data

MDPI

Perspective

Blockchain for Patient Safety: Use Cases, Opportunities and Open Challenges

Dounia Marbouh [1], Mecit Can Emre Simsekler [1,*], Khaled Salah [2], Raja Jayaraman [1] and Samer Ellahham [3]

[1] Department of Industrial and Systems Engineering, Khalifa University of Science and Technology, Abu Dhabi P.O. Box 127788, United Arab Emirates
[2] Department of Electrical Engineering and Computer Science, Khalifa University of Science and Technology, Abu Dhabi P.O. Box 127788, United Arab Emirates
[3] Department of Cardiovascular Medicine and Quality, Cleveland Clinic Abu Dhabi, Abu Dhabi P.O. Box 112412, United Arab Emirates
* Correspondence: emre.simsekler@ku.ac.ae; Tel.: +971-(0)-2-501-8410; Fax: +971-(0)-2-447-2442

Abstract: Medical errors are recognized as major threats to patient safety worldwide. Lack of streamlined communication and an inability to share and exchange data are among the contributory factors affecting patient safety. To address these challenges, blockchain can be utilized to ensure a secure, transparent and decentralized data exchange among stakeholders. In this study, we discuss six use cases that can benefit from blockchain to gain operational effectiveness and efficiency in the patient safety context. The role of stakeholders, system requirements, opportunities and challenges are discussed in each use case in detail. Connecting stakeholders and data in complex healthcare systems, blockchain has the potential to provide an accountable and collaborative milieu for the delivery of safe care. By reviewing the potential of blockchain in six use cases, we suggest that blockchain provides several benefits, such as an immutable and transparent structure and decentralized architecture, which may help transform health care and enhance patient safety. While blockchain offers remarkable opportunities, it also presents open challenges in the form of trust, privacy, scalability and governance. Future research may benefit from including additional use cases and developing smart contracts to present a more comprehensive view on potential contributions and challenges to explore the feasibility of blockchain-based solutions in the patient safety context.

Keywords: patient safety; blockchain; medical errors; communication; knowledge sharing; interoperability; healthcare operations; digital health

Citation: Marbouh, D.; Simsekler, M.C.E.; Salah, K.; Jayaraman, R.; Ellahham, S. Blockchain for Patient Safety: Use Cases, Opportunities and Open Challenges. *Data* **2022**, *7*, 182. https://doi.org/10.3390/data7120182

Academic Editors: Bijan Raahemi and Waeal J. Obidallah

Received: 21 September 2022
Accepted: 13 December 2022
Published: 16 December 2022

1. Introduction

Medical errors lead to significant patient safety challenges that harm thousands of patients worldwide every year [1]. Patient safety refers to the absence of avoidable harm to patients while receiving care and the elimination of preventable harm to a tolerable level. Organizational leadership, transparent policies, talented healthcare providers, systematic reporting, and effective patient involvement in their care are all needed to ensure sustainable and significant safety improvements [2]. However, more than 134 million adverse events occur annually in hospitals, resulting in 2.6 million deaths because of unsafe care [3]. These medical errors are the result of several deficiencies that hinder the full potential of the healthcare system; these include poor interoperability [4,5], lack of incident reporting [6], communication [7], and lack of efficient data sharing [8], among others.

To prevent these adverse events, various tools and methods, such as communication protocols and clinical decision support tools, have been developed and implemented [9,10]. Despite these efforts, there remains a lack of communication and interoperability issues between stakeholders arising from inconsistent data storage and reporting methods, which restrict providers from delivering quality care [11]. Furthermore, the current healthcare systems suffer from the lack of "correct" information, systematic reporting [6] and adequate

data sharing among stakeholders [8]. These are some significant challenges leading to operational failures, adverse events and medical errors [12]. Various studies also highlighted that fragmented communication among healthcare stakeholders contributes to increased medical errors [7,13–15].

The healthcare system started learning from the experiences of other high-risk domains and industries, namely, the nuclear industry and aviation [16,17], to develop a movement toward high reliability [18]. Examples of approaches and lessons learnt from high-risk industries include root cause analysis of safety incidents, now widely used in health care. Proactive risk assessment tools (such as failure modes and effects analysis) are now also used [19]. Proactive risk management and commitment to continuous learning and improvement are other lessons learnt from the high-risk industries [20]. In principle, these approaches can potentially enhance healthcare organizations' safety records. There are also several technological advances using artificial intelligence (AI) that can improve patient safety by automating tasks, enabling information sharing, reducing variation in practice, intercepting potential errors and improving clinical decision-making. Despite these substantial efforts, more improvement is needed in various areas, including communication, incident reporting and knowledge sharing among stakeholders.

To mitigate the fragmentation of data and communication, the lack of effective and efficient data sharing and the inconsistent data storage and reporting in healthcare systems, implementing an emerging technology such as blockchain can be beneficial since it offers decentralization. Blockchain is a decentralized, immutable and distributed record of transactions that are stored on a network of nodes over geographically dispersed locations [21–23]. Blockchain is classified as public, private, or a consortium based on who can participate in the network and how transactions get verified. By making each transaction auditable and permissionless, blockchains ensure data trust, integrity and verifiability [24]. Data are also secured thanks to cryptography that creates a provenance of transactions and makes the records tamper-evident. This technology can also be perceived as a consecutive chain of transactions chronologically appended to the previous ones. This is achieved by the network's participants, who contribute to solving the cryptographical puzzle, which then enhances the security of the system from malicious alterations and frauds [24]. In health care, the blockchain can enable better security, trust and transparency of medical data, processes and transactions and is actively being explored as a potential tool to improve care delivery [21]. Blockchain has many features, such as data security and privacy [25] and autonomy [26], which can significantly enhance the existing healthcare systems. In addition to the unique features, blockchain technology can also create decentralized transaction environments, which is why the healthcare industry is a good candidate. In addition to these benefits, this technology has promising opportunities for the healthcare industry, which are summarized in Table 1 as follows:

Table 1. Opportunities of Blockchain Technology in Health Care.

Healthcare Industry Challenges	Description	Blockchain Technology Opportunities
Fragmentation of Data	Fragmentation arises when healthcare systems are unable to communicate effectively between each other. This limits the utility of health data in answering critical medical questions [27].	▪ Decentralization of storage for patient data [21]. ▪ The ledger can be seen by all the participants and it is not owned by a central authority [12]. ▪ Decentralization of Internet of Things (IoT) data [28].

Table 1. *Cont.*

Healthcare Industry Challenges	Description	Blockchain Technology Opportunities
System Interoperability and Patient Data Access	Electronic health record (EHR) systems are an effective method to share patients' data. However, it is still a challenge to access scattered patient data through multiple channels because current EHRs are geographically limited or are affiliated to different hospitals.	▪ Decentralization of networks across geographies [29]. ▪ Automation, distribution and security of patient data access [30]. ▪ Real-time updates and data access across the network regardless of the location and trust levels [21].
Data Security	Medical data may be at risk of being leaked by malicious attackers in centralized networks. Centralization also make sensible health data vulnerable to single-point attack [31].	▪ Digitalization of participants' identity for enhanced data security (private and public keys) [31]. ▪ The technology is resilient to single point of failure and insider attacks [31].
Data Inconsistency	Data coming from different resources and systems face many challenges because of the inconsistency in naming, storing, structure and format [32], which restricts providers from delivering proper care [12].	▪ Smart contracts offer rule-based and consistent practices for patient data access and analysis [33]
Cost-Effectiveness	In centralized systems, there is a need for traditional intermediaries to manage and maintain the network. This results in excessive fees lost to third parties [34].	▪ Removal of central/third party eliminates the time lag in accessing data and saves fees paid to that party [35]. ▪ By allowing network participants to perform costless verification, blockchain lowers the costs of auditing transactions [34].

Blockchain can address critical problems, such as public health management, claims validation, and supply chain management [36]. Furthermore, various healthcare practices involve data stored with third parties, which is a significant concern for many stakeholders, including patients. Therefore, blockchain technology can potentially elevate such concerns and afford transparency to health data management processes while diminishing the risks of data mishandling or misuse that could affect patient safety [37]. Blockchain has long been discussed in health care in general, but little attention and research have focused solely on the area of patient safety in particular. Consequently, this study aims to make the following contributions:

- Discuss, analyze and explore the potential applications of blockchain to improve patient safety within some healthcare systems.
- Discuss some open research issues and challenges that impede the adoption of blockchain to fully realize its potential in optimizing operations in the healthcare industry.

The outline of the paper is as follows. The selected use cases are presented in Section 2. The potential implications of blockchain technology on patient safety, including implementation challenges, requirements and potential opportunities, are discussed in Section 3. Finally, conclusions, key findings and future research directions are revealed in Section 4.

2. Use Cases

The potential of blockchain technology has been witnessed in almost all sectors, and health care is no exception. Considering blockchain's system-wide applications in healthcare systems, it is imperative to understand the key responsibilities of the system users. The main stakeholders that will play a role in this technology are the healthcare

providers, patients, regulatory entities, manufacturers, distributors, insurance companies and researchers. Table 2 below summarizes their key roles and responsibilities:

Table 2. Roles and Responsibilities of Stakeholders in Patient Safety Context.

Stakeholder	Role	Key Responsibilities
Healthcare providers	Enter accurate and complete documentation into the system. Providers include (doctors, nurses, admins, pharmacists, etc.).	▪ Effective diagnosis and treatment. ▪ Exploit information and data on the system for better diagnosis. ▪ Accurate information reporting and documentation.
Patients	Provide accurate information to healthcare professionals (e.g., nurses, physicians, etc.).	▪ Access personal clinical data. ▪ Monitor and manage their data. ▪ Aggregate, exchange, donate or trade their health records. ▪ Report incidents.
Regulatory Authorities	Review and generate action plans. Develop guidance and advice.	▪ Develop guidance to minimize risks to patients. ▪ Analyze and monitor aggregated data.
Researchers/Academia	Explore further improvements and potential contributions to the technology.	▪ Research new methods to improve processes. ▪ Give insights and identify trends in health care. ▪ Conduct research on how to improve patient experience.
Manufacturers	Use raw materials to produce a medical device or a drug.	▪ Follow safety regulations and rules. ▪ Report issues with the manufactured goods. ▪ Verify any mishandling, fraud or counterfeiting.
Distributors	Buy large quantities of medical devices or drugs from manufacturers and sell them to healthcare providers.	▪ Follow safety rules and regulations. ▪ Ensure appropriate storage and handling of devices/drugs. ▪ Verify and report any mishandling, fraud or counterfeiting.
Insurance Companies	Investigate and honor valid medical insurance claims.	▪ Investigate claims. ▪ Pay claims to patients.

While Table 2 presents the roles and key responsibilities of the stakeholders, it is also essential to understand how they communicate with each other in blockchain-based systems. To address this, we explore the role of blockchain in the following six use cases that have a potential association with patient safety. A use case describes the behavior of a given system and its interactions with the participating actors. It provides a structure that illustrates functional requirements within the context of a system process. The use case also identifies external expectations for the system and specific features of the system. A use case can be expressed as a graphical element in a diagram or a textual document [38]. In this study, we provide graphical and textual elements to visualize the use case better.

Furthermore, we discuss opportunities and some open research challenges to realize its potential benefits in the patient safety context. All of the illustrated use cases feature the use of a decentralized storage system such as IPFS, Filecoin and Storj.io to store large-sized

data efficiently [39]. The integration of blockchain with such systems can overcome the storage limitations of blockchain technology. A decentralized storage system (e.g., IPFS) generates an irreversible hash of the stored data. Such hashes can be immutably recorded on the blockchain to assure that data stored on the decentralized storage system has not been modified [21].

2.1. Medical Devices

Medical devices are imperative in all areas of health care and play an essential role in the diagnosis, prevention and treatment of disorders and injuries. They range from physical devices such as advanced sticking plaster or scalpels to digital medical devices that contain software and digital networking capabilities such as pulse oximeters [40,41].

The current medical devices supply chain does not enable stakeholders to track all the transactions or monitor the device throughout every stage, compromising patient safety. In addition, the current supply chain of medical devices is centralized and insecure and lacks transparency across participants, which permits the central party to alter data without informing the other parties [42]. Alternatively, a blockchain-based solution would present data privacy and security, transparency, decentralization, immutability, traceability and verified transaction records. The blockchain can enhance the data integrity of the medical devices' supply chain and their traceability across the supply chain. It can also support the verification of medical devices' counterfeiting to enhance patient safety [43].

Blockchain technology can permanently store data related to various stages, phases and events of medical device manufacturing, such as (i) design and development, (ii) production, (iii) quality checks and (iv) distribution, to authorized businesses. Once the medical devices are distributed, providers can easily access the blockchain to identify, trace and verify the device information before dispensing it. Smart contracts can also provide opportunities to detect medical-device-related frauds and eliminate third-party services' role in monitoring these devices' logistics, including during distribution.

The immutability feature assures that the details about the medical device cannot be altered or deleted by anyone. Furthermore, smart contracts can use provenance data to identify the falsified and substandard medical devices produced and shipped through unlicensed manufacturers. For supply chain logistics services, smart contracts can be designed to track the conditions of containers when handling medical devices during their shipment to ensure their safety [44]. Furthermore, when the preassigned conditions for the medical devices' shipment are violated, the smart contracts can inform the appropriate authorities automatically. Sensors can also be placed in the containers to identify any illicit attempts that might interrupt the conditions of the packages carrying the medical devices [45]. Suspicious activities would be recorded and reported in real time to the relevant authority. The other advantages of blockchain for the logistics of medical devices include transparency, automation and reduced operational failures [46].

Figure 1 presents a generic blockchain-based system that can monitor the supply chain of medical devices. This system would consist of five smart contracts and a decentralized storage system. The pre-market contract would collect the design and development information of the device. The order management contract would provide information about the order details and the handling information provided by the GPS and sensors placed in the packages. Post-market contracts would provide data about any operational failure or defect within the product. The FDA or any other regulatory entity can use the data of the post-market contract to monitor and regulate the medical devices dispensed for enhanced patient safety. The role of the patient in this subsystem will consist of uploading any defects or issues with the defects. The patient can also use this platform to donate unwanted medical devices.

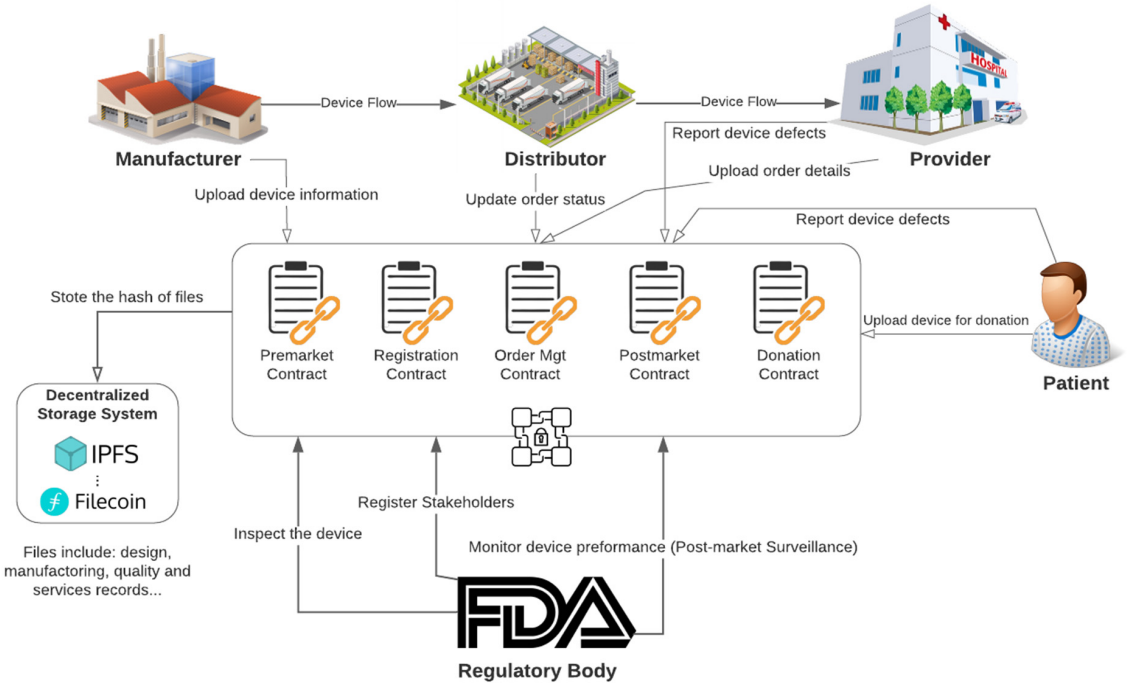

Figure 1. Blockchain-based Medical Devices Logistics Monitoring System.

2.2. Prescription Tracking (Opioid)

The opioid epidemic takes a significant toll with reference to livelihood globally. For instance, in 2019, nearly 50,000 people in America passed away from overdoses related to opioids [47]. The abuse and addiction of opioids is a severe crisis that impacts public health, the economy and social welfare. The Centers for Disease Control and Prevention (CDC) claims that the overall financial burden of opioid abuse in the US is $78.5 billion annually, including addiction rehabilitation treatments, criminal justice involvement, financial support for victims and lost productivity [48]. In 2020, the COVID-19 pandemic exacerbated this crisis [49] as hospital visits for opioids had increased by 34% [50]. Several public and private agencies actively implement different interventions to contain this epidemic. One promising intervention is the Prescription Drug Monitoring Program (PDMP), a database sharing health information on controlled substance prescriptions [51].

PDMPs proved to be effective within state limits in providing clinicians with information on a patient's controlled substance prescription history and screening those who may be at risk for abuse or diversion [52]. Consequently, several states have endorsed the adoption of PDMPs by listed dispensers and prescribers to make informed medical decisions [53]. However, several challenges hinder the success of the current PDMPs on a national level; these include (a) the lack of standardization across the states, (b) centralization of data and therefore vulnerability to various threats and (c) lack of interoperability and constrained data sharing across states [47]. As a result of these challenges, the PDMP users tend not to have information on patients' recent prescriptions [54]. Patients with opioid misuse tendencies or addiction can exploit these system gaps with doctors and pharmacy shops across different states and, consequently, get more than the necessary drug dosage.

Therefore, developing a robust real-time prescription-tracking system that is trusted, secure, transparent and accessible to all participants is essential [51]. The inherent features of blockchain technology, such as transparency, immutability, automation and easy access, are suitable for attaining these goals. Unlike the PDMPs that are (i) centralized, (ii) prone to data leakage, (iii) vulnerable to the point of failure and (iv) inherently incapable of efficiently tracing the data provenance of the drug, a blockchain-based monitoring system would allow providers and dispensers to record opioid transaction records securely and transparently.

The real-time dissemination of prescription and dispensing information would alleviate numerous challenges in the existing US opioid system, mainly the duplicated opioid orders for the same patient. Consequently, patients taking opioids will have regulated and restricted access to these drugs, which will increase their safety in return. Figure 2 illustrates a generic blockchain-based system that can control prescribing controlled drugs like opioids. This subsystem can detect if the patient is doctor-shopping to avoid prescription abuse.

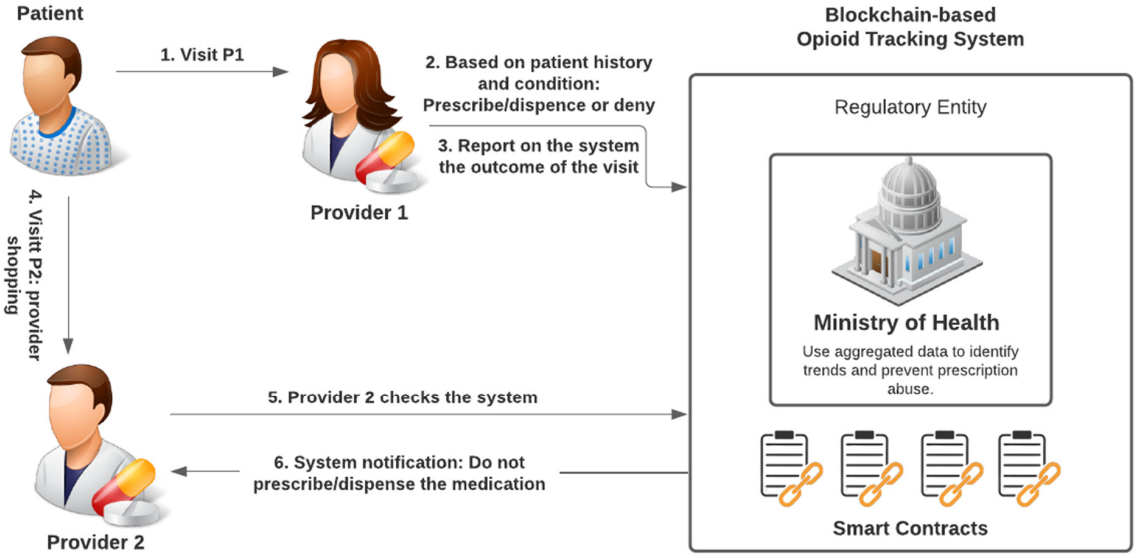

Figure 2. Blockchain-based Controlled Drugs (Opioid) Monitoring System.

2.3. Remote Patient Monitoring (RPM)

The COVID-19 pandemic has caused enormous disruptions and posed real challenges to healthcare providers worldwide [55]. As physical interaction between patients and healthcare providers has unexpectedly become fraught with dangers, interest in digital technologies has intensified. Digital wearable technology has paved the way for new opportunities in the realm of medical sensors, specifically for remote patient monitoring (RPM) [30]. RPM enables patients to assess and share their medically vital signs with providers while using mobile health (mHealth) apps together with medical devices such as blood pressure sensors. The collected medical data from different patients can be grouped and presented on a dashboard that can then be monitored by a provider [56].

Centralization is a major obstacle in the current RPM systems. In fact, data in existing RPM systems are vulnerable to a wide range of data breaches (internal and external), compromising the safety of patients and the reliability of these systems [55]. In addition, in existing RPM systems, providers cannot handle the silos of patient medical records created by limited data integrity and sharing, which can compromise treatment efficiency and, thus, patient safety. Blockchain technology can be a solution as it can provide a view of the health records for all participating stakeholders [55]. Thanks to the transparency of health records, providers in the system would be able to trace and verify patients' medical histories before recommending any treatment and thus avoid medical errors [57].

Figure 3 presents a generic blockchain-enabled system that can be used to monitor patients remotely [55]. The wearable devices generate data that is transferred to the blockchain network and stored in a decentralized system. The provider accesses this data to assess the patient's condition and send timely feedback to improve patient care. Other stakeholders can be granted access to the network. For example, researchers can use the aggregated data to improve patient care and safety, track and understand some conditions and identify trends. As per the patients' role, they will be uploading sensor-related data and would be receiving health-related notifications and alerts in case of a

serious condition. Other stakeholders involve regulatory entities that review the wearable devices' performance and regulate its dispensing for enhanced patient safety.

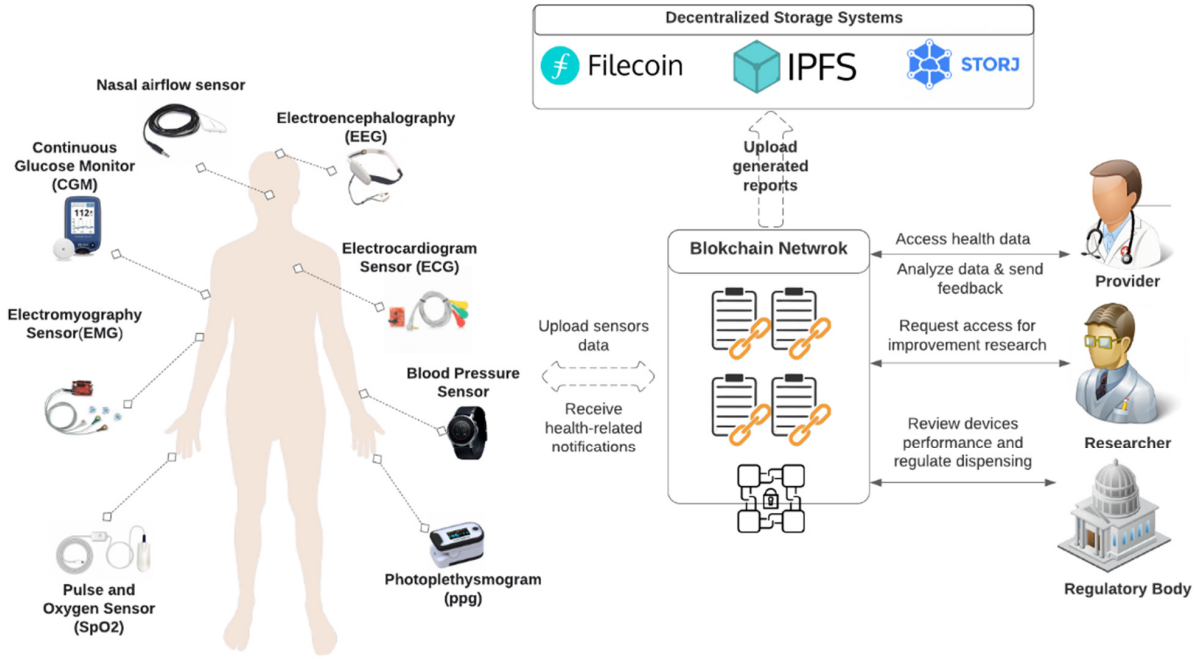

Figure 3. Blockchain-enabled Remote Patient Monitoring System.

2.4. Counterfeit Drugs

The World Health Organization (WHO) defines counterfeit drugs as "drugs that are manufactured fraudulently, mislabeled, with low quality, hiding the source detail or identity and do not follow the defined standard" [58]. These drugs might include certain genuine ingredients. However, they may also contain lethal ingredients. If consumed, they can lead to dangerous health complications [59]. Currently, the pharmaceutical industry is dependent on central databases based on the Electronic Data Interchange (EDI). The central database approach is expensive and makes large-scale interoperability nearly unachievable [60].

Furthermore, this system is also fraught with many risks such as diversion, trust gaps between the siloed systems, counterfeits and single points of failure. Therefore, having a decentralized, transparent and reliable system is required to alleviate some of these challenges. Thanks to its built-in features, blockchain technology can be piloted by the pharmaceutical industry as a solution to tracking and tracing the manufactured and shipped drugs. Blockchain can also remove the need for individual wholesalers to handle large volumes of product lists and thus mitigate errors and offer significant savings to the entire supply chain [61].

Using blockchain, stakeholders can execute many transactions such as (i) verifying drug information, (ii) tracking orders information, (iii) tracing orders and (iv) updating records. Figure 4 presents a blockchain-backed system that can be used to trace drugs. The users of the system include patients, manufacturers, distributors, pharmacies and providers. This blockchain-enabled system can allow users to control and oversee the supply chain of drugs and assist in detecting frauds. The participating stakeholders can also verify the authenticity of drugs and identify signs of tampering or poor handling during their shipment. Blockchain technology's inherent features, such as transparency, would also enable storing all movements, ownership details and modifications to the drug. The participants' data would also be registered and stored within the blockchain system. Consequently, the participants are able to connect to the blockchain network and verify the relevant transactions. Hence, patients will obtain permission to verify the complete

details of dispensed drugs, which will increase their safety. Thereby, this would enhance the security levels of the pharmaceutical supply chain and the levels of safety for the patients.

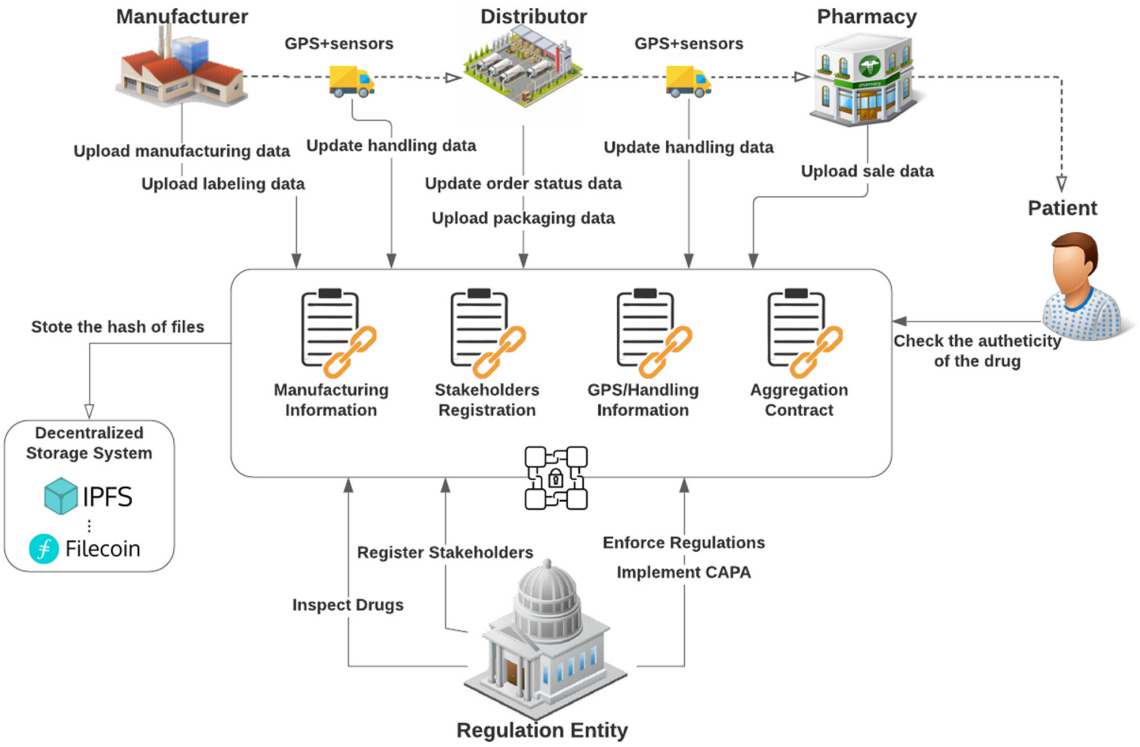

Figure 4. Blockchain-backed Drugs Traceability System.

2.5. Electronic Health Records

Electronic health records (EHRs) involve sensitive and vital medical data linked to patients, often exchanged among clinicians, radiologists and pharmacists for successful examination, diagnosis and treatment. Throughout the transmission, storage and dissemination of these sensitive data across several healthcare stakeholders, data can eventually be lost, unrecorded or modified. As a result, the treatment of the patient could be compromised, which can present serious threats to patient safety [62,63]. For patients who suffer from chronic conditions, such as HIV, cancer or diabetes, the prevalence of these threats can grow because of the lengthy record of follow-ups, rehabilitation and pre- and post-treatments [63]. In recent studies by CRICO, the risk management arm of the Harvard Medical Institutions, of more than 23,000 patient safety issues and medical error claims, it was found that out of every ten medical error cases, three are due to a communication deficiency. Communication issues are not unique to providers with low "people skills" or patients with understanding shortfalls. Nor is the issue limited to misunderstood or misspoken language. Adverse events arise because the medical data was misdirected, unrecorded or never received or retrieved. Moreover, it is estimated that 80% of serious adverse events occur because of miscommunication between healthcare providers during patient transfers [64].

One effective solution to mitigate the patient safety issues stemming from fragmented communication is to achieve healthcare interoperability. Interoperability refers to the capability of various software applications and IT systems, such as the EHR system, to share data, cross-communicate and make use of the exchanged data regardless of the stakeholders' location. Attaining interoperability would allow providers to share patient medical records (with the patient's permission), irrespective of the location of participants or their trust levels. Transparent and secure data sharing is critical to delivering an effective diagnosis, informing medical decisions and treatment, and avoiding any possible adverse events [65]. Data sharing would also enhance the accuracy of diagnosis by collecting recommendations

and opinions of several medical professionals and preventing inadequacies and adverse events in the treatment and medication plans [66].

Figure 5 presents a generic blockchain-enabled system that can be used to manage patients' health records. This network would capture and store the visit details, medical tests and results. The patient grants access to providers who can retrieve this data in real time. Consequently, all providers would gain access to identical updated records and make informed medical decisions regardless of their location or trust levels. By increasing the interoperability, patient data aggregation, analysis and communication are also improved. This makes it easier to consider all facets of a patient's condition, supporting diagnostic and therapeutic decision-making. The off-chain participating stakeholders, if granted access, can also use the same data to perform various tasks such as clinical research, understanding medical conditions, processing insurance claims and identifying diagnostic discrepancies.

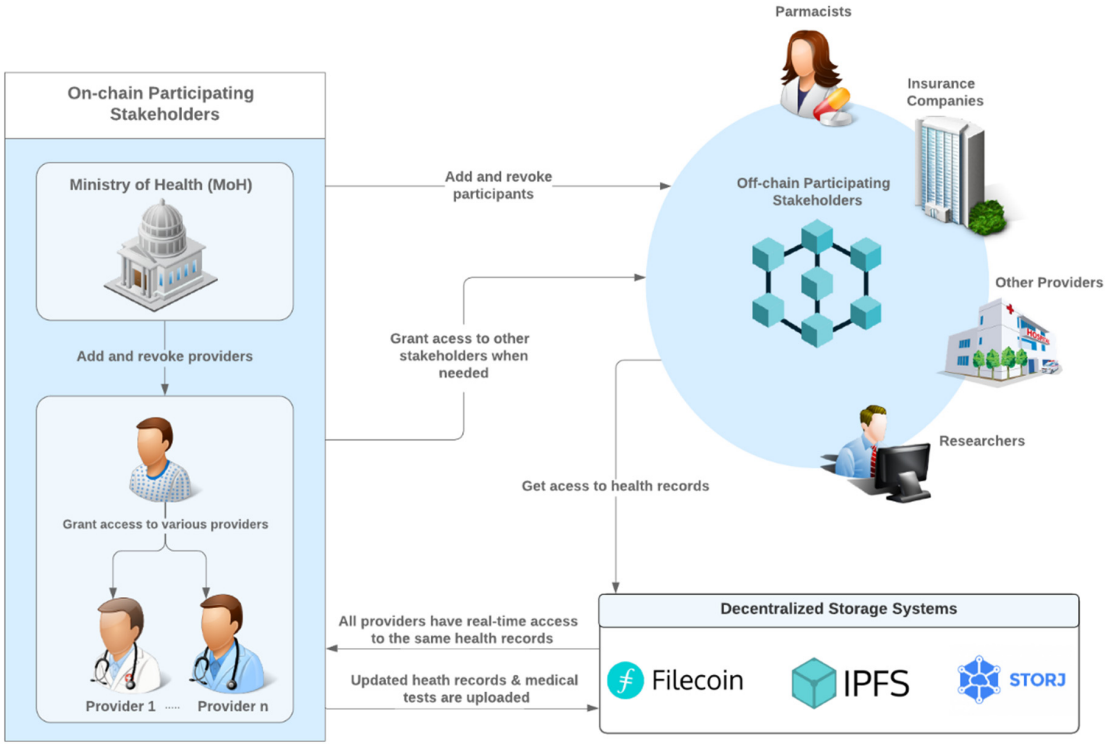

Figure 5. Blockchain-based Health Records Management System.

2.6. Incident Reporting System

Incident reporting systems (IRSs) are widely used tools for risk management in accelerating patient safety worldwide. The main drive of incident reporting is to advance the safety of patients by learning from previously made mistakes [67]. Some hospitals may have their internal incident reporting system, the so-called local reporting management system (LMRS), used for incident reporting. Some countries have implemented national-level centralized reporting systems to share learning with all possible stakeholders [33]. As of now, the IRS has several issues and problems that hinder its full potential, such as the lack of information dissemination in real time, absence of incentives, lack of security and privacy, fragmentation of adverse-events data across different providers [68] and the inability to have feedback on the actions taken, if any, of the incident [69]. Centralization is also a serious hindrance in current incident reporting systems that threaten patients' data leakage and single point of failure. To address the current needs of the reporting systems, blockchain technology and its unique features can be exploited. This technology's key opportunities, such as data transparency, decentralization, security, privacy, payment settlement and traceability, can be of great use to ensure a better reporting culture and system [33].

A blockchain-based incident reporting system solution can support traceability and transparency and align communications among network participants. It can also guarantee data privacy, immutability and security while reassuring the collection of incidents from various stakeholders. The IPFS technology can also be added and integrated to store various files, such as incident reports. This proposed solution can also guarantee the consistency and reliability of reporting while preserving high efficiency even in a non-fully trusted environment [33].

Confidentiality and ease of use are essential incentives in reporting that might be provided by blockchain technology. Figure 6 presents a generic system overview diagram of a blockchain-based incident reporting system. This system enables several network participants to report incident data in privacy, security and transparency. Another unique feature of this system is the incentivizing and rewarding of reporting entities to further encourage the reporting culture. By adding an incentive mechanism and the analysis and feedback mechanisms, healthcare providers and patients would be encouraged to report and share incidents. This solution can also benefit other stakeholders who can use the incident data for several purposes. For instance, researchers can use these data to identify and analyze the trends of incidents. Patients in this platform would be able to report incidents to alert others and receive feedback for enhanced safety. Regulatory entities can also use the incident data to enforce regulations and implement corrective action plans to enhance patient care and safety [33].

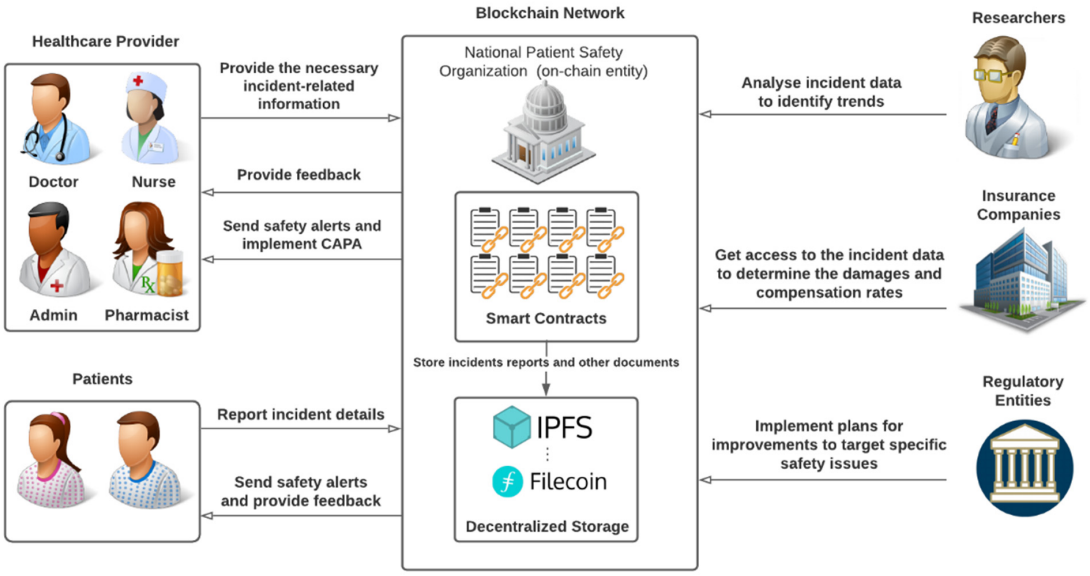

Figure 6. Blockchain-based Incident Reporting System.

3. Discussion

Healthcare systems are siloed and centralized, making them prone to deletion, alterations and fraud. These current centralized systems have reliability issues [29] as they are vulnerable to single points of failure [45]. They also offer limited opportunities for collaboration and coordination among stakeholders, such as the government, regulatory bodies and providers [46]. Such centralized systems also fail to offer transparency, traceability and immutability of stored data [70]. Blockchain, on the other hand, is a promising technology that can assist in improving healthcare systems by connecting stakeholders to improve patient safety. It can reshape healthcare systems by streamlining operations and communication, enforcing trust and eliminating fragmentation of data sharing [21,71].

Table 3 summarizes the opportunities above and highlights the key challenges and requirements for the achievement of each use case. This summary is the result of an extensive literature review. It also represents the opportunities this technology can bring about for the selected application areas to introduce the features of blockchain.

Table 3. Blockchain for Patient Safety: Use Cases, Opportunities and Open Challenges.

Application	Current Challenges	Requirements	Blockchain Opportunities	Stakeholders	Implementation Challenges
Medical Devices	▪ Failure to rapidly detect safety issues related to marketed medical devices ▪ Failure to monitor the device's handling [72] ▪ Lack of security and standardization of PMS data [43]	▪ Identification of mishandling ▪ Fast identification of counterfeit [72] ▪ Detection of medical devices fraud [43] ▪ Increase the scrutiny of device safety [43]	▪ Transparency of medical devices logistics [73] ▪ Verification of authenticity of medical device [73] ▪ Secure real-time exchange of PMS data [43] ▪ Notify authorities when preassigned conditions for the shipment are violated [46]	▪ Patients ▪ Healthcare providers ▪ Distributors ▪ Manufacturers ▪ Regulators	▪ Integrating this blockchain-based system with existing healthcare systems [73] ▪ GDPR and data privacy [44]
Incident Reporting System (IRS)	▪ Lack of information dissemination in real time [69] ▪ Absence of incentives ▪ Lack of security and privacy [68] ▪ Fragmentation of adverse-events data across different providers [13] ▪ Centralization of the reporting system [33]	▪ Alignment of stakeholders' communication [33] ▪ Real-time dissemination of incidents [33] ▪ Creation of an incentivizing system for reporting [33,74] ▪ Standardization of incidents reporting across providers [33]	▪ Assurance of traceability of reported incidents [61] ▪ Consistency of incident reporting ▪ Incentive solution to reporting parties ▪ Establishing an interconnective system [33]	▪ Patients ▪ Hospital staff ▪ Pharmacists ▪ Insurance companies ▪ Regulatory entities	▪ A large amount of incident data: IRS can produce large volumes of data that require rapid processing [33] ▪ Scalability: block size and creation time [21]
Electronic Health Records (EHRs)	▪ Lack of interoperability between disparate systems [75] ▪ Fragmented communication among providers [7] ▪ Low security and privacy of patient data [31]	▪ Improvement of stakeholders' communication [8] ▪ Achieve the ability to communicate and exchange data promptly [8] ▪ Eliminate the need of re-doing medical tests [23] ▪ Data sharing among providers [65]	▪ Access to complete medical history of patients for an informed diagnosis [62] ▪ Data access and control based on consent management [76] ▪ Streamlined hospital operations and communication [75] ▪ Transparent payment settlement [75]	▪ Patient ▪ Hospital staff ▪ Pharmacists ▪ Researchers ▪ Insurance companies	▪ Vulnerabilities in smart contracts can influence its usual performance, resulting in disruption of the patient health history [77] ▪ Scalability: block size and creation time [21] ▪ Providers' willingness and readiness to switch to a new system [78]

Table 3. *Cont.*

Application	Current Challenges	Requirements	Blockchain Opportunities	Stakeholders	Implementation Challenges
Remote Patient Monitoring	▪ Limited data sharing among providers compromises safety ▪ The inability of health organizations to manage the silos of patient health records due to limited data sharing ▪ Risk of external and internal patient data breaches [30]	▪ Prompt feedback to the patient [33] ▪ Allow patients to join and exit the network easily [12] ▪ Enable data sharing among providers [8] ▪ Easier payments settlement ▪ Patient data privacy [55]	▪ Sending feedback to patient in real-time for effective treatment and increased safety [55] ▪ Preserving patient anonymity [31] ▪ Establishing trust among RPM participants ▪ Automating the payments settlement [56] ▪ Trigger timely alerts to providers and health centers [55]	▪ Patient ▪ Providers ▪ Researchers ▪ Regulators	▪ Large-sized health data: RPM produce large volumes of data that require rapid processing [55] ▪ Registering and verifying sensors: sensors used by providers need to be registered and verified by the blockchain to avoid errors in diagnosis and treatment [57]
Prescription Tracking (Opioid)	▪ Lack of standardization of documentation across the US states [48] ▪ Asymmetric information among stakeholders [53] ▪ Vulnerability to use system gaps to doctor shop ▪ Lack of interoperability ▪ Constrained data sharing across states [47,48,54]	▪ Track and trace the medical history of the patient [47] ▪ Verify reported data to identify any possible addiction [54] ▪ Trace the data provenance of the drug [54]	▪ Provide prompt and real-time dispensing and prescribing information [48,54] ▪ Automating the dispensing process [54] ▪ Seamlessly identify a patient that may have an addiction [47] ▪ Preserving patient anonymity [31]	▪ Patient ▪ Hospital staff ▪ Pharmacists ▪ Regulators	▪ Regulations on opioid vary globally [48] ▪ Lack of clarity on compliance [47]
Counterfeit Drugs	▪ Inability to promptly identify safety issues associated with drugs [60] ▪ Failure to track the handling of the drugs [79] ▪ Absence of information about the shipment handling [46]	▪ Ability to track and trace the origin of the drug [79] ▪ Check non-compliance with safety rules and regulations [46] ▪ Identification of any sign of tampering or inadequate handling during the shipment [80] ▪ Verification of drugs authenticity [58]	▪ Transparency of drugs logistics [79] ▪ Easy verification of the authenticity of the drug [58] ▪ Assurance of compliance with FDA handling rules [80] ▪ Notify authorities when preassigned conditions for the shipment are violated [46]	▪ Patient ▪ Hospital staff ▪ Pharmacists ▪ Researchers ▪ Manufacturers ▪ Distributors	▪ This technology cannot be easily plugged into current healthcare systems [21] ▪ Throughput and latency: the high latency of the network can result in lower transaction throughput [21] ▪ Scalability [21]

It is essential to understand the critical characteristics that blockchain has and the promising solutions it offers. However, it is also essential to analyze the challenges this technology may encounter. Implementing this technology will pave the way toward various opportunities but also challenges to key stakeholders. These implementation challenges include the following:

Interoperability. The proposed blockchain-enabled systems for patient safety are expected to offer well-suited solutions for different issues, such as privacy, security, integrity, interoperability and data sharing. Interoperability is very crucial to achieve smooth data sharing among several blockchain networks. Currently, the different blockchain platforms cannot interchange information (i.e., Bitcoin and Hyperledger). In addition, it is challenging to propose standardized interoperability-supported solutions because of the variations in consensus protocols, languages and protection levels of the smart contracts [21]. Considering the complex nature of the healthcare industry, the proposed interoperability solution must ensure secure, transparent, low cost and privacy-preserving features.

Healthcare System Readiness. The literature confirms that blockchain requires a strong synergy among the stakeholders, not only healthcare providers, patients and managers but also suppliers and blockchain experts, to have a successful implementation. Blockchain is still in its infancy and is therefore facing standardization and introduction challenges. Medical facilities lack the expertise to utilize this technology. In fact, blockchain systems would ideally involve providers and patients as end users. As a result, the system may face competing interests in the interface design and presentation of data. In addition, failure to design an easily accessible user interface can lead to reduced workflow efficiency, undermine the patient–physician relationship and increase clinician burnout [81]. Therefore, it is imperative to have all the system's stakeholders aligned with the right expertise to facilitate the introduction of this technology in a ready environment.

Lack of Legislation. Distributed technologies such as blockchain have gained momentum and attracted several healthcare organizations [82]. However, governments have not yet established regulatory practices over blockchain. Hence, the adoption of this technology will necessitate substantial buy-in from the global healthcare participants [83]. Blockchain technology is still evolving, and regulatory frameworks, standards and regulations regarding its applicability are still in the early phase [84]. For instance, there are many challenges around the proper laws and rules to regulate the ownership of medical transactions and records in health care [85]. Medical data ownership is an important issue that needs to be tackled because of the significant number of stakeholders in health care and the complexity of the system. In addition, the current healthcare system's medical rules, laws and regulations are key challenges that still need to be addressed appropriately. Therefore, this technology still requires comprehensive study to establish guidelines and regulations for the healthcare industry. Some organizations have started proposing architectures for blockchain governance, integration and interoperability [82].

Scalability. The scalability is one major limitation that hinders the widespread implementation of blockchain in the healthcare industry [12]. Health records involve sizeable volumes of data, such as medical tests and images—notably for patients with chronic diseases. These large-scale datasets are difficult to electronically share because of the size limitations in blocks [26]. Conventional centralized systems are sophisticated and mature to manage thousands of transactions per second. Visa, for instance, can handle more than 1700 transactions per second [12], while Ethereum can only process 20 transactions, approximately, per second. As per the private blockchains, the processing nodes operate under reliable parties, so scalability is not a problem. There are various ways to deal with the scalability issue; these include (a) adding a second layer to the primary blockchain network (lightning network), (b) sharding techniques and (c) directed acyclic graph (DAG) [21,86].

Cyber-attacks. Blockchains are mainly prone to attacks known as the 51% attack [87]. Fraudulent and malicious attacks are increasingly more complicated because of the increase in cyber organizations and sophisticated malware threats. Valuable and sensitive data such as medical information are desirable to several users and organizations, and they

might attempt stealing them [88]. This type of attack occurs when one or a group of miners manipulate more than half of the overall mining hash rate of the system. By manipulating more than half of the computing power, the fraudulent or malicious participant can create blocks faster than the rest of the network. Consequently, the network becomes obliged to shift to the desired chain of the attacking party. However, though these types of attacks are achievable, the likelihood of a successful one is very low [89]. Recent studies also highlighted this issue in similar contexts, including COVID-19 [90] and health insurance authentication [91].

4. Conclusions

In this paper, we discussed the potential contribution of blockchain technology to improve patient safety. We presented six use cases with relevant stakeholders that could benefit from the reliability, trust and collaboration features of blockchain. Furthermore, we identified and presented issues that may hinder the widespread adoption of blockchain technology in the patient safety context. Our key findings and recommendations include:

- Blockchain presents several benefits, such as an automated, decentralized, transparent and immutable architecture, which proves valuable for transforming health care and enhancing patient safety.
- The benefits of blockchain technology, such as security, decentralization, traceability and transparency, can significantly assist healthcare stakeholders in developing solutions to improve patient safety.
- Blockchain technology has the potential to provide an accountable and collaborative milieu for stakeholders that are involved in the delivery of care.
- While blockchain offers key opportunities, it also brings challenges in various forms, such as governance issues, interoperability, security, privacy and scalability.

Our study has some limitations. It should be noted that this is a perspective paper with no empirical evidence to report. For instance, no smart contract was developed to explore the contributions and limitations of blockchain in various measures, e.g., transparency, traceability and communication among stakeholders, in the given six case studies. Future studies can develop smart contracts along with cost and security analysis to explore the feasibility of blockchain-based solutions in health care. Furthermore, various technologies, e.g., IPFS technology to store patient clinical data and operational data, can be integrated and evaluated for their implications for patient safety.

There are six use cases presented in this study. Future research may benefit from including additional use cases to present a more comprehensive view on potential challenges and contributions with blockchain technology in the patient safety context.

Author Contributions: Conceptualization, D.M., M.C.E.S. and K.S.; Methodology, M.C.E.S.; Validation, M.C.E.S., K.S., R.J. and S.E.; Formal analysis, M.C.E.S.; Resources, M.C.E.S.; Writing—original draft, D.M. and M.C.E.S.; Writing—review & editing, M.C.E.S., K.S., R.J. and S.E.; Visualization, D.M., M.C.E.S. and K.S.; Supervision, M.C.E.S., K.S. and R.J. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Khalifa University of Science and Technology under Award CIRA-2019-001 and RCII-2019-002-Research Center for Digital Supply Chain and Operations Management. The funding body had no direct involvement in the design, data collection, analysis, and interpretation, or in writing the manuscript.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declared no potential conflict of interest with respect to the authorship and/or publication of this article.

References

1. Shojania, K.G.; Thomas, E.J. Trends in Adverse Events over Time: Why Are We Not Improving? *BMJ Qual. Saf.* **2013**, *22*, 273–277. [CrossRef] [PubMed]
2. Simsekler, M.C.E.; Qazi, A. Adoption of a Data-Driven Bayesian Belief Network Investigating Organizational Factors That Influence Patient Safety. *Risk Anal.* **2020**. [CrossRef] [PubMed]
3. Dhingra-Kumar, N.; Brusaferro, S.; Arnoldo, L. Patient Safety in the World. In *Textbook of Patient Safety and Clinical Risk Management*; Donaldson, L., Ricciardi, W., Sheridan, S., Tartaglia, R., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 93–98. ISBN 978-3-030-59403-9.
4. Li, E.; Clarke, J.; Neves, A.L.; Ashrafian, H.; Darzi, A. Electronic Health Records, Interoperability and Patient Safety in Health Systems of High-Income Countries: A Systematic Review Protocol. *BMJ Open* **2021**, *11*, e044941. [CrossRef] [PubMed]
5. Heubusch, K. Interoperability: What It Means, Why It Matters. *J. AHIMA* **2006**, *77*, 26–30.
6. Clarke, J.R. How a System for Reporting Medical Errors Can and Cannot Improve Patient Safety. *Am. Surg.* **2006**, *72*, 1088–1091. [CrossRef]
7. Robben, S.H.; Huisjes, M.; van Achterberg, T.; Zuidema, S.U.; Olde Rikkert, M.G.; Schers, H.J.; Heinen, M.M.; Melis, R.J. For the ZOWEL NN Study Group Filling the Gaps in a Fragmented Health Care System: Development of the Health and Welfare Information Portal (ZWIP). *JMIR Res. Protoc.* **2012**, *1*, e10. [CrossRef]
8. Krahe, M.A.; Wolski, M.; Mickan, S.; Toohey, J.; Scuffham, P.; Reilly, S. Developing a Strategy to Improve Data Sharing in Health Research: A Mixed-Methods Study to Identify Barriers and Facilitators. *Health Inf. Manag. J.* **2020**, 183335832091720. [CrossRef]
9. Webb, J.; Sorensen, A.; Sommerness, S.; Lasater, B.; Mistry, K.; Kahwati, L. Advancing Perinatal Patient Safety through Application of Safety Science Principles Using Health IT. *BMC Med. Inform. Decis. Mak.* **2017**, *17*, 176. [CrossRef]
10. Wang, Y.; Coiera, E.; Runciman, W.; Magrabi, F. Using Multiclass Classification to Automate the Identification of Patient Safety Incident Reports by Type and Severity. *BMC Med. Inform. Decis. Mak.* **2017**, *17*, 84. [CrossRef]
11. Hawashin, D.; Jayaraman, R.; Salah, K.; Yaqoob, I.; Simsekler, M.C.E.; Ellahham, S. Blockchain-Based Management for Organ Donation and Transplantation. *IEEE Access* **2022**, *10*, 59013–59025. [CrossRef]
12. Vazirani, A.A.; O'Donoghue, O.; Brindley, D.; Meinert, E. Implementing Blockchains for Efficient Health Care: Systematic Review. *J. Med. Internet Res.* **2019**, *21*, e12439. [CrossRef]
13. Manser, T. Fragmentation of Patient Safety Research: A Critical Reflection of Current Human Factors Approaches to Patient Handover. *J. Public Health Res.* **2013**, *2*, e33. [CrossRef] [PubMed]
14. Kern, L.M.; Safford, M.M.; Slavin, M.J.; Makovkina, E.; Fudl, A.; Carrillo, J.E.; Abramson, E.L. Patients' and Providers' Views on Causes and Consequences of Healthcare Fragmentation in the Ambulatory Setting: A Qualitative Study. *J. Gen. Intern. Med.* **2019**, *34*, 899–907. [CrossRef] [PubMed]
15. Bourgeois, F.C. Patients Treated at Multiple Acute Health Care Facilities: Quantifying Information Fragmentation. *Arch. Intern. Med.* **2010**, *170*, 1989. [CrossRef] [PubMed]
16. Kapur, N.; Parand, A.; Soukup, T.; Reader, T.; Sevdalis, N. Aviation and Healthcare: A Comparative Review with Implications for Patient Safety. *JRSM Open* **2016**, *7*, 2054270415616548. [CrossRef] [PubMed]
17. Simsekler, M.C.E.; Card, A.J.; Ward, J.R.; Clarkson, P.J. Trust-Level Risk Identification Guidance in the NHS East of England. *Int. J. Risk Saf. Med.* **2015**, *27*, 67–76. [CrossRef]
18. Sheikhtaheri, A.; Sadeqi-Jabali, M.; Hashemi-Dehaghi, Z. Physicians' Perspectives on Causes of Health Care Errors and Preventive Strategies: A Study in a Developing Country. *Iran. J. Public Health* **2018**, *47*, 720–728.
19. Simsekler, M.C.E. The Link Between Healthcare Risk Identification and Patient Safety Culture. *Int. J. Health Care Qual. Assur.* **2019**, *32*, 574–587. [CrossRef]
20. Liberati, E.G.; Peerally, M.F.; Dixon-Woods, M. Learning from High Risk Industries May Not Be Straightforward: A Qualitative Study of the Hierarchy of Risk Controls Approach in Healthcare. *Int. J. Qual. Health Care* **2018**, *30*, 39–43. [CrossRef]
21. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for Healthcare Data Management: Opportunities, Challenges, and Future Recommendations. *Neural Comput. Appl.* **2021**. [CrossRef]
22. Mackey, T.K.; Kuo, T.-T.; Gummadi, B.; Clauson, K.A.; Church, G.; Grishin, D.; Obbad, K.; Barkovich, R.; Palombini, M. 'Fit-for-Purpose?'—Challenges and Opportunities for Applications of Blockchain Technology in the Future of Healthcare. *BMC Med.* **2019**, *17*, 68. [CrossRef]
23. Sultana, M.; Hossain, A.; Laila, F.; Taher, K.A.; Islam, M.N. Towards Developing a Secure Medical Image Sharing System Based on Zero Trust Principles and Blockchain Technology. *BMC Med. Inform. Decis. Mak.* **2020**, *20*, 256. [CrossRef]
24. Amir Latif, R.M.; Hussain, K.; Jhanjhi, N.Z.; Nayyar, A.; Rizwan, O. A Remix IDE: Smart Contract-Based Framework for the Healthcare Sector by Using Blockchain Technology. *Multimed. Tools Appl.* **2020**. [CrossRef]
25. Onik, M.M.H.; Aich, S.; Yang, J.; Kim, C.-S.; Kim, H.-C. Blockchain in Healthcare: Challenges and Solutions. In *Big Data Analytics for Intelligent Healthcare Management*; Academic Press: Cambridge, MA, USA, 2019; pp. 197–226; ISBN 978-0-12-818146-1.
26. Zhang, P.; Schmidt, D.C.; White, J.; Lenz, G. Blockchain Technology Use Cases in Healthcare. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2018; Volume 111, pp. 1–41; ISBN 978-0-12-813852-6.
27. Agrawal, R.; Prabakaran, S. Big Data in Digital Healthcare: Lessons Learnt and Recommendations for General Practice. *Heredity* **2020**, *124*, 525–534. [CrossRef]

28. Al Breiki, H.; Al Qassem, L.; Salah, K.; Habib Ur Rehman, M.; Sevtinovic, D. Decentralized Access Control for IoT Data Using Blockchain and Trusted Oracles. In Proceedings of the 2019 IEEE International Conference on Industrial Internet (ICII), Orlando, FL, USA, 11–12 November 2019; pp. 248–257.
29. Natsiavas, P.; Rasmussen, J.; Voss-Knude, M.; Votis, K.; Coppolino, L.; Campegiani, P.; Cano, I.; Marí, D.; Faiella, G.; Clemente, F.; et al. Comprehensive User Requirements Engineering Methodology for Secure and Interoperable Health Data Exchange. *BMC Med. Inform. Decis. Mak.* **2018**, *18*, 85. [CrossRef]
30. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *J. Med. Syst.* **2018**, *42*, 130. [CrossRef]
31. Shi, S.; He, D.; Li, L.; Kumar, N.; Khan, M.K.; Choo, K.-K.R. Applications of Blockchain in Ensuring the Security and Privacy of Electronic Health Record Systems: A Survey. *Comput. Secur.* **2020**, *97*, 101966. [CrossRef]
32. Hammad, R.; Barhoush, M.; Abed-alguni, B.H. A Semantic-Based Approach for Managing Healthcare Big Data: A Survey. *J. Healthc. Eng.* **2020**, *2020*, 8865808. [CrossRef]
33. Marbouh, D.; Simsekler, M.C.E.; Salah, K.; Jayaraman, R.; Ellahham, S. Blockchain-Based Incident Reporting System for Patient Safety and Quality in Healthcare. In *Trust Models for Next-Generation Blockchain Ecosystems*; Rehman, M.H.U., Svetinovic, D., Salah, K., Damiani, E., Eds.; EAI/Springer Innovations in Communication and Computing; Springer International Publishing: Cham, Switzerland, 2021; pp. 167–190; ISBN 978-3-030-75106-7.
34. Azzolini, D.; Riguzzi, F.; Lamma, E. Studying Transaction Fees in the Bitcoin Blockchain with Probabilistic Logic Programming. *Information* **2019**, *10*, 335. [CrossRef]
35. Chiu, J.; Koeppl, T.V. *Blockchain-Based Settlement for Asset Trading*; Queen's University, Department of Economics: Kingston, ON, Canada, 2018.
36. Jayaraman, R.; Al Hammadi, F.; Simsekler, M.C.E. Managing Product Recalls in Healthcare Supply Chain. In Proceedings of the 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bangkok, Thailand, 16–19 December 2018; pp. 293–297. [CrossRef]
37. Yoon, H.-J. Blockchain Technology and Healthcare. *Healthc. Inform. Res.* **2019**, *25*, 59. [CrossRef]
38. Armour, F.; Miller, G. *Advanced Use Case Modeling: Software Systems*; Pearson Education: London, UK, 2000.
39. Zahed Benisi, N.; Aminian, M.; Javadi, B. Blockchain-Based Decentralized Storage Networks: A Survey. *J. Netw. Comput. Appl.* **2020**, *162*, 102656. [CrossRef]
40. Stern, A.D.; Gordon, W.J.; Landman, A.B.; Kramer, D.B. Cybersecurity Features of Digital Medical Devices: An Analysis of FDA Product Summaries. *BMJ Open* **2019**, *9*, e025374. [CrossRef]
41. Tervoort, T.; De Oliveira, M.T.; Pieters, W.; Van Gelder, P.; Olabarriaga, S.D.; Marquering, H. Solutions for Mitigating Cybersecurity Risks Caused by Legacy Software in Medical Devices: A Scoping Review. *IEEE Access* **2020**, *8*, 84352–84361. [CrossRef]
42. Clauson, K.A.; Breeden, E.A.; Davidson, C.; Mackey, T.K. Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare:: An Exploration of Challenges and Opportunities in the Health Supply Chain. *Blockchain Healthc. Today* **2018**. [CrossRef]
43. Pane, J.; Verhamme, K.M.C.; Shrum, L.; Rebollo, I.; Sturkenboom, M.C.J.M. Blockchain Technology Applications to Postmarket Surveillance of Medical Devices. *Expert Rev. Med. Devices* **2020**, *17*, 1123–1132. [CrossRef]
44. 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]
45. Ahmad, R.; Salah, K.; Jayaraman, R.; Yaqoob, I.; Ellahham, S.; Omar, M. Blockchain and COVID-19 Pandemic: Applications and Challenges. *IEEE TechRxiv* **2020**. [CrossRef]
46. Omar, I.; Debe, M.; Jayaraman, R.; Salah, K.; Omar, M.; Arshad, J. Blockchain-Based Supply Chain Traceability for COVID-19 PPE. *TechRxiv* **2020**. [CrossRef]
47. Raghavendra, M. Can Blockchain Technologies Help Tackle the Opioid Epidemic: A Narrative Review. *Pain Med.* **2019**, *20*, 1884–1889. [CrossRef]
48. Florence, C.S.; Zhou, C.; Luo, F.; Xu, L. The Economic Burden of Prescription Opioid Overdose, Abuse, and Dependence in the United States, 2013. *Med. Care* **2016**, *54*, 901–906. [CrossRef]
49. El-Tallawy, S.N.; Nalamasu, R.; Pergolizzi, J.V.; Gharibo, C. Pain Management During the COVID-19 Pandemic. *Pain Ther.* **2020**, *9*, 453–466. [CrossRef]
50. Baumgartner, J.C.; Radley, D.C. The Spike in Drug Overdose Deaths During the COVID-19 Pandemic and Policy Options to Move Forward. *Commonw. Fund* **2021**. Available online: https://www.commonwealthfund.org/blog/2021/spike-drug-overdose-deaths-during-covid-19-pandemic-and-policy-options-move-forward (accessed on 1 September 2022).
51. Chenthara, S.; Wang, H.; Ahmed, K.; Whittaker, F.; Ji, K. A Blockchain Based Model for Curbing Doctors Shopping and Ensuring Provenance Management. In Proceedings of the 2020 International Conference on Networking and Network Applications (NaNA), Haikou City, China, 10–13 December 2020; pp. 186–192.
52. D'Souza, R.S.; Lang, M.; Eldrige, J.S. Prescription Drug Monitoring Program. In *StatPearls*; StatPearls Publishing: Treasure Island, FL, USA, 2021. Available online: http://www.ncbi.nlm.nih.gov/books/NBK532299/ (accessed on 1 September 2022).
53. Islam, M.M.; McRae, I.S. An Inevitable Wave of Prescription Drug Monitoring Programs in the Context of Prescription Opioids: Pros, Cons and Tensions. *BMC Pharmacol. Toxicol.* **2014**, *15*, 46. [CrossRef]

54. Gonzales, A.; Smith, S.R.; Dullabh, P.; Hovey, L.; Heaney-Huls, K.; Robichaud, M.; Boodoo, R. Potential Uses of Blockchain Technology for Outcomes Research on Opioids. *JMIR Med. Inform.* **2021**, *9*, e16293. [CrossRef]
55. 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. Inf.* **2021**, *148*, 104399. [CrossRef]
56. Hathaliya, J.; Sharma, P.; Tanwar, S.; Gupta, R. Blockchain-Based Remote Patient Monitoring in Healthcare 4.0. In Proceedings of the 2019 IEEE 9th International Conference on Advanced Computing (IACC), Tiruchirappalli, India, 13–14 December 2019; pp. 87–91.
57. Jamil, F.; Ahmad, S.; Iqbal, N.; Kim, D.-H. Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals. *Sensors* **2020**, *20*, 2195. [CrossRef]
58. Sylim, P.; Liu, F.; Marcelo, A.; Fontelo, P. Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention. *JMIR Res. Protoc.* **2018**, *7*, e10163. [CrossRef]
59. Jamil, F.; Hang, L.; Kim, K.; Kim, D. A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital. *Electronics* **2019**, *8*, 505. [CrossRef]
60. Anand, R.; Niyas, K.; Gupta, S.; Revathy, S. Anti-Counterfeit on Medicine Detection Using Blockchain Technology. In *Inventive Communication and Computational Technologies*; Ranganathan, G., Chen, J., Rocha, Á., Eds.; Lecture Notes in Networks and Systems; Springer: Singapore, 2020; Volume 89, pp. 1223–1232; ISBN 9789811501456.
61. Musamih, A.; Salah, K.; Jayaraman, R.; Arshad, J.; Debe, M.; Al-Hammadi, Y.; Ellahham, S. A Blockchain-Based Approach for Drug Traceability in Healthcare Supply Chain. *IEEE Access* **2021**, *9*, 9728–9743. [CrossRef]
62. Dubovitskaya, A.; Xu, Z.; Ryu, S.; Schumacher, M.; Wang, F. Secure and Trustable Electronic Medical Records Sharing Using Blockchain. *AMIA Annu. Symp. Proc. AMIA Symp.* **2017**, *2017*, 650–659.
63. Siyal, A.A.; Junejo, A.Z.; Zawish, M.; Ahmed, K.; Khalil, A.; Soursou, G. Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives. *Cryptography* **2019**, *3*, 3. [CrossRef]
64. CRICO. *Malpractice Risks in Communication Failures*; The Risk Management Foundation of the Harvard Medical Institutions: Boston, MA, USA, 2015.
65. 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]
66. Madine, M.M.; Salah, K.; Jayaraman, R.; Yaqoob, I.; Al-Hammadi, Y.; Ellahham, S.; Calyam, P. Fully Decentralized Multi-Party Consent Management for Secure Sharing of Patient Health Records. *IEEE Access* **2020**, *8*, 225777–225791. [CrossRef]
67. Hagley, G.; Mills, P.D.; Watts, B.V.; Wu, A.W. Review of Alternatives to Root Cause Analysis: Developing a Robust System for Incident Report Analysis. *BMJ Open Qual.* **2019**, *8*, e000646. [CrossRef]
68. Anderson, J.E.; Kodate, N.; Walters, R.; Dodds, A. Can Incident Reporting Improve Safety? Healthcare Practitioners' Views of the Effectiveness of Incident Reporting. *Int. J. Qual. Health Care* **2013**, *25*, 141–150. [CrossRef]
69. Macrae, C. The Problem with Incident Reporting: Table 1. *BMJ Qual. Saf.* **2016**, *25*, 71–75. [CrossRef]
70. Omar, I.A.; Jayaraman, R.; Salah, K.; Simsekler, M.C.E.; Yaqoob, I.; Ellahham, S. Ensuring Protocol Compliance and Data Transparency in Clinical Trials Using Blockchain Smart Contracts. *BMC Med. Res. Methodol.* **2020**, *20*. [CrossRef]
71. Guttman, O.T.; Lazzara, E.H.; Keebler, J.R.; Webster, K.L.W.; Gisick, L.M.; Baker, A.L. Dissecting Communication Barriers in Healthcare: A Path to Enhancing Communication Resiliency, Reliability, and Patient Safety. *J. Patient Saf.* **2018**, *1*, e1465–e1471. [CrossRef]
72. Casino, F.; Dasaklis, T.K.; Patsakis, C. A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
73. Reda, M.; Kanga, D.B.; Fatima, T.; Azouazi, M. Blockchain in Health Supply Chain Management: State of Art Challenges and Opportunities. *Procedia Comput. Sci.* **2020**, *175*, 706–709. [CrossRef]
74. Kingston, M.J.; Evans, S.M.; Smith, B.J.; Berry, J.G. Attitudes of Doctors and Nurses towards Incident Reporting: A Qualitative Analysis. *Med. J. Aust.* **2004**, *181*, 36–39. [CrossRef]
75. Dubovitskaya, A.; Baig, F.; Xu, Z.; Shukla, R.; Zambani, P.S.; Swaminathan, A.; Jahangir, M.M.; Chowdhry, K.; Lachhani, R.; Idnani, N.; et al. ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care. *J. Med. Internet Res.* **2020**, *22*, e13598. [CrossRef]
76. Mayer, A.H.; da Costa, C.A.; da Rosa Righi, R. Electronic Health Records in a Blockchain: A Systematic Review. *Health Inform. J.* **2020**, *26*, 1273–1288. [CrossRef]
77. Khan, S.N.; Loukil, F.; Ghedira-Guegan, C.; Benkhelifa, E.; Bani-Hani, A. Blockchain Smart Contracts: Applications, Challenges, and Future Trends. *Peer-Peer Netw. Appl.* **2021**, *14*, 2901–2925. [CrossRef]
78. Alzahrani, S. Assessment of the Blockchain Technology Adoption for the Management of the Electronic Health Record Systems. Ph.D. Thesis, Portland State University, Portland, OR, USA, 2021.
79. Uddin, M.; Salah, K.; Jayaraman, R.; Pesic, S.; Ellahham, S. Blockchain for Drug Traceability: Architectures and Open Challenges. *Health Inform. J.* **2021**, *27*, 146045822110112. [CrossRef]
80. Tandon, A.; Dhir, A.; Islam, A.K.M.N.; Mäntymäki, M. Blockchain in Healthcare: A Systematic Literature Review, Synthesizing Framework and Future Research Agenda. *Comput. Ind.* **2020**, *122*, 103290. [CrossRef]
81. Mehta, S.; Grant, K.; Ackery, A. Future of Blockchain in Healthcare: Potential to Improve the Accessibility, Security and Interoperability of Electronic Health Records. *BMJ Health Care Inform.* **2020**, *27*, e100217. [CrossRef]

82. Wasim Ahmad, R.; Hasan, H.; Yaqoob, I.; Salah, K.; Jayaraman, R.; Omar, M. Blockchain for Aerospace and Defense: Opportunities and Open Research Challenges. *Comput. Ind. Eng.* **2021**, *151*, 106982. [CrossRef]
83. Attaran, M. Blockchain Technology in Healthcare: Challenges and Opportunities. *Int. J. Healthc. Manag.* **2022**, *15*, 70–83. [CrossRef]
84. Agbo, C.; Mahmoud, Q.; Eklund, J. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* **2019**, *7*, 56. [CrossRef]
85. Leeming, G.; Cunningham, J.; Ainsworth, J. A Ledger of Me: Personalizing Healthcare Using Blockchain Technology. *Front. Med.* **2019**, *6*, 171. [CrossRef]
86. Mazlan, A.A.; Mohd Daud, S.; Mohd Sam, S.; Abas, H.; Abdul Rasid, S.Z.; Yusof, M.F. Scalability Challenges in Healthcare Blockchain System—A Systematic Review. *IEEE Access* **2020**, *8*, 23663–23673. [CrossRef]
87. Sayeed, S.; Marco-Gisbert, H. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Appl. Sci.* **2019**, *9*, 1788. [CrossRef]
88. Ye, C.; Li, G.; Cai, H.; Gu, Y.; Fukuda, A. Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting. In Proceedings of the 2018 5th International Conference on Dependable Systems and Their Applications (DSA), Dalian, China, 22–23 September 2018; pp. 15–24.
89. Chen, H.S.; Jarrell, J.T.; Carpenter, K.A.; Cohen, D.S.; Huang, X. Blockchain in Healthcare: A Patient-Centered Model. *Biomed. J. Sci. Tech. Res.* **2019**, *20*, 15017–15022.
90. Malik, H.A.M.; Shah, A.A.; Muhammad, A.; Kananah, A.; Aslam, A. Resolving Security Issues in the IoT Using Blockchain. *Electronics* **2022**, *11*, 3950. [CrossRef]
91. Sutanto, E.; Mulyana, R.; Arisgraha, F.C.S.; Escrivá-Escrivá, G. Integrating Blockchain for Health Insurance in Indonesia with Hash Authentication. *J. Theor. Appl. Electron. Commer. Res.* **2022**, *17*, 1602–1615. [CrossRef]