sustainability

MDPI

Article

Tracking of Clinical Documentation Based on the Blockchain Technology—A Polish Case Study

Łukasz Wyciślik [1,*] and Elżbieta Marcinkowska [2]

[1] Department of Applied Informatics, Faculty of Automatic Control, Electronics and Computer Science, Silesian University of Technology, 44-100 Gliwice, Poland
[2] Department of Economics, Finance and Environmental Management, Faculty of Management, AGH University of Science and Technology, 30-067 Cracow, Poland; emarcink@zarz.agh.edu.pl
* Correspondence: lwycislik@polsl.pl

Received: 14 October 2020; Accepted: 13 November 2020; Published: 16 November 2020

Abstract: The article presents the concept of application DLT (distributed ledger technologies) for building the electronic clinical documentation tracking system. After a short introduction to block chain issues, and discussion about the attempts of its application on various fields of everyday human life, including healthcare, basic requirements for tracking of clinical documentation system are presented, followed by the proposition of its architecture leveraging the distributed ledger technologies. The paper is concluded with a discussion about the possibilities of running such a system, regarding constraints coming from local legal regulations and general data protection regulation (GDPR), but also economic and social conditions, including ecological ones, which are part of the sustainable development trend.

Keywords: block chain; clinical documentation; distributed ledger technology; Poland; sustainability

1. Introduction

Blockchain is a type of groundbreaking information technology, which is supported by cryptography. It is a distributed digital recording system, functioning due to a consensus mechanism and made its debut as the platform on which Bitcoin [1], the first cryptocurrency was built. So far, more than 1000 different cryptocurrencies have been introduced to the financial market. Cryptocurrencies are believed to be the future of financial instruments, which means blockchain technologies will be at in the middle of it all when that happens [2]. Such high expectations in relation to blockchain technology are caused by several features that it brings that have never been met before and are subject of a constant researching [3,4]:

- no need for a trusted central institution to coordinate the transactions,
- when needed, public access to information about completed transactions, enabling everyone to review and verify them (in the case of the use of public blockchain technology, however, because solutions in the industry are more and more inclined to protect information, they more often move toward using private blockchain technology),
- a distributed ledger that makes the system as a whole resistant to failures by removing SPOFs (single point of failures),
- consensus mechanisms that make sure all ledger mirrors are synchronized with each other and most of the parties agreed on which transactions are legitimate and are added to the ledger,
- non-repudiation of ordered transactions and strong immutability of transactions history achieved thanks to using public key infrastructure and complex computing,
- privacy enabling hiding identity of transaction parties.

All of the above sound very promising, not only in terms of building stable and secure financial instruments, but also in terms of rolling out these concepts on the other fields of everyday human activities both regarding public and commercial services.

Indeed, since the development of blockchain technology, many ideas for its application have been created. Besides cryptocurrencies [5,6], other benefits are also worth mention here, e.g., e-government [7,8], energy [9,10], banking [11,12], and supply chain [13] issues. As of the time of writing this paper, the latest blockchain application announcement was from the automotive industry, where car maker BMW implemented blockchain, together with the VeChain company, to solve the problem of odometer fraudulence, which is a widespread problem in Germany.

However, although the history of bitcoin dates back to the year 2009, blockchain technologies have not found widespread use in everyday human activity, and most implementations are still only of a pilot nature. This is probably due to the fact that this technology also brings several limitations, both technical and social. Among them, the following should be mentioned, at least:

- limited throughput in committing new transactions,
- low performance of queries regarding the current state of ownership of given resources (usually it must be calculated based on the transaction history),
- high demand for computing resources when using, e.g., PoW (proof-of-work) algorithms,
- legal regulations that are in conflict with the possibility of using a distributed ledger technologies,
- lack of social trust for emerging technologies refuting the paradigm of the need for a trusted central coordinator [14,15].

In addition, many researchers note that the implementation of solutions based on blockchain technologies may also have side effects. Examples of environmental side effects caused by the high energy requirements of computer systems carrying out complex mathematical calculations are often cited here. The electricity required to maintain some cryptocurrency systems is so significant that the resulting carbon dioxide emissions can increase the greenhouse effect [16]. These concerns mean that the legitimacy of using these technologies is often the subject of sustainability considerations. Other investigations concern the issues of the possibility of improving the resistance to security breaches of blockchain technology, which are known from the past, especially in the area of cryptocurrencies [17].

All the advantages, together with the risks associated with the use of blockchain technology mentioned above, mean that each application of it should be preceded by a decision-making process, from which the premises for its use should result. For example, it is difficult to imagine a patient who would be forced to own a technical infrastructure that would allow replication of the entire register of an insurance institution that is responsible for his treatment processes. Some researchers see multi-criteria optimization processes in such decisions and even try to build synthetic indicators to help each time make such a decision [18]. Furthermore, in the field of healthcare, there are many attempts to apply blockchain technologies. On the one hand, data regarding health are always treated as extremely sensitive, and thus confidential, so the healthcare industry is very cautious about implementing new technologies. However, on the other hand, these technologies are promising to meet the expectations of patients, doctors, and other parties in strengthening data privacy and reliability. It should also be noted that although, globally, the objective of legal regulations regarding health services is common, their implementation and organization of healthcare markets in individual countries are very different. This creates problems in the design of global solutions and makes focus on technological evolution more in the national scope.

