Medical Blockchains and Privacy in Austria - Technical and Legal Aspects

Andreas Kolan
Josef Ressel Center BLOCKCHAINS
St. Pölten Univ. of Applied Sciences
S. Pölten, Austria
is161314@fhstp.ac.at

Simon Tjoa
Josef Ressel Center BLOCKCHAINS
St. Pölten Univ. of Applied Sciences
S. Pölten, Austria
simon.tjoa@fhstp.ac.at

Peter Kieseberg
Josef Ressel Center BLOCKCHAINS
St. Pölten Univ. of Applied Sciences
S. Pölten, Austria
peter.kieseberg@fhstp.ac.at

2020 International Conference on Software Security and Assurance (ICSSA) | 978-1-6654-3246-7/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICSSA51305.2020.00009

***Abstract*—The utilization of blockchains in the medical domain has been discussed for quite some time, with multiple academic projects targeting various application domains in this field. Still, many countries feature underlying laws and regulations that make this utilization hard to impossible, especially when considering the sensitive nature of medical records. In this work we analyze the specific situation in Austria and analyse the two major regulations that need to be taken into account, the EU-wide GDPR and the Austria-specific ELGA, with respect to blockchain applications in the medical sector in Austria. Furthermore, we outline several additional key issues that need to be taken into consideration, as well as the problem of the most prominent solution, linking to external storage from the blockchain.**

***Keywords*-blockchain; health care; Privacy; data protection; GDPR**

I. Introduction

Since the publication of the Bitcoin paper by Satoshi Nakamoto in 2008 and the first implementations of blockchains like Bitcoin [1] or Etherum [2], there is a hype around this technology and the possibilities that comes with it. In the beginning the main research and development of this technology was focused around the financial sector. With time going by, many other industries have shown their interest, including the medical sector, especially considering benefits like data integrity, confidentiality and availability for e.g. tamper proofed medical records or medical research data.

Nowadays, medical data is mostly stored in digital form, bringing great benefits for the patients, like fast and targeted treatments, as well as a solid basis for medical research. But with more and more medical data stored in a digital way the risk of this data being stolen [3] or being altered, whether by unlawful manner or simply through errors in data processing, increases. When talking about the handling of medical data, very often a potential health risk is involved. If this data is misinterpreted due to a faulty storage or due to network errors, this can lead to a life-threatening or even fatal situation. The use of blockchains could prevent such conscious or unconscious alteration of data and thus contribute positively to the health of everyone. In some solutions, like MedRec [4], data itself is not even stored directly on the blockchain. Only a reference to the storage location resides directly on the blockchain, thus minimizing the risk of data theft. Still, while many developments are currently in its infancy, it is clear that research and development of blockchain based medical use cases is of great value for patients, practitioners and researchers alike.

Another aspect to be considered is the handling of personal data. In times, where personal data is considered to be a valuable asset and nobody really knows who has stored which data about them and for what purpose this data is used, the need for a sufficiently secure legal situation is essential for the handling of personal data and privacy. For this reasons the EU has issued the ”General Data Protection Regulation” [5] (GDPR). The GDPR regulates data protection and the handling of personal data that is electronically recorded and processed in the European Union (EU). This leads to the question on how the GDPR affects the use of blockchain solutions in the medical sector, and whether it even makes the use of such technologies impossible. leading to a major topic of this work.

This led to the following research question that shall be answered within this work: Is it possible to operate a medical blockchain in accordance with the General Data Protection Regulation (GDPR). This gives rise to two subordinate questions:

- If so is this technology at all practicable for this purpose?
- Are possible legal impediments sufficient to prevent this new technology?

In order to answer these questions, we will first discuss major use case scenarios for the integration of blockchains into medical data systems and afterwards discussing the legal implications with respect to privacy and data protection as imposed by the GDPR.

II. Possible use cases in the medical sector

In this section we discuss selected use cases from the field of medical systems. It must be noted that due to our personal experience in this field we do not focus on the

978-1-6654-3246-7/20/$31.00 ©2020 IEEE
DOI 10.1109/ICSSA51305.2020.00009

issue of providing research data to external labs, as many approaches in this field do, but rather on the everyday work in large hospitals.

A. blockchains as suitable solutions for medical applications

The general discussion on the issue of reasonableness of switching to blockchain technologies for given applications has been discussed by several researchers in the past and more often than not these analysis results in the conclusion that the added complexity of the blockchain does not benefit the use case (see e.g. [6]), as it is possible and less complex to implement the same features with standard solutions. The National Institute of Standards and Technology (NIST) offers a flowchart [7, p. 42 Fig.6] that serves as a decision-making aid and should help to determine whether a blockchain is suitable for the planned use case or not. The flowchart consists of six questions, if all six questions can be answered with yes, using a blockchain would be a viable solution. Following, we will answer these questions with respect to a medical environment.

