New Era for Technology in Healthcare Powered by GDPR and Blockchain

O. P. Stan and L. Miclea

Abstract

The development of patients' electronic healthcare records has been hampered by bureaucracy and by heavy regulation within the medical field. Medical data recorded in a patient health records is a valuable source of information that can be used by doctors and researchers to improve the quality of healthcare and the quality of life. Medical data should be owned and controlled by the patient instead of being scattered in different healthcare systems that does not support transfer and semantic interoperability between different healthcare providers. Blockchain technology has demonstrated in the financial field that it is possible to create a safe, secure and auditable mechanism by using a decentralized network along with a public ledger. But with the adoption of the newly General Data Protection Regulation, all technological advances discovered by the Blockchain are now blocked. In this paper we present the main aspect of the GDPR and Blockchain technology in healthcare and a way in which this two can work together.

Keywords

GDPR • Blockchain • Personal data • Information governance • Medical informatics system

1 Introduction

The information's stored in an electronic healthcare record are sensitive and critical data used to diagnose and to provide the best treatment a patient can have. Throughout a life time, a patient can visit several medical units or hospitals, and doctors, in order to provide the best medical services, must have access to the entire history of a patient.

If the patient has to share its clinical data for research purposes or transfer them from one hospital to another, even with his or her consent, the trial is a lengthy process. Lately, a number of methods have been tried to get the transfer of this information in a safe and secure environment, but at the same time to achieve the semantic and syntactic interoperability of data [1, 2]. Because of this, a number of medical standards have emerged, such as HL7, openEHR, EN/ISO 13606 and the newest FHIR.

Aggregation of data for research purposes also requires consent, unless data are anonymous. However, it has been demonstrated that the independent release of local anonymous medical data corresponding to the same patient and coming from different sources (e.g., several health care institutions visited by the patient) could lead to patient de-identification and, therefore, confidentiality [3].

Due to the interoperability and security characteristics of medical information system [4], when Blockchain appeared, IT professionals in the medical field breathed lightly. They realized that this new technology is an important step in creating a mechanism for transfer and anonymization of the information in different medical units as well as research centers. But as early as May 2018, the European Community launched a new regulation named General Data Protection Regulation (GDPR) [5] on a person's personal data. The medical field is no exception to this new regulation.

In this paper we will present the main aspects of GDPR in health, what is Blockchain and how could revolutionize the medical system and the breach on how this two can coexist together.

2 General Data Protection Regulation

The General Data Protection Regulation (GDPR) [5] was launched by the European Parliament on April 14, 2016 and will enter into force from May 25, 2018, in all member states

O. P. Stan (✉) · L. Miclea
Faculty of Automation and Computer Science,
Department of Automation, Technical University
of Cluj Napoca, Cluj Napoca, Romania
e-mail: ovidiu.stan@aut.utcluj.ro

S. Vlad and N. M. Roman (eds.), *6th International Conference on Advancements of Medicine and Health Care through Technology; 17–20 October 2018, Cluj-Napoca, Romania*, IFMBE Proceedings 71,
https://doi.org/10.1007/978-981-13-6207-1_49

of the European Union. The GDPR will replace the Directive 95/46/EC and was designed to strengthen and to harmonize the data privacy laws of all European Community citizens. Basically, the GDPR is a new data framework law that enables citizens of EU to control their personal data and sensitive personal information’s [6].

The GDPR seeks to harmonize the legislation on personal data within the European Community. This regulation lists the essential rights and freedoms of individuals with regard to the safety of their individual data [4].

At the same time, GDPR requires non-EU IT&C professionals to provide greater privacy concerns due to the fact that the GDPR also has extraterritorial applications. Even though data processors and data operators from outside the EU are increasingly using the international landscape for business globalization, with this new law, their responsibilities have grown heavily. This measure of the EU comes as a response to the effects of globalization, the increasing use of cloud computing, advanced technical advances, and new ransom ware attacks [7].

2.1 Personal Data

Personal data is defined in GDPR as any complex information (physical, genetic, mental, cultural, social, etc.) that can be used to identify a person directly or indirectly. These can be names, addresses and even online identifiers. Thus, as soon as GDPR enters into force, IP address information, cookies, etc. will be considered personal data if they can be used without too much effort in order to identify a person. At the same time, there is no differentiation of personal data related to the active environment—at home or at work [5, 6].

The GDPR define the sensitive personal data as being that complex information regarding political affiliation, sexual orientation, religious beliefs, racial or ethnic origin.

