Blockchain Tree for eHealth

1st Sergii Kushch
Security and Trust research unit
Bruno Kessler Foundation
Trento, Italy
CONFIRM Centre, University of Limerick
Limerick, Ireland
kushch@yaros.co

2nd Silvio Ranise
Security and Trust research unit
Bruno Kessler Foundation
Trento, Italy
ranise@fbk.eu

3rd Giada Sciarretta
Security and Trust research unit
Bruno Kessler Foundation
Trento, Italy
giada.sciarretta@fbk.eu

Abstract—Design of access control mechanisms for healthcare systems is challenging: it must strike the right balance between permissions and restrictions. In this work, we introduce a novel approach based on the Blockchain technology for storing patient medical data and creation an audit logging system able to protect health data from unauthorized modification and access. The proposed method has a tree structure: a main chain linked with patient’s identity and one or several subchains used for storing additional critical data (e.g., medical diagnoses or access logs).

Index Terms—Blockchain, ID-card, Personal Data Protection, Blockchain Tree, Blockchain in Healthcare

I. INTRODUCTION

Design of access control mechanisms for healthcare systems is challenging. On the one hand, as these mechanisms deal with sensitive data, they must guarantee: confidentiality, in the sense that only the patient and doctors with specific access control policies and purposes can access the patient’s Electronic Health Records (EHR); and integrity, the EHR should not be modified without a clear evidence. On the other hand, they should protect safety of the patient, thus allowing doctors to access patient’s information quickly and without interruptions (e.g., in case of emergency). However, along with this flexible and frictionless access control comes the temptation of taking advantage of it. Indeed, as reported in [1], 58% of incidents involved insiders and this fact makes healthcare the only industry in which the generation of blocks by this algorithm is too expensive. In addition, the miners, who mine new blocks, should be paid for each transaction. For the healthcare systems, it would be optimal to use an algorithm in which the generation of blocks is as cheap as possible and all transactions are free.

a) Healthcare Use Case: As shown on Figure 1, the nodes of the considered network are servers of local branches of the healthcare system (hospitals, polyclinics or other medical organizations) that store citizens’ personal information and their electronic health records. The users of the information are patients, doctors, as well as authorized third parties. The network structure is a classical peer-to-peer (P2P) topology in which all elements are interconnected. All nodes are equal. The network has a fixed number of nodes. Each node is verified and included in the list of approved nodes. This list is stored on each node and only devices from this list can create new blocks.

The main contribution of this paper is the introduction of a novel approach based on creation of a Blockchain tree, which is considered as a distributed storage of patient’s EHR as well as an audit logging system able to protect EHRs from unauthorized modifications, and the use of the Proof of Authority (POA) consensus algorithm. In this case, all access attempts (successful and unsuccessful) will be stored in one of the subchains. This will not allow insiders to change logs about access (to hide privilege abuse) and any changes to EHRs
without authorized access.

b) Paper Structure: The structure of this paper is as follows. In Section II we provide the background on Blockchain technology. Our approach of using the Blockchain Tree in the healthcare system is presented in Section III. Finally, we present the conclusions obtained from our research and discuss the possibilities for future work in Section V.

II. BACKGROUND

Blocks of Blockchain are permanently recorded files that contain information about users’ transactions. All transactions in a block are represented as strings in hexadecimal format (raw transaction format), which is hashed to obtain transaction identifiers (txid). On their basis, a hash of the block is built, which is taken into account by the subsequent block, ensuring the immutability and coherence of the registry. The unit hash value is compiled using the Merkle Tree, the concept of which was patented by Ralph Charles Merkle in 1979.

A Merkle Tree or hash tree is a binary tree, leaf nodes of which are transaction hashes, and internal vertices are the results of the addition of the values of the associated vertices. The process is repeated until a single hash is obtained - the root of the Merkle tree (Merkle Root).

Figure 2 shows an example of a hash tree with four transaction-leaves L1, L2, L3, and L4. The construction of the tree is as follows: (i) Hash 0-0, Hash 0-1, Hash 1-0, and Hash 1-1 are calculated as the hashes of the associated transactions (hash(L1), hash(L2), hash(L3), and hash(L4), respectively); (ii) Hash 0, Hash 1 are calculated from the sum of transaction hashes (hash(Hash 0-0 + Hash 0-1), hash(Hash 1-0 + Hash 1-1), respectively); (iii) finally the Top Hash is calculated as hash(Hash 0 + Hash 1). This scheme can be generalized for a tree with n leaves. Since the Merkle tree is binary, the number of elements at each iteration must be even. Therefore, if a block contains an odd number of transactions, then the latter one is duplicated and added to itself, e.g., hash(hash(L5) + hash(L5)).

