big data and cognitive computing

MDPI

Systematic Review

Medical IoT Record Security and Blockchain: Systematic Review of Milieu, Milestones, and Momentum

Simeon Okechukwu Ajakwe [1,*,†], Igboanusi Ikechi Saviour [1], Vivian Ukamaka Ihekoronye [2], Odinachi U. Nwankwo [2], Mohamed Abubakar Dini [2], Izuazu Urslla Uchechi [2], Dong-Seong Kim [2,†] and Jae Min Lee [2,†]

[1] Information and Communication Technology Convergence Research Centre, Kumoh National Institute of Technology, Gumi 39253, Republic of Korea; ikechisaviour@kumoh.ac.kr
[2] Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi 39253, Republic of Korea; ihekoronyevivian@gmail.com (V.U.I.); odinachifoot@gmail.com (O.U.N.); m.raji202010@gmail.com (M.A.D.); uursla8@gmail.com (I.U.U.); dskim@kumoh.ac.kr (D.-S.K.); ljmpaul@kumoh.ac.kr (J.M.L.)
* Correspondence: simeon.ajakwe@kumoh.ac.kr
† These authors contributed equally to this work.

Abstract: The sensitivity and exclusivity attached to personal health records make such records a prime target for cyber intruders, as unauthorized access causes unfathomable repudiation and public defamation. In reality, most medical records are micro-managed by different healthcare providers, exposing them to various security issues, especially unauthorized third-party access. Over time, substantial progress has been made in preventing unauthorized access to this critical and highly classified information. This review investigated the mainstream security challenges associated with the transmissibility of medical records, the evolutionary security strategies for maintaining confidentiality, and the existential enablers of trustworthy and transparent authorization and authentication before data transmission can be carried out. The review adopted the PRSIMA-SPIDER methodology for a systematic review of 122 articles, comprising 9 surveys (7.37%) for qualitative analysis, 109 technical papers (89.34%), and 4 online reports (3.27%) for quantitative studies. The review outcome indicates that the sensitivity and confidentiality of a highly classified document, such as a medical record, demand unabridged authorization by the owner, unquestionable preservation by the host, untainted transparency in transmission, unbiased traceability, and ubiquitous security, which blockchain technology guarantees, although at the infancy stage. Therefore, developing blockchain-assisted frameworks for digital medical record preservation and addressing inherent technological hitches in blockchain will further accelerate transparent and trustworthy preservation, user authorization, and authentication of medical records before they are transmitted by the host for third-party access.

Keywords: blockchain; data; digital certificate; health care; medical record; 5G; security

Citation: Ajakwe, S.O.; Saviour, I.I.; Ihekoronye, V.U.; Nwankwo, O.U.; Dini, M.A.; Uchechi, I.U.; Kim, D.-S.; Lee, J.M. Medical IoT Record Security and Blockchain: Systematic Review of Milieu, Milestones, and Momentum. *Big Data Cogn. Comput.* **2024**, *8*, 121. https://doi.org/10.3390/bdcc8090121

Academic Editor: Domenico Ursino

Received: 2 August 2024
Revised: 1 September 2024
Accepted: 6 September 2024
Published: 12 September 2024

1. Introduction

Disruptive technologies and advancements in generational networks have driven digital transformations across various fields, including health care, where critical and sensitive patient medical records are transmitted in real-time across different terminals. Medical IoT Records (MIRs) refer to personalized digital health information generated from various interconnected devices through health information systems. MIRs include a wide range of data, such as a patient's personal information (security numbers, credit card details, phone numbers, etc.); demographic data; medical history; laboratory test results; and other essential, intangible information [1]. However, the transition from automation to interconnection; personalization; intelligentization; and real-time application in delivering effective, patient-centered health care is limited by several security challenges.

Information is a valuable asset in the digital, data-driven cyberspace (DDDC), and unauthorized access to an individual's health status by a third party can be a powerful tool to harm, discredit, or damage that person's reputation. Therefore, the sensitivity of such highly classified documents necessitates multilateral and bi-directional authentication and authorization between the information owner and its stored location before access for viewing or transmission is granted. Unauthorized transmission or examination of classified and sensitive information, such as health or medical records, by a third party constitutes a breach of trust by the host and is a crime punishable under medical and Information Technology (IT) laws and policies [2].

Over time, there have been numerous cases of unauthorized exposure and transmission of medical records, leading to various court litigations. In response, several innovative approaches, particularly the use of digital certificates (DCs), have been proposed to enhance the preservation and privacy of medical records, aiming to prevent unauthorized access [3–8]. Each of these proposed DC methods has its unique features, advantages, and drawbacks, which introduce certain limitations. Despite these commendable efforts, the ongoing challenge in securing medical records still lies in ensuring effective ownership authorization before the host transmits such highly sensitive data to any other user for access.

Numerous surveys and case studies on the preservation of the privacy of medical IoT (Internet of Things) records have been conducted to address the issue of ownership authorization [9–16], as summarized in Table 1. However, these surveys do not thoroughly address the latest and emerging security concerns related to the transmission, authentication, and preservation of medical records, nor do they emphasize the crucial role of blockchain technology in enhancing patient data privacy and security. Blockchain technology provides a secure, decentralized, and tamper-resistant platform for storing and transmitting sensitive data, with the potential to revolutionize data security in the healthcare sector [17]. There are various innovations and practical applications of blockchain in improving the security of medical record preservation and transmission, as depicted in Figure 1. With increasing global investment in and demand for seamless e-healthcare delivery [18], which requires the continuous flow of user data among involved parties, it is essential to explore the development of security technologies that ensure data privacy and confidentiality. Despite advancements in disruptive technologies and cybersecurity frameworks, recent incidents of misuse and unauthorized access to health-related data have been documented [19–22].

Figure 1. Applications and use cases of blockchain technology in medical record preservation.

This review explored and addressed current security challenges related to the preservation, authorization, and authentication of medical IoT records before they are accessed or transmitted through a thorough examination and detailed analysis of existing literature.

The specific contributions of this review are summarized as follows:

- We conducted an empirical examination of the transcending evolution of digital certificates for medical record preservation.
- We assessed the adoption of blockchain technology in enhancing data privacy in medical record transmission.
- We closely explored the significant impact of cybersecurity and generational networks in exposing sensitive and vital health records for unauthorized access.

- We highlighted security issues and provided advanced research directions for the improvement of medical record privacy and preservation by incorporating blockchain technology and allied security frameworks.

Section 2 summarizes the adopted review methodology, while Section 3 highlights the transcending dynamics of medical digital certificates for medical IoT record authentication. Section 5 presents case studies of artificial intelligence and blockchain applications with the aim of ascertaining medical record security. Section 4 closely examines advanced cybersecurity technologies and approaches in terms of providing medical data preservation. Section 6 explores the next-generation and network-related security issues associated with secured medical record transmission. Finally, Section 7 hints at the alignment of the security and sustainability of privacy preservation for medical IoT records and concludes the paper with engaging insights on future research directions. Figure 2 provides the study map of this review at a glance.

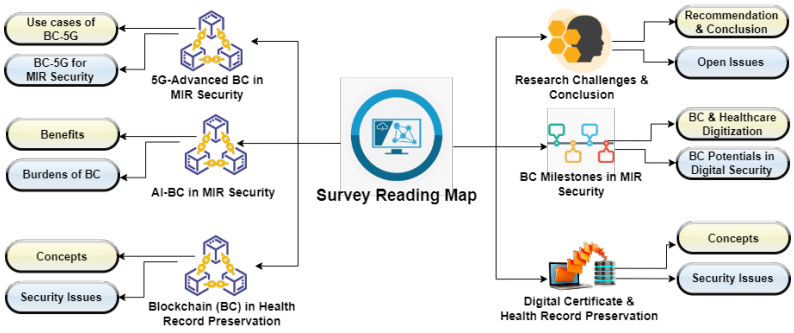
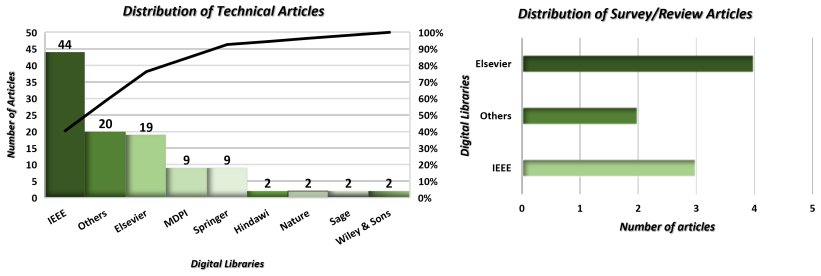


Figure 2. The survey reading map highlighting the important sections.

2. Review Methodology

To achieve an exhaustive review with improved qualitative analysis, enhanced article selection sensitivity, and specificity, this review adopted both the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) [23] and the Sample population, Phenomenon of Interest, Design of Study, Evaluation, Research (SPIDER) [24] qualitative review methodology.

The *sample population* of documents used in this study comprises articles and conference proceedings from reputable digital repositories. Online reports were also included via the chain-referral sampling method. Initially, a preliminary search of 354 documents was conducted, which was subsequently streamlined to 122 articles (9 surveys, 4 online reports, and 109 technical papers) based on the article selection, exclusion, and inclusion criteria, as summarized by the review article distribution statistics presented in Figure 3.



Distribution of Reviewed Articles

Types of Articles Used	Quantity
Survey/Review	9
Technical Articles	109
Online Reports	4
Total Reviewed Articles	**122**

Figure 3. Distribution of articles used for quantitative and qualitative analysis.

In total, 10 digital libraries (see Figure 4) were searched, namely Elsevier, Hindawi, IEEE, MDPI, Nature, Sage, Springer, Wiley & Sons, and others (Researchgate, PeerJ, NIH, etc.) for surveys and technical papers. At the same time, different online reports were accessed using snowballing.

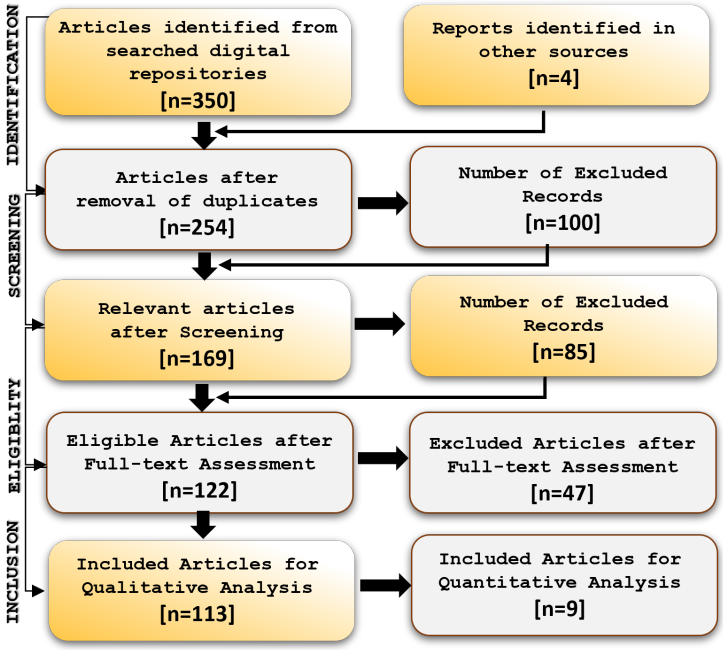


Figure 4. The PRISMA/SPIDER strategy for article gathering, screening, eligibility, and inclusion.

The *phenomenon of interest* used for exhaustive search of repositories includes keywords such as "medical record" and "preservation" or "medical record" and "security", "medical record" and "blockchain", "health record" and "security", "health record" and "blockchain", "health record" and "preservation", etc. These keywords were chosen to reflect the participants, interventions, comparators, outcomes, and study design/limitations (PICOS) strategy to meet the review scope and objective, as well as to give room for heterogeneity in article selection.

The *design of study* used in this review for article gathering, screening, and eventual inclusion is summarized by Figure 4. After the preliminary screening of identified articles, duplicates were excluded. Thereafter, each article was screened for relevance, and eligibility criteria were applied to determine its inclusion or exclusion based on a full-text assessment. The *evaluation and research type* criteria for article inclusion, exclusion, and eligibility are summarized as follows:

1. Articles published in reputable journals and conference proceedings;
2. Articles published in the English language;
3. Articles with publication dates within the last 10 years (2013–2023);
4. Articles with titles and contents covering the stated review scope and objectives.

In total, 9 articles were used for qualitative analysis, and 113 articles were used for quantitative analysis. A summary of related reviews in comparison with this study is highlighted in Table 1, justifying the relevance of this study.

Table 1. Comparison of related surveys on blockchain adoption for medical record security.

