Cloud Computing and Data Science
http://ojs.wiserpub.com/index.php/CCDS/

UNIVERSAL WISER PUBLISHER

Research Article

A Risk Analysis on Blockchain Technology Usage for Electronic Health Records

Christian Ploder*, Teresa Spiess, Reinhard Bernsteiner, Thomas Dilger, Rebecca Weichelt

Department Management, Communication & IT, Management Center Innsbruck, Innsbruck, Austria
Email: Christian.Ploder@mci.edu

Received: 26 January 2021; **Revised:** 12 March 2021; **Accepted:** 25 March 2021

Abstract: Health data is one of the most valuable data and highly sensitive. Its careful handling is essential in today's digitalized world and cloud technology use for sharing. Health Information Systems facilitate the storage and accessibility of health data for better care along the patient path. As the integration of all historical patient data, the Electronic Health Record is at the heart of health data management. The centralization of stored health data represents a single point of failure and trust, making data exchange across institutions difficult and insecure. Blockchain technology builds on consensus mechanisms and immutable chains of blocks for validating and securing data transactions as a modern decentralized approach. The application of blockchain technology for Electronic Health Records is promising but still a young concept. Due to the wide range of discussion, this paper aims at identifying risks by using blockchain technology in the eHealth sector. Based on a systematic literature review, various authors' argumentations and findings are examined and concluded to set up the empirical study. The semistructured qualitative interview study aims to find out the threats of blockchain. The paper concludes with an overall discussion and some implementation recommendations.

***Keywords*:** eHealth, blockchain application, Electronic Health Records, eHealth risks

1. Introduction

Blockchain is considered one of the most disruptive global technological transformations since the Internet in the 2000s. The unique characteristics of blockchain are its decentralization and a network of distributed, connected nodes that execute the transactions [1, 2]. That way, blockchain offers a solution to centralization's often criticized idea [3-5]. It is characterized by its ingenious encryption system, the immutability of records, and traceability virtues [6]. For those reasons, even the military trusts blockchain technology [7]. The application cases primarily control the supply chains of defense, cybersecurity in communications, and other areas under experimentation, such as weapon systems activation [7]. The blockchain trend started with the virtualization of money into cryptocurrencies, with Bitcoin being the first, followed by many others. Already in 2016, roughly 80% of $ U.S. bank deposits only existed virtually as so-called ledger entries [8].

Parallel to the blockchain trend, the healthcare sector is experiencing a transformation, initiated through digitalization and increasing collaboration [9]. Voices for a digital, cross-institutional collection, storage, and

DOI: https://doi.org/10.37256/ccds.222021777

transmission of health data are getting louder. The necessity to access patient data at different healthcare facilities and by the patients themselves is growing with the networking of systems and institutions. However, a standardized solution for the digital storage of all historical patient health data, called Electronic Health Record (EHR), is still missing. According to [10], every patient in the U.S. has almost 20 different health records. Every year 150 exabytes of health data are being stored [11], but based on various standards and records. Considering that medical records have ten times the value of other data on the black market [11], there is no doubt that sensitive health data needs superior protection. Specifically, digital data is exposed to hacker attacks. Estonia's example shows that a combination of both trends, blockchain, and EHR, can be an interesting perspective for the future of health data storage (E-estonia (n.d.). healthcare).

Many information systems exist in healthcare, but often with different technical standards implemented, which leads to trouble in connecting them. A Healthcare Information System (HIS) manages health data with patients' trust, expecting to receive the best patient treatment. These days, HIS still lacks interoperability depending on countries, regions, providers, etc. [12]. As part of a HIS, the EHR system aims to foster a cross-institutional exchange of health data. The goal is to have a complete patient record with all health-relevant data for successful and efficient patient care. The EHR fulfills these conditions by providing an IT infrastructure that enables the management and exchange of health data among institutions, IT systems, stakeholders, and, of course, the patient [13]. EHR communicates with other systems via interoperability standards and contains sensitive patient data. Thus, it needs protection with the best-suitable technology. Various new technologies are being developed to ensure privacy and the integrity and confidentiality of health data [14]. Blockchain could be a possible solution for these needs.

It has recently gained traction in the financial sector through the cryptocurrencies Bitcoin and Ethereum. Financial data share similar requirements regarding privacy and security requests. Researchers are now looking for a possible solution to combine EHR with blockchain technology in the healthcare sector [15]. Data leaks and successful HIS attacks visualize the problems concerning the protection and sensitive handling of patient data, even though HIS are told to be secure [16]. Hospitals, private companies, and even international health and political organizations such as the EU discuss the benefits and possibilities of blockchain implementation for standardizing and facilitating EHR exchange. Within the last few years, a wide range of scientific studies appeared on potential use cases. Due to a considerable amount of research on this topic, it seems necessary and relevant to provide an overview of blockchain technology's current status quo with a particular focus on EHR. Since all digital health services are based on some kind of HIS, especially on the EHR, as a historical file storing all patient-related data [17], the collection of relevant literature will be focused on this specific scope.

2. Theoretical background

The theoretical background is based on a systematic literature analysis following the steps of [18]: (1) problem formulation, (2) literature search, (3) literature evaluation, (4) analysis and interpretation, and at least the (5) presentation of the results. This five-step approach was expanded by [19]. After the formulation of the research question, the selection criteria were defined and logically combined to use them for the search in the following scientific databases: general databases (SpringerLink, Science Direkt, Emerald), technical databases (IEEE Xplore), and medical databases (PubMed, JMIR) to tackle all different angles needed to get an overview of the topic. An overall number of 436 literature references have been found. In the next step, the references are aggregated and interpreted. The results of the literature analysis are presented in the following subsections.

2.1 *Blockchain*

Countries utilize national payment systems for the clearance and settlement of transactions. As a result, transaction processes became slow, expensive, prone to errors, and influenced by more actors than the end-to-end transaction partners [20]. This architecture of individual interacting systems follows a centralized approach since central authorities control the process execution [21]. The implication is that each system is a closed one, managing and processing transactions. For this purpose, all systems keep their records for the storage of accounts and transaction information. In technical terms, this is referred to as a general ledger, meaning a data store. To ensure the functioning of a single system, a lot of effort is required. From a security perspective, protection against manipulation, break-ins, and unpredicted

downtime to assure correctness and functionality are crucial. Such a centralized system represents a potential single point of failure and entails a corresponding operational risk for the involved parties [3]. Passing across several of these systems during one financial transaction process leads to an accumulation of costs, risks, and time [4].

Given these inefficiencies in processes across all industries, with financial transactions as an example, it would be desirable to carry out direct transactions between partners without additional intermediaries in many concerns [5]. Regarding the points of criticism mentioned, a central system to manage all process steps at once would be necessary. However, the problem is that single institutions would control all transactions [22]. Based on the technological developments of the past years, a distributed approach is a viable alternative. Blockchain is one famous, modern digital decentralized approach [23]. It had its roots in 2008 when everything started with Bitcoin [24]. However, blockchain is valid for many more industry sectors than finance [25], and the usage for EHR will be presented later in this paper.

2.1.1 *Definition*

Although no universal definition exists, many authors highlight the decentralization and access to information in a transparent network [26-28]. Therefore, blockchain can be described as a peer-to-peer network with no central authority but with the right of approval, including all participants that shapes an environment of democratic consensus and decentralized trust [23]. This access to right structure ensures that all participants receive a copy of the blockchain.