2.2 Deciphering Terminology

GDPR introduces innovative provisions as data controllers and data processors. Data controllers are those who established what will happened with personal data while the data processors represent the organizations or the individual who processes this information on behalf of the controller. This fact has an important impact in software/hardware systems and even in cloud systems since IaaS, SaaS and PaaS is now considered to be data processors [8].

According GDPR [5], data controller is not necessarily an individual. Most of the time, data controller is an organization. In fact, any company that stores personal data about a European Community citizen is considered a data controller and is responsible for processing employees’ data but also for its customers’ data. The data controller concept also exists in the US law, but there are a few differences. In the US, the person who administratively controls a paper or paperless document is called a custodian. The difference between the two terms is that the custodian is only in possession of the information while the data controller in GDPR has the power to determine the purpose and the way of processing the personal data.

The data processor’s responsibilities are strongly highlighted in the GDPR, but the most important duties of the processor are stated in Art. 28 and Art. 42. They refer to the fact that the processor must offer reasonable assurances that the data security right is attained. GDPR also makes no distinction if data processing is performed by individuals or a computer, and in defining the data process it is included the entire life cycle of the information (from the collection till the destruction). For example, within GDPR, if a person examines any document then this process is seen as a form of processing. In other words, if a person or company uses personal data in some way, then they think you have processed them [9].

2.3 Data Transfer Process in GDPR

GDPR also presents aspects of the transfer of information both within and outside the European Community. The term “cross-border” is used when data transfer is desired within European Community. The transfer of information to countries outside the European Union is called “third-country data transfers” [5]. This information exchange process may take place not only between countries but also towards an area or territory of a country or an international organization but only after the recipient’s security and equipment level has been considered adequate by the European Commission. If there is no such adequate compliance document, the transfer can only be done after the adoption of a supervisory authority, in accordance with Art. 46.2 of the GDPR [5]. If the transfer of information is done within the acceptance of the subject and not by being comply with the EU Regulation, then a consensus document must be explicitly created and should contain all the necessary information in order to inform the subject of all the risks a data transfer may encounter [10, 11, 12].

2.4 GDPR and Healthcare Sector

One of the most affected areas by this new law on processing personal data is healthcare. The GDPR present and define a new concept namely “data concerning health”. This concept aggregate all personal data of a patient that discloses information about their past, present or future physical and mental health [5]. It also includes all the administrative information collected by medical units during a hospital episode or during a simple general practitioner visit such as registration number, unique identification number, all data derived from laboratory test, laboratory results, etc.

Today's medical information systems contain a lot of personal information of patients that can be used to lead to major breakthroughs in medicine. But, unfortunately, the Art. 5 in GDPR, states that keeping personal data longer than necessary and without altering the original purpose for collection is not allowed.

Therewith, taking into account the importance and the sensitivity of the data handled in a medical information system, GDPR adds a series of 5 additional regulations when it talks about processing data concerning health. Firstly, under the conditions provided in Art. 9.2, it specifies that data controllers and data processors must enquire the explicit consent of the person to process their information. The individual exposure referred to in Art. 22 does not refer to the data on the health of the individual unless the individual has been explicitly given his consent or if the processing thereof is a public interest mentioned as such. Even if they are processed because it is a public interest, it is necessary to take all the necessary measures in order to protect the rights and the confidentiality of the data subjects. If medical information is processed on a large scale, then it is necessary to add an upshot assessment on the protection of these data. The Art. 37 brings additional charge, namely that a data protection agent should be appointed for organizations where the main activities involve large-scale processing of data concerning health. The last additional ground rule added by GDPR through the Art. 30.2 specifies that data controllers must keep a written record (audit) of all processing activities performed for and on behalf of the data controllers [5, 13, 14].

3 Blockchain Technology

Originally developed to keep financial transactions, Blockchain is actually an open decentralized database. The difference between Blockchain and the traditional way used by the banks or by the governments with a centralized database, Blockchain technology uses a distributed registry on a network of nodes (peer-to-peer) as show in Fig. 1. The decentralized cryptographic model in the Blockchain allows users to rely on each other and to make peer-to-peer transactions without the need for intermediaries [15].

The openness propriety of the Blockchain is in a consequence of the fact that all transactions made on the Blockchain are public and anyone can join and create their own transactions.

