Analysis of Blockchain in the Healthcare Sector: Application and Issues

Article *in* Symmetry · August 2022

DOI: 10.3390/sym14091760

3 authors:

Ammar Odeh
Princess Sumaya University for Technology
75 PUBLICATIONS **693** CITATIONS
SEE PROFILE

Ismail Keshta
AlMaarefa College for Science and Technology
58 PUBLICATIONS **532** CITATIONS
SEE PROFILE

Qasem Abu Al-Haija
Princess Sumaya University for Technology
211 PUBLICATIONS **1,715** CITATIONS
SEE PROFILE

symmetry

MDPI

Review

Analysis of Blockchain in the Healthcare Sector: Application and Issues

Ammar Odeh [1], Ismail Keshta [2] and Qasem Abu Al-Haija [1,*]

[1] Computer Science/Cybersecurity Department, Princess Sumaya University for Technology, Amman 11941, Jordan
[2] Computer Science and Information Systems Department, College of Applied Sciences, AlMaarefa University, Riyadh 13713, Saudi Arabia
* Correspondence: q.abualhaija@psut.edu.jo

Abstract: The emergence of blockchain technology makes it possible to address disparate distributed system security concerns in formerly ridiculous practices. A key factor of this ability is the decentralization of the symmetrically distributed ledgers of blockchain. Such decentralization has replaced several security functionalities of centralized authority with the use of cryptographic systems. That is, public or asymmetric cryptography is the key part of what makes blockchain technology possible. Recently, the blockchain experience introduces the chance for the healthcare field to implement these knowhows in their electronic records. This adoption supports retaining and sharing the symmetrical patient records with the appropriate alliance of hospitals and healthcare providers in a secure decentralized system, using asymmetric cryptography like hashing, digitally signed transactions, and public key infrastructure. These include specialized applications for drug tracking, applications for observing patients, or Electronic Health Records (EHR). Therefore, it is essential to notice that the principled awareness of the healthcare professionals is the leading point of the right perception ethics. In this work, we provide a thorough review of the issues and applications of utilizing blockchain in the healthcare and medical fields emphasizing the particular challenges and aspects. The study adopted a systematic review of secondary literature in answering the research question. Specifically, this paper aims to investigate how blockchain technology can be applied to improve the overall performance of the healthcare sector and to explore the various challenges and concerns of the application of blockchain in the healthcare system.

Keywords: healthcare; blockchain; symmetric ledgers; asymmetric cryptography; integrity

Citation: Odeh, A.; Kesha, I.; Al-Haija, Q.A. Analysis of Blockchain in the Healthcare Sector: Application and Issues. *Symmetry* **2022**, *14*, 1760. https://doi.org/10.3390/sym14091760

Academic Editors: Chin-Ling Chen and Jian-Qiang Wang

Received: 23 June 2022
Accepted: 16 August 2022
Published: 23 August 2022

1. Introduction

Blockchain applications are used by a variety of industries, including finance, healthcare, manufacturing, and education, to benefit from the distinctive set of properties that this technology possesses. Blockchain technology (BT) provides advantages in credibility, trustworthiness, organization, and transparency [1]. With its special blend of properties, including decentralization, immutability, and transparency, blockchain technology (BT) has a great deal of promise to support a variety of industries [2]. We anticipate that this technology will have positive applications in academia and science.

One sector where blockchain is anticipated to have a big influence is healthcare. Researchers and practitioners in health informatics constantly struggle to keep up with the advancement of this field's young but quickly expanding body of research. This article presents a comprehensive assessment of recent studies investigating the use of blockchain technology in the healthcare industry [3].

Healthcare is an important sector for both the developed and upcoming nations [4]. The overall capabilities of the medical and healthcare sector have been improved further

by initiating innovative and latest computer technologies within the sector. Such advancements in computer technologies may help physicians and other relevant health providers with the timely diagnosis and management of numerous health-related problems [5]. Different revolutionary and emerging computer technologies have since been applied within other sectors with highly promising outcomes. Such technologies comprise the Internet of Things, Blockchain, Data Mining, Cloud Computing, and the Internet of Things, Blockchain, Data Mining, Cloud Computing, and Internet of Things, Blockchain Data Mining, Cloud Computing, and many others [6].

As Ratta et al. (2021) [7] described, Blockchain is a point-to-point distributed network within which no single third party has been involved in the communication and transaction. Blockchain operates mainly by maintaining a symmetrical copy of the decentralized ledger for all users under the security of asymmetric cryptography. All the undertakings are isolated and not linked to other relevant transactions. For instance, the popular innovatory idea of cryptocurrency is supported by blockchain technology [8]. Similarly, cryptocurrency is highly believed to be very secure and unable to be hacked; the same blockchain concept can be applied in other sectors to enhance security and privacy issues. The healthcare sector is one of the relevant industries where the technology can effectively be applied.

Within the Blockchain, a ledger system that is publicly distributed is accessible to any individual in a symmetrical manner. In this case, the blockchain ledger is the list of records that keep the required information sequentially [9]. The block is the container with all the individual transaction details in this case. The block has both the header and the details of the transaction. The header is responsible for keeping all the information related to the block [10]. With its associated security features, Blockchain can easily be into the healthcare system to enhance the effectiveness of the sector's operations. The present paper seeks to establish how Blockchain can be applied in the healthcare sector, highlighting the specific challenges and concerns.

1.1. Blockchain Principles

A Blockchain is a public, decentralized, and distributed database managed by multiple participants, across multiple nodes connected through a peer-to-peer (P2P) network. Blockchain acts as a distributed ledger technology (DLT) where users can digitally verify the issued transactions without the need for trusted third-party (TTP) authority [11]. Typically, Blockchain presents a secure and autonomous consentaneous approach to expanding the DLT over time while keeping the data immutable and irrefutable [12]. The main characteristics of Blockchain-DLT are demonstrated in Figure 1.

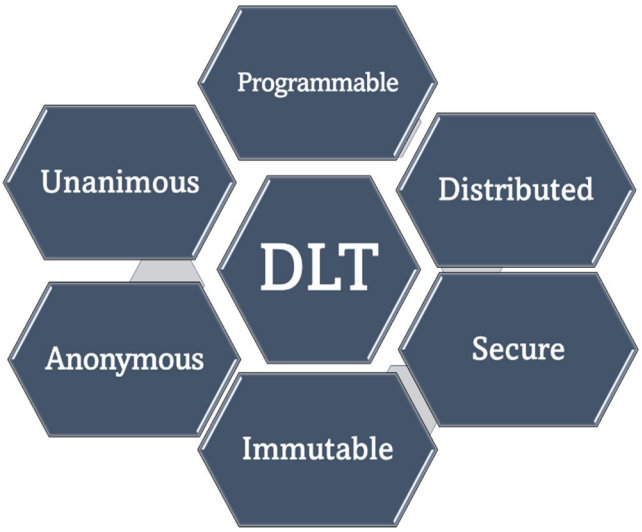

Figure 1. Main properties of distributed ledger technology (DLT) [12].

Blockchain is a sort of DLT that records the transactions using an immutable cryptographic signature called a hash using an algorithm (e.g., SHA 256) [13]. That is, changing one block in the chain is going to be directly noticeable as tampered with. Therefore, for the blockchain system to be corrupted by the hacker, almost, all blocks across the distributed chain need to be changed. Figure 2 illustrates the principle blockchain anatomy. Every node will have a complete copy of the ledger (blocks) and the block is composed of several data (transactions' list, …etc.). Blocks are connected by connecting every block with its predecessor and subsequent through a hash value. The blocks are linked together chronologically and cannot be modified after they are recorded without writing the entire ledger history again [14]. Nodes use a defined algorithm to reach a consensus on what ledger version is true and accurate [15].

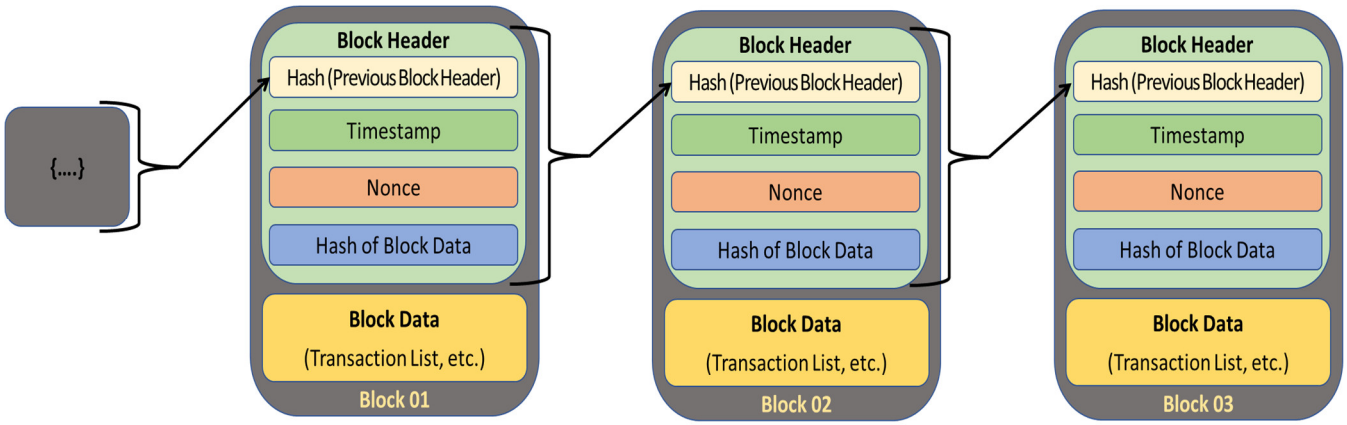

Figure 2. The Principles of a Blockchain Anatomy [15].

Blockchain has a wide range of applications, it provides solutions addressing several security concerns such as industrial applications, financial applications, medical/healthcare applications, smart grid and others [16]. For instance, in healthcare, a blockchain network is useful to preserve and exchange patient data. Blockchain applications can accurately identify serious and even hazardous errors in the healthcare and medical fields. Blockchain is crucial in processing duplicity in clinical trials for better healthcare outcomes [9].

1.2. Symmetric Decentralized Ledgers of Blockchain

Decentralized ledgers or DL are a set of databases distributed throughout a network and spanning over various topographical sites [17]. A ledger comprises a compilation of transactional accounts that are globally controlled by multiple parties in distinct sites and organizations [18]. The participants can assess distributed ledgers at each network node and obtain a symmetrical (identical) version of the distributed data. Once any changes happened in the ledger (such as editing, adding, deleting, …), then the new changes are repeated and reproduced to all participants in order to maintain the symmetry and accuracy of all records across the decentralized database in a synchronized manner [19]. Figure 3 illustrates an example of decentralized Ledgers of Blockchain maintaining symmetrical copies of the ledger [20].

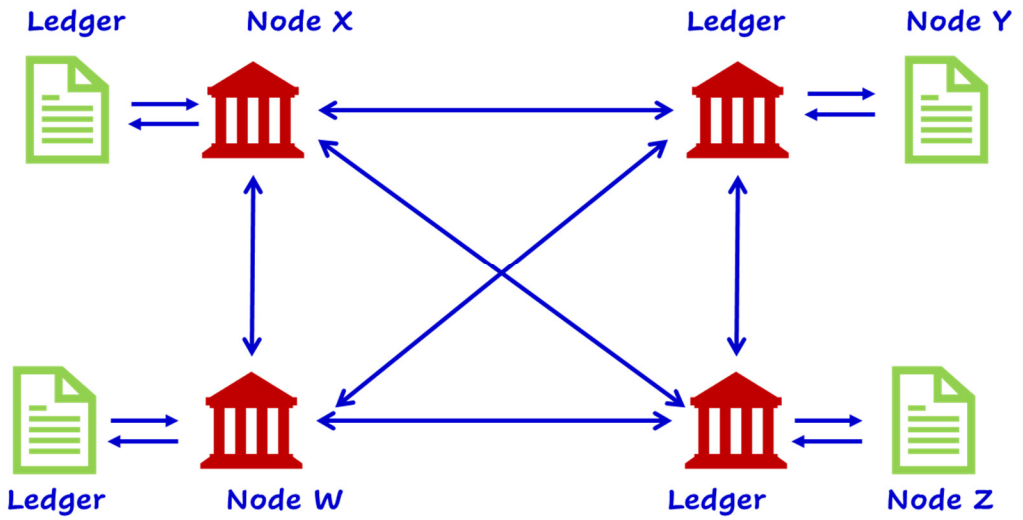

Figure 3. An example of decentralized Ledgers of Blockchain [20].

1.3. Asymmetric Cryptography in the Blockchain

Asymmetric cryptography is effective due to the use of two distinct keys: a public key used mainly for encryption or verifying key and a private key used mainly for decryption or signing key [21]. Asymmetric keys cryptography is perfectly matched for use in blockchain technology to authenticate identities for transactions and personnel.

A major characteristic of blockchain security relies on its pseudonymous where users need not disclose their real identities to establish a new blockchain account, rather, they are identified by means of addresses that depend on asymmetric cryptography [22]. Such asymmetric addresses for digital signatures where the user must sign the transaction digitally with his private key when making a transaction with a blockchain account can be later verified by the corresponding verification key (public key) to verify that the account owner authorizes the transaction. This makes it possible to authenticate transactions without revealing the identity of an account's owner [23].

Also, transactions run the Blockchain since they transmit value/code between different accounts to be performed on a smart contract policy. Each transaction on the Blockchain is digitally signed using an asymmetric digital signature crypto-algorithm. This, in turn, provides transaction authentication and anti-spoofing. Figure 4 illustrates an example of using asymmetric cryptography in the Blockchain to maintain integrity and confidentiality [24].

Figure 4. An example of using asymmetric cryptography in Blockchain [24].

1.4. Our Objectives

At present, we provide a review of the issues and applications of utilizing blockchain in the healthcare and medical fields emphasizing the particular challenges and aspects. Specifically, as per the broad objectives, the study seeks to achieve the following specific objectives:

- To demonstrate the blockchain application in the medical/healthcare sector and its major role in enhancing the overall performance of the medical/healthcare fields.
- To explore the various issues and challenges of applying blockchain technology in the medical/healthcare fields.

1.5. Paper Structure

The remaining parts of this paper are organized as follows: Section 2, reviews the most important state-of-the-art studies including a table to summarize the related work. Section 3, materials and methods, provides the complete details of the methodical study including the study design, search strategy and search performance, sampling procedure, the process of data collection, synthesis and analysis of data, and ethical considerations. Section 4 presents the findings and discussions including the current issues in the healthcare sector and how Blockchain can help in addressing such issues, the application of blockchain within the healthcare system (drug traceability, electronic health record), challenges, and issues associated with using blockchain in the healthcare sector. Section 5 provides the conclusion and recommendations of the proposed study. Section 6 emphasizes the main contributions and novelty of the study. Section 7 provides some limitations of the proposed work. Finally, managerial implications and future works are provided in Sections 8 and 9.

2. Related Works

Bigini G. et al. (2020) [25] examined the Blockchain's role in Internet of Things (IoT) applications. They summarized surveys and research papers that sought to understand current market conditions and identify obstacles to a user-centric approach to the industry's development. A number of papers have been examined to see how they use Blockchain to move toward a system that is more user centric.

The primary goal of Ratta P et al. (2021) [7] was to use cutting-edge computer technologies like the Internet of Things (IoT) and Blockchain to improve the efficiency of healthcare systems. Ratta P et al. (2021) indicated that IoT and Blockchain technologies can be used in a variety of healthcare applications. It is worth mentioning that Ratta P et al. (2021) indicated that these two technologies have enormous potential in the healthcare industry once they are integrated.

Rahmani MK et al. (2022) [26] highlighted the obstacles of trust issues in a cloud environment and potential use cases of blockchain adoption. The study's findings on the difficulties of cloud computing include the following: centralization, enormous overhead, trust evidence, reduced adaptability, and inaccuracy.

Sharma et al. (2021) [27] offered a detailed literature analysis that addresses the different prospects of applying blockchain technology in healthcare. The review explores the effort done to facilitate the merger of IoT and Blockchain in the medical sector. Sharma et al. (2021) [27] stressed that the Internet of Medical Things paradigm also encourages further research into advanced alternatives to suggest blockchain as a service that provides access to essential consistent blockchain infrastructures for different users or devices. The healthcare applications of blockchain technology are constantly being improved, but there are significant challenges to overcome and important decisions to be made in the future. There is still a need for more testing, experiments, and research before the widespread use of blockchain technology in the healthcare industry can be considered safe. We summarize the related works in Table 1 below.

Table 1. Summary of related work.

Reference	Description	Advantage	Limitations
Reegu et al. [28]	Blockchain assists in sharing health-related records among various stakeholders	The study addresses the first objective of the application of blockchain technology in healthcare sector.	It fails to address the challenges associated with blockchain technology in healthcare sector
Raatta et al. [7]	Application of blockchain and internet of things in healthcare and medical sector	The study addresses the first objective of the application of blockchain technology in healthcare sector.	No mention of challenges associated with blockchain technologies
Ullah, et al. [29]	When Internet of Things is integrated with blockchain, then it makes the entire drug traceability system to become more reliable and secure	Highlight the importance of blockchain technology in healthcare sector	No mention of challenges associated with blockchain technologies
Siyal, et al. [30]	Blockchain is applied to develop a kind of atmosphere where two different parties are able to trust one another.	There exist numerous ways through which blockchain can be implemented, though the common approach	No mention of challenges associated with blockchain technologies
Makridakis, et al. [31]	Blockchain system never poses the capability to discover and eliminate the usage of drugs that have not been authorized.	It shows security concerns that cannot be addressed by blockchain technology	No mention of the wider application of blockchain technology in healthcare industry.
Abunadi [32]	Blockchain is applied to develop a kind of atmosphere where two different parties are able to trust one another.	Blockchain is more transparent since one change in the transaction process will automatically get reflected for all the relevant users	It fails to address the challenges associated with blockchain technology in healthcare sector
Mehta [33]	Interoperability within healthcare means exchanging relevant information with each other within the entire blockchain network.	Within the healthcare industry, making sure that there is appropriate interoperability among different institutions may be a great challenge	No mention of the wider application of blockchain technology in healthcare industry.
Attaran [34]	Lack of trust among the patients and other groups of important stakeholders is also a major issue in the application of blockchain within the healthcare system.	The study addresses the second objective on the challenges of the application of blockchain technology in healthcare sector.	No mention of the wider application of blockchain technology in healthcare industry.
Reegu [35]	Despite the fact that cloud sharing usually makes it easy and convenient to transfer medical images, subsequently improving and streamlining overall patient care, the major stumbling block to the widespread usage is still fear as well as unease regarding the technology	There are a number of issues and concerns regarding the storage and sharing of relevant medical images	No mention of the wider application of blockchain technology in healthcare industry.
This work	It seeks to establish methods for preserving security and privacy while implementing blockchain technology in the healthcare sector. It is important for the designers of the blockchain technologies as well as the common users as it outlines the manners in which the security and privacy of the persons involved can be assured even as the technology continues to gain widespread usage and application in healthcare setups.		

3. Materials and Methods

3.1. Study Design

The research focused on the specific research topic by developing a systematic review of viable secondary literature. Torres-Carrión PV (2018) [36] argues that a vast amount of data exists pertinent to medical data encryption. Conducting the present research using existing secondary data is achievable. A more extensive definition of a secondary literature review entails interpreting and analyzing data that other groups of researchers have

previously collected. The viability of the research approach arises from the cost and time savings because it does not encompass going to the field to collect data. The term desktop review arises from the ease with which researchers can review data on a desktop. Resource and time availability determined how the researcher selected the approach. Secondary data are easily accessible and assist the researcher in illustrating the problems with clear and better insight. The study guaranteed that the information application was accurate, current, and relevant.

3.2. Search Strategy and Search Performance

The process of secondary literature search encompasses picking easily accessible secondary literature on online platforms. Another determining factor to literature selection included content relevant to the research topic, such as blockchain application in the medical and healthcare sector and illustrating specific concerns and challenges. To establish suitable and relevant search terms, research questions developed were categorized in terms of population, intervention, and outcomes. This was critical in constructing reliable search terms for this research.

3.2.1. Population

As per the research question, the population in this study is healthcare providers and vendors who use blockchain within the healthcare sector.

3.2.2. Intervention

Establish how blockchain technology can be applied to improve the general performance of the medical sector and the various challenges and concerns of the application of blockchain in the healthcare system.

3.2.3. Outcome

Uses of blockchain in the healthcare sector and associated challenges. As this is mainly an exploratory study, the papers that are reviewed are empirical studies, case studies, theoretical studies, and scholarly articles. For the first research question, which is "how blockchain technology can be applied to improve the general performance of the medical sector?", an example of search terms include:

- Population-Medical sector
- Intervention-blockchain technology
- Outcome-impact/usage/challenges

As different studies are aimed at being collected, both descriptive and analytical research will be inclusive of all the other types of research conducted and this will not be used as a discriminatory factor in searching for the research studies.

A search string was developed using the Boolean operators with a trial search conducted using the following: ("blockchain technology" OR "medical sector" OR "impact/usage") AND ("application" OR "performance" OR "healthcare" OR "improve"). From the information that was retrieved, the search strings that were used are given as:

- Search string 1:
  ("blockchain technology" OR "medical sector" OR "impact/usage")
- Search string 2:
  (OR "medical sector" OR "impact/usage")
- Search string 3:
  ("application" OR "performance" OR "healthcare" OR "improve").
- Search string 4:
  (Challenges" OR "blockchain technology")

- Search string 6:

  ("Security challenges" OR "Privacy challenges" OR "information technology ").

3.2.4. Study Selection Process

The inclusion and exclusion criteria used in selecting the information are given below.

3.2.5. Inclusion Criteria

The inclusion criteria for picking a specific article for the study are addressing medical data encryption and emphasizing the challenges and concerns relevant to the encryption process. Other areas considered include:

- Studies that described the application of blockchain technology within the healthcare sector.
- Studies describing challenges and concerns of application of blockchain in healthcare systems.
- Studies highlighting the security and privacy concern related to the use of blockchain in the healthcare system.

3.2.6. Exclusion Criteria

Some of the studies and publications were not included in this study and the exclusion criteria that were used include:

- Studies that were not specific to the current two study objectives.
- Studies that were not describing the application of blockchain technology in the healthcare sector.
- Studies that were not describing the security and privacy issues related to blockchain technology.

3.3. Sampling Procedure

Secondary literature sampling involves picking easily accessible secondary literatureon online platforms. Another factor in literature selection included content relevant to the research topic, such as blockchain application in the medical and healthcare sector and illustrating specific concerns and challenges [37]. The inclusion criteria for picking a specific article for the study are addressing medical data encryption and emphasizing the challenges and concerns relevant to the encryption process.

Researchers prioritized data collected via random procedures when selecting secondary literature to incorporate into the study [38]. An evaluation of scholarly article abstracts and titles occurred alongside an extensive analysis after generating a hard copy of the articles. We then confirmed the relevance of the articles to the topic of evaluation by subsequently scanning the sources. The only articles accepted were those with content pertinent to the topic of medical data encryption concerns and challenges.

3.4. The Process of Data Collection and Application of PRISMA

From a general point of view, a Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) flowchart was incorporated into this study to exhibit the condition of the associated examinations. It is essential to state that the advocated procedure of data abstraction was pursued to pick and code relevant studies for proper inclusion in the process of the systematic review. The researcher's search evaluated the relevant documents to highlight the variations of medical data encryption and associated concerns and challenges. Appropriate scholarly sources encompassed periodicals, articles, and books focusing on content about medical data trust and encryption and concerns and challenges over time [39]. Relevant articles and books were generated using the university database. Specific keywords sufficed to generate the initial articles. The researcher performed a search for articles using various databases, such as PubMed, EBSCOhost, ERIC,

and Google Scholar. The keywords used for the general search process included medical, data, and encryption. Paper and article selection occurred relevant to the search results so long as the respective sources aligned with the relevant inclusion criteria.

A specific highlight of the search outcomes reveals that the search generated 4450 records, encompassing health organization records and conventional research studies. Regardless of the accessibility of a large amount of data because of the search strategy, the researcher removed all the duplicates using the process of data cleaning. After eliminating duplicate sources, the researcher was left with 2765 articles. In addition, a review of abstracts and titles occurred to confirm that the sources aligned with the relevant inclusion criteria. The final elimination occurred pertinent to the research designs and methodology. A total of 615 articles were excluded because they never met the inclusion criteria, while only 455 met the eligibility Assessment of Full Texts from which 170 were not Full-text accessible articles. More articles were excluded based on population (45), Intervention (25), Comparator (25), and Outcome (20). Only 35 articles were eventually included in the research process. The PRISMA study flowchart, Figure 5, demonstrates the search results.

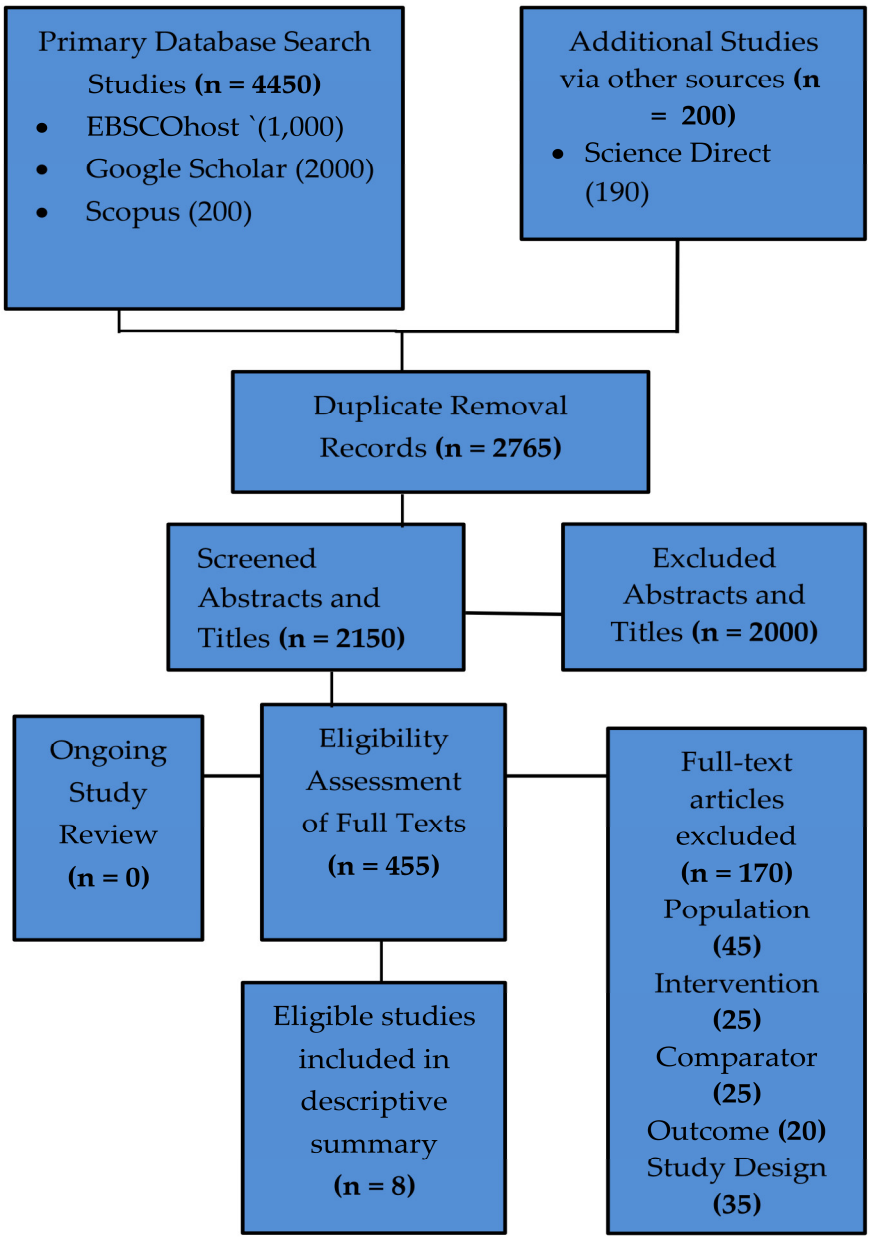

Figure 5. PRISMA flowchart Source: (Generated by the Authors).

3.5. Synthesis and Analysis of Data

Ongoing and recursive data analysis protocols were applicable for data analysis. The specific occurrences entailed reading literature review contents and grouping them pertinent to various themes [40]. The current study focuses on assessing the concerns and challenges of medical data encryption and suggests strategies for addressing such concerns and challenges [38].

The following data were extracted from each publication: time of review, target population, authors, specific privacy and security challenges, and application of blockchain technologies.

3.6. Ethical Considerations

Generating relevant approvals from specific authorities was the first step toward addressing the arising ethical concerns. In addition, while conducting the research, the literature was generated with a faithful intention, such as with proper acknowledgments to eliminate plagiarism via reference listing.

4. Findings and Discussions

4.1. Current Issues in the Healthcare Sector and How Blockchain Can Help in Addressing them

The heavy burden associated with healthcare costs as well as concerns regarding increased medical errors instigated a catalyst for general improvement in the overall delivery of healthcare services. Scholars identify the value-based approach to the delivery of healthcare services achievable from the availability and analytics of big amounts of patient data that are collected using health information technology such as blockchain [41]. The recognition of the value of blockchain technology in the improvement of healthcare delivery has prompted players in the sector to contribute many financial incentives to promote the adoption and consequently the implementation of the technology in healthcare facilities [42].

According to Donawa et al. (2019), the use of blockchain in electronic health records provides a health record storage service that therefore facilitates web-based accessibility. The system is frequently designed to give people complete authority over creating, managing, and sharing their electronic health records with friends, family, healthcare professionals, and other relevant data users [43]. As illustrated by Abunadi (2021), the main advantage of such a system is the security and confidentiality associated with it. Scholars acknowledge that the blockchain system is more reliable and secure compared to the paper storage of medical records. It is important to note, however, that there are still a number of issues of concern that are linked to the usage of blockchain in electronic health records. The aim of the current article is to provide a comprehensive investigation of the challenges and aspects of the application of blockchain in EHRs [41].

Patel, Parthit, et al. (2018) report that blockchain has always been proposed to address the issues attributed to data access and privacy [44]. Fatokun, et al. (2021) explain that it is a blockchain for electronic health records, that is to say, a growing list of blocks that comprise records that are linked through the application of cryptographic hash. There are numerous advantages linked to blockchain in electronic health records. Blockchains can be used to help secure the Internet of Things (IoT) in the healthcare sector. A governance paradigm is used by the blockchain to enforce business logic, which is understood by all participants. A smart contract can therefore be used to govern the necessary access control rules and achieve HIPAA compliance [45]. Additionally, as Keshta, et al. (2021) pointed out, the relevant stakeholder groups have the right to store data in blocks that cannot be edited retrospectively, which means blockchain can be managed by all of these organizations together [46].

4.2. Application of Blockchain within the Healthcare System

The adoption of blockchain in healthcare supports retaining and sharing symmetrical patient records with the appropriate alliance of hospitals and healthcare providers in a secure decentralized system, using asymmetric cryptography like hashing, digitally signed transactions, and public key infrastructure. There are numerous specific applications which include: traceability of drugs and patient monitoring or rather HER.

4.2.1. Drug Traceability

Traceability of drugs is always undertaken using a centralized approach within which aspects such as authentication and privacy of data, as well as the system flexibility, are never realized. Several decentralized models have always been proposed to solve issues related to drug traceability [47]. For the privacy and authenticity of traceability data, a blockchain system known as Drugledger has widely been proposed. Drugledger usually integrates the Blockchain with the whole drug supply chain to easily trace such drugs [48]. Drugledger specifically has two different flows of drugs: the information that flows regarding the drug ledge and the physical flow of the real drug, all of which goes to the drug ledge network in the formula of a chain network of drugs. This new system alters the traditionally understood protocols by grouping the healthcare professionals into various parts: QSP, query service provider; CSP, certificate service provider; and ASP. However, it is important to note that the drug traceability scenario, as illustrated in the present paper, looks so simple theoretically but is overly complex within the real-life case scenario [49].

However, Hamza et al. (2020) [50] highlight that the entire drug traceability system becomes more dependable and secure when the internet of things is integrated with Blockchain. Numerous frameworks have been suggested in the healthcare field regarding drug traceability or patient monitoring systems. The researchers in [7] suggested a structure to help curb drug fraud by tracking every drug within the supply chain system. The greatest aim in this scenario is to help reduce incidences of counterfeit drugs within the Blockchain. The specific and commonest technologies that can be applied to help improve the traceability and visibility of commonest technologies that can be applied to help improve the traceability and visibility of commodities such as drugs are RFID and Blockchain [51].

For a more transparent movement of the drugs, the Gcoin Blockchain model, in which G stands for global control, is suggested; the model equally changes the drug supply chain system from regulating to inspection and surveillance of the drugs [52]. This means a government model that is combined with a decentralized autonomous organization.

Blockchain is applied to develop a kind of atmosphere where two different parties can trust one another. There are numerous ways through which Blockchain can be implemented, though the common approach, as claimed by Siyal et al. (2019) [53], is Gcoin Blockchain. As further argued by the scholar, Gcoin Blockchain can easily track every drug in the same ways Blockchain tracks the movement in bitcoin. It assists in building a superior level of trust and transparency between sellers and buyers [53]. It is important to note further that Gcoin aims to improve overall data efficiency.

In India, for instance, several lives are considered at risk due to the use of fake drugs. A proposed framework of Blockchain can therefore be applied to help detect the possibility of fake drugs within the supply chain. Such suggested frameworks are based on Hyperledger fabric kind of architecture, within which one PC works as the main beneficiary and five different computers are applied when making the orders. The system is fully dependent on blockchain technology [54]. Moreover, the supply chain of drugs from the drug-producing stores to the local intermediaries and clinics or retail drug shops and hospitals is managed by the application of Blockchain, which assists in tracking all the fake drugs.

The system, in this case, was tried in several case scenarios such as audits of drugs in distribution, stolen drugs, or fake distribution of drugs. The blockchain system was compared with other systems in numerous parameters such as resistance against any given

point of failure, detection of counterfeit drugs, identification of diverted drugs, spying for drug shortage, security, privacy, transparency, and immutability [4]. However, Makridakis et al. (2019) [55] outline that the blockchain system never poses the capability of discovering and eliminating the usage of drugs that have not been authorized.

Regarding medicine, the commonest threat is that the manufactured medicine is never received by the pharmacy and can easily get replaced with a counterfeit supply chain. As emphasized by [56], the supply chain approach can never trace drugs that have landed in the wrong hands. For instance, India produced the majority of counterfeit medicines in 2017 and presently it is approximated that close to 35% of counterfeit medicine was sold across distinct parts of the globe. To come out of these problems, Abunadi (2021) [41] proposed the usage of Blockchain and claimed that it is more transparent since one change in the transaction process will automatically get reflected to all the relevant users. With its decentralization concept, Blockchain can analyze the results on two platforms: Hyperledger and Ethereum. Within the Ethereum Blockchain, every operation needs some fees. Miner is provided money to perform transactions and maintain the Ethereum network [57]. There has never been a major need to know your Customer (KYC) within such a process, resulting in some sort of blind spot, which shows us the individual who might be using the account. Blockchain applying Hyperledger, on the other hand, never needs fees, making it easy for the individual producer to undertake the transaction.

4.2.2. Electronic Health Record

An electronic record includes the necessary vital administrative and clinical data of the patient like demographics, diagnosed clinical problems, medication, and laboratory data, among other reports. Using paper as a means of recording patient data has proved to be very extensive and non-reliable as the world has since gone digital [56]. As a result, most healthcare organizations have resorted to using electronic records to keep their data. Blockchain, a decentralized type of database whose data block is specifically linked chronologically, has widely been applied to enhance HER performance. Arunkumar (2020) points out that numerous parties within the healthcare industry need to manage the personal HER blockchain collaboratively, like the medical specialists, insurance departments, and the hospital. Since the traditionally known EHR system is trademarked with decentralized design, only one unit of supplier controls the code base, database, and system outputs [58]. It has become difficult for the centralized systems to have full confidence from the hospital management, doctors, and patients [41]. Therefore, Blockchain has been considered the solution to the trust issue associated with a centralized electronic health record system. With blockchain technology, all the patient information is stored in the Blockchain through the use of meta mas, and the details of each patient are stored in the Blockchain as independent data blocks. Each block comprises encrypted data. The system record health-related information of an individual patient so that respective health care providers and the patients can easily consult it themselves. In most cases, the data are usually encrypted by a specified algorithm to encrypt all the patient data into a single line bit that is subsequently stored in the block [59].

As Donawa et al. (2019) [43] noted, using Blockchain in electronic health records offers a convenient and symmetric health record storage service that promotes easy accessibility of such records through the web. The system is often designed to allow the patients full control of generating, managing, and consequently sharing their electronic health records with friends, family, healthcare providers, and other relevant data consumers. Abunadi (2021) [41] illustrates that such a system's main advantage is security and confidentiality. Scholars acknowledge that a blockchain system is more reliable and secure than paper storage of medical records. However, it is important to note that several issues of concern are still linked to using Blockchain in electronic health records. The present paper presents a thorough examination of the aspects and issues concerning the use of blockchains in EHRs. For example, Alla et al. (2018) [60] indicated that the patient could lose

control across the prevailing EHRs in the course of live actions, despite the fact that the service provider constantly retains the principal stewardship.

Cunningham et al. (2018) [32] report that Blockchain has always been proposed to address the issues attributed to data access and privacy. Fatokun et al. (2021) [35] explain that it is a blockchain for electronic health records, which is to say, a growing list of blocks comprising records linked through the application of cryptographic hash as an asymmetric crypto-algorithm. There are numerous advantages linked to Blockchain in electronic health records. For instance, a Blockchain is a linked peer-to-peer database in which data integrity, availability, and response time are fully guaranteed. Blockchains can adequately facilitate internet of things security in electronic health.

Moreover, the Blockchain works within the governance model, which helps enforce business logic that all the participants accept. It is, therefore, very possible to exploit a smart contract or chain code to control the relevant control policy on access and achieve HIPAA compliance. Keshta et al. (2021) [36] also highlighted that Blockchain is additionally managed collectively by the relevant stakeholders, some of whom. Some have the right to record data in the block that cannot alter retroactively.

Mehta et al. (2020) [31] noted that Blockchain in the electronic health record is symmetrically distributed and append access rights to only its ledger shared among the specified users. Fine-grained access to the ledger is equally implemented to realize an appropriate balance between availability and privacy. Figure 6 below illustrates the possible access rights of users as applied in the BlockHealthChain. The rights, in this case, include read permission, write permission, read permission with anonymized EHRs, and authorization permission.

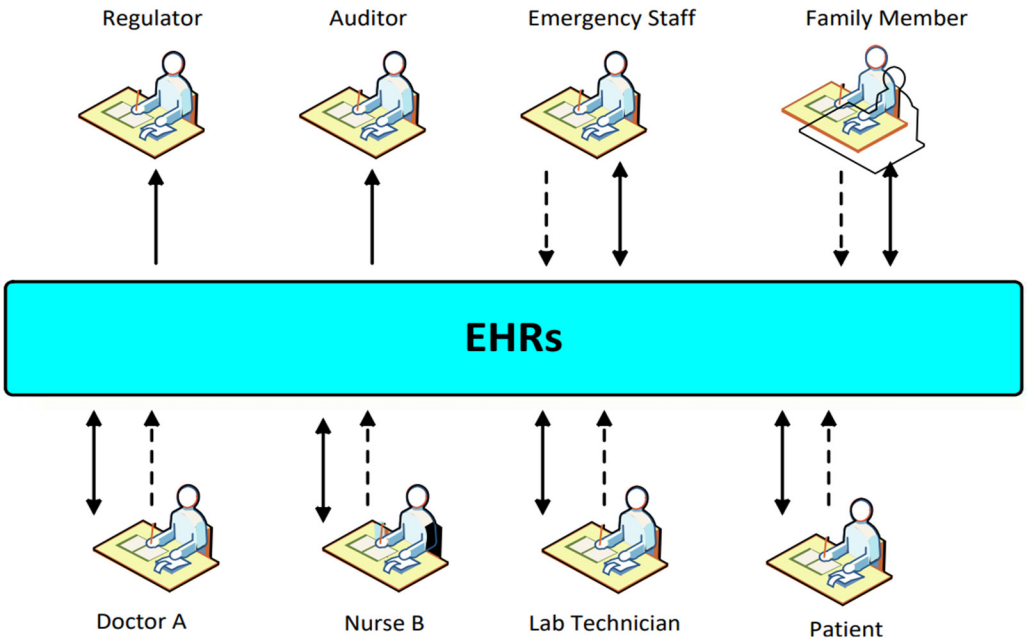

Figure 6. Possible access rights of users as applied in the BlockHealthChain.

It is clear from the figure that within blockchain protocol, different users tend to have different access qualifications for EHRs. With this arrangement, patients have the right to control access to electronic health records, including individual patient-reported information. The former comprises numerous contents like allergies, demographic information, and numerous contents allergies, demographic information, and monitoring data collected from the applied instruments [47]. The latter, in this case, refers to the updated medical record by the staff of doctors. The patient can authorize family members or health care providers to read and write their personal health information, minimizing the potential risks of tracking and replicating healthcare data.

Nurses, doctors, emergency staff, and laboratory technicians control and manage access to the electronic health record that is updated by themselves. Additionally, they effectively use or disclose protected health information for the diagnosis, treatment, and payment without seeking authorization from the patient [22]. This means having the authorization to grant read or write permission to other relevant entities, in which case the electronic health records are shared within the healthcare organizations.

Attaran (2020) [30] additionally indicated that several classes of users submit various EHRs containing test results, encounter comments, and demographic. For instance, the test result includes several fields: Patient ID, patient name, technician ID, type, indicator, and final result. Each electronic health record in the Blockchain corresponds to a transaction, which must be executed accurately and included within the ledge. All the electronic health records pose lifecycle as shown in Figure 7 below.

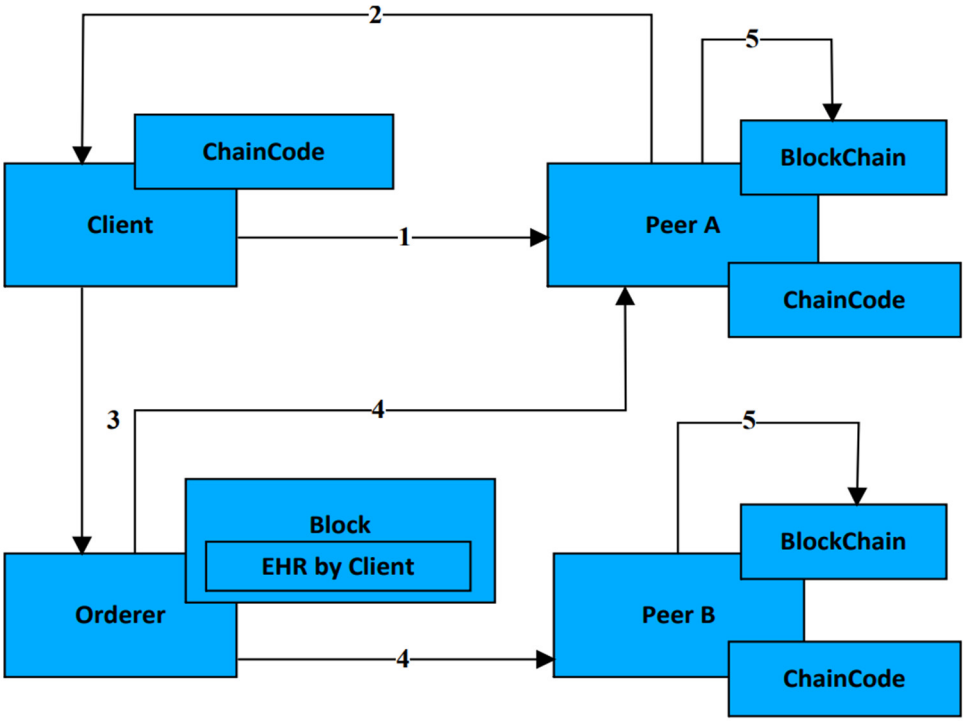

Figure 7. illustrates the electronic health records lifecycle.

4.3. Challenges and Issues Associated with Using Blockchain in the Healthcare Sector

The major challenges in the application of blockchain technology within the healthcare sector include interoperability, security, lack of standardization, storage requirements, hospitals' hesitation to share patient data, lack of trust among patients, lack of skills among doctors and medical practitioners, and lastly, accountability and data ownership.

Interoperability within healthcare means exchanging relevant information with each other within the entire blockchain network. It is the major concern based on the large and diverse group of providers and its large open existence [23]. There might exist various players such as private doctors, physicians, insurance institutions, players such as private doctors, physicians, insurance institutions, and players such as private doctors, physicians, insurance institutions, and hospitals, among others. Ensuring appropriate interoperability among different institutions may be a great challenge in healthcare.

Moreover, the idea of decentralization is considered very much secure, and some other security issues are associated with it. Since data are usually decentralized within the Blockchain, meaning such personal data are widely distributed within the symmetric public ledger, this can result in privacy leakage. Blockchain offers an environment where peo-

ple trust or know and can securely share data. In some case scenarios, however, such objectives may fail, especially when those who have access to such data become malicious in their dealings [20]. A majority of the patients may become highly uncomfortable in making public or sharing their individual medical information as a result of security reasons.

Nagasubramanian (2020) also points out the handling, storage requirement, and scalability issue [22]. It is not practical to safely maintain data for all the patients. The medical record is usually in the form of laboratory reports, images, and documents. Storage of medical records of various groups of patients using digital methods may need colossal storage capacity [23]. The medical transaction of every individual stored in a distributed way with the same type of record stored in various locations may need some huge extra storage capacity, which may significantly impact the healthcare system.

Blockchain does not have adequate standardization, even though it is a trending technology adopted worldwide. In the networks and provinces in which the notions of traceability and security are concerned, Blockchain appears to be missing the extremely applicable standardization. Attaran (2020) [30] described the correct standardization of technologies and protocols as crucial.

Equally, the hospitals and the associated entities may be hesitant to share the specified information. Most hospitals may be reluctant to share their patient medical records and the associated data, for instance, in for-profit circumstances, as they would wish to charge different fees from their respective customers [25,34]. On a similar note, insurance institutions and hospitals might be reluctant to share their data, as it might be advantageous for the healthcare institution to keep the fees-related data among themselves. It is particularly important to build a strong trust between the concerned parties and convince them to share their data for appropriate healthcare service delivery.

Another noticeable and essential issue in utilizing blockchain in healthcare applications is the shortage of trust between patients and other critical stakeholders, as contended by Attaran (2020) [30]. The majority of patients may be unwilling to reveal and impart their EHRs in the public realm to other objects in the third party. Therefore, it is very necessary to develop trustworthiness between the individual patients on the subject of the confidentiality and privacy features of Blockchain in the field of healthcare schemes [19].

Additionally, asking physicians and other groups of healthcare providers to move from paper to technology can be a major challenge. Electronic records and prescriptions rather than paper-based prescriptions can be a major challenge to most people. For example, doctors always do not fill the fields considered to be unnecessary within their routine work. Despite all that, in the case scenario of electronic records, the physicians cannot omit the fields that have been marked as mandatory. Similarly, depending on technologies such as Blockchain and the Internet of Things for remote monitoring can generate questions among physicians concerning their efficiency and accuracy [7]. Technology-related healthcare accuracy, performance, and efficiency depend on the doctor's skills and training. Therefore, before introducing such technologies into the actual practice, adequate training and the necessary skills should be imparted to the respective doctors to help build their confidence in applying such technologies [33].

Attaran (2020) illustrates that data accountability and ownership are other major challenges in deploying blockchain technologies within the healthcare industry [30]. Banu (2020) reports that although cloud sharing usually makes it easy and convenient to transfer the medical image, subsequently improving and streamlining overall patient care, the major stumbling block to its widespread usage is still fear and unease regarding the technology. There are several issues and concerns regarding storing and sharing relevant medical images. Possibly the main hurdle for numerous practices and facilities is the right high-speed bandwidth required to transfer images quickly. Primary deduplication, storage, and compression will help dramatically minimize bandwidth usage while improving performance [45]. Due to low bandwidth, image latency has become essential for the relevance of the cloud's relevant user communication of the image by the users, and relevant

performance criteria usually drive analysis applications. It is unclear that remote rendering offers low display latency for all the relevant medical imaging applications when assessing the server via the internet is necessary.

Ethics is the main guide of the moral consciousness among health care professionals. Confidentiality (also called secretiveness) is one of the core principles of ethics. The relationship between the patient and the medical expert is only based on trust [37]. Therefore, every bit of image data needs to be made under the main premise that all health information of any given patient will at all times be made confidential not only by the healthcare provider but also by any other individual with the legal and professional right to access such records. There is always a great need for such information to be protected from access by any unauthorized persons or disclosure to any family member except in the circumstances that it is required by law or in the situation where the patient has given out consent in writing [6]. The above findings show that most healthcare organizations still use paper record sets. Healthcare organizations still use paper records for each patient. Few medical practitioners have been reported using normal computer software for data encryption. This is contrary to other 'scholars' arguments that medical image records must always be stored in a safe place without fail to address. The universally accepted standard for keeping such data requires that if an electronic system is applied while entering the image of the patient, then there is a need for it to have a password and login for anyone to access such image [7]. There is also a great need to perform m backup of all the records on the removable medium that will enable the recovery of data images in the event the system fails. A breach of confidentiality is always considered to have occurred when the private information that a given healthcare provider has learned from the patient is passed to a third party without permission from the patient or court order. Systematically, confidentiality concerns can be addressed by applying robust asymmetric crypto algorithms.

Literature has affirmed that information communication in the current times has become more effective and efficient. However, security concerns over safe data transfer have risen [38,43]. Cyber-attacks and other related threats targeted at the system of information communication render network and system security an aspect worth considering deeper within the realm of information communication technology [22]. With the advance in technology, hackers and intruders have overly complicated tools they can use to bypass the traditionally known generic network security system to cause intentional harm to the whole system. Specifically, cyber security threats are currently exploiting the connectivity and complexity found in the existing infrastructure and launches attacks on systems considered legitimate. Even with such predicaments, it is important to note that the performance of the healthcare industry depends on the reliable working of the important infrastructure, whose safety might be put at a higher risk by the cyber-attacks [18]. Such attacks have major impacts on the general viability of the healthcare organization that might have been affected and even on the public company's reputation. System failures and crashes are good examples of the risks that most organizations currently dread in their daily operations. For this reason, numerous security measures have been considered necessary even as blockchain technology is being implemented, especially the asymmetric cryptosystems.

In the midst of such measures, the network intrusion detection system (NIDS) is apparently existed to improve the security of computing resources against anomalies such as cyber threats and attacks [26]. NIDS usually investigates and foresees activities of a given system aiming of thwarting such behaviors that might be adopted as malicious. The intrusion, in this case, can always occur in several ways: a legitimate user of a given system misusing the privileges they have of accessing the system, a legitimate user trying to gain additional access privileges, and an external attacker trying to access the system [27]. In this case, the network intrusion detection system works by either recognizing the attacks or malicious activities or blocking them or detecting them by looking at the signatures of the attack within the log files. However, organizations are yet to achieve much with the current

network security systems; organizations are yet to achieve much with the current network security systems, even such a system [20].

The literature affirms that the uncertainty related to today's clinical decision situations necessitates healthcare providers to apply the most sophisticated quantitative models that move beyond the general capabilities of the known traditional simple linear models. As the uncertainty and complexity of the data continue to increase, the model's general capability need also needs to equally increase so that the highly nonlinear relationships within the existing variables can also be captured [21]. This is where artificial neural networks and blockchain technologies fit into clinical decision-making.

Such models can be traditional of diverse types: decision analysis, optimization, simulation, and other things. Artificial neural networks and blockchain applications represent the modern approach to modeling. Artificial neural networks and blockchain applications can also be associated with data-driven clinical decision support. In that regard, neural networks offer a method for analyzing or forecasting past data [9]. Though it is commonly known as the black-box approach, or rather, a heuristic method, within the last decade, blockchain technologies have greatly been studied by known statisticians to gain an accurate understanding of individual power prediction from the statistical point of view.

5. Conclusions and Recommendations

This study provides a detailed review of the issues and applications of utilizing blockchain in the healthcare and medical fields emphasizing the particular challenges and aspects. This includes specific applications such as drug traceability, observation of patients, and Electronic Health Records (ERH). Confidentiality (also called secretiveness) is one of the core principles of ethics. The relationship between the patient and the healthcare professional expert is only based on trust. Every medical record, therefore, needs to be made under the main premise that all health information of any given patient will at all times be made confidential not only by the doctor but also by any other members of the healthcare team who have the legal and professional right to access such records. There is always a great need for such information to be protected from access by any unauthorized persons or disclosure to any family member except in the circumstances that it is required by law or in the situation where the patient has given out consent in writing. As for protecting the data from any project, the data from any of the above findings show securely, blockchain technology has failed to securely protect the data from unauthorized dealers. This is contrary to the academic expectations that always medical records must be stored in a safe place without fail to address. The universally accepted standard for keeping medical records requires that the theocentric system be applied while entering the patient's records. It needs a password and login for anyone to access the data. This factor is not applicable in Blockchain as each data set is presented in blocks and can be accessed individually. There is also a great need to back up all the records on the removable medium that will enable data recovery if the system fails. A breach of confidentiality is always considered to have occurred when the private information that a given dental practitioner has learned from the patient is passed to a third party without permission from the patient or court order. Equally, Blockchain does not have adequate Standardization, although it is a trending technology adopted in numerous countries worldwide. It has been observed that blockchain lacks the proper security standardization, especially within networks and realms. While those not concerned with the patient data might intentionally attempt to access information on the patient identity or location by intercepting communication between the patient and the healthcare providers, such efforts may be thwarted when proper security control systems are put in place. Numerous breaches can easily be prevented by putting a high-quality security plan specializing in the simplest and most common reasons for data breaches within the blockchain system.

6. Contributions and Novelty of the Study

As the healthcare system becomes more interconnected, more also as several wireless medical devices begin to connect to the web-enabled information technology system, they become very much vulnerable. The vulnerability, in this case, is not only based on the malicious hackers but from some other relevant threats like the computer virus and malware. Even with such threats, most governments require ways through which they can reduce healthcare costs within their countries. The analysts in these countries seriously think that blockchain technology will be of great help to them in a greater reduction in spending in the future to come. Blockchain, like any new technology, brings with it new challenges and risks. There are some characteristics that distinguish privacy and security challenges in the IoT, necessitating a deeper investigation into the subject. The current study is therefore extremely important because it seeks to establish methods for preserving security and privacy while implementing blockchain technology in the healthcare sector. The study in this case is important both to the designers of the blockchain technologies as well as the common users as it outlines the manners in which the security and privacy of the persons involved can be assured even as the technology continues to gain widespread usage and application in healthcare setup.

7. Limitations

This study had a number of limitations. Usually, academic and professional literature focuses more on the usage of blockchain technologies without including the aspects of security and privacy preservation in the medical sector. The current study applied a systematic review of secondary literature which might actually not reveal the current information on the ground but only relied on what others had studied. The limited amount of time and resources has equally restrained the data collection process. This might fail to give more representative results. Failing to use primary data, in this case, is a limitation of its own since the researcher only relied on what had been developed by others. Any error or bias committed in such articles is directly transferred to the present study and this might significantly impact the legality and trustworthiness of the study. Such a prospective study needs to include both primary and secondary methods of data collection so as to enhance the overall validity and reliability of the study findings.

It would be ineffective and costly to supply massive records on the blockchain, such as entire EHRs. A blockchain makes it challenging to query data, which restricts how data may be used for research, statistics, and medical applications. Participants in the network are violating users' data privacy.

Lately, the enormous potential for healthcare data management to deliver more precise and economical patient care was attractive. This is due to large-scale problems such as single point of failure, data privacy, and centralized stewardship healthcare data management systems. Blockchain's replication mechanism, privacy, and security features have a bright future in the healthcare industry since they can address several ingrained problems with the health management system. However, most of the recent blockchain studies in the healthcare industry have been concentrated on the permission-less Bitcoin network, which has issues including high energy consumption, limited scalability, delay-tolerance, and delay-sensitive data, traffic overhead, complexity, and low security.

8. Managerial Implications

Since healthcare research imposes gathering, storing, and usage of vast quantities of exclusively identifiable EHRs for individuals, which might be sensitive and potentially humiliating, protective and secure mechanisms for data are crucial.

If security is compromised, the people whose health information was improperly accessed risk a variety of negative outcomes. The mere fact that others are aware of private information makes the publication of that information potentially harmful.

The study demonstrates how blockchain technology may be used to boost the medical industry's overall performance and investigates the many issues and obstacles associated with using blockchain in the healthcare system.

The blockchain acceptance model might be empirically verified in later studies. The perceived utility and perceived usability of blockchain technology in comparison to other technologies require further study. The first and most important step in this direction is this study. Researchers might concentrate on every aspect of the blockchain and look at how it can give organizations and enterprises new chances. In the context of technology acceptance, the study may also serve as proof of the ability to draw knowledge from the collective intelligence of Twitter users.

We think that blockchain technology will be essential for Internet of Things applications. In today's research communities, blockchain technology innovations and their implementation in IoT applications to improve quality of life are hot subjects. However, before utilizing blockchain technology in IoT applications, there are a number of issues and required limitations that must be investigated and solved. This survey will help academics pinpoint and resolve problems related to developing and incorporating blockchain-based technologies for Internet of Things applications.

To more fully comprehend, define, and assess the value of blockchain technology in healthcare, further research is still required. As part of continuous attempts to address the issues of scalability, latency, interoperability, security, and privacy in relation to the usage of blockchain technology in healthcare, additional research is also required.

9. Future Directions

As a future direction, we will seek to analyze and investigate the adoption of blockchain in several other aspects of digital medical and healthcare use cases, such as the blockchain-based system for medical supply chain transparency, a blockchain-based system for patient-centric electronic health records, shared blockchain-based digital contract between manufacturers, distributors and healthcare organizations to reduce payment disputes claims), and a blockchain-based system for medical staff credential verification (to track the experience of trusted medical and healthcare professionals to rationalize the hiring process for healthcare organizations). Finally, it is worth exploring blockchain for a comprehensive end-to-end IoT security strategy for remote monitoring (Internet of Medical Things -IoMT).

Author Contributions: Conceptualization, A.O. and I.K.; methodology, A.O., and Q.A.A.-H.; software, A.O.; validation, A.O., I.K. and Q.A.A.-H.; formal analysis, Q.A.A.-H.; investigation, A.O. and I.K.; resources, A.O. and Q.A.A.-H.; data curation, I.K., and Q.A.A.-H.; writing—original draft preparation, A.O., I.K. and Q.A.A.-H.; writing—review and editing, A.O. and Q.A.A.-H.; visualization, Q.A.A.-H.; funding acquisition, I.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Not Applicable.

Acknowledgments: The authors sincerely acknowledge the Princess Sumaya University for Technology and the Researchers Supporting Program (TUMA-Project-2021-14), AlMaarefa University, Riyadh, Saudi Arabia, for supporting steps of this work.

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

Abbreviations

Abbreviation	Meaning
her	Electronic Health Records
BT	Blockchain technology
(DLT)	distributed ledger technology
(TTP)	trusted third-party
SHA	Secure Hash Algorithm
DL	Decentralized ledgers
IoT	Internet of Things
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
ERIC	Education Resources Information Center
HIPAA	Health Insurance Portability and Accountability Act
HER	healthcare electronic records
QSP	query service provider
CSP	certificate service provider
ASP	application service provider
RFID	Real-Time Location Systems
G	global control
PC	Personal Computer
KYC	know your Customer
ID	identification
NIDS	network intrusion detection system
IoMT	Internet of Medical Things
TUMA	Technology and the Researchers Supporting Program

References

1. Alammary, A.; Alhazmi, S.; Almasri, M.; Gillani, S. Blockchain-based applications in education: A systematic review. *Appl. Sci.* **2019**, *9*, 2400.
2. Rocha, G.d.S.R.; de Oliveira, L.; Talamini, E. Blockchain applications in agribusiness: A systematic review. *Future Internet* **2021**, *13*, 95.
3. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain technology in healthcare: A systematic review. *Healthcare* **2019**, *7*, 56.
4. Reegu, F.A.; Mohd, S.; Hakami, Z.; Reegu, K.K.; Alam, S. Towards trustworthiness of electronic health record system using blockchain. *Ann. Rom. Soc. Cell Biol.* **2021**, *25*, 2425–2434.
5. Makridakis, S.; Christodoulou, K. Blockchain: Current challenges and future prospects/applications. *Future Internet* **2019**, *11*, 258.
6. Alex, K.; Seema, S.; Subrata, C. Security and Privacy Challenges in Blockchain Application. In *The Data-Driven Blockchain Ecosystem: Fundamentals, Applications, and Emerging Technologies*; CRC Press: Boca Raton, FL, USA, 2022.
7. Ratta, P.; Kaur, A.; Sharma, S.; Shabaz, M.; Dhiman, G. Application of blockchain and internet of things in healthcare and medical sector: Applications, challenges, and future perspectives. *J. Food Qual.* **2021**, *2021*, 7608296.
8. Al-Haija, Q.A.; Alsulami, A.A. High Performance Classification Model to Identify Ransomware Payments for Heterogeneous Bitcoin Networks. *Electronics* **2021**, *10*, 2113.
9. Abbas, A.; Alroobaea, R.; Krichen, M.; Rubaiee, S.; Vimal, S.; Almansour, F.M. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. *Pers. Ubiquitous Comput.* **2021**, 1–14.
10. Dutta, P.; Choi, T.-M.; Somani, S.; Butala, R. Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transp. Res. Part E Logist. Transp. Rev.* **2020**, *142*, 102067.
11. Mettler, M. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–17 September 2016; pp. 1–3.
12. Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141.
13. Crosby, M.; Pattanayak, P.; Verma, S.; Kalyanaraman, V. Blockchain technology: Beyond bitcoin. *Appl. Innov.* **2016**, *2*, 71.
14. Michael, C.; Nachiappan, P.P.; Sanjeev, V.; Vignesh, K. Blockchain Technology: Beyond Bitcoin. Applied Innovation Review. Available online: https://www.appliedinnovationinstitute.org/blockchain-technology-beyond-bitcoin/ (accessed on 1 June 2022).

15. Kaci, A.; Rachedi, A. Toward a machine learning and software defined network approaches to manage miners' reputation in blockchain. *J. Netw. Syst. Manag.* **2020**, *28*, 478–501.
16. Abu Al-Haija, Q.; Smadi, A.A.; Allehyani, M.F. Meticulously Intelligent Identification System for Smart Grid Network Stability to Optimize Risk Management. *Energies* **2021**, 14, 6935. https://doi.org/10.3390/en14216935.
17. Nabben, K. Blockchain security as "people security": Applying sociotechnical security to blockchain technology. *Front. Comput. Sci.* **2021**, *62*, 599406.
18. Dubey, R.; Gunasekaran, A.; Bryde, D.J.; Dwivedi, Y.K.; Papadopoulos, T. Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting. *Int. J. Prod. Res.* **2020**, *58*, 3381–3398.
19. Manski, S.; Bauwens, M. Reimagining new socio-technical economics through the application of distributed ledger technologies. *Front. Blockchain* **2020**, *2*, 29.
20. Sunyaev, A. Distributed ledger technology. In *Internet Computing*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 265–299.
21. Guo, H.; Yu, X. A Survey on Blockchain Technology and its security. *Blockchain Res. Appl.* **2022**, *3*, 100067.
22. Justinia, T. Blockchain technologies: Opportunities for solving real-world problems in healthcare and biomedical sciences. *Acta Inform. Med.* **2019**, *27*, 284.
23. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* **2019**, *25*, 1398–1411.
24. Pillai, B.; Biswas, K.; Muthukkumarasamy, V. Cross-chain interoperability among blockchain-based systems using transactions. *Knowl. Eng. Rev.* **2020**, *35*, e23.
25. Bigini, G.; Freschi, V.; Lattanzi, E. A review on blockchain for the internet of medical things: Definitions, challenges, applications, and vision. *Future Internet* **2020**, *12*, 208.
26. Rahmani, M.K.I.; Shuaib, M.; Alam, S.; Siddiqui, S.T.; Ahmad, S.; Bhatia, S.; Mashat, A. Blockchain-Based Trust Management Framework for Cloud Computing-Based Internet of Medical Things (IoMT): A Systematic Review. *Comput. Intell. Neurosci.* **2022**, *2022*, 9766844.
27. Sharma, A.; Kaur, S.; Singh, M. A comprehensive review on blockchain and Internet of Things in healthcare. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4333.
28. Reegu, F.A.; Al-Khateeb, M.O.; Zogaan, W.A.; Al-Mousa, M.R.; Alam, S.; Al-Shourbaji, I. Blockchain-based framework for interoperable electronic health record. *Ann. Rom. Soc. Cell Biol.* **2021**, *30*, 6486–6495.
29. Nazir, S.; Ali, Y.; Ullah, N.; García-Magariño, I. Internet of things for healthcare using effects of mobile computing: A systematic literature review. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 5931315.
30. Bamakan, S.M.H.; Moghaddam, S.G.; Manshadi, S.D. Blockchain-enabled pharmaceutical cold chain: Applications, key challenges, and future trends. *J. Clean. Prod.* **2021**, *302*, 127021.
31. Makridakis, S.; Polemitis, A.; Giaglis, G.; Louca, S. Blockchain: The next breakthrough in the rapid progress of AI. *Artif. Intell.-Emerg. Trends Appl.* **2018**, *27*, 10.
32. Abunadi, I.; Kumar, R.L. Blockchain and business process management in health care, especially for COVID-19 cases. *Secur. Commun. Netw.* **2021**, *2021*, 2245808.
33. Bindlish, S.; Chhabra, S.; Mehta, K.; Sapra, P. Blockchain in Health Care: A Review. *Cyber Secur. Digit. Forensics* **2022**, *122*, 423–430.
34. Attaran, M. Blockchain technology in healthcare: Challenges and opportunities. *Int. J. Healthc. Manag.* **2022**, *15*, 70–83.
35. Reegu, F.; Daud, S.M.; Alam, S. Interoperability Challenges in Healthcare Blockchain System-A Systematic Review. *Ann. Rom. Soc. Cell Biol.* **2021**, *25*, 15487–15499.
36. Torres-Carrión, P.V.; González-González, C.S.; Aciar, S.; Rodríguez-Morales, G. Methodology for systematic literature review applied to engineering and education. In Proceedings of the 2018 IEEE Global Engineering Education Conference (EDUCON), Canary Islands, Spain, 17–20 April 2018; pp. 1364–1373.
37. Ahmad, A.; AbuHour, Y.; Younisse, R.; Alslman, Y.; Alnagi, E.; Abu Al-Haija, Q. MID-Crypt: A Cryptographic Algorithm for Advanced Medical Images Protection. J. Sens. Actuator Netw. **2022**, 11, 24. https://doi.org/10.3390/jsan11020024.
38. Tranfield, D.; Denyer, D.; Smart, P. Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *Br. J. Manag.* **2003**, *14*, 207–222.
39. Rother, E.T. Systematic literature review X narrative review. *Acta Paul. Enferm.* **2007**, *20*, v–vi.
40. Crowther, M.; Lim, W.; Crowther, M.A. Systematic review and meta-analysis methodology. *Blood J. Am. Soc. Hematol.* **2010**, *116*, 3140–3146.
41. Abunadi, I.; Kumar, R.L. BSF-EHR: Blockchain security framework for electronic health records of patients. *Sensors* **2021**, *21*, 2865.
42. Mbunge, E.; Batani, J.; Gaobotse, G.; Muchemwa, B. Virtual healthcare services and digital health technologies deployed during coronavirus disease 2019 (COVID-19) pandemic in South Africa: A systematic review. *Glob. Health J.* **2022**, *6*, 102–113.
43. Donawa, A.; Orukari, I.; Baker, C.E. I am scaling blockchains to support electronic health records for hospital systems. In Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 10–12 October 2019.
44. Patel, P.; Majumder, S.; Shevkar, S.; Shalu, H. EMRs with Blockchain: A Distributed Democratised Electronic Medical Record Sharing Platform. In Proceedings of the International Conference on Blockchain, Melbourne, Australia, 6–8 December 2021; pp. 16–26.

45. Fatokun, T.; Nag, A.; Sharma, S. Towards a blockchain assisted patient owned system for electronic health records. *Electronics* **2021**, *10*, 580.
46. Keshta, I.; Odeh, A. Security and privacy of electronic health records: Concerns and challenges. *Egypt. Inform. J.* **2021**, *22*, 177–183.
47. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *Neural Comput. Appl.* **2021**, *34*, 11475–11490.
48. Konapure, R.R.; Nawale, S.D. Smart Contract System Architecture for Pharma Supply chain. In Proceedings of the 2022 International Conference on IoT and Blockchain Technology (ICIBT), Ranchi, India, 6–8 May 2022; pp. 1–5.
49. Sohan, M.; Al, F.A.; Khan, S.R.; Anannya, N.J.; Ahad, M.T. Towards a secured smart IoT using light weight blockchain: An aim to secure Pharmacy Products. *arXiv* **2022**, arXiv:2206.06925.
50. Kamenivskyy, Y.; Palisetti, A.; Hamze, L.; Saberi, S. A Blockchain-Based Solution for COVID-19 Vaccine Distribution. *IEEE Eng. Manag. Rev.* **2022**, *50*, 43–53.
51. Kramer, M.P.; Bitsch, L.; Hanf, J.H. The Significance of Blockchain Governance in Agricultural Supply Networks. In *Sustainable Agricultural Value Chain*; IntechOpen: London, UK, 2022.
52. Almutairi, K.; Hosseini Dehshiri, S.J.; Hosseini Dehshiri, S.S.; Hoa, A.X.; Arockia Dhanraj, J.; Mostafaeipour, A.; Issakhov, A.; Techato, K. Blockchain Technology application challenges in renewable energy supply chain management. *Environ. Sci. Pollut. Res.* **2022**, *6*, 1–18.
53. Goyal, S.; Sharma, N.; Bhushan, B.; Shankar, A.; Sagayam, M. Iot enabled technology in secured healthcare: Applications, challenges and future directions. In *Cognitive Internet of Medical Things for Smart Healthcare*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 25–48.
54. Khan, S.N.; Loukil, F.; Ghedira-Guegan, C.; Benkhelifa, E.; Bani-Hani, A. Blockchain smart contracts: Applications, challenges, and future trends. *Peer-Peer Netw. Appl.* **2021**, *14*, 2901–2925.
55. Kumar, T.; Kaur, S. Blockchain Technology: Present and Future Perspectives. In *Applications, Challenges, and Opportunities of Blockchain Technology in Banking and Insurance*; IGI Global: Hershey, PA, USA, 2022; pp. 258–265.
56. Hussien, H.M.; Yasin, S.M.; Udzir, N.I.; Ninggal, M.I.H.; Salman, S. Blockchain technology in the healthcare industry: Trends and opportunities. *J. Ind. Inf. Integr.* **2021**, *22*, 100217.
57. Fang, H.S.A.; Tan, T.H.; Tan, Y.F.C.; Tan, C.J.M. Blockchain personal health records: Systematic review. *J. Med. Internet Res.* **2021**, *23*, e25094.
58. Arun Kumar, B. Developing Business-Business Private Block-Chain Smart Contracts Using Hyper-Ledger Fabric for Security, Privacy and Transparency in Supply Chain. In *Data Management, Analytics and Innovation*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 429–440.
59. Li, X.; Wang, Z.; Leung, V.C.; Ji, H.; Liu, Y.; Zhang, H. Blockchain-empowered data-driven networks: A survey and outlook. *ACM Comput. Surv.* **2021**, *54*, 1–38.
60. Akhter Md Hasib, K.T.; Chowdhury, I.; Sakib, S.; Monirujjaman Khan, M.; Alsufyani, N.; Alsufyani, A.; Bourouis, S. Electronic health record monitoring system and data security using blockchain technology. *Secur. Commun. Netw.* **2022**, *2022*, 2366632.