2.1.2 *Characteristics*

Blockchain operates a network of different participants in which each node has the same rights. Any person can operate the nodes [29]. To maintain the same rights, an unequal balance of power is not permitted. That is ensured by providing all nodes with the same information and the same right to add new information to the network. Consequently, each node owns a ledger copy, which is essential protection against network manipulation, as it is unlikely that the majority of nodes are involved [30]. The functionality of the network remains intact even if individual nodes or node segments fail. The same applies to the addition and removal of nodes. The complete redundancy caused by the ledger's distribution is a means against unilateral power, manipulation, and failure, whereby the system's architecture alone provides protection mechanisms [31]. The blockchain approach is universally applicable since the blockchain represents an information store due to the generic function. The possible range of applications is correspondingly broad [30]. Assets represent an object such as a document or a cryptocurrency. Storing these objects in blocks and linking them by a unique, unchangeable characteristic ensures an immutable record [32]. Blockchain fulfills various functions, especially the mediation function when it comes to the distribution of data to all parties. In principle, the blockchain can be summarized as a record of all executed transactions [33].

2.1.3 *Private vs. public blockchain*

As such, a blockchain can be used in public or private mode. A public blockchain is, for example, the Bitcoin blockchain. Here, all transactions can be viewed by anyone at any time. That means that the participants know which transactions took place but do not know which participant carried out this transaction because only cryptographic addresses are used in Bitcoin. No person-identifying information is disclosed [34]. That ensures anonymity through pseudonymization [35]. In public blockchain approaches, there is usually a high demand for anonymity of specific data. For data leaks, which have occurred frequently in centralized systems, there is a wide range of possible attacks due to redundancy.

On the other hand, a private blockchain is a closed system operated as a shared system among several cooperation partners or in-house as an alternative to existing technology. Instead of public access to the blockchain, it is limited to a group of authorized persons [36]. Due to data protection issues, this variant is preferred for many applications-especially in European Union states which have to be compliant with General Data Protection Regulation (GDPR) [37, 38].

2.1.4 *Permissionless vs. permissioned blockchain*

Furthermore, a distinction is made between permissionless and permissioned blockchain. Only authorized participants can set up a transaction; others only have read access to the blockchain. A permissionless blockchain does

not differ between participants' authorizations [34]. In conjunction with the public and private modes of the blockchain, different combinations are possible. Depending on the mix, there are also effects on the requirements for consensus mechanisms. Private blockchains are not secured with a similar complexity level as public blockchains because of the higher trust if participants are known to each other compared to anonymous networks [36].

2.1.5 *The structure of a block*

The structure of a block includes different features. It is divided into two sections-the header and a block's body [39]. According to [39], "the block header includes (1) Block version: indicates which set of block validation rules to follow. (2) Parent block hash: a 256-bit hash value that points to the previous block. (3) Merkle tree root hash: the hash value of all the transactions in the block. (4) Timestamp: current timestamp as seconds since 1970-01-01T00:00 UTC. (5) nBits: current hashing target in a compact format. (6) Nonce: a 4-byte field, which usually starts with 0 and increases for every hash calculation." [39]. The block body contains the transaction data, consisting of a count and the list of transactions. The count indicates how many transactions have already been carried out [40]. Transaction data consists of input, namely the public key (= ID) of the sender, the amount transacted, the receiver's public key, and the transaction output [41].

With that concept, all blocks are connected to the so-called blockchain (see Figure 1). Within the chain, every block has the own and the previous hash stored, which is the fingerprint of every block. If the hash from one block is changed after the initial establishment (as shown in Figure 1), the blocks' linking is broken, and the whole chain loses validity. Such blocks are called malicious blocks.

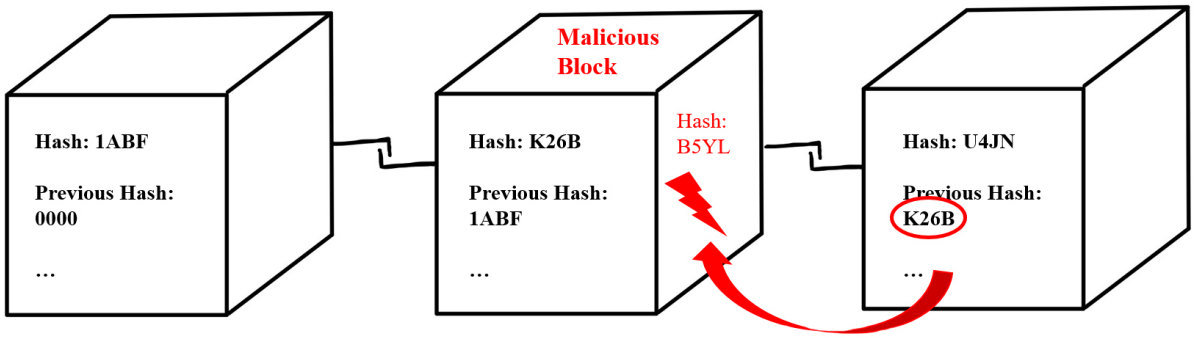

Figure 1. Blockchain schema (own illustration)

2.1.6 *Blockchain security risks*

Although the advantages of blockchain technology are treated frequently, the downsides and risks are way less discussed. In that regard, Antonopoulos A. M. [42] discusses various consensus attacks. With a 51% attack, an attacker controls 51%, or more mining power of the blockchain network is used. This superior mining power enables the attacker to execute distributed denial-of-service (DDoS) attacks and double-spend his transactions. The 51% threshold of mining power almost guarantees success. However, it can also be successful with less than 51% of the mining power. Acquiring 51% of the total supply of a cryptocurrency seems to be a complicated endeavor. As described by [43], this can be achieved at almost no cost if the attack happens at a very early stage of the blockchain lifespan. Despite the previously described attack, there is also a threat of forks on public blockchain systems. Those can happen unwittingly when two miners find a new block and propagate it. That results in a fork until the following block for one of the previous two blocks is found [42].

Weber I., et al. [44] discuss the availability in blockchain systems which is also one of the three significant properties (Confidentiality, Integrity, and Availability) of data security. One of the recently published academic evidences discussing data integrity in blockchain systems is [45]. This paper discusses how to achieve data integrity when a blockchain is used as a data management system rather than integrity on the blockchain itself. Li X. [46]

conducted a risk analysis of blockchain systems previously. This paper analyzed generic risks in blockchain without any limits. The identified risks are 51% Vulnerability, Private Key Security, Criminal Activity, Double Spending, Transaction Privacy Leakage, Criminal, vulnerable and under-optimized smart contracts, underpriced operations. The identified risks by [46] are generic risks that are not focused on data integrity. Hence, it cannot be ruled out that the research (results) conducted in this research will partly overlap with the results in the study by [46]. Nevertheless, the given study results will not be used as a basis for the research conducted in this research due to its different focus.

2.2 *eHealth*

Digitalization has played an increasingly important role in the healthcare sector for decades [9]. The increase in chronic illnesses and multiple-morbid persons in need of care poses new healthcare system challenges. Without digitalization, it would be much more challenging to provide adequate medical care to an aging society and rural areas. However, communication between physically distant health service providers is still insufficient for many patients' comprehensive care [47]. The availability of information independent of time and place and the digital exchange of knowledge of the health staff increasing work efficiency and bring actual cost savings in the health system as a positive side effect [48]. Dual diagnoses and treatments become unnecessary if the entire professional staff has the same information about the respective patient [49]. The literature describes the extensive possibilities in the digitalization of the healthcare system as "Electronic Health" (eHealth) [50].

