applied sciences

MDPI

Review

Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research

Seyednima Khezr [1,*], Md Moniruzzaman [1], Abdulsalam Yassine [2] and Rachid Benlamri [2]

[1] Department of Electrical and Computer Engineering, Lakehead University, 955 Oliver Road, Thunder Bay, ON P7B 5E1, Canada; mmoniruz@lakeheadu.ca

[2] Department of Software Engineering, Lakehead University, 955 Oliver Road, Thunder Bay, ON P7B 5E1, Canada; ayassine@lakeheadu.ca (A.Y.); rbenlamr@lakeheadu.ca (R.B.)

* Correspondence: skhezr@lakeheadu.ca; Tel.: +1-807-633-5840

Received: 1 April 2019; Accepted: 22 April 2019; Published: 26 April 2019

Abstract: One of the most important discoveries and creative developments that is playing a vital role in the professional world today is blockchain technology. Blockchain technology moves in the direction of persistent revolution and change. It is a chain of blocks that covers information and maintains trust between individuals no matter how far they are. In the last couple of years, the upsurge in blockchain technology has obliged scholars and specialists to scrutinize new ways to apply blockchain technology with a wide range of domains. The dramatic increase in blockchain technology has provided many new application opportunities, including healthcare applications. This survey provides a comprehensive review of emerging blockchain-based healthcare technologies and related applications. In this inquiry, we call attention to the open research matters in this fast-growing field, explaining them in some details. We also show the potential of blockchain technology in revolutionizing healthcare industry.

Keywords: blockchain technology; healthcare; data management; supply chain management; internet of medical things

1. Introduction

The rapid uptake of digitization in healthcare has led to the generation of massive electronic records about patients. Such growth poses unprecedented demands for healthcare data protection while in use and exchange. The rise of blockchain technology as a responsible and transparent mechanism to store and distribute data is paving the way for new potentials of solving serious data privacy, security, and integrity issues in healthcare. Blockchain technology has attracted considerable attention from industry as well as academics over the past few years. Indeed, new blockchain applications and research studies surface every day [1–4]. A blockchain technology is identified as a distributed ledger technology for peer-to-peer (P2P) network digital data transactions that may be publicly or privately distributed to all users, allowing any type of data to be stored in a reliable and verifiable way [1,5]. Another main concept of the blockchain is the smart contract, a legally binding policy that consists of customizable set of rules under which different parties agree to interact among each other in the form of decentralized automation [6,7]. The blockchain technology has given rise to numerous smart contract applications in several areas, ranging from energy resources [8], financial services [9,10], voting [11–13] and healthcare [6]. Blockchain technology offers transparency and eradicates the need for third-party administrators or intermediaries [1]. It uses consensus mechanisms and cryptography to verify the legitimacy of a transaction in a trustless and unreliable environment [1,14]. In a blockchain distributed P2P network of transactions, the receiving node checks the message; if the message is correct, then it stores it in a block. A consensus algorithm is

then used to confirm the data in each block; this is called "Proof-of-work (PoW)". The block will be added into the chain after performing the consensus algorithm, every node in the network admits this block and incessantly spreads the chain [15,16]. One of the most prominent applications of blockchain technology is healthcare. The potential of blockchain in healthcare is to overcome the challenges related to data security, privacy, sharing and storage [17,18]. One of the requirements for the healthcare industry is Interoperability. It is the ability of two parties, either human or machine, to exchange data or information precisely, efficiently, and consistently [19–22]. The goal of interoperability in healthcare is to facilitate the exchange of health-related information, such as electronic health record (EHR), among healthcare providers and patients so that the data can be shared throughout the environment and distributed by different hospital systems [23–26]. Moreover, interoperability enables providers to securely share patient medical records (given patient permissions to do so), regardless of the provider's location and trust relationships between them [27]. This is specifically important considering that the source of healthcare data is diverse. This aspect of interoperability is resolved by using blockchain technology which showed potential to store, manage, and share EHRs safely amongst healthcare communities [28]. Additionally, increasing costs of healthcare infrastructures and software in the industry have caused tremendous pressure on world economies [29]. In the healthcare sector, blockchain technology is positively affecting healthcare outcomes of companies and stakeholders to optimize business processes, improve patient outcomes, patient data management, enhance compliance, lower costs, and enable better use of healthcare-related data [30]. Equally important is the ability of blockchain technology to influence the flow of drugs and medical equipment in a long complicated healthcare supply chain. A blockchain for the healthcare supply chain promises to eliminate the risk of counterfeited drugs that endanger patients across the globe. Blockchain technology is currently being explored across various healthcare applications such as data management, storage, devices connectivity and security in the internet of medical things (IoMT). Most benefits provided by blockchain technology in the above-mentioned application areas impacted positively quality of experience (QoE) of most stakeholders and end users, including patients, care givers, researchers, pharmaceutical companies, and insurance companies. The ability to share healthcare data without the risk of jeopardizing users' privacy and data security is one essential step to make the healthcare system smarter and improve the quality of healthcare services and users' experience. The purpose of this paper is to provide a timely review on the applications of blockchain technology in healthcare and their impact on healthcare economies, QoE, and new business opportunities.