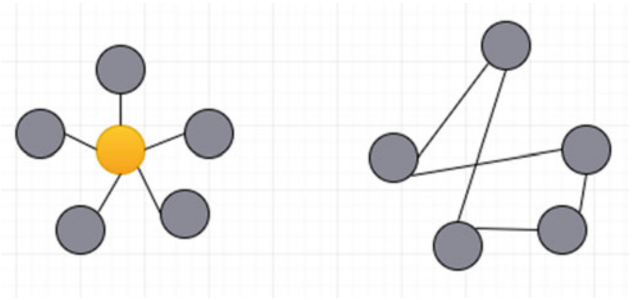


Fig. 1 Difference between centralize (left) and a P2P network (right)

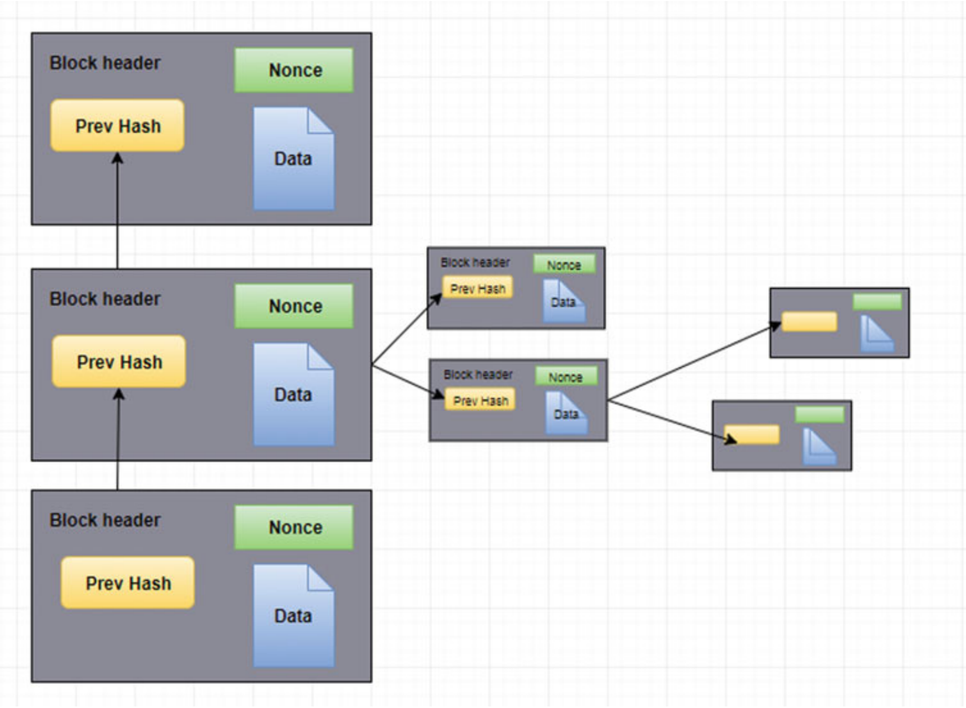
P2P networks interact with each other as the human interact within people's social groups. They did not appear with the Blockchain, they have existed for a long time. Although it has a number of advantages, they also have their flaws, of which the most important are the safety and security gasp. This issue was resolved in 2008 with the emergence of the Bitcoin virtual currency. This virtual currency introduced a solution by adding a mathematical model in order to ensure the integrity of the system. Therefore, Blockchain is composed of a series of complex elements or process such as: description of the property; protecting the property of non-authorized access; storage of transaction data (ledger); preparing these ledgers in order to be distributed among an unsafe environment; creating a system with and from these ledger; adding new transactions to the already existing ledger; the process of determining what is the ledger with the most accurately truth.

A Blockchain can be represented as a stack in a vertical position where blocks are kept one over the other. The lowest block is the foundation of the entire stack. Blocks are linked together, and each block holds a reference to the previous block in the chain. These blocks use the SHA-256 hash algorithm in order to be identified. A block may have only one parent, but may have as many children as it wants (Fig. 2).

Basically, a block represents a set of transactions. If we analyze the block, it has several properties. First of all, they are safe from changes. This is because each block contains an identifier created by applying a SHA-256 function over the inside data of the block. This identifier number is named *hash* and its role is to verify the integrity of the transaction. When the hash of a block is created it is used not only the inside block data but also the hash of the previous block, making them dependent. This makes the whole blockchain free from changes, because if we change the hash of block N, then the hash of the $N + 1$ block automatically changes.