In Blockchains, hash trees allow simplified verification of transactions: the verification of the integrity of the Blockchain entries is done by checking the hash blocks. Indeed, the main advantage is that clients, willing to verify the integrity of data, do not need to recalculate all the hashes to verify the transaction information. They only need to ask for Merkle proof: it consists of the concatenation of the left and the right hash of a branch, and validation of the result according to the parent branch. This step is repeated until the Merkle root is found. By adding the requested hashes and comparing them with the root, the client makes sure that the transaction is in its place.

This approach allows us to work with comparatively large amounts of data, since it significantly reduces the load on the network, while only the necessary hashes are downloaded. For example, the weight of a block with five maximum size transactions is more than 500 kilobytes. The weight of the Merkle proof in the same case will not exceed 140 bytes.

Created block must be confirmed by more than 50%+1 of verified nodes. After that, information is written in the block, added to the chain and sent to other nodes. Thus, each element of the system stores a complete Blockchain. In the case of detecting a change of information in an existing block, this block will be automatically replaced with the “right” one that exists on at least 50%+1, of other nodes of the network.

Given that the blocks in the chain are sequentially linked to each other, the alteration of one block will lead to change of the entire chain. This will be detected and corrected by the rest of the network nodes.

III. MAIN RESULTS

The solution we offer consists of several interconnected parts. We propose to create a Blockchain in which each block contains information about one person (name, surname, date of birth, etc.) that allows you to uniquely identify them. In its turn, each block is a “Genesis Block” for a subchain containing medical record for the same person. Also, we suggest to create a second subchain to save user logs.

A. Blockchain Structure

As shown in Fig. 3, the solution we propose consists of several interconnected parts organized as a Blockchain tree.
Each main block (green color - B0, B1, ..., Bn) contains information about a patient (name, surname, date of birth, etc.) and is a “Genesis Block of two subchains.

Subchain 1 (yellow) contains a medical record for the related patient. The blocks have two indices:

- the 1st (from 1 to n) is the block number in the main Blockchain and represents the patient identity;
- the 2nd (from 1 to m) is the block number in Subchain 1 and represents the medical record of the patient.

For example, B23 is the third medical block of the second patient. It should be noted that the list of diagnoses, prescriptions, test results are constantly updated. Doctors should have access to both latest results and entire medical history. Therefore, each block in the chain stores a link to the previous block, recursively. Thus, our solution allows a client to automatically assemble both latest results and all the links to the history into a single document.

Another level of protection is the ability to add information to the Blockchain only after validating the patient’s card and entering the user’s password (or using another cardholder authentication method).

Subchain 2 (red) contains user logs and consists of an additional index (from 1 to k). For example, B234 is the fourth log block of the third medical block of the second patient. In our opinion, addition of a block containing the logs will help investigate cases of unauthorized access incidents, since the logs stored in a Blockchain will be impossible to change or delete. Also, it will be impossible to change stored information (diagnoses, prescribed treatment, etc.) for the purpose of insurance fraud or for other illegal purposes.

By entering the user’s password (or using another cardholder to the Blockchain only after validating the patient’s card and assembling both latest results and all the links to the history into a single document.

For example, B23 is the third medical block of the second patient. It should be noted that the list of diagnoses, prescriptions, test results are constantly updated. Doctors should have access to both latest results and entire medical history. Therefore, each block in the chain stores a link to the previous block, recursively. Thus, our solution allows a client to automatically assemble both latest results and all the links to the history into a single document.

Another level of protection is the ability to add information to the Blockchain only after validating the patient’s card and entering the user’s password (or using another cardholder authentication method).

Subchain 2 (red) contains user logs and consists of an additional index (from 1 to k). For example, B234 is the fourth log block of the third medical block of the second patient. In our opinion, addition of a block containing the logs will help investigate cases of unauthorized access incidents, since the logs stored in a Blockchain will be impossible to change or delete. Also, it will be impossible to change stored information (diagnoses, prescribed treatment, etc.) for the purpose of insurance fraud or for other illegal purposes.

After creating a new block in the yellow Subchain, a new block is also created in the red Subchain that contains four hashes: HASH of the main block containing basic information about a patient; HASH of the new block of the yellow Subchain; HASH of the previous block of the red Subchain; HASH of the current block (Fig. 4).

Thus, triple cross-reference between two Blockchains is performed, which significantly complicates the possibility of tampering with blocks or parts of a chain.

There are different possible interactions with our system: on-boarding of a new patient, logging new health data, reading an existing health data. Let us assume that the user has undergone the procedure for obtaining valid access credentials.

The on-boarding of a new patient leads to the creation of the following blocks in our Blockchain tree: (i) a block in the main Blockchain containing personal information; (ii) a genesis block for Subchain 1; and (iii) a genesis block for Subchain 2.

Logging of patient’s health data by a medical officer leads to creation of a new block in Subchain 1 with automatic creation of the corresponding block in Subchain 2. The block in Subchain 1 contains new health data, while the block in Subchain 2 contains log information about doctor’s identity, date, local time, place, which information was added and so on. In case of unsuccessful entry, the new block contains information about access attempt.

Instead, the reading of patient’s health data in Subchain 1 (for example, to retrieve information about test results, appointments, etc.) automatically creates a new block only in Subchain 2. This block contains information about user’s identity (patient or doctor), date, local time, place, which information was viewed and so on. In case of unsuccessful entry, the new block contains the access attempt.
B. Further Considerations

We report below some discussions on borderline cases and some extra features that should be taken into consideration.

a) The Change of Fiscal Code: The main identifier the chain is attached to is a personal identifier. In Italy, this is the fiscal code. However, it should be noted that this code is tied to a person’s name and surname, thus it will change if they change. In this case, we will need to create an additional block in the Blockchain. This block will contain information about the new code, the old code, a link to the previous card and link to the rest of (the main) Blockchain, which existed before the name change. In this way, we avoid a Blockchain rupture. Repeated name changes can complicate the system, however, this will help to avoid identity fraud. One of the ways to avoid this Blockchain complication is to introduce a single ID as a personal identifier that does not change during life.

b) Stop Adding New Records in Blockchain: It is also necessary to envisage a scenario when the patient changes the citizenship or dies. In this case, it is necessary to block the possibility to add new blocks to the patient’s Subchain 1. After Subchain 1 is closed, saved information can only be viewed (without a chance of adding new data). Subchain 2 continues to grow with each following access or access attempt. This will provide additional protection of the system against possible fraud with fake recipes and medical insurance. We suggest to add a “Final Block” that marks the end of the Subchain and forbids addition of any new information.

c) Collection of information from several blocks by user interface: The block contains the latest test results and a link to previous test results of the same type. If the user needs to build a history of tests or a medical record - the records are read sequentially from all the blocks that contain them by clicking on the links.

The software of an user interface (Fig. 5) requests information from the last block. If the block contains the necessary record, it is added to the report, if not, the service record is read from the next block, etc.

IV. RELATED PROJECTS

Currently, there are several start-ups and commercial projects aimed at implementing Blockchain in healthcare. Developed on the Ethereum Blockchain, MedRec [21] is a “system that gives priority to the patient agency by providing a transparent and accessible review of the medical history or medical record.” MedRec is designed to store all patient’s information in one place, which makes it easier for patients and doctors to look through it.

Connecting Care [22] “uses care coordination and financial forecasting to help suppliers in integrated payments understand what happens to patients when they leave the hospital.” It is currently on the market, helping health care providers determine how much they will earn on patient care when included multiple organizations.

The Thai Medical University Hospital and Digital Treasury [23] recently released phrOS. It aims at increasing transparency between medical institutions by placing all the patient’s medical information in the Blockchain.

Bloxine FarmaTrust [24] intends to help fight counterfeit drugs. The chain of supply visibility tracks drug changes or changes in any way. And finally, the Consumer Confidence app allows customers to see their drug life cycle.

Electronic health records (EHR) can be complex in management. The patient’s EHR by one healthcare provider may differ from the EHR by another provider. MTBC [25] intends to change this by using application programming interfaces (APIs) and Blockchain. The idea is to pass over control into the patient’s hands. The patient will be able to decide whether to transfer records from one doctor to another. The Blockchain API works on the Hyperledger platform and is currently available.

Hashed Health, a company focused on development of Blockchain for healthcare, intends to make healthcare sector authorities more transparent and accessible. With Professional Credentials Exchange [26], chain members can check credentials and track records from various health professionals. This simplifies the process of hiring and provides the unchanging history of a professional medical career.

Change Healthcare develops a wide range of products focused on payments and management of data in the health sector. One of their latest developments [27] simplifies claims management and profitable cycle management. It helps healthcare systems manage claims and money orders, improve patient fee collection, minimize bans and under-payments, and manage daily income and business cycles more efficiently.

With MedicalChain [28] you get full access to and control over your personal medical data. Users can give doctors immediate access to their medical card use their mobile devices while they are stored in a reliable Blockchain. Patients can also wear bracelets that medical workers can scan to access a person’s medical history if they are unconscious. It also offers telemedicine communication that allows online video consultation with doctors.

As it can be seen from the aforementioned list, existing projects are aimed at finance, medicines and information
exchange between patients and medical institutions. In
dition, most of the existing blocks are commercial projects.
Unlike them, our model involves free participation of medical
institutions. Moreover, there will be no need to pay for each
transaction, which is reasonable for such an important sphere
as provision of medical care. Another important point is the
registration of access to user’s personal information for a
separate Blockchain. This will protect the system from hacking
and in the case of disclosure of confidential information, it will
quickly find the culprit, as the system is protected from erasure
or replacement of access logs.

V. CONCLUSION AND DISCUSSION

In this paper we introduce a novel methodology based on
Blockchain technology for building storage, access control
and document verification mechanisms in healthcare. The
proposed work is based on Subchains, connected to a main
Blockchain and each other. The solution is more security
than currently existing due using of the mutual intersection
of several Blockchains in one system. This makes the process of
hacking and falsification of critical information more difficult,
since in the event of an attack it will be necessary to change
not one but several Blockchains, which considerably increases
the cost of such an attack and makes it unprofitable for the
attacker. The noted above methodology for building a storage
system, access control and document verification can be used
not only for medical-cards but also for other documents, for
example for ID-cards, driver’s licenses, education documents,
personal medical information and social security cards, etc.

In addition, the proposed way to build a Blockchain allows
you to create an arbitrary number of additional Subchains and
control access to information they contain. For the healthcare
system, this may be, for example, information on the availability
of health insurance, which needs to be updated regularly.

Obviously, this work is only the first step in introducing the
proposed concept into the system of preserving and protecting
personal information in medicine, as well as to increase the
level of access control in the sphere. The proposed methodology
still requires further improvement in order to contribute to
its reliable implementation and legal compliance (in particular
referring to GDPR). For example, we left out some problems of
building real networks, such as devices and communication lines
delays. In future work, we will consider the problem of
using various consensus algorithms with different types of
Blockchains.

REFERENCES

[1] (2018, Dec) Protected health information data breach report.
Verizon. [Online]. Available: https://enterprise.verizon.com/resources/reports/2018/protected_health_information_data_breach_report.pdf

[2] (2019) A blockchain platform for the enterprise. Hyperledger Fabric. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.4/

[3] L. Debin and L. J. Camp, “The bitcoin backbone protocol: Analysis and applications,” Proof of Work can Work, Fifth Workshop on the Economics of Information Security, 2006.

[4] by E. Oswald and M. Fischlin, Eds., The Bitcoin Backbone Protocol: Analysis and Applications, ser. Lecture Notes in Computer Science, vol. Vol.957. Springer, Dec 2015. [Online]. Available: https://ia.cr/2014/765

[5] S. Matsuo, K. Miyazaki, A. Otsuka, and D. Basin, How to evaluate the security of real-life cryptographic protocols? the cases of ISO/IEC 29128 and CRYPTREC., ser. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. Jan 25-28 2010, vol. Vol.6054, no. 11, pp. 182–194. [Online]. Available: https://doi.org/10.1007/978-3-642-14992-4_16

[6] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, “Proof of activity: Extending bitcoin’s proof of work via proof of stake,” SIGMETRICS Perform. Eval. Rev., vol. 42, no. 3, pp. 34–37, Dec 2014.

[7] (2018, Mar) Eos.io technical white paper v2. Eos.IO. [Online]. Available: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

[8] A. Koles. (2018, Jun) How blockchain could change the global remittance industry. [Online]. Available: https://www.bankingtech.com/2018/06/how-blockchain-could-change-the-global-remittance-industry/

[9] (2018) Blockchain in logistics, perspectives on the upcoming impact of blockchain technology and use cases for the logistics industry. DHL Trend Research. [Online]. Available: https://www.logistics.dhl/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf

[10] S. Kushch and F. Prieto-Castrillo, “A review of the applications of the blockchain technology in smart devices and distributed renewable energy grids,” CADCAI: Advances in Distributed Computing and Artificial Intelligence Journal, vol. 6, no. 3, Dec 2017. [Online]. Available: http://revistas.usal.es/index.php/2255-2863/article/view/ADCAI2017637584

[11] F. Prieto-Castrillo, S. Kushch, and J. M. Corchado, “Distributed sequential consensus in networks: Analysis of partially connected blockchains with uncertainty,” Complexity, vol. 2017, Nov 2017. [Online]. Available: https://doi.org/10.1155/2017/4832740

[12] Blockchain for Dynamic Nodes in a Smart City, Apr. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8767336

[13] BloXHIE: A BLOCKchain-Based Platform for Healthcare Information Exchange, 2018.

[14] M. Jakobsson and A. Juels, Proofs of Work and Bread Pudding Protocols. Kluwer Academic Publishers, 1999, pp. 258–272.

[15] Proof of Work can Work, May 2004.

[16] V. Buterin. (2013, Nov) What proof of stake is and why it matters. [Online]. Available: https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463

[17] U. W. Chohan, Proof-of- Stake Algorithmic Methods: A Comparative Summary, ser. TNotes on the 21st Century. University of New South Wales, Canberra, Feb 2018. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3131897

[18] A. Beikverdi. (2015, Mar) Proof-of-importance: How nem is going to add reputations to the blockchain. [Online]. Available: https://cointelegraph.com/news/proof-of-importance-nem-is-going-to-add-reputations-to-the-blockchain

[19] I. Bentov, A. Gabizon, and A. Mizrahi, Cryptocurrencies without Proof of Work, ser. Lecture Notes in Computer Science. Springer, Berlin, 2016, vol. Vol.9604.

[20] (2012) Hash tree.svg. Azaghal. [Online]. Available: https://commons.wikimedia.org/w/index.php?curid=1815788

[21] (2019) Blockchain to improve medical record access. [Online]. Available: https://cointelegraph.com/news/blockchain-to-improve-medical-record-access

[22] (2018) Simplyvital health. SimplyVital Health. [Online]. Available: https://www.simplyvitalhealth.com/

[23] (2018) Healthcare blockchain operating system. [Online]. Available: https://phros.io/thome

[24] (2018) Farmatrust progress report dec 2018. FarmaTrust. [Online]. Available: https://medium.com/@farmatrust/farmatrust-progress-report-dec-2018-4282442e0d7b

[25] (2018) Mtbc takes electronic health records to the next level with blockchain technology. MTBCInc. [Online]. Available: https://it.mtbc.com/news-releases/news-release-details/mtbc-takes-electronic-health-records-next-level-blockchain

[26] (2018) Farmatrust progress report dec 2018. FarmaTrust. [Online]. Available: https://medium.com/@farmatrust/farmatrust-progress-report-dec-2018-4282442e0d7b

[27] (2018) Mtbc takes electronic health records to the next level with blockchain technology. MTBCInc. [Online]. Available: https://it.mtbc.com/news-releases/news-release-details/mtbc-takes-electronic-health-records-next-level-blockchain

[28] (2018) Nashvillle and austin. two it cities and the race for healthcare innovation. Hashed Health. [Online]. Available: https://hashedhealth.com/newsletter-may-2019/

[29] (2017) Change healthcare announces general availability of first enterprise - scale blockchain solution for healthcare. ChangeHealthcare. [Online]. Available: https://www.changehealthcare.com/

[30] (2019) The medicalchain whitepaper. MedicalChain. [Online]. Available: https://medicalchain.com/en/whitepaper