Blockchain-based approach for e-health data access management with privacy protection

Liviu Hirtan
University Politehnica of Bucharest
Bucharest, Romania
liviuhirtan@yahoo.com

Piotr Krawiec
National Institute of Telecommunications
Warsaw, Poland
P.Krawiec@itl.waw.pl

Ciprian Dobre
University Politehnica of Bucharest
Bucharest, Romania
ciprian.dobre@cs.pub.ro

Jordi Mongay Batalla
National Institute of Telecommunications
Warsaw, Poland
J.Mongay@itl.waw.pl

***Abstract*—Blockchain is a technology that offers the ability to create new business models and solves trust issues in a more efficient way. It can lead to many research opportunities and business innovations. Academia and industry proposed many blockchain based software solutions within a wide range of domains. In this paper we present a system design where blockchain technology is proposed to be used in the healthcare system, where the vital information regarding the medical analyses are shared between hospitals, medical clinics and research institutes based on access policies defined by the patients. In order to protect confidential data, our solution involves the use of two types of chains: a private one, the sidechain, which keeps information about real ID of the patients, and a public one, the mainchain, which stores information about patients' health data marked with a temporary ID. To test it, we developed the design using Hyperledger Fabric framework. Presented experimental results show good performance of the system in relation to the following metrics: 1) the time needed to identify the medical data for a particular patient, and 2) the mainchain propagation time of all the blocks within the peer to peer network.**

Keywords—blockchain, e-health, data privacy, data access management

I. INTRODUCTION

More and more areas of people's daily lives continuously evolve into digitized forms. This also applies to healthcare, where a variety of health related information is generated by clinics, hospitals and different e-health applications [1]. During their life, people interact with a large number of medical specialists, each of them stores data in their IT systems, leading to a fragmented system and databases that are not interconnected.

Blockchain is a new technology that supports sharing of values. In recent years, it has been applied in various areas, the most important is the financial one. Blockchain is a digital ledger where there are stored all the executed transactions. It uses a distributed, peer-to-peer network to make a continuous growing list of ordered records called blocks. Every block contains a set of signed transactions and is validated by the network itself, by means of a consensus mechanism. Copies of the blockchain are distributed on each participating node in the network. Blockchain can be considered a permanent database because the implemented algorithms prevent alteration of the already stored information.

Any system responsible with handling and storing medical data must take into account the user rights imposed by the legislation in force, such as European General Data Protection Regulation (GDPR) EU 2016/679 on the protection of personal data. GDPR applies to any entity that processes personal/health data and is established in the European Union, or is established outside the EU, but processes data of persons from EU. Implementing such rules in blockchain technology is a real challenge, considering the fact that most blockchain implementations are built as an immutable ledger.

In this paper we propose an innovative model of health care IT system based on privacy preserving. Users are recognized as owners of their own data and have full control over it. They can apply various security policies, such as sharing data with specific clinics or institutions and can contribute anonymously to certain statistics. The blockchain uses public key cryptography to create an immutable, append-only, timestamped chain of content. Our system design proposes two types of blockchains: a public mainchain and a private sidechain. Depending on the type of node (trusted or untrusted), each of them has a copy of the mainchain, or both blockchains. Due to privacy reasons and a large amount of data generated by all the participating institutions and devices, the content of the nodes is formed only by a set of links to health data, permissions and other auxiliary information. The data themselves (the medical analysis) could be stored either by the institutions that generated it or in the cloud.

The article is organized as follows. The next section presents an overview of related works in the scope of blockchain-based solutions for healthcare. Section III describes the proposed system design, including detailed description of the applied transactions and security mechanisms. In Section IV we present experimental results in order to evaluate the performance of the proposed system. At last, the final section concludes the article.

II. RELATED WORKS

Within healthcare, a number of blockchain-based solutions have been proposed to integrate clinics, doctors, and patients with the aim of providing improved quality services in a timely manner.

978-1-7281-1016-5/19/$31.00 ©2019 IEEE

In [2], the authors present an application entitled MedRec that uses smart contracts built over a public Ethereum blockchain to define patient-provider relationship, viewing and data retrieval permissions too. The mining algorithm is Proof-of-Work; medical stakeholders are rewarded for their contribution to aggregate anonymized medical data as mining rewards. Using such a system in real life, where personal data, whether anonymous, is used for purposes other than the original one, may determine clients not to use such services. In addition, if it is not used an efficient anonymization process, the patients' identity can be disclosed, so the protection of personal data is no longer met.