2.2.1 *Definition of eHealth*

The different definitions of eHealth often addressed concrete ideas or solutions for the healthcare system, which was initially strongly criticized. The Journal of Medical Internet Research (JMIR) issued six articles titled "What Is eHealth?". The editorial board advised against deciding for one single definition of eHealth in their collaborated work "CONSORT-eHealth". It is a continuously changing term, circulating in a dynamic environment; its application and stakeholders define it [51-56].

EHealth comprises the fields of telemedicine, eHealth in prevention, health promotion and care, eHealth and economics, digitalization of information and content, and eHealth for research and health reporting [57]. Therefore, the superordinate fields of IT, medicine, and health management can be derived as visible in Figure 2. Since IT enhances the two other fields, it is crucial to look closely at the respective technology, especially in hospitals and similar companies in the health sector.

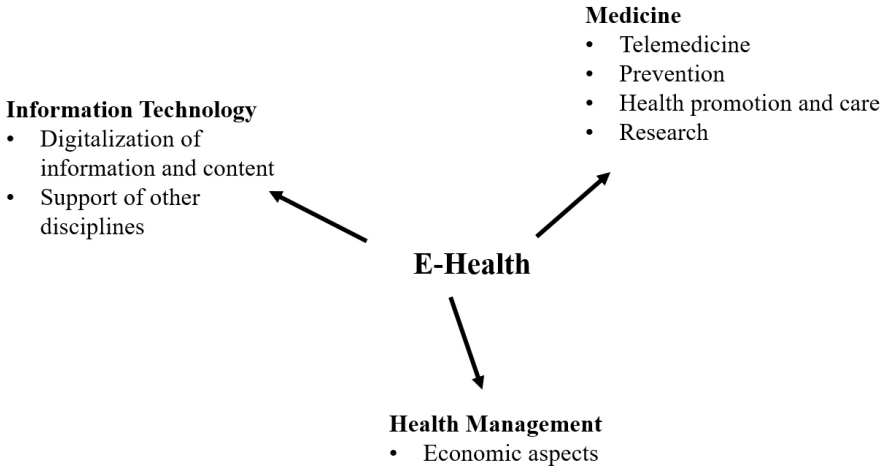

Figure 2. Fields of e-Health (own illustration)

2.2.2 *Clinical information system and EHR*

The Clinical Information System (CIS) is a system with a permanent database. It contains all information about individual patients. Only in rare cases, the CIS serves as a holistic information system in which all integrated systems and components are from one single manufacturer. Usually, one finds software from different providers [58]. Even if networking only within a single institution is intended, the support requirements for such heterogeneous software environments are high, both initially and long-term. If data handling and communication standards vary significantly among software, a separate server might be necessary to translate third-party applications.

First and foremost, all systems involved should use the same interface standards and support the same data structure for documents to enable fast, error-free, and seamless communication [59]. Product providers and system administrators should also look at clinical workflows to efficiently implement optimal software. Because overall, the success of clinical information systems depends on how easily and quickly physicians can use information technology [59, 60].

Those systems also serve as an electronic medical record (EMR). An EMR is the local digital storage of patient data and often delivers the required data for EHR. A wide range of solutions and products for EMR exist [61]. Waegemann C. P. [61] describes an EMR as follows: "The electronic patient [medical] record is a fully functional electronic record for a patient. It is created and managed by healthcare institutions. Physicians and nurses use this record interactively as a standard tool, which has partially replaced the earlier paper-based patient record. Images or multimedia data are also part of this record." [61]. Since the EMR is the local digital storage of patient data, it often delivers the required data for the EHR. A wide range of solutions and products for EMR and many standards and workflows can be implemented [62]. The best-known examples for standards in EMR are Integrating the Healthcare Enterprise (IHE), Health Level (HL) 7, Fast Healthcare Interoperatbility Resources (FHIR), and Digital Imaging and Communication in Medicine (DICOM) for communication in a hospital information system. EMR is not uniform and requires individual adaptation to the standards mentioned above [63, 64]. However, the implementation of a cross-institutional solution is challenging. Most EMR has in common that they are different and heterogeneous because the EMR is a locally limited and locally defined solution with other characteristics. If an EMR is introduced, it must be clarified how it is developed in detail and the local requirements [65]. The requirements regulation is by national initiatives or International Health Enterprise (IHE) Affinity Domains and the increasingly prominent smartphone-driven solutions of companies [66].

2.3 *Blockchain in health information systems*

Application fields of blockchain for health purposes are manifolded. Well-known are networks of anamnesis, diagnostics, and therapy by cooperative sharing of unalterable, reliable patient data. Other areas in medicine, such as research and development, billing, and insurance, can also be effectively integrated within blockchain [6, 67-70]. Using blockchain, anonymized patient data can be made available to the research community to develop Big Data cases [71, 72]. Simultaneously, the therapies and medication results can be fed back to the treating physicians and the pharmaceutical industry [73]. Physicians and hospitals can seamlessly pass on their findings and therapies to pharmacies, therapists, and aftercare institutions. Laboratory findings can be digitally integrated before, during, and after treatment and thus quickly be made available to all relevant entities [74]. A further area of application is telemedicine. Here doctors are consulted online via the app or computer [75]. That can include the initial visit in minor cases, specialists in anamnesis, diagnosis, therapy, subsequent follow-up care, and physiotherapeutic treatment. Blockchain-enabled telemedicine also plays a crucial role during the persistent pandemic of COVID-19. [76] claims that blockchain can significantly improve patient health data analysis and transmission referred to as the so-called "Internet of Medical Things" data for diagnosis and medication. Even rehabilitation on distance and quarantine might benefit from blockchain implementation since it facilitates treatment recommendations between the different health professionals and patients [76].

However, it has to be considered that healthcare data belongs to personal data in a non-private environment and contains compassionate information about a person (patient). Thus, there is an absolute necessity to keep health data appropriately confidential and to protect it against non-agreed publication, dissemination, disclosure, storage, or use [37, 77-79]. Furthermore, the EU also covered personal data processing by the General Data Protection Regulation (GDPR).

The reputational and financial loss of having sensitive data leaked can be severe and has the potential to ruin

companies and institutions and harm the patient [80]. The consequences are immense, but ensuring the necessary security proves to be a complicated task. According to [81], ensuring EMR/EHR ecosystems' safety and the underlying systems and components that form the ecosystem is crucial yet challenging due to the interplay and complexity between the systems and components. Therefore, securing this EMR/EHR ecosystem has been an active research area for companies and healthcare organizations [14].

From the presented literature and beyond, we found that the EHR requires secure data storage and sharing functionalities which can be answered with the application of Blockchain. Beyond this, Blockchain allows tracing who accessed patient data and enabled a secure access control. A more detailed application description of Blockchain for the named EHR requirements is visible in Table 1.