- **Need of shared consistent data store?**
  Currently, uniform and central access to medical data is far from being implemented in most countries, even though this would make the treatment of patients much easier because all data could always be taken into account for diagnosis. So a uniform access to medical data using blockchains could improve medicine and healthcare.
- **Does more than one entity need to contribute data?**
  Since every producer of medical data such as healthcare providers, doctors or laboratories would deliver medical data, this question can clearly be answered with yes.
- **Data Records once written are never updated or deleted?**
  As shown later on in this paper, it is not advisable to store data directly on the blockchain, because data once written to the blockchain can only be deleted or changed with a lot of effort. It is a better idea to store only references to where the data can be found, see e.g. the solution provided by MedRec [4].
- **Sensitive identifiers will not be written to the data store?**
  This question is difficult to answer, because medical data is usually sensitive and should therefore not be stored in a publicly accessible manner. A possible solution would be to only store pseudonyms in the blockchain. The answer cannot undoubtedly answered with yes, but it is not a definite no either. This question needs to be considered in more detail before implementation, whether or not this should be seen as an obstacle to use in medicine.
- **Have the entities with write access a hard time to decide who should be in control of this data?**
  The health care providers, governments and insurances disagree who should have control over this data. The sole control over medical data of a person should lie with the person him-/her-self, but actually a patient should not have write access to his/her medical data either. An X-ray image actually belongs to the patient, as it is a picture of his/her body and can therefore be seen as personal data. If this patient now wants that this picture has to be deleted after the diagnosis, which is legally secured by the GDPR or ELGA for data protection reasons, it has to happen. Here the legal regulations for the storage duty of medical data must be considered. This could become a problem for a hospital in case of lawsuits concerning this case, if there is no evidence of what really happened.
- **Need of tamper proof log of all write access to the data store?**
  A clear yes can be given to this question, every access to medical data should be monitored. If data is ever stolen or changed, there should be a possibility to find out who has accessed that data.

Based on these answers it is clear that the use of blockchains in medicine has a legitimate reason, still, the questions regarding where and how sensitive data should be stored and processed and who is the owner of this data, require a more detailed verification. But before considering to use a blockchain or not it should be evaluated whether the cost calculation works out and the use of a blockchain delivers a great enough benefit to start the time-consuming process of implementation.

Gajendra [8] describes a few possible use cases for blockchain in medicine, a few of these ideas will be discussed in detail: Electronical medical health records, Data provisioning for medical research, issuing and verification of prescriptions, monitoring of drug production and distribution in the Pharmaceutical Industry.

B. Electronical Medical Records (EMR)

Nowadays, everyone receives medical treatment during his or her lifetime, during which health data is collected and digitally stored. At the moment, however, this data is stored separately for each health care provider, in addition each health care provider uses different systems for collection and storage, including outdated systems. One of the most significant challenges faced by the medical industry today lies in the sharing of the previously collected data with other providers while maintaining data integrity and protecting patient privacy. In the case of a later treatment with another provider, gaining access to this data could prove difficult and time consuming.
With the help of blockchain it would be possible to store and process this personal medical data per person in a secure way. Blockchains offer many different ways to reach this,

e.g. it would be possible to entrust each patient with full control over his or her personal health records and not, as it is the case today, many providers holding parts of a person's health data. Thus the medical history of a person can be taken into account for the rest of his/her life with every new visit to the doctor. This enables a faster and more thorough treatment of patients as a wrong treatment can be avoided by considering previous treatments. With this technology it would even be conceivable at some point in the future to operate a uniform medical record for the whole world, to provide the correct treatment at any given time and place.

Most of the use cases in a medical environment are largely based on an existing unified EMR system. Since most applications involve patient data, an implementation of such a solution is required before it could be used on a large scale.

C. Medical research

One of the main problems with medical studies is finding the right number of patients who meet the required criteria to participate in a study. A recent study [9] says that only 16% of patients are aware of ongoing trials that could benefit their health. As suggested in [10], blockchains and smart contracts could be used to participate more easily in medical studies, for example it could be possible to search completely anonymously for certain medical criteria that correspond to the searched inclusion criteria. Smart contracts could be used to automatically collect health data, of course only with the consent of the patient, and then forward this data anonymously to the medical researchers. On the other hand, the patients could search for or could be informed about suitable existing medical trials. Another benefit could lie in effective tracking and managing consent agreements, research data, side-effects and other metadata. Another requirement of clinical trials is that all examinations and results must be accurately recorded to confirm the authenticity of the study. Every study thus needs a tamper-proof protocol so that it can be verified by the authorities to prove correctness.

