to researchers and receive cryptocurrencies as compensation [10]. Finally, blockchain can be used to combat counterfeit drugs and prescriptions. Applying blockchain principles to the pharmaceutical supply chains (usually in conjunction with Internet of Things devices, such as sensors and surveillance systems) increases visibility and reliability throughout the life cycle of a drug. The increased interest in the healthcare domain for blockchain solutions is evident by the sheer number of initiatives and applications, as shown in Figure 2.

B. GDPR and National Legislations

The General Data Protection Regulation (GDPR) 2016/679 [12] is a piece of legislation that was developed to safeguard data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also governs the export of personal data outside of the EU and EEA regions. The GDPR is primarily intended to give individuals control over their personal data and to simplify the rules of compliance for international companies by consolidating regulations within the EU [13]. It was issued on 14 April 2016 and entered into force on 25 May 2018 [14].

According to the GDPR, personal data is defined as information that describes an individual, such as identification, physical characteristics, education, employment, financial status, interests, activities, and habits among others. In addition, the personal data of a person referring to his/her racial or ethnic origin, political views, religious or philosophical beliefs, medical records or health status, social welfare, love life, criminal prosecution, convictions as well as participation in associations/ organisations related to the above are characterised as sensitive. Sensitive data is protected by law with stricter regulations compared to personal data [15] and cannot be used to identify or profile an individual. According to the GDPR, citizens have a number of rights [16] with regard to their personal data, the most important of which are the rights to information, access, correction, deletion, objection, notification, automatic decision making and data portability. To ensure compliance with the above, according to the GDPR, the management of personal data by companies and other organisations should be explicitly defined and governed by specific principles [17].

To begin with, organisations must ensure beyond any reasonable doubt that there are legitimate reasons for collecting and using personal data by obtaining the informed consent of their clients for such purposes. In addition, and regarding data processing, companies must ensure that they accurately store only the data that is necessary for the purpose of the processing for which consent has been obtained (data minimisation principle). The explicit consent of individuals is also required for the transfer and processing of their data by third parties. For this reason, consent forms are used, which state in detail the purposes of data collection, as well as the processing they will undergo. To comply with the above, the GDPR recommends that organisations appoint a data protection officer (DPO), who acts as a single point of contact between customers, the organisation and supervising authorities and provides advice on security measures. and data protection policies. Finally, the GDPR recommends conducting a data protection impact assessment (DPIA) to identify and manage potential threats to personal data, especially in systems that implement innovative/emerging technologies in traditional systems.

As already mentioned, according to the GDPR, medical information about a person is considered as sensitive personal data. As such, it is a given that organisations active in the health sector are responsible for storing and processing medical data by following the basic provisions of the GDPR. However, in most countries of the EU there are some additional fundamental rights regarding patient data, which are defined by national legislations and must be respected by organisations that operate in said countries. For example, in the Greek legislation, according to article 12 of Law 2472/ 97 [18], patients have the right to access their data and receive their official medical files, certified from the healthcare facility where they have been treated. In addition, law 3418/2005 [19] regulates the conditions for granting access rights to a patient's medical record to a relative. This right of access is allowed only in exceptional cases, in which the third party acts as a legal representative, has an official written authorisation, or to protect the vital interests of patients in cases that they are unable to provide their consent (e.g., a patient has lost consciousness). On the other hand, medical professionals, especially when they also act as data controllers, have the obligation to report accidental or illegal damage, loss, alteration, and disclosure (unauthorised) of data to the respective supervisory authorities. To comply with the aforementioned rights and obligations, data controllers must provide patients with the relevant documents that describe the respective regulations and ensure they have their explicit and informed consent (temporary or permanent) for processing their data.

III. ACHIEVING GDPR COMPLIANCE IN BLOCKCHAIN PROJECTS AND INITIATIVES

GDPR compliance when it comes to blockchain, concerns the way that this technology is used in various cases and applications and is considered to be a critical issue for the European Commission. Therefore, there are some important issues that need to be addressed, under the GDPR, regarding the protection of personal data in a blockchain. In particular, the structure and storage of data in a blockchain network is done in such a way that it does not allow the deletion or correction of data once it is registered in the chain, according to the immutability property. Therefore, even if the controller of a network can be identified, it becomes impossible for that controller to delete or update the file of a transaction without irreversibly damaging the blockchain ledger, since the hash of each block (which is representative of the data in the block) is also dependent on the hash of the previous block. In other words, blockchain is built entirely on the assurance that transactions will never be

 ISBN: 978-1-61208-763-4

forgotten or deleted, aiming to build decentralised trust as well as develop and expand the network of participants.