Table 1. Application areas of blockchain for EHR purposes

EHR Requirements	Blockchain application
Storing health data [39, 80, 82, 83]	With its distribution network and consensus mechanism, the Blockchain allows for a secure decentralized storing option for the massive volume of sensitive HER
Sharing health data [10, 15, 84-92]	Both the health providers and especially the patients can easily access health data from any facility in a Blockchain-based system. That ensures control for the patient and fast passing-on data for optimal care
Audit logging of health data [93-97]	For audit logging, the Blockchain provides a record of all historical data of access and changes to an EHR, which can be very useful for later occurring issues with the health data content and monitor who entered a patient's EHR
Managing the identity of health data accessors [98-103]	Following the requirement of privacy of health data, Blockchain permits access to EHR only to identified authorized entities by identification mechanisms

Blockchain can be considered a relatively young technology whose capacities have not yet been fully explored and transferred into practice [98]. Given this positive correlation between EHR requirements and Blockchain capabilities, the threats it poses to sensitive patient data require further investigation that leads to the following research question:

Which threats do blockchain implementation pose to the EMR/EHR as part of Health Information Systems?

3. Methodological approach

To gain insights on the stated research question, the researchers have decided to adopt a qualitative approach based on interviews. Before the research interview, personal data was collected. That includes the full name, residency, and job description, but private data were not included in the transcript to ensure total privacy to every respondent. When conducting a semistructured interview, some predefined guiding questions are necessary. According to [104], an interview starts with a vast topic and then narrows the topic and questions down. By following this scheme, the authors developed a semistructured interview guideline. After the interviews, a transcription was conducted using the tool QCAmap, which is available for free online (https://www.qcamap.org/ui/home). This tool can also support the content analysis following the approach of [105].

To be able to conduct high-quality research, the authors take actions to enhance data validity and reliability. As previously described, this research will use qualitative data collected during focus interviews, analyzed using the qualitative content analysis, as published by [105]. Additionally, the ideas of intercoder reliability have been implemented.

The interview guiding questions were formulated around the integrity threats on blockchain systems, namely accuracy, completeness, timeliness, and validity or authorization (Example questions: In which situations a private blockchain may deliver inaccurate or wrong data? How can data on a private blockchain be incomplete? Under what circumstances a private blockchain would deliver outdated information? How can data stored in a private blockchain be invalid or not authorized?). The first interview partners were recruited based on the professional network of the authors. After conducting these interviews successfully, snowball sampling was used to find more appropriate candidates. After

six interviews, saturation was reached, and no additional interviews were conducted for this particular purpose. The participant's data was anonymized and can be described as follows: (I1) Professor, USA, (I2) Blockchain Developer, Singapore, (I3) Professor, Austria, (I4) Blockchain Advisor, USA, (I5) IT-Consultant, Germany, (I6) Founder of a blockchain startup, Austria.

4. Findings

In this section, the interviews' results are shortly presented before being further discussed in the following section. In total, six participants were interviewed, with an average interview duration of 42 minutes for every interview. Multiple threats/risks that blockchain poses to data integrity could be identified in the interviews. The findings are visible in Table 2. The first column represents the category ID, the second column the title of the category. The absolute frequency indicates the number of marked passages in the data for each category. A category can be mentioned more than once during an interview. Therefore the total frequency in some cases is higher than the number of conducted interviews. The absolute frequency is only used to indicate how often a particular category is in the data set, but there are no results based on this variable.

Table 2. Identified threats to data integrity in blockchain systems

Category	Category title	Absolute frequency
D1	Consensus attack (51% attack)	4
D2	Low-quality smart contract code	3
D3	Alternative chain	4
D4	Misuse of private key	3
D5	Incorrect data input	5
D6	A blockchain contains historical data	2
D7	Node is malicious/out of sync	8
D8	Data on the blockchain cannot be deleted	2
D9	No central authority	2
D10	Trust in protocol developers	6
D11	Trust in third parties	3

5. Discussion

This chapter will discuss/explain the elaborated threats on using blockchain technology in more detail and show the same possible implications connected to the Emergency Medical Service (EMS)/EHR usage.

5.1 *D1: Consensus attack (51% attack)*

This risk is already widely-known among blockchain experts. Despite its name, it is unnecessary to control 51% of the mining power to conduct this attack successfully. According to [42], this attack is possible when controlling about 30% of the total mining power. When entities control the majority of the mining power, they can publish wrong blocks containing inaccurate data, which threatens the integrity of the data on the blockchain. This risk has also been identified by [5].

In the context of digital patient data storage, medical professionals would lose the patient's health background information that could lead to unfair treatment or no treatment at all.

5.2 *D2: Poor contract code*

The low quality of contract code is often not considered, just like the repercussions that lousy code can have on users and ecosystems. In contrast to the private systems, in public systems where anybody can deploy Smart Contracts, it cannot be ruled out that some poorly written code exists. There are several sources of error; for example, the code could contain syntax or spelling errors. Smart Contracts are automatically executed contracts when a condition is met and have if-then rules [106, 107]. Another possibility would be the missing implementation of error handling and producing an invalid result on the blockchains (I6). A significant example of poorly written smart contract code is the Decentralized Autonomous Organization (DAO) incident, which happened in 2016. Poorly written contract code threatens the correctness, completeness, and validity of the blockchain's data. A similar risk has also been identified by [5].

5.3 *D3: Alternative chain*

It is possible that there is a fork on the blockchain, and more than one chain is existing that can have several reasons. The first possibility is that somebody wants to change to protocol and challenge the original chain. That already happened several times to bitcoin, where people forked it to bitcoin unlimited or bitcoin XT. The most recent and successful for bitcoin is Bitcoin Cash, which was forked at block #478559 on August 1st, 2017. Such forks always threaten the blockchain's ecosystem and can mislead new users because they don't know which chain is the "real" one. Another scenario of an alternative chain is an inadvertent fork of the blockchain. That can happen if two miners find a new block of the chain simultaneously and propagate it to the network (I1). Most of the time, this threat only exists for a short time because if another block is found, the longer chain (which has more PoW done) is the valid chain (I6). However, the block with no child block can lead to issues, such as transferring coins. A lot of institutions (for example, cryptocurrency exchanges) require more than one confirmation on transactions (depending on the value of the transaction) [42]. That is not possible on the bitcoin network when a block does not have a direct successor. An alternative chain is a risk to the correctness and completeness of the data stored on the blockchain. In the EHR context, treatment data may be lost, or important information may be missing.

5.4 *D4: Misuse of private key*

In blockchain systems, users rely on PVI (Public vital infrastructures) to generate their public and private keys. Besides financial transactions, blockchains are also used for identity management within projects like Civic. Misuse can lead to loss of monetary funds and identity theft, and much more (I6, I1). When an individual is misusing a private key, the data's integrity is reduced because of the risk of authorization and validation.

5.5 *D5: Incorrect data input*

When storing data into a database, there are often rules on how and what data to hold; however it is possible in most systems that wrong data can be stored in the database, even though there are mechanisms to prevent it. When using blockchain systems, such mechanisms are often missing, and therefore there is an increased chance of storing incorrect data in the blockchain (I2). A blockchain is, under normal circumstances, an immutable data store. Therefore it is not possible to remove data that is incorrect (I3). On the bitcoin blockchain, before a transaction gets confirmed, it is checked against several rules. This process prevents publishing inaccurate data on the blockchain network. On some blockchains, it is possible to include profanities. For example, in bitcoin, these data are stored in the coinbase part of a block. Several marriage proposals on the bitcoin blockchain are not relevant for bitcoin operating and can be considered inaccurate data (https://blockchair.com/bitcoin/block/416236).