In [3], it is presented a blockchain–based architecture where the system uses public key infrastructure to represent users' digital identities. Identities are recorded directly in the blockchain to ensure that users holding the corresponding private key can log in. Those identities are created for clinicians to facilitate data sharing and to get better decisions for patients, but this contravenes the protection of personal data.

An attribute-based signature scheme with multiple authorities is described in [4], in which a patient endorses a message according to the attribute without disclosing any information. The system design considers the following entities: a server on which information is stored, a number of *N* authorities, data verifiers, and patients. Authorities are represented by different organizations within the medical system, such as medical research institutes, hospitals, medical insurance companies, etc. and have the role to accept the registration and exchange of patients' medical data. Although the mathematical model assures the confidentiality of the patient's identity, entities that should not have access to data, such as research institutes or insurance companies, must not be included in the process of identifying patients. Also, using a single server to store medical data of all patients would make the system fail when the entity is not connected to the network.

Q. Xia et al. [5] propose a blockchain-based system that provides medical data sharing among medical big data custodians in a trust-less environment. The main purpose of the blockchain is to maintain an immutable database where actions related to delivery and request of data are stored. The authors introduce a special type of child-block that is attached to the parent block as a side block. Its role is to save logs created by smart contracts with requests from different entities. Each data request is signed by the user and checked by the authenticator. If the request is valid, then the requestor will receive the requested information, encrypted, along with a smart contract. It will be activated with data decryption and will monitor the data. Processing and consensus nodes receive information regarding data handling, which will attach to the corresponding parent block – containing particular data request - as a side block.

In [6] it is proposed a blockchain-based healthcare system that integrates the patients, medical sensors, doctors and hospitals. The data are stored outside blockchain to enhance the performance, whereas the blockchain is used to store only part of data or a pointer to it. Nodes known as gateways, are devices that have enough power and energy, and could be laptops or mobile phones. The medical sensors transmit information to the system only through the gateways. Smart contracts are used to maintain the access policies, for example patient-doctor relationships, but the way to accomplish this task is not described.

In turn, in [7] the authors present a healthcare blockchain approach for sharing patient data. The trust is based on a network consensus, which is an agreement on the proof of structural and semantic interoperability. During this process, known as Proof of Interoperability, the miners check if the analyses are interoperable with a known set of semantic and structural constraints. Therefore, the medical analyses of the patients are also visualized by other entities besides the medical clinic where the analyses were performed. Without much details, the authors use smart contracts as security policies.

The various literature reviewed in this section does not provide concrete information or provides no information on how the confidentiality of personal data is ensured. Medical analyses are personal data that must be accessible only to the patient and to well-established entities. Reviewed proposals, as well as many others (for example, [8-11]), keep patient's IDs in publicly accessible blockchain transactions, and thus make patients vulnerable to tracking records of their medical services. Our approach offers to patients the certainty that their data is well protected, jointly with her/his privacy. The proposed solution puts the patients first, so their medical data can be accessed only through security policies, and the policy transactions are accessible through publicly available blockchain. However, the public blockchain contains the patient's temporary ID only, therefore it does not allow tracking history of patient medical treatment. Moreover, in our system design, patients are considered owners of their own medical analysis, have full control over them, even if those are stored on clinics' datacenters. In the following sections we detail this concept by presenting the system architecture, practical application and experimental results.

III. Design of the proposed system

In this section we present the design of a secure system that ensures the confidentiality and authenticity of the patient's medical data. The system includes the main actors of the health system, such as patients, doctors, medical institutions (hospitals, clinics, etc.) and other entities that want to access the medical data (for example research institutes, emergency service, insurance companies, employers, etc.). The system contains information such as the entities that have access to data, their type, the doctors and the patients within the system, patients' medical information, and access policies to these data. Patients are recognized as owners of their medical analysis results, have full control over them and can apply access policies any time. Data dissemination is done through blockchain technology, and each node within the network has a complete copy of the ledger.