Nevertheless, the correction and deletion of personal data are two basic rights provided to data owners by the GDPR. To comply with GDPR provisions, organisations developing blockchain applications employ various encryption techniques, in combination with the destruction of the key that provides access to the blockchain data. Another technique that is widely used is the storage of data in central databases and the use of blockchain to store and verify transactions between users of the system, thus minimising the security and privacy risks arising from the need to respect GDPR regulations. Especially regarding the right to be forgotten, non-blockchain storage allows deletion of user data. The fact that the data cannot be deleted from the blockchain does not affect the system in this case, since after data deletion from the centralised storage the only data remaining in the blockchain are the hashes of the transactions, which cannot lead to the identification of the user (especially since the data to which the hashes point have been deleted). The same is true in networks where data storage is done in a decentralised manner, such as in a private cloud or the mobile device of each user.

The aforementioned GDPR obligations do not mean that blockchain is an ineffective solution that is hard to implement and maintain in healthcare ICT systems. In Section II, it was explained that blockchain can actually solve most current challenges and shortcomings. In fact, in a way, blockchain and the GDPR are similar as they both focus on empowering the user and increasing visibility, data privacy and security. The only issue when it comes to developing GDPR-compliant blockchain systems is that of data deletion/correction and that can be bypassed as already explained. However, the fact of the matter remains that blockchain is an emerging technology and its implementation in domains other than cryptocurrencies is relatively new. One the one hand, this means that users and stakeholders of blockchain systems are largely unfamiliar with the technology and oftentimes suspicious of its attributes, which makes sense as the actual algorithmic part that ensures security in a blockchain is not easy to comprehend. On the other hand, and given that non-cryptocurrency blockchains are just now emerging, the technical specifications of implementing such systems have not yet been specified for each distinct domain in a way that ensures legal and ethical compliance and at the same time maximises the effectiveness of the technology. This should be viewed as an opportunity to set out the legal and ethical requirements that must be met in such cases and create roadmaps that will guide blockchain development efforts in the future. While, different areas of implementation have their own requirements and require different roadmaps, the consolidation of legal and ethical obligations by the GDPR means that knowledge generated for a given domain may be transferred and applied in other domains as well.

As such, in healthcare-related blockchain projects the following actions are deemed as necessary to guide the efforts for achieving GDPR compliance.

1. Informed consent: Blockchain initiatives must draft informed consent forms that set out the rights of patients and the legal obligations of the data controller and participating organisations. If user data populate the system, the consent form must explicitly explain the reasons for data gathering and ensure that those reasons are grounded on a legal basis. The same is true for the analysis of user data and their use by third parties.
2. Data Protection Impact Assessment (DPIA): While there are a number of prerequisites that define whether a DPIA must be performed, in healthcare blockchains that deal with sensitive data, a DPIA is considered necessary in almost all cases. The DPIA is an excellent opportunity for blockchain initiatives to pinpoint potential risks and explain how such risks will be resolved. It is imperative to note that a DPIA must be exhaustive when it comes to data privacy risks. For example, even if malicious attacks in a blockchain system are almost impossible, this risk should still be mentioned in a DPIA along with the explanation of how blockchain maintains system security. This should also be seen as an opportunity to educate non-technical stakeholders and legal entities on blockchain's properties and steadily increase trust in the technology.
3. Appointment of a DPO: Every blockchain development effort should have a DPO appointed. It is important that DPOs have legal backgrounds and are knowledgeable on the GDPR, since they validate the measures taken at each step and can also act as a point of contact with national and EU GDPR offices for clarifications and other matters.
4. Privacy-by-design: It is important that the privacy by design principle is followed when developing a medical blockchain, meaning that all security measures must be set out from the start, before the system is implemented. In a medical blockchain, the privacy-by-design principle sets out the following conditions/measures:
    a. Non-blockchain storage: To comply with the users' right of data deletion, all personal and sensitive data must be stored in non-blockchain repositories. In that case, the blockchain adds an additional level of security in the system as it validates all data transactions. In that case, the non-blockchain solutions that may be used by patients for data storage (e.g., cloud, IPFS, mobile devices) must also be set out from the beginning.
    b. Anonymisation/pseudonymisation: Despite the security offered by blockchain, it is considered a good practice to anonymise/pseudonymise personal and sensitive data that can lead to a user's identification.
    c. Patients' rights: It is important that all legal requirements that concern patient rights on their data (access, sharing, deletion etc.) are set out before development starts. This usually entails researching the legal and ethical landscape, stakeholder interviews etc. When such legal requirements are set out, they can be

 ISBN: 978-1-61208-763-4

programmed in smart contracts, which are used to verify whether a data transaction can be performed.

It can be surmised from the above that GDPR compliance requires informed consent, risk assessment, and the design of all security measures before development starts. In addition, blockchain initiatives and consortia should periodically assess the legal and ethical landscape to uncover changes or updates in the respective legislation or even innovative approaches that facilitate compliance.

