Blockchain storage solution for Healthcare and Insurance

March 2023

Authors

Alex Weber

Data Management

Bozidar Puljic

Operations

Grégoire Prétat

Management

Kanoj Kanna

BD/CRM

Laura Corrado

Operations

Liam Tessendorf

Website

SMART CONTRACTS LAB

Abstract

The storage of healthcare data is essential for many stakeholders in the healthcare industry, such as hospitals, patients, and insurance companies. However, the past Corona pandemic has shown delays and inefficiencies due to the patients' data storage difficulties. Furthermore, various cyberattacks have shown that the current storage solutions bear potential security risks. This paper attempts to demonstrate to insurance companies and healthcare providers the possibilities and advantages of blockchain-based storage solutions for Electronic Health Records, how blockchain can solve existing problems, and the explicit advantages and disadvantages. The focus is on the possible applications for insurance companies and their advantages in this segment. Furthermore, this paper provides an in-depth exploration of blockchain-based solutions for enhancing EHR storage, as proposed by several researchers. The majority of these solutions utilize a blockchain in combination with the Inter Planetary File System (IPFS), which is the focus of this paper. Given the sensitivity of EHR data, privacy and security are crucial considerations when sharing such information. As a result, this paper examines the requirements for an effective and secure EHR storage system.

Table of Contents

Table of Figures

1. Introduction

In recent years academia and industry have been exploring potential applications for blockchain technology (McGhin et al., 2019). According to a paper published by Yang et al. (2019), the healthcare industry, and more specifically the management of electronic health records, is an area with great potential.

The healthcare industry faces many challenges, one of them being the fragmentation of health records. A patient usually visits multiple healthcare providers during his lifetime, leading to snapshots of his health saved at various locations (Cerchione et al., 2023). Furthermore, security has been a big concern recently, as numerous healthcare institutions were victims of cyber-attacks (Kumar et al., 2021). As patients' data contains confidential information, the storage of data in healthcare has unique requirements regarding privacy and security. With its inherent features, such as immutability and decentralization, blockchain technology could meet the requirements and help overcome the challenges (McGhin et al., 2019). The use of blockchain technology would not only transform the healthcare industry but also impact insurance companies significantly.

Many papers provide a blockchain-based solution for healthcare data management. Only few of them consider insurance companies. Additionally, most literature targets researchers and professionals with a technical background. We aim to close this gap by providing an understandable overview of the possibilities for insurance companies and healthcare providers as well as a starting point for curious readers who want to use our contribution for future research. Therefore we analyzed recent papers, especially other literature reviews on blockchain-based solutions for EHRs, and investigated whether blockchain technology can solve the current problems in the healthcare domain for storing and sharing EHR data. A healthcare storage solution should be able to store large amounts of data, protect sensitive data, and ensure secure and efficient data sharing. It is in the interest of insurance companies that these requirements are complied with.

Taking previous research into consideration, we examine whether a blockchain-based solution for the storage of healthcare data can improve the status quo and what the specific benefits for insurance companies and healthcare providers are. Additionally, we aim to explain what properties a blockchain-based solution needs for a successful implementation. Abbreviated from the research questions, we hypothesize the following:

- **H_1:** A blockchain-based solution meets the requirements for the storage of sensitive healthcare data.
- **H_2:** A blockchain-based storage solution poses several benefits for insurance companies.

The following section introduces healthcare data storage solutions currently in use and their associated problems. Section 3 provides a brief introduction to the technical aspects of blockchain technology. In section 4 we explore how this novel technology can be implemented for the storage of EHR and discuss the most critical factors of a solution. We then present a use case in which the interaction between the insurance, doctor, and patient is illustrated in a comprehensible way. In section 5 we propose the benefits this approach poses specifically for insurance companies, followed by the problems that could generally arise from using a blockchain-based storage solution and the use case. Section 7 introduces further research. Lastly, we explain the methods we used and present our conclusion.

2. Current state of healthcare data management

According to the paper of S. Lee (2020), there is an abundance of health information available, and healthcare providers face challenges in accessing this information quickly and in a helpful way. The researcher claims this is partly due to the fragmentation of healthcare systems, which may lead to classified information that is not easily shared between healthcare providers and organizations. S. Lee (2020) also mentions that there is a lack of standardization in the procedure in which health data is collected and stored, which might result in difficulties comparing data across different organizations. The solution to these problems presented in the paper of S. Lee (2020) is digital transformation. The author highlights the importance of replacing paper-based systems for healthcare information with digital solutions, such as the storage of the digitalized pieces of information on cloud systems which enable healthcare providers to improve information flow, automate processes, and make the overall workflow more efficient. According to the writer, this will lead to better patient care, improved outcomes, and reduced costs.

The healthcare industry has experienced a significant impact from the COVID-19 pandemic, as reported by Faction (2020). There has been a shift towards data-driven technologies that allow for remote care and virtual consultations, increasing the amount of data generated and stored by healthcare organizations. By utilizing advanced data storage systems, healthcare organizations are exploring innovative solutions to manage the influx of data. These systems reduce costs, improve accessibility to valuable insights, and optimize the potential of data management to enhance overall healthcare quality and improve patient outcomes (Faction, 2021).

2.1 Current healthcare data storage solutions

The three common ways of storing healthcare data are on-premises storage, public cloud storage, and hybrid cloud storage (Faction, 2021). On-premises storage involves storing data on physical servers on the healthcare provider's site, giving healthcare organizations full control over the data storage environment but this first solution is costly and faces scaling issues. In contrast, the public cloud is maintained by a third-party cloud provider, and data is saved on remote servers, which can be accessed through the internet (Redhat, 2022). According to the author, the second solution is very interesting due to its scalability and cost efficiency. However, the loss of control of the data as well as privacy are important concerns.

Between the on-premises and the cloud solution, there is a hybrid cloud storage solution, a combination of an on-premises and a cloud storage solution (Microsoft, n.d.). As mentioned in the same article, this system stores a part of the data on the provider's on-premises servers, whilst the non-sensitive data are stored on a third-party cloud provider's remote server which improves scalability (Redhat, 2022).