Considering personal data protection, the system covers two types of nodes: trusted and untrusted, as well as two types of blockchains, as shown in Figure 1. Depending on the nodes' level of confidence, they can access only the public blockchain known as mainchain (untrusted nodes) or both blockchains, more exactly the mainchain and the private blockchain known as sidechain (trusted nodes).

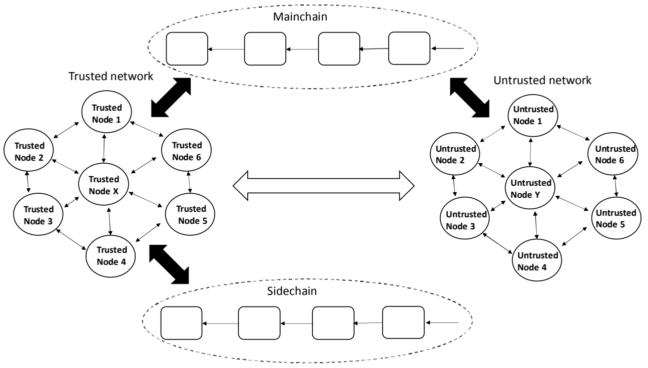

Figure 1: Logical concept of the system design

Among the main actors of the health system there are the medical institutions (hospitals, clinics, etc.), but also other institutions that want to access the medical analyses (research institutes, insurance companies, employers, etc.). Within the system design, those entities are represented as nodes. Their role is to store a copy of the blockchain, to process incoming requests and to query the information. Nodes are divided into trusted nodes (approved medical institutions) – their role is to validate transactions and take decision if a new transaction is inserted within the blockchain; and untrusted nodes – all other entities who want to access medical data, as shown in Figure 2.

As it was mentioned above, the solution involves the existence of two types of ledgers: a mainchain that is accessible by all the nodes and a sidechain that is accessible only by the trusted nodes. Each type of blockchain is represented as an immutable linked list of blocks and each block is represented by one or more transactions.

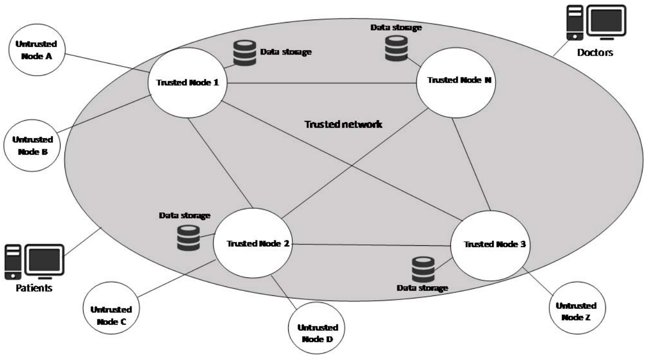

Figure 2: Peer to peer network

Figure 3 illustrates two types of transactions kept in a mainchain: *storage* transaction and *policy* transaction. Storage transactions are created following the interaction between a patient and a medical institute. After the patient gives her/his consent, information about her/his medical analysis is published in the mainchain, and the analysis is stored in the clinic's internal database. So, within the mainchain there is saved only a reference (pointer) to the patient's health data, whereas the data is kept securely in dedicated storage infrastructure, protected by adequate security mechanisms, both in terms of access control and anomaly detection [12][13]. Taking into account that all the nodes within the network have access to this blockchain, mainchain transactions do not contain personal information such as name, birth date, etc. These information are stored at external repository, for example using the OpenMRS, an open source electronic medical record system [14]. On the other hand, each mainchain transaction contains a unique temporary ID that can discreetly identify the patient.

The sidechain is distributed and maintained only by trusted nodes. To protect personal information, untrusted nodes do not have access to this ledger. According to Figure 4, each block is represented by a transaction created by the entity (a trusted node) that created a storage or policy transaction within the mainchain. The information stored in the sidechain is required to link the patients' temporary ID that is found within the mainchain transactions and the patients' real identity.

