ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2017
Seria: ORGANIZACJA I ZARZĄDZANIE z. 108 Nr kol. 1983

Paweł SZEWCZYK
Wyższa Szkoła Bankowa w Poznaniu
Wydział Zamiejscowy w Chorzowie
pszewczyk@neostrada.pl

POTENTIAL APPLICATIONS OF THE BLOCKCHAIN TECHNOLOGY IN HELTHCARE

Summary. Patients, and in general, citizens, are anxious when it comes to sharing their social and health data. They do not trust governments, payers, hospitals or general practitioners when it comes to the exchange and recording of their data. They need to be assured of their privacy. A review of potential applications of the blockchain technology as a novel approach to secure health data storage, existing implementation obstacles, and a plan for transitioning incrementally from current technology to a blockchain solution is presented.

Keywords: healthcare, blockchain technology, secure storage of patient records

POTENCJALNE ZASTOSOWANIA TECHNOLOGII BLOCKCHAIN W OCHRONIE ZDROWIA

Streszczenie. Pacjenci i ogólnie obywatele są zaniepokojeni możliwością udostępniania swoich danych społecznych i zdrowotnych. W pracy przedstawiono przegląd potencjalnych zastosowań technologii blockchain - nowego podejścia do zapewnienia bezpieczeństwa przechowywania danych zdrowotnych, przeszkód w jego wdrożeniu oraz plan stopniowego przechodzenia do tych rozwiązań.

Słowa kluczowe: ochrona zdrowia, technologia blockchain, bezpieczne przechowywanie danych pacjenta

1. Introduction

Patients interact with a staggering number of health care providers through the course of their lives - from pediatrician, to university physician, dentist, employer health plan provider, specialists, and more. At each stage, they leave data scattered across a particular jurisdiction's system. This leads to a fragmented data trail and decaying ease of access, as providers often retain primary data stewardship either via default practices or explicit legal provisions.

Security measures should be in place and must be transparent to patients. In addition, with the advent of sensors and smart devices, exchanging citizen or patient recorded data, including identity, biometric and genetic data, will encounter a similar sentiment of reluctance from patients. A blockchain network, together with smart contracts, would solve the issues [4]. The patient can see who has consulted, modified or otherwise accessed his/her data.

Pharmaceutical companies are certainly ready. When examining the entire supply chain (from pharmaceutical manufactures, shipment, distributors, hospitals, prescribing doctors, pharmacies, points of sale down and customers) a wide range of inconsistent methods of passing information and transactions are being used. The need to develop a single undisputable ledger of truth is needed. Documentation is different among various parties in the supply chain, information is being lost and unauthorised handling of goods in the chain occurs. A high number of errors and inconsistent exchange of information occurs. There are no standard rules governing the passing of transactions, verification of actors within the supply chain, nor the transaction tracking that is passed up the chain to suppliers from the end point of sale. Blockchain could certainly solve these shortcomings [1].

In this paper a review of potential applications of the blockchain technology as a novel approach to secure health data storage, existing implementation obstacles, and a plan for transitioning incrementally from current technology to a blockchain solution is presented.

2. The blockchain as the new database

The technology concept behind the *blockchain* is similar to that of a database, except that the way one interacts with that database is different [9]. For developers, the blockchain concept represents a paradigm shift in how software engineers will write software applications in the future, and it is one of the key concepts that needs to be well understood. One needs to really understand the following five key concepts, and how they interrelate to one another in the context of this new computing paradigm:

- the *blockchain,*
- decentralized consensus,
- trusted computing,
- smart contracts, and
- proof of work/stake.

This computing paradigm is important because it is a catalyst for the creation of decentralized applications, a next-step evolution from distributed computing architectural constructs. Decentralized applications are going to enable a decentralization trend at the societal, legal, governance, and business levels.

Another new paradigm about the blockchain is that data and programs are public. Semi-public to be precise, because the information is cryptographically secure, and only visible if one has access rights. It means anyone can publish data on the blockchain. Previously, everything important was behind hidden databases, or a physical service counter, and one had to go somewhere to verify something. Now, one will learn to expose data, and break databases into pieces, without security fears.

Compiling a transportable, yet integrated medical record is an old and hard problem to solve. One cannot expect the blockchain to address all the issues related to health care and technology. The regulatory hurdles are not to be underestimated, especially if blockchain approaches create a conflict with the current laws.

The theory is attractive: publish your medical record safely on the blockchain and be assured that you or an authorized person can access it anywhere in the world.

Other healthcare usages might include [8]:

- Using a combination of multisignature processes and *Quick response* (QR) codes, we can grant specific access of our medical record or parts of it, to authorized healthcare providers.
- Sharing our patient data in the aggregate, while anonymizing it to ensure privacy is maintained. This is helpful in research, and for comparing similar cases against one another.
- Recording and time-stamping delivery of medical procedures or events, in order to reduce insurance fraud, facilitate compliance and verification of services being rendered.
- Recording the maintenance history of critical pieces of medical equipment, for example, a *magnetic resonance imaging* (MRI) scanner, providing a permanent audit trail.
- Carrying a secure wallet with our full electronic record in it, or our stored DNA, and allowing its access, in case of emergency.
- Verifying provenance on medications, to eliminate illegal drug manufacturing.

3. Secure storage of patient records

Today’s methods of recording and sharing patient data have a number of limitations that restrict patients’ access to their clinical records, reduce availability of essential data to care providers, and ultimately present a barrier to transforming healthcare into a learning health system. Storing patient healthcare data in a blockchain-based storage scheme can remediate these shortcomings [6].

Today, in USA, nearly all medical records are stored in *electronic health record* (EHR) systems, yet data remains largely non-portable [6]. Several factors contribute to the difficulty of providing and controlling access to healthcare data. Many healthcare providers err when interpreting HIPAA requirements [5], sharing data only when absolutely required. This extends to restricting patients and their proxies from accessing data about their own health. Some institutions perceive data stewardship as a competitive advantage. Owning the patient's medical record promotes "stickiness," while sharing it allows the patient to seek care from another institution. Healthcare providers perceive the patient's medical record as their property rather than the patient's. While, for example in the USA, this is true in a legal sense [6], it creates unnecessary and sometimes costly obstacles for patients that need or want to move their medical records to another location.

The difficulty in securely moving and sharing health data in a timely manner has detrimental impacts on patient care. As adoption of electronic health records increases, failing to execute on the promise of sharable health data is not the only problem facing EHR systems. Broader adoption of electronic health records has enabled previously unknown levels of health data breaches [13]. A majority of patients are concerned about privacy and security of medical records, and some patients withhold information from their healthcare provider because of these concerns.

4. Blockchain-based medical record storage and data exchange

A possible solution to these (and many other) issues is the implementation of a patient controlled, blockchain-based system for clinical record maintenance and sharing. To understand how blockchain technology can improve the security and efficiency of electronic health data storage and sharing, it is first necessary to provide an overview of blockchain technology and its benefits [1]. Blockchain technology rests on the following three foundational tenets:

- First, data is stored in a public, immutable transaction ledger that anyone can read. Because the transactions can never be deleted or changed, there is always a complete and irrefutable record of all transactions.
- Second, blockchains are implemented in a decentralized network of computing nodes, which makes them robust against failures and attacks. Decentralization also means that no entity owns or controls the blockchain.

- Third, the metadata describing each transaction is available to everyone on the system, but that does not mean the data stored within the blockchain is readable. Blockchain relies on pseudo anonymity (replacing names with identifiers) and *public key infrastructure* (PKI), which allows the blockchain's contents to be encrypted in a way that is prohibitively expensive to crack. When applying blockchain technology to health data, each of these foundational tenets applies.

4.1. Immutable Transaction Ledger

Blockchain was originally conceived as an infrastructural component of the cryptocurrency, *Bitcoin* [12]. The transactions on Bitcoin's blockchain represent financial transactions: moving specific amounts of Bitcoin from one account to another. Anyone can verify which account a particular Bitcoin belongs to by using appropriate software tools to examine the transactions on the public blockchain.

In a healthcare context, transactions would consist of documentation of specific episodes of healthcare services provided. Healthcare providers, payers and patients would contribute encrypted data, which would reference a patient *identity* (ID), to a public blockchain [11]. This could include clinical data that is stored in EHR systems today; claims history and gaps in care from payers; and family history and device readings from patients. This information would be encrypted and stored in the blockchain and could only be decrypted by parties that have the patient's private key. Because the ledger is immutable, no one can erase or alter the record. Updates include metadata records of the date, time, location and entity making the update. In this way, a blockchain-based medical record will be self-auditing.

4.2. Distributed Network

Financial, legal, healthcare and other types of transactions have some common requirements. It is necessary to establish the identities of the parties involved in the transaction, maintain trust, ensure that transactions are recorded properly and cannot be altered, and that the infrastructure in which transactions occur is stable. Prior to blockchain, the only way to achieve these goals was to establish a strong central authority to provide these services, for example banks, governments and clearinghouses. In the domain of health records, each hospital or health system serves as its own central authority to provide record keeping and transmission services.

Blockchain replaces the centralized infrastructure with a distributed one. The blockchain software is running on thousands of nodes distributed across an entire network. To process a transaction, it is distributed to all the network nodes, and the transaction is cleared when the nodes have reached a consensus to accept the new transaction into the common ledger. The process is technologically sophisticated, but it replaces entire record keeping and transaction processing institutions. This lowers transaction overhead in terms of price and execution time. It also means there is no single point of failure, providing a more robust, safer infrastructure.

4.3. Strong Encryption

Public Key Cryptography is an encryption system that uses pairs of keys: a “public key” available to everyone and a “private key” that is known only to its holder. Either key may be used to encrypt a message, but the other key must decrypt the message. Practically speaking, there are two use cases involving public and private keys. First, a sender can encode a message with a public key and be sure that only the holder of the private key can decrypt it. Second, a message or document can be encrypted with a private key. If the message makes sense when it is decrypted using the corresponding public key, it’s guaranteed that the holder of the private key is the party that encrypted the message. This is sometimes called “signing” a message because it is analogous to someone putting his unique signature on a document.

Blockchain also supports a concept called *M*-of-*N* signatures or “multisig,” meaning that there are a total of *N* cryptographic keys, and at least *M* of them have to be present in order to decrypt the data. In this way, the patient can provide keys to authorized caregivers, doctors and others to grant access without the patient′s specific key. For example, this is useful when the patient is incapacitated and cannot provide consent to access the data.

Public Key Cryptography is an important concept for blockchain. All transactions are signed with private keys as a way of establishing the participants’ identities. In the context of storing healthcare data in a blockchain, cryptography would have the additional role of encrypting the contents of the message, so that only intended users can read its contents [7].

5. Implementing a Blockchain Solution

To implement a blockchain-based healthcare record system, EHRs and other record keeping systems would encrypt and send a transaction containing patient care documents – encounter notes, prescriptions, family histories, etc. – into the public healthcare blockchain. The transaction would include a digital signature from the contributor to trace provenance and the patient’s blockchain ID as the recipient of the transaction. After the documents are stored in the blockchain, patients would use a web-based or mobile application to view their blockchain contents and to grant or revoke access to specific parties [6].

Years of heavy regulation and a long-standing focus on compliance have co-opted the ability of the healthcare industry to implement novel data sharing approaches. We now face a critical need for such innovation, as personalization and data science prompt patients to engage in the details of their healthcare and restore agency over their medical data. When designing new systems to overcome current *electronic medical registry* (EMR) challenges, we must prioritize patient agency. Patients benefit from a holistic, transparent view of their medical history, and in the age of online banking and social media, patients are increasingly willing, able and desirous of managing their data on the web and on the go. Recently, a team of researchers of the MIT Media Lab has been working on a prototype system entitled Med Rec [2], which enables patients with one-stop-shop access to their medical history across multiple providers: *smart contracts* [10] on an *Ethereum* blockchain [3] aggregate data pointers (references to medical records that are stored elsewhere) into "patient-provider relationships." MedRec [2] restores patient agency by empowering users with a focal point for access and review of their medical history, and an easy mechanism for sharing their data across medical jurisdictions. Patients can authorize a new doctor to review their record and obtain a second opinion, or grant viewership rights to a guardian they trust. Grandparents can seamlessly share medical data with their families, to reduce the mystery of family health history. Furthermore, the authorization log persists in the distributed network, providing crucial back-up and restore functionality. Patients can leave and rejoin the system multiple times, for arbitrary periods, and regain access to their history by downloading the latest blockchain from the network. However, one has to consider the following remarks made by the authors [2]:

- The MedRec system is a prototype still under development and they would not recommend out-of-the-box-use of the current system as it is yet to be fully tested, and analyzed.
- Not all provider records can or should be made available to patients (i.e. psychotherapy notes, or physician intellectual property), thus MedRec does not presume to be an automatic content-management system for all of a physician's output.

6. Conclusions

Interoperability and the need to connect data silos for more seamless delivery systems and improved patient safety fall within the realm of emerging blockchain solutions. From employee wellness programs that address the need for privacy of data to peer-to-peer insurance models, blockchain offers the opportunity to develop new business models. Many of the activities in the financial sector that address identity management systems have analogous applications in healthcare. The road ahead for blockchain and healthcare will also require substantial intra-industry cooperation as well as dialogues between the public and private sectors on the roles of standards and regulatory frameworks. The primary challenge to adoption of the blockchain technology in healthcare is that it is still a nascent technology. Thus, there are unknown factors or vulnerabilities. But they won't stop it from being widely adopted. Trust will grow. Regulations will be enacted and standards will be adopted.

Bibliografia

1. Definitions and Explanations to Understand Blockchain Technologies; http://www.blockchaintechnologies.com/about; (7.11.2016).
2. Ekblaw A., Azaria A., Halamka J.D., Lippman A.: A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data, White Paper; IEEE 2nd International Conference on Open & Big Data 2016; http://dci.mit.edu/assets/papers/eckblaw.pdf; (5.05.2017).
3. Ethereum Project; https://en.wikipedia.org/wiki/Ethereum; (5.05.2017).
4. Hekster N.: Healthcare Rallies for Blockchain: Q&A with Dr. Nicky Hekster IBM Healthcare & Life Sciences Industries Blog; https://www.ibm.com/blogs/insights-on-business/healthcare/category/healthcare-industry-insights/; (7.02.2017).
5. HIPAA: Health Insurance Portability and Accountability Act of 1996; enacted by the 104th United States Congress.
6. Ivan D.: Moving Toward a Blockchain-based Method for the Secure Storage of Patient Records; Blockchain Challenge on ONC Tech Lab; http://oncprojectracking.healthit.gov/wiki/x/q4Pe; (24.04.2017).
7. Lewis A.: A gentle introduction to blockchain technology; Bits on blocks. Thoughts on blockchain technology; Blog posted on 9.09.2015; https://bitsonblocks.net/about/; (12.11.2016).
8. Mougayar W.: The business blockchain. John Wiley & Sons, Inc., Hoboken, New Jersey, USA 2016; pp. 118-119.
9. Mougayar W.: Understanding the blockchain; O'Reilly Media, Inc.; January 16, 2015; http://www.oreilly.com/; (20.10.2016).
10. Smart Contracts; https://en.wikipedia.org/wiki/Smart_contract; (5.05.2017).
11. Szewczyk P: Application of the distributed ledger technology in administration. Blockchain-based identity system. Chorzowskie Studia Polityczne, Chorzów (2017, in print).
12. Szewczyk P.: Potential impact of the Blockchain technology on the financial sector. Zeszyty Naukowe WSB w Poznaniu, Poznań (2017, in print).
13. The Healthcare Blockchain Summit: Overview; 20-21.03.2017; Washington, DC; http://tcbi.org/hcblockchainsummit/; (12.04.2017).