Furthermore, healthcare data can be divided into categories, e.g., patient/disease registries, and electronic health records (EHRs). The latter includes a patient's medical history and test results (Faction, 2021). Among these types of data, the ones we will focus on in this paper are EHRs, as they are comprehensive summaries of the patient's health status & medical histories (Faction, 2021). According to the paper of Dash et al. (2019), this is the main advantage of this data type because it can also include records of past diagnoses, prescribed medications, known allergies, demographic information, clinical notes, and results of laboratory tests.

With this abundance of information, healthcare professionals are better equipped to make informed decisions regarding patient care and treatment, positively impacting patient outcomes (Dash et al., 2019).

2.2 Problems of current healthcare data storage solutions

According to Filatov (2020), there may be a problem with storing or receiving a large amount of healthcare data because privacy and regulatory implications would partially prevent storing this kind of data in the cloud or make it available to outstanding parties. Furthermore, storing the same data on-premises would require significant compliance and security efforts and may be followed by shortcomings in informatics and administration resources, which could potentially result in less accessibility of data (Filatov, 2020). Regarding the paper of Kumar et al. (2021), current storage solutions face numerous threats. According to them, if some healthcare data is saved locally, there is a problem that it might be lost or corrupted, because there exists no backup. Another area for improvement may exist in the misplacement or integration of data that would result in severe consequences (Kumar et al., 2021).

Other threats mentioned in the paper of Kumar et al. (2021) are cyberattacks. The data may be blocked through Distributed Denial of Service (DDoS) attacks, lost by ransomware, uncovered with phishing attacks, and leaked by other data providers (Kumar et al., 2021). There are some terms to be defined to get a better understanding:

1. DDoS attack is a cyberattack in which infected computers overload a system or network with traffic so that it becomes congested and unavailable (Dong et al., 2019).
2. Ransomware is malicious malware that encrypts data of targeted hard drives and is often followed by a demand for ransom to decrypt the data (O'Kane et al., 2018).
3. Phishing is a network attack in which the attacker sets up a fake version of an existing website to trick an online user into revealing personal data (Gupta et al., 2017).

By looking at the USA, according to Starks and Beard (2022), one of the largest non-profit hospital chains called CommonSpirit Health, was presumably attacked by ransomware, which harmed 140 clinics and 1000 care sites scattered around the country.

Some of the consequences were the rerouting of ambulances, the adjustment of patient schedules, and the suspension of IT systems which may contain EHRs. According to the survey of the Ponemon Institute (2022), in which 641 IT and IT safety professionals from the healthcare sector participated, the top six cybersecurity concerns ordered by their importance are insecure medical devices, ransomware, insecure mobile apps, employee negligence or error, cloud compromises and BEC/spoof phishing. Additionally, 89% of the participants in the research group indicated that they suffered cyberattacks in the last year.

By referring to Lindner (2017), hacking hospitals has become increasingly sophisticated, which is a threat to the clinics and patients in Switzerland. The journalist interviewed the security manager of Hint AG and concluded that nursing homes with 50 employees and hospitals with over 4000 employees could be attacked. How many hacks have been conducted on Swiss hospitals can only be guessed, according to the journalist, because reporting such incidents to the public could result in loss of image and imitation of attack. Additionally, there is a problem that the Center for Information Assurance, called Melani, only keeps track of cyber-attacks that are reported voluntarily (Lindner, 2017). Nevertheless, Mäder (2020) writes about a public example in Switzerland that occurred on July 21st, 2020 at the private hospital chain Hirslanden Group, where attackers accessed the central servers via malware in an email attachment. According to the journalist, it is unknown why the attackers encrypted only administrative data and not medical patient data. However, with backup copies to recover encrypted data, the incident lasted about six days, and patient care was not at risk (Mäder, 2020).

In another interview, Lindner (2017) got in touch with Urs Albert Meyer, a former senior pharmacologist at the Biozentrum of the University of Basel, and concluded that the interconnection of data and system might drive modernization and efficiency but also that every communication channel is a potential access point and this is likely to make the system more vulnerable (Lindner, 2017).

3. Technical background knowledge

3.1 Blockchain technology

Blockchain technology is built on a chain of secure record blocks connected using advanced cryptography. Kumar et al. (2021) state that each block contains the previous block's cryptographic hash, timestamp, and transaction data. The blockchain serves as a digital public ledger for storing transactions that can be publicly verified. It is a decentralized database that is maintained by the nodes in the network. Each block records a set of transactions in a data structure where each newly generated one is added to the blockchain, which causes the size of the blockchain to increase continuously (Kumar et al., 2021).

Kumar et al. (2021) highlight that individuals can join a blockchain network by adding a node, and every node has an identical copy of the public ledger. This paper specified that participants of the blockchain network could transfer coins or tokens to one another, which is recorded in a blockchain block.

The blockchain is then updated to every node in the network and is immutable. To authenticate users, digital signatures are used, and all blocks in the blockchain are logically linked to each other using a particular data structure (Kumar et al., 2021).

When one party initiates a transaction, Kumar et al. (2021) underline that the hash of the previous block, timestamp, public key of the receiver party, and the digital signature of the sender party's node is stored in the block and then permanently written to the blockchain. The blockchain software manages the entire transaction, and only digital signatures are used for identification and authentication, which ensures complete anonymity for the real-life identity of the parties involved (Kumar et al., 2021).

One of the key advantages of using blockchain is its robust security features, including transactional integrity, robust authentication mechanisms, and the immutability of stored data (Kumar et al., 2021). The study also highlights that the blockchain is highly reliable and resistant to failures due to its decentralized structure, which enables direct peer-to-peer transactions, eliminating the need for third-party exchanges or intermediaries and the associated fees.

3.2 Cryptographic hash functions

According to Srivastava et al. (2019), the security of the blockchain's data depends on the blockchain's cryptographic properties, particularly the hash reference that links the blocks together. The same paper highlights that understanding hashing is essential to understand blockchain technology. This paper specified that hashing is performed using a mathematical cryptographic hash function that takes any size of data as input and produces a fixed-size output called a hash value. An essential property of the hash function is that a marginal change in the input will result in a completely different hash value in the output (Srivastava et al., 2019).

Hashing an entire block in the blockchain follows the same principle as hashing any other input. However, suppose someone has the hash value of a file or block. In that case, it is challenging to determine the input of the hash function due to its non-invertible property highlighted in the paper of Srivastava et al. (2019).

To guess the input based on the hash value alone, a brute force attack must be performed, which involves trying all possible combinations of inputs, which can be an incredibly time-consuming and computationally intensive process (Srivastava et al., 2019).