IV. CONCLUSIONS AND NEXT STEPS

The scope of this publication was to showcase blockchain as an emerging technology that can facilitate the reengineering of data governance practices in healthcare, as well as assess the respective legal and ethical landscape so that guidelines for compliance can be generated. All in all, it can be surmised that the GDPR is not a piece of legislation aiming to create limitations for innovative technologies, but rather to set out the requirements that must be met by technical solutions to ensure privacy and security. In fact, when the GDPR came into practice, many researchers thought that the right to data deletion will mean the end for EU blockchain initiatives. However, that is not the case as it led to blockchain's role as a security infrastructure to come into the forefront of technical solutions instead of its role as a database. At the moment, the end goals of blockchain and the GDPR seem quite similar, both aiming to empower the data owner and bring forth a new age in data management. The guidelines that have been generated to achieve GDPR compliance are not hard to implement and keep track of, while the technical requirements that must be met follow the lines of effective programming practices instead of imposing hard constraints that will affect the end-result. It is imperative that in this period, researchers, legal experts and developers work together to set out roadmaps for compliance in various areas and domains. Such roadmaps will facilitate more ethical technical solutions in the future.

ACKNOWLEDGMENT

This paper was written under the context of the IMPILO project, which is funded by the Greek operational program "Competitiveness, Entrepreneurship, Innovation" - EPANEK (2014–2020), in the national action: "RESEARCH - CREATE - INNOVATE", with project code T1EDK-01382.

REFERENCES

[1] C. Esposito, A. Santis, G. Tortora, H. Chang, and K.K.R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" IEEE Cloud Computing 5, pp. 31–37, 2018.

[2] S Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", 2008. Available at: https://bitcoin.org/bitcoin.pdf.

[3] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, "A blockchain based approach to health information exchange networks." Proceedings of NIST Workshop Blockchain Healthcare, Gaithersburg, pp. 1–10, 2016.

[4] D. Drescher, "Blockchain basics: A non-technical introduction in 25 steps." 1st ed. Apress, Frankfurt, 2017.

[5] K. Kotobi and S.G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access.", ieee vehicular technology magazine 13.1, pp. 32-39, 2018.

[6] P. Franco, "Understanding bitcoin: Cryptography, engineering, and economics." 1st ed. Wiley Finance Series, New York, NY, 2014.

[7] C.C. Agbo, Q.H. Mahmoud, and J.M. Eklund, "Blockchain technology in healthcare: A systematic review." Healthcare. Multidisciplinary Digital Publishing Institute, pp. 56, 2019.

[8] A. Petre and N. Hai, "Opportunities and challenges of blockchain technology in the healthcare industry." Medecine sciences 34(10), pp. 852-856, 2018.

[9] T. Polansek, "CME, ICE prepare pricing data that could boost bitcoin". Available at: https://www.reuters.com/article/us-cme-group-bitcoin-idUSKCN0XT1G1, 2016. Accessed in August 2020.

[10] Bowhead Health, Bowhead. Available at: https://bowheadhealth.com/. Accessed in August 2020.

[11] A. Coravos, "Where are the healthcare blockchains?", Available at: https://blog.andreacoravos.com/where-are-the-healthcare-blockchains-8fcf6a3e28f8. Accessed in August 2020.

[12] European Commission, "Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016." European Commission, Brussels. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed in August 2020.

[13] Council of the European Union, "Presidency of the Council: Compromise text. Several partial general approaches have been instrumental in converging views in Council on the proposal for a General Data Protection Regulation in its entirety. The text on the Regulation which the Presidency submits for approval as a General Approach appears in annex." Brussels, 2015. Available at: https://www.swlaw.com/publications/legal-alerts/2544. Accessed in August 2020.

[14] European Parliament, "Implementation of GDPR since 25 May 2018. Available at: https://eugdpr.org/. Accessed in August 2020.

[15] Administration of Personal Data Protection, "General Data Protection Regulation." Available at: https://www.dpa.gr/portal/page?_pageid=33,213319&_dad=portal&_schema=PORTAL. Accessed in August 2020.

[16] European Commission, "General Data Protection Regulation – chapter 3." GDPR, 2016. Available at: https://gdpr-info.eu/art-3-gdpr/. Accessed in August 2020.

[17] European Commission, "General Data Protection Regulation – chapter 5." GDPR, 2016. Available at: https://gdpr-info.eu/art-5-gdpr/. Accessed in August 2020.

[18] Greek Government Gazette, "Law 2472/1997, Protection of citizens from personal data processing– Right of access (article 12). "SGG 50/A/10.4.1997. Available at: https://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal &_schema=PORTAL#12. Accessed in August 2020.

[19] Greek Government Gazette, "Law 3418/2005, Code of medical ethics." SGG 287/A/28.11.2005. Available at: http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=162,112,178,83,91,84,31,147. Accessed in August 2020.

 ISBN: 978-1-61208-763-4