5.6 *D6: A blockchain contains historical data*

Data on blockchain nowadays is transactional data of cryptocurrencies. If there is no updated transaction, the data on the blockchain is outdated. Because there is all the historical data stored in the blockchain, an older state of the information is seen as the most current one (I2). For every update of a value, a transaction has to be approved. The historical data threatens the timeliness of the data and therefore reduces the degree of achieved data integrity.

5.7 *D7: Malicious node*

When using a blockchain, most users don't run their full nodes to participate in the network. Most of them run software to access the blockchain on a node, saving a lot of computing and storage. Blockchains are mostly designed to be trustless, but when connected to a node, the user trusts somebody. This node can, of course, act maliciously. For example, the node could not be synchronized to the rest of the blockchain networks. Therefore you could see an outdated version of the blockchain (I1). That threatens the timeliness of data and reduces the degree of achieved data integrity. As described by [42], block propagation is not real-time because there is a physical limitation in network transmission. Another possibility is that the node provides the user that is connected to a fake blockchain. That can only happen in combination with a malicious wallet (I3, I6). In this case, the correctness and completeness of the data are being compromised.

5.8 *D8: Data on the blockchain cannot be deleted*

As aforementioned, a blockchain contains the whole history of the data on the blockchain. Therefore, once something is stored in a blockchain, it is almost impossible to revoke it. In most cases, this is an advantage for blockchain technology (when thinking of financial transactions). If data is stored in the chain that should, later on, be deleted from the chain, it is a high effort for the owner and publisher. For example, if confidential data from a government is published in a public blockchain, this data is visible as long as the blockchain network exists (I3). Data that cannot be deleted constitutes a risk to the validity and accuracy of the stored data. That is especially also valid for patient data. Patients become transparent to anyone who can access the Blockchain. There might be cured diseases that might still impact insurance rates. Furthermore, patients might simply keep their medical history to themselves.

5.9 *D9: No central authority*

A blockchain has a decentralized organization/politics, so a single entity cannot be made responsible for processing or fulfilling a transaction. When conducting a bitcoin transaction, senders will type the receiving address most of the time and then send bitcoin. An address in the bitcoin ecosystem is 27 to 34 characters long and includes a mixture of letters and numbers. If a typo happened, the transaction is sent anyway, and the chances are high that the funds are lost. There is no authority to call or contact to undo the transaction and send the funds back (I4). This pattern also applies to errors in the system (in the blockchain protocol), where there is often no central authority that can decide on how to fix a particular problem. And if there were such a powerful authority, the next risk, "Trust in Protocol Developers," would have to be considered. When no central authority approves transactions, data, or executed contracts on the blockchain, the data's validity, authorization, and correctness are threatened.

5.10 *D10: Trust in protocol developers*

A lot of blockchain projects are struggling with decentralized governance (I6). The protocol developers maintaining the code have a lot of power in the ecosystem. In some cases, those figureheads and coders of leading projects can make the organization act in their interest (I4). For example, in 2016, after the DAO hack, the Ethereum team decided to fork the blockchain to restore the stolen funds to its users. While this may sound good, people argue that it breaks the basic tenets of a public blockchain [108]. When looking at the bitcoin protocol developers, only a handful of them contribute to code regularly and therefore have a lot of power in the ecosystem (https://github.com/bitcoin/bitcoin/graphs/contributors). Other blockchain projects try to tackle this problem by setting up a more decentralized governance and development structure consisting of known parties (https://www.cardano.org/en/home/).

5.11 *D11: Trust in other third parties*

Bitcoin was designed as a peer-2-peer payment system. However, nowadays, this is not always the case especially in the world of cryptocurrencies, most people use exchanges like Bitfinex for buying and selling coins. Therefore, a lot of people rely on those third parties when making transactions (I4). A lot of organizations are already aware of that, and decentralized exchanges are emerging. Another problem with cryptocurrency exchanges is the key management. All

centralized exchanges do not give access to the private key of an account. Therefore, a user has to trust the exchange that they are not signing any authorized transactions without their knowledge (I6). Exchanges can threaten the data's authorization and validity on the blockchain/transaction by misusing their users' keys. Wallets can be published by various vendors and are not always from the same organization as the blockchain itself [42]. Therefore, there are also trust in the developer of the third-party wallet is needed. A fraudulent wallet threatens the correctness and completeness of the data on the blockchain.

6. Conclusion

Overall, 11 risks or threats to data integrity on blockchain systems were identified. Only a private blockchain seems appropriate for EMR/EHR implementation to apply blockchain technology, not only based on the threats which need to be overcome. To avoid incorrect data and therefore threaten a blockchain's integrity, the design of the applications based on the blockchain is crucial. For example, mechanisms to check data before storing it permanently can improve the data quality. To prevent flawed nodes, a user should make sure the nodes they connect to are trustworthy. As a node operation, it is essential to keep no node synchronized, which can be better achieved by reducing network delays and having security measures against DDoS attacks. A missing central authority can threaten the integrity of data on a blockchain because of the disappeared supervision. To reduce this risk, the individuals or organizations responsible for the blockchain must achieve a well-balanced governance model that is decentralized but maintains the quality of a centralized authority. Preventing the abuse of the system by powerful parties such as protocol developers is difficult.

Table 3 builds on Table 1 and Table 2, combining EHR requirements with identified Blockchain threats. It displays the constraints of Blockchain for the application for EHR purposes.

Table 3. Blockchain threats concerning EHR requirements

EHR Requirements	Blockchain threats
Storing health data	Storage might be at risk of attack (D1), Storage is permanent, leading to wrong data entries being unreversible (D5, D8) and potentially outdated data (D6), treatments might be affected by incorrect data or incomplete data (D2, D7, D10)
Sharing health data	Timeliness of data is threatened by old data entries (D6), Trust in Developers (D10), and other third parties (D11) is required
Audit logging of health data	Poor contract code (D2), Malicious nodes (D7), or wicket protocols (D10) prevent correct audit logging of health data, duplicated health data due to alternative chains prevents keeping the audit log history (D3)
Managing the identity of health data accessors	Misuse of private key threatens the correct identification of accessors (D4), the absence of a central authority might impact the rightful access of EHR (D9), trust in third parties is required (D11)

Given the constraints of Blockchain in EHR, it still is a very considerable technology. It can fulfill the EHR requirements. Thereby, blockchain allows to keep track of each individual's medical treatments, distributes data to relevant and authorized parties, and stores the audit log.

Overall, most threats arise from incorrect or incomplete data leading to insufficient data integrity. Moreover, it should be considered that blockchain comes with the disadvantage of high computational power requirements and scalability constraints.

However, we consider blockchain for EHR purposes as very useful, despite having to keep in mind the risks it comes with.

7. Limitations

This research comprises only six interviews. Although the number of newly identified risks declined with every

interview, it cannot be ruled out that a higher number of high qualified participants would increase the number of identified threats. Also, some of the participant's native language is not English. Hence, it cannot be ruled out that some parts of the answers or questions were understood wrong. The data has been analyzed with the content analysis framework by Mayring. The use of a different analysis method may lead to different results. Besides, the authors utilized the online tool QCAmap for content analysis. The authors worked as conscientiously, precisely, and objectively as possible.

Lastly, it is to mention that current eHealth systems are probably equally exposed to cyber attacks as other systems. This research did not comprise a comparison to these systems. To fully evaluate whether to apply blockchain for eHealth, this evaluation should be made.

Conflict of interest

The authors declare that they have no competing interest.