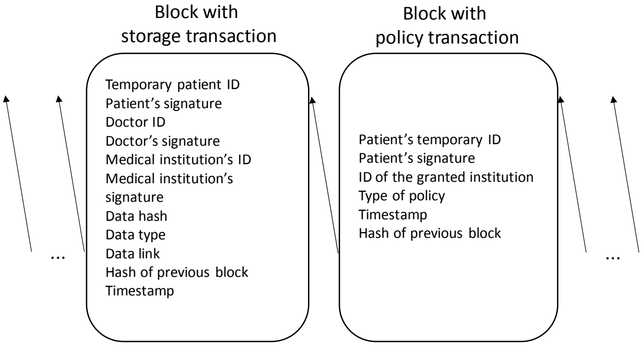

Figure 3: Mainchain storage and policy transactions

Each trusted node keeps a white list of all trusted nodes in the network. Trusted nodes authenticate to each other using the Public Key Infrastructure (PKI). We assume that adding a new node to the white list is managed by the supervising entity (for example national public health agency). In this way, the mainchain is a kind of permissioned blockchain, where all entities can send requests and browse the ledger, but only trusted nodes are allowed to add new blocks. In turn, the sidechain is a private blockchain, since it is accessible solely for trusted nodes. Therefore, for both blockchains fast and lightweight consensus algorithms can be applied that rely on majority confirmation. After a storage / policy transaction is created, it is broadcasted to all trusted nodes. These nodes check the transaction validity and, if majority of them consider the transaction to be a valid one, the origin node creates the new block attaching the transaction to the mainchain, and next broadcast the updated ledger to the entire peer-to-peer network. Similarly, the same procedure is applied in the sidechain case, except the last step when the ledger is redistributed only to trusted nodes.

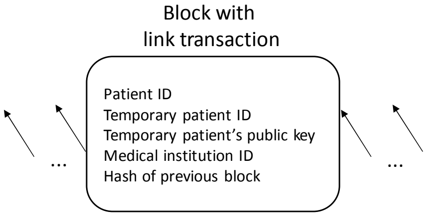

Figure 4: Sidechain link transactions

A. Transactions

As we mentioned in the previous section, the mainchain includes two types of transactions: *policy* and *storage*, whereas in the sidechain there are only *link* transactions.

Storage transactions are created by medical institutions as a consequence of analyses made on patients. This type of transaction contains the following characteristics (see Figure 3): the temporary patient ID (unique for each transaction), the patient's digital signature for proving that the transaction had been accepted by the patient, the doctor's ID, the doctor's signature, the medical institution's ID, the medical institution's signature, the timestamp, the data type, the data link, the data hash and the hash of the previous block. After a patient is consulted within a medical institution, the system authenticates his/her identity using PKI scheme and queries the sidechain for a unique temporary patient ID useful for storing the related transaction into the mainchain. The metadata about medical analysis are sent to the patient's wallet application signed with the clinic's signature and the doctor's signature. The patient reads them and, if he/she agrees, signs and returns to the medical node that next creates a new mainchain transaction.

The medical institution who created the mainchain transaction is also responsible for creating a new transaction within a sidechain that records the correspondence between the temporary patient ID and real identity. Next, the medical node broadcasts the transaction to all other trusted nodes. The white list nodes check the transaction, more exactly validate all the signatures: the medical institution which created it, the doctor's signature and the patient's signature, as well as authenticate the sending node. If the transaction passes the requirements, the new block is appended to the blockchain and the medical institution broadcast it. Medical analyses are stored in a database external to the blockchains, but internal to the medical institution. At this stage, the correspondence between the patient's temporary ID and patient's real identity is known only by him/her (it is kept in the wallet application) and the trusted nodes within the white list (through a sidechain transaction). This prevents untrusted nodes (research institutes, health insurance companies, employers, etc.) to discover personal information, because they are not allowed to query the sidechain. Medical institution is responsible for the medical data preservation and data authenticity, nevertheless the mainchain can be used to verify if the data has been modified using the hash stored in each storage transaction.

Policy transactions are created when the patient applies a certain security policy regarding his medical data. This type of transaction contains the following characteristics (see Figure 3): the patient's signature, the patient's temporary ID (from the storage transaction) / the list of patient's temporary IDs (if there are more than one, since single policy transaction may involve different medical records), the ID of the granted institution (research institutes, assurance companies etc.) that created the transaction, the type of policy (allow/deny) and the hash of previous block. The entity which stores the medical analysis is responsible to create the storage transaction when the patient requests it. After the patient contacts the institution who stores the data, it creates a policy transaction signed by the patient and broadcasts it into the entire peer-to-peer network. All the nodes within the white list verify the transaction's validity. If the transaction passes this requirement, it is appended to the mainchain.

