Blockchain and health

Olivier Hueber

Blockchain and health

For a health blockchain compatible with Covid-19 data management

Olivier Hueber[Δ]
Université Côte d'Azur, GREDEG-CNRS

Abstract

Managing the profusion of health data from either caregivers, patients and any other stakeholder institution in the health system leads to the creation of numerous databases which are rarely effectively coordinated with one another. In addition, the same information can be recorded several times by different parties, which is a source of many errors. In addition, such large databases are vulnerable to hacking and are subject to strict legal rules for controlling data confidentiality.
The dramatic experience of the global Covid-19 pandemic has highlighted the great difficulty of effectively monitoring patients with existing information systems. Given this observation, it appears that the creation of a decentralized health blockchain with limited access is a solution to rationalize the management of health data while preserving the essential rules of confidentiality, scalability and traceability.

Keywords: Blockchain technology, Covid-19, Health Blockchain, Coronavirus, Bitcoin, Sidechain

JEL code: I11, I18, D82, D85

Introduction

Every health system is suffering on the one hand, from overconsumption of medicines and medical procedures and on the other hand, from a considerable loss of informations. We can consider that, because of its size and the number of stakeholders involved, any health system is in a situation of diminishing returns. To avoid duplication of medical acts, wasting of acts, medical overconsumption and in general the non-synchronization of medical acts, the creation of a large register of medical acts, namely a health blockchain, could solve most of the problems linked to the inherent complexity of any health system.
The need for a health blockchain is all the more imperative since the Covid-19 pandemic taught us that effective data tracking and management was the key factor in achieving success in bringing people out of containment and defeat this virus. Surveillance for communicable diseases, such as Nipah or Covid-19 viruses, is a very complex and often ineffective continuous process due to the interaction of a very large number of organizations and self-regulators operating under centralized information systems. In addition, the recording of health information by stakeholders in databases is often seen by them as a bureaucratic workload. for example, in France, the daily data on mortality due to Covid-19 during the confinement period were always decreasing during weekends and systematically went up on Mondays simply because the persons in charge of reporting statistical information were fewer to work weekends. A health Blockchain can help the numerous health institutions and actors to manage data more efficiently during the pandemics. A health blockchain can also track with accuracy informations

Δ olivier.hueber@univ-cotedazur.fr

concerning health emergencies. The health blockchain can also automate secure data sharing and storage at different levels of healthcare institutions, patients and caregivers. In Estonia, the electronic identity card system, which includes patient health data, uses Blockchain technology to optimize data privacy and security. The data are only accessible to authorized persons. The electronic health record integrates the data of the whole provided by the partners participating in the care paths, each patient can access it online.

From an economic point of view, the establishment of a health blockchain makes it possible to fight effectively against the two well-known sources of market inefficiencies inherent in any health system, namely the phenomena of adverse selection and moral hazard.

For reasons of confidentiality, anonymity and security, the health blockchain proposed here does not store informations but stores links referring to information by controlling who has access or not to such and such a link. It is on the basis of this triple objective of efficiency, anonymity and security that we propose here the main principles of building a health blockchain.

Literature review

Blockchain is defined as a "digital, decentralized, and distributed ledger in which transactions are logged and added in chronological order with the goal of creating permanent and tamperproof records" (Treiblmaier, 2018, p. 574). The blockchain most known to the public is that of Bitcoin (Nakamoto, 2009). Since then, this blockchain technology has been used in many fields such as tourism, law, energy and also, what interests us here, the health sector. Blockchains and distributed ledgers increases cost saving on removing intermediaries that process manual transactions (Holbrook, 2020, Chapter 6).

Blockchain technology can provide a holistic and comprehensive assessment of an individual's health. A literature on blockchains, often written by researchers in artificial intelligence, is in development. It is especially at the level of the link between medical tourism and blockchain technology that the economic litterature has developed in recent years (Rejeb et al., 2011). The blockchain technology can strengthen disease surveillance systems in cases of disease outbreaks and pandemies resulting in local and global health emergencies (Bhattacharya and al., 2019). Surveillance is defined here as systematic, ongoing collection and analysis of data and the timely dissemination of information to those who need to know so that the action can be taken. These works design interconnected, and compatible technology networks collecting information through electronic sensors and encoded in one or more blockchains (Zhao et al., 2018). Such an architectures require investments before building a health blockchain (Mukherjee P., Singh D., 2020). Interoperability between different health information is often at the heart of research in the field of health blockchains (Shahnaz and alii. 2019). Interoperability and coordination between different databases already exists in the field of cryptocurrencies based on blockchain technology by using the sidechain technology (Hueber O., 2019)

The theoretical literature on 'memory' is particularly suitable to study the role of a health blockchain (Kocherlakota, 1998). By extending such a literature to the analysis of health markets, memory is a publicly observable record of past medical acts or medical decisions that patients, caregivers and social health institutions can consult prior to making a medical decision. In a health blockchain, the compromise between confidentiality and disintermediation is fundamental. It is not possible to verify the data for which we do not have access (Greenspan G., 2018). As security and privacy are key elements of the health blockchain, the *proof of zero knowledge* procedure can be used to verify the veracity of the information contained in a new block in the blockchain (sharma et al., 2020).

Key economic issue

The specific designs of consensus protocols in a health blockchain have economic implications. These have to be taken into consideration in designing the protocols too. The first economic contribution of a health blockchain relates to the savings linked to the protection and the rationalisation of health files. Even today, health systems include numerous patient files classified differently according to pathologies or categories of caregivers. Often the same information appears in different files and like any file, the risk of hacking is permanent. The blockchain technology can reform health database interoperability with in-built authentication verifications, which decreases the risk of data theft or lost (Peterson et al., 2016). Network security in the health blockchain setting is a robust consensus. A health blockchain greatly reduces the existence of the wellknown moral hazard' phenomenon inherent in any health system. The more patients have good health coverage, the more they are prone to overconsumption. It is health coverage that modifies consumption behavior and even the production of health services. For instance, an optician will tend to offer certain glasses to the detriment of others not according to their intrinsic quality but according to the future reimbursement of their insured client.

In addition to the phenomenon of moral hazard, for which a health blockchain can fight effectively, the phenomenon of adverse selection can also be countered. It has been well known for a long time that the phenomenon of adverse selection stems from information asymmetries (A. Akerlof, 1970). Such information asymmetries are very important in the health field. The COVID-19 pandemic is - within the healthcare community and among patients - marked by innumerable information asymmetries. There is an information asymmetry between the prescribing state and its operating agent, namely, the health institution (or the health system). This question joins the work of economists Jean-Jacques Laffont and Jean Tirole (1991) on agency theory. The assessment of resources dedicated to health by the State with regard to the objectives set for the health system (the operator) is the subject of objective and performance agreements which in the presence of information asymmetries require difficult negotiations. The outcome of such negotiations is in most cases unsatisfactory. In some cases expenditures are constrained for purely financial reasons (such as the insufficient purchase of FFP2 masks for medical personnel), in other cases, it is activity pricing policies which lead to decision-making not always in accordance with medical logic. Blockchain technology allows, due to its construction, to overcome the phenomenon of information asymmetry. Everyone has the opportunity to know about the same information at the same time. This information can be detailed by making all the contents of a block in the chain visible (header and content) or more succinct by making visible only part of the contents of a block (for example only the header) while retaining the symmetry of the information .

Thanks to its security, immutability and above all transparency characteristics, blockchain technology makes it possible to reduce the asymmetry of information present on economic markets, including the health markets. In the health field, the blockchain protocol allows the various health actors to have a platform on which it is possible to share, monetize and trace data privately. Health actors can thus control access to data while developing incentives to collect and share data from different stakeholders.
Although blockchain technology first of all considerably reduces information asymmetry and the phenomenon of moral hazard, such a technology also greatly reduces transaction costs as conceived by James Tobin (1956) with its "shoe leather cost" analogy. In health systems, finding relevant information about a patient's health data is time consuming and costly.

Technical overview

There are two main categories of blockchains namely open access blockchains, like the blockchain of the famous Bitcoin, and limited access blockchains. In open access blockchains, all the informations contained in the blockchain are readable by stakeholders. For confidentiality reasons, this type of open access blockchain is not suitable for recording medical data. In the health field, it is preferable to create blockchains with limited access to data and information.

The health blockchain architecture that we are proposing here aims to free itself on the one hand, from the constraints of interoperability of the various medical systems and procedures and on the other hand, from the problems of scalability and storage capacity. Interoperability, scalability and storage capacity are the major obstacles raised by the literature. To free ourselves from these constraints while preserving anonymity, security and reliability, we propose to separate the health blockchain from the very content of the informations. More precisely, it is necessary to separate what we will call the health wallet and the health blockchain. Private data relating to the health of a patient remains always and exclusively contained in the wallet of health. The health blockchain, on the other hand, only records the history of accessible data and does not record the content of this data.

For instance, Bob performed a blood test at his city's hospital on October 5 at 5:30 p.m. This information, along with the results of this analysis, is recorded in Bob's health wallet. The Health Blockchain, on the other hand, records only a cryptographic code referring to the BOB health portfolio. Then, from this code, some stakeholders in the health system (caregivers, patients, health insurance fund, etc.) will be able to access all or part of the informations relating to this blood test carried out by Bob.

The prerequisites for the creation of a health wallet blockchain based technology are as follows:
- protected and anonymous data controlled by the patient,
- an electronic wallet with different compartments according to different degrees of security
- an energy-saving and time-reactive technology

The health wallet based on blockchain technology must be able to be opened according to the different degrees of confidentiality, on the one hand at the level of the people authorized to access the data (patient, caregiver, employer, health insurance ...) and on the other hand, in terms of the nature of the data read or written. The work prior to the creation of any electronic wallet based on blockchain technology consists in configuring access to data according to the categories of actors and according to the nature of the different information (see table 1).

Unlike the famous Bitcoin's blockchain, the creation of a new block added to a health blockchain does not require to be based on a proof of work based on a hash-based proof-of-work. Adding a simple SHA-256 type code without resorting to a mining process is less energy consuming and is much faster than a blockchain like the Bitcoin's one. Each time a new medical procedure is performed, it is the subject of a new block on the health blockchain. This new block can be added to the blockchain depending on the nature of the act, by the caregiver, by the health insurance fund, by the occupational medicine or by the patient himself. The defining feature of a health blockchain architecture is its ability to allow decentralized record-keepers to maintain a uniform view on the state of medical acts and the order of such a medical acts – a decentralized consensus.

Table 1. Accessibility of data and categories of stakeholders

	Patient		referring physician		emergency service		current employer		health insurrance	
Data category	writing	reading	writing	reading	writing	reading	writing	Reading	writing	reading
Basic information relating to emergency care (blood group, age, food intolerance, allergies, social security number, insurance company)	yes	yes	yes	yes	No	yes	no	Yes	yes	yes
Medical records, test results, medical imagery, current medical treatments	no	yes	yes	yes	No	yes	no	No	no	no
Sick leave	no	yes	yes	yes	No	no	yes	Yes	no	Yes
Authorization or not of organ donation	yes	yes	no	yes	No	yes	no	no	no	Yes
Health information entered voluntarily thanks to the health information of connected objects (connected watch, connected scale ...)	yes	yes	no	yes	No	yes	no	no	no	No

Assume the case of a patient (P) who wishes to consult a doctor (D). The patient holds two cryptographic keys, namely a public key (Ppub) and a private key (Ppriv). The private key (Ppriv) is a secured password allowing access to the information entered in the electronic health card of the patient (its health wallet). The public key (Pbub) is the health card number, for example the patient's social security number. The patient uses his private key (Ppriv) to send a coded message (N ') corresponding to a medical consultation request (N). Everyone can publicly verify that the patient is the author of the coded message because he is the only one who can sign it with his private key.
The written function (W) of the coded message (N ') is:

$$W(P_{priv}, N) = N' \quad (1)$$

To decode the message (N ') relating to a consultation request indicating the reasons for this request, the doctor uses a read function (R) with the patient's public key (Pub).

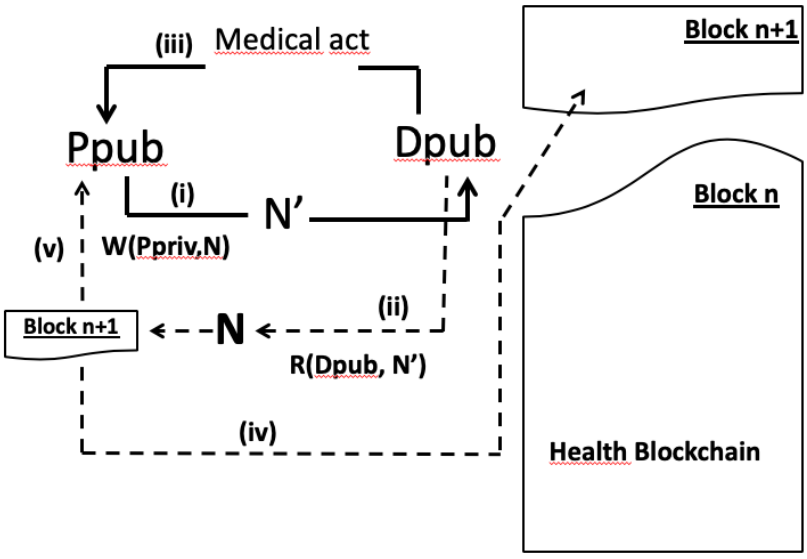
$$R(P_{pub}, N') = N \quad (2)$$

The read function allows the doctor to read the message (N) without knowing the patient's private key (Ppriv). Once the reading function is activated and the message read, the doctor accepts or does not agree to perform the medical act (here a consultation of the patient). If the doctor agrees to perform the medical procedure, once the procedure is actually performed, he adds a new block to the health blockchain himself. This block is a SHA-256 type code (see figure 1). The advantage of such a type of code is that it is a hash which means that it is one way and cannot be decrypted. For example, the SHA-256 code of the message "medical consultation for Mr. Smith by Dr. Ricardo on October 3, 2020" is: da87b4c661634ac4a44108f6eff005bba34bee956c646d5c0ca11cbcaf69e21a.

The health's blockchain can only contain information relating to medical procedures performed by the various players (analyzes, reimbursements, consultations, ...). Payments from patients to caregivers can be included as additional information. In our example, the doctor can also bill the patient with his public key (Dpub), who will then be reimbursed all or part of the cost of the consultation by his health insurance fund.

In a traditional blockchain, like the famous bitcoin's one, each block of the ledger has two main areas namely a header and a content. The header stores control information and the content stores details abouts transactions (for more details, see Grech 2017). The described health blockchain here separates he header of each block from its content.

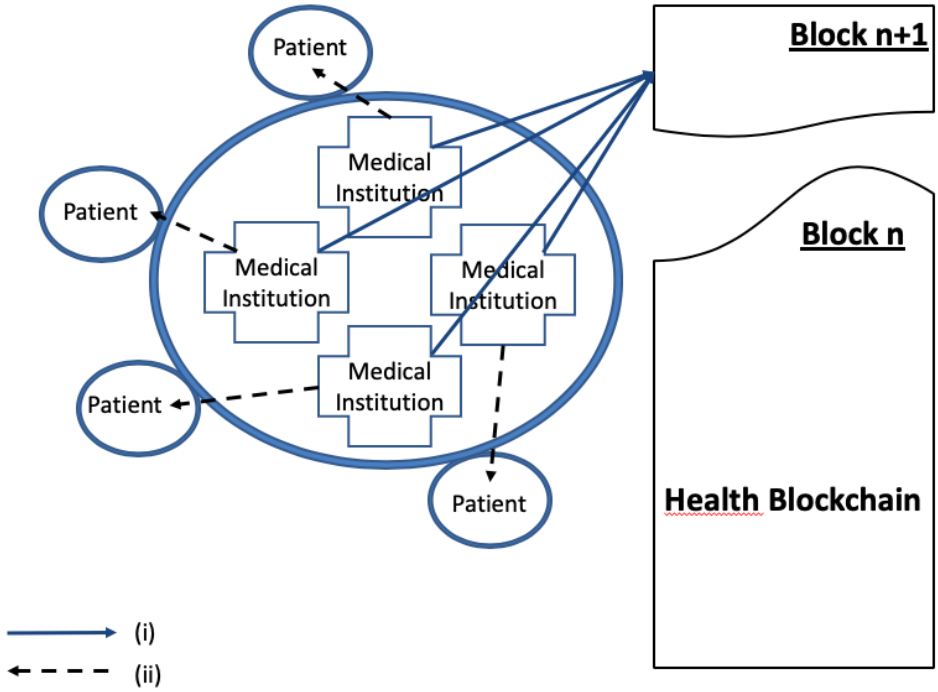
Figure 1. Creation of a new block on the health blockchain following a new medical act



In the preceding Figure (Fig. 1), steps (i), (ii), (iii), (iv) and (v) describe the ordering of operations from the writing of the initial message requesting a medical act to the realization of this act and its inscription as a new block in the health blockchain.

If we extend the mechanism described above to various stakeholders in the health system, the overall architecture creates a firewall between the general ledger of medical acts (the health blockchain) and the confidential information held by patients and health professionals (see figure 2).

Figure 2: Linkages between the health blockchain and health wallets of patients



In the figure above, the bold arrow (i) corresponds to the creation, by the institution that performed a medical procedure for a patient, to the creation of a new block on the blockchain. The dotted arrow (ii) corresponds to the recording in the health wallet of informations relating to the medical act. In the vocabulary of the cryptographic science, patients and medical institutions in this architecture are called nodes. In this decentralized network, data are located in the network of personal computers of patients, caregivers or others medical institutions public and private (called nodes) without any central control. Adding a new block to the blockchain proceeds from a "trust-in-the-third-party" mechanism where a medical act is decided when the willing parties approve it by a digital signature. Proof of zero knowledge is a security measure that verifies the veracity of the information entered on the health blockchain. Without going into details here, proof of zero knowledge is a security measure that allows a controller to show that it knows confidential information on the network without actually revealing it. Already, many privacy-based cryptocurrencies such as ZCash and Monero use this zero knowledge proof method to secure their transactions and make them private between users. For example, by using this zero knowledge proof method in the field of a health blockchain, it is possible in cryptography to answer the question "Have I been close to someone with Covid-19?" with a specific "yes" without disclosing who that person is.

During the pandemy of Covid-19, data collected on patients admitted for consultation or to hospital were mainly stored in national centralized databases and many people could updating it [Crowd-sourced]. The choice of such a centralized database tends to be victim of data manipulation or false data updatings by faulty nodes. This problem can be solved by storing the data concerning patients of Covid-19 in the health blockchain as proposed it here. The health blockchain can detect COVID-19 infected cases. On this bases, health authorities can predict the infection risk in real times.

Conclusion

The blockchain technology effectively enables efficient and cost-effective tracking and management of health data. However, building a health blockchain cannot, like the famous Bitcoin or most existing blockchains, be a large open book that everyone can check. A scalable health blockchain capable of making information both symmetrical and confidential must be a decentralized network with limited access, the blocks of which only show the information headers linking this information to private electronic health purses. In addition, by creating a health blockchain, it is necessary to rely on the countless information contained in already existing health databases. When necessary, certain information from these databases can be linked to the health blockchain. To do this, sidechain technology can be implemented.

References

A. *Akerlof., G*. (1970) “The Market for “Lemons” : Quality Uncertainty and the Market Mechanism, The Quarterly Journal of Economics, Volume 84, Issue 3, August *1970*, Pages 488–500

Bhattacharya S., Singh A., Hossain MD. M., (2019) “Strengthening public health surveillance through blockchain technology, AIMS Public Health, 6(3), pp.326-333

Grech A., Camilleri A.F. (2017) « Blockchain in Education”, Publications office of the European Union.

Greenspan G., (2018à “Where Blockchains Add Real Value », Innovations Technology Governance Globalization 12 (1-2), pp. 58-69, July.

Holbrook, J. (2020). Enterprise Blockchain Economics. In Architecting Enterprise Blockchain Solutions, J. Holbrook (Ed.).

Hueber, O. (2019) “Sidechain end Volatility of cryptocurrencies based on the blockchain technology” International Journal of Community Currency Research 23 Issue 2 (Summer 2019) 35-44

Kocherlakota, N.R. (1998) ‘Money is memory’, *Journal of Economic Theory*, Vol. 81, No. 2, pp.232–251.

Laffont J. J., Tirole J. (1991), « The Politics of Government Decision-Making : A Theory of Regulatory Capture », *Quarterly Journal of Economics*, 106,1089-1127.

Mukherjee P., Singh D. (2020) The Opportunities of Blockchain in Health 4.0. In: Rosa Righi R., Alberti A., Singh M. (eds) Blockchain Technology for Industry 4.0. Blockchain Technologies. Springer, Singapore

Nakamoto S., (2009) “Bitcoin: A peer-to-peer electronic cash system”, https://www.bitcoin.org/bitcoin.pdf

Peterson K, Deeduvanu R, Kanjamala P, et al. (2016) A blockchain-based approach to health information exchange networks. *Proc. NIST Workshop Blockchain Healthcare* 1: 1–10.

Rejeb, A. & Keogh, John & Treiblmaier, Horst. (2019). The Impact of Blockchain on Medical Tourism.

ShahnazA., Qamar U., Khalid A., "Using Blockchain for Electronic Health Records," in *IEEE Access*, vol. 7, pp. 147782-147795, 2019.

Sharma, Bhavye & Halder, Raju & Singh, Jawar. (2020). Blockchain-based Interoperable Healthcare using Zero-Knowledge Proofs and Proxy Re-Encryption. 1-6. 10.1109/COMSNETS48256.2020.9027413.

Tobin J., (1956) “ The Interest Elasticity of the Transactions Demand for Cash,”*Review of Economics and Statistics* 38, 241-247.

Treiblmaier, H. (2018) « The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. » Supply Chain Management: An International Journal, 23(6), 545–559.

Zhao,Huawei et al. (2018) « Efficient key management scheme for health blockchain », *CAAI Transactions on Intelligence Technology*, 3 (2):114