Reference

[1] Tanenbaum AS, van Steen M. *Distributed Systems: Principles and Paradigms*. 2nd ed. NJ, U.S.: Prentice-Hall, Inc.; 2016.

[2] Buterin V. *The Meaning of Decentralization*. Medium.com. 2017. Available from: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 [Accessed 13th April 2021].

[3] Wang H, Ma S, Dai HN, Imran M, Wang T. Blockchain-based data privacy management with Nudge theory in open banking. *Future Generation Computer Systems*. 2020; 110: 812-823. Available from: doi: 10.1016/j.future.2019.09.010.

[4] Osmani M, El-Haddadeh R, Hindi N, Janssen M, Weerakkody V. Blockchain for next generation services in banking and finance: cost, benefit, risk and opportunity analysis. *Journal of Enterprise Information Management*. 2020. Available from: doi: 10.1108/JEIM-02-2020-0044.

[5] Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. *Future Generation Computer Systems*. 2020; 107: 841-853. Available from: doi: 10.1016/j.future.2017.08.020.

[6] Shi S, He D, Li L, Kumar N, Khan MK, Choo KKR. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers and Security*. 2020; 97: 101966. Available from: doi: 10.1016/j.cose.2020.101966.

[7] Palomo-Zurdo RJ. Blockchain: The decentralization of power and its application in defense. *Bie3: Boletín IEEE*. 2018. Available from: http://www.ieee.es/publicaciones-new/documentos-de-opinion/2018/DIEEEO70-2018.html [Accessed 13th April 2021].

[8] Chen J, Micali S. *Algorand*. Cornell University; 2017. Available from: https://arxiv.org/abs/1607.01341

[9] Brennen JS, Kreiss D. *Digitalization*. Hoboken, NJ: John Wiley & Sons, Inc.; 2016. Available from: doi: 10.1002/9781118766804.wbiect111.

[10] Rouhani S, Butterworth L, Simmons AD, Humphery DG, Deters R. MediChain TM: A Secure Decentralized Medical Data Asset Management System. 2018. Available from: doi: 10.1109/Cybermatics_2018.2018.00258.

[11] European Commission. Commission Staff Working Document accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digita. 2018. Available from: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-enabling-digital-transformation-health-and-care-digital-single-market [Accessed 13th April 2021].

[12] Kobusinge G. Putting interoperability on health-information-systems' implementation agenda. *Proceedings of the 53rd Hawaii International Conference on System Sciences*. 2020. Available from: doi: 10.24251/HICSS.2020.443.

[13] Winter A, Haux R, Ammenwerth E, Brigl B, Hellrung N, Jahn F. *Health Information Systems*. London: Springer; 2011. Available from: doi: 10.1007/978-1-84996-441-8.

[14] Puppala M, He T, Yu X, Chen S, Ogunti R, Wong STC. Data security and privacy management in healthcare applications and clinical data warehouse environment. *2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)*. USA: Las Vegas, NV; 2016. p.5-8. Available from: doi: 10.1109/BHI.2016.7455821.

[15] Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and trustable electronic medical records sharing using blockchain. *AMIA Annual Symposium Proceedings*. 2018; 2017: 650-659.
[16] An S, Xiao C, Stewart WF, Sun J. Longitudinal adversarial attack on electronic health records data. *WWW '19: The Web Conference San Francisco CA USA May, 2019*. 2019. p. 2558-2564. Available from: doi: 10.1145/3308558.3313528.
[17] Kuhn KA, Giuse DA. From hospital information systems to health information systems. *Methods of Information in Medicine*. 2001; 40(4). Available from: doi: 10.1055/s-0038-1634170.
[18] Fettke P. State-of-the-Art des State-of-the-Art. *Eine Untersuchung der Forschungsmethode "Review" innerhalb der Wirtschaftsinformatik*. 2006; 48(4): 257. Available from: doi: 10.1007/s11576-006-0057-3.
[19] Crawford CC, Boyd CC, Jonas WB. Systematic reviews in practice. Samueli Institute, Alexandria, VA. 2015.
[20] Peters GW, Panayi E. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. *New Economic Windows*. 2016; 239-278. Available from: doi: 10.1007/978-3-319-42448-4_13.
[21] Underwood S. Blockchain beyond bitcoin. *Communications of the ACM.* 2016; 59(11). Available from: doi: 10.1145/2994581.
[22] Brancaccio E, Giammetti R, Lopreite M, Puliga M. Centralization of capital and financial crisis: A global network analysis of corporate control. *Structural Change and Economic Dynamics*. 2018. Available from: doi: 10.1016/j.strueco.2018.03.001.
[23] Witzig P, Salomon V. Cutting out the middleman: A case study of blockchain technology induced reconfigurations in the Swiss financial services industry. 2019. Available from: doi: 10.4337/9781788115131.00008.
[24] Möser M. Anonymity of bitcoin transactions: An analysis of mixing services. *Münster Bitcoin Conference*. 2013.
[25] Houben R, Snyers A. Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. 2018.
[26] H. Hui et al. Survey on blockchain for internet of things. *Journal of Internet Services and Information Security*. 2019; 9(2): 1-30.
[27] Risius M, Spohrer K. A blockchain research framework: What we (don't) know, where we go from here, and how we will get there. *Business & Information Systems Engineering.* 2017; 59(6): 385-409. Available from: doi: 10.1007/s12599-017-0506-0.
[28] Xu X, et al. A Taxonomy of blockchain-based systems for architecture design. *2017 IEEE International Conference on Software Architecture (ICSA)*. Gothenburg, Sweden; 2017. p. 243-252. Available from: doi: 10.1109/ICSA.2017.33.
[29] Dinh TTA, Liu R, Zhang M, Chen G, Ooi BC, Wang J. Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering.* 2018. p. 1366-1385. Available from: doi: 10.1109/TKDE.2017.2781227.
[30] Ahram T, Sargolzaei A, Sargolzaei S, Daniels J, Amaba B. Blockchain technology innovations. *2017 IEEE Technology & Engineering Management Conference (TEMSCON)*. 2017. Available from: doi: 10.1109/TEMSCON.2017.7998367.
[31] Swan M. *Blockchain: Blueprint for a New Economy*. 1st ed. Beijing: O'Reilly; 2015.
[32] Hepp T, Wortner P, Schönhals A, Gipp B. Securing Physical Assets on the Blockchain. *CryBlock' 18: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*. Switzerland: Zug; 2018. p. 60-65. Available from: doi: 10.1145/3211933.3211944.
[33] Carminati B, Rondanini C, Ferrari E. Confidential business process execution on blockchain. *2018 IEEE International Conference on Web Services (ICWS)*. USA: San Francisco, CA; 2018. p. 58-65. Available from: doi: 10.1109/ICWS.2018.00015.
[34] Wust K, Gervais A. Do you need a blockchain? *Crypto Valley Conference on Blockchain Technology (CVCBT)*. 2018. p. 45-54. Available from: doi: 10.1109/CVCBT.2018.00011.
[35] Banque de France. The dangers associated with the development of virtual currencies: the example of bitcoin. *Focus*. 2013; 10(5): 1-6.
[36] Hao Y, Li Y, Dong X, Fang L, Chen P. Performance analysis of consensus algorithm in private blockchain. *2018 IEEE Intelligent Vehicles Symposium (IV)*. China: Changshu; 2018. p. 280-285. Available from: doi: 10.1109/IVS.2018.8500557.
[37] European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da. *Official Journal of the European Union*. 2016; L119.
[38] Herian R. Regulating disruption: Blockchain, GDPR, and questions of data sovereignty. *Journal of Internet Law*. 2018; 22(2): 1-16.