If changes are made to the existing data block, then all nodes present in the network run an algorithm to evaluate, verify and match transaction information across Blockchain's history. If most nodes approve the transaction, then a new block is added to the existing chain.

Fig. 2 Blockchain architecture



If someone wants to add a new block to the chain, then a resource-consuming operation needs to be done. In order to get rid of this problem, some techniques are used, such as Proof of Work in Bitcoin or Proof of Stake [16].

The location where the blocks are assembled and after that added to the block of blocks is called *miners*.

In order to summarize this section, the Blockchain is immutable. In nodes are kept individual copies of the ledger and in order to reach a consensus to the real register each individual copies are compared. Blocks and transactions are also validated through the nodes, and they are all looking for illegal transactions using cryptography. This leads to the emergence of a monetary stimulus in order to provide the computing power to the block. This way transparency and openness is guaranteed by using the resources needed to solve complicated mathematical algorithms.

4 Bonding Blockchain and GDPR

Comparing GDPR and Blockchain we realize that the major difference is evidenced by the fact that GDPR specify that personal data must be deleted when the need for storage expires or when a person withdraws consensus.

The main characteristic of the Blockchain is that the inside data is immutable and cannot be edited. The revolutionary feature of the Blockchain is that information is stored in a variety of distributed systems to ensure the highest level of security. Data inside a block cannot be deleted or edited but only updated by creating a mining node, therefore by adding another block to the existing chain. Thus, all the transactions within a Blockchain are transparent which contradicts GDPR.

Currently, due to the fact how GDPR is written, it is clear that is incompatible with Blockchain. Of course compromises can be made. For example, even if you cannot delete information inside of a block, you can separate the information stored on the chain. However, if block platforms begin to divide the stored information, then the security provided by Blockchain is compromised. Also, within the GDPR, the deletion term is not defined even if the terms erase and erasure appear 12 times in the entire document. Even though the data is deleted, there are many ways to recover it. A method by which the block of chains can do this is by destroying the encryption key and so the data can no longer be accessed. In this way, logical deletion is achieved, a method recommended by the medical standards in the field such as HL7, openEHR or EN/ISO13606.

Concluding, the only way the two can coexist is to convince authorities that deleting data does not necessarily mean physical deletion but also that if data is inaccessible is also a form of deletion.

The fundamental element of the Blockchain, hashing, is based on the fact that data is converted in a way that it cannot be returned to its original state. GDPR defines a person's personal data as those data through which a person can be identified. If they are completely anonymous then they are outside the sphere of influence of GDPR.

Therefore, if all of a data concerning health are stored only as a hash on a block, it could be argued that the existence of hashes in a Blockchain is not a violation of GDPR because it is sufficiently anonymous.

The GDPR specifications and regulations were principally focused on CRUD methodology (Create|Read|Update|Delete) systems. Blockchain technology does not use these principles. Since the data in a Blockchain cannot be erased/deleted, the principle behind Blockchain is CRAB (Create|Retrieve|Append|Burn). Adding information, which replaces the Update method, specifies that only new transactions can be added, and the Burn operation means that the encryption keys used for hashing the information are deleted or removed.

At the same time, according to Article 29 [8], advisory article, it is specified that data hash is in fact a pseudonymization process by which the data is disconnected from the individual. This conclusion is based on a mathematical conclusion that it still leaves a gateway to attack the information. Also, by encrypting all the data with an encryption key and then deleting this key at the request of the person leads to a result in which those data can no longer be used and accessed, and thus they may be erased.