Link transactions are created in conjunction with storage transactions. This type of transaction contains the following fields (see Figure 4): the patient ID, the temporary patient ID (unique to each link transaction), the temporary patient public key (unique to each link transaction), the medical institution ID (which created the related storage transaction) and the hash of previous block. These transactions are stored within the sidechain that is maintained and accessed only by trusted nodes. Its role is to save the correspondence between the patient's real identity (patient ID) and his/her temporary identity, generated independently for each performed medical analysis. In this way, the system ensures the confidentiality of personal data because browsing of data stored in the mainchain, which is accessed by all the nodes, does not make it possible to trace the history of a given patient's medical events.

It should be noted that the architecture and mechanisms of the proposed system comply with the requirements imposed by the legislation regarding the protection of personal data, such as EU General Data Protection Regulation (GDPR).

One of the rights granted by GDPR is to access one's own personal data. The medical institutions ensure the data availability and authenticity, so users have the opportunity to query the blockchain about each transaction regarding its ID. Another assured right is data portability – a user has the possibility to transfer its data from one data controller to another. In our system design, data access is made through the security policies stored within blockchain. The right of an user to object to the processing its personal data is ensured by the fact that processing personal data is made only after the patient agrees to access it. The right of data erasure is performed by the medical institutions that store / control data. As the data is not stored within the blockchain, the process will not disagree with the blockchain immutability concept. Right to rectification is done through right to data erasure and the creation of a new storage transaction. The right in case of breach is ensured by the fact that an user can check if her/his data have been altered through the data hash stored in the mainchain. Through policy transactions that are public, the user can see who has (or had previously) access to her/his medical data, so the right to be informed is achieved.

B. Proposed security mechanism

The purpose of the proposed security mechanism is to protect the identity of patients and the confidentiality of personal data. The system uses methods such as sidechains and temporary IDs to guarantee the patient's anonymity. Moreover, the patients' consent to the publication of data is represented by digital signatures. Digital signatures are also used to associate medical analysis with doctors that made them and the issuing medical institutions. Since the mainchain is accessible by non-trusted entities, all stored information that can be attributed to patients, such as the ID or electronic signature, is unique to each entry.

Table I presents the algorithm for creating storage transaction, which includes the generation of patient public-private keys and signing medical analysis. The mechanism is based on cryptographic key pairs used for authentication and messages signing. In our implementation, we use the public-key cryptosystem RSA [15], one of the most popular asymmetric cryptography algorithm. On the left side of the table there are presented the operations performed by the patient through his/her dedicated application. The right side of the table presents the operations performed by the clinic node, more exactly the entity that generates the medical analysis.

TABLE I. STORAGE TRANSACTION GENERATION

Patient application		Clinic node
Patient Id	→	
r_1, r_2 – large random prime numbers belonging to Z_q		
Compute $n = r_1 * r_2$		
Compute $ø = (r_1-1)(r_2-1)$		
Choose e ($1<e< ø$ and $gcd(e, ø)=1$)		
Compute d ($1<d< ø$ abd $e*d≡1 \bmod ø$)		
Generate $[sk_i=(n, D_i), pk_i=(n, E_i)]$		
pk_i	→	
	←	Generate $uID_k \notin \{uID_1, uID_2, uID_3, ...\}$
		Generate m
		Compute $s_d=m^{Dd} \bmod n_d$
		Compute $s_c=m^{Dc} \bmod n_c$
	←	(s_d, s_c, m)
Compute $s_p=m^{Di} \bmod n_i$		
(s_p, s_d, s_c, m)	→	

The key pair (sk_i, pk_i) is generated at patient wallet application; each pair of keys is unique for each medical analysis *m*. The client publishes his public key (pk_i) as the trusted nodes verify the storage transaction validity (the key is later stored in the link transaction). Similar to the public-private key pair, the patient's identity is unique within the mainchain. The patient has a static ID which is found in the sidechain and is known only by trusted nodes. In the next steps, the patient receives the result of the medical analysis, m, signed by the clinic (s_c) and by the doctor (s_d). The public keys are shared on a dedicated key server; thus the patient can verify both signatures. Signing the medical analysis by patient (s_p) implies that he/she agrees to publish the data in the mainchain. After acceptation of medical analysis by the patient, the clinic node generates a storage transaction and distributes it to the other nodes to verify.

TABLE II. TRANSACTION VERIFICATION

Generator trusted node		i^{th} trusted node
(s_p, s_d, s_c, m)	→	
		Compute $v_p = s_p^{Ep} \bmod n_p$
		Compute $v_d = s_d^{Ed} \bmod n_d$
		Compute $v_c = s_c^{Ec} \bmod n_c$
a_i	←	$[H'(m) = H(v_p)]$ && $[H'(m) = H(v_d)]$ && $[H'(m) = H(v_c)]$
if $\frac{\sum_{i=1}^{n} a_i}{n} > \frac{50}{100}$ $(s_p, s_d, s_c, m) \subset \{(s_{pk}, s_{di}, s_{cj}, m_k)_{k=1:n,\ i=1:z,\ j=1:q}\}$		
	→	$\{(s_{pk}, s_{di}, s_{cj}, m_k)_{k=1:n,\ i=1:z,\ j=1:q}\}$

Table II presents the transaction verification mechanism within the consensus phase. On the left side of the table are presented the operations performed by the generator trusted node that is the source of the new transaction, and on the right side of the table are presented the operations performed by each of the trusted nodes (except the generator node). The transaction is a message (*m*) signed by the patient (s_p), the doctor (s_d) and the clinic (s_c). Trusted nodes check each of these signatures using the public key of each of the three entities: (n_p, E_p), (n_d, E_d), (n_c, E_c). Public keys are known by the entire peer-to-peer trust network. The result of those three operations is a new set of messages (v_p, v_d, v_c). Message digest *H()* is calculated for each of these values. In addition, the message digest *H'()* of the signed data is computed. If each pair of digests is equal, then the signatures are valid. For the entire transaction to be valid, all three signatures must pass this verification. Each trusted node executes those operations and sends to the generator trusted node his answer a_i (1 or 0). The generator trusted node collects all the answers from all the trusted nodes and computes the percentage of positive answers. If more than 50% of the trusted nodes considers that the transaction is valid, the generator appends the new block to the mainchain and broadcasts it to the entire peer-to-peer network.

The security level in the proposed schemas is determined by the parameter *n* (which jointly with *e* creates a public key), more precisely its length, in bits - the more sensitive is the information, the longer the key length must be. According to the NIST recommendation [16], we propose to use the minimum value of 2048 bits.

IV. IMPLEMENTATION AND VALIDATION

To evaluate the system presented in previous sections, we use open source Hyperledger Fabric framework [17] and Linux Ubuntu operating system. The purpose of the implementation is to test the proposed solution, to identify security breaches, leakage of information, identify possible components that were not taken into account when the system was designed, and to identify possible system optimization.

The prototype application implements the main components of a blockchain based software such as blockchain display, blockchain query, adding new transaction, transactions validation, creating blocks and appending them to blockchain, broadcast blockchain, and blockchain integrity check. Within a single operating system, the application creates a virtual network in which terminals are considered as nodes. These terminals can emulate both, trusted and untrusted nodes. Within trusted nodes, the user can perform operations such as mainchain view, sidechain view, add storage transactions and add policy transactions. Within untrusted nodes, there can be performed actions such as view mainchain and query the application to obtain the reference to medical analysis based on patients' temporary IDs that are found in the mainchain and are unique for each analysis.

Performance tests have been done by test automation, introducing functions for automatically generating a large amount of data, and for measuring the execution time. Their purpose is to test the performance of the system, the ability to handle a large amount of data, the execution time, and the correctness of software modules implementation. In the following, there are presented two tests that take into account the time needed to identify the medical data for a given patient, and the mainchain propagation time to all the blocks within the peer to peer network.

The tests were performed on the virtual machine on which are installed and configured the prototype application and other auxiliary software modules, such as frameworks, libraries, and packages required to run. Within the virtual machine the trusted nodes are simulated with the processing unit and storage unit, the untrusted nodes with the processing unit and storage unit, and the peer-to-peer network. The virtual machine's operating system is Linux Ubuntu, and the technical features are i7 1,8 GHz 2 core processor and 8 GB RAM. Before the tests, the peer-to-peer network had been checked to meet the operational requirements, which covers: verification of transaction creation module, verification of broadcast module and verification of untrusted nodes data access process.

Figure 5 presents the results, with 95% confidence intervals, of the test that measures the time needed to identify medical data for a given patient. Axis OY represents the time it takes to find the patient's records (in milliseconds), and the OX axis represents the number of blocks stored in the mainchain. According to our system design, medical data request can be made from untrusted nodes. During this stage, it is searched through mainchain the security policy that specifies the correspondence between the medical data and the entities that are allowed to access it. If the policy is identified, the requested data will be provided to the untrusted node with the corresponding ID. It should be noted that even on an ordinary personal computer the search time is satisfactory, as it is a few seconds for the blockchain of a length 150,000 blocks. Moreover, the system shows good scalability, as search time increases linearly with blockchain length, so we can expect that even for a ledger with millions of blocks the search time will be still acceptable using the appropriate technical infrastructure (servers with good performance metrics).

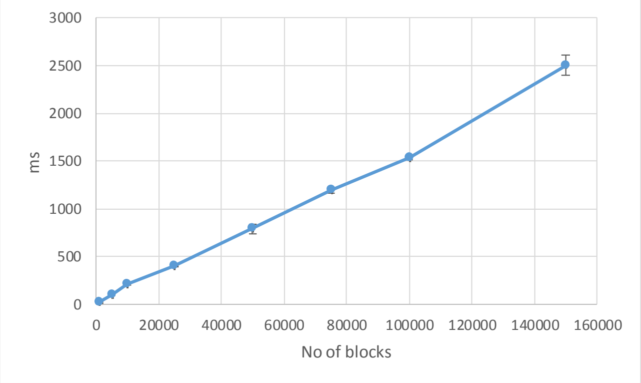

Figure 5: Time required to find the medical data of a given patient

Figure 6 presents the results, with 95% confidence intervals, of the test that measures the propagation time of the mainchain to all nodes according to the number of blocks. The OY axis represents the time (in seconds) after which other nodes update their ledger and the OX axis represents the number of blocks in the mainchain.

The propagation of mainchain is a result of validation of a new storage or policy transaction within the consensus mechanism. After more than 50% of the nodes consider the transaction to be legitimate, the source node has the responsibility to create a new block that will include the transaction, attach this block to the local mainchain, and transmit the new mainchain to all nodes within the peer-to-peer network. It is the worst case scenario because it assumes that the whole ledger is transferred. Although such a case concerns rather infrequent situations as connection of a new node to the system or recovery after node failure, it shows acceptable values (about 2 minutes for the ledger with 150,000 blocks). During the standard operation of the system there is no need to transfer the whole chain each time, but only the lasts blocks of the ledger. In this case, the propagation time has an almost constant value of 8 seconds (see Figure 6).

However, the propagation time of the mainchain to all nodes, in a real world application depends greatly on the geographic position of the medical clinics' IT equipment and the bit rate available in the network.

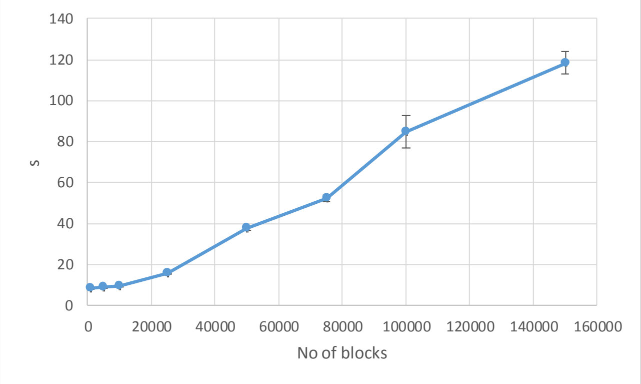

Figure 6: Propagation time of the mainchain to all the nodes

V. Conclusion

Medical analyses are personal data that must be accessible to the patient and to well-established entities. This paper describes a collaborative system involving the sharing of medical data between medical entities and ancillary institutions such as research institutes, insurance companies, etc. Using technologies such as blockchain and public key cryptography, the system design ensures the confidentiality of personal data and recognizes the patient as the owner of his data. Thereby, the proposed system meets the requirements imposed by regulations on personal data protection. Access to data is transparent, so health information can be accessed by ancillary entities based only on security policies. The application's workflow ensures that medical information created by a medical unit is validated by other trustworthy entities. The implementation of such a protocol in real life would bring many advantages to all the actors involved. Patients should easy manage their medical analyses, hospitals can provide a better quality medical service, while research institutions can get easy access to a very useful health database.

Our future works will focus on integration of the proposed system with real medical data storage infrastructure that implements international standards for healthcare data exchange, such as HL7 [18] and openEHR [19].

Acknowledgment

The research presented in this paper is partially supported by projects: NETIO Tel-MonAer (cod SMIS2014+ 105976), SPERO (PN-III-P2-2.1-SOL-2016- 03-0046, 3Sol/2017), ROBIN (PN-III-P1-1.2-PCCDI-2017-0734) and the Ambient Assisted Living (AAL) project vINCI: "Clinically-validated INtegrated Support for Assistive Care and Lifestyle Improvement: the Human Link" (AAL2017-63-vINCI) cofunded by The National Centre for Research and Development, Poland.

References

[1] Yannis Nikoloudakis et al., “Vulnerability assessment as a service for fog-centric ICT ecosystems: A healthcare use case”, Peer-to-Peer Networking and Applications Journal, January 2019, DOI: 10.1007/s12083-019-0716-y

[2] Ariel Ekblaw, Asaph Azaria, John D. Halamka, Andrew Lippman: “A Case Study for Blockchain in Healthcare: ‘MedRec’ prototype for electronic health records and medical research data”. 2nd International Conference on Open and Big Data, 2016.

[3] Peng Zhang, Jules White, Douglas C. Schmidt, Gunther Lenz, S. Trent Rosenbloom: “FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data”. Elsevier, 2018.

[4] Rui Guo, Huixian Shi, Qinglan Zhao, Dong Zheng: “Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems”. IEEE Access, 2018.

[5] Qi Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, Mohsen Guizani: “MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain”. IEEE Access, 2017.

[6] Nabil Rifi, Elie Rachkidi, Nazim Agoulmine, Nada Chendeb Taher: “Towards Using Blockchain Technology for eHealth Data Access Management”. Fourth International Conference on Advances in Biomedical Engineering (ICABME), 2017.

[7] Kevin Peterson, Rammohan Deeduvanu, Pradip Kanjamala, Kelly Boles: “A Blockchain-Based Approach to Health Information Exchange Networks”. ONC/NIST Use of Blockchain for Healthcare and Research Workshop, 2016.

[8] Dubovitskaya A. et al. “Secure and trustable electronic medical records sharing using blockchain:, Proceedings of the AMIA 2017, American Medical Informatics Association Annual Symposium; Washington, DC, USA. 4–8 November 2017.

[9] S. Amofa et al., "A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data," 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, 2018, pp. 1-6. doi: 10.1109/HealthCom.2018.8531160

[10] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, 2017, pp. 1-5. doi: 10.1109/PIMRC.2017.8292361

[11] M. A. Rahman et al., "Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications," in IEEE Access, vol. 6, pp. 72469-72478, 2018. doi: 10.1109/ACCESS.2018.2881246

[12] Markakis, Evangelos, et al. "Acceleration at the Edge for Supporting SMEs Security: The FORTIKA Paradigm." IEEE Communications Magazine 57.2 (2019): 41-47

[13] M Gajewski et al., “Two-tier anomaly detection based on traffic profiling of the home automation system”, Computer Networks 158, pp. 46-60, 2019

[14] Tsampi, Katerina, et al. "Extending the Sana Mobile Healthcare Platform with Features Providing ECG Analysis." Mobile Big Data. Springer, Cham, 2018, pp. 289-321

[15] K. Moriarty (ed.) et al., “PKCS #1: RSA Cryptography Specifications Version 2.2”, RFC 8017, IETF, November 2016

[16] NIST Special Publication 800-57 Part 3, Revision 1. Available online: http://dx.doi.org/10.6028/NIST.SP.800-57pt3r1

[17] Hyperledger Fabric – open source blockchain framework. Project webpage: https://www.hyperledger.org/projects/fabric

[18] HL7: Health Level Seven. Project webpage: http://www.hl7.org

[19] The *openEHR* Foundation. Project webpage: https://www.openehr.org