D. Issue and verification of prescriptions

Abuse of prescription drugs means taking them in an unprescribed amount or even taking drugs that are issued to someone else. This abuse leads to countless dead and drug addicts every year worldwide. A blockchain solution could avoid some of these problems. Suppose a doctor prescribes a drug to a patient using such a solution. The patient has access to this prescription via his/her smartphone and goes to the pharmacy to pick up the medication. The pharmacist can easily verify that the patient is receiving the correct medication. This whole process is then stored as a transaction in the blockchain, can no longer be changed and can be used as a log about the delivery of the medication at a given time. This solution would also completely prevent the falsification of prescriptions filled out on paper. Another positive aspect of such a solution would be that a patient would not be able to obtain a prescription from two different doctors and then sell or misuse it, because each doctor can see which medication was prescribed earlier to this patient.

E. Monitor Drug production and distribution in the Pharmaceutical Industry

In developing countries one out of ten medications is counterfeit according to the WHO [11]. When we follow up our example from above, a blockchain solution can also assure the patient that he/she receives original medicine, since the authenticity and integrity of the production chain could be secured with a logistic blockchain. The same logic that could be used to track the way of a prescription, could also be used for the production and distribution of prescriptive drugs. Based on this data, the patient can determine when and where this medicine was manufactured. With such a solution it is possible to monitor the whole supply chain of the medical industry, preventing counterfeit drugs to be infused into the market. Chronicled [12] provides such a solution with Mediledger [13] a confidential chain of custody and physical chain of custody supply chain solution.

III. Solutions already in use

In this section, we give a brief overview on solutions already in use or (mainly) suggested by researchers at the time of writing this paper. Since the market is very saturated with possible solutions at the moment, we take a closer look at a few solutions to show what could possible be done with blockchains in medical environments.

A. Guardtime KSI

In 2016 Estonia decided to secure the health records of their entire population of 1,3 million people with the Guardtime KSI blockchain [14], a company founded in 2007 in Estonia with a wide variety of Business associates. KSI stands for *Keyless Signature Infrastructure* as the name promises, unlike classical asymmetric cryptography, that no key is needed to determine the authenticity of data. KSI fully relies on the security of hash-functions and the availability of the data in a *hash calendar*. A hash calendar is a data structure that is used to measure the passage of time by adding hash values to an append-only database with one hash value per elapsed second. To achieve this, a hash value is calculated for each file to be processed and combined into a Merkle hash tree. Within a defined time period, this process concatenates all data and creates a top-root hash. This top-root hash is then appended to the already existing top-root hashes of the past, thus building the KSI blockchain. The steps to calculate the hash value of a file can easily be repeated, thus allowing virtually everyone to verify the authenticity of a digital asset. To calculate the required hash

values and Merkle trees, an *Aggregation Network* is needed, where the Hardware is provided by the Estonian government and is maintained by Guardtime. This Network is topped by a Core Cluster which handles the network consensus. There are also Gateways which work as protocol adapters to support external protocols and interaction with the outside world [15].

B. MedRec

The Massachusetts Institute of Technology developed MedRec [4], an approach for a permissioned blockchain for managing access and sharing of EMR's across different providersm based on Ethereum and built around three Smart Contracts.

1) **Registrar Contract:** Allowing a patient to enroll their participation in the blockchain and link their Ethereum address to an unique identifier. With this identifier the patient can then be recognized in the blockchain and thus it is ensured that no patient exists twice.
2) **Patient-Provider Relationship Contracts:** This contract is issued between two nodes of the network, which in this case means nothing else than linking the patient data to a provider. These links can be used to determine which patient and provider have access to this data. In this link nothing else is stored than a data query that is specified for the system of the provider and can only be used there. In order not to store these queries unprotected in the blockchain, they are made unrecognizable by using a hash function. Before a Patient-Provider Relationship Contract is issued the Registrar Contract is run to see if the patient is already enrolled, if so the Patient-ID is fetched and linked to the Relationship Contract.
3) **Summary Contract:** This contract holds a list of all Patient-Provider Relationship contracts from a person. With this contract, the complete medical history of a patient, which is stored in the blockchain, can be mapped. The summary contract may also be used to manage notifications of changes to data or the release of data to third parties, of course only after approval of the patient.