4. Blockchain-based EHR solutions

Blockchain technology could provide a new model for health information exchange by making EHRs more efficient and secure. Any proposed blockchain-based architecture should support the storage of medical data and should follow the user throughout his life (Mayer et al., 2020). EHRs contain important, private, and sensitive patient information that must be constantly protected and available. In a recent study of a systematic review of different blockchain solutions in the health domain, Mamun et al. (2022) claim that the four main factors to ensure a successful implementation of a blockchain-based EHR solution are scalability, privacy, security, and accessibility.

Many solutions using blockchain technology are currently being researched, and it is too early to say which one will be implemented (Kumar et al., 2021).

Nonetheless, numerous solutions are being built around the usage of the InterPlanetary File System (IPFS), which is a system that enables storing data in a decentralized manner. Nine out of the ten solutions analyzed by Kumar et al. (2021) were built around IPFS. For this reason, we will dive deeper into the technology behind IPFS and how storing medical data would work using this novel technology when combined with blockchain technology. This section provides a summary of possible implementations of blockchain-based EHR solutions and the different technical details insurance companies and collaborating parties would have to focus on, as illustrated in Figure 1.

4.1 Blockchain types

In the solutions presented in different literature, a blockchain is usually the central component of the proposed architecture for storing EHRs (Kumar et al., 2021; Mayer et al., 2020). The blockchain can be responsible for storage, authorization, fault tolerance, and disaster recovery. Blockchain technologies can be divided into three types: public, consortium, and private. Insurances and collaborating parties must decide on which type of blockchain they want to implement their EHR solution (Mayer et al., 2020).

4.1.1 Public Blockchains

Anyone can check and verify data transactions and participate in reaching a consensus. A user's identity address is generated using a pseudo-anonymous hash value, meaning one cannot know exactly who the address belongs to (Mamun et al., 2022).

Public blockchains typically offer financial incentives to participate in the network, which is why there are some interaction costs (e.g., transaction fees). So, whenever someone wants to upload or download a document such as EHRs, they would be charged for it (Mamun et al., 2022). Examples of public blockchains are Bitcoin and Ethereum.

4.1.2 Private Blockchains

Not everyone can participate in the blockchain, and nodes are restricted. Only invited participants can join the network, making the network distributed but centralized (Mamun et al., 2022). Mamun et al. (2022) state that private blockchains are usually used within one company or organization for supply chain management, electronic voting, digital asset management, and data preservation. According to Mamun et al. (2022), private blockchains consume less power than public blockchains and are faster in adding blocks to the chain. However, the cost of licensing, running, and maintaining a private blockchain may be higher than the cost of interacting with a public blockchain (Mayer et al., 2020).

4.1.3 Consortium Blockchains

The data in the blockchain can be open or private, and the network is considered to be partly decentralized (Mayer et al., 2020). Similarly, to a private blockchain, a consortium blockchain can only be accessed by registered participants. A consortium blockchain is not used by a single organization but is distributed over several organizations.

This means that a single organization cannot undertake any illegal activity, as without the consent of the other network participants, one cannot perform any operation (Mamun et al., 2022).

4.2 Factors for a successful implementation of a blockchain-based EHR solution

4.2.1 Scalability limitations of blockchains

The chain structure of blockchains helps support the ever-growing medical records by maintaining a continuously growing linked list of medical records. However, storing all healthcare data on the blockchain itself would result in an enormous blockchain, which would be far too large for a node to download, store and validate. Additionally, this would result in very high costs, depending on the blockchain being used (Ober, 2018). A solution to this is to store the actual data off-chain by using a system like IPFS and to have pointers to the off-chain data. In this way, the hash of the data can be stored on the blockchain, but the actual data is stored off-chain. The hash is cryptographically guaranteed to be unique to the content. When combining this with blockchain technology, it is possible to timestamp the data in a way that prevents data tampering.

IPFS, as proposed by Benet (2014), is a peer-to-peer system that enables storing and accessing files, websites, applications, and data. The three fundamental principles of IPFS are:

1. unique identification via content addressing
2. content linking via directed acyclic graphs (DAGs)
3. content discovery via distributed hash tables (DHTs)

The paper of Benet (2014) highlights that in contrast to finding content on the internet by where the file is stored, IPFS uses content addressing to identify content by what is in the file.

Every piece of content that uses the IPFS protocol has a unique content identifier (CID) which is the hash of the data contained in the file. To ensure that systems are interoperable, IPFS leverages the Interplanetary Linked Data (IPLD) project. IPLD translates between hash-linked data structures, allowing data unification across distributed systems (Benet, 2014).

Benet (2014) also mentions that in IPFS, DAGs are used to link content together. IPFS uses a data structure called Merkle DAGs, where each node has a unique identifier, a hash of the node's content. A Merkle DAG is a DAG where each node has an identifier resulting from hashing the node's contents using a cryptographic hash function like SHA256 (Benet, 2014). This means that Merkle DAGs can only be constructed by starting at the leaves (from nodes without children) and proceeding up the DAG (Benet, 2014). Furthermore, any node in a Merkle DAG is immutable, so any change in any of the nodes would result in a different DAG.

To construct a Merkle DAG representing some content, IPFS often splits it into blocks. According to Benet (2014), this has the benefit that different parts of the file can come from different sources. Also, this means that each block has its own CID. Furthermore, splitting the file into different blocks allows sharing parts of a Merkle DAG if you have two similar files. E.g., if you update a website, only updated files receive new content addresses, and the rest can still refer to the same blocks for everything else (Benet, 2014).

To find content, IPFS uses a distributed hash table (DHT). A hash table is a database of keys to values, which makes it distributed when the hash table is split across all the peers in a distributed network. The libp2p project provides the DHT and handles peers connecting and talking to each other (Benet, 2014). Once the desired content is found, one must connect to it and get it. To request and send blocks to other peers, IPFS uses a module called Bitswap. Bitswap allows you to send a "wantlist" of all desired blocks and have your peers send you the requested blocks. One can verify the blocks by hashing their content and comparing the resulting CIDs to the CIDs you requested (Benet, 2014).

All in all, IPFS is an excellent addition to blockchain technology when storing large amounts of data, such as EHRs. Whereas blockchain technology is excellent at timestamping data, it is not meant to store large amounts of data. IPFS, on the other hand, is good at storing data in a tamper-proof way, but there is no way of proving when the data was added to the IPFS network. Combining these two technologies results in an excellent solution for storing EHRs.