It is also worth noting that research on the possibility of using blockchain technology in medicine, and in particular on the management of EHR (Electronic Health Record), has been going on almost from the very beginning of this concept; however, the results of recent years' research do not indicate that the scientific community is reaching consensus. On the contrary, there are still discussions about what part of data should be stored in the chain, and what part outside it, which of medical business processes should be supported by blockchain and which not necessarily [19–22]. These considerations

are most often carried out either at very general levels of abstraction or, conversely, focus on specific aspects of implementation, such as performance or security. However, most often, individual proposals also disregard the existing state of health care organization in a given country/territory, and their implementation would have needed its complete reconstruction. However, could there exist a solution that could be implemented in practice and would not require re-implementation of software already used in clinics? This question motivated the authors, who witnessed the transformation of the Polish health care system involving modern IT technologies from the very beginnings, to propose the concept and its validation for using blockchain technologies to implement the national distributed register of clinical documentation on the top of, already existing at the side of national clinics, medical documentation repositories—therefore, it is not a proposal to build yet another clinical documentation repository. The use of blockchain technology to create a register of sharing/tracking medical documents introduces the protection of medical records on a level that would not be possible with the use of traditional architectures. Non-reputable information about shared medical records can be unquestionable evidence in cases of privacy violations or, worse, the use of data to the detriment of the patient. From this comes the second advantage: being aware that the records cannot be distorted, a potential attacker will be discouraged from the act of crime even before committing it.

Thus, the contribution of this article is an indication of the possibility of applying the blockchain technology for tracking clinical documentation in Poland, and ultimately in the Polish legal and organizational environment, and with the use of already operating local clinical documentation repositories. To do this, the bases and specifics of clinical data and blockchain technologies were introduced in Theoretical background chapter. In the Material and Methods chapter, blockchain technologies were briefly characterized in the context of systems storing medical data. Then, the features that a system implemented in a Polish location should have were discussed in more detail, and next, the functional and non-functional requirements model was introduced. In the Results and discussion chapter, the system architecture model of the proposed solution was presented, followed by the discussion of the possibilities of its implementation in the context of legal, economic, and social aspects. In the Results and discussion chapter, the system architecture model of the proposed solution was presented, and then the possibilities of its implementation were discussed in the context of legal, economic, and social aspects. The article ends with the Conclusion chapter, which contains a brief summary of the results obtained and the directions for further research.

2. Theoretical Background

Clinical data are of key importance when it comes to the successful treatment of patients. At the same time; however, they have a nature that makes it difficult to fully use them for therapeutic processes automation which in turn is a barrier to increasing the quality and availability of medical services worldwide. One of these difficulties is problems with the standardization and structuring of medical data. Different fields of medicine focus on different scopes of clinical data, the degree of development and wealth of individual countries or institutions allows for the collection of data at different levels of detail, as well as different treatment standards require the collection of specific data. Of course, this has been recognized and has resulted in the development of a series of standards designed to address these issues for decades [23]. However, practice shows that establishing a standard is easier than implementing it. This has been noticed in many countries and the example of Saudi Arabia was analyzed in detail as early as 2013 [24]. Furthermore, in Poland, the national implementation of the HL7 CDA is been developing since 2011, and it is being implemented in the national health care units to this day (https://www.cez.gov.pl/HL7POL-1.3.1.2/plcda-1.3.1.2/plcda-html-1.3.1.2/plcda-html-1.3.1.2/index.html). The developed standard is already used and even required by law, but is so sophisticated that its implementation guide has over 200 pages. Another feature that hinders the use of clinical data is their large volume—especially in the case of data coming from RIS (Radiology Information System) and PACS (Picture Archiving and Communication System) systems. The amount of data in the world is projected to double every 2 years, leaving us with 50 times more data (44 zettabytes,

or 44 trillion gigabytes) in 2020 than in 2011 [25]. Taking into account such a growth rate and the fact that in many countries medical records must be kept for 20 or even more years, this creates a real risk of disrupting medical processes, especially in the case of documents such as imaging diagnostics, which, in addition, are most often stored only locally, i.e., at the place of their first use. This case also illustrates the third difficulty in processing medical records—namely, their very large distribution [26]. Usually, making an accurate diagnosis can be the more effective the more detailed patient data is collected. However, in the course of his life, the patient usually visits unrelated specialist clinics, which means that his clinical details have a very little chance of meeting at the place of the current diagnosis. All the above-mentioned problems are additionally augmented by the fact that clinical data are strictly sensitive, and facilitating access to them may, on the one hand, improve the treatment, and hence the patient's health, but on the other hand, interception of these data by an unauthorized party may for the same patient be a lethal threat [27]. Considering the above, it can be concluded that medical records should be made available in accordance with local standards and that they are highly distributed; however, since they are sensitive, they should be made available only with the knowledge and consent of their owner. Therefore, there is a need to build a solution for registering newly created clinical documents and the facts of their sharing in a non-repudiation way. The end of the previous sentence requires a closer look at one of the most revolutionary IT technologies of the last decade.

A blockchain is a distributed computing architecture consisting of several computing units called nodes. It is used to maintain a register of transactions in a particularly reliable manner because this reliability results from the combined trust in each of its participants. Thus, it is, in a way, a paradigm shift of the reliability of IT systems, where, according to the traditional understanding, the greatest protection, and thus the credibility of processed information, can be obtained by building centralized datacenters. However, in the case of such central systems, the question may be asked whether the party supervising such a system is and will be impartial and whether we can and will be able to trust it in all circumstances. So, in the case of blockchain technology, the lack of centralization gives possibilities to rise the trustworthiness to a higher level. Each of the nodes participating in a given blockchain system operates independently in terms of keeping and sharing transaction history. However, they join forces to get consensus when creating and committing new transactions. This means that there is no longer need to trust individual people, because it is enough 'to trust math' [28]. The easiest way to understand the complexity of getting mutual agreement on the common state of a ledger is by recalling The Byzantine Generals Problem [29]. Individual transactions are grouped into larger blocks, which are indivisible units of data exchange between nodes. Blocks containing consecutive transactions are chained in such a way that the seal (most often implemented as a hash function) of the previous block is part of the current one. As a result, any attempt to modify past data will be easily detected and rejected. As it can be seen, the seemingly simple concept of the blockchain idea has complex implementations, which carries an overhead on both the data volume and the performance of transaction processing (the so-called bandwidth), so when choosing this technology, one should not expect profits other than non-repudiation of the data—what is more, these overheads should be taken into account, for example by limiting the scope of the data to be chained.