Furthermore, a *System Node* is needed to communicate with the already existing data structure of each provider. MedRec integrates data protection, as no data is stored directly on the blockchain.

C. FHIRChain

The FHIRchain [16] is a blockchain based on the "Fast Healthcare Interoperability Resources" (FHIR) standard. This standard describes data formats and elements for EMR's and provides an interface to exchange them, with a focus on healthcare and meets the requirements of the Office of the National Coordinator (ONC) interoperability roadmap [17] that outlines the steps necessary to implement a uniform digital health care system in the United States until 2024.

FHIRchain uses public key cryptography to identify patients and doctors. In this procedure, a key pair is generated for each participant, the public key is used as *Digital Health Identifier* and subsequently stored in the blockchain for identification purposes and for tamper-protection. For reasons of scalability and data protection FHIRchain does not store data directly on the blockchain, but only references to where this data can be found. Like MedRec, FHIRchain has a connector that handles access to the data directly in the database. Furthermore a token based permission model is used to access the data, the data is protected with a mechanism called "sign then encrypt" [18]. where data is signed and encrypted and only those who have access to the digital identity public key can access it.

D. Scrybe

Scrybe [19] was developed by a team of researchers of different Universities. The approach is a tamper-proofed blockchain-based data provenance tool to enhance clinical trials data integrity and provide non-repudiation.

In he first step, the personal data of a patient such as the participant's family background, health history or medical background is collected and stored. This step could be avoided with an already implemented EMR system. Once this has been done, a reference is made to where this data can be found in the form of a transaction and is then stored on the blockchain, thus the confidential data never leaves the secure server. This transaction is digitally signed by the researcher in charge of the trial. All further data regarding the participant is then added to the record. including references to the actual data store saved on the blockchain. After completion of the study, the second step is the evaluation of the collected data by the authorities to verify the integrity of the data. The auditors query the results of the test series in the blockchain and thus are enabled to evaluate and verify the guaranteed unchanged data.

Again, no data is actually stored on the blockchain, allowing each participant of the chain to keep the data of the trial in their own secure locations.

E. EU Projects

In April 2018 the EU created the European blockchain Partnership (EBP) [20] and cooperate in the establishment of a European blockchain Services Infrastructure (EBSI). This partnership aims for a EU-wide cross-border public services using blockchain technology, within this partnership also My Health My Data (MHMD) [21] was created from

the "Collective Awareness Platforms for Sustainability and Social Innovation" (CAPSS). MHMD is a Horizon 2020 research and innovation program, which aims at fundamentally changing the way sensitive data is shared. MHMD tries to develop a dynamic consent interface, so that patients can handle their data on their own, allow, refuse or withdraw access to them according to their needs, allowing patients to access their data in a personal cloud from any personal device from anywhere. Another important aspect of MHMD is the de-identification and encryption of personal data before it is made available for researchers or analysts, thus ensuring compliance with the GDPR.
MHMD Technology is based on Hyperledger Fabric [22] using Smart Contracts. Medical data is stored separately in the data centers of each participant and only a hashed reference to where the data is stored is made publicly available. This hash value is matched to a real individual in an offline database and is only accessible for the owner of the database where this data is stored, as well as the patient.

Currently, the only working solution in a real life environment is, at the moment, Guardtime with KSI blockchain in Estonia, the others solely propose interesting approaches and ideas.

IV. General Data Protection Regulation (GDPR) and Elektronische Gesundheitsakte (ELGA)

This chapter takes a closer look at the legal situation in Austria for the use of blockchains under consideration of GDPR [5] and ELGA [23] in a medical environment. First, we take a closer look at the GDPR whether operating a productive medical blockchain in compliance with the GDPR is legally possible at all. Thereafter, ELGA is considered under the same conditions; in the absence of existing work on ELGA, only the legal text is considered here. To conclude the chapter, we bring these three topics, GDPR, ELGA and blockchain, to a common denominator.

A. General Data Protection Regulation GDPR

The GDPR has been in use for almost two years, and developers and manufacturers are still unsure, because of Article 17 "The right to be forgotten" and other paragraphs, whether it is possible to operate a blockchain in accordance with the GDPR or not. The EU is also aware of this important issue and commissioned a study by the Panel for the Future of Science and Technology to analyse the legal situation [24]. Also MHMD is aware of this problem and has carried out a data protection impact assessment [25] to clarify this situation. Other researcher have also examined this topic, for example "blockchain in EU E-Health" [26] or "Privacy by blockchain Design: A blockchain enabled GDPR compliant Approach for Handling Personal Data" [27] and many more.

A very important distinction has to be made between anonymization and pseudonymization, since the use of a blockchain may result in pseudonymised data such as hashed user data, which needs to be regarded as personal data and must be treated accordingly.

1) GDPR and Medical Data: Under Article 4 (13, 15), the concepts of genetic and health data is defined. Article 9 (1) clearly defines that the processing of special categories of personal data, which includes genetic and health data, is not allowed. In the same article under paragraph 2 however, they then repeal this allowance under certain conditions. Important here is Article 9 (2a):

> *"The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject."* [5]

Therefore personal medical data is clearly covered because it can be attributed to a natural person and as long as the data subject has given his consent. So the GDPR has to be taken into account when implementing a medical blockchain.

As already mentioned in this paper, personal medical data should not be stored directly on the blockchain, as it would be a security risk. A better way to handle this, is to store only references to where this data can be found on the blockchain. Still, this opens up new questions regarding the integrity protection provided by the blockchain, especially if no hash values of he data will be stored alongside the references in the blockchain, as this would allow attackers to exchange the data at the reference point, thus not requiring changes to the blockchain for changing data. Storing additional information alongside the reference ist often a problem, as according to the GDPR Recital 26, a natural person is considered identifiable, either directly or indirectly, as soon as it is possible to draw conclusions about their personal information. A reference such as a membership ID or similar, with access to the reference table, could allow conversion of this data to its origins and thus allow identification of the person. This backwards conversion of data results in personal data and is therefore protected. For these reasons, Article 32 defines that personal data shall be stored in pseudonymised and encrypted form without exception and that a procedure shall be in place to regularly review, assess and evaluate the effectiveness of technical and organisational measures to ensure the security of the processing.

2) Important Data Subject Rights: The GDPR under Chapter 3 Articles 12 to 22 defines several key rights for individuals that need to be taken into account when

providing a medical blockchain. Following we list the most important rights with respect to medical blockchains:

- **Right to be informed (Article 13 and 14)**: The data subject has the right to be informed on how their collected, processed and stored data is used and for what purposes
- **Right of access (Article 15)**: The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data.
- **Right to rectification (Article 16)**: The data subject has the right to have incorrectly recorded data corrected.
- **Right to erasure, right to be forgotten (Article 17)**: The data subject has the right to obtain the deletion of any personal data stored or collected concerning him/her.
- **Right to restriction of processing (Article 18)**: The data subject has the right to restrict the collection, processing or usage of his/her personal data.
- **Right to data portability (Article 20)**: The data subject has the right to receive his/her personal data in a structured, commonly used and machine-readable format and to transfer this data to an other data controller of choice.
- **Right to object to processing of data (Article 21)**: The data subject has the right to object to the processing of his/her personal data without explicit consent and to know how and by whom such data are processed.

On the one side, some of these rights support the use of a blockchain, as with a blockchain, the right to limit processing is easy to implement, as it is possible for the owner of the data, the patient, to refuse the processing of his or her data, e.g. through a smart contract via their Smartphone. Also the right to be informed and the right of access can be easily implemented. Data portability could also be easily achieved if a standard in medical data could be agreed upon.

On the other side, the issues of rectification and erasure pose big issues regarding the non-changeability of blockchains. To mitigate this, the data shall not stored on the blockchain directly as pointed out above, which again could lead to issues regarding the integrity protection property of the approach. Thus, the blockchain technology stands directly diametrically to GDPR compliance, at least regarding naive approaches, as the GDPR was created with the idea of centralized data stores in mind, The EU has already recognized this issue with MHMD [21] and their studies regarding it, though.

B. The Elektronische Gesundheitsakte (ELGA)

In accordance with Article 9 (4) GDPR: *"Member States may introduce or maintain additional conditions, including limitations, as far as the processing of genetic, biometric or health data is concerned."* in Austria this is done by the ELGA Act [23] (ELGA-A). ELGA and GTel-G have the GDPR as their basis and extends it to include specific cases in the health sector in Austria. An essential feature of the public health system in Austria is equal and easy access for all health services, regardless of age, place of residence, origin and social status. Since this access is handled differently from province to province, the ELGA Act enables this uniform access for everyone. It regulates both the ELGA participants rights, as well as the rights and obligations of ELGA health service providers. The law also defines what format and structure health results must have and who is responsible for implementing each ELGA component. Together with the Health Telematics Act (GTelG 2012) [28], it forms the legal basis for the handling, processing and access of health data in Austria. In addition, several other laws need to be followed, that are mentioned for completeness: (i) General Data Protection Regulation (GDPR), (ii) the Data Protection Act (DSG), (iii) the Doctors Act (ÄrzteG 1998), (iv) the Hospitals and Health Resorts Act (KAKuG), (v) the Pharmacy Act, (vi) the General Civil Code (ABGB), (vii) the Patientencharta (Article 15(a)-Agreements to ensure patient rights) and (viii) the E-Government Act (E-GovG).

1) Legal aspects of ELGA-A and the GTel-G: The ELGA Act defines the structure, form and standards of ELGA health data, interaction-relevant, non-prescription drugs, as well as authorization and a logging systems. The Gtel-G defines the minimum standard of data security for the processing of electronic health and genetic data and their secure transmission. In addition, the development and control of health telematics creates and broadens the necessary information basis to facilitate the handling of medical data.

2) ELGA Participants and Data storage: According to §15 (1) GTel-G, ELGA is an opt-out model, i.e. everyone participates as long as one does not actively opt out §15 (2). §18 (1) GTel-G defines that the participants have to be recorded in a patient index, this index includes all persons who are insured in the Austrian social insurance system and have not opted out. The participants must be clearly identified in electronic form under §18 (4) GTel-G. According to §20 (1) GTel-G, ELGA health data must be stored on a suitable data storage device in the EU area and must be retained for 10 years. Stored data may not be changed, but if circumstances arise that influence the course of treatment, additionally, an updated version must be stored. In addition, according to §20 (2) GTel-G this health data must be stored in a reference register, which contains links to this data, which must also be located in the EU area. Responsible for this data is, according to Article 4 (7) GDPR, the ELGA health service provider, which generated the data. The ELGA health service provider is the institution or physician where the findings or diagnostic image was taken, such as a hospital or laboratory. Furthermore, it is

defined under §20 (3) GTel-G, that the storage of health data must be decentralized in those organizations where they were created. An exception is e-medication §16a GTel-G, which requires encrypted central storage of the data in order to facilitate access for doctors and institutes. E-medication comprises the drugs prescribed by the respective physician or the drugs dispensed by pharmacies, as well as their interaction-relevant properties. This prerequisites are ideal for the use of a medical blockchain, as no patient data is stored in a publicly accessible manner, this also complies with the legal requirements of the GDPR.

3) Medical data standards and data processing: In §16 ELGA-A it is defined that ELGA health data must meet certain medical standards, for this reason §16 (1) ELGA-A, defines eight implementation guidelines, where the standards to be used are defined and explained in detail. Like the FHIRChain, ELGA relies on international medical standards defined by the IHE [29] and HL7 [30] such as "Cross-Enterprise Document Sharing" (XDS) or the "Clinical Document Architecture, Release 2.0" (CDA) to unify and facilitate data exchange between healthcare providers more easily and in a standardized way. §14 and §15 ELGA-A defines the structure and format of interaction-relevant medication data for prescription and non-prescription drugs.

Defining access rights to this data is another important part: According to §14 (1) GTel-G, the processing of ELGA health data is only permitted if ELGA subscribers and the ELGA health service provider are clearly identified and according to §14 (2) GTel-G personal ELGA health data may only be used by the ELGA health care providers involved in the treatment. All others will not have access to this data, such as employers, employees, personnel consultants, insurance companies, administrative authorities, courts, members of the Austrian social insurance system and health and accident care institutions, unless they are involved in the treatment or care of an ELGA participant. These restrictions are intended to comply with data protection regulations of the individual and the GDPR. However, they should also ensure that ELGA participants are not disadvantaged by unlawful access to their data by, for example, an insurance company or an employer.

4) ELGA Users Rights: Under §16 the rights of ELGA users are defined, the rights include the following:

- Right of Information and access to the health data concerned, as well as log data.
- The right to determine which data in the form of electronic references is included in the ELGA system. Participants with HIV diseases, mental illnesses, information about genetics or abortions must be made aware of this right in particular, because it could disadvantage them, if this data would appear in the ELGA system.
- Define individual access authorisations according to § 21 (3) GTel-G, this includes:
  - To show or hide health data and electronic references concerning them or to arrange for their deletion. If deletion is not possible for legal or technical reasons, ELGA references must be made inaccessible.
  - Shorten or lengthen the period for existing access authorizations
  - Allow a trusted healthcare provider to have access rights.
- The participants must not suffer any disadvantage in terms of medical care or cost income. However, they are responsible for any consequences of not mentioning a previous illness.

These rights correspond to the GDPR and define them in detail on ELGA health data.

C. Operating a medical blockchain with the specifications given by ELGA and GDPR

The answer, whether to utilize blockchains in the medical sector, cannot easily be answered with "yes" or "no", considering that the key feature of immutability of data on a (public) blockchain conflicts with the data protection requirements of the GDPR. The right to change or delete personal data is very important, as it should be up to each individual to decide who has stored what data about them. Major approaches regarding medical blockchains, as proposed by other researchers and projects, state that patient data should not be stored directly in the blockchain, thus taking data protection aspects into account and allows better scalability due to the smaller data volume stored directly on the blockchain. Furthermore, if only references were to be stored in the blockchain, only these reference links could be made inaccessible for the corresponding references, as defined in ELGA-A, i.e. with regards to the blockchain, the public and private keys would be deleted. It is not clear whether this is in accordance with the GDPR, since these keys and the associated data are also regarded as personal data according to the GDPR and therefore the consent of the person concerned must be obtained. Furthermore, another key issues arises: The point of utilizing a blockchain typically lies in wanting to provide extra integrity, i.e. making it hard to impossible for any participant in the system to manipulate data. With removing the data from the blockchain to extra storage and solely providing a link to the data location inside the blockchain, this benefit suffers greatly, especially when needing to consider (and implement) methods for data un-linking and re-linking to new (corrected) versions. However, if one further considers what easy access to medical data can mean for treatment, research or prescriptions, the use of such a solution would be a positive contribution to the health system. Implementation would certainly not be easy, but with ELGA there is a solid foundation on which to build a blockchain solution upon since many problem areas such as data encoding or access are already defined.

V. Conclusion

Blockchains offer a new way of storing, managing and processing data in many ways. possibly transforming and revolutionizing the way we handle data. Since this technology is still in its infancy and is just beginning to gain a foothold in a variety of application areas such as finance, medicine, identity management, supply chain management and many more, it is not yet possible to estimate how far it will establish itself.

Especially the medical sector could benefit from introducing blockchain technologies, as many companies and research institutions have already recognized, be it for data provisioning for medical studies, establishing electronic health records, or managing medical production or prescriptions, as well as many other possible use cases. For the further use of such solutions, a uniform application of medical standards [31], [32] is essential to facilitate the exchange of medical data more easily.

Another issue requiring attention in the European area is the GDPR, which was created with the idea of central data storage in mind. An essential part of this regulation is the deletion or modification of existing data at the request of the affected user, which is in stark contrast to key features provided by blockchain technologies. A possible solution lies in only storing references to the data in the blockchain, still opening up new problems with respect to data integrity, the very key feature a blockchain-based solution is typically implemented. Furthermore, under some circumstances, these references must be considered personal data in EU law as well, thus this solution has to be analysed in more detail. Alternatively, there would have to be made changes in the GDPR, which is already planed through the European blockchain Partnership [20].

To address the problem of deletion, one possibility would be to exclude these references and make them inaccessible, i.e. to delete the public and private keys so that no one has access to the references which are stored in the blockchain. From a purely legal point of view, the original data cannot be deleted due to the documentation obligation that exists in Austria, since according to the hospital law (Spitalsgesetz) §48 (7) [33] this data must be kept for at least 10 years up to 30 years. The storage has to take place in such a way that an abusive knowledge or changes of the content is excluded, which would actually again speak for the use of a blockchain.

Summarized, a medical blockchain solution could be beneficial for both the individual and the medical providers, still there is a lot to be done to bring medical blockchains into use in a broad field, but the course has been set and it is only a question of time until this happens.

Acknowledgements

This research was funded by the Josef Ressel Center for Blockchain Technologies & Security Management (BLOCKCHAINS). The financial support by the Christian Doppler Research Association is gratefully acknowledged.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic cash system," *Bitcoin*, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] V. Buterin, "A next-generation smart contract and decentralized application platform," Tech. Rep., 2013.

[3] digitalguardian, "Top 10 Biggest Healthcare Data Breaches of All Time (January 2019," 2018. [Online]. Available: https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time

[4] V. T. Azaria Asaph, Ekblaw Ariel and L. Andrew, "MedRec: Using blockchain for medical data access and permission management," in *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, 2016.

[5] "General data protection regulation," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[6] K. Wust and A. Gervais, "Do you need a blockchain?" in *Proceedings - 2018 Crypto Valley Conference on Blockchain Technology, CVCBT 2018*. Institute of Electrical and Electronics Engineers Inc., 11 2018, pp. 45–54.

[7] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *Draft NISTIR*, vol. 8202, 2018.

[8] G. J. Katuwal, S. Pandey, M. Hennessey, and B. Lamichhane, "Applications of blockchain in healthcare: Current landscape & challenges," *arXiv preprint arXiv:1812.02776*, 2018.

[9] A. Thoma, F. Farrokhyar, L. McKnight, and M. Bhandari, "How to optimize patient recruitment," *Canadian Journal of Surgery*, vol. 53, no. 3, p. 205, 2010.

[10] J. Cunningham and J. Ainsworth, "Enabling patient control of personal electronic health records through distributed ledger technology," in *MEDINFO 2017: Precision Healthcare Through Informatics: Proceedings of the 16th World Congress on Medical and Health Informatics*, vol. 245. IOS Press, 2018, p. 45.

[11] T. Kelesidis and M. E. Falagas, "Substandard/counterfeit antimicrobial drugs," *Clinical microbiology reviews*, vol. 28, no. 2, pp. 443–464, 2015.

[12] Chronicled. Chronicled. [Online]. Available: http://www.Chronicled.com

[13] ——, "The mediledger project 2017 progress report." [Online]. Available: https://uploads-ssl.webflow.com/59f37d05831e85000160b9b4/5aaadbf85eb6cd21e9f0a73b_MediLedger 2017 Progress Report.pdf

[14] Estonia. ehealth authority partners with guardtime to accelerate transparency and auditability in health care. [Online]. Available: https://e-estonia.com/ehealth-authority-partners-with-guardtime-to-accelerate-transparency-and-auditability-in-health-care/

[15] A. Buldas, A. Kroonmaa, and R. Laanoja, "Keyless signatures' infrastructure: How to build global distributed hash-trees," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2013.

[16] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 267–278, 01 2018.

[17] "Connecting health and care for the nation, a shared nationwideinteroperability roadmap," 2020. [Online]. Available: https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

[18] H. Krawczyk, "The order of encryption and authentication for protecting communications (or: How secure is SSL?)," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2139 LNCS, 2001, pp. 310–331.

[19] R. R. Brooks, K. C. Wang, L. Yu, J. Oakley, A. Skjellum, J. S. Obeid, L. Lenert, and C. Worley, "Scrybe: A Blockchain Ledger for Clinical Trials," *"In IEEEClinical Trials Forum"*, 2018. [Online]. Available: https://blockchain.ieee.org/images/files/images/clinicaltrialsforum-2018/Clemson_WhitePaper.pdf

[20] "European blockchain partnership," 2018. [Online]. Available: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50954

[21] M. LLC. myhealthmydata. [Online]. Available: http://www.myhealthmydata.eu

[22] "Hyperledger," 2020. [Online]. Available: https://www.hyperledger.org

[23] "Gesamte rechtsvorschrift für elga-verordnung 2015," 2015. [Online]. Available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009157

[24] "Blockchain and the General Data Protection Regulation : can distributed ledgers be squared with European data protection law? : study," *European Parliament*, 2019.

[25] C. L. P. Rocco. Myhealthmydata (mhmd): Deliverable 2.6 - privacy-by-design and compliance assessment. [Online]. Available: https://www.poa.network/for-users/whitepaper/poadao-v1/proof-of-authority

[26] U. M. Gassner, "Blockchain in EU e-health - blocked by the barrier of data protection?" *Compliance Elliance Journal*, vol. 4, no. 3, pp. 3–20, 2018. [Online]. Available: http://ul.qucosa.de/api/qucosa%3A32042/attachment/ATT-0/

[27] C. Wirth and M. Kolain, "Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data," *In Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET)*, p. 6, 2018.

[28] "Gesamte rechtsvorschrift für gesundheitstelematikgesetz 2012," 2012. [Online]. Available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008120

[29] "Integrating the health enterprise," 2020. [Online]. Available: https://www.ihe.net

[30] "Health level seven international," 2020. [Online]. Available: https://www.hl7.org

[31] D. Kalra, "Electronic health record standards," *Yearbook of medical informatics*, vol. 45, pp. 136–44, 02 2006.

[32] R. H. Dolin, L. Alschuler, S. Boyer, C. Beebe, F. M. Behlen, P. V. Biron, and A. Shabo, "HL7 clinical document architecture, release 2," *Journal of the American Medical Informatics Association*, vol. 13, no. 1, pp. 30–39, 01 2006.

[33] "V-sg - spitalgesetz 2001," 2001. [Online]. Available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=LrVbg&Gesetzesnummer=20000372