[39] Zheng Z, Xie S, Dai HN, Chen X, Wang H. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services.* 2018; 14(4): 352-375. Available from: doi: 10.1504/IJWGS.2018.095647.
[40] Liu Q, Li K. Decentration transaction method based on blockchain technology. *2018 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*. China: Xiamen; 2018. p. 416-419. Available from: doi: 10.1109/ICITBS.2018.00111.
[41] Horizen Academy. *Technology*. 2019. Available from: https://academy.horizen.io/technology/ [Accessed 13th April 2021].
[42] Antonopoulos AM. *Mastering Bitcoin*. Sebastopol, CA: O'Reilly Media; 2015.
[43] Houy N. It will cost you nothing to "kill" a proof-of-stake crypto-currency. *SSRN Electronic Journal*. 2014. Available from: doi: 10.2139/ssrn.2393940.
[44] Weber I, et al. On availability for blockchain-based systems. *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*. 2017. p. 64-73, Available from: doi: 10.1109/SRDS.2017.15.
[45] Gaetani E, Aniello L, Baldoni R, Lombardi F, Margheri A, Sassone V. Blockchain-based database to ensure data integrity in cloud computing environments. *Italian Conference on Cybersecurity*. 2017.
[46] Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. *Future Generation Computer Systems.* 2020; 107: 841-853. Available from: doi: 10.1016/j.future.2017.08.020.
[47] Lapão LV. The future of healthcare: The impact of digitalization on healthcare services performance. *Studies Health Technology Informatics*. 2016; 228: 675-679. Available from: doi: 10.1007/978-3-319-99289-1_22.
[48] Lokshina I, Lanting C. A qualitative evaluation of IoT-Driven eHealth: Knowledge management, business models and opportunities, deployment and evolution. *Data-Centric Business and Applications*. 2019; 20: 23-52. Available from: doi: 10.1007/978-3-319-94117-2_2.
[49] Farahani B, Firouzi F, Chang V, Badaroglu M, Constant N, Mankodiya K. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems*. 2018; 78(2): 659-676. Available from: doi: 10.1016/j.future.2017.04.036.
[50] Srivastava S, Pant M, Abraham A, Agrawal N. The technological growth in eHealth services. *Computational and Mathematical Methods in Medicine*. 2015; 894171. Available from: doi: 10.1155/2015/894171.
[51] Ahern DK, Kreslake JM, Phalen JM. What is eHealth (6): perspectives on the evolution of eHealth research. *Journal of Medical Internet Research*. 2006; 8(1): e4. Available from: doi: 10.2196/jmir.8.1.e4.
[52] Boogerd EA, Arts T, Engelen LJ, van de Belt TH. What Is eHealth: Time for An Update? *JMIR Research Protocols*. 2015; 4(1): e29. Available from: doi: 10.2196/resprot.4065.
[53] Della Mea V. What is e-health (2): the death of telemedicine? *Journal of Medical Internet Research*. 2001; 3(2): e22. Available from: doi: 10.2196/jmir.3.2.e22.
[54] Eysenbach G. What is e-health? *Journal of Medical Internet Research*. 2001; 3(2): e20. Available from: doi: 10.2196/jmir.3.2.e20.
[55] Oh H, Rizo C, Enkin M, Jadad A. What is eHealth (3): a systematic review of published definitions. *Journal of Medical Internet Research*. 2005; 7(1): e1. Available from: doi: 10.2196/jmir.7.1.e1.
[56] Pagliari C, et al. What is eHealth (4): a scoping exercise to map the field. *Journal of Medical Internet Research*. 2005; 7(1): e9. Available from: doi: 10.2196/jmir.7.1.e9.
[57] Fischer F, Krämer A. *eHealth in Deutschland: Anforderungen und Potenziale Innovativer Versorgungsstrukturen*. Berlin and Heidelberg: Springer Verlag; 2016. Available from: doi: 10.1007/978-3-662-49504-9.
[58] Snyder KD, Paulson P. Healthcare information systems: analysis of healthcare software. *Hospital Topics*. 2002; 80(4): 5-12. Available from: doi: 10.1080/00185860209598004.
[59] Kramme R. *Informationsmanagement und Kommunikation in der Medizin*. Berlin: Springer; 2017. Available from: doi: 10.1007/978-3-662-48778-5.
[60] Tu SW, et al. Modeling guidelines for integration into clinical workflow. *Studies in Health Technology and Informatics*. 2004; 107(Pt 1): 174-178.
[61] Waegemann CP. An electronic health record for the real world. *Healthcare Informatics: The Business Magazine for Information and Communication Systems*. 2001; 18(5): 55-60.
[62] Mon DT. Defining the differences between the CPR, EMR, and EHR. *Journal of AHIMA*. 2004; 75(9): 74-75, 77.
[63] Hong N, et al. Integrating structured and unstructured EHR data using an FHIR-based type system: A case study with medication data. *AMIA Summits on Translational Science Proceedings*. 2018; 2017: 74-83.
[64] Ratib O, Swiernik M, McCoy JM. From PACS to integrated EMR. *Computerized Medical Imaging and Graphics*. 2003; 27(2-3): 207-215. Available from: doi: 10.1016/S0895-6111(02)00075-7.
[65] Keshavjee K, et al. Best practices in EMR implementation: A systematic review. *AMIA Annual Symposium Proceedings*. 2006; 2006: 982.