4.2.2 Privacy

According to Mamun et al. (2022), blockchain-based systems' privacy is the primary concern. Mamun et al. (2022) reviewed many papers that presented blockchain solutions in the health domain and found three properties to ensure privacy, including pseudo-anonymity, smart contracts, and audit trails. First, the blockchain provides pseudo-anonymity, which means that the user (patient) has no visible identifier that can be directly linked to his identity. Another privacy mechanism is smart contracts. Smart contracts are blockchain-stored programs that are executed when certain conditions are met. For example, as described by Mamun et al. (2022), the patient can decide who has access to his EHRs and who is restricted from interacting with the EHRs.

Another essential tool that can be used to monitor the usage of EHRs is an audit trail (Mamun et al., 2022). It gives a chronological record of all the actions done on the EHRs.

4.2.3 Security

When considering a blockchain-based solution for sharing EHR, the second most important aspect is security, as Mamun et al. (2022) claimed. It can be divided into three sub-categories: confidentiality, integrity, and availability (Mamun et al., 2022). Blockchain maintains confidentiality, meaning that only authorized parties get access to the data using cryptographic tools that encrypt data. Marangappanavar and Kiran (2020) described a possible way of using a cryptographic method: if a party other than the owner (patient) wants to have access to the EHRs of a patient, they have to give the patient their public key. Then, the data owner can grant access by adding the address of the requester to the record (Marangappanavar & Kiran, 2020). Integrity means the data is accurate, consistent, and complete (Mamun et al., 2022). Blockchains use hash functions to ensure integrity, which is explained in section 3.1. Besides that, a blockchain is a distributed ledger. Hence there is an extremely minimal possibility of information loss. At the same time, it must be ensured that the services are accessible whenever the customer requires them. This task is challenging, and failing to complete it could have significant consequences (Mamun et al., 2022).

4.2.4 Accessibility

Furthermore, a blockchain-based solution must ensure that the EHRs are accessible securely and efficiently. Mamun et al. (2022) identified three primary characteristics of proper accessibility: access control, authorization, and platform independence. With access control, the patient can define who gets access to his EHR and what access is granted (Sookhak et al., 2021). This is important, as not every party should be able to read the whole EHR of an individual.

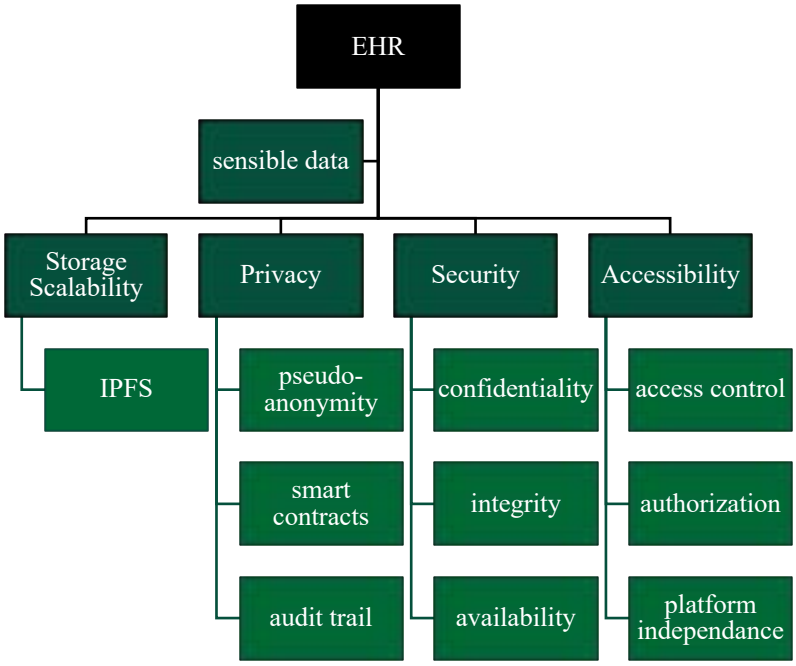

Figure 1: Four main factors for a successful implementation of a healthcare storage solution

For instance, an insurance company will not have the same access rights as a doctor. The authorization process is another critical step to prevent misuse by malicious users. Often this process is solved by cryptographic methods. Additionally, the system used for the usage, storage, and sharing of EHRs should run on all platforms (Mamun et al., 2022). The goal is to make it as user-friendly as possible.

4.3 Use Case: Process of storing and sharing EHRs

The illustration in Figure 2 gives a brief overview of how patients, doctors, and insurance can interact with each other. Of course, there are different blockchain solutions, but the process is essentially the same. Here is an example: The insurance demands a medical report before paying out a claim to a patient. The patient goes to his doctor for a medical report. The medical report is submitted to the blockchain by the doctor, who already has the right to upload and examine documents. This is recorded as a transaction, which generates a hash. Through the hash, the insurance can check the medical report, if they have the corresponding access rights. Therefore, access needs to be authorized by the patient, which can be solved with cryptographic tools. If the insurance approves the medical report for the claim, it can transfer the compensation to the patient. This can also be executed efficiently in the form of a smart contract.