Year	Ref.	Database	Target Area/Focus	Major Findings	Survey	Case Studies
2009	[9]	×	Preservation of patient medical records	Basic electronic record techniques	×	✓
2011	[3]	×	Digital certificate using PGP	Digital certificate techniques	✓	✓
2019	[10]	×	Patient privacy perspective toward HIE	Privacy policies	✓	✓
2019	[12]	×	Medical data-sharing schemes	Data-sharing approaches	✓	✓
2021	[11]	×	Real-world development challenges of BC	Broad spectrum of blockchain technologies	×	✓
2021	[13]	✓	Privacy preservation and security of health care	Privacy issues in health care	✓	✓
2021	[14]	×	Blockchain network solutions	Blockchain solutions in health care	✓	✓
2021	[15]	×	IoT and blockchain technology-based SWOT	Blockchain in medical IoT devices	✓	✓
2021	[16]	×	BC applications	Adaptive and simultaneous response	✓	✓
2022	[25]	×	BC in medical systems	Audit control and lightweight issues	✓	✓
2022	[26]	×	Healthcare privacy issues in BC	Adaptability and flexible application concerns	✓	✓
2023	[27]	×	BC in health care	Security and application issues	✓	✓
2024	Ours	✓	Blockchain for medical IoT record security	Reliable digitization is BC+AI+Metaverse	✓	✓

3. Digital Certificate and Evolution of Medical Data Preservation

Medical IoT Records (MIRs), a subset of electronic medical records (EMRs), have revolutionized the healthcare sector by making patient data more accessible, improving accuracy, and reducing the likelihood of errors. However, the use of digital technology also introduces privacy and security concerns, especially when handling sensitive medical information. A digital certificate (DC) is a document that utilizes a combination of public and private-key encryption to verify the identity of an individual, device, or organization [28]. Over the years, DCs have been crucial in ensuring the security, privacy, and authenticity of electronic records [29]. They help secure the transmission of data between healthcare providers and patients, and they also verify the authenticity of electronic medical records, protecting against cyber threats and data breaches in the healthcare sector. This ensures that sensitive information is accessible only to authorized individuals. A typical DC includes details such as the certificate owner's name; the certificate's serial number; its expiration date; a public key linked to the certificate owner; and a digital signature from the issuing authority, which confirms the certificate's authenticity.

Digital certificates (DCs) are typically issued by Certification Authorities (CAs) accredited by the Health Information Trust Alliance (HITRUST) [30]. HITRUST is a non-profit organization that establishes standards and best practices for the protection of sensitive healthcare data. The evolution of digital certificate technology reflects the continuous efforts to enhance security and privacy in the preservation of medical IoT records (MIRs). Table 2 outlines various digital certificate methods used to safeguard patient health records.

Table 2. Digital certificate approaches for privacy preservation of medical record data.

Sno.	Ref.	Technology	Description
1.	[3]	Pretty Good Privacy (PGP)	Combines data compression, symmetric-key cryptography, and public-key cryptography.
2.	[4]	Simple Distributed Security Infrastructure (SDSI)	A self-signed, decentralized DC that does not require a CA for authenticity but is very fragile to forgery.
3.	[5]	Public-Key Cryptography (PKC)	A mathematical DC approach that uses a pair of private and public keys to ensure encryption and privacy.
4.	[6]	Digital Signature Algorithm (DSA)	An algorithm that increases authentication security by increasing the difficulty of solving discrete logarithm problems.
5.	[31]	Secure Hash Algorithm (SHA)	Widely used in combination with PKI and DSA to increase data encryption.

Pretty Good Privacy (PGP) is a software program used for data encryption and decryption that enhances the security of digital files by combining data compression, symmetric-key cryptography, and public-key cryptography with the latest version being PGP 3. This added security creates additional challenges for intruders trying to access the contents of a patient's record. PGP does not establish a fixed port number between the client and server, preventing intruders from easily accessing the connection. To intercept and modify data, intruders must guess the correct port number [3]. Although PGP is widely used in various applications, it has limitations in key management. PGP relies on a web-of-trust model, which requires users to verify the identities of their contacts and establish trust before exchanging encrypted messages. This process can be time-consuming and impractical, especially for users needing to exchange encrypted messages with many individuals. As a result, there has been a decline in the use of PGP key servers [32].

Similarly, the Simple Distributed Security Infrastructure (SDSI) was developed to tackle the challenges associated with large-scale Public-Key Infrastructure (PKI) deployment [4]. The core concept of SDSI is to allow users to create and manage their own digital certificates without depending on a centralized certificate authority, removing the need for a trusted third party, which can be costly and difficult to manage on a large scale. In SDSI, digital certificates are self-signed and can form a web of trust, where users can verify the authenticity of each other's certificates by checking signatures from other trusted users. SDSI has made a significant impact on digital certificate technology and PKI, influencing modern PKI solutions. However, its main drawback is the lack of a certificate revocation mechanism [33], which can lead to security risks when certificates are compromised or when participant authorizations are revoked.

Additionally, Public-Key Infrastructure (PKI) was introduced as a digital certificate security architecture to enhance the security of data exchanged within a network [5]. PKI utilizes a mathematical method known as public-key cryptography, which employs a pair of related cryptographic keys—one public and one private—to verify the sender's identity (through signing) and/or ensure privacy (by encrypting data) [5]. The public key is used to encrypt messages, while the private key is used for decrypt them, enabling secure communication between parties. PKI technology is regarded as the foundation of digital certificate technology. However, a notable limitation of public-key cryptography (PKC) is its significant computational demands, resulting in slower performance and longer processing times compared to symmetric-key cryptography [34]. As a result, PKC may not be the best option for applications requiring real-time performance or high-speed processing.

To ensure an effective method for attaching and verifying digital signatures to digital certificates, the Digital Signature Algorithm (DSA) was developed. DSA was introduced as a standardized approach for signing electronic documents and messages to ensure authenticity, integrity, and non-repudiation [35]. The security of DSA is based on the

difficulty of solving the discrete logarithm problem, which makes it a reliable method for generating and verifying digital signatures [6]. DSA is widely utilized in the healthcare sector to securely sign digital certificates. However, the use of smaller key sizes in DSA compared to other public-key algorithms increases its susceptibility to cryptographic attacks [36].

Lastly, the Secure Hash Algorithm (SHA) was developed as a set of cryptographic hash functions designed to generate a fixed-size hash value from a piece of data [31]. These hash functions are commonly used in various applications, including password protection, secure protocols, and digital signatures. The hash function processes an input of an arbitrary length and produces a fixed-length output [7]. SHA is frequently used in conjunction with other technologies, such as PKI and DSA. Although SHA is widely regarded as secure for many applications, it is not entirely immune to certain types of attacks. These include collision attacks (where two different inputs produce the same output hash) [37], length extension attacks (where an attacker can extend the hash output without knowing the original input) [38], and quantum computing attacks (which use quantum computers to challenge cryptographic systems that are currently considered secure) [39].

The application of digital certificates for the preservation of medical data encounters various challenges related to privacy, security, and management. However, recent technological advancements, including artificial intelligence (AI) and blockchain, offer promising solutions to these issues and enhance the security of MIRs [40,41]. AI can be utilized for sophisticated encryption and security management, while blockchain provides a decentralized and secure method for storing medical data [42]. The integration of AI and blockchain has the potential to elevate security and privacy levels for medical data, ensuring that sensitive information is safeguarded while allowing authorized access as needed. These advanced technologies offer significant potential for the future of medical data preservation, introducing a more secure approach to managing medical records [43]. Examining blockchain technology and its unique features helps to highlight the advancements in the preservation of secure digital healthcare data.

4. Blockchain Adoption for Health Record Security

Blockchain technology can revolutionize the health sector via the introduction of secured algorithms to manage patients' confidential health records [44]. According to IBM, 70% of healthcare executives are optimistic about the advantageous impact the integration of blockchain technology will make in the health sector, especially on the provision of distributed and transparent architectures for the dissemination of EMRs [45]. The processing of medical data and patient records is essential for the analysis of previously prescribed medicines and understanding the severity of prior ailments in a patient [46]. In essence, trustworthy systems that are tamper-proof and immutable should be utilized to store, secure, and disseminate health information appropriately. Consequently, privacy and security are serious concerns with respect to the maintenance of patients' confidential data in the health domain. Thus, blockchain technology enhances the healthcare system through improved transparency and privacy among patients and practitioners, despite inherent shortcomings.

The global COVID-19 pandemic has heightened the need for digital certificates in the healthcare sector. While centralized databases, cloud-based storage, and hybrid storage (a mix of centralized and cloud solutions) have been used to effectively store Medical IoT records (MIRs), these methods often fall short in terms of interoperability and security, highlighting the need for enhancements [47]. MIR interoperability refers to the ability to share patient health records across various healthcare systems with different hardware and software and to access this information easily despite system differences. Furthermore, the scale at which MIR data breaches occur calls for more stringent measures to ensure data privacy. Blockchain technology offers a solution by enabling the storage of digital health certification issuers and receivers, along with document signatures (hashes), in a secure database ledger (blockchain) distributed across the blockchain network. Using

blockchain for digital health certificates provides benefits such as easy validation, efficient verification, transparency, effective traceability, and strong security [47]. Recent research has explored various advanced blockchain applications to enhance the security of health records, emphasizing the importance of selecting the appropriate blockchain network type for system deployment.

4.1. Blockchain Network Types

Blockchain networks can broadly be categorized into the following three types: public, private, and consortium blockchain networks. Each type focuses on different environments and accesses.

4.1.1. Public Blockchain

This method uses a public, decentralized blockchain network where every user can access the same data. Public health records are well suited for this kind of blockchain, which enables a safe, impenetrable, and transparent method of managing and storing health data. To achieve secured management of medical information in the IoT, the authors of [48,49] proposed the use of the IoT to produce, preserve, and authenticate healthcare certificates. The authors of [48] proposed PA, which creates and verifies medical certificates by acting as a communication medium between the backend blockchain network and application entities such as hospitals, patients, doctors, and IoT devices. It also ensures different security characteristics, such as secrecy, authentication, and access control, through the use of smart contracts. Although accidents involving personal medical information can occur on the server, they are more common during information sharing and data transmission [49]. As a result, blockchain technology is used to increase the trustworthiness of such personal information management systems. This study used the blockchain-based Internet of Things to enable intelligent healthcare that incorporates blockchain technology.

Nonetheless, the decentralized architecture of a public blockchain potentially introduces privacy concerns. As medical records stored using this system would be accessible to the public, compromising the health records of patients is highly possible [47]. Furthermore, owing to the large number of nodes in a public blockchain network, the transactional time needed to access health records may be slower than on a private blockchain, making such public networks unsuitable during emergency situations [50].

4.1.2. Private Blockchain

Private blockchain networks limit stakeholders' participation by granting permissions specifically to a limited group of individuals in the network. As a permissioned type of blockchain with restricted and trusted entities, a private blockchain offers a more efficient consensus approach due to the limited number of nodes validating transactions in the network. To ensure an easy verification process for digital health certificates and strict supervision of the entities generating and validating digital certificates, the authors of [47] proposed the use of a proxy re-encryption (PRE) service that aids patients in the sharing of their private data using a hierarchical private blockchain system. Although the PRE concept is a public-key encryption approach that provides functionality for encrypted data to be shared with third parties, the threshold scheme proposed by these authors prevents the unapproved conversion of encrypted patient data by third parties. In addition, to ensure the protection of sensitive medical records of patients and the control of digital health certificates, ref. [51] integrated a private blockchain-based system controlling access by both authorized and unauthorized actors, citing the health sector in Morocco as a case study. The Ethereum blockchain platform enables only authorized parties to access and verify the complete sensitive data of patients, thereby eliminating attempts at data forgery and tampering.

The authors of [52] offered an IoT–blockchain integration architecture based on EVM blockchain infrastructure and a rich–thin client IoT strategy to address the issues posed by constrained IoT resources when implementing Blockchain mining in IoT systems. The

architecture is determined by how the resources' loads are distributed. Thin clients are devices with limited resources, whereas rich clients have more resources. Both types of client can access the blockchain and collect data, but only rich clients can perform mining operations. This kind of combination helps strengthen an IoT-based blockchain network.

Other authors applied blockchain to secure life and property in healthcare environments [53] in order to facilitate the use of unmanned aerial vehicles (or drones) and provide coordinated access to the airspace. Malicious attackers can easily launch a number of attacks, including replay, man-in-the-middle, impersonation, and privileged insider attacks because the communication between the deployed drones and their ground station server is wireless. In the IoD environment, implementing strong authentication, access control, and key management protocols is crucial to defending against such assaults. Moreover, the blockchain method is strengthened against many kinds of assault when combined with authentication.

However, the major limitation of private blockchains with respect to MIRs, apart from scalability and centralization issues, is interoperability [54]; that is to say, private blockchains may pose incompatibility bottlenecks with other blockchain networks and/or healthcare providers, thereby hindering collaboration with prospective stakeholders. The centralized nature of this type of blockchain makes also the network vulnerable once the central authority is compromised [55].

4.1.3. Consortium Blockchains

The consortium blockchain approach merges the advantages of public and private blockchains to create a more flexible solution. For example, a hybrid blockchain in the healthcare sector might feature a private component for sensitive data and a public component for general health information. All stakeholders agree on a set of rules, which are enforced by a consensus algorithm. To address trust and privacy issues related to medical data, certain authors proposed a hybrid blockchain-based framework for the sharing of electronic health records (EHRs), incorporating various sharing mechanisms while ensuring interoperability and efficiency across different medical organizations. The HB-EMRS framework utilizes both off-chain and on-chain storage and includes smart contracts to connect all participants within the consortium. Access to confidential data is restricted to authorized organizations only. Additionally, HB-EMRS employs both permissionless and permissioned blockchains to facilitate effective and efficient EHR sharing. Similarly, in [56], a hybrid blockchain named HonestChain was introduced, which fosters trustworthy and incentive-based collaboration between organizations accessing and providing healthcare records. Within this consortium, requesters (those requesting health records) and providers (those supplying health records) are treated as peers and are assigned reputation scores based on their contributions. These reputation scores help mitigate challenges related to loss of value and missed opportunities, thereby improving access to protected data.

The authors of [57] proposed a consortium blockchain-based medical data-sharing program, concentrating on privacy protection and medical data-sharing concerns. To implement medical record access regulations on the consortium blockchain network and keep encrypted medical records off-chain, they developed a hybrid storage mode specifically for patients. It is possible to implement access permission control and access history tracking by utilizing blockchain technology and smart contracts.

Although implementing the consortium blockchain approach ensures data integrity and enables the secure dissemination of MIRs among authorized nodes, the limited accessibility offered by such networks is a major challenge. In a situation where a consortium blockchain is employed to use incentives to encourage the participation of patients in sharing medical health data and for healthcare administrators to adopt the system, blockchain currency, such as Ether or Bitcoin, is provided as incentives for transaction fees and mining activities. There is no doubt that such an incentivized approach will introduce inequity in an emergency scenario [58].

4.2. Blockchain Consensus Algorithms

A consensus algorithm is a procedure that is used in distributed ledger systems and blockchains to get numerous participants (or nodes) to agree on the system's current state. Despite possible faults or malevolent actors, its main job is to guarantee that every node in the network agrees on a single version of the blockchain or ledger [59,60]. There are several consensus algorithms, but we focus on the five that are most widely used.

4.2.1. Proof of Work (PoW)

Users invest computational effort in solving a mathematical problem before transactions are sent. The Proof of Work (PoW) technique was first developed to stop spam attacks [61]. The first time a Byzantine fault-tolerant consensus method was used in a public blockchain network was when Satoshi Nakamoto introduced proof of work (PoW) into the Bitcoin system [62]. PoW uses a competition amongst blockchain nodes to solve a mathematical problem; the first node to solve it gets to add a block to the chain and receive rewards. Nodes use certain techniques to calculate nonce values to reach a network goal [61]. If it is successful, the node broadcasts the block so that others can verify it. PoW has some disadvantages, such as high computational costs, lengthy consensus times, and low transaction throughput, although it can be considered one of the most secure consensus methods [63].

4.2.2. Proof of Stake (PoS)

In 2011, the Proof of Stake (PoS) method was presented as a solution to the high computing costs and inefficiencies of the proof of work (PoW) algorithm [61]. It was initially incorporated into digital currency Peercoin. In contrast to proof of work (PoW), which uses processing power to verify transactions, proof of stake (PoS) chooses accounting nodes according to the quantity and duration of tokens they own. A larger stake increases a node's likelihood of validating transactions and earning rewards, which lowers the complexity of the "mining" process, speeds up block and transaction processing, and increases consensus efficiency. Its disadvantages include the possibility of lowering user engagement by rewarding nodes with higher stakes, which can lower overall blockchain activity.

4.2.3. Delegated Proof of Stake (DPoS)

The representative election method and the Delegated Proof of Stake Algorithm are comparable. Each node in the system is given a certain amount of votes based on the quantity of currency it possesses [61]. Nodes that they deem more trustworthy are chosen by voting to serve as decision makers in the consensus process. Multiple decision makers are assigned based on the number of votes received, and decision makers alternate when obtaining the accounting rights of the block. Any node inside the system has the potential to make decisions. The decision-making identity is canceled if the present decision maker violates the blockchain protocol. To expand the group of decision makers, the system assigns additional members. The accounting rights are not overly focused on one node, thanks to the multi-decision-maker method, which can stop over-centralization. The benefits of the PoS and PoW algorithms are combined in the DPoS algorithm. DPoS consensus allows for speedier communication between nodes. This allows nodes to finish block packaging, broadcasting, and verification quickly, which greatly improves system transaction throughput. Because DPoS does not rely on computer resources, it uses less energy. The system's transaction processing speed increases dramatically and the system's transaction delay decreases as a result of the election of decision makers. Simultaneously, it allows a large number of nodes to easily enter and quit the blockchain system. Its scalability is strong, and changes in node size have little to no impact on the system's performance.

4.2.4. Proof of Authority (PoA)

Instead of depending on computing power or stake, the Proof of Authority (PoA) blockchain consensus algorithm uses a group of pre-approved, reliable validators to safe-

guard the network [64]. PoA depends on the authority and reputation of a small group of reliable entities to authenticate transactions and create new blocks, in contrast to proof of work (PoW) and proof of stake (PoS), which use competitive methods. In a proof-of-authority network, validators are selected according to their identity and reliability, which streamlines the consensus procedure and increases transaction speed and throughput. PoA can, however, also increase the risk of centralization because the reliability of the chosen authorities is crucial to the security and integrity of the network. PoA is especially well-suited for private or consortium blockchains, where members have built trust and aim to strike a compromise between efficiency and security, notwithstanding these reservations.

4.2.5. Practical Byzantine Fault Tolerance (BFT)

With this method, a consensus is attained when more than two-thirds of the nodes have a positive opinion of the block. All nodes are required to participate in the voting process to add the next block. One-third of the platforms' typical activity does not harm the PBFT. This makes reaching a consensus quicker and more cost-effective than using proof of work. Furthermore, this approach does not require any asset to be staked for the consensus process, in contrast to proof of stake [65].

4.3. Blockchain Smart Contracts

Blockchain smart contracts are self-executing contracts that have the conditions of the deal explicitly encoded into their code. Smart contracts are implemented on a blockchain network that, upon the fulfillment of predetermined criteria, automatically enforces and carries out the contractual terms. Because of this automation, there is no longer a need for middlemen, which reduces the possibilities of fraud and human error. Since changes cannot be made once a contract is launched, smart contracts function on decentralized networks, which guarantee the transparency and immutability of the contract conditions. They can make procedures more effective and economical by facilitating, confirming, and enforcing a variety of agreements, from financial transactions to supply chain management. Through the utilization of blockchain's innate security characteristics, smart contracts provide a reliable means of carrying out and documenting transactions in an impenetrable fashion. To ensure they function as intended and eliminate vulnerabilities, they also need to be carefully coded and audited [66].

Several solutions involving the use of smart contracts have been proposed in the medical domain. The authors of [67] used a smart contract to secure the sharing of health data for a mobile cloud-based e-health system. The authors of [68] used a smart contract for organ matching and waiting list management. The authors of [66] used smart contracts as a smart healthcare system for medical records. Interesting applications of smart contracts have also been reported outside the health domain, such as in the access control [69], finance [70], and other domains.

4.4. Summary of Blockchain for Medical IoT

The choice of network type (public, private, or consortium) and the accompanying consensus algorithm depends on the environment and the priority behavior desired in the network (decentralization, speed, energy efficiency, scalability, etc.). The uses of IoT and blockchain in health care cut across patient data sharing, security of the healthcare environment, management of algorithmic processes using smart contracts, and secure communication among hospital equipment.

5. AI–Blockchain Integration in Medical IoT Record Security

The adoption of major enabling technologies, including the Internet of Things (IoT), artificial intelligence (AI), blockchain, and next-generation wireless networks (5G/6G), has led to a significant shift in the healthcare industry [71]. Introducing these technologies in the healthcare sector has enhanced patient care and quality of life [72,73]. A succinct

discussion on the use cases of blockchain technology and allied technologies in the medical sector is presented forthwith.

5.1. Traceable Data and Security

Blockchain technology offers a safe, decentralized, and tamper-proof platform for storing and transmitting sensitive data, with the potential to revolutionize data security in the healthcare sector. The use of encryption to secure data is one of the main advantages of adopting blockchain technology for healthcare data security [74]. Blockchain makes it challenging for unauthorized parties to access or modify a patient's data recorded on a private or public network without being traced. As a decentralized security network, there is no single point of control or failure in a blockchain, which reduces the risk of data breaches [75]. The capacity to securely and effectively transmit information between numerous parties is another advantage of utilizing blockchain in health care. To increase collaboration and patient outcomes, healthcare providers can, for instance, use blockchain to securely send patient records to one another. Blockchain technology can also be used to confirm the legitimacy of pharmaceuticals, medical gadgets, and other products [16], which is important in tracing the genuineness of both outpatient and inpatient drug prescription and administration, especially for forensic analysis, autopsy, and drug security auditing. This can also aid in preventing the entry and circulation of fake pharmaceutical products onto the market, which could have detrimental effects on patient safety. Finally, the automation of numerous healthcare operations (see Figure 5), including claims processing and medicine supply chain management, is possible thanks to smart contracts (SCs) on the blockchain [42,43]. The deployment of SCs has been shown to result in a relative reduction in the possibility of fraud and boosted productivity in health information management systems, as well as the healthcare sector at large [76]. Overall, even though there are still many obstacles to be cleared, using blockchain in healthcare has the potential to significantly increase data security and offer a more reliable and effective healthcare system to all stakeholders.

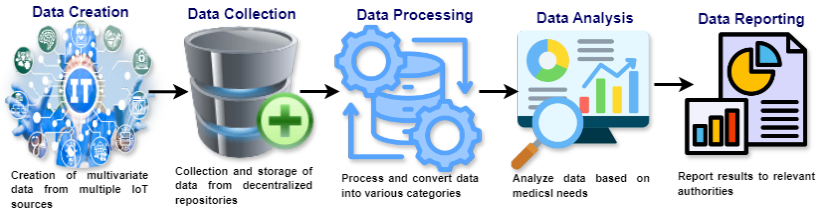


Figure 5. Current status of clinical trials, highlighting the various processes and phases involved.

5.2. Transparent Clinical Trials and Medical Reportage

Blockchain technology has the potential to enhance the transparency, effectiveness, and security of clinical trial operations, which have remained consistent issues in clinical experiments and findings [77]. The capacity to safely store and distribute trial data is one of the main advantages of adopting blockchain in clinical trials. Information on patient recruitment, the trial protocol, patient consent forms, and the outcomes may be included [78]. All parties engaged in a trial may trust the data because of the blockchain's decentralized and immutable structure, which keeps them safe from alteration [79,80]. Additionally, by making trial data available to the public, blockchain technology can assist in increasing the transparency of clinical studies. The legitimacy of verdicts can be improved, and the public's belief in the judicial process can grow as a result. Blockchain-based patient registries are another possible use case for the technology in clinical trials. This may offer a safe environment for patients to take part in several trials, easing the administrative strain on trial staff and facilitating the development of huge, diversified patient databases [81]. There are still many challenges to be addressed for the successful alignment of blockchain technology and clinical trials, such as the need for the integration of regulatory frameworks and standardization among industry associations [82], the right

combination of artificial intelligence (AI) models and big data [83], the promotion of unified data standards [82], etc. However, the use of blockchain in clinical trials has the potential to significantly enhance the trial process and eventually benefit both patients and the healthcare sector as a whole [84,85].

5.3. Tractable Supply Chain Management

There is a significant intersection between medical supply chain management and blockchain technology with respect to securing medical IoT records. The medical supply chain encompasses all the stages involved in producing, distributing, and delivering medical products and services from suppliers to end users [86]. Blockchain, as a digital ledger technology, can enhance the accountability, security, and transparency of supply chain operations, particularly in protecting patient information generated by various connected medical devices [87]. Managing the medical supply chain is challenging due to the need for regulatory compliance, traceability, and patient safety [88]. Blockchain technology can provide a secure and transparent method to track products and verify their authenticity, thereby supporting patient safety and reducing the risk of counterfeit pharmaceuticals or medical devices entering the supply chain [88]. Additionally, blockchain can secure medical IoT records by offering a decentralized platform for the management of patient data, providing a safe, transparent, and efficient way to monitor and control the movement of medical supplies and related information, which can also serve as metadata for advanced analytics [89].

One of the key advantages of integrating blockchain into the healthcare supply chain is improved traceability [90] as highlighted in Figure 6. By using blockchain to track the movement of goods from manufacturers to end users, it becomes easier to quickly identify the origin of issues, such as counterfeit drugs or contaminated medical devices [91]. Another benefit of implementing blockchain in the healthcare supply chain is increased transparency. Blockchain provides a shared platform for all participants, which helps to build trust, reduce the risk of fraud, and mitigate other forms of corruption. Additionally, blockchain technology can streamline and automate various processes within the healthcare supply chain [92]. For example, smart contracts can automate payments and the release of goods, reducing the risk of fraud and enhancing efficiency. Lastly, blockchain technology can enhance regulatory compliance by providing regulators with accurate and up-to-date data on the flow of goods, enabling better oversight and ensuring that all parties adhere to regulations [93].

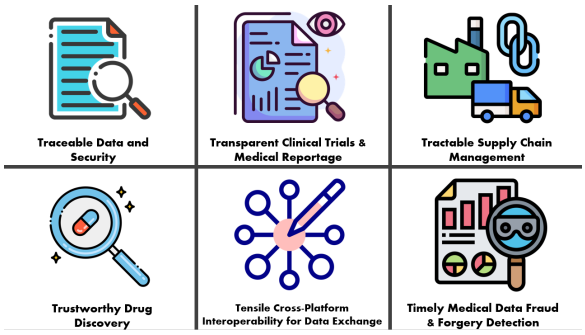


Figure 6. Potential and prospects of blockchain technology in medical IoT record preservation and transmission fidelity.

While there are challenges to address, such as the need for standardization and appropriate regulatory frameworks, the integration of blockchain into the healthcare supply chain offers significant improvements in efficiency, transparency, and security. This advancement benefits both patients and the healthcare industry as a whole. Furthermore, the interplay between blockchain technology and the medical supply chain, particularly in securing medical IoT records and ensuring cooperative, transparent management of medical supplies and patient data, can be further enhanced by incorporating artificial intelligence algorithms

into the process [94]. By leveraging these technologies, the healthcare sector can improve patient outcomes and reduce the risks of fraud, forgery, and data breaches.

5.4. Trustworthy Drug Discovery

While there may be some overlap between drug discovery and blockchain technology for medical IoT record retention, the connection between these areas is relatively narrow but still significant. Drug discovery involves identifying new drugs, while blockchain, a decentralized and distributed digital ledger technology, is used for secure and transparent transactions [41]. On the other hand, preserving medical IoT records involves managing and storing patient health data generated by various connected medical devices [87]. Nonetheless, there are potential applications for blockchain technology and IoT in enhancing the drug discovery process [41]. One of the key benefits of utilizing blockchain in drug discovery is its ability to securely store and share large volumes of data [93]. Blockchain can be employed to manage data related to drug candidates, trial protocols, and results, facilitating more efficient collaboration among researchers and accelerating the drug development process. Additionally, blockchain enhances data quality and reduces the risk of data manipulation [78]. By leveraging blockchain to store and manage data, the accuracy and immutability of the information are preserved, thereby improving the reliability of drug discovery outcomes.

Blockchain technology can also enhance accountability and transparency in the drug discovery process. For example, blockchain-based systems can be employed to track the allocation of funding and other resources, allowing researchers to gain insights into resource utilization and ensuring that funds are used as intended [76]. Another potential application is the use of blockchain-based patient registries, which can reduce the administrative workload for trial staff, facilitate the creation of comprehensive and diverse patient datasets, and provide patients with a secure platform for participating in drug trials [95]. Additionally, blockchain can improve regulatory compliance by offering regulators access to accurate and up-to-date information on the drug discovery process, enabling better oversight and ensuring that all parties adhere to regulatory requirements.

5.5. Tensile Cross-Platform Interoperability for Data Exchange

Blockchain technology and the interoperability of medical IoT devices and platforms are crucial components for the enhancement of security and preservation of patient data and outcomes, thereby fostering transparent and reliable digital healthcare delivery. Interoperability refers to the ability of different systems and devices to seamlessly exchange data with each other [96]. This capability allows various medical devices, MIR systems, and other healthcare technologies to share information, regardless of their manufacturer or the specific technology used [77]. Moreover, interoperable MIR systems facilitate medical professionals in accessing a patient's complete medical history (assuming appropriate permissions are granted), enabling more informed decisions about their care.

The integration of medical IoT device interoperability with blockchain technology can lead to a more effective and secure healthcare system, particularly in ensuring the security of MIRs. Blockchain enables the creation of a secure, seemingly immutable, and tamper-proof record of a patient's medical history [97]. This means patient data are accessible only to authorized individuals, significantly reducing the risk of data breaches and security issues [98] by ensuring that Internet-connected medical devices and sensors, which collect and distribute patient data, are all authenticated and traceable. Medical IoT enhances patient care by providing real-time data to healthcare professionals, enabling remote monitoring and improving diagnostic outcomes while addressing concerns about the exposure of sensitive data to the public domain [99,100]. By incorporating blockchain into the interoperable medical IoT framework, healthcare practitioners can gain effective and secure access to patient medical histories. This integration allows various devices and systems within the network to communicate while maintaining user exclusivity and data

privacy. Consequently, healthcare providers can obtain real-time information from the Medical IoT, which can improve patient outcomes and reduce costs.

5.6. Timely Medical Data Fraud and Forgery Detection

One of the main benefits of deploying AI–blockchain systems to detect medical data forgery and fraud is their ability to securely store and manage large volumes of data [101,102]. Blockchain ensures data accuracy and immutability, which helps reduce the risk of fraud and tampering with patient information. Additionally, the combination of blockchain and AI allows for the rapid evaluation of large datasets to identify patterns and trends, which can highlight fraudulent activities [103]. AI algorithms can analyze data stored on the blockchain network to uncover trends and anomalies that may indicate fraud, enabling faster and more efficient detection [75,104,105]. Furthermore, blockchain technology and explainable AI algorithms contribute to greater transparency and accountability in digital health care [106,107].

6. 5G-Blockchain for Preservation of Secured Medical Data

Fifth-generation networks, commonly known as 5G, represent a significant advancement in telecommunications, offering enhanced latency and high data transmission speeds. These features support and drive various technologies, including autonomous vehicles, drones, surgical robots, and virtual/augmented reality. The generation of and access to Medical IoT records (MIRs) would be impractical without 5G, which also raises privacy and transmission issues for users and stakeholders in digital health care [77]. Blockchain technology is widely recognized as a key tool in enhancing the security, trustworthiness, tamper resistance, and decentralization of data within 5G networks, offering numerous advantages [108]. Given its anonymous and immutable characteristics, blockchain is considered highly effective in ensuring data privacy and security in 5G environments, particularly for the preserving medical data and enabling secure, anonymous data sharing [109]. The evolving trends in medical data preservation, utilizing various materials, tools, and technologies, are explored further in [110].

6.1. Offline Medical Record Preservation

Patient medical information is highly sensitive and must be managed with the utmost care. In developing countries, this information is often stored in paper files, which can result in delays when retrieving data and complicate access due to the slow and laborious search processes involved [111]. Additionally, paper-based records are prone to loss and do not facilitate modern electronic data sharing between hospitals, clinics, and patients. This traditional storage method is fragmented across various medical institutions, leading to challenges such as inaccessible information, incomplete data, and illegible handwriting [111,112].

In contrast, in some developed countries, medical information is stored on private servers within individual health institutions [113]. This means that only the hospital where a patient receives a diagnosis has access to their medical records; other hospitals and the patient cannot access these records instantly without revisiting the original hospital [111]. This method also introduces latency and consumes resources [111]. As people move between different locations, their medical records may be dispersed across various institutions, further complicating access. This approach has become outdated due to its limitations, including a hospital-centric model, lack of electronic data sharing between institutions, and inadequate security and privacy protections, in addition to issues of duplication and redundancy [113].

6.2. Online Medical Record Preservation

To overcome the limitations of traditional offline methods for the preservation of medical information, researchers have developed automation systems like electronic medical record (EMR) systems that use cloud computing to link various hospitals, clinics, and patients [114]. This cloud-based approach allows medical information to be stored, ac-

cessed, and retrieved electronically in real time, addressing issues of latency and facilitating seamless connectivity among different entities involved in managing medical records. Despite these advancements, cloud-based EMR systems have not fully resolved security and privacy concerns, as cloud platforms remain susceptible to cyber attacks that could compromise medical data [115]. This vulnerability is partly due to the separation of cloud service providers and healthcare institutions, as well as the lack of data access control, which should ideally be managed by the patient. Modern medical record systems require that patients give explicit consent or approval through consent management applications and procedures before their data can be accessed [16].

Due to the privacy and security challenges of current medical data storage technologies, it has become crucial to integrate personalization features into medical records to enhance security measures. Researchers have explored advancements in blockchain technology as a promising solution to address the privacy and security issues inherent in cloud-based systems [113]. An in-depth examination of recent research into the integration of 5G and blockchain technology for medical information records (MIRs) reveals significant progress in securing MIR data and advancing digital healthcare delivery.

6.3. Use Cases of 5G-Blockchain for MIR Security

The primary goal of many research initiatives focused on securing digital healthcare services is to ensure the fidelity, preservation, and authentication of MIRs through blockchain applications, as illustrated in Figure 7. To enhance the integrity and trustworthiness of MIR security, the authors of [116] developed SPChain, an electronic medical data-sharing technology. This system uniquely allows for the uploading and labeling of erroneous electronic medical records. Additionally, SPChain features a reputation-based consensus algorithm that incentivizes healthcare institutions to participate in the mining process, utilizing proof of reputation to request patients' electronic medical records. The findings indicate that SPChain effectively defends against blockchain attacks while safeguarding the privacy and security of medical records stored on the blockchain. Other blockchain use cases for medical record security are summarized in Table 3.

Table 3. Blockchain approaches for medical record security.

Sno.	Ref.	Model	Potential
1.	[116]	SPChain	A reputation-based consensus algorithm that incentivizes healthcare institutions to participate in the mining process, utilizing proof of reputation to request patients' electronic medical records.
2.	[117]	SEMRES	An efficient triple encryption mechanism for electronic medical records to address data privacy, data correctness, and data security.
3.	[118]	BLOSSOM	A blockchain algorithm consisting of a cryptographic hash of the records, proof of work, and a Merkle tree formulation for EMRs.
4.	[119]	SEMRAchain	A system based on access control (Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC)) and a smart contract approach to guarantee not just visibility but also trustworthiness, credibility, and immutability.
5.	[120]	BeHeDaS	A permission-mode blockchain system with a hyper-fabric ledger that uses a world state on a peer-to-peer chain, i.e., its smart contracts do not require a complex algorithm to yield controlled transparency for users.

Similarly, the authors of [121] introduced an electronic medical record (EMR) system using a private blockchain called "Hyperledger", designed to efficiently manage medical data storage and sharing. In this system, patients have direct control over their medical information, allowing them to authorize healthcare providers to update or access their records. This approach tackles security and privacy concerns related to medical data storage. However, the research prototype has not yet been tested with real patient data, and its performance has not been evaluated in practical scenarios [121].

To enable personalized control over MIR transmission, Factom [122] utilized blockchain technology to ensure the security, integrity, privacy, and transparency of patients' medical records. To address latency issues related to real-time connectivity in blockchain adoption, the authors of [123] developed a blockchain prototype that enables secure and scalable sharing of clinical data. Additionally, the authors of [111] suggested an off-chain approach for the sharing of medical information, where doctors' requests, queries, and data retrieval occur off-chain. Moreover, the authors of [124] proposed a method whereby hospitals manage medical data storage to improve transmissibility. However, a notable limitation of this approach is that patients have limited control over their medical records because the hospitals hold the data.

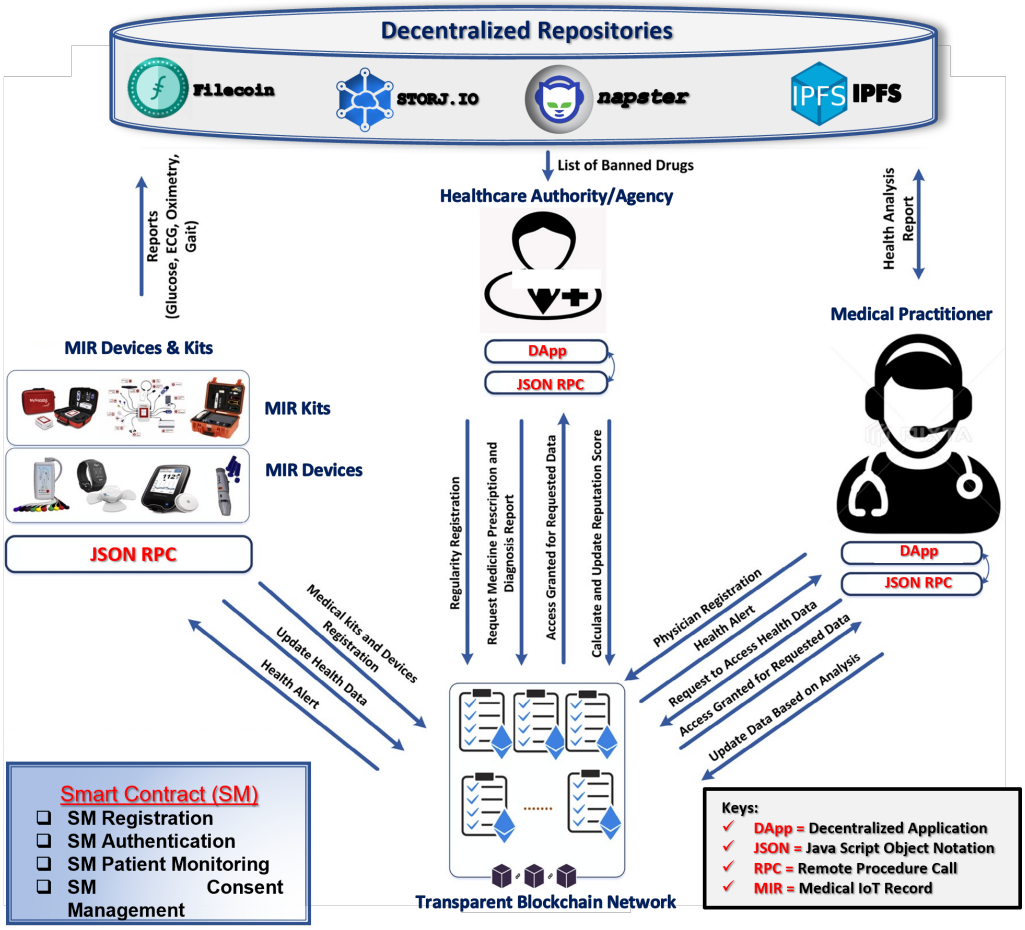


Figure 7. Achieving MIR transmission fidelity, preservation, and authentication via blockchain network for secured digitization of healthcare services.

To advance the automation of blockchain and cryptography in managing data and security for MIRs, the authors of [113] proposed a blockchain system using Ethereum-based smart contracts. This system allows patients to manage their medical information in a secure, trustworthy, traceable, transparent, immutable, and decentralized manner. The implementation also includes interplanetary file systems (IPFSs) and re-encryption oracles to enable secure storage, retrieval, and sharing of medical data [113]. To enhance transparency in handling and transmitting MIRs, another study [125] introduced a technology for medical data management and sharing. This research deployed smart contracts and blockchain to improve healthcare processes, ensuring privacy, security, availability, and access control for electronic medical records (EMRs). The technology provides comprehensive access control, facilitating the secure and efficient exchange of medical information

among patients, doctors, research organizations, hospitals, and other stakeholders while maintaining privacy [125].

Finally, miniaturized medical IoT devices, such as implanted wearables, require an energy-efficient security architecture to continuously transmit data across the network [77]. Consequently, blockchain technology must be adapted to maintain its decentralization and immutability while also being lightweight to ensure secure storage and sharing of medical information in these small devices. To tackle the challenge of lightweight blockchain security for MIRs, the authors of [126] developed a streamlined medical information dissemination system based on blockchain technology. This prototype employs proxy re-encryption to allow doctors to access patients' medical records securely. Since medical information is transmitted in an encrypted format, the scheme ensures security. Additionally, the system includes a feature allowing patients with similar symptoms to connect and discuss their conditions [126].

7. Blockchain Milestones in MIR Security

The adoption and application of blockchain in medical record management and security have both pros and cons. A succinct overview of the benefits and the technical challenges facing blockchain technology adoption in health data management is presented hereafter. Figure 8 shows the developmental strides and milestones of blockchain technology toward the digitization of health care, highlighting the various levels of digital health care and the underlying associated technologies.

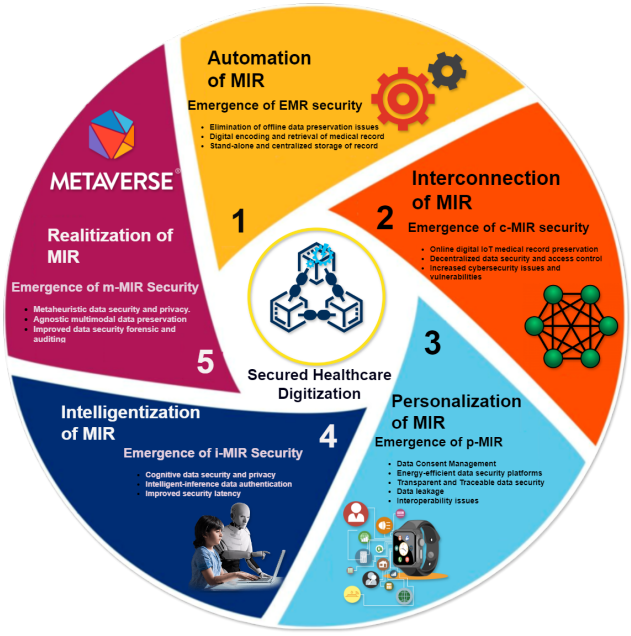


Figure 8. The milestones of blockchain for MIR security and preservation towards the actualization of secured digitization of health care, highlighting the various stages and underlying security improvements from automation to realization.

7.1. Blockchain Benefits and Digitization of Healthcare

The benefits of blockchain technology adoption in the quest to actualize healthcare digitization are enormous [127]. A few of these benefits are outlined in a cursory format below.

7.1.1. Accuracy of Health Information

The history of the medical data of a patient is fragmented among many platforms, like hospitals, insurance companies, etc.By using blockchain, the collection of data is automated and always up-to-date. The record is transparent, as every transaction is imitable and auditable on the network. The immutable and secure data structure allows

medical professionals to view the entire health history on the blockchain, allowing them to provide better treatment [128,129].

7.1.2. Accentuated Interoperability of MIR Platforms

Many health record systems suffer from compatibility issues. This is because there are many manufacturers with a lot of technical differences. Thus, electronic information sharing is limited [130–132]. With blockchain technology as the hub of digital healthcare record security and with decentralized applications managing the MIR distribution process at the front end, interoperability is achieved seamlessly across different healthcare delivery platforms.

7.1.3. Authentic Protection of Health Records

The centralized nature of most medical record databases makes successful cyber attacks easy [48]. Due to these centralization characteristics, unauthorized modification of medical records is possible. However, blockchain technology prevents the loss of data in cases of unexpected natural disasters [133].

7.1.4. Alleviation of Administrative and Handling Costs

Medical data saved on a public blockchain are complete and accessible from anywhere. This saves costs and time spent in gathering fragmented data scattered across different databases in most current medical record management systems [134,135].

7.1.5. Authorized Global Accessibility of MIRs

Apart from a reduction in the cost of accessing medical records, putting medical data on the blockchain also allows professionals to have full access to the medical history of patients to enable proper drug prescription and straight-to-the-point conclusions on the likely cause of a medical issue, especially when an emergency procedure needs to be carried out [84,136].

7.1.6. Assured Auditing Process for Medical Data

It is necessary to audit medical processes. However, the operations of legacy medical data management systems can be artificially broken to prevent the auditing process. The immutability and authentication of blockchain technology make it easy for processes such as auditing to happen easily and reliably [137].

8. Blockchain Milieu for MIR Security and Recommended Possible Solutions

Although blockchain holds a lot of promise in medical record management, it still has some technical issues preventing real-world mass adoption, especially in the healthcare sector for the actualization of digitization of healthcare delivery in response to the fourth industrial revolution. The challenges facing blockchain adoption in the healthcare sector and some possible solutions are presented in this subsection.

8.1. Difficulty in Information Exchange

The exchange of information among state holders might be difficult in a blockchain network. Those involved might be specialized staff (for example, nurses and doctors) insurance companies, or various departments in the same health center. The variety of involved entities makes it difficult to guarantee proper information exchange [138]. This could be resolved if all the parties involved were to have distinct accounts on the blockchain network, with different levels of permission assigned according to levels of privilege.

8.2. Data and Privacy Leakage

A decentralized network is not immune to data leakage. When such an event happens, everyone in the blockchain network can potentially verify the leaked data on the public ledger. In the case of a 51% attack, the security of the blockchain network cannot be

guaranteed [138]. In the case of information leakage, like a public key owner being made public, the owner of the account could transfer ownership of the medical data to another account, thereby regaining some privacy. It is, by far, easier for an attacker to hijack a centralized computer than a decentralized blockchain network. Therefore, to limit 51% attacks, medical data should be stored on very highly decentralized public networks like Ethereum or Layer 2 solutions built on highly decentralized Layer 1 networks.

8.3. Debilitating and Large Storage Requirements

Medical data exist in different forms, ranging from text to images and sounds. Storing this type of data consumes storage space, and sometimes, it may be necessary to store such data in multiple locations in the same or different formats. Hence, the use of blockchain would further increase storage demand, since every full node in the network stores the entirety of blockchain data [85]. Solutions providing considerable storage efficiencies were proposed in [139], using smart auto mining to prevent unnecessary resource usage, including storage space. Further storage management methods can be applied by making larger sets of data non-fungible tokens (NFTs), thereby preserving their originality on a blockchain without too much storage cost.

8.4. Distinct Technologies and Protocol Conformity Standardization

The ease of deploying blockchain projects, especially with smart contracts in areas requiring trust and security, means that blockchain adoption is becoming widespread. With this level of access, there is a need for conformity in standards [136,140]. Just like standards already existing in blockchain smart contracts like ERC20 for crypto tokens, ERC721 for NFTs, and so on, there should be a standard for medical data on blockchains.

8.5. Definition and Regulation of Roles in Distributive Data Sharing

Hospitals feel reluctant to adopt blockchain technology, as it may expose some of their internal information to external parties. For instance, pricing policy will be available to other parties, such as insurance companies and other competing hospitals [137]. The privilege and access of every user should be defined in the development process of blockchain-enabled medical record management systems to prevent unauthorized access to certain information. There should also be an authoritative body that assigns each stakeholder a level of privilege.

8.6. Depletion of Distribution Rights of Patients to Data Exclusivity

Some patients are reluctant to share their health records with third parties [137]. In a robust solution, the patient should have the right to decide who has access to their medical record for a determined duration of time. This allows the patient to be in full control of their health data due to the sensitivity and confidentiality attached to such records and the damage they could cause if accessed by an unauthorized user.

8.7. Drug Prescription Platform Difficulty

The use of electronic means to prescribe medication might have caused more work for doctors, who have to provide more information in prescriptions compared to when written on paper. With the adoption of blockchain, the technical skill needed to write a simple prescription will increase [137]. Medical practitioners who are not compliant with electronic prescriptions will, no doubt, require training. However, the design of the blockchain architecture should not deviate significantly from the original model, especially for the institution involved.

8.8. Data Ownership Rules and Processes

Ownership of data and the responsibility for allowing access to create, read, or write on the database are discussed in this section. Blockchain medical data models should consider and ensure all the benefits of the current system while adding the benefits of blockchain

technology [137]. In most of current medical data management systems, hospitals own the data [141]. However, to reduce privacy issues, patients should have the technical and legal right to control access to their medical data. This can be achieved by applying blockchain technology. The patient would have the ability to create an account ub the database and would give access to others to either read or write into it based on their privileges as stipulated by the authorized body.

8.9. Contemporary Research Issues and Future Directions

A current challenge in medical data preservation is the lack of coordinated access control [142]. Ensuring the privacy and security of medical data is crucial, but achieving well-organized data access and sharing remains problematic [142]. Some researchers advocate for patients to have control over access to their data [121], while others propose that an independent regulatory authority should manage access permissions for healthcare providers [113]. Both approaches have their advantages and disadvantages. For instance, an unconscious patient in an ICU may be unable to manage access to their records, whereas centralizing access control could introduce delays in the transmission of data to hospitals or clinics. The challenge is to design a blockchain-based solution that effectively addresses these various scenarios of access control involving patients, hospitals, central authorities, insurance companies, and other stakeholders [84,143]. Integrating edge-friendly artificial intelligence algorithms, such as federated learning [144] and explainable AI [145], into existing blockchain security frameworks could enhance the security and sophistication of digital platforms for medical information privacy and preservation.

Another challenge in blockchain-based medical record preservation is the tamper resistance of smart contracts post-deployment. Once a smart contract is deployed on the blockchain, it cannot be altered or updated, which poses significant issues if the contract has vulnerabilities that need addressing [113]. Exploring methods to integrate Metaverse technology, digital twin technology, self-supervised learning algorithms [146], and reverse software engineering into blockchain-based digital healthcare platforms could provide a viable solution to these issues.

Lastly, interoperability issues present a significant challenge in blockchain-based digital health record systems. This problem arises due to the limited global integration of Ethereum-based blockchains across various regions, which becomes evident when a patient travels internationally [113]. In such cases, the patient must re-register within the new country's blockchain smart contract system [113]. To address this, there is a need for the development of universal security frameworks that allow for seamless integration and migration across borders; minimize bureaucratic interference; and ensure reliable, transparent, and traceable security for medical information. This approach would support the digitalization of healthcare delivery and meet the needs of stakeholders in the health sector.

9. Conclusions

The confidentiality and uniqueness of medical records highlight the critical importance of a robust security framework for their preservation and access, which can significantly impact the progress of digital health care. This survey examines how blockchain technology contributes to the transparent, traceable, and reliable security of medical record management and transmission. It traces the evolution of medical record preservation from digital certificates to the recent integration of 5G and advanced blockchain technologies. Additionally, it addresses the challenges and complexities associated with incorporating blockchain into existing healthcare systems, aiming to advance the fourth industrial revolution and enhance digital healthcare. This evolution encompasses a shift from automation to interconnected systems, personalization, and intelligent solutions, ultimately striving to offer not only functional health care but also a patient-centered, experiential approach to well-being.

The ongoing advancement of blockchain technology, through the resolution of its existing limitations and its increasing integration into healthcare systems, will likely lead

to the realization and maintenance of secure medical record preservation, confidentiality, integrity, and transparent access. Moving forward, the goal is to create a blockchain-based security framework for medical IoT records that ensures that user consent protocols are thoroughly vetted and verified before personal medical information is transmitted or accessed by third parties.

Author Contributions: Conceptualization, S.O.A., I.I.S., D.-S.K. and J.M.L.; methodology, S.O.A., I.I.S., D.-S.K. and J.M.L.; software, S.O.A., I.I.S., V.U.I., O.U.N., M.A.D. and I.U.U.; validation, S.O.A., I.I.S., D.-S.K. and J.M.L.; investigation, S.O.A., I.I.S., V.U.I., O.U.N., M.A.D. and I.U.U.; resources, S.O.A., I.I.S., V.U.I., O.U.N., M.A.D. and I.U.U.; data curation, S.O.A. and I.I.S.; writing—original draft preparation, S.O.A., I.I.S., V.U.I., O.U.N., M.A.D. and I.U.U.; writing—review and editing, S.O.A.; visualization, S.O.A.; supervision, S.O.A., I.I.S. and J.M.L.; project administration, S.O.A., I.I.S. and J.M.L.; funding acquisition, D.-S.K. and J.M.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003) (50%) and by MSIT under the Innovative Human Resource Development for Local Intellectualization support program (IITP-2024-2020-0-01612) (50%) supervised by the IITP.

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

References

1. Kruse, C.S.; Mileski, M.; Vijaykumar, A.G.; Viswanathan, S.V.; Suskandla, U.; Chidambaram, Y. Impact of electronic health records on long-term care facilities: systematic review. *JMIR Med. Inform.* **2017**, *5*, e7958. [CrossRef] [PubMed]
2. Dizon, M.A.C.; Upson, P.J. Laws of encryption: An emerging legal framework. *Comput. Law Secur. Rev.* **2021**, *43*, 105635. [CrossRef]
3. Shafinah, K.; Ikram, M.M. File Security based on Pretty Good Privacy (PGP) Concept. *Comput. Inf. Sci.* **2011**, *4*, 10.
4. Lampson, B.; Rivest, R. A Simple Distributed Security Infrastructure. MIT—Massachussetts Institute of Technology. 1996; Volume 12; p. 2006. Available online: https://people.csail.mit.edu/rivest/pubs/RL96.ver-1.1.html (accessed on 15 April 2024).
5. Sharma, K.; Shrivastava, G. Public key infrastructure and trust of web based knowledge discovery. *Int. J. Eng. Sci. Manag.* **2014**, *4*, 56–60.
6. Kaur, R.; Kaur, A. Digital signature. In Proceedings of the 2012 International Conference on Computing Sciences, Washington, DC, USA, 14–15 September 2012; pp. 295–301.
7. Lin, C.H.; Yeh, Y.S.; Chien, S.P.; Lee, C.Y.; Chien, H.S. Generalized secure hash algorithm: SHA-X. In Proceedings of the 2011 IEEE EUROCON-International Conference on Computer as a Tool, Lisbon, Portugal, 27–29 April 2011; pp. 1–4.
8. Myers, M.; Ankney, R.; Malpani, A.; Galperin, S.; Adams, C.X. *509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP*; Technical Report; The Internet Society: Reston, VA, USA, 1999.
9. Huang, L.C.; Chu, H.C.; Lien, C.Y.; Hsiao, C.H.; Kao, T. Privacy preservation and information security protection for patients' portable electronic health records. *Comput. Biol. Med.* **2009**, *39*, 743–750. [CrossRef] [PubMed]
10. Shen, N.; Bernier, T.; Sequeira, L.; Strauss, J.; Silver, M.P.; Carter-Langford, A.; Wiljer, D. Understanding the patient privacy perspective on health information exchange: A systematic review. *Int. J. Med. Inform.* **2019**, *125*, 1–12. [CrossRef]
11. Hossein, K.M.; Esmaeili, M.E.; Dargahi, T.; Khonsari, A.; Conti, M. BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications. *Comput. Commun.* **2021**, *180*, 31–47. [CrossRef]
12. Jin, H.; Luo, Y.; Li, P.; Mathew, J. A review of secure and privacy-preserving medical data sharing. *IEEE Access* **2019**, *7*, 61656–61669. [CrossRef]
13. Raghav, N.; Bhola, A. Blockchain based privacy preservation in healthcare: a recent trends and challenges. *Psychol. Educ. J.* **2021**, *58*, 5315–5324.
14. Balasubramanium, S.; Sivasankar, K.; Rajasekaran, M.P. A Survey on Data privacy and preservation using Blockchain in Healthcare organization. In Proceedings of the 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 4–5 March 2021; pp. 956–962.
15. Sharma, A.; Kaur, S.; Singh, M. A comprehensive review on blockchain and Internet of Things in healthcare. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4333. [CrossRef]
16. Ahmad, R.W.; Salah, K.; Jayaraman, R.; Yaqoob, I.; Ellahham, S.; Omar, M. The role of blockchain technology in telehealth and telemedicine. *Int. J. Med. Inform.* **2021**, *148*, 104399. [CrossRef] [PubMed]
17. Zhang, J.; Zhong, S.; Wang, T.; Chao, H.C.; Wang, J. Blockchain-based systems and applications: A survey. *J. Internet Technol.* **2020**, *21*, 1–14.
18. Hesse, B.W.; Hansen, D.; Finholt, T.; Munson, S.; Kellogg, W.; Thomas, J.C. Social participation in health 2.0. *Computer* **2010**, *43*, 45–52. [CrossRef]

19. Stark, B.; Gewald, H.; Lautenbacher, H.; Haase, U.; Ruff, S. Misuse of 'Break-the-Glass' Policies in Hospitals: Detecting Unauthorized Access to Sensitive Patient Health Data. In *Research Anthology on Privatizing and Securing Data*; IGI Global: Hershey, PA, USA, 2021; pp. 1231–1256.
20. Osundina, K.S. Unauthorized Disclosure of Medical Information, Patient Rights and Legal Consequences as It Affect Patients and Healthcare Providers. Available online: https://iiardjournals.org/404.php/ (accessed on 9 March 2024).
21. Maksymiv, T.; Chaplinskyi, R. Ways of unauthorized access to medical data and approach to organize secure access using blockchain technology. In Proceedings of the 2020 10th International Conference on Advanced Computer Information Technologies (ACIT), Deggendorf, Germany, 16–18 September 2020; pp. 791–795.
22. Keshta, I.; Odeh, A. Security and privacy of electronic health records: Concerns and challenges. *Egypt. Inform. J.* **2021**, *22*, 177–183. [CrossRef]
23. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *BMJ* **2009**, *6*, 264–269. [CrossRef]
24. Foley Library. *SPIDER: Mixed Methods Qualitative Research Questions*; Foley Library: Spokane, WA, USA, 2022.
25. Liu, Q.; Liu, Y.; Luo, M.; He, D.; Wang, H.; Choo, K.K.R. The Security of Blockchain-Based Medical Systems: Research Challenges and Opportunities. *IEEE Syst. J.* **2022**, *16*, 5741–5752. [CrossRef]
26. Fatima, N.; Agarwal, P.; Sohail, S.S. Security and Privacy Issues of Blockchain Technology in Health Care—A Review. In *ICT Analysis and Applications*; Fong, S., Dey, N., Joshi, A., Eds.; Springer: Singapore, 2022; pp. 193–201.
27. Wenhua, Z.; Qamar, F.; Abdali, T.A.N.; Hassan, R.; Jafri, S.T.A.; Nguyen, Q.N. Blockchain technology: Security issues, healthcare applications, challenges and future trends. *Electronics* **2023**, *12*, 546. [CrossRef]
28. Harn, L.; Ren, J. Generalized digital certificate for user authentication and key establishment for secure communications. *IEEE Trans. Wirel. Commun.* **2011**, *10*, 2372–2379. [CrossRef]
29. O'Brien, M.; Weir, G.R. Understanding digital certificates. In Proceedings of the 2nd International Conference on Cybercrime Forensics Education & Training, Kent, Canterbury, UK, 1–2 September 2008.
30. Akinsanya, O.O.; Papadaki, M.; Sun, L. Current cybersecurity maturity models: How effective in healthcare cloud? In Proceedings of the CERC, Darmstadt, Germany, 29–30 March 2019; pp. 211–222.
31. Dang, Q.H. *Secure Hash Standard*; National Institute of Standards & Technology: Gaithersburg, MD, USA, 2015.
32. Mathew, A. The Limits to Peer Production in Security Infrastructures: Technological and Regulatory Challenges to the PGP Web of Trust. In Proceedings of the Sixth European Multidisciplinary Conference on Global Internet Governance Actors, Regulations, Transactions and Strategies, Nicosia, Cyprus, 13–14 April 2022.
33. Halpin, H. All that is Solid Melts into Air: Towards Decentralized Cryptographic Access Control. In Proceedings of the 17th International Conference on Availability, Reliability and Security, Vienna, Austria, 23–26 August 2022; pp. 1–6.
34. Ferguson, N.; Schneier, B.; Kohno, T. *Cryptography Engineering: Design Principles and Practical Applications*; John Wiley & Sons: Hoboken, NJ, USA, 2011.
35. Chen, L.; Moody, D.; Regenscheid, A.; Robinson, A. *Digital Signature Standard (DSS)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023. [CrossRef]
36. Kerry, C.F.; Gallagher, P.D. *Digital Signature Standard (DSS)*; FIPS PUB. 2013; pp. 186–192. Available online: https://en.wikipedia.org/wiki/Digital_Signature_Standard (accessed on 9 March 2024).
37. Wang, X.; Yin, Y.L.; Yu, H. Finding collisions in the full SHA-1. In *Proceedings of the Advances in Cryptology–CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2005*; Proceedings 25; Springer: Berlin/Heidelberg, Germany, 2005; pp. 17–36.
38. Cortez, D.M.A.; Sison, A.M.; Medina, R.P. Cryptographic randomness test of the modified hashing function of SHA256 to address length extension attack. In Proceedings of the 2020 8th International Conference on Communications and Broadband Networking, Auckland, New Zealand, 15–18 April 2020; pp. 24–28.
39. Bernstein, D.J.; Lange, T. Post-quantum cryptography. *Nature* **2017**, *549*, 188–194. [CrossRef]
40. Singh, S.; Rathore, S.; Alfarraj, O.; Tolba, A.; Yoon, B. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Gener. Comput. Syst.* **2022**, *129*, 380–388. [CrossRef]
41. Omidian, H.; Omidi, Y. Blockchain in pharmaceutical life cycle management. *Drug Discov. Today* **2022**, *27*, 935–938. [CrossRef] [PubMed]
42. Kumar, A.; Singh, A.K.; Ahmad, I.; Kumar Singh, P.; Verma, P.K.; Alissa, K.A.; Bajaj, M.; Ur Rehman, A.; Tag-Eldin, E. A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare. *Sensors* **2022**, *22*, 5921. [CrossRef] [PubMed]
43. Chen, Z.; Xu, W.; Wang, B.; Yu, H. A blockchain-based preserving and sharing system for medical data privacy. *Future Gener. Comput. Syst.* **2021**, *124*, 338–350. [CrossRef]
44. Razzaq, A.; Mohsan, S.A.H.; Ghayyur, S.A.K.; Al-Kahtani, N.; Alkahtani, H.K.; Mostafa, S.M. Blockchain in Healthcare: A Decentralized Platform for Digital Health Passport of COVID-19 Based on Vaccination and Immunity Certificates. *Healthcare* **2022**, *10*, 2453. [CrossRef]
45. Hasselgren, A.; Kralevska, K.; Gligoroski, D.; Pedersen, S.A.; Faxvaag, A. Blockchain in healthcare and health sciences—A scoping review. *Int. J. Med. Inform.* **2020**, *134*, 104040. CrossRef]

46. Alnafrani, M.; Acharya, S. SecureRx: A blockchain-based framework for an electronic prescription system with opioids tracking. *Health Policy Technol.* **2021**, *10*, 100510. [CrossRef]
47. Pericàs-Gornals, R.; Mut-Puigserver, M.; Payeras-Capellà, M.M. Highly private blockchain-based management system for digital COVID-19 certificates. *Int. J. Inf. Secur.* **2022**, *21*, 1069–1090. [CrossRef] [PubMed]
48. EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. *Inf. Sci.* **2023**, *629*, 703–718. [CrossRef]
49. Jeong, S.; Shen, J.H.; Ahn, B. A Study on Smart Healthcare Monitoring Using IoT Based on Blockchain. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 9932091. [CrossRef]
50. Saranya, R.; Murugan, A. A systematic review of enabling blockchain in healthcare system: Analysis, current status, challenges and future direction. *Mater. Today Proc.* **2023**, *80*, 3010–3015. [CrossRef]
51. Sara Ait, B.; Aaroud, A.; Sabiri, K.; Rguibi, M.A.; Cherradi, B. Design and implementation of a New Blockchain-based digital health passport: A Moroccan case study. *Inform. Med. Unlocked* **2022**, *35*, 101125. [CrossRef]
52. Bataineh, M.R.; Mardini, W.; Khamayseh, Y.M.; Yassein, M.M.B. Novel and Secure Blockchain Framework for Health Applications in IoT. *IEEE Access* **2022**, *10*, 14914–14926. [CrossRef]
53. Wazid, M.; Bera, B.; Mitra, A.; Das, A.K.; Ali, R. Private blockchain-envisioned security framework for AI-enabled IoT-based drone-aided healthcare services. In Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, New York, NY, USA, 25 September 2020; DroneCom '20; pp. 37–42. [CrossRef]
54. Schmeelk, S.; Kanabar, M.; Peterson, K.; Pathak, J. Electronic health records and blockchain interoperability requirements: A scoping review. *JAMIA Open* **2022**, *5*, ooac068. [CrossRef]
55. Ghosh, P.K.; Chakraborty, A.; Hasan, M.; Rashid, K.; Siddique, A.H. Blockchain Application in Healthcare Systems: A Review. *Systems* **2023**, *11*, 38. [CrossRef]
56. Purohit, S.; Calyam, P.; Alarcon, M.L.; Bhamidipati, N.R.; Mosa, A.; Salah, K. HonestChain: Consortium blockchain for protected data sharing in health information systems. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 3012–3028. [CrossRef] [PubMed]
57. Zhang, D.; Wang, S.; Zhang, Y.; Zhang, Q.; Zhang, Y. A Secure and Privacy-Preserving Medical Data Sharing via Consortium Blockchain. *Secur. Commun. Netw.* **2022**, *2022*, 2759787. [CrossRef]
58. Han, Y.; Zhang, Y.; Vermund, S.H. Blockchain Technology for Electronic Health Records. *Int. J. Environ. Res. Public Health* **2022**, *19*, 15577. [CrossRef]
59. Mingxiao, D.; Xiaofeng, M.; Zhe, Z.; Xiangwei, W.; Qijun, C. A review on consensus algorithm of blockchain. In Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, 5–8 October 2017; pp. 2567–2572. [CrossRef]
60. Ajakwe, S.O.; Saviour, I.I.; Kim, J.H.; Kim, D.S.; Lee, J.M. BANDA: A Novel Blockchain-Assisted Network for Drone Authentication. In Proceedings of the 2023 Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN), Virtual, 4–7 July 2023; pp. 120–125.
61. Xiong, H.; Chen, M.; Wu, C.; Zhao, Y.; Yi, W. Research on Progress of Blockchain Consensus Algorithm: A Review on Recent Progress of Blockchain Consensus Algorithms. *Future Internet* **2022**, *14*, 47. [CrossRef]
62. Nakamoto, S.; Bitcoin, A. A Peer-to-Peer Electronic Cash System. Bitcoin. 2008; Volume 4, p. 15. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 12 March 2024).
63. Ajakwe, S.O.; Kim, D.S.; Lee, J.M. Drone transportation system: Systematic review of security dynamics for smart mobility. *IEEE Internet Things J.* **2023**, *10*, 14462–14482. [CrossRef]
64. Manolache, M.A.; Manolache, S.; Tapus, N. Decision Making using the Blockchain Proof of Authority Consensus. *Procedia Comput. Sci.* **2022**, *199*, 580–588. CrossRef]
65. Bamakan, S.M.H.; Motavali, A.; Babaei Bondarti, A. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Syst. Appl.* **2020**, *154*, 113385. [CrossRef]
66. Mendoza Arvizo, A.I.; Avelar Sosa, L.; García Alcaraz, J.L.; Cruz-Mejía, O. Beneficiary Contracts on a Lightweight Blockchain Architecture Using Smart Contracts: A Smart Healthcare System for Medical Records. *Appl. Sci.* **2023**, *13*, 6694. [CrossRef]
67. Chinnasamy, P.; Albakri, A.; Khan, M.; Raja, A.A.; Kiran, A.; Babu, J.C. Smart Contract-Enabled Secure Sharing of Health Data for a Mobile Cloud-Based E-Health System. *Appl. Sci.* **2023**, *13*, 3970. [CrossRef]
68. Igboanusi, I.S.; Nnadiekwe, C.A.; Ogbede, J.U.; Kim, D.S.; Lensky, A. BOMS: Blockchain-enabled organ matching system. *Sci. Rep.* **2024**, *14*, 16069. [CrossRef]
69. Chinnasamy, P.; Vinodhini, B.; Praveena, V.; Vinothini, C.; Sujitha, B.B. Blockchain based Access Control and Data Sharing Systems for Smart Devices. *J. Physics Conf. Ser.* **2021**, *1767*, 012056. [CrossRef]
70. Igboanusi, I.S.; Dirgantoro, K.P.; Lee, J.M.; Kim, D.S. Blockchain side implementation of Pure Wallet (PW): An offline transaction architecture. *ICT Express* **2021**, *7*, 327–334. [CrossRef]
71. Ajakwe, S.O.; Ajakwe, I.U.; Taesoo, J.S.; Kim, D.S.; Lee, J.M. CIS-WQMS: Connected intelligence smart water quality monitoring scheme. *Internet of Things* **2023**, *23*, 100800–100819. [CrossRef]
72. Alabdulatif, A.; Khalil, I.; Saidur Rahman, M. Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis. *Appl. Sci.* **2022**, *12*, 11039. [CrossRef]
73. Sinha, A.; Patel, A.; Jagdish, M. *Application of Blockchain in Healthcare*; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2022. [CrossRef]

74. Mancer, M.; Akram, K.M.; Barka, E.; Okba, K.; Sihem, S.; Harous, S.; Athamena, B.; Houhamdi, Z. Blockchain Technology for Secure Shared Medical Data. In Proceedings of the 2022 International Arab Conference on Information Technology (ACIT), Abu Dhabi, United Arab Emirates, 22–24 November 2022; pp. 1–6. [CrossRef]
75. Dini, M.A.; Ajakwe, S.O.; Saviour, I.I.; Ihekoronye, V.U.; Nwankwo, O.U.; Uchechi, I.U.; Haryadi, G.A.; Putra, M.A.P.; Kim, D.S.; Jun, T.; et al. Patient-centric blockchain framework for secured medical record fidelity and authorization. In Proceedings of the Korean Institute of Communication and Sciences Summer Conference, Jeju Island, Republic of Korea, 21–24 June 2023; pp. 300–301.
76. Awasthi, C.; Nawal, M.; Mishra, P.K. Security Concerns of Fog Computing in Field of Healthcare using Blockchain: A Review. In Proceedings of the 2021 International Conference on Communication information and Computing Technology (ICCICT), Mumbai, India, 25–27 June 2021. [CrossRef]
77. Ajakwe, S.O.; Nwakanma, C.I.; Kim, D.S.; Lee, J.M. Key Wearable Device Technologies Parameters for Innovative Healthcare Delivery in B5G Network: A Review. *IEEE Access* **2022**, *10*, 49956–49974. [CrossRef]
78. Hu, J.; Zhu, P.; Qi, Y.; Zhu, Q.; Li, X. A patent registration and trading system based on blockchain. *Expert Syst. Appl.* **2022**, *201*, 117094. [CrossRef]
79. Anwar, A.; Goyal, S.B.; Ghosh, A. Tracking Clinical Trials and Enhancement of Security Control with Blockchain for Medical Record. In Proceedings of the 2021 IEEE 6th International Conference on Computing, Communication and Automation (ICCCA), Arad, Romania, 17–19 December 2021; pp. 632–636. [CrossRef]
80. Rahman, M.A.; Hossain, M.S.; Islam, M.S.; Alrajeh, N.A.; Muhammad, G. Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach. *IEEE Access* **2020**, *8*, 205071–205087. [CrossRef] [PubMed]
81. Curbera, F.; Dias, D.M.; Simonyan, V.; Yoon, W.A.; Casella, A. Blockchain: An enabler for healthcare and life sciences transformation. *IBM J. Res. Dev.* **2019**, *63*, 8:1–8:9. [CrossRef]
82. Hang, L.; Chen, C.; Zhang, L.; Yang, J. Blockchain for applications of clinical trials: Taxonomy, challenges, and future directions. *IET Commun.* **2022**, *16*, 2371–2393. [CrossRef]
83. Zhavoronkov, A.; Ivanenkov, Y.A.; Aliper, A.; Veselov, M.S.; Aladinskiy, V.A.; Aladinskaya, A.V.; Terentiev, V.A.; Polykovskiy, D.A.; Kuznetsov, M.D.; Asadulaev, A.; et al. Deep learning enables rapid identification of potent DDR1 kinase inhibitors. *Nat. Biotechnol.* **2019**, *37*, 1038–1040. [CrossRef]
84. Xia, Q.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. *IEEE Access* **2017**, *5*, 14757–14767. [CrossRef]
85. Linn, L.A.; Martha B. Koo, M. Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research. In Proceedings of the ONC/NIST Use of Blockchain for Healthcare and Research Workshop, Gaithersburg, MD, USA, 7 September 2016; Volume 17, pp. 1–10.
86. Bocek, T.; Rodrigues, B.B.; Strasser, T.; Stiller, B. Blockchains everywhere—A use-case of blockchains in the pharma supply-chain. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; pp. 772–777. [CrossRef]
87. Nawale, S.D.; Konapure, R.R. Blockchain & IoT based Drugs Traceability for Pharma Industry. In Proceedings of the 2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Cardiff, UK, 21–23 June 2021; pp. 1–4. [CrossRef]
88. Niu, B.; Dong, J.; Liu, Y. Incentive alignment for blockchain adoption in medicine supply chains. *Transp. Res. Part E Logist. Transp. Rev.* **2021**, *152*, 102276. [CrossRef]
89. Ajakwe, S.O.; Arkter, R.; Ahakonye, L.A.C.; Kim, D.S.; Lee, J.M. Real-Time Monitoring of COVID-19 Vaccination Compliance: A Ubiquitous IT Convergence Approach. In Proceedings of the 2021 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 20–22 October 2021; pp. 440–445. [CrossRef]
90. Khatter, K.D. Non-functional requirements for blockchain enabled medical supply chain. *Int. J. Syst. Assur. Eng. Manag.* **2022**, *13*, 1219–1231. [CrossRef]
91. Kumar, B.; Mohanraj, T.; ShahulHammed, S.; Santhosh, R. A Study of BlockChain Technologies and health Care Systems. In Proceedings of the 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 7–9 October 2020; pp. 265–267. [CrossRef]
92. Omar, I.A.; Jayaraman, R.; Debe, M.S.; Salah, K.; Yaqoob, I.; Omar, M. Automating procurement contracts in the healthcare supply chain using blockchain smart contracts. *IEEE Access* **2021**, *9*, 37397–37409. [CrossRef]
93. Premkumar, A.; Srimathi, C. Application of Blockchain and IoT towards Pharmaceutical Industry. In Proceedings of the 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 6–7 March 2020; pp. 729–733. [CrossRef]
94. Abbas, K.; Afaq, M.; Ahmed Khan, T.; Song, W.C. A Blockchain and Machine Learning-Based Drug Supply Chain Management and Recommendation System for Smart Pharmaceutical Industry. *Electronics* **2020**, *9*, 852. [CrossRef]
95. Ramdasani, U.; Vinzuda, G.; Tanwar, S.; Gupta, R.; Guizani, M. DuBloQ: Blockchain and Q-Learning Based Drug Discovery in Healthcare 4.0. In Proceedings of the 2022 International Wireless Communications and Mobile Computing (IWCMC), Dubrovnik, Croatia, 30 May–3 June 2022; pp. 284–289. [CrossRef]

96. Yuksel, M.; Dogac, A. Interoperability of Medical Device Information and the Clinical Applications: An HL7 RMIM based on the ISO/IEEE 11073 DIM. *IEEE Trans. Inf. Technol. Biomed.* **2011**, *15*, 557–566. [CrossRef]
97. Shukla, M.; Lin, J.; Seneviratne, O. BlockIoT: Blockchain-based health data integration using IoT devices. In Proceedings of the AMIA Annual Symposium Proceedings. American Medical Informatics Association, San Diego, CA, USA, 30 October–3 November 2021; Volume 2021, p. 1119.
98. Jain, S.; Anand, A.; Gupta, A.; Awasthi, K.; Gujrati, S.; Channegowda, J. Blockchain and Machine Learning in Health Care and Management. In Proceedings of the 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), Bengaluru, India, 21–22 February 2020; pp. 1–5. [CrossRef]
99. Yaeger, K.; Martini, M.; Rasouli, J.; Costa, A. Emerging blockchain technology solutions for modern healthcare infrastructure. *J. Sci. Innov. Med.* **2019**, *2*. [CrossRef]
100. Nichol, P.B.; Brandt, J. Co-creation of trust for healthcare: The cryptocitizen framework for interoperability with blockchain. *Res. Propos.* **2016**, 1–9. [CrossRef]
101. Saldamli, G.; Reddy, V.; Bojja, K.S.; Gururaja, M.K.; Doddaveerappa, Y.; Tawalbeh, L. Health care insurance fraud detection using blockchain. In Proceedings of the 2020 Seventh international conference on software defined systems (SDS), Paris, France, 20–23 April 2020; pp. 145–152.
102. Ihekoronye, V.U.; Ajakwe, S.O.; Kim, D.S.; Lee, J.M. Cyber Edge Intelligent Intrusion Detection Framework For UAV Network Based on Random Forest Algorithm. In Proceedings of the 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 19–21 October 2022; pp. 1242–1247. [CrossRef]
103. McGhin, T.; Choo, K.K.R.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 62–75. [CrossRef]
104. Liu, W.; Yu, Q.; Li, Z.; Li, Z.; Su, Y.; Zhou, J. A blockchain-based system for anti-fraud of healthcare insurance. In Proceedings of the 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 6–9 December 2019; pp. 1264–1268.
105. Ajakwe, S.O.; Ihekoronye, V.U.; Ajakwe, I.U.; Jun, T.; Kim, D.S.; Lee, J.M. Connected Intelligence for Smart Water Quality Monitoring System in IIoT. In Proceedings of the 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 19–21 October 2022; pp. 2386–2391. [CrossRef]
106. Sharma, M.; Goel, A.K.; Singhal, P. Explainable AI Driven Applications for Patient Care and Treatment. In *Explainable AI: Foundations, Methodologies and Applications*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 135–156.
107. Farrugia, D.; Zerafa, C.; Cini, T.; Kuasney, B.; Livori, K. A real-time prescriptive solution for explainable cyber-fraud detection within the iGaming industry. *Sn Comput. Sci.* **2021**, *2*, 215. [CrossRef]
108. Jain, G.; Jain, A. 22—Blockchain for 5G-enabled networks in healthcare service based on several aspects. In *Blockchain Applications for Healthcare Informatics*; Tanwar, S., Ed.; Academic Press: Cambridge, MA, USA, 2022; pp. 471–493. CrossRef]
109. Hewa, T.; Braeken, A.; Ylianttila, M.; Liyanage, M. Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT. In Proceedings of the GLOBECOM 2020—2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020. [CrossRef]
110. Cameron, L. Keeping Your Medical Records Safe in the Cloud: Researchers Analyze Blockchain as a Solution. *IEEE Comput. Soc.* **2020**, *18*. Available online: https://www.computer.org/publications/tech-news/research/blockchain-health-medical-records-cloud-security (accessed on 20 May 2024).
111. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* **2018**, *25*, 146045821876969. [CrossRef]
112. Executive, N. *Information for Health: An Information Strategy for the Modern NHS 1998–2005: A National Strategy for Local Implementation*; NHS/Department of Health: England, UK, 1998.
113. Madine, M.M.; Battah, A.A.; Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y.; Pesic, S.; Ellahham, S. Blockchain for Giving Patients Control Over Their Medical Records. *IEEE Access* **2020**, *8*, 193102–193115. [CrossRef]
114. Hombal, U.; Dayananda, R.B. A Review on Security and Privacy Preserving Mechanisms of Electronic Health Records in Cloud. In Proceedings of the 2021 Asian Conference on Innovation in Technology (ASIANCON), Pune, India, 27–29 August 2021; pp. 1–4. [CrossRef]
115. Bibal Benifa, J.; Venifa Mini, G.; Krishnan, S. Chapter 14—Blockchain-based health care monitoring for privacy preservation of COVID-19 medical records. In *Blockchain for Smart Cities*; Krishnan, S., Balas, V.E., Julie, E.G., Robinson, Y.H., Kumar, R., Eds.; Elsevier: Amsterdam, The Netherlands, 2021; pp. 259–294. CrossRef]
116. Zou, R.; Lv, X.; Zhao, J. SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. *Inf. Process. Manag.* **2021**, *58*, 102604. [CrossRef]
117. Mondal, S.; Shafi, M.; Gupta, S.; Gupta, S.K. Blockchain based secure architecture for electronic healthcare record management. *GMSARN Int. J.* **2022**, *16*, 413–426.
118. Johari, R.; Kumar, V.; Gupta, K.; Vidyarthi, D.P. BLOSOM: BLOckchain technology for Security of Medical records. *ICT Express* **2022**, *8*, 56–60. [CrossRef]

119. Mhamdi, H.; Ayadi, M.; Ksibi, A.; Al-Rasheed, A.; Soufiene, B.O.; Hedi, S. SEMRAchain: A secure electronic medical record based on blockchain technology. *Electronics* **2022**, *11*, 3617. [CrossRef]
120. Oladele, J.K.; Ojugo, A.A.; Odiakaose, C.C.; Emordi, F.U.; Abere, R.A.; Nwozor, B.; Ejeh, P.O.; Geteloma, V.O. BEHeDaS: A Blockchain Electronic Health Data System for Secure Medical Records Exchange. *J. Comput. Theor. Appl.* **2024**, *1*, 231–242. [CrossRef]
121. Usman, M.; Qamar, U. Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology. *Procedia Comput. Sci.* **2020**, *174*, 321–327. CrossRef]
122. Factom Announces Partnership with Healthnautica. 2015. Available online: https://www.prweb.com/releases/2015/04/prweb12673607.htm (accessed on 12 April 2024).
123. Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G.; Rosenbloom, S.T. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 267–278. [CrossRef]
124. Du, M.; Chen, Q.; Chen, J.; Ma, X. An Optimized Consortium Blockchain for Medical Information Sharing. *IEEE Trans. Eng. Manag.* **2021**, *68*, 1677–1689. [CrossRef]
125. Khatoon, A. A Blockchain-Based Smart Contract System for Healthcare Management. *Electronics* **2020**, *9*, 94. [CrossRef]
126. Liu, X.; Wang, Z.; Jin, C.; Li, F.; Li, G. A Blockchain-Based Medical Data Sharing and Protection Scheme. *IEEE Access* **2019**, *7*, 118943–118953. [CrossRef]
127. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for Healthcare Data Management: Opportunities, Challenges, and Future Recommendations. *Neural Comput. Appl.* **2022**, *34*, 11475–11490. [CrossRef]
128. Cornelius, C.A.; Qusay, H.M.; J. Mikael, E. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* **2019**, *7*, 56. [CrossRef]
129. Wang, S.; Wang, J.; Wang, X.; Qiu, T.; Yuan, Y.; Ouyang, L.; Guo, Y.; Wang, F.Y. Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 942–950. [CrossRef]
130. Khan, W.A.; Khattak, A.M.; Hussain, M.; Amin, M.B.; Afzal, M.; Nugent, C.; Lee, S. An adaptive semantic based mediation system for data interoperability among Health Information Systems. *J. Med. Syst.* **2014**, *38*, 28. [CrossRef] [PubMed]
131. Reisman, M. EHRs: The Challenge of Making Electronic Data Usable and Interoperable. *Pharm. Ther.* **2017**, *42*, 572–575.
132. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [CrossRef]
133. Alam Khan, F.; Asif, M.; Ahmad, A.; Alharbi, M.; Aljuaid, H. Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustain. Cities Soc.* **2020**, *55*, 102018. [CrossRef]
134. Vazirani, A.; o'Donoghue, O.; Brindley, D.; Meinert, E. Blockchain vehicles for efficient Medical Record management. *NPJ Digit. Med.* **2020**, *3*, 1. [CrossRef]
135. Kassab, M.; DeFranco, J.; Destefanis, G.; Graciano Neto, V. Exploring Research in Blockchain for Healthcare and a Roadmap for the Future. *IEEE Trans. Emerg. Top. Comput.* **2019**, *9*, 1835–1852. [CrossRef]
136. Kumar, T.; Ramani, V.; Ahmad, I.; Braeken, A.; Harjula, E.; Ylianttila, M. Blockchain Utilization in Healthcare: Key Requirements and Challenges. In Proceedings of the 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, Czech Republic, 17–20 September 2018; pp. 1–7. [CrossRef]
137. Vonitsanos, G.; Panagiotakopoulos, T.; Kanavos, A. Issues and Challenges of using Blockchain for IoT Data Management in Smart Healthcare. *Biomed. J. Sci. Tech. Res.* **2021**, *40*, 32052–32057.
138. Boulos, M.N.K.; Wilson, J.T.; Clauson, K.A. Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare. *Int. J. Health Geogr.* **2018**, *17*, 25. [CrossRef]
139. Igboanusi, I.S.; Allwinnaldo, A.; Alief, R.N.; Ansori, M.R.R.; Lee, J.M.; Kim, D.S. Smart auto mining (SAM) for industrial IoT blockchain network. *IET Commun.* **2022**, *16*, 2123–2132. [CrossRef]
140. Stagnaro, C. *White Paper: Innovative Blockchain Uses in Health Care*; Freed Associate. 2017. Available online: https://s3.amazonaws.com/arena-attachments/1649918/a272c30523a39678dadcddc272d53a24.pdf?1516914525 (accessed on 5 May 2024).
141. 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*, 1–20. [CrossRef]
142. Deepa, M.; Roshni Naveena, S.; Harini, N.D.; Sravika, V.; Soundarya, S.; Reshma, S. A Novel Electronic Medical Record Design Using Cryptography and Steganography Techniques. In Proceedings of the 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2–4 December 2021; pp. 377–382. [CrossRef]
143. Yu, Y.; Li, Q.; Zhang, Q.; Hu, W.; Liu, S. Blockchain-Based Multi-Role Healthcare Data Sharing System. In Proceedings of the 2020 IEEE International Conference on E-Health Networking, Application & Services (HEALTHCOM), Virtual Conference, 1–2 March 2021; pp. 1–6. [CrossRef]
144. Salim, M.M.; Park, J.H. Federated learning-based secure electronic health record sharing scheme in medical informatics. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 617–624. [CrossRef] [PubMed]

145. Ali, S.; Armand, T.P.T.; Athar, A.; Hussain, A.; Ali, M.; Yaseen, M.; Joo, M.I.; Kim, H.C. Metaverse in Healthcare Integrated with Explainable AI and Blockchain: Enabling Immersiveness, Ensuring Trust, and Providing Patient Data Security. *Sensors* **2023**, *23*, 565. [CrossRef] [PubMed]
146. Shurrab, S.; Duwairi, R. Self-supervised learning methods and applications in medical imaging analysis: A survey. *PeerJ Comput. Sci.* **2022**, *8*, e1045. [CrossRef] [PubMed]