Architecture and Value Analysis of a Blockchain-Based Electronic Health Record Permission Management System

Michaël Verdonck, Geert Poels
Faculty of Economics and Business Administration, Ghent University;
michael.verdonck@ugent.be;
Geert.Poels@ugent.be;

Abstract. Adopting healthcare information systems and electronic health records (EHRs) result in various benefits for the healthcare sector such as real-time decision support and availability of critical medical information. Despite the many benefits that are associated with adopting EHRs, the transition to digitally stored and shared records hold various challenges regarding the privacy and security of medical data. This paper aims to offer an alternative design to manage EHRs with blockchain technology, where the emphasis of our design lies in adopting blockchain and smart contracts as a permission management database. We present a general overview of the architecture of our blockchain-based EHR permission management system and describes the value exchanges that take place between the different parties participating in the EHR ecosystem in which our blockchain-based system is to be implemented.

1 Introduction

Medical data is progressively being represented and stored electronically [1]. As such, health information technology and electronic health records (EHRs) are increasingly viewed as means to improve the efficiency, quality and safety of health systems [2]. Adopting healthcare information systems and EHRs result in various benefits for the healthcare sector such as real-time decision support for clinicians or making critically clinical information available to health providers [3]. Besides healthcare advantages, health information exchange in the form of EHRs are estimated to have substantial financial benefits [4, 5]. However, despite the many benefits that are associated with adopting EHRs, the transition to digitally stored and shared records holds various challenges regarding the privacy and security of medical data [6, 7]. Data stored electronically is prone to be copied, distributed, and mined for confidential information. Data breaches and the consequent loss or misappropriation of data can expose patients' confidential information and lead to hefty fines for hospitals[1]. Another issue related to adopting EHRs is the lack of interoperability between the different systems that store patient's data. These interoperability challenges are related to the sharing of data

[1] https://eurocloud.org/news/article/fine-of-eur-460000-imposed-on-dutch-haga-hospital-by-dutch-data-protection-officer-the-first-dutch/

between different information systems storing EHRs, where each have their own data format and protocol to share EHRs.

In order to tackle these problems, recent research efforts have been investigating the application of distributed ledger technology, more in particular *blockchain* technology. While originally introduced as a technology to support new forms of digital currency [8], blockchain has evolved as a promising foundation to support any type of transactions in society. In its essence, a blockchain is a data structure that is composed of an ordered, back-linked list of blocks of transactions [9]. Through the years, several new blockchain technologies have emerged, that act both as a database that records data transactions between parties, while also providing a computational platform for executable programs, i.e., *smart contracts*. More specifically, smart contracts can carry and conditionally transfer digital assets or tokens between parties [10]. Since smart contracts are stored and executed on the blockchain platform (assuming a public blockchain), they can be publicly viewed by parties having access to this platform. This feature also makes that their execution runs in a predictable and transparent manner. Consequently, these unique features give blockchains and smart contracts certain advantages such as traceability, transparency and enhanced security. For instance, a survey by IBM [11] predicts that blockchain technology will be used to manage clinical trial records, supervised compliance and EHRs.

Given this new technology's distinct advantages, several research efforts have aimed to leverage the unique properties of blockchain to manage authentication, confidentiality, accountability and data sharing of EHRs. For instance, Azaria et al. [12] developed the blockchain implementation 'MedRec' to demonstrate how principles of decentralization might be applied to largescale data management in an EHR system. They propose a modular design in order to integrate existing, local data storage solutions while facilitating interoperability. Through incentivization (e.g., access to aggregate, anonymized data) of medical stakeholders such as researchers and public health authorities, they aim to engage these stakeholders in becoming the miners of the blockchain network. Another solution called 'MedBlock' focuses on the privacy of information by adopting the blockchain for access control and encryption purposes. In their design, a certification authority acts as a system administrator of the blockchain, where the blockchain manages pointers of the record as to find the true storage address of information of the EHR. A processing layer that is composed of local community hospitals and their servers can access and modify patient records, which are then uploaded to a supervising hospital. While the above mentioned blockchain-based EHR systems have their respective advantages and strengths, the adopted blockchain is often implemented to simply store the memory address of an EHR record, where different records are still stored and secured at databases of local hospitals. Consequently, interoperability between healthcare providers remains a problem, while they are also still responsible for the security and maintenance of their own data – an expensive and strenuous task.

This paper aims to offer an alternative design to manage EHRs with blockchain technology. More specifically, the emphasis of our design focuses on adopting blockchain and smart contracts as a *permission management* database and engine. Additionally, we aim to leverage the strengths of each actor or technology within our design, allowing every actor to focus on their specific responsibilities and core tasks. For instance, a healthcare provider should not be occupied with maintaining and securing patient data. Instead, a healthcare provider should have the data available of a certain patient when needed to fulfill its responsibility to deliver care to that specific patient. Thus, this paper aims to design a blockchain-based EHR permission management system, that facilitates the automation of a patient's permissions to EHR access and updates for different parties, e.g., healthcare providers, patients, governing bodies, etc. Through the introduction of smart contracts, we aim to design an information system that leverages both the advantages of blockchain technology (traceability, immutability and authentication) and the advantages of existing software systems and database management systems (transaction speed, storage availability etc.).

The section below gives a general overview of the architecture of our blockchain-based EHR permission management system and describes the value exchanges that take place between the different parties participating in the EHR ecosystem in which our blockchain-based system is to be implemented. To facilitate the value analysis, e^{3}value modeling is used as a tool. The e^{3}value model of the EHR ecosystem shows for each involved party the value that is captured from using the proposed blockchain-based EHR permission management system.

In our conclusion, we will discuss future research efforts that we will undertake to implement and evaluate this blockchain-based EHR management system.

2 Architecture of a blockchain-based EHR management system

In our design, we identify five roles: *patient*, *requestor* (e.g., healthcare provider, insurance company, researcher etc.), *governing body* (e.g., government), *data custodian* and the *smart contract(s)* (or more generally the blockchain itself). While other research efforts have focused on creating a network without a governing body [12, 13] – we believe that this role is still crucial. We do not argue that a blockchain implementation without governing body cannot be accomplished, we believe however that the technology is still too immature and lacks an overall adoption in current society. Hence, we propose a blockchain-based information system that is highly dependent on a governing body in order to be operational and to be adopted by healthcare providers and patients. Below, we will discuss the role, actions and tasks of each actor of our design in more detail. Figure 1 gives a general overview of the different interactions that take place between the users and the system.

Additionally, we will describe the main value exchanges that take place between the different parties participating in this ecosystem through the e^{3}value model shown in Figure 2. As an early requirement engineering technique, e^{3}value modeling is used to study the business ecosystem in which a new IT system is to be implemented. The technique has been used before to help analyzing whether blockchain-based systems build a sustainable business case for the ecosystem parties [14]. The value analysis focuses on how the blockchain-based system will affect (i.e., enable, facilitate, automate, optimize, etc.) the creation and delivery of value within the ecosystem.

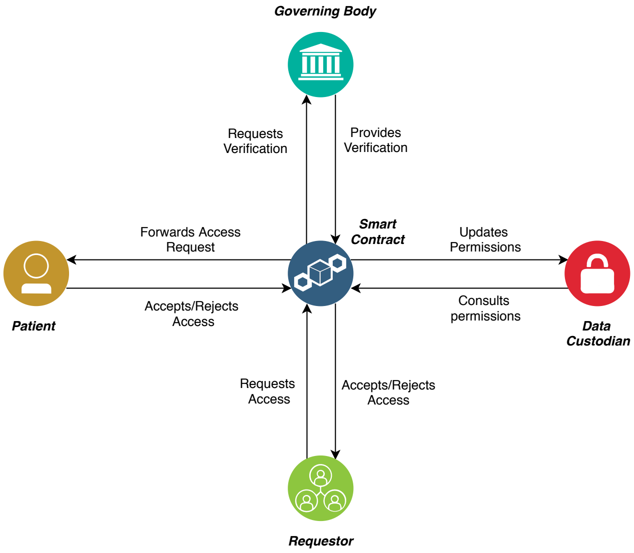

Figure 1: User interactions of the Blockchain-based EHR Permission Management System

Patient

A patient will have full control over his or her patient record. As can be viewed in the value model in Figure 2, a patient requests privacy and traceability over his/her EHR data while giving or denying permission requests that are being handled by the smart contract. More specifically, a patient will be able to do more than only accept or decline the request. A patient can specify the access of a certain healthcare provider (or health insurer for that matter) by deciding if the access provided should only be read, or if the requestor can also modify the record – for instance to add additional information to the record concerning a certain treatment. Moreover, a certain time frame can be assigned to any healthcare provider that requires access (e.g., ranging from a day to a year). Through querying the ledger of the blockchain, a patient will have at any time a full overview of all the healthcare providers that have access to their record, and when healthcare providers have viewed and/or adapted their record. The access to a patient's record can also be revoked at any moment.

Since permissions are managed by a smart contract on the blockchain, we need a unique identifier in order to be able to assign the record to the right patient. While in many countries' persons are identified through for example their national identification number or social security number, it would be ill-advised to select a patient's social security number as the unique identifier for our blockchain-based EHR system. In the case where a blockchain is public, its contents can be viewed by anyone. Adopting social security numbers or other national identifiers would therefore result in considerable privacy issues. A unique digital identification principle is therefore lacking. Hence, in our design we will adopt the unique identification properties of blockchain cryptography by assigning every patient their own pair of public and private keys. Permission requests from healthcare providers will be sent by the smart contract to the public key of the respective patient. A patient can always verify that they are the owner of the public key through their private key. Access requests will also be confirmed or denied through a signature of the private key. To safeguard a patient's digital identity, the public key of a specific patient will be linked with their social security number by the governing body, for instance the national government or another supervising institution. As such, whenever a patient would lose control over their private key, a new private key can be assigned to this patient and linked accordingly to their social security number through the governing body. This principle will be further explained also in the sections 'Governing Body' and 'Smart Contract/Blockchain' below.

Requestor

The requestor is the party that desires access rights to the patient's health record. In most cases this will be a healthcare provider such as a hospital or general practitioner, but the requestor could as well be an insurance company or research institution. As represented in the value model, a requestor then uses the medical data in order to perform the healthcare tasks that are required and updates the patient record if required and if permitted. Hence, a requestor can request access to a patient's record with either read and/or write permission and can indicate a certain time frame to which the requestor would like to have access to the record. The requestor is notified by the smart contract when any requests have been accepted or denied by the patient. A requestor will also have an overview of all the requests that have been accepted (including read/write permissions and assigned time frame) and the requests to records that have been denied. This overview can be generated by querying the ledger of the blockchain. Similar to a patient, a requestor will have its own unique digital identity in the form of a public/private key pair. A request to a patient's record will thus be signed by a requestor's private key in order to allow the smart contract to verify that the requestor is genuine (and not an imposter). Again, the digital identify of a requestor will be linked with its national identifier by the governing body in order to keep track of the digital identity of for instance recognized healthcare providers.

Governing Body

In our design, the governing body maintains all essential information about patients, requestors and data custodians (see section below). Its primary responsibility is to serve as the objective and reliable source of information for the different actors interacting with the blockchain-based EHR system. We believe an institute such as the national government of a country is the most evident choice to assign as governing body since a national government already stores and verifies these essential data. However, any type of institution that is capable of performing these tasks can of course be assigned as governing body (e.g., when rolling out the system on a supra-national scale, an international institution may assume the role of governing body). An important remark considering our design is that the governing body is also the creator/owner of the smart contract(s). It is therefore the governing body that can create, destroy or redeploy a smart contract. As also represented in the value model in Figure 2, the smart contract(s) supported by the EHR data management system that runs on information systems of the governing body, perform the value activity of EHR access control and permission management. The smart contract(s) thus complements the existing information and database management systems that would typically manage current information on patients, healthcare providers etc. Blockchain technology is therefore adopted in our design to leverage its strengths in facilitating and automating certain tasks such as permission management of EHR health records in combination with the strengths of existing information and database management systems.

As also already mentioned above, when discussing patient and requestor, the governing body is responsible for managing and linking the digital identities of these actors (including also the data custodian) with their national identities (e.g. social security number). First, this is important to compensate for the loss or theft of a private key. In this case, a patient can notify the governing body of the loss of control over the public/private key pair to which the governing body can respond by no longer recognizing the public key as a valid digital identity of that patient. The patient can then create a new private key by him- or herself and then share the new public key with the governing body. The governing body can then verify if the newly generated public key actually does belong to that specific person - similar to the case where a person would lose his or her identification documents. Hence, our design incorporates that a patient will always choose (and consequently control) their own private key and only share their public key to third parties such as the governing body. A patient can thus through the governing body easily link a new digital identifier to him- or herself and does not lose access to the patient record in case control would be lost over the private key. Finally, a second advantage of the management of digital identities by the governing body relates to the detection of illegitimate requests to a patient record. Since every healthcare provider has to register to the governing body in order to practice healthcare, the smart contract(s) can easily verify that a public key corresponds to a recognized healthcare provider.

Data custodian

The data custodian is the actor responsible for the storage and security of the healthcare records of patients. Currently hospitals are responsible for the management and security of the healthcare records of their patients. This has become an arduous and expensive task, even more with legal governance increasing their focus on the protection of individual’s data and privacy (e.g. GDPR). We believe that implementing and maintaining highly secure data management systems for every single hospital and healthcare provider is not a sustainable design choice. Therefore, we argue that specialized data custodians focus solely on the secure storage of patient’s health records, which is represented as a value activity in our value model. Additionally, by having one actor maintaining patient records, there is only one structure in which the data is being stored and distributed. This strongly improves the current situation on interoperability, where now hospitals each have their own type of databases and data structure for storing records.

Similar to patients and requestors, a data custodian has to be recognized by the governing body that it is capable and trustworthy of performing this task. The data custodian receives permission updates from the smart contract(s) when access has been given to or revoked from a certain healthcare provider for a specific patient record. Additionally, the data custodian can always consult the smart contract(s) for the different permission given by patients to healthcare providers. Finally, the patient record will always be mapped to a fixed-size value with a hashing function (e.g. SHA-3). Any change in the patient file will therefore always result in a different hash value for that record. This allows the system to carefully trace all the changes that have been made in a patient record by a certain requestor at a specific time.

Smart Contract/Blockchain

In our design the smart contract(s) automate permission management of patient's healthcare records. The contract(s) are written and controlled by the governing body[2] and can thus be seen as an extension of its information systems. It is for this reason that the smart contract is not represented as a separate actor in the value model. The smart contract(s) manage incoming requests to patient records from requestors and verify their identity with the information of the governing body of recognized healthcare providers (through an API). Requests are then sent to patients, who can decide to grant or deny the request to their patient record. When a request is accepted, the data custodian that stores the respective record is notified by a smart contract to add read/write rights for the respective healthcare provider to the granted patient record. A requestor is also informed by a smart contract if the request was accepted or declined by the patient.

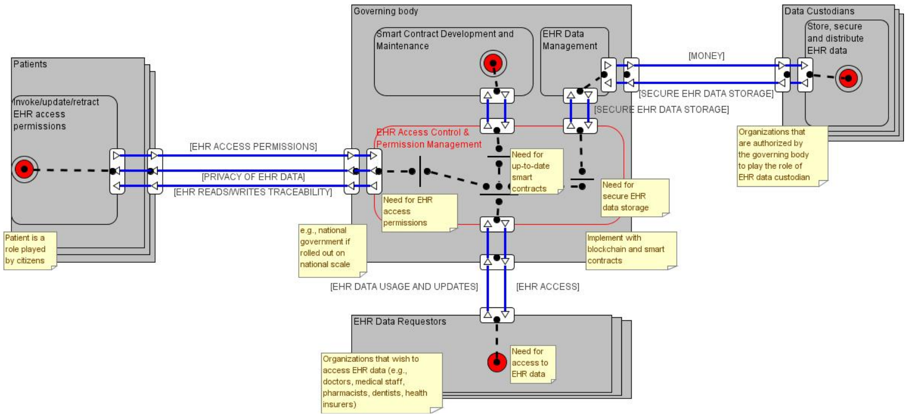
Patients
Invoke/update/retract EHR access permissions
Patient is a role played by citizens
[EHR ACCESS PERMISSIONS]
[PRIVACY OF EHR DATA]
[EHR READS/WRITES TRACEABILITY]
Governing body
Smart Contract Development and Maintenance
EHR Data Management
EHR Access Control & Permission Management
Need for up-to-date smart contracts
Need for EHR access permissions
Need for secure EHR data storage
e.g., national government if rolled out on national scale
Implement with blockchain and smart contracts
[MONEY]
[SECURE EHR DATA STORAGE]
[SECURE EHR DATA STORAGE]
Data Custodians
Store, secure and distribute EHR data
Organizations that are authorized by the governing body to play the role of EHR data custodian
[EHR DATA USAGE AND UPDATES]
[EHR ACCESS]
EHR Data Requestors
Organizations that wish to access EHR data (e.g., doctors, medical staff, pharmacists, dentists, health insurers)
Need for access to EHR data

Figure 2: E^{3}value model for a blockchain-based EHR permission management system

[2] Of course, outsourcing this value activity to another new ecosystem actor or market segment is a possibility, though outsourcing to parties in the role of EHR Data Requestors and Data Custodians should be avoided.

3 Conclusion & Future Research

The recent emergence of distributed and blockchain technology facilitate certain advantages such as traceability, transparency and enhanced security. Given this new technology's distinct advantages, several research efforts have already been proposed to leverage the unique properties of blockchain technology to manage authentication, confidentiality, accountability and data sharing of EHRs. This paper aims to offer an alternative design to manage EHRs with blockchain technology. More specifically, the emphasis of our design focuses on adopting blockchain and smart contracts as a *permission management* database and engine. We provide a general overview of the architecture of our blockchain-based EHR permission management system and describes the value exchanges that take place between the different parties participating in the EHR ecosystem in which our blockchain-based system is to be implemented. Additionally, we aim to leverage the strengths of each actor or technology within our design, allowing every actor to focus on their specific responsibilities and core tasks. In future research efforts, we will leverage this design into an actual implementation of this blockchain-based information system and evaluate this system to existing EHR management systems.

References

1. Jha, A.K., Doolan, D., Grandt, D., Scott, T., Bates, D.W.: The use of health information technology in seven nations. International Journal of Medical Informatics. 77, 848–854 (2008). https://doi.org/10.1016/j.ijmedinf.2008.06.007.
2. Chaudhry, B., Wang, J., Wu, S., Maglione, M., Mojica, W., Roth, E., Morton, S.C., Shekelle, P.G.: Systematic review: impact of health information technology on quality, efficiency, and costs of medical care. Annals of internal medicine. 144, 742–752 (2006).
3. Wang, S.J., Middleton, B., Prosser, L.A., Bardon, C.G., Spurr, C.D., Carchidi, P.J., Kittler, A.F., Goldszer, R.C., Fairchild, D.G., Sussman, A.J., Kuperman, G.J., Bates, D.W.: A cost-benefit analysis of electronic medical records in primary care. The American Journal of Medicine. 114, 397–403 (2003). https://doi.org/10.1016/S0002-9343(03)00057-3.
4. Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D.W., Middleton, B.: The Value Of Health Care Information Exchange And Interoperability: There is a business case to be made for spending money on a fully standardized nationwide system. Health Affairs. 24, W5-10-W5-18 (2005). https://doi.org/10.1377/hlthaff.W5.10.
5. Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., Taylor, R.: Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, And Costs. Health Affairs. 24, 1103–1117 (2005). https://doi.org/10.1377/hlthaff.24.5.1103.
6. Matthias, W., Christian, J., Rainer, R.: Secondary Use of Clinical Data in Healthcare Providers; an Overview on Research, Regulatory and Ethical Requirements. Studies in Health Technology and Informatics. 614–618 (2012). https://doi.org/10.3233/978-1-61499-101-4-614.
7. Sahama, T., Simpson, L., Lane, B.: Security and Privacy in eHealth: Is it possible? 5 (2013).
8. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. 1–9 (2008).

9. Antonopoulos, A.M.: Mastering Bitcoin: Programming the open blockchain. " O'Reilly Media, Inc." (2017).
10. Staples, M., Chen, S., Falamaki, S., Ponomarev, A., Rimba, P., Tran, A.B., Weber, I., Xu, X., Zhu, L.: Risks and opportunities for systems using blockchain and smart contracts. Data61 (CSIRO), May. (2017).
11. IBM Institute for Business Value: Healthcare rallies for blockchains. (2017).
12. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: MedRec: Using Blockchain for Medical Data Access and Permission Management. In: 2016 2nd International Conference on Open and Big Data (OBD). pp. 25–30 (2016). https://doi.org/10.1109/OBD.2016.11.
13. James, C., John, A.: Enabling Patient Control of Personal Electronic Health Records Through Distributed Ledger Technology. Studies in Health Technology and Informatics. 45–48 (2017). https://doi.org/10.3233/978-1-61499-830-3-45.
14. Poels, G., Kaya, F., Verdonck, M., Gordijn, J.: Early Identification of Potential Distributed Ledger Technology Business Cases Using e3value Models. In: Guizzardi, G., Gailly, F., and Suzana Pitangueira Maciel, R. (eds.) Advances in Conceptual Modeling. pp. 70–80. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-34146-6_7.