Nonetheless, leveraging blockchain technology, healthcare organizations could potentially improve their processes in many fields [30,31]. One is obviously healthcare insurance [32] in terms of processes of the insurance policy purchases, billing, and claims. Blockchain can also be applied as a distributed database providing information about storing and accessing medical products during the logistics process in the pharmaceutical supply chain [33]. Furthermore, the field of clinical trials can be supported by blockchain technologies to gather more reliable data [34,35]. Prescription of medicines and their reimbursement is one of the most costly areas of the whole of health care issues, so it is no wonder that also here attempts are made to implement more detailed and reliable control [36]. An electronic health record (EHR) management is another subject of research [37] and should be probably the most crucial area to be improved, because on instant access to reliable health records human life may depend.

There are a lot of solutions that have already gone beyond the conceptual phase, but it seems that they are still far from the maturity of the production stage. It is worth mentioning such projects as Medicalchain, Patientory, MediLedger, MediChain, and MedRec [38]. The last is an attempt to apply the blockchain technology for building a global, consistent repository of clinical documents.

There have also been recent attempts to use blockchain technology to control access to EHRs, which states a functional subset of the broader propositions discussed in this paper. Beinke et al., for instance, investigate the stakeholders' interests in implementing individual requirements related to EHR systems that blockchain technology may support [39]. Although this study provides an interesting overview of this problem, especially from the requirements perspective, the proposed solution is very general and does not refer to any currently used data exchange standards. An interesting and quite detailed approach to sharing HER records was presented by Norwegian researchers [19]; however, there were no proposals for registering patient consent for sharing clinical documents among medical entities. In another study [20], the author argues that he believes that storing the content of the medical records in any system that is privately controlled defeats the cause of the public control of the data. Therefore, he moves away from storage of a simple hash of the data to storing the medical record on the chain to enable complete. However, other research published two years earlier [21] argues the opposite, and this view seems to prevail in most scientific studies. It is also easier to be implemented, because in most cases it does not require changing the software already operating at medical service providers, and the immutability of the clinical documentation stored in these systems can be ensured by cryptography. Finally, Xiao et al. propose [22] a hybrid solution where the basic metadata is stored on the blockchain and the clinical document data is kept centrally in a "secure cloud". However, they do not explain what a secure cloud is and why such a solution is better than, e.g., than relying only on asymmetric cryptography.

Furthermore, in Poland, efforts were made (National Register of Medical Services—'RUM—Rejestr Usług Medycznych' and Electronic Platform for Collection, Analysis, and Sharing of Digital Medical Records—'P1' projects) [35] to build a global system to store and share medical records, but despite the government support for them, no success was achieved (these projects, however, even did not involve the use of blockchain technology). Recently, strenuous attempts have been made in Poland to amend the legislation imposing the obligation to keep medical records in an electronic manner (Regulation of the Minister of Health of 6 April 2020 on the types, scope and templates of medical documentation and the method of its processing: http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20200000666). Although large hospitals and clinics have been processing medical records electronically for some time using dedicated commercial software, smaller outpatient clinics, and private clinics will now be motivated to do so. All this helps to improve the implementation of processing and transfer of medical data, which will probably contribute to the improvement of treatment processes as such, but also carries the risk of data leakage or distortion. Although the IT systems supporting health processes so far built by the government are centralized systems, but in the case of clinical documentation, it is worth considering the use of a distributed ledger system, which can better guarantee the transparency, non-repudiation and availability of data.

At the same time, the Estonian government carried out a series of reforms regarding the e-government area, which resulted in the implementation of blockchain technology in the ground of healthcare, including EHR, a system for civic voting and many others [5].

3. Materials and Methods

As the aim of the article is to propose an IT system architecture that enables the tracking of the patient's clinical documentation, taking into account such aspects as non-repudiation of collected data and data availability, it would seem that each of the advantages of blockchain technology (such as decentralization, non-repudiation, global availability) could provide a valuable contribution to the system that stores medical records. However, the question arises whether each of these features is

suitable for use in the processing of sensitive data related to patient health, the processing of which is often subject to legal regulations established at various legislative levels.

Additionally, it is worth identifying potential barriers in the form of limitations in various aspects of human activity:

- institutional (i.e., the current way of organizing the health care market in a given area),
- social (such as the technological awareness of society—especially the part of it that uses medical services the most, or the ecological consequences),
- economic (what will be the costs of the implemented solution and who will have to bear them),
- and finally, organizational (will the implemented solution realistically improve the effectiveness of the treatment processes).

To propose a software solution architecture, we must first define the system features and the functional and non-functional requirements for it. The proposal made in this paper assumes building system of distributed ledger storing information describing:

- localization of clinical documents regarding a given patient,
- his consents to share this documentation with other entities,
- and every use of this documentation by authorized entities.

Thus, the need to build a central repository of medical records is not assumed—documents are stored as usual, in computer systems of individual clinics, and are exchanged between them by means of standardized protocols with the consent of patients. This proposal is in line with global standards for the exchange of health documentation and at the same time, it takes into account also Polish legislative specifics and e-government systems currently in operation in Poland (e.g., electronic signature system for citizens—leGO/pol. ePUAP [40]).

3.1. Functional Requirements

The functional requirements are described using object-oriented modeling. The structural dependencies are presented in Figure 1 using the strict UML (Unified Modeling Language) class diagram notation (https://www.omg.org/spec/UML/2.5.1/PDF). Rectangles denote classes here, which can be instantiated as objects. Solid lines connecting the classes indicate associations between them, and at their ends, there are descriptions indicating the cardinality of a given association. A label of the association indicates its role, and the arrow next to the label shows the direction of the relationship. For example, the clinical entity produces a lot of clinical documents. However, a given clinical document must be produced by exactly one concrete clinic. The dashed line, on the other hand, indicates a weaker relationship called dependency. The dashed line indicates a weaker relationship called dependency, and the direction of the arrow indicates which class depends on which.

The diagram should be read as follows. The clinical entities are producing clinical documents, each of which relates to a particular patient. The patient may grant permission on (or revoke permission from) a concrete clinical document to the clinical document consumer (in particular and most often they will be other clinics, but in general, they may be, e.g., authorized state bodies, insurance companies), so the permissioned clinical document consumer might access clinical document produced by a particular clinical entity. All executed permissions (i.e., access granted on the given clinical document) are being registered to enable patients to track all of them.

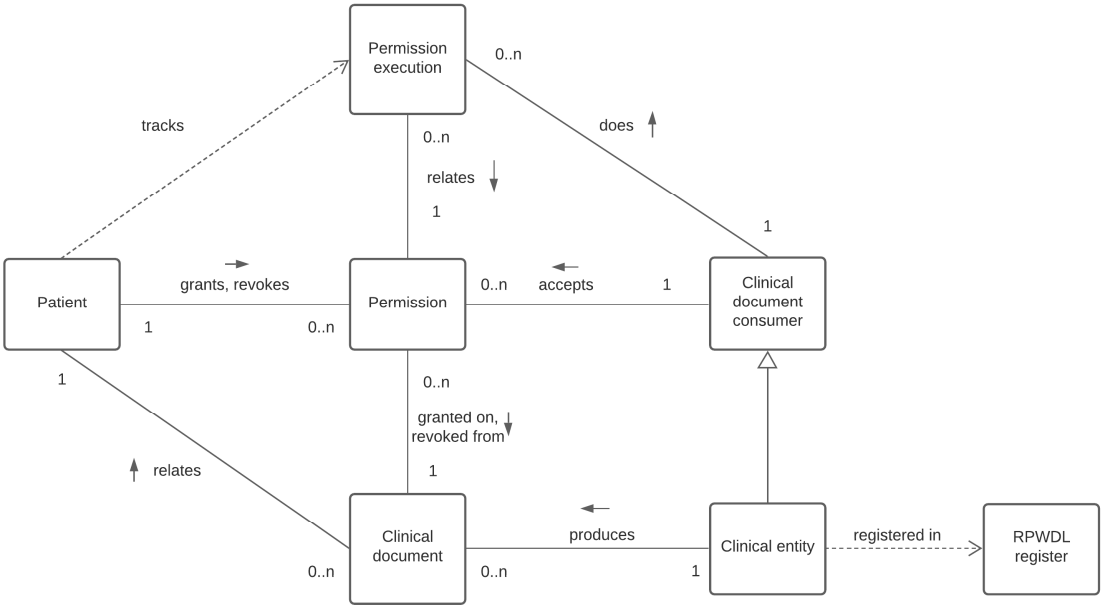

Figure 1. The UML domain class model.

So, as we can see, three major actors of such system can be identified. The first is the clinical entity, shown in the Figure 2, which produces and, on the other hand, consumes clinical documents being produced by other clinical entities. Each of the entities is able to access a given document has to accept permission first, that is granted it on a concrete clinical document. The second one is the clinical document consumer, which is a generalization of the clinic, as it can also be, for example, government agencies or insurance companies.

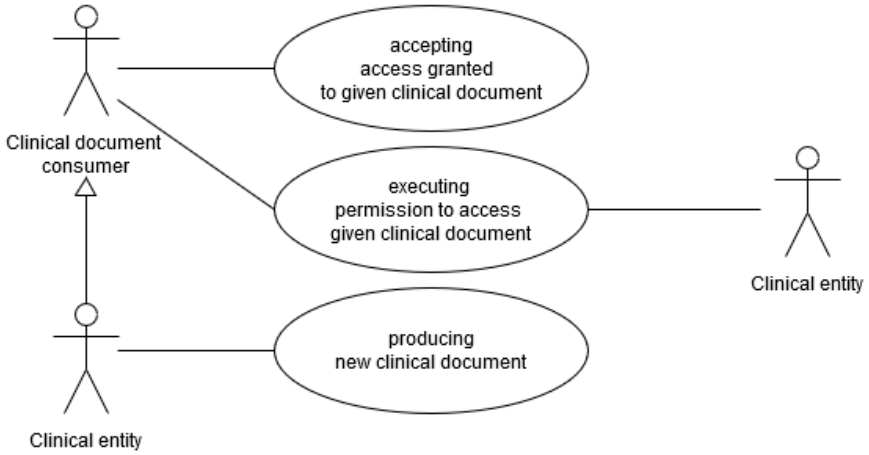

Figure 2. The use-case diagram for the medical entity.

The third actor here is obviously the patient, and his use cases has been presented in the Figure 3. Their responsibilities are granting and revoking access on his particular clinical documents to and from particular clinical entities. They are also able to monitor/track documents being produced and being accessed by particular entities.

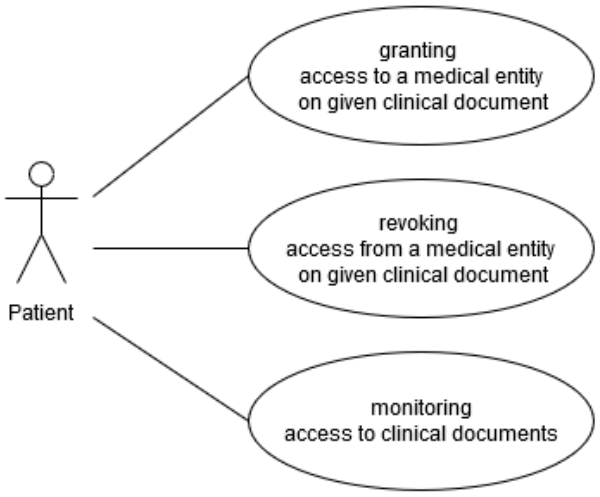

Figure 3. The use-case diagram for the patient.