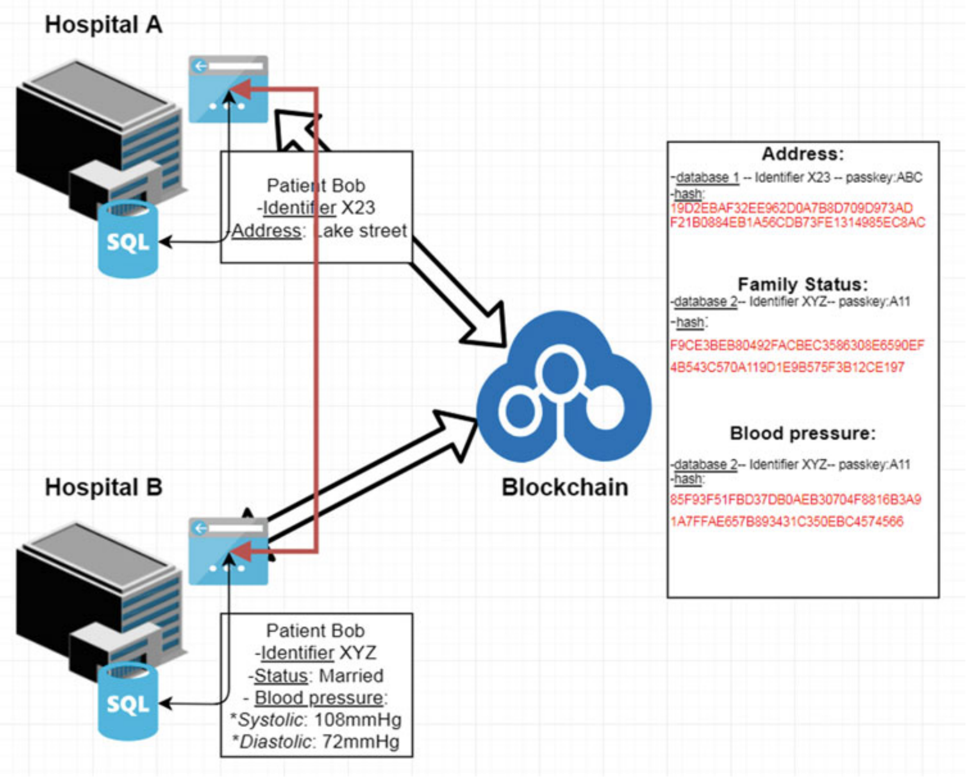
Another measure that can be taken is that personal data is stored outside the Blockchain.

Another issue raised by the GDPR is that the personal data of a European Community citizen should be physically store only on the territory of the European Community. Here's the big problem, because in Blockchain there is no control over who and where a node is hosted. To solve this problem, a foundation or organization can be set up to secure this GDPR regulation by building a public Blockchain, but authorizations are only hosted in nodes.

One method to solve the above problems is exemplified in Fig. 3. First of all, personal data is stored outside the Blockchain and the reference to that information along with a hash of these data, as well as all necessary metadata is stored on the Blockchain. In the scenario shown in Fig. 3 there are two hospitals, Hospital A and Hospital B, each with their own databases, but both are connected to a Blockchain. If we assume that from the Hospital A we want to access the patient Bob information's from the Hospital B, in order to complete his medical history, at the moment, after the patient's consent, the informatics system in Hospital A makes a request to the informatics system from Hospital B based on the name and national number identification of Bob. Based on this request, the IT system receives the requested information.

By connecting the two hospitals to a Blockchain, the operation changes as follows. Because Hospital A does not know in which medical clinics are stored other medical information related with Bob, the informatics system from Hospital A sends a request to the Blockchain to retrieve all Bob's specific medical data. The Blockchain checks if the

Fig. 3 Overall communication process with Blockchain


Hospital A
SQL
Patient Bob
-Identifier X23
-Address: Lake street
Hospital B
SQL
Patient Bob
-Identifier XYZ
-Status: Married
- Blood pressure:
*Systolic: 108mmHg
*Diastolic: 72mmHg
Blockchain
Address:
-database 1 -- Identifier X23 -- passkey:ABC
-hash:
19D2EBAF32EE962D0A7B8D709D973AD
F21B0884EB1A56CDB73FE1314985EC8AC
Family Status:
-database 2-- Identifier XYZ-- passkey:A11
-hash:
F9CE3BEB80492FACBEC3586308E6590EF
4B543C570A119D1E9B575F3B12CE197
Blood pressure:
-database 2-- Identifier XYZ-- passkey:A11
-hash:
85F93F51FBD37DB0AEB30704F8816B3A9
1A7FFAE657B893431C350EBC4574566

applicant, Hospital A, has all the rights to access this information. If Hospital A has the appropriate authorization, he gets the link and the hash of the required data. The link represent any kind of information such as API access address, required key, link to other databases, etc. Therefore, the Blockchain functions as a national registry that specifies who and where it holds information. On the basis of the information received from the Blockchain, Hospital A can now take and process the data directly from the Hospital B database. Once this information has been received, it is also possible to check through the Blockchain and more precisely through the hash whether the data has been altered. If the hash of the data received by Hospital A is the same as that of the Hospital B blocks, it means they keep their authenticity, and so we obtain also the syntactic and semantic interoperability.