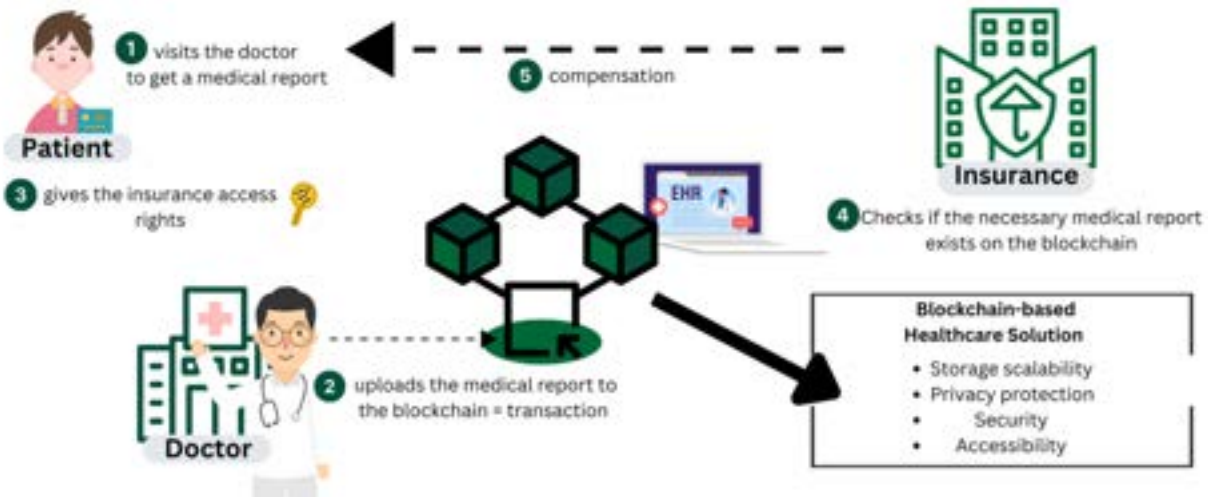

Figure 2: Use case about the medical record and insurance claim

5. Potential benefits for Insurance Companies

The healthcare industry is characterized by many interconnections, requiring collaboration among numerous parties, as shown in Figure 3 (Sravan et al., 2018). Because patients' health records contain private information, data storage in the health industry must meet further requirements regarding security and privacy. As further health information can easily be obtained through smart devices, medical procedures are increasing, and patients are seeing multiple doctors, the amount of data is continuously growing (McGhin et al., 2019). Furthermore, this leads to multiple fragmented records of the same patient located at different institutions (Cerchione et al., 2023). Using blockchain technology to create a distributed EHR system, can help meet the specific requirements of the healthcare industry (McGhin et al., 2019). In the following, potential benefits for insurance companies are presented.

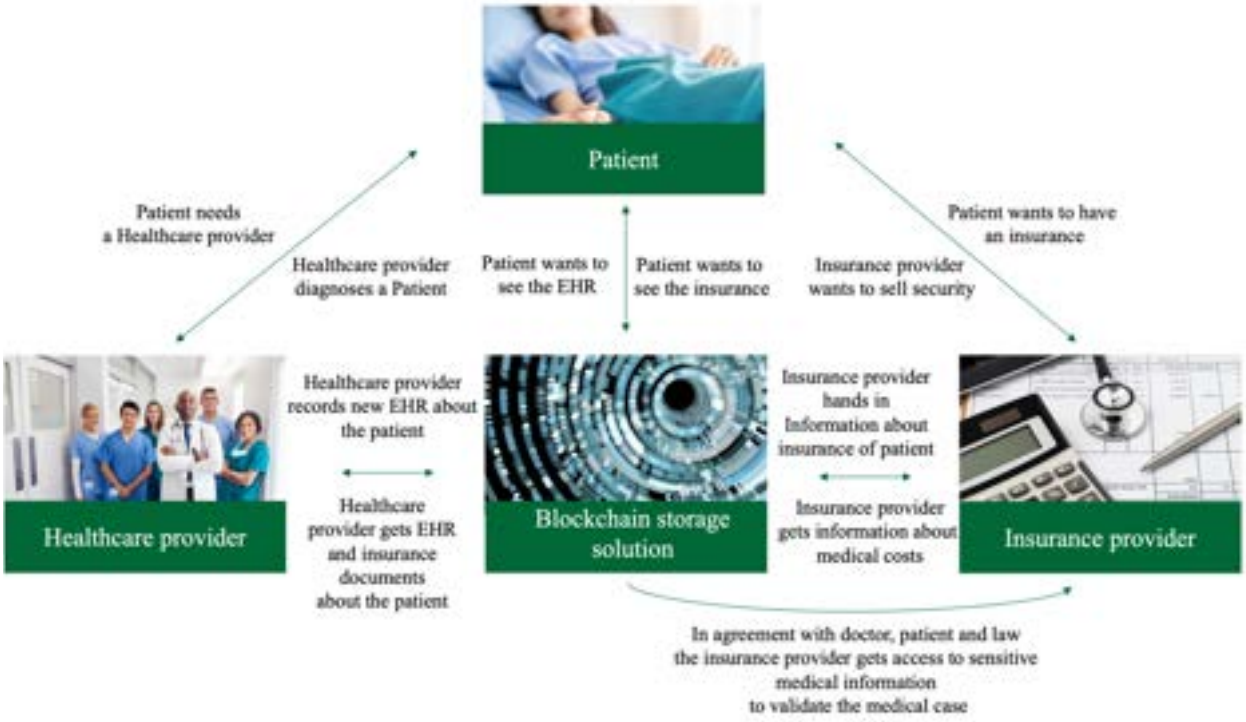

Figure 3: Interconnectivity between patient, healthcare provider, and insurance provider

5.1 Interoperability

As previously mentioned, fragmented health records from one patient stored at various health institutions is a problem the healthcare industry faces nowadays (Cerchione et al., 2023). By using blockchain technology to store EHR on a distributed database, interoperability between different systems and the integrity of healthcare records can be significantly improved (Yang et al., 2019).

The following scenario described by Tanwar et al. (2020) further shows how blockchain can help solve the problem of fragmented health records: A patient arrives at a clinic and is evaluated in the accident and emergency department.

To get a better picture of the patient's medical history and previous treatment, the clinician has to obtain previous records from the patient's primary care provider. As the patient might have seen different specialists in the past, the clinician again has to obtain health records by sending requests to the specialists' offices. It then can take several days to receive the data, which is often incomplete. With a blockchain registry storing the patient's data, the clinician could quickly identify if the patient was seen at other clinics or had already received treatment for the same condition. Having all the data readily available would allow for a better understanding of the patient's overall health, reduce duplication and avoid unnecessary examinations. Hence, using blockchain could result in time and cost savings, improved efficiency, and better healthcare for the patient (Tanwar et al., 2020).

5.2 Security

During the COVID-19 outbreak in 2020, multiple healthcare institutions were the victims of cyber-attacks. This put patients' sensitive medical data at risk and made institutions inoperable and unable to provide patients with healthcare (Kumar et al., 2021). The data loss ultimately affects healthcare insurance providers too, as they depend on health records for correct claims management. By using blockchain technology to store EHR and thus eliminating the risk of a centralized server, hacking becomes nearly impossible (Golda Careline S & Godhavari, 2022).

5.3 Transparency

As one of the key features of blockchain technology is immutability, records cannot be modified, making information on it secure and trusted (Tanwar et al., 2020). According to Khezr et al. (2019), the blockchain would allow for health records to be time-stamped and therefore make sure that no one can tamper with them. This could significantly improve fraud detection processes for insurance companies (Mendoza-Tello et al., 2021).

Additionally, improved transparency through access to a shared ledger would facilitate the communication between a patient and the insurance company regarding treatment costs and medications (Dubovitskaya et al., 2017). This could benefit insurance companies by improving patient satisfaction and making processes more efficient.

5.4 Cost savings & efficiency

The decentralized storage of transactions allows blockchain to reduce costs and improve efficiency significantly (Zheng et al., 2018). The increase in efficiency through the solution of interoperability is intuitive. Consider the time saved during a visit to the doctor. On the one hand, decentralized storage solutions between the patient and the healthcare provider allow the doctor to access the historical medical records and act more quickly without having to use the patient's central storage system (McGhin et al., 2019). Furthermore, access to a patient's health records is crucial to correctly prescribe medications and treatments (Tanwar et al., 2020). According to Golda Careline S and Godavari (2022), a single master patient file reduces the chances of medical errors and mismatches. Hence, better accessibility to data will lead to more effective healthcare, which further helps in reducing costs for health insurance companies.

On the other hand, the storage of documents becomes obsolete for the patient. Documents such as vaccination cards or health insurance policies can be retrieved directly by any health institution, wherever they are located. This can be particularly useful in international interactions between healthcare providers.

The time saved in processing a patient reduces investigation and treatment costs, and thus both parties benefit, the patient and the health facility, as well as third parties such as the according insurance companies involved. Decentralized storage eliminates the need for the respective intermediaries of insurance companies and the health institutions responsible for transferring the information (Kuo et Al., 2017). In addition, the institutions save themselves the maintenance and backup of their own servers, which is usually associated with high IT costs. The reduced personnel and IT expenditures alone play a significant role in the advantages of blockchain solutions for EHRs. Furthermore, according to a McKinsey & Company report (2017), insurers can achieve cost savings of 20% by investing in digital transformation, as well as a significant increase in income growth and customer service.

6. Challenges of using blockchain technology for healthcare data managemen

This section focuses on possible problems when implementing a blockchain-based EHR solution.

6.1 Technical Challenges

According to Kumar et al. (2021), the main technical challenges of implementing a blockchain-based EHR storage solution are how to handle the registration of different entities to participate in the distributed network (if the blockchain is of the type private or consortium) and how to manage access rights in emergency scenarios. Furthermore, a critical challenge will be to make a fully decentralized system and not only decentralized storage (e.g., by using IPFS but at the same time, one entity controls all the blockchain nodes) (Kumar et al., 2021).

6.2 Legal challenges

When implementing a solution using blockchain technology, a significant challenge must be addressed: data ownership. Although we believe that patients should have the right to control their data, there is a wide gap in legislation around the world regarding health data ownership. According to Liddell et al. (2021), in the case of Western European countries, some cases in France and Germany suggest that information may be treated as personal property. However, there is no widespread recognition of this concept by the European General Data Protection Regulation (GDPR). The same paper also mentions another case in Australia where healthcare data is not considered property. Liddell et al. (2021) also highlight the contrasting situation in the US, where confidential information is recognized as property and can be transferred to others. In contrast, some states consider medical or genetic information as the patient's or individual's property. The law which covers these issues is the Health Insurance Portability and Accountability Act (HIPAA).

Even so, individuals in the UK and the US are likely to have property rights over their information if it falls under the intellectual property or trades secret law, underlines the same paper. Recent legal cases have indicated that courts are generally only willing to recognize this information as property if it is protected by intellectual property or contractual agreements (Liddell et al., 2021).

6.3 Challenge in Standardization and Regulation

According to Siyal et al. (2019), standardization by international authorities could facilitate information sharing and support preventive safety measures. However, they also note that the development stage of blockchain technology presents a challenge for establishing standards in this area.

As presented in our use case, the patient can authorize a third party to access his information by a smart contract. Han et al. (2022) mentioned that it is important to have regulations regarding smart contracts because of the potential distrust of doctors, patients, and healthcare providers in blockchain technology. They suggest that it may come from a fear of incorrect entry and usage of private information. Therefore, regulations could help to overcome this challenge.

6.4 Social challenges

Shahnaz et al. (2019) focused on the issue of understanding blockchain technology, as they noted that it is a technology that is still not widely comprehended by many individuals. Siyal et al. (2019) state that changing to a new technology is challenging. They emphasize that this is especially true for the health sector, as it may not be adopting digitalization fast enough and this would make it more difficult to implement blockchain technology. This information indicates that healthcare organizations would face a time-consuming period of transformation from the available EHR system to a whole other system (Shahnaz et al., 2019). It is also mentioned that given the recent investment in electronic health records, eliminating the current record systems would not be in the best interest of patients and medicine (Pirtle & Ehrenfeld, 2018). With this information in mind, we believe that the shift towards adopting a blockchain storage solution may be slow.

6.5 Challenge in cost of implementation

According to a journal contribution by Golda Careline S. and Godhavari (2022), the cost could be a limiting factor in adopting a blockchain-based EHR system. They mention that a more significant part of the expense may be due to the hardware and software needed to accomplish the implementation. Another costly disadvantage that the authors mention is that the implementation could disrupt the work process and temporarily reduce productivity. It is stressed by the authors that these costs are temporary and that the efficiency and revenue gains of the benefits may outweigh the expenses. We agree with what the authors suggest because we also see the potential benefits of the technology. However, there may not exist a specific national or international EHR storage solution yet, so the cost of implementation is currently difficult to quantify.

7. Further Research

The assessment of the risk of its customers is one of the biggest challenges for insurance companies (NAIC, 2020).

When it comes to pricing insurance plans, there is an asymmetric distribution of information between the insurance company and the client. This principal-agent relationship has two consequences: adverse selection and moral hazard. The first concerns the correct selection of policyholders from the insurance company's point of view.

Moral hazard, on the other hand, describes policyholders' behavior change due to incentives arising from the contract (Shi et al., 2016). Finally, the paper highlights that insurance companies can screen more efficiently with a blockchain solution to store EHR.

This could be negotiated with the customer through a customized insurance policy (e.g., the insurance company could calculate a premium for the customer based on their historical demand for healthcare provisions) (Shi et al., 2016). Similar offers from insurance companies are already known. For example, customers are offered an application to track their sports activities. In this case, the sporting activity has a positive influence on the customer's pricing of the contract. It should be noted, however, that there is a risk of excluding people or putting them at a disadvantage by setting up customized contracts penalizing. Thus, the blockchain solution to store EHR represents an essential risk of abuse for insurers resulting from discriminatory contracts or other price manipulations based. Further research could be based on smart contracts that address this exclusion problem and the misuse of customers' healthcare data in general.

Furthermore, the world of blockchain-stored EHRs opens many more useful investigations for institutions in the healthcare industry. For example, following Holly et al. (1998), the likelihood of at least one inpatient stay is increased if the client's supplemental insurance plan previously used medical treatments. For example, research such as that in the Holly et al. paper could be used to predict hospital occupancy rates and thus avoid overloaded intensive care units (ICU) as we have experienced during the COVID-19 pandemic in many countries.

Blockchain-based data storage has significant potential for improving processes, particularly in specific sub-areas of the healthcare sector, such as pharmacy, dentistry, and optometry (Azaria et al., 2016). For example, blockchain technology could enable pharmacies to communicate better with each other and improve control over the demand for drugs. Using smart contracts could optimize the process of transferring information and money between pharmacies, insurance companies, and their customers. Dentists could use patient data to monitor the behavior and offer better service. In contrast, opticians could use blockchain-based storage to access customer data in a decentralized manner without requiring customers to remember their measurements. Often, this personal information is recorded in a physical document or backed up locally by the respective parties, which would become obsolete with blockchain technology.

Despite the numerous potential benefits and exciting research ideas, McGhin et al. (2019) highlight the importance of further education in these areas to create a robust ecosystem for a better patient-centered data empowerment age. Moreover, as blockchain technology is not without problems, there are still clear security challenges that must be addressed.

8. Methodology

For this report we mainly used a review method to find existing literature related to implementing blockchain technology for the storage of EHR. Relevant papers were searched using Scopus, Swisscovery, SpringerLink, IEEE Xplore, Wiley Online Library, SAI, Google Scholar, Genios, and MDPI. Additionally, we used websites to find relevant articles on current developments.

Furthermore, there are various types of healthcare data. We decided to concentrate on EHRs, as they play a vital role in the exchange of information between healthcare providers and insurance companies and are the primary focus of most research papers on this topic.

In our research process, we found out that there are hundreds of blockchain solutions for healthcare storage. However, many of these solutions differed in a few properties. Fortunately, some systematic literature reviews on the papers proposed a blockchain system for EHR storage.

Our goal was not to find the best possible solution but to determine what essential properties the system should have. Therefore, we have given the characteristics using the systematic review's critical findings of Mamun et al. (2022). For better comprehension, we provided some examples to explain the implementation of blockchain solutions in healthcare.

9. Conclusion

All things considered, healthcare providers and insurance companies could increase the coordination capacity and security in sharing patient health information by using a blockchain-based solution. The disparity of healthcare systems and the lack of standardization in how data is collected and stored present significant challenges for healthcare providers in accessing health information efficiently. Digital transformation can improve information flow, automate processes, and make workflow more efficient, leading to better patient care, improved outcomes, and reduced costs. The features and characteristics of blockchain technology, when combined with IPFS, can provide a new model for health information exchange by making EHRs more efficient and secure.

As we have covered several benefits for insurance providers in section 5, our second hypothesis on the benefits for insurance companies cannot be rejected within this paper. Moreover, the requirements for the storage of sensitive healthcare data can be met if blockchain technology considers the four main factors we presented in section 4.2, which can be achieved with the tools we discussed. However, implementing such a system requires addressing challenges related to technical obstacles, current law, standardization as well as the cost of implementation. These challenges lead us to reject our first hypothesis.

Despite these issues, blockchain technology can help reduce duplication, avoid unnecessary examinations, improve efficiency, and facilitate communication between patients, insurance companies, and healthcare providers. In addition, implementing such a system could improve patient satisfaction and make processes more efficient. Overall, blockchain technology has the potential to disrupt the storage solutions of healthcare data and enables great research opportunities for the whole industry including several sub-areas of healthcare providers.

10. References

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. *2016 2nd International Conference on Open and Big Data (OBD).* https://doi.org/10.1109/obd.2016.11

Benet, J. (2014, July 14). *IPFS - Content Addressed, Versioned, P2P File System*. https://arxiv.org/pdf/1407.3561

Cerchione, R., Centobelli, P., Riccio, E., Abbate, S., & Oropallo, E. (2023). Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem. *Technovation*, *120*. https://doi.org/10.1016/j.technovation.2022.102480

Dash, S., Shakyawar, S. K., Sharma, M., & Kaushik, S. (2019). Big data in healthcare: management, analysis and future prospects. *Journal of Big Data, 6(1), 1–25.* https://doi.org/10.1186/S40537-019-0217-0/FIGURES/6

Dong, S., Abbas, K., & Jain, R. (2019). A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments. *IEEE Access*, *7*, 80813–80828. https://doi.org/10.1109/ACCESS.2019.2922196

Dubovitskaya, A., Xu, Z., Ryu, S., & Schumacher, M. (2017). Secure and Trustable Electronic Medical Records Sharing using Blockchain. *American Medical Informatics Association Annual Symposium*, *2017*, 650–659.

Faction. (2021, March 3). *Healthcare Data Storage Options: On-prem, Cloud Or Hybrid.* Factioninc.Com. https://www.factioninc.com/blog/hybrid-multi-cloud/healthcare-data-storage-options-on-prem-cloud-or-hybrid/

Filatov, T. (2020, February 25). *Distributed storage of permissioned access healthcare patient data using IPFS and blockchain*. Dappros. https://www.dappros.com/202002/distributed-storage-of-permissioned-access-healthcare-patient-data-using-ipfs-and-blockchain/

Golda Careline S, L., & Godhavari, T. (2022). Implementation of Electronic Health Record and Health Insurance Management System using Blockchain Technology. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *13*(6). https://doi.org/10.14569/IJACSA.2022.0130679

Gupta, S., Singhal, A., & Kapoor, A. (2017). A literature survey on social engineering attacks: Phishing attack. *Proceeding - IEEE International Conference on Computing, Commun ication and Automation, ICCCA 2016*, 537–540. https://doi.org/10.1109/CCAA.2016.-7813778

Han, Y., Zhang, Y., & Vermund, S. H. (2022). Blockchain Technology for Electronic Health Records. *International Journal of Environmental Research and Public Health*, 2022, 19(23), 15577. https://doi.org/10.3390/IJERPH192315577

Holly, A., Gardiol, L., Domenighetti, G., & Bisig, B. (1998). An econometric model of health care utilization and health insurance in Switzerland. *European Economic Review*, *42*(3–5), 513–522. https://doi.org/10.1016/S0014-2921(98)00003-8

Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. *Applied Sciences*, 9(9), 1736. https://doi.org/10.3390/app9091736

Kumar, S., Bharti, A. K., & Amin, R. (2021). Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions. *Security and Privacy*, *4*(5). https://doi.org/10.1002/spy2.162

Kuo, T., Kim, H., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association.* Doi: 10.1093/jamia/ocx06

Liddell, K., Simon, D., & Lucassen, A. (2021). Patient data ownership: who owns your health? *Journal of Law and the Biosciences*, *8*(2). https://doi.org/10.1093/jlb/lsab023

Lindner, M. (2017, February 5). *Hacker im Spital* [Hackers in the hospital]. *NZZ Am Sonntag*. https://nzz.genios.de/document/NZZS__201702050203653087/hitlist/10?all=

Mamun, A. A., Azam, S., & Gritti, C. (2022). Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction. *IEEE Access*, *10*, 5768–5789. https://doi.org/10.1109/ACCESS.2022.3141079

Marangappanavar, R. K., & Kiran, M. (2020). Inter-Planetary File System Enabled Blockchain Solution For Securing Healthcare Records. *2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP)*, 171–178. https://doi.org/10.1109/isea-isap49340.2020.235016

Mäder, L. (2020, November 25). *Spitäler stehen im Visier von Cyberkriminellen* [Hospitals targeted by cybercriminals]. *Neue Zürcher Zeitung*. https://nzz.genios.de/document/NZZ__202011250278942698/hitlist/0?all=

Mayer, A. H., Da Costa, C. A., & Da Righi, R. R. (2020). Electronic health records in a Blockchain: A systematic review. *Health Informatics Journal*, *26*(2), 1273–1288. https://doi.org/10.1177/1460458219866350

McGhin, T., Choo, K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, *135*, 62–75. https://doi.org/10.1016/j.jnca.2019.02.027

McKinsey & Company (2017). Digital disruption in insurance: Cutting through the noise.

Mendoza-Tello, J. C., Mendoza-Tello, T., & Mora, H. (2021). Blockchain as a Healthcare Insurance Fraud Detection Tool. In A. Visvizi, M. D. Lytras, & N. R. Aljohani (Eds.), *Research and Innovation Forum 2020* (pp. 545–552). Springer. https://doi.org/10.1007/978-3-030-62066-0_41

Microsoft. (n.d.). *Public Cloud vs Private Cloud vs Hybrid Cloud | Microsoft Azure. azure.microsoft.com.* Retrieved February 26, 2023, from https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds/#overview

NAIC (2020). NAIC Macroprudential Risk Assessment Overview. *NAIC: National Association of Insurance Commissioners.* https://content.naic.org/sites/default/files/inline-files/Macroprudential%20Risk%20Assessment_0.pdf

Ober, M. (2018). *The Decentralized Power of Ethereum and IPFS: How to Create Immutable Files*. https://medium.com/pinata/ethereum-and-ipfs-e816e12a3c59

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *IET Networks*, *7*(5), 321–327. https://doi.org/10.1049/IET-NET.2017.0207

Pirtle, C., & Ehrenfeld, J. (2018). Blockchain for Healthcare: The Next Generation of Medical Records?. *Journal of Medical Systems*, 42, 1–3. https://doi.org/10.1007/s10916-018-1025-3

Ponemon Institute. (2022). Cyber insecurity in healthcare: The cost and impact on patient safety and care. https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf

Redhat. (2022, July 25). *Types of cloud computing.* Redhat.Com.https://www.redhat.com/en/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud

S. Lee, J. (2020, May 17). *Tackling the demands of a digital world in an analogue healthcare industry | Healthcare Digital*. Healthcare-Digital.Com. https://healthcare-digital.com/technology-and-ai/tackling-demands-digital-world-analogue-healthcare-industry

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using Blockchain for Electronic Health Records. *IEEE Access*, 7, 147782–147795. https://doi.org/10.1109/ACCESS.2019.2946373

Shi, P., Zhang, W., & Boucher, J. P. (2016). Dynamic Moral Hazard: A Longitudinal Examination of Automobile Insurance in Canada. *Journal of Risk and Insurance*. https://doi.org/10.1111/JORI.12172

Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of Blockchain Technology in Medicine and Healthcare: Challenges and FuturePerspectives. *Cryptography*, 3(1), 3. https://doi.org/10.3390/CRYPTOGRAPHY3010003

Sookhak, M., Jabbarpour, M. R., Safa, N. S., & Yu, F. R. (2021). Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues. *Journal of Network and Computer Applications*, *178*, 102950. https://doi.org/10.1016/j.jnca.2020.102950

Sravan, N. P. V., Baruah, P. K., Mudigonda, S. S., & Kandala, P. K. (2018). Use of Blockchain Technology in integrating Heath Insurance Company and Hospital. *International Journal of Scientific & Engineering Research*, *9*(10), 1664–1669.

Srivastava, G., Dhar, S., Dwivedi, A. D., & Crichigno, J. (2019). Blockchain Education. *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), 1–5. https://doi.org/10.1109/CCECE.2019.8861828*

Starks, T., & Beard, M. (2022, October 6). An 'unprecedented' hospital system hack disrupts health-care services. *The Washington Post*. https://www.washingtonpost.com/politics/2022/10/06/an-unprecedented-hospital-system-hack-disrupts-health-care-services/

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*, 102407. https://doi.org/10.1016/j.jisa.2019.102407

Yang, G., Li, C., & Marstein, K. E. (2019). A blockchain-based architecture for securing electronic health record systems. *Concurrency and Computation: Practice and Experience*, *33*(14). https://doi.org/10.1002/cpe.5479

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, *14*(4), 352. https://doi.org/10.1504/ijwgs.2018.095647