[66] Dogac A, Laleci GB, Aden T, Eichelberg M. Enhancing IHE XDS for federated clinical affinity domain support. *IEEE transactions on information technology in biomedicine: A publication of the IEEE Engineering in Medicine and Biology Society*. 2007; 11(2): 213-221. Available from: doi: 10.1109/titb.2006.874928.
[67] Akkaoui R, Hei X, Cheng W. EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange. *IEEE Access*. 2020. p. 113467-113486. Available from: doi: 10.1109/ACCESS.2020.3003575.
[68] Girardi F, de Gennaro G, Colizzi L, Convertini N. Improving the healthcare effectiveness: The possible role of EHR, IoMT and blockchain. *Electronics*. 2020; 9(6): 884. Available from: doi: 10.3390/electronics9060884.
[69] Murugan A, Chechare T, Muruganantham B, Kumar SG. Healthcare information exchange using blockchain technology. *International Journal of Electrical and Computer Engineering.* 2020; 10(1): 421-426. Available from: doi: 10.11591/ijece.v10i1.pp421-426.
[70] Patil RM, Kulkarni R. Universal storage and analytical framework of health records using blockchain data from wearable data devices. *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*. India: Bangalore; 2020. p. 311-317. Available from: doi: 10.1109/ICIMIA48430.2020.9074909.
[71] Dwivedi AD, Srivastava G, Dhar S, Singh R. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors (Basel, Switzerland)*. 2019; 19(2): 326. Available from: doi: 10.3390/s19020326.
[72] Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A. Blockchain in healthcare and health sciences-A scoping review. *International Journal of Medical Informatics*. 2020; 134: 104040. Available from: doi: 10.1016/j.ijmedinf.2019.104040.
[73] Ullah HS, Aslam S, Arjomand N. Blockchain in healthcare and medicine: A contemporary research of applications, challenges, and future perspectives. *Arxiv*. [Preprint] 2020. Available from: https://arxiv.org/abs/2004.06795 [Accessed 13th April 2021].
[74] Dubovitskaya A, Novotny P, Xu Z, Wang F. Applications of blockchain technology for data-sharing in oncology: Results from a systematic literature review. *Oncology*. 2020; 98(6). Available from: doi: 10.1159/000504325.
[75] Ichikawa D, Kashiyama M, Ueno T. Tamper-resistant mobile health using blockchain technology. *JMIR Mhealth and Uhealth*. 2017; 5(7): e111. Available from: doi: 10.2196/mhealth.7938.
[76] Dai HN, Imran M, Haider N. Blockchain-enabled internet of medical things to combat COVID-19. *IEEE Internet of Things Magazine*. 2020. p. 52-57.
[77] Commission of the European Communities. Communication from the commission: On a European programme for critical infrastructure protection. 2006.
[78] Council of the European Union. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal of the European Union*. 2008; L345: 75-82.
[79] Kupwade Patil H, Seshadri R. Big data security and privacy issues in healthcare. *2014 IEEE International Congress on Big Data*. USA: Anchorage, AK; 2014. p. 762-765. Available from: doi: 10.1109/BigData.Congress.2014.112.
[80] Al Omar A, Rahman MS, Basu A, Kiyomoto S. MediBchain: A blockchain based privacy preserving platform for healthcare data. *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*. 2017. p. 534-543. Available from: doi: 10.1007/978-3-319-72395-2_49.
[81] Esposito C, de Santis A, Tortora G, Chang H, Choo KKR. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput. (IEEE Cloud Computing)*. 2018. p. 31-37. Available from: doi: 10.1109/MCC.2018.011791712.
[82] Liu J, Li X, Ye L, Zhang H, Du X, Guizani M. BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. *GLOBECOM 2018-2018 IEEE Global Communications Conference*. 2018. Available from: doi: 10.1109/GLOCOM.2018.8647713.
[83] Zhao H, Zhang Y, Peng Y, Xu R. Lightweight backup and efficient recovery scheme for health blockchain keys. *2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)*. Bangkok, Thailand; 2017. p. 229-234. Available from: doi: 10.1109/ISADS.2017.22.
[84] Tariq F, Khan ZA, Sultana T, Rehman M, Shahzad Q, Javaid N. Leveraging fine-grained access control in blockchain-based healthcare system. 2020; 1151. Available from: doi: 10.1007/978-3-030-44041-1_10.
[85] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for secure EHRs sharing of mobile cloud based e-health systems. *IEEE Access*. 2019. p. 66792-66806. Available from: doi: 10.1109/ACCESS.2019.2917555.
[86] Kim MG, Lee AR, Kwon HJ, Kim JW, Kim IK. Sharing medical questionnaries based on blockchain. *2018 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*. Spain: Madrid; 2018. p. 2767-2769. Available from: doi: 10.1109/BIBM.2018.8621154.
[87] Seol K, Kim YG, Lee E, Seo YD, Baik DK. Privacy-preserving attribute-based access control model for XML-based electronic health record system. *IEEE Access*. 2018. p. 9114-9128. Available from: doi: 10.1109/

ACCESS.2018.2800288.
[88] Wang S, Zhang Y, Zhang Y. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *IEEE Access*. 2018. p. 38437-38450. Available from: doi: 10.1109/ACCESS.2018.2851611.
[89] Roehrs A, Da Costa CA, Da Righi RR, Rigo SJ, Wichman MH. Toward a model for personal health record interoperability. *IEEE Journal of Biomedical and Health Informatics*. 2019; 23(2): 867-873. Available from: doi: 10.1109/JBHI.2018.2836138.
[90] Rifi N, Rachkidi E, Agoulmine N, Taher NC. Towards using blockchain technology for eHealth data access management. *2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME)*. Beirut, Lebanon; 2017. p. 1-4. Available from: doi: 10.1109/ICABME.2017.8167555.
[91] Jabbar R, Fetais N, Krichen M, Barkaoui K. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. 2020. Available from: doi: 10.1109/ICIoT48696.2020.9089570.
[92] Dubovitskaya A, et al. ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. *Journal of Medical Internet Research*. 2020; 22(8): e13598. Available from: doi: 10.2196/13598.
[93] Benchoufi M, Ravaud P. Blockchain technology for improving clinical research quality. *Trials*. 2017; 18(1): 335. Available from: doi: 10.1186/s13063-017-2035-z.
[94] Castaldo L, Cinque V. Blockchain-based logging for the cross-border exchange of eHealth data in Europe. *Security in Computer and Information Sciences*. 2018; 821: 46-56. Available from: doi: 10.1007/978-3-319-95189-8_5.
[95] Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*. 2017. p. 14757-14767. Available from: doi: 10.1109/ACCESS.2017.2730843.
[96] Kushch S, Ranise S, Sciarretta G. Blockchain Tree for eHealth. 2019. Available from: doi: 10.1109/GCIoT47977.2019.9058412.
[97] Angraal S, Krumholz HM, Schulz WL. Blockchain Technology: Applications in healthcare. *Circulation: Cardiovascular Quality and Outcomes*. 2017; 10(9): e003800.
[98] Kuo TT, Kim HE, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association.* 2017; 24(6): 1211-1220. Available from: doi: 10.1093/jamia/ocx068.
[99] Houtan B, Hafid AS, Makrakis D. A survey on blockchain-based self-sovereign patient identity in healthcare. *IEEE Access*. 2020. p. 90478-90494. Available from: doi: 10.1109/ACCESS.2020.2994090.
[100]Hardjono T, Pentland A. Verifiable Anonymous Identities and Access Control in Permissioned Blockchains. *Arxiv.* [Preprint] 2019. Available from: https://arxiv.org/abs/1903.04584 [Accessed 13th April 2021].
[101]Guo H, Li W, Nejad M, Shen CC. Access control for electronic health records with hybrid blockchain-edge architecture. *2019 IEEE International Conference on Blockchain (Blockchain)*. USA: Atlanta, GA; 2019. p. 44-51. Available from: doi: 10.1109/Blockchain.2019.00015.
[102]Fan K, Wang S, Ren Y, Li H, Yang Y. MedBlock: Efficient and secure medical data sharing via blockchain. *Journal of Medical Systems*. 2018; 42(8): 136. Available from: doi: 10.1007/s10916-018-0993-7.
[103]Mikula T, Jacobsen RH. Identity and access management with blockchain in electronic healthcare records. *2018 21st Euromicro Conference on Digital System Design (DSD)*. Prague, Czech Republic; 2018. p. 699-706. Available from: doi: 10.1109/DSD.2018.00008.
[104]Gillham B. *Research Interview*. London: Continuum International Pub. Group; 2001.
[105]Mayring P. Qualitative content analysis. *Forum Qualitative Social Research*. 2000; 1(2). Available from: doi: 10.17169/fqs-1.2.1089.
[106]Buterin V. *Ethereum Whitepaper*. 2013. Available from: https://ethereum.org/en/whitepaper/ [Accessed 13th April 2021].
[107]Buterin V. A Next-Generation Smart Contract and Decentralized Application Platform. 2015. Available from: https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [Accessed 13th April 2021].
[108]Falkon S. The Story of the DAO-Its History and Consequences. 2017. Available from: https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee.