MEDINFO 2019: Health and Wellbeing e-Networks for All
L. Ohno-Machado and B. Séroussi (Eds.)

doi:10.3233/SHTI190292

Possible Usages of Smart Contracts (Blockchain) in Healthcare and Why No One Is Using Them

Alain Giordanengo[a,b]

[a] *Department of Computer Science, UiT The Arctic University of Norway, Norway,*
[b] *Norwegian Centre for E-health Research, University Hospital of North Norway (UNN), Tromsø, Norway*

Abstract

Security, privacy, transparency, consent, and data sharing are major challenges that healthcare institutions must address today. The explosion of the Internet of Things (IoT), the enactment of the General Data Protection Regulation (GDPR), the growing trend of patients self-managing their diseases, and the eagerness of patients to share their self-collected health data with primary and secondary health organisations further increase the complexity of these challenges. Smart contracts, based on blockchain technology, can be a legitimate approach for addressing these challenges. Smart contracts define rules and penalties in an agreement, enforce those rules, and render them irrevocable. This paper presents a state-of-the-art review (as of May 2018) of the possible usages of smart contracts in healthcare and focuses on data sharing between patients, doctors, and institutions.

Keywords:

smart contracts, healthcare, blockchain, trust

Introduction

Since the enactment of the General Data Protection Regulation (GDPR) in May 2018, the security, privacy, transparency, and consent for patient-owned medical data have been at the forefront of the concerns of healthcare institutions. The explicit consent of patients for processing health data and the transparency notice explaining what data will be collected, how it will be collected and patients' rights to full access to their health data [1] have greatly affected healthcare information systems.

In addition to the data generated by healthcare institutions, patients are increasingly active in managing their diseases by collecting health data using mobile devices and sensors [2]. Sharing patients' self-collected data with medical systems has a positive effect on disease management [3], and patients are eager to participate [4].

Blockchain technology is receiving extensive publicity in healthcare and has promised great improvements, such as smart healthcare management and patient empowerment [5]. Smart contracts implemented using blockchains, sometimes referred to as Blockchain 2.0, are protocols permitting the verification and enforcement of legal agreements between two or more parties and rendering them irrevocable. Interest in smart contracts has been growing ever since the creation of Ethereum, the first blockchain-based solution that integrated smart contracts, which was publicly released in 2015. Smart contracts can allow patients to manage access to their health records, secure data exchange, and ensure the privacy of those exchanges [6].

This paper presents a state-of-the-art review of the possible usage of smart contracts in healthcare, their objectives, and their limitations, with a focus on data sharing, and discusses why no one is using them in a real situation today.

Methods

Scientific and grey literature search

The author followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology to perform a scientific and grey literature search. Figure 1 shows the keywords and the search query selected by the author. Three peer-reviewed online databases were searched: PubMed, IEEE Xplore and Web of Science, together with Google Scholar. The author tailored the search query for each online database according to its specific functionalities. The search query was limited to the metadata fields: title, abstract and keywords.

---

smart contracts[Title/Abstract/Keywords] AND
(clinical[Title/Abstract/Keywords] OR
healthcare[Title/Abstract/Keywords])

Figure 1: Search query and keywords used for the scientific literature review.

The author imported all the results from PubMed, IEEE Xplore and Web of Science, as well as the results displayed on the first page of Google Scholar, to Rayyan [7], an online tool that facilitates the review process. The author chose Rayyan based on its lack of cost and flexibility compared to other tools [8]. The author first excluded results based on their metadata fields (title, abstract and keywords) using criteria listed in the next section. The author then reviewed the remaining results for inclusion based on the full texts.

Inclusion and exclusion criteria

The papers needed to meet several criteria to be included in this review. The papers needed to do one of the following:

- Describe a model or an implementation using smart contracts in a healthcare-related situation;
- Illustrate an idea for, or the potential effects of, smart contracts in healthcare systems or medical workflow.

Systematic or literature reviews that provided sufficient information regarding smart contract usages in healthcare were also included.

Papers focusing on the blockchain technology stack or smart contract algorithms, but without illustrating their uses in a clinical setting, were excluded.

Studies reported in languages other than English were excluded.

Data categorisation and data collection

The content of the papers has been organised according to a taxonomy defined by the author for presenting an overview of the usage of smart contracts in healthcare. The categories comprise the following:

1. *State of the presented work*: the part of the life cycle in which the described work is positioned (e.g. proof-of-concept [POC], prototype, production);
2. *Objective*: the situations in which the smart contracts can be used and what their goals are, or what challenges they are addressing;
3. *Content of the smart contracts*: the data or information that the smart contracts contain;
4. *Technology stack*: the frameworks, components, software, or standards on which the smart contracts rely on;
5. *Concerned Actors*: the actors affected by the introduction of the presented work in healthcare (e.g. electronic health records vendors, clinicians, patients);

The author used these categories to evaluate and analyse the included papers. Each included paper was expected to address at least one of these categories.

Results

Reviews on literature

Figure 2 shows the selection of articles. In total, forty-three articles were identified from the literature search: thirty-three from peer-reviewed literature and ten from Google Scholar. Eight duplicates were identified and removed. The author reviewed titles, keywords and abstracts of thirty-five papers, and fifteen were excluded based on the criteria specified in the previous section, leaving twenty articles for full-text assessment. Ten further articles were identified for exclusion for the following reasons:

- Out-of-scope papers (8): five papers cited healthcare settings as potential examples but did not include them at any stage of their studies, while two others limited their trials to blockchain technology that did not involve smart contracts. One paper focused on metrics for assessing blockchain-based healthcare apps instead of describing a model or an idea.
- Inappropriate description (1): the description or testing of an idea included insufficient details that would permit solid reproduction of the claims made.
- Full article innaccessible for review (1).

Ten papers were included in the final collection and analysis.

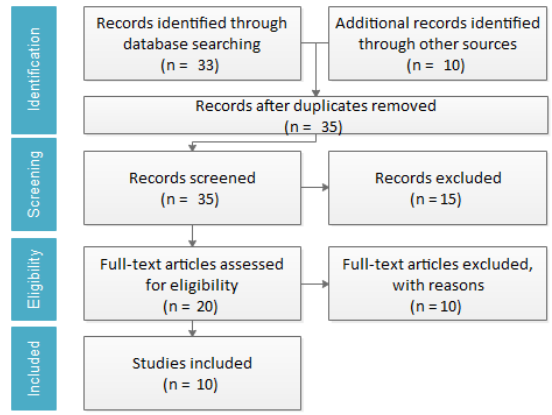

Figure 2: PRISMA flow diagram

Data extraction from included articles

The evaluation and analysis of the included articles (Table 1) are based on the categorizations described previously in the methods section.

State of the presented work

It is important to note that none of the nine studies (omitting one literature review) presented have reached the production stage. Of the nine presented studies, one is a model (i.e. a solution that is not entirely functional), three are POCs (i.e. demonstrating the feasibility of a concept) and five are prototypes (i.e. providing almost all features of an end product). None have been tested in a real-life situation.

Objectives of smart contracts, their contents and concerned actors

Six studies used smart contracts for managing data sharing. These studies concerned patients, medical workers and healthcare institutions.

- Dubovitskaya et al. [9] defined a prototype using smart contracts for exchanging data between patients and doctors and to manage access permissions. The smart contracts contain three types of blocks: 1) patient-defined permissions for allowing doctors to access or share patient- or healthcare-generated health data. The permissions can specify a data category, particular rights (read, write, and share) and a timeframe. They can also force the anonymisation of data. 2) clinical metadata, which contains all required information for accessing the corresponding data files stored off-chain (i.e. in a classic cloud solution). The clinical metadata also contains a hash of the data files to ensure the unforgeability of the data stored in the cloud. 3) patient private data directly attached to the chain by the patient, such as self-collected health data. This is the only prototype system that allows patients to exchange their data actively, without relying solely on data generated by healthcare institutions.
- Dagher et al. [10] proposed using six smart contracts as access controls for sharing medical records between healthcare and insurance providers. The first contract records the users and the mining operations. The second classifies users as patients, providers or third-parties. The third defines the relationships between users. The fourth defines the ownership of medical records, the fifth specifies the access permissions for those records and the last shares symmetric encryption

keys (SEK). Patients interact with the blockchain by changing the access permissions, while the providers use the SEKs to encrypt or decrypt medical records before sending or after receiving them via an off-chain communication channel.

- Azaria et al. [11] used several smart contracts in their data-sharing prototype for different purposes: 1) registrar contracts, which map participant (patient) identification strings (e.g. social security numbers) to their public signing keys to be used in a blockchain. These contracts also contain policies regarding the creation or updating of identities, and only certified institutions can generate them. 2) patient–provider relationship contracts, which allow patients to fine tune the access rights of their providers regarding any portion of their medical data. These contracts also contain data pointers and can be used between providers. 3) summary contracts, which contain the history of all contracts signed by all parties. For instance, they include all the patient–provider relationship contracts of a patient, who can consult them. They also act as a backup.
- Xia et al. [12] used smart contracts for sharing medical data between cloud providers and medical and research organisations. The smart contracts are used for three main purposes: 1) encrypting medical reports, 2) identifying actions performed on sent data, and 3) revoking access to violated data. The smart contracts contain a data sensitivity level, IDs of the owner and requestor (i.e. who is requesting the data), data IDs, permissions and the cryptographic keys.
- The POC defined by Ahram et al. [13] used smart contracts but for limited purposes compared to the previous studies. First, a smart contract ensures that a patient and only a patient is creating the initial version of their medical records during the first visit to a clinic. A second type of smart contract then ensures the update or transfer of the medical record by or to a provider.
- The POC by Saravanan et al. [14] used smart contracts for sharing health data with clinicians that has been self-collected using sensors. The contracts contain access logs and the shared health data. This solution requires patients to share their private keys with their clinicians off-chain before starting to use the solution.

Two other studies rely on smart contracts for improving medical trials. These studies concern researchers, participants in medical trials and research institutions.

- Benchoufi and Ravaud [15] proposed using two smart contracts to ensure the integrity and transparency of medical trials. The first ensures the irrevocability of the trial protocol by containing the protocol of the study and the statistical analysis plan and by defining the data monitoring committee. The second smart contract contains patient enrolment data (consent and information forms), data collection, trial monitoring, data management and data analysis. Using this approach, the authors claim that the reproduciability is improved and study reports and dissemination of results are impartial. Any public institution can monitor the flow and progress of a study and verify its validity.
- Nugent et al. [16] proposed similar usage of two smart contracts for improving the data transparency in clinical trials. The first is a regulator contract, containing clinical trial authorisation details, which is managed by public regulators (e.g. US Food and Drug Administration). The second is a trial contract, managed by the research organisations, which is used for storing trial protocols, consent forms and anonymised participant information.

The final study, by McFarlane et al. [17], focused on the adjudication of medical billing and the provision of medical access in case of emergency. In the first situation, a smart contract containing patient identification, institution denomination, and the debt owed would be issued. The smart contract would be auto-updated once the patient has paid the debt. In the second situation, a smart contract containing a secondary private key (derived from the original private key) could be issued by the patient to allow emergency services to access medical records, should the patient be unresponsive, have their mobile phone present and have configured emergency access to that phone by bypassing the lock screen. The second situation is only an early model, and no more details are given.

Technology

While a comparison of the different blockchain technologies is outside the scope of this article, it is interesting to note that none of the studies are interoperable, even if they use the same blockchain "family". This is due to the use of proprietary data types, with different types of rules and custom codes for managing the automatic execution of smart contracts. In addition, only one addresses interoperability issues by proposing the use of the Fast Healthcare Interoperability Resources (FHIR) specification to represent medical data.

Five types of technologies are used in these studies. Ethereum, a permission-less blockchain (i.e. any user can create and run code, and its execution relies on miners), was the most used (6 studies of 9), together with specialised libraries or languages that targetthis blockchain, such as Solidity (a contract-oriented high level language targetting the Ethereum Virtual Machine). One of the studies relies on Hyperledger, which is a permissioned blockchain. The authors of that study claimed that Hyperledger is more suited for sharing data than Ethereum [9]. It is permission-limited, and the impersonalisation and risk of data misuse due to the anonymisation of permission-less-typed blockchains both increase the likelihood of a Hyperledger system being used and remove the need to pay for transaction execution (mining). Another study relies on IBM blockchain, and one proposes the usage of ErisDB (renamed Monax in 2017 - https://monax.io/2016/11/08/eris-0120-release/) as well as Ethereum.

Conclusion and Discussion

This paper shows that smart contracts could be used in healthcare in different situations, from data sharing to the improvement of clinical trials. Two studies presented allow patients to upload their self-collected data into a blockchain and share it with their clinicians.

However, the small numbers of studies included (n=9, omitting a literature review) and the fact that none of them were at a commercialisation or production stage raise questions about the usability of this technology in real-life situations. A wider systematic review of blockchain technology, conducted in 2016, showed the same limited results, with only three articles examining smart contracts and no production-ready services [18]. Several possibilities could explain this situation in healthcare:

1. Blockchain will not change how medical records are stored. Blockchain is usable as a registry only, because inserting vast amounts of medical data, such as computed tomography (CT) scans, would render the Blockchain bloated and difficult to manage. The challenges of medical data storageing are the same, whether blockchain is used or not.
2. Blockchain technology is not necessary when trusted parties or regulators control the decision-making processes (e.g. creating smart contracts or mining), as in healthcare. Moreover, private blockchains are arguably only a shared database with at best a journaling of the data, which has existed since the seventies [19]. However, blockchain has proved its usefulness in decentralized situations in which parties cannot be trusted, even if some security issues remain unaddressed today [18].
3. Accessing encrypted patient data in the blockchain requires the healthcare institutions to use the patients' private keys (the public keys being used for encrypting the data). The sharing of a private key renders it public, and therefore not secure. In addition, this raises the question of trusted parties, described in point 2.
4. The GDPR states that patients have full access to their data [1], meaning that they have the opportunity to both manage the access rights and to move any portion or all of their data from one provider to another. Moving data between providers implies the deletion of data held by the old provider. However, it is not possible to delete anything from a blockchain without voiding its integrity and recalculating all the hashes.
5. Some of the actors cited are vapourware. For instance, ErisDB (or Monax, as it is now branded) provides no documentation nor access to a single piece of code, but still advertises its products. These practices increase doubts about the usefulness of the technology.
6. There are contradictions regarding the potential impacts of the costs of using a blockchain-based solution by healthcare institutions; some suggest that cost savings could be made [20] while others point out probable cost increases due to the nature of blockchain itself (e.g. computational power and storage increase due to data replication) [21].

Based on these considerations, the author believes blockchain-based technologies are not adapted and not ready yet for usage in healthcare, at the time this study was conducted (May 2018). Moreover, another study has suggested that the usage of these technologies is extremely immature and lacks public or expert knowledge, making it hard to form a clear strategic vision of its true future potential [22].

References

[1] V. Hordern, Data Protection Compliance in the Age of Digital Health, *European Journal of Health Law* **23** (2016), 248-264.

[2] M. Haghi, K. Thurow, and R. Stoll, Wearable Devices in Medical Internet of Things: Scientific Research and Commercially Available Devices, *Healthcare Informatics Research* **23** (2017), 4-15.

[3] M. Peleg, Y. Shahar, S. Quaglini, T. Broens, R. Budasu, N. Fung, A. Fux, G. Garcia-Saez, A. Goldstein, A. Gonzalez-Ferrer, H. Hermens, M.E. Hernando, V. Jones, G. Klebanov, D. Klimov, D. Knoppel, N. Larburu, C. Marcos, I. Martinez-Sarriegui, C. Napolitano, A. Pallas, A. Palomares, E. Parimbelli, B. Pons, M. Rigla, L. Sacchi, E. Shalom, P. Soffer, and B. van Schooten, Assessment of a personalized and distributed patient guidance system, *Int J Med Inform* **101** (2017), 108-130.

[4] M.S. Thomas Pickard, Big Desire to Share Big Health Data: A Shift in Consumer Attitudes toward Personal Health Information, *AAAI Publications, AAAI Spring Symposium Series* (2014).

[5] M. Mettler, Blockchain technology in healthcare: The revolution starts here, *IEEE 18th International Conference on e-Health Networking, Applications and Services* (2016), pp. 1-3.

[6] K. Peterson, R. Deeduvanu, P. Kanjamala, and K.B. Mayo, A Blockchain-Based Approach to Health Information Exchange Networks, (2016).

[7] O. Mourad, H. Hossam, F. Zbys, and E. Ahmed, Rayyan---a web and mobile app for systematic reviews, *Systematic Reviews* **5** (2016), 210.

[8] L. Kellermeyer, B. Harnke, and S. Knight, Covidence and Rayyan, *Journal of the Medical Library Association : JMLA* **106** (2018), 580-583.

[9] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, Secure and Trustable Electronic Medical Records Sharing using Blockchain, *CoRR* (2017).

[10] G.G. Dagher, J. Mohler, M. Milojkovic, and P.B. Marella, Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, *Sustainable Cities and Society* **39** (2018), 283-297.

[11] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, MedRec: Using Blockchain for Medical Data Access and Permission Management, *2nd International Conference on Open and Big Data* (2016), pp. 25-30.

[12] Q. Xia, E.B. Sifah, K.O. Asamoah, J. Gao, X. Du, and M. Guizani, MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain, *IEEE Access* **5** (2017), 14757-14767.

[13] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, Blockchain technology innovations, *IEEE Technology & Engineering Management Conference* (2017), pp. 137-141.

[14] M. Saravanan, R. Shubha, A.M. Marks, and V. Iyer, SMEAD: A secured mobile enabled assisting device for diabetics monitoring, in: *IEEE International Conference on Advanced Networks and Telecommunications Systems* (2017), pp. 1-6.

[15] M. Benchoufi and P. Ravaud, Blockchain technology for improving clinical research quality, *Trials* (2017),335.

[16] T. Nugent, D. Upton, and M. Cimpoesu, Improving data transparency in clinical trials using blockchain smart contracts, *F1000Research* **5** (2016), 2541.

[17] C. McFarlane, M. Beer, J.J. Brown, and N. Prendergast, Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1.1, (2017).

[18] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, Where Is Current Research on Blockchain Technology?-A Systematic Review, *PLoS ONE* **11** (2016), e0163477.

[19] A. NARAYANAN, "Private blockchain" is just a confusing name for a shared database, URL:https://freedom-to-tinker.com/2015/09/18/private-blockchain-is-just-a-confusing-name-for-a-shared-database/. Accessed: 2019-03-22. (Archived by WebCite® at http://www.webcitation.org/773slK5tg), (2015).

[20] Credit Suisse, Blockchain. URL:https://www.finextra.com/finextra-downloads/newsdocs/document-1063851711.pdf.

Accessed: 2019-03-17. (Archived by WebCite® at http://www.webcitation.org/76wJ7KQJD), (2016).
[21] D. Wood, ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER, (2014).
[22] I. Radanović and R. Likić, Opportunities for Use of Blockchain Technology in Medicine, *Applied Health Economics and Health Policy* **16** (2018), 583-590.
[23] E. Karafiloski and A. Mishev, Blockchain solutions for big data challenges: A literature review, *IEEE EUROCON 2017 -17th International Conference on Smart Technologies* (2017), pp. 763-768.

Address for correspondence

Alain Giordanengo
email: alain.giordanengo@ehealthresearch.no

Table 1 – Papers included in the review

Ref.	State	Objective of smart-contracts	Content	Technology	Actors
[17]	Model	1. Adjudication of medical billing 2. Emergency access of health records allowance	Patient (1) Institution (1) Debt (1) Secondary private key (2)	Ethereum FHIR Amazon Web Services ErisDB	Patients Institutions Debt collectors Insurances Emergency Services
[23]	Literature Review	---	Reference Paper [11]	---	---
[9]	Prototype	Data sharing between patients and doctors, with data generated from both sides	Permissions (patients to doctors) Clinical Metadata Patients' private data	Hyperledger Chaincode ARIA Varian Cloud Go	Doctors Patients
[15]	POC	Improving medical trials by managing consent and ensuring integrity and transparency of the trials	Trial protocol and setup (1) Patients enrolment (2) Data Collection (2) Trial Monitoring (2) Data Management (2) Data Analysis (2)	Ethereum Solidity Chainscript	Trial participants Researchers
[13]	POC	Consent of the patients Record transfer between healthcare networks	Any Protected Health Information Involved health networks	IBM Blockchain Bluemix NodeJS	Patients Doctors
[16]	Prototype	1. Capturing clinical trial authorization 2. Storing clinical trial protocols and collected data	Clinical trial authorization Protocols Collected data	Ethereum Javascript Solidity	Regulators Research Organizations Researchers Doctors Patients
[11]	Prototype	1. Mapping patients ID to their public keys 2. Logging patient-providers relationships, access rights and data retrieval pointers 3. Managing Medical Record history	Patients ID Patients Ethereum address Provider ID Patients-Providers relationships Access permissions Data pointers	Ethereum PyEthereum PyEthApp SQLite Flask	Patients Providers
[10]	Prototype	1. User registration and mining 2. Classify users as patients/providers/third party 3. Relationships of nodes 4. Ownerships of medical records 5. Permission access to medical records 6. Proxy re-encryption	Ethereum address Users ID Relationship status Access Conditions Hashes Symmetric Encryption Key	Ethereum QuorumChain Ethereum-Go	Patients Providers Healthcare Insurance
[12]	Prototype	1. Encrypt reports 2. Identify actions performed on sent data 3. Revoke access to violated data	Cryptographic keys Reports Permissions Data sensitivity level IDs	Undisclosed	Cloud providers Research organizations Medical organizations
[14]	POC	Share self-collected health data	Medical data Access logs	Ethereum	Patients Clinicians