There are currently several review papers in the open literature dealing with the application of blockchain technology in domains such as finance [31–34], internet of things (IoT) [35–39], energy sector [8,40,41], government [42–44], and privacy and security [15,45–47]. While a few review papers are addressing the applications of blockchain technology in healthcare, a broad comprehensive critical review of the most recent research on blockchain-based healthcare applications is not covered. For example, the work presented by Mettler [48] provides a short review of healthcare applications that use blockchain technology. The study considers only three areas, public health management, user-oriented medical, and drug counterfeiting. Although the study was the first to present a high level review of emerging blockchain-based healthcare applications, it focuses mainly on functional aspects and benefits of such technology. In 2017, Kuo et al. [49] published another review paper on healthcare and biomedical applications based on blockchain technology. The work in Kuo et al. [49] mainly discusses traditional blockchain technology (bitcoin features) and its architecture. Then, the authors describe some aspects of blockchain technology for medical record management, insurance claim process, biomedical research, and health data ledger. In addition, the authors did not explain the technical aspects on how knowledge would be centrally distributed. In a similar study, Stagnaro et al. [50] describe some use cases for applying blockchain technology in healthcare. The use cases were particularly focusing on interoperability claims adjunction and patient care records, as well as supply chain management (SCM). The main shortcoming of the study is the limitation of use cases, and does not narrowly track novel blockchain based healthcare applications. Hölbl et al. [51] provide an

organized analysis of healthcare applications that use blockchain technology. The authors discussed a number of published articles in this domain from 2008 to 2019 and provided a systematic literature review. However, it does not critically assess the experiments conducted in the studied application domains. In another related work, Radanović and Likić [52] reviewed blockchain technology in medicine, including health insurance, EHRs, drug supply, biomedical research, procurement processes, and medical education. Similar to other surveys, the paper did not study some of the important blockchain-based healthcare applications, such as smart contract, data sharing, interoperability and cloud storage. Siyal et al. [53] discussed several blockchain-based healthcare applications, including fraud detection, neuroscience research, clinical research, and EHR. The main issue in Siyal et al. [53] work is that many recently published papers were not included. McGhin et al. [54] provided a review on healthcare industry requirements to protect patients' medical information using blockchain. This survey [54] discussed limited applications for healthcare such as OmniPHR [55], Medrec [56], Pervasive social network (PSN) [57], MeDshare [58] and Healthcare Data Gateway [59].

Based on the conducted literature review, we believe that no review paper so far conducted a comprehensive classification for blockchain technology in healthcare applications. To address this shortcoming, we aim, in this paper, to provide the reader with technical background in diverse blockchain-based healthcare applications, focusing on latest development as well as achievements in this area. This paper provides a broad technical study of recent blockchain technologies deployed in healthcare, and analyzes their strengths and weaknesses. The paper also discusses current research challenges, open issues, and research perspectives in each of the healthcare application areas. In outline, the contributions of this article are as follows:

- Providing a review of the various current usages of blockchain technology for healthcare applications.
- Discussing the key challenges for the healthcare applications in the blockchain technology.
- Describing and stressing the guidelines for future investigation and open issues about blockchain-based healthcare applications.
- Discussing the benefits and drawbacks of existing blockchain-based healthcare applications.

The remainder of this article is as follows. In Section 2, emerging blockchain-based healthcare applications are broadly classified and the workflow from raw data to stakeholders within healthcare blockchain architecture is described. Section 3 describes the blockchain in health data management, for which Section 4 describes recent progress in blockchain supply chain management. Section 5 discusses recent research in IoMT, Healthcare IoT Infrastructure and Data Security and Artificial Intelligence (AI). Finally, conclusions and future research directions are provided in Section 6.