3.2. Non Functional Requirements

Furthermore, several non-functional requirements should be implemented to address the security, accessibility, or privacy issues. It is worth noting that the issues related to the security of information systems are dealt with by a separate branch of research, and for the purposes of these considerations only the most important aspects have been presented.

3.2.1. Authentication

All parties connecting to the system should be authenticated and authorized. However, it should be noticed that in the case of patients authentication mechanisms used should be commonly accepted, free of charge and secure enough to enable its usage in governmental services. Healthcare professionals, however, can be equipped with secure authentication means by clinical entities.

3.2.2. Non-Repudiation

All transaction ordered should be registered in the way not letting for any doubts whether they have been conducted or not. In short, the transactions should be digitally signed by transaction issuers.

3.2.3. Privacy

Parties not involved in a given transaction must not be able to access transaction details.

3.2.4. Immutability

The system architecture should prevent any fraud related to changing the data of past transactions. At the same time, the system should be constructed so as not to have to trust the central entity.

3.2.5. Auditing (Observing)

The system should have the function of sharing transaction data for auditing institutions. This need dictates the need to allow investigations to be carried out in the event of suspected unauthorized use of medical data.

4. Results and Discussion

For the considerations in this article, it is sufficient to stay on a certain level of abstraction. It does not matter here whether, for example, the data storage layer (of clinical documents) will be implemented on the basis of a specific database platform; thus, it is enough to develop the logical architecture that

could be further developed and described (e.g., using Philippe Kruchten 4+1 View Model of Software Architecture) into more detailed description in case of a pilot implementation.

The proposed logical architecture of the system showing its basic components is presented in the Figure 4. The usage of local clinical documentation repositories is assumed. Each time a new document is produced, a ledger contract is executed to store on ledger information including the patient a document is related to the clinic that produced a document, the digital signature of document and configuration data (endpoint address, etc.) needed to retrieve a document. This way, information about each document can be found on the ledger, but using the mechanisms of encrypted transactions, it can be visible only for parties involved, i.e., the given patient the document concerns and the clinic where the document was created.

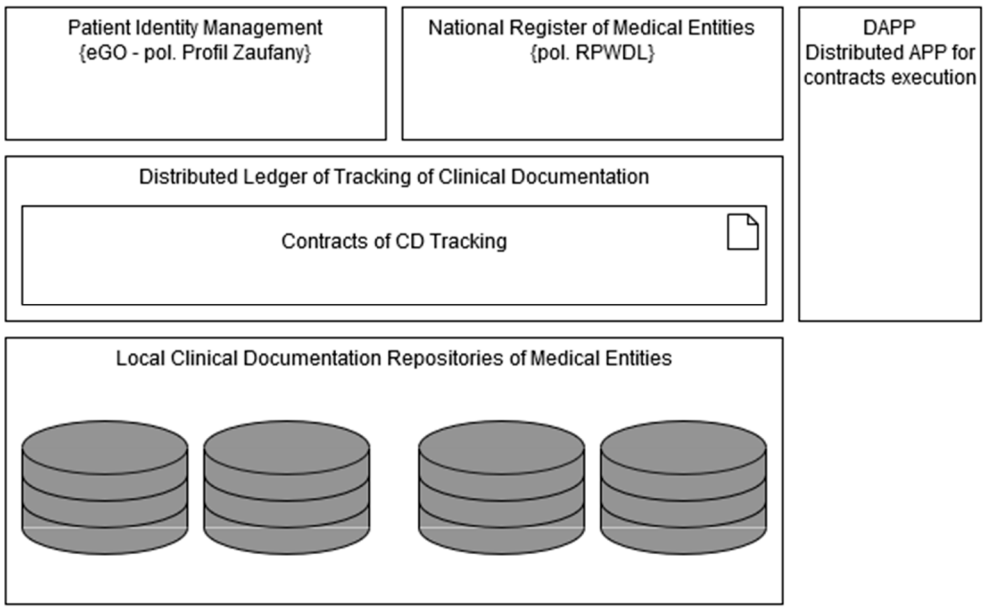

Figure 4. The logical architecture of system.

Patients interact with the system using DApp—the distributed application that after authorizing users let them execute contracts (grant, revoke) on distributed ledger. Each transaction is signed electronically by its issuer. In order to find the entity that one wants to share the document with, he can search among the dictionary data provided publicly by the National Register of Medical Entities (https://rpwdl.csioz.gov.pl/).

4.1. Technologies

One of the challenges here is to exchange clinical data in a way that allows the recipient to understand shared documents. Although these data are not stored on the ledger, but remain at the place of their creation come from many local clinical documentation repositories, the use of appropriate standards is crucial for the correct functioning of the entire system. Fortunately, the international standard for exchanging medical records—The HL7 Clinical Document Architecture (CDA) [41]—is already widely used in Poland, and it is recommended here as well [42]. However, although the HL7 CDA defines the substantive content of the messages, it does not specify the transport layer in any way. This is not a big obstacle, but a common packaging standard should be defined—it seems that nowadays the most popular architectural style RESTfull implemented at the level of HTTP calls is suitable.

The second challenge is to apply the best fitting distributed ledger technology. As personal authentication is needed here, one of the permissioned blockchain should be used. It seems that in this category the greatest maturity and production ready level achieved, such products as Hyperledger [43]

and Corda [44]; however, the last one is designed for peer-to-peer communication only, so its application would require an additional shared repository storing and sharing data about all produced documents. It is worth noting here that, due to this peer-to-peer implementation, Corda is argued not to be the true blockchain solution [45].

Another issue is the cryptography involved in the artifacts signing process. Signing contracts in blockchain usually assumes access to private key of the issuer, while in this solution, it is assumed to use the signature implemented by the eGo system, which authorizes the user with a password and does not give direct access to the cryptographic key. Thus, although the signature of the contract itself would be carried out with the key generated by the user, in order to guarantee legal effect, the content of the transaction should be additionally signed by the eGo system, which further complicates the solution.

4.2. Legal Regulations

Building and running any IT system in a public space it should be assured that it complies with legal regulations regarding both domain-specific regulations and general ones. The basic legal act regulating the issues of medical documentation in Poland is the Act of 6 November 2008, on Patient Rights and the Patient Rights Ombudsman. This Act in art. 30 para. 1 refers to the Regulation of the Minister of Health of 9 November 2015 on the types, scope, and patterns of medical documentation and the manner of its processing defining what constitutes medical documentation, how it should be processed and made available. The concept of electronic medical records is introduced by the Act of 28 April 2011 on the information system in health care. In a short time, the Polish Ministry of Health will also announce a law concerning strictly issues related to the exchange of medical records [46].

It is worth noting that one of the biggest obstacles in the implementation of blockchain technology, especially in the public sector, is problems with the interpretation of the provisions of the GDPR Act in the context of this technology. The two biggest problems are the emphasis on increasing data privacy and the right to be forgotten in the context of distributed ledger and blockchain immutability [47,48]. However, these problems are noticed and result in the continuous development of blockchain technology, e.g., [49].

4.3. Economic Factors

Implementation of the system in accordance with the proposed architecture gives a relatively low overhead on the amount of computing resources needed for its construction and maintenance. Despite the fact that medical records, and in particular raw results (scans) of medical imaging diagnostics, are known for their high demand for data storage space, in the proposed solution, these data remain where they are generated, and there they must be stored for the period required by law. Therefore, this part of system does not represent an additional cost for any participant in the healthcare system. The IT systems of individual clinics must of course implement the common data sharing interfaces, but it is proposed to use the existing standards that fit in with the general directions of development of medical information systems. Many of systems being used already implement these standards.

The system components that need to be developed from scratch are part of the core—a registry system capable of replication for all stakeholders, and a distributed DApp class application for all patients included in the system. The small number of previously specified use cases indicates that the cost of producing these components is not high, since the cost of production more complex systems was acceptable for some of aforementioned startup projects.

4.4. Social Factors

In this section, three main factors can be mentioned: social trust, general technical education of the society, and the impact on the natural environment.

An attempt to introduce (especially on a global scale) each novelty will find its opponents whose opposition will result from trying to make political capital, inborn skepticism, or rational arguments.

Therefore, it is easiest to make changes gradually, in an evolutionary way, e.g., starting from less crucial fields of everyday human life or offering some changes as facultative. Today, as mentioned earlier, we are witnessing the successful implementation of the voting system in one of the European countries [5]. Since many countries have implemented a correspondence system as an alternative to the traditional voting system and it was positively received by the public, the easier it would be to implement an alternative one based on blockchain technologies, which would gradually build social acceptance also in the field of healthcare. Finally, it should be noted that many people have already trusted the blockchain technology used to implement cryptocurrencies, and national institutions are the entities that raise the most doubts.

Technical education of the society in the use of computer applications, including mobile applications, is growing day by day. This is probably mainly due to the e-commerce field, or rather its hybrid branch—mobile applications implementing loyalty programs implemented by popular chain grocery stores. This category of mobile applications, together with social networking applications, encourages even the most reluctant people to reach for the phone and dive into the Internet. It should be assumed that in the very near future the possibility of using a web application in every area of life will cease to be determined by the age of its potential recipient, but for the time being such a barrier does exist, and in the field of medicine it is even more acute, as older people use the healthcare system most often.

There are many reports on the impact of blockchain technology on the natural environment, and in particular on its high energy demand, which in turn enhances the greenhouse effect. It should be noted, however, that in most cases, these reports relate to blockchain technology used to implement cryptocurrencies, where the overall monetary volume is, by definition, limited to protect the currency from over-supply leading to inflation. This was achieved through the constant increase in difficulty (resulting in the need to increase the amount of computing power) in digging up new coins. In fact, it is this factor, along with the coin mining race, which consumes so much energy. The use of blockchain technology for other applications and implementing more modern consensus algorithms greatly reduces its negative impact on the natural environment.

5. Conclusions

This paper, on the example of Polish conditions, presents the concept and architecture proposal of the system being built to support secure and reliable tracking of clinical documentation. The key concept is, contrary to several unsuccessful attempts of building a central system, to leverage existing clinical document repositories scattered across the whole healthcare infrastructure owned by clinics that are already obliged by legal regulations to maintain their own infrastructure. Adding a ledger component of a relatively small footprint to each interested party makes it possible to track clinical documents exchange between these parties in a secure and distributed way, where each party owns a proof of authorization to share/get given document and a proof of usage (if it has been performed) of this authorization. This does not need to trust in any central system, and at the same time enables verification of shared documents regarding its consistency (in terms of compatibility with the original).

The system can be implemented in an evolutionary way, e.g., initially in clinics networks, whose operators would like to assure their (selected) patients that their medical records are duly stored and shared, and to make this fact credible by using technologies of high immutability.

It should be noted that the global information revolution has resulted in increased social awareness of the importance of personal data. This resulted in the creation of various legal regulations (e.g., GDPR) to protect the user. For example, a user, as the owner of information describing himself, has the right to request its removal. These system requirements resulting from legal regulations obviously contradict the concept of an immutable ledger with recorded data that cannot be changed or deleted, i.e., the foundations of the classic blockchain technology. However, even then, it is possible to 'de-personalize' the stored data by giving a new identity to the person concerned. However, this is a radical step with a very large impact on the life of a given person so far, and therefore impractical.

However, at the same time, it should be remembered that general laws give way to specific laws, so the promised law on the exchange of medical records could enable the implementation of the blockchain system, just as it did in Estonia.

Even if the central system for tracking clinical documentation would have finally been built by the Polish government, there are still grounds for implementing the proposed distributed ledger solution as a complementary approach increasing the credibility of the business processes being implemented not due to trust in central institutions, but thanks to the use of strong cryptography mechanisms.

As problems with the compatibility of blockchain foundations with the implementation of regulations on the protection of personal data have already been noticed, these technologies are also evolving in directions allowing for at least partial implementation of mitigating mechanisms. As data non-repudiation is still a hot topic in the field of data processing, work is also underway to develop alternative approaches to traditional blockchain technologies. An example of such a solution is the recently publicly available service of the Amazon Web Services provider called Quantum Ledger Database (QLDB) [50]. This direction will be a further subject of the authors' research.

Author Contributions: Conceptualization, Ł.W.; Funding acquisition, Ł.W.; Methodology, Ł.W.; Validation, E.M.; Writing—original draft, Ł.W.; Writing—review and editing, E.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Statutory Research funds of Department of Applied Informatics, Silesian University of Technology, Gliwice, Poland (02/100/BK_20/0003).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 4 November 2019).
2. Iansiti, M.; Lakhani, K.R. The truth about blockchain. *Harv. Bus. Rev.* **2017**, *95*, 118–127.
3. Zhu, X.; Shi, J.; Huang, S.; Zhan, B. Consensus-oriented cloud manufacturing based on blockchain technology: An exploratory study. *Pervasive Mob. Comput.* **2020**, *62*, 101113. [CrossRef]
4. Feng, J.; Zhao, X.; Chen, K.; Zhao, F. Guanghua Zhang Towards random-honest miners selection and multi-blocks creation: Proof-of-negotiation consensus mechanism in blockchain networks. *Future Gener. Comput. Syst.* **2020**, *105*, 248–258. [CrossRef]
5. Bhardwaj, S.; Kaushik, M. Blockchain—Technology to Drive the Future. *Smart Comput. Inform.* **2018**, *78*, 263–271.
6. Vandervort, D.; Gaucas, D.; Jacques, R.S. Issues in Designing a Bitcoin-like Community Currency. *Financ. Cryptogr. Data Secur.* **2015**, *8976*, 78–91.
7. Ølnes, S.; Jansen, A. Blockchain Technology as s Support Infrastructure in e-Government. *Electron. Gov.* **2017**, *10428*, 215–227.
8. Zhao, Z.; Chan, T.H.H. How to Vote Privately Using Bitcoin. *Inf. Commun. Secur.* **2016**, *9543*, 82–96.
9. Aitzhan, N.Z.; Svetinovic, D. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *Trans. Dependable Secur. Comput.* **2018**, *15*, 840–852. [CrossRef]
10. Münsing, E.; Mather, J.; Moura, S. Blockchains for decentralized optimization of energy resources in microgrid networks. In *2017 IEEE Conference on Control Technology and Applications (CCTA)*; Institute of Electrical and Electronics Engineers: Piscataway Township, NJ, USA, 2017; pp. 2164–2171.
11. Wu, T.; Liang, X. Exploration and practice of inter-bank application based on blockchain. In Proceedings of the 12th International Conference on Computer Science and Education (ICCSE) 2017, Houston, TX, USA, 22–25 August 2017; pp. 219–224.
12. Guo, Y.; Liang, C. Blockchain application and outlook in the banking industry. *Financ. Innov.* **2016**, *2*, 24. [CrossRef]
13. Toyoda, K.; Mathiopoulos, P.T.; Sasase, I.; Ohtsuki, T. A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain. *IEEE Access* **2017**, *5*, 17465–17477. [CrossRef]

14. Laurie, H.; Yogesh, K.D.; Santosh, K.M.; Nripendra, P.R.; Viswanadh, A. Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *Int. J. Inf. Manag.* **2019**, *49*, 114–129.
15. Nawari, O.; Shriraam, R. Blockchain and the built environment: Potentials and limitations. *J. Build. Eng.* **2019**, *25*, 100832. [CrossRef]
16. Truby, J. Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies. *Energy Res. Soc. Sci.* **2018**, *44*, 399–410. [CrossRef]
17. Khan, F.A.; Asif, M.; Ahmad, A.; Alharbi, M.; Aljuaid, H. Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustain. Cities Soc.* **2020**, *55*, 102018. [CrossRef]
18. Mapar, M.; Jafari, M.J.; Mansouri, N.; Arjmandi, R.; Azizinezhad, R.; Ramos, T.B. A composite index for sustainability assessment of health, safety and environmental performance in municipalities of megacities. *Sustain. Cities Soc.* **2020**, *60*, 102164. [CrossRef]
19. Yang, G.; Li, C.; Marstein, K.E. A blockchain-based architecture for securing electronic health record systems. *Concurr. Comput. Pr. Exp.* **2019**. [CrossRef]
20. Chawdhuri, R.D. Patient Privacy and Ownership of Electronic Health Records on a Blockchain. In *Blockchain–ICBC 2019. ICBC 2019. Lecture Notes in Computer Science*; Joshi, J., Nepal, S., Zhang, Q., Zhang, L.J., Eds.; Springer: Cham, Switzerland, 2019; Volume 11521. [CrossRef]
21. Rifi, N.; Rachkidi, E.; Agoulmine, N.; Taher, N.C. Towards using blockchain technology for eHealth data access management. In Proceedings of the 2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME), Beirut, Lebanon, 19–21 October 2017; pp. 1–4. [CrossRef]
22. Xiao, Z.; Li, Z.; Liu, Y.; Feng, L.; Zhang, W.; Lertwuthikarn, T.; Goh, R. EMRShare: A Cross-Organizational Medical Data Sharing and Management Framework Using Permissioned Blockchain. In Proceedings of the 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, 11–13 December 2018; pp. 998–1003.
23. Schulz, S.; Stegwee, R.; Chronaki, C. Standards in Healthcare Data. In *Fundamentals of Clinical Data Science*; Kubben, P., Dumontier, M., Dekker, A., Eds.; Springer: Cham, Switzerland, 2019. [CrossRef]
24. Alkraiji, A.; Jackson, T.; Murray, I. Barriers to the Widespread Adoption of Health Data Standards: An Exploratory Qualitative Study in Tertiary Healthcare Organizations in Saudi Arabia. *J. Med. Syst.* **2013**, *37*, 9895. [CrossRef]
25. Austin, C.; Kusumoto, F. The application of big data in medicine: Current implications and future directions. *J. Interv. Card. Electrophysiol.* **2016**, *47*, 51–59. [CrossRef]
26. Boonn, W.; Langlotz, C. Radiologist use of and perceived need for patient data access. *J. Digit. Imaging* **2009**, *22*, 357–362. [CrossRef]
27. Dyke, S.; Dove, E.; Knoppers, B. Sharing health-related data: A privacy test? *NPJ Genom. Med.* **2016**, *1*, 16024. [CrossRef]
28. Nofer, M.; Gomber, P.; Hinz, O.; Schiereck, D. *Blockchain," Business & Information Systems Engineering: The International Journal of Wirtschaftsinformatik*; Springer: Berlin, Germany; Gesellschaft für Informatik e.V. (GI): Bonn, Germany, 2017; Volume 59, pp. 183–187.
29. Lamport, L.; Shostak, R.; Pease, M. The Byzantine Generals Problem. ACM Trans. Program. *Lang. Syst.* **1982**, *4*, 382–401.
30. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. Medblock: Efficient and secure medical data sharing via blockchain. *J. Med Syst.* **2018**, *42*, 1–11. [CrossRef] [PubMed]
31. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.-K.R. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [CrossRef]
32. Zhang, P.; Schmidt, D.C.; White, J.; Lenz, G. Blockchain technology use cases in healthcare. *Adv. Comput.* **2018**, *111*, 1–41.
33. Bocek, T.; Rodrigues, B.B.; Strasser, T.; Stiller, B. Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; pp. 772–777.
34. Shae, Z.; Tsai, J.J.P. On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017; pp. 1972–1980.

35. Maslove, D.M.; Klein, J.; Brohman, K.; Martin, P. Using Blockchain Technology to Manage Clinical Trials Data: A Proof-of-Concept Study. *JMIR Med Inform.* **2018**, *6*, e11949. [CrossRef]
36. Engelhardt, M.A. Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. *Technol. Innov. Manag. Rev.* **2017**, *7*, 22–34. [CrossRef]
37. A Case Study for Blockchain in Healthcare: 'MedRec' Prototype for Electronic Health Records and Medical Research Data. Available online: https://dci.mit.edu/research/blockchain-medical-records/ (accessed on 20 June 2020).
38. Blockchain Technology in Global Healthcare, 2017–2025. Available online: https://store.frost.com/blockchain-technology-in-global-healthcare-2017-2025.html (accessed on 20 June 2020).
39. Beinke, J.H.; Fitte, C.; Teuteberg, F. Towards a Stakeholder-Oriented Blockchain-Based Architecture for Electronic Health Records: Design Science Research Study. *J. Med. Internet Res.* **2019**, *21*, e13585. [CrossRef]
40. Kuchta, Ł. Completing a legal action with the use of the signature confirmed by the trusted ePUAP profile as a special form of legal action. *Roczniki Administracji i Prawa* **2017**, *17*, 315–335.
41. CDA®Release 2. Available online: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=7 (accessed on 20 June 2020).
42. Polska Implementacja Krajowa HL7 CDA. Available online: https://www.csioz.gov.pl/HL7POL-1.3.1/plcda-html-1.3.1/plcda-html-1.3.1/index.html (accessed on 20 June 2020).
43. Hyperledger. Available online: https://www.hyperledger.org/ (accessed on 20 June 2020).
44. Open-Source Blockchain Platform for Business. Available online: https://www.corda.net/ (accessed on 20 June 2020).
45. R3's Corda Uncovered: It's not Blockchain. Available online: https://www.gtreview.com/magazine/volume-15issue-3/r3s-corda-uncovered-not-blockchain/ (accessed on 20 June 2020).
46. MZ: Będzie Ustawa o Dokumentacji Medycznej, Czyli Porządek Zamiast Rewolucji. Available online: http://www.rynekzdrowia.pl/Technologie-informacyjne/MZ-bedzie-ustawa-o-dokumentacji-medycznej-czyli-porzadek-zamiast-rewolucji,193344,7.html (accessed on 20 June 2020).
47. Making Blockchain Comply with GDPR: The Challenges and Fixes. Available online: https://www.altoros.com/blog/making-blockchain-comply-with-gdpr-challenges-and-fixes/ (accessed on 20 June 2020).
48. Blockchain and GDPR. Available online: https://www.ibm.com/downloads/cas/2EXR2XYP (accessed on 20 June 2020).
49. Hyperledger Fabric Blockchain Integrates 'GDPR Compliant' Privacy Solution. Available online: https://bitcoinexchangeguide.com/hyperledger-fabric-blockchain-integrates-gdpr-compliant-privacy-solution/ (accessed on 20 June 2020).
50. Amazon Quantum Ledger Database (QLDB). Available online: https://aws.amazon.com/qldb/ (accessed on 20 June 2020).