RESEARCH ARTICLE OPEN ACCESS

# Blockchain Based Health Care Administration

**R.NAVIN KUMAR MCA., M.Phil..,M.THIRUMOORTHI **
Professor, Department of MCA, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India.
Email: navinsoccer07@gmail.com
Final MCA, Department of MCA, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India.
Email: thirumoorthi.g02@gmail.com

**********

## Abstract:

Block chain could be a technology that gives the power to form new business models and solves trust issues during a more efficient way. It can cause many research opportunities and business innovations. Academia and industry proposed many block chain based software solutions within a large range of domains. during this paper we present a system design where block chain technology is proposed to be utilized in the healthcare system, where the vital information regarding the medical analyses are shared between hospitals, medical clinics and research institutes supported access policies defined by the patients. so as to safeguard confidential data, our solution involves the employment of two sorts of chains: a personal one, the sidechain, which keeps information about real ID of the patients, and a public one, the main chain, which stores information about patients' health data marked with a brief ID. To test it, we developed the planning using Hyper ledger Fabric framework. Presented experimental results show good performance of the system in regard to the subsequent metrics: 1) the time needed to spot the medical data for a specific patient, and 2) the main chain propagation time of all the blocks within the peer to see network.

*Keywords* —Block chain, 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 spread of health related information is generated by clinics, hospitals and different e-health applications [1]. During their life, people interact with an oversized number of medical specialists, each of them stores data in their IT systems, resulting in a fragmented system and databases that don't seem to be interconnected. Block chain could be a new technology that supports sharing of values. In recent years, it's been applied in various areas, the foremost important is that the financial one. Block chain may be a digital ledger where there are stored all the executed transactions. It uses a distributed, peer-to-peer network to create endless growing list of ordered records called blocks. Every block contains a collection of signed transactions and is validated by the network itself, by means of a consensus mechanism. Copies of the block chain are distributed on each participating node within the network. Block chain is 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 consideration the user rights imposed by the legislation in

effect, like European General Data Protection Regulation (GDPR) EU 2016/679 on the protection of private data. GDPR applies to any entity that processes personal/health data and is established within the international organisation, or is established outside the EU, but processes data of persons from EU. Implementing such rules in blockchain technology could be a real challenge, considering the actual fact that almost all blockchain implementations are built as an immutable ledger. during this paper we propose an innovative model of health care IT system supported privacy preserving. Users are recognized as owners of their own data and have full control over it. they'll apply various security policies, like sharing data with specific clinics or institutions and may contribute anonymously to certain statistics. The blockchain uses public key cryptography to make an immutable, append-only, timestamped chain of content. Our system design proposes two styles of blockchains: a public mainchain and a non-public sidechain. reckoning on the sort of node (trusted or untrusted), each of them contains a copy of the mainchain, or both blockchains. because of privacy reasons and an outsized amount of knowledge generated by all the participating institutions and devices, the content of the nodes is made only by a collection of links to health data, permissions and other auxiliary information. the info themselves (the medical analysis) can be stored either by the institutions that generated it or within the cloud. The article is organized as follows. the following section presents an summary of related works within 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 leads to order to judge the performance of the proposed system. At last, the ultimate section concludes the article.

## II. RELATED WORKS

Within healthcare, variety of blockchain-based solutions are proposed to integrate clinics, doctors, and patients with the aim of providing improved quality services during a timely manner. [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 his or her contribution to aggregate anonymized medical data as mining rewards. Using such a system in reality, where personal data, whether anonymous, is employed for purposes apart from the initial one, may determine clients to not use such services. additionally, if it's not used an efficient anonymization process, the patients' identity are often disclosed, that the protection of private data is not any longer met.

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

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

Q. Xia et al. [5] propose a blockchain-based system that has medical data sharing among medical big data custodians in a very trust-less

environment. the most purpose of the blockchain is to keep up an immutable database where associated with delivery and request of knowledge are stored. The authors introduce a special form of child-block that's attached to the parent block as a side block. Its role is to avoid wasting 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, together with a sensible contract. it'll be activated with data decryption and can monitor the info. Processing and consensus nodes receive information regarding data handling, which is able to attach to the corresponding parent block – containing particular data request - as a side block.

In [6] it's proposed a blockchain-based healthcare system that integrates the patients, medical sensors, doctors and hospitals. the information are stored outside blockchain to boost the performance, whereas the blockchain is employed to store only a part of data or a pointer to that. Nodes called gateways, are devices that have enough power and energy, and will be laptops or mobile phones. The medical sensors transmit information to the system only through the gateways. Smart contracts are wont to maintain the access policies, as an examplepatient-doctor relationships, but the thanks to accomplish this task isn't described.

In turn, in [7] the authors present a healthcare blockchain approach for sharing patient data. The trust is predicated on a network consensus, which is an agreement on the proof of structural and semantic interoperability. During this process, called 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 also are 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 varied literature reviewed during this section doesn't provide concrete information or provides no information on how the confidentiality of private data is ensured. Medical analyses are personal data that has to be accessible only to the patient and to well-established entities. Reviewed proposals, yet as many others (for example, [8-11]), keep patient's IDs in publicly accessible blockchain transactions, and thus make patients prone to tracking records of their medical services. Our approach offers to patients the understanding that their data is well protected, jointly with her/his privacy. The proposed solution puts the patients first, so their medical data will be accessed only through security policies, and therefore the policy transactions are accessible through publicly available blockchain. However, the general public blockchain contains the patient's temporary ID only, therefore it doesn't 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, whether or not those are stored on clinics' datacenters. With in the following sections we detail this idea by presenting the system architecture, employment and experimental results.

## III. DESIGN OF THE PROPOSED SYSTEM

In this section we present the planning of a secure system that ensures the confidentiality and authenticity of the patient's medical data. The system includes the most actors of the health system, like 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 like the entities that have access to data, their type, the doctors and therefore the patients within the system, patients' medical information, and access policies to those data. Patients are recognized as owners of their medical analysis results, have full control over them and may apply access policies any time. Data dissemination is completed through blockchain technology, and every node within the network incorporates a complete copy of the ledger.

Considering personal data protection, the system covers two varieties of nodes: trusted and untrusted, furthermore as two varieties of blockchains, as shown in.

Figure 1. counting on the nodes' level of confidence, they will accessonly the general public blockchain referred to as mainchain (untrusted nodes) or both blockchains, more precisely the mainchain and also the private blockchain referred to as sidechain (trusted nodes).

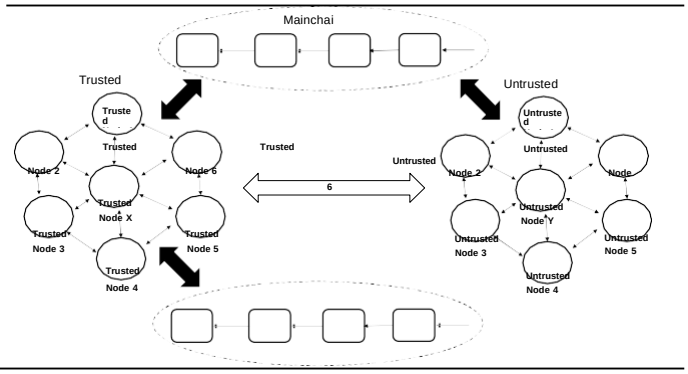


Figure 1: Logical concept of the system design

Among the most actors of the health system there are the 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 duplicate of the blockchain, to process incoming requests and to question the data. Nodes are divided into trusted nodes (approved medical institutions) – their role is to validate transactions and take decision if a brand new transaction is inserted within the blockchain; and untrusted nodes – all other entities who want to access medical data, as shown in Figure 2.existence of two forms of ledgers: a mainchain that's accessible by all the nodes and a sidechain that's accessible only by the trusted nodes. Each style of blockchain is represented as an immutable linked list of blocks and every block is represented by one or more transactions.

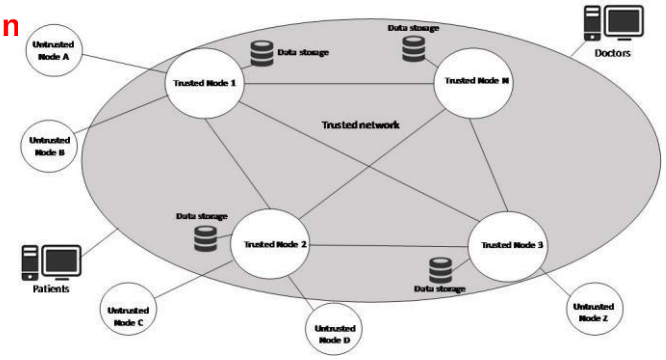


Figure 2: Peer to peer network

Figure 3 illustrates two styles of transactions kept in an exceedingly 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 within the mainchain, and also the analysis is stored within the clinic's internal database. So, within the mainchain there's saved only a reference (pointer) to the patient's health data, whereas the info 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 consideration that each one the nodes within the network have access to the present blockchain, mainchain transactions don't contain personal information like name, birth date, etc. These information are stored at external repository, as an example using the OpenMRS, an open source electronic anamnesis system[14].

On the opposite hand,each mainchain transaction contains a novel temporary ID which will discreetly identify the patient. The sidechain is distributed and maintained only by trusted nodes. to shield personal information, untrusted nodes don't have access to the present ledger. in line with 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 knowledge stored within the sidechain is required to link the patients' temporary ID that's found within the mainchain transactions and also the patients' real identity.

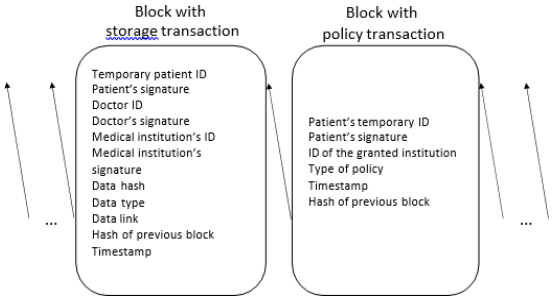


Figure 3: Mainchain storage and policy transactions

Each trusted node keeps a white list of all trusted nodes within the network. Trusted nodes authenticate to every other using the general public Key Infrastructure (PKI). We assume that adding a replacement node to the white list is managed by the supervising entity (for example national public health agency). during this way, the mainchain may be a reasonably permissioned blockchain, where all entities can send requests and browse the ledger, but only trusted nodes are allowed to feature new blocks. In turn, the sidechain may be a private blockchain, since it's accessible solely for trusted nodes. Therefore, for both blockchains fast and light-weight consensus algorithms are often applied that depend on majority confirmation. After a storage/policy transaction ismade, it's broadcasted to any or all trusted nodes. These nodes check the transaction validity and, if majority of them consider the transaction to be a sound one, the origin node creates the new block attaching the transaction to the mainchain, and next broadcast the updated ledger to the whole peer-to-peer network. Similarly, the identical procedure is applied within the sidechain case, except the last step when the ledger is redistributed only to trusted nodes.

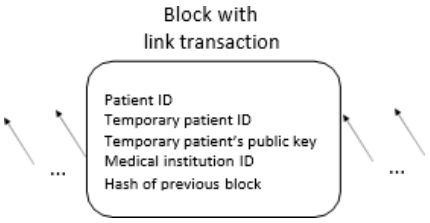


Figure 4: Sidechain link transactions

## A. Transactions

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

Storage transactions are created by medical institutions as a consequence of analyses made on patients. this sort of transaction contains the subsequent characteristics (see Figure 3): the temporary patient ID (unique for every 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 info type, the information link, the info hash and also the hash of the previous block. After a patient is consulted within a health center, the system authenticates his/her identity using PKI scheme and queries the sidechain for a singular 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 also the doctor's signature. The patient reads them and, if he/she agrees, signs and returns to the medical node that next creates a replacement mainchain transaction. The health facility who created the mainchain transaction is additionally answerable for creating a replacement transaction within a sidechain that records the correspondence between the temporary patient ID and real identity. Next, the medical node broadcasts the transaction to any or all other trusted nodes. The white list nodes check the transaction, more exactly validate all the signatures: the health facility which created it, the doctor's signature and also the patient's signature, further as authenticate the sending node. If the transaction passes the necessities, the new block is appended to the blockchain and therefore the clinic broadcast it.

Medical analyses are stored during a database external to the blockchains, but internal to the treatment room. At this stage, the

correspondence between the patient's temporary ID and patient's real identity is understood only by him/her (it is kept within the wallet application) and also the trusted nodes within the white list (through a sidechain transaction). This prevents untrusted nodes (research institutes, insurance companies, employers, etc.) to find personal information, because they're not allowed to question the sidechain. health center is liable for the medical data preservation and data authenticity, nevertheless the mainchain will be accustomed verify if the information has been modified using the hash stored in each storage transaction.

Policy transactions are created when the patient applies a specific security policy regarding his medical data. This sort of transaction contains subsequent 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 over one, since single policy transaction may involve different medical records), the ID of the granted institutionz2` (research institutes, assurance companies etc.) that created the transaction, the sort of policy (allow/deny) and also the hash of previous block. The entity which stores the medical analysis is responsible to form the storage transaction when the patient requests it. After the patient contacts the institution who stores the information, it creates a policy transaction signed by the patient and broadcasts it into the complete peer-to-peer network. All the nodes within the white list verify the transaction's validity. If the transaction passes this requirement, it's appended to the mainchain.

Link transactions are created in conjunction with storage transactions. this kind of transaction contains the subsequent fields (see Figure 4): the patient ID, the temporary patient ID (unique to every link transaction), the temporary patient public key (unique to every link transaction), the treatment room ID (which created the related storage transaction) and also the hash of previous block. These transactions are stored within the sidechain that's maintained and accessed only by trusted nodes. Its role is to save lots of the correspondence between the patient's real identity (patient ID) and his/her temporary identity,generated independently for every performedmedical analysis. during this way,the system ensures the confidentiality of private data because browsing ofknowledge stored withinthe mainchai n, which is accessed by all the nodes, doesn't 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 go with the necessities imposed by the legislation regarding the protection of private data, like EU General Data Protection Regulation(GDPR).

One of the rights granted by GDPR is to access one's own personal data. The medical institutions make sure the data availability and authenticity, so users have the chance to question the blockchain about each transaction regarding its ID. Another assured right is data portability – a user has the likelihood to transfer its data from one data controller to a different. In our system design, data access is created through the safety policies stored within blockchain. the correct of an user to object to the processing its personal data is ensured by the very fact that processing personal data is formed only after the patient agrees to access it. the correct of information erasure is performed by the medical institutions that store / control data. because the data isn't stored within the blockchain, the method won't ail the blockchain immutability concept. Right to rectification is finished through right to data erasure and therefore the creation of a brand new storage transaction. the correct just in case of breach is ensured by the actual fact that an user can check if her/his data are altered through the information hash stored within the mainchain. Through policy transactions that are public, the user can see who has (or had previously) access to her/his medical data, therefore the right to be told is achieved.

### B. Proposed securitymechanism

The purpose of the proposed security mechanism is to guard the identity of patients and also

the confidentiality of private data. The system uses methods like sidechains and temporary IDs to ensure the patient's anonymity. Moreover, the patients' consent to the publication of knowledge is represented by digital signatures. Digital signatures are wont to associate medical analysis with doctors that made them and therefore the issuing medical institutions. Since the mainchain is accessible by non-trusted entities, all stored information that may be attributed to patients, like the ID or electronic signature, is exclusive to every entry. Table I presents the algorithm for creating storage transaction, which has the generation of patient public-private keys and signing medical analysis. The mechanism relies on cryptographic key pairs used for authentication and messages signing. In our implementation, we use the public- key cryptosystem RSA [15], one among the foremost 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 proper 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 mod 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 (ski, pki) is generated at patient wallet application; each pair of keys is exclusive for every medical analysis m. The client publishes his public key (pki) because the trusted nodes verify the storage transaction validity (the secret's later stored within the link transaction). almost like the public- private key pair, the patient's identity is exclusive within the mainchain. The patient incorporates a static ID which is found within the sidechain and is thought only by trusted nodes. within the next steps, the patient receives the results of the medical analysis, m, signed by the clinic (sc) and by the doctor (sd). the general public keys are shared on a frenzied key server; thus the patient can verify both signatures. Signing the medical analysis by patient (sp) implies that he/she agrees to publish the information within the mainchain. After acceptation of medical analysis by the patient, the clinic node generates a storage transaction and distributes it to the opposite nodes to verify.

TABLE II. TRANSACTION VERIFICATION

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

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's the source of the new transaction, and on the correct side of the table are presented the operations performed by each of the trusted nodes (except the generator node). The transaction may be a message (m) signed by the patient (sp), the doctor (sd) and also the clinic (sc). Trusted nodes check each of those signatures using the general public key of every of the three entities: (np, Ep), (nd, Ed), (nc, Ec). Public keys are known bythe entire peer-to-peer trust network. The results of those three operations could be a new set of messages (vp, vd, vc). Message digest H() is calculated for every of those values. additionally, the message digest H'() of the signed data is computed. If each pair of digests is equal, then the signatures are valid. For the whole 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 ai (1 or 0). The generator trusted node collects all the answers from all the trusted nodes and computes the proportion of positive answers. If quite 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 whole peer-to-peer network.

The security level within the proposed schemas is decided by the parameter n (which jointly with e creates a public key), more precisely its length, in bits - the more sensitive is that the information, the longer the key length must be. in keeping with 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 OS. the aim of the implementation is to check the proposed solution, to spot security breaches, leakage of knowledge, identify possible components that weren't taken under consideration when the system was designed, and to spot possible system optimization. The prototype application implements the most components of a blockchain based software like blockchain display, blockchain query, adding new transaction, transactions validation, creating blocks and appending them to blockchain, broadcast blockchain, and blockchain integrity check. Within one software package, the applying creates a virtual network within which terminals are considered as nodes. These terminals can emulate both, trusted and untrusted nodes. Within trusted nodes, the user can perform operations like mainchain view, sidechain view, add storage transactions and add policy transactions. Within untrusted nodes, there will be performed actions like view mainchain and query the appliance to get the regard to medical analysis supported patients' temporary IDs that are found within the mainchain and are unique for every analysis. Performance tests are done by test automation, introducing functions for automatically generating an outsized amount of information, and for measuring the execution time. Their purpose is to check the performance of the system, the flexibility to handle an oversized amount of information, the execution time, and also the correctness of software modules implementation. within the following, there are presented two tests that take under consideration the time needed to spot the medical data for a given patient, and therefore the mainchain propagation time to any or all the blocks within the peer to look network.

The tests were performed on the virtual machine on which are installed and configured the prototype application and other auxiliary software modules, like 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 therefore the peer-to-peer network. computer the search time is satisfactory, because it may be 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 will expect that even for a ledger with various blocks the search time are still acceptable using the acceptable technical infrastructure (servers with good performance metrics).

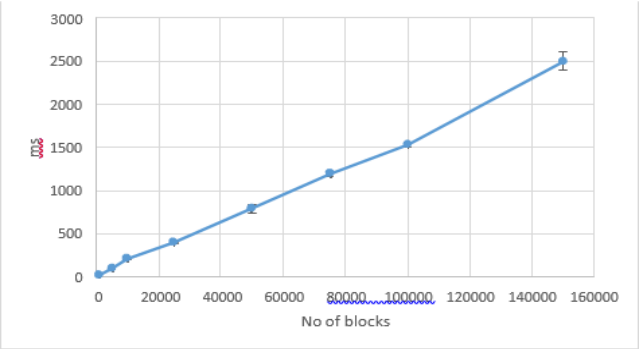


Figure 5: Time required to find the medical data of a given patient

Figure 6 presents the results, with 95% confidence intervals, of the test that measures the propagation time of the mainchain to all or any nodes in step with the amount of blocks. The OY axis represents the time (in seconds) after which other nodes update their ledger and also the OX axis represents the amount of blocks within the mainchain. The propagation of mainchain could be a results of validation of a brand new storage or policy transaction within the consensus mechanism. After over 50% of the nodes consider the

150,000 blocks). During the quality operation of the system there's no have to transfer the entire chain whenever, but only the lasts blocks of the ledger. during 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 or any nodes, in a very world application depends greatly on the geographic position of the medical clinics' IT equipment and therefore the bit rate available within the network.

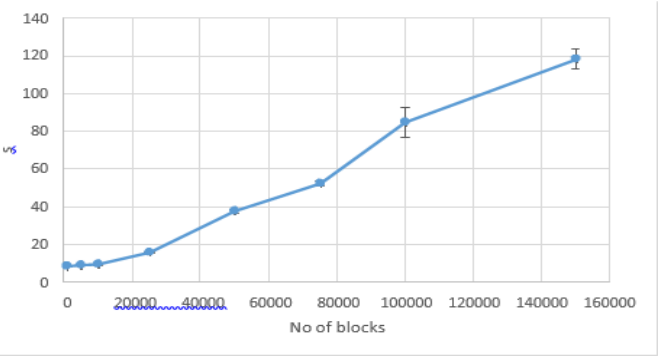


Figure 6: Propagation time of the mainchain to all the nodes

## V. CONCLUSION

Medical analyses are personal data that has to 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 like research institutes, insurance companies, etc. Using technologies like blockchain and public key cryptography, the system design ensures the confidentiality of private data and recognizes the patient because the owner of his data. Thereby, the proposed system meets the necessities imposed by regulations on personal data protection. Access to data is transparent, so health information is 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 world would bring many advantages to all or any the actors involved. Patients should easy manage their medical analyses, hospitals can provide a higher quality medical service, while research institutions can get easy accessibility to a awfully useful health database.

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

## ACKNOWLEDGMENT

The research presented during 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 therefore the Ambient Assisted Living (AAL) project vINCI: "Clinically-validated INtegrated Support for Assistive Care and Lifestyle Improvement: the Human Link" (AAL2017-63-vINCI) co-funded 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