2. Blockchain-Based Healthcare Applications

Blockchain technology is redefining data modeling and governance deployed in many healthcare applications. This is mainly due to its adaptability and abilities to segment, secure and share medical data and services in an unprecedented way. Blockchain technology is at the centre of many current developments in the healthcare industry. Emerging blockchain-based healthcare technologies are conceptually organized into four layers, including data sources, blockchain technology, healthcare applications, and stakeholders. Figure 1 illustrates a representation of blockchain-based workflow for healthcare applications.

Initially, all the data from medical devices, labs, social media, and many other sources are consolidated and create raw data that subsequently grew in scale to big data. This data is the essential ingredient of the whole blockchain-based healthcare, and it is the principal component which creates the first layer of the stack. Blockchain technology sits on the top of the raw data layer that is considered the core framework in pursuit to create a secured healthcare architecture that is divided into four components. Each blockchain platform has different features such as consensus algorithms and protocols [60]. Blockchain platforms facilitate users to create and manage their

transactions. Several blockchain platforms were created and are currently in use, such as Ethereum [61], Ripple [62], and Hyperledger Fabric [63]. The primary components of the blockchain are smart contracts, signatures, wallet, events, membership and digital assets. For communicating with other programs and frameworks, or even across different networks, a wide range of protocols could be used. This may include for instance, P2P, centralized, decentralized, and distributed. Policymakers could make a choice either public, private or even federate based on the range of requirements they need to fulfill. Once the platform is created by implementing blockchain technology, the next phase is to ensure that the applications are integrated with the whole system. Blockchain-based healthcare applications can be classified into three broad classes. Firstly, data management, including global scientific data sharing for research and development (R&D), data management, data storage (e.g., cloud-based applications) and EHRs. The second class represents SCM applications, including clinical trials and pharmaceuticals. Finally, the third class covers the IoMT, including a confluence of healthcare IoT and medical devices, healthcare IoT infrastructure and data security, and AI. Figure 2 illustrates healthcare applications in the blockchain. Finally, at the top of the hierarchy comes the stakeholder layer, which consists of parties who are benefiting from blockchain based healthcare applications such as business users, researchers, and patient. The main concerns of users at this layer is to effectively share, process and manage data without jeopardizing its security and privacy.

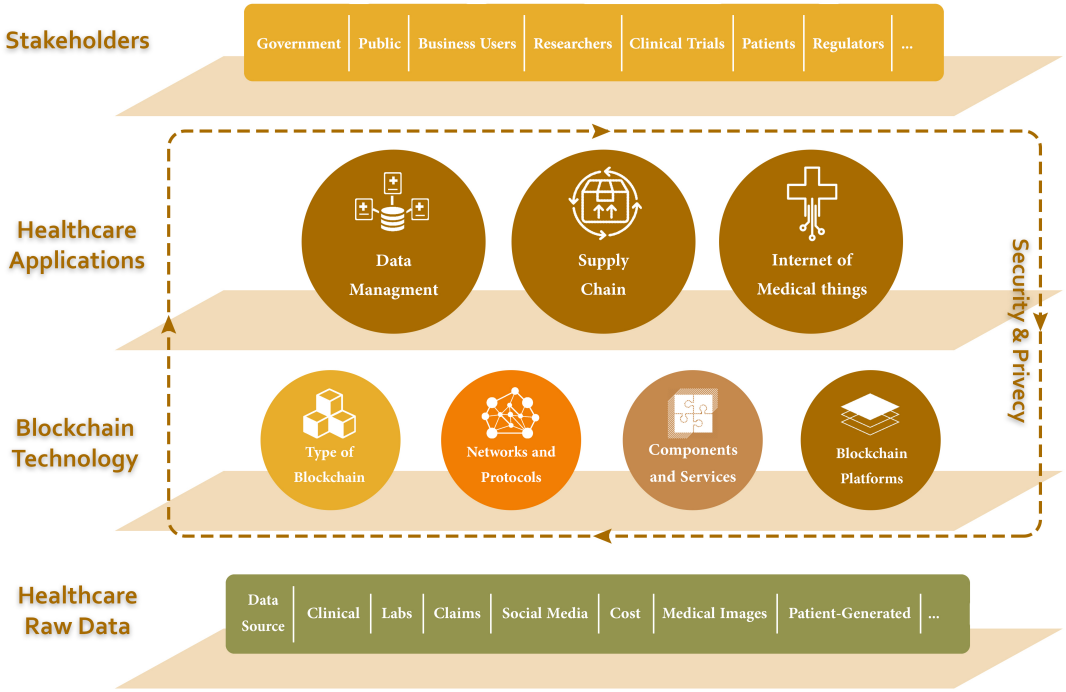

Figure 1. A workflow of blockchain-based healthcare applications. The workflow is composed of four main layers including healthcare raw data, blockchain technology, healthcare application, and stakeholders. The blockchain as a decentralized technology enables multiple stakeholders to benefit from healthcare applications.