5 Conclusions

If we look at these two concepts, GDPR and Blockchain, we can easily see that there is a vexed question. If we are referring to data portability, consent management, audibility of legal access, then Blockchain fits like a glove for GDPR. Instead, if we look at other issues, such as the right to delete information, we can see that GDPR and Blockchain want totally different things.

By those specified in the previous chapters, we believe that one can still realize such a system that complies with the GDPR rules but at the same time create a chain of blocks that can help improve the quality of the medical act and improve the patient's quality of life.

The method described in Sect. 3 is 100% compatible with GDPR specifications. This way you can physically delete data from databases from medical units. Even though Blockchain keeps hash and link to them, this link leads to nowhere and is thus useless. In the scenario presented above, the Blockchain is in fact only an access control environment, acting as a national register, the method successfully implemented in [17].

If we look at Blockchain's proposed motto, then we have to specify that the benefit of transparency disappears because if we store the data outside the Blockchain we cannot have information and control as to who and when accessed the data and why. Another problem is that once the computer system in Hospital A once has the medical records in Hospital B it does not have to go through Blockchain again. Also, once the data is stored outside Blockchain you cannot know exactly who is the owner and the data controllers of the data.

Acknowledgements The research presented in this paper was supported by the national project SeMed (2933/55/GNaC 2018).

Conflict of Interest The authors declare that they have no conflict of interest.

References

1. Gabor-Harosa, F.M., Stan, O.P., Daina, L., Mocean, F.: Proposed model for a Romanian register of chronic diseases in children. Comput. Methods Programs Biomed. **03**(130), 198–204 (2016)
2. Ovidiu, S., Miclea, L.: Local EHR management based on FHIR. In: 2018 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), Cluj Napoca, Romania, 24–26 May 2018
3. Dubovitskaya, A., Urovi, V., Vasirani, M., Aberer, K., Schumacher, M.I.: A cloud-based ehealth architecture for privacy preserving data integration. In: IFIP Advances in Information and Communication Technology, book series (IFIPAICT), vol. 455, Springer
4. Tont, G., Vladareanu, L., Munteanu, R.A., Tont, D.: Some aspects regarding human error assessment in resilient sociotechnical systems. In: 2nd WSEAS International Conference on Sensors and Signals/2nd WSEAS Int Conf on Visualization, Imaging and Simulation/2nd WSEAS International Conference on Materials Science Location: Morgan State Univ, Baltimore, MD, 07–09 Nov 2009
5. Regulations: Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 27 Apr 2016, Official Journal of the European Union
6. Allen & Overy: The EU General Data Protection Regulation (2017)
7. European Data Protection Supervisor: The history of the general data protection regulation. https://edps.europa.eu/data-protection_en. Accessed on Feb 2018
8. Art. 29 Working Party: Opinion 05/2012 on Cloud Computing. Adopted in 1 July 2012
9. Art. 29 Working Party: Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing. Adopted in 22 Sept 2015
10. Pyle, E., Manyé, L.B., Swerdloff, J., Sharp, L.G., Irvin, R.E., Koziol, J., Jiwnani, S., Holt, S., Goodloe, V.: Decoding GDPR—comparing terms used in GDPR with their U.S. e-discovery counterparts. Judicature **102**(1) (2018)
11. Seo, J., Kim, K., Park, M., Park, M., Lee, K.: An analysis of economic impact on IoT under GDPR. In: 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, South Korea, 18–20 Oct 2017
12. Dorca, V., Popescu, S., Munteanu, R., Chioreanu, A., Peleskei, C.: Agile approach with Kanban in information security risk management. In: IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), Cluj Napoca, Romania, 19–21 May 2016
13. Vojkovic, G.: Will the GDPR slow down development of smart cities. In: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia
14. Katulic, T., Katulic, A.: GDPR and the reuse of personal data in scientific research. In: 2018 41st International Convention on

Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia

15. Tapscott, D., Tapscott, A.: Blockchain revolution: how the technology behind bitcoin and other cryptocurrencies is changing the world. Portfolio, 12 June 2018, ISBN: 978-1101980149
16. King, S., Nadal, S.: PPCoin: peer-to-peer crypto-currency with proof-of-stake. Self-Published paper, Aug 2012
17. Stan, O., Sauciuc, D., Miclea, L.: Medical informatics system for Romanian healthcare system. In: 2011 E-Health and Bioengineering Conference (EHB), Iasi, Romania, 24–26 Nov 2011