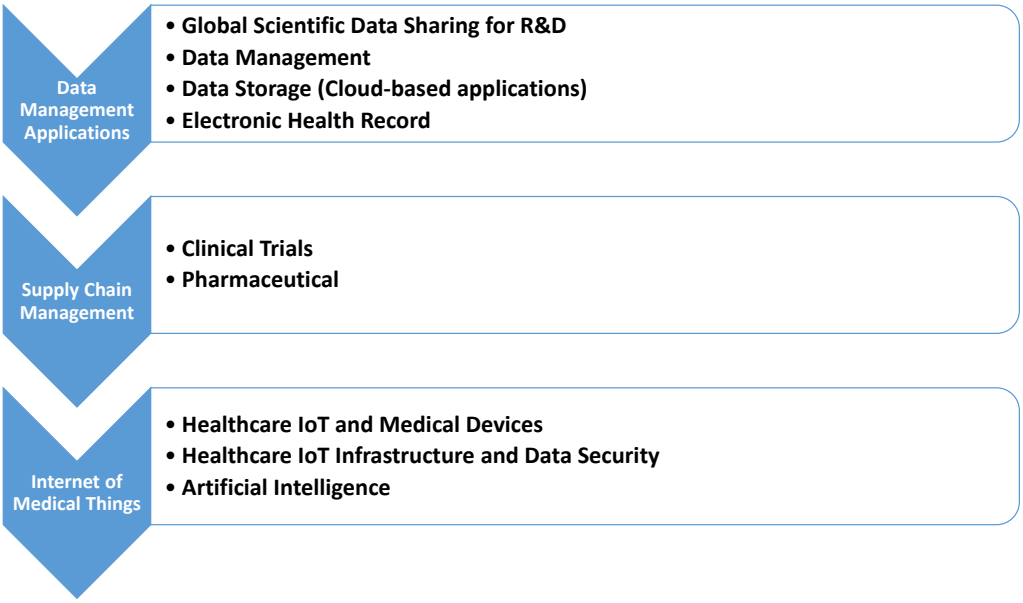

Figure 2. Blockchain-based healthcare applications.

3. Blockchain-Based Healthcare Management Applications

With the progress in electronic health-related data, cloud healthcare data storage and patient data privacy protection regulations, new opportunities are opening for health data management, as well as for patients' convenience to access and share their health data [64]. Securing data, storage, transaction, and managing their smooth integration are immensely valuable to any data-driven organization, especially in healthcare where blockchain technology has the potential to resolve these critical issues in a robust and effective way. Figure 3 shows seven steps of healthcare data management workflow in blockchain, which are discussed below. Blockchain based applications in this category include data sharing, data management, data storage (e.g., cloud-based applications) and EHR, which are discussed in details below.

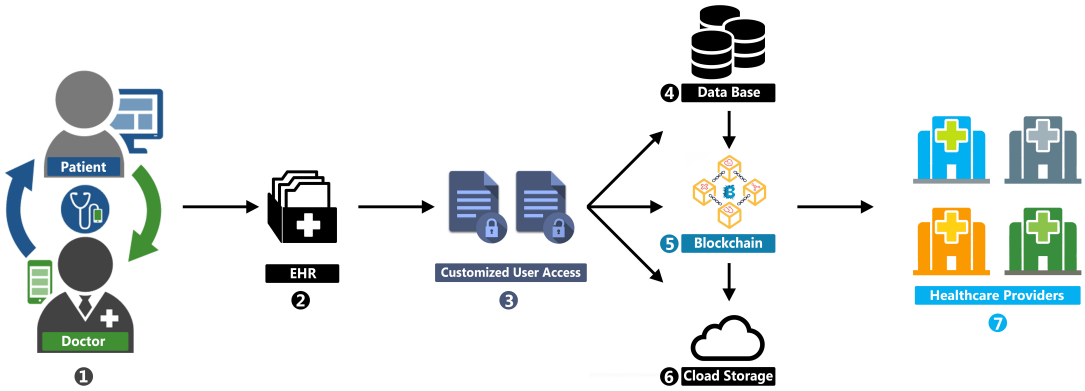

Figure 3. Healthcare data management in blockchain.

- Step-1: Primary data is generated by the interaction between a patient and their doctors and specialists. This data consists of medical history, current problem and other physiological information.
- Step-2: An EHR is created for each patient using the primary data collected in the first step. Other medical information such as those generated from nursing care, medical imaging, and drug history are also included in EHR.
- Step-3: Individual patient who has the ownership of sensitive EHR, and customized access control is given only to the owner of this property. Parties who want to access such valuable information must request permission which is forwarded to the EHR owner, and the owner will decide to whom access will be granted.
- Step-4, 5, and 6: These three steps are part of the core of the whole process including database, the blockchain, and cloud storage. Database and cloud storage store the records in a distributed manner and a blockchain provides extreme privacy to ensure customized authentic user access.
- Step-7: Healthcare providers such as ad hoc clinic, community care center, hospitals are the end user who wants to get access for a safe and sound care delivery which will be authorized by the owner. For example, no matter where you are treated in the globe, your health record will be available and accessible on your phone and validated through a distributed ledger such as blockchain, to which healthcare providers would continue to add to over time [65].

3.1. Global Scientific Data Sharing

Sharing of healthcare and medical data is one main and essential step to improve the quality of healthcare providers and make the healthcare system smarter [59]. Sharing health records could happen between individuals. For instance, a patient who wants to share his medical history with a doctor at their first meeting [66]. In addition, sharing could happen between an individual and a stakeholder, such as a patient sharing his medical history with an insurance company or a research centre. Even the data could be shared beyond borders [67]. However, the operational mechanism of today's health-related systems has some limitations. One limitation is that patients hardly have access to their health records. Therefore, they have no idea about the sharing of their own health data among unknown parties [68]. To improve the interaction and collaboration with the healthcare industry, blockchain technology could play a crucial role, enabling and securing a convenient sharing mechanism of electronic health data. This is considered one of the most crucial contributions of blockchain based healthcare [69]. Below, we describe some of the contributions made in this regard.

Castaldo and Cinque [67] suggested a logging system to facilitate and improve the exchange of electronic health data across multiple countries in Europe in the most secure manner using private blockchain. Yue et al. [59] developed a healthcare data sharing application, namely Healthcare Data Gateway (HGD), based on the blockchain architecture. The provided solution helps control and share client's data easily without compromising privacy. It provides an excellent way to increase the intelligence of healthcare systems and at the same time keeps patient data private. Moreover, Vishal Patel [70] presented a framework for cross-domain image sharing by using blockchain technology as a distributed data store to create a ledger of radiological studies and control image sharing by customized user permission. In a similar study, Fan et al. [71] developed a MedBlock framework based on blockchain technology to solve data management and data sharing problem in an electronic medical records (EMRs) system and improve medical information sharing. Patients can access the EMRs of different hospitals through the MedBlock framework by avoiding the previous medical data being segmented into various databases. In addition, data sharing and collaboration via blockchain could help hospitals get a prior understanding of patients' medical history before the consultation. Ji et al. [72] proposed a multi-level location sharing scheme based on blockchain technology. The goal was to achieve the privacy-preserving location sharing by blockchain for telecare medical information systems. They define the primary requirements for location sharing decentralization, confidentiality, variability, multi-level privacy protection, irretrievability, and unforgeability by using Merkle tree and order-preserving encryption. The experimental results showed that the scheme is practical and

feasible for patients and medical staff, and can be applied to location information protection in telecare information systems [72]. Shen et al. [73] proposed MedChain, an efficient session-based healthcare data sharing based on blockchain. MedChain uses a digest chain structure approach to check the integrity of a shared medical IoT data stream. This is done to overcome the efficiency issues of existing systems such as Medrec [56] and MedBlock [71]. The evaluation results show that MedChain can achieve higher efficiency and satisfy the security requirements of healthcare data sharing [73].

3.2. Data Management

Even though many companies, especially healthcare institutions, are data driven, and the volume of data generated in this era or another era like the IoT is growing significantly [74], data security and privacy are continuously violated both unintentionally or by illicit users. As a result, many institutions have experienced an enormous loss of reputation and capital. Different users of health data have different roles, and access to data should be governed by privileges allocated to these roles. Such mode of access can be ensured, in a seamless way, by blockchain technology. Below, we describe some blockchain technologies that have been developed for such a purpose.

MedRec [56] is a decentralized EMR management system in which data permission and operation are recorded in the blockchain, and execution is completed by smart contracts. MedRec collaborates supplier's complete medical information for data authentication, confidentiality, auditing, and sharing, and gives patients a comprehensive, immutable medical data and service. In another study, Zhu et al. [75] proposed an approach for achieving a controllable blockchain data management in the cloud environment to address the concerns of users about the lack of control on the posted ledgers. In their model, they designed a special trust authority node to allow users to terminate and prevent any potentially malicious actions even in a majority attack. In another contribution made by Genestier et al. [76], a new idea of reshaping the consent management in the healthcare system which mainly provides user to control the whole health record data by using blockchain was introduced. However, there is no authorization design and no access control in their implementation.

3.3. Data Storage (Cloud-Based Applications)

Every transaction in a healthcare based blockchain is stored in blocks on decentralized storage system. In a healthcare system, patient medical data are organized in EHRs, which are considered the building blocks of a large distributed medical storage [77]. The latter could be stored on-premise, or on the cloud where security is the primary concern. Cloud storage is mainly the composition of numerous storage devices, connected all together to form a large volume of storage, to accommodate a lot of Information Technology infrastructure. A blockchain based healthcare system is one example of such IT infrastructure. Cloud storage technology has its advantages of fast transmission, good sharing, storage capacity, low cost, easy access, and dynamic association [78]. Al Omar et al. [79] proposed a patient-centric healthcare data management system in a cloud environment using blockchain technology as storage which helps to attain privacy. The main idea of this work is to keep sensitive healthcare data on the blockchain by defining a set of security and privacy requirements to achieve accountability, integrity, and security. Kaur et al. [80], however, introduced a new term BlockCloud, which is, in fact, the blend of blockchain implemented in a cloud environment. The idea behind implementing the cloud is to keep the data distributed and safe under the same roof without involving third parties. The study addressed challenges to how medical providers and organizations, public health agencies, healthcare service providers, and governments need to collaborate and create policy enforcement [80,81].

3.4. Electronic Health Record

Traditional medical records are paper-based, and it is tedious to keep track of chronological evolution of patient's health status [82]. In addition, they are prone to erroneous data, which results sometimes in patients getting maltreatment. Information technology provided the opportunity to alleviate such effort by introducing EHRs. Electronic access to health records enabled physician practices to significantly improve quality of treatment [83]. Furthermore, EHR enables better disease management and increased levels of preventive care. In addition, the digital record provides better decision-support functions and increased collaboration amongst caregivers. Therefore, there is increasing recognition of its role among the healthcare community [84]. Many research work was developed to design blockchain technology in order to secure, share, and store EHR data both within and across institutions. Chen et al. [85] developed a secure blockchain framework for medical data sharing by designing secure cloud storage for patients' sensitive medical record. In this framework, medical data management is achieved using a digital archive that has access control rights of its owners' information. This is stored by deploying cloud encryption under the chain. In a related study, Guo et al. [86] introduced an attribute-based signature scheme utilizing blockchain technology with multiple authorities to guarantee and validate EHRs. It facilitates group message broadcasts and could resist to collusion attacks. Wang and Song [78] proposed a secure cloud-based EHR system based on blockchain and attribute-based cryptosystem. To encrypt medical data, they used a blend of identity-based encryption and identity-based signatures at the same time to implement digital signs. On top of that blockchain, other techniques are used to ensure the integrity and traceability of medical facility. While the above-mentioned three studies have mainly focused on the cryptographic aspects to secure EHR blocks, Roehrs et al. [55] have addressed different challenges related to the unification of scattered health record, and the access management of healthcare provider's stakeholders. These two issues were solved by proposing OmniPHR, a distributed model for integrating personal health records (PHR) that uses a parallel database to store PHR in blocks and combined structural semantic interoperability and up-to-date vision of different PHR formats. Finally, in a completely different approach, Hussein et al. [87] developed a framework for securing medical record using blockchain technology based on genetic algorithms and discrete wavelet transforms. The proposed method utilizes a modified cryptographic hash generator for generating the necessary user security key. Additionally, MD5 (a message-digest algorithm using a hash function that produces a 128-bit hash value [88]) strings were used to produce a new key format by adopting a discrete wavelet transform. This approach enhances general system security and immunity to various attacks. Table 1 provides a summary of healthcare data management mechanisms in blockchain technology.

Table 1. Comparison of the data management mechanisms for healthcare in the blockchain.

Article	Blockchain Technology	Type of Data	Merits	Limitations
[67]	• The MultiChain platform do not rely on the Proof-of-work. • Private blockchain.	EHR	• Sharing of health data and securely improving audit logging.	• Except for the EU, no other cross border country is discussed.
[59]	• Private blockchain.	EHR and PHR	• Smart App based on blockchain to control and share healthcare data.	• No consideration for scalability and availability. • Data sharing is limited.
[70]	• Proof-of-stake. • Private blockchain.	Medical image records	• Securely sharing medical images.	• No consideration of data searching [73].
[71]	• Hybrid consensus mechanism based on practical byzantine fault tolerance. • Proof-of-stake.	EMR	• Securely sharing of healthcare data.	• Medblock failed to provide enough privacy for the patient's identity and energy efficiency [89].
[72]	• Proof-of-work.	Location	• Multi-layer location sharing schema.	• No discussion provided about under which critical condition a patient's location data will be retrieved.
[73]	Undefined.	EHR	• Securely sharing of healthcare data.	• High storage overhead and the breadcrumbs mechanism is looking up a single record.
[56]	• Ethereum platform. • Proof-of-work.	Medical records	• EHR management and sharing of healthcare data.	• No consideration of key replacement capability.
[75]	• Ethereum platform.	EHR	• Data management in the cloud environment. • High scalability.	• Practically not feasible.
[76]	• Hyperledger platform.	Medical records	• Managing personal data in the e-health.	• There is no access control and exhaustive authorization consideration [90,91].
[79]	• Ethereum platform.	Healthcare data	• Cost effective smart contracts.	• No consideration of interoperability between different parties.
[80]	• Undefined.	EMR	• Store and manage EMR in a cloud environment.	• The exact cost of the system is not known.
[85]	• Undefined	PHR	• Patients control their personal medical data.	• Interoperability is not tested across several healthcare parties.
[86]	• Undefined.	EHR	• Facilitate the privacy of patients and maintain the immutability of EHRs by attribute-based signature scheme.	• This system is not cost-effective for large number of users.
[78]	• Consortium blockchain.	Medical records	• Coupling encryption, and signature for robust security.	• The system is not fully automated.
[55]	• Undefined.	PHR and EHR	• High control access enhanced mobility.	• The input data to OmniPHR framework must be in the format of OmniPHR standard otherwise rejected [54].
[87]	• Undefined.	Medical records	• Securing and managing medical records by using a genetic algorithm.	• It is very difficult to verify the level of security offered by this system.

3.5. Blockchain Use Cases in Healthcare Data Management

Health Education: The primary use of the blockchain is as a mechanism for recording transaction of the Bitcoin digital currency, but this mechanism could be used in an education field too [92,93]. The base of education is the exchange of knowledge as well as skills from multiple sources. It assumes the trustworthiness of all the parties involved. With the proliferation of online learning, it becomes challenging for regulatory agencies to control the alteration of knowledge in medical education [94,95]. According to Funk et al. [94], the health professions educators' blockchain technology could potentially improve the quality of education and educational impact on multiple generations of learners. It can also help build a relative value of educational interventions. Additionally, any institution adopting blockchain technology would be able to provide certification on their own without any third party in between. Blockchain could also affect medical library management in many ways, including gathering, preserving, sharing authoritative information by creating timestamped, verifiable versions of journal articles [96]. By using blockchain in healthcare, we can ensure that the knowledge is secured and is not altered at all. For example, storing educational information in records with blockchain technology will easily allow health educators to track their impact as their students ultimately become educators themselves, and eventually pass along their knowledge to each subsequent class of students. It will also allow for easy tracking of the most utilized and most effective learning modules. Additionally, without any help from the third-party, certification could be provided to the right people. These ideas represent the potential benefit that blockchain technology could bring to health education.

Enrollment Data Management: Enrolling members into health care plans, healthcare delivery, criteria, credentialing records result in enrollment administrative data. Although the primary producer of this data is a government agency, the federal government and state governments, we can use data that generates from small, medium and even large healthcare providers [97]. The legacy of managing such a diverse dimension of data is manual, which requires an extensive process of checking references, credentials, and eligibility. Consequently, to some extent, the whole process is prolonged. This overwhelming task for administrative assistance slows down the entire enrollment process and constitutes a barrier for an efficient healthcare system. However, this information could be stored into a blockchain to check reliable references and relevant records with the shortest possible time. In pursuit of increased enrollment process efficiency, this could benefit an administrative assistant through procedural simplification, eligibility inquiries, network management, and coordination.

Security: The blockchain technology has reached a great boom in the health sector, due to its importance to overcome security challenges of the EHR in Healthcare [98]. EHRs have the potential to improve the delivery of healthcare [99]. It is created when a patient is admitted to a hospital, and when a physician diagnoses a patient, or when a diagnostic result such as an MRI scan is stored in the EHR system [100]. Therefore, security of such digital information is given utmost priority, and currently using blockchain for a safe and secure healthcare data [53]. Keeping the value of data, and reducing storage cost for data management in healthcare blockchain technology plays a significant role. Due to its unique capability, blockchain technology is the only answer for securing digital information, and it continues to play a crucial role in the future of enterprise data management.

4. Supply Chain Management

SCM is designed to include best practices of the industry to streamline the entire delivery processes from ordering to supply [101,102]. SCM is a challenging prospect in healthcare; with scattered ordering settings of medical supplies, drugs and critical resources, there is inherit risk of compromising the supply chain process that might directly impact patients' safety [103,104]. According to a study by the World Health Organization (WHO) [105], more than 100,000 people die in Africa due to improper dosing from counterfeited drugs ordered from not known or trusted vendors. In addition to product and drug counterfeiting, lacking product registry and packaging errors in a healthcare facility may disrupt the entire SCM [106]. Blockchain is particularly key monitoring technology for tapping into the whole process of drugs and medical products movement [107]. Since all transactions are recorded onto

the ledger, and every node in the blockchain maintains a record of the transaction, it is easy to verify the origin of the drug, the vendor and the distributor instantly. Furthermore, the distributed ledger of the blockchain allows healthcare officials and physician to check and authenticate the credentials of suppliers [108]. With better insight into the supply chain through proper and timely authentication process, pharmacies and healthcare providers will be able to ensure that the flow of authentic drugs continues to reach those patients who need it the most. In this regard, blockchain technology holds a great promise for establishing a trusted network of vendors that allow healthcare administrators to guard patients from disreputable suppliers. Furthermore, blockchain technology promises significant enhancement on demand forecasting, data provenance, fraud prevention, and transaction. Figure 4 illustrates a pharmaceutical SCM process using blockchain technology.

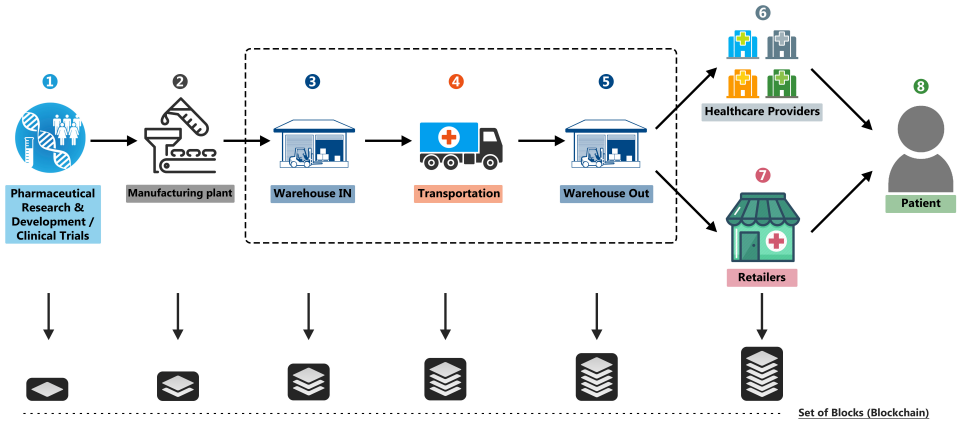

Figure 4. Supply chain management in blockchain.

- Step-1: A block is created upon the invention of a new medicine or medical care which includes patent protection and a long process of clinical trials. This information is recorded in the digital ledger as a form of transaction.
- Step-2: Once the clinical trial is successful, the patent is sent to the manufacturing plant for test prototype and mass production. Every product has its own unique identity that is integrated with another transaction or block in the blockchain including other relevant information.
- Step-3: Once the mass production along with packaging is finished, medicine is gathered in a warehouse for future distribution. Information such as, time, lot number, barcode, expiry date are included in the blockchain.
- Step-4: Transportation information is also included in the blockchain which may include time out from one warehouse (IN) to other, mode of transportation, authorized agent, and other information.
- Step-5: A third-party distribution network is normally responsible for distributing drugs and medical supplies to healthcare providers or retailers. A warehouse (OUT) for each third party is used for this purpose from where all distribution endpoints are linked. A separate transaction is also integrated into the blockchain.
- Step-6: Care providers such as hospitals, or clinics need to provide information, for example, batch number, lot number, product owner, expired date to authenticate, and prevent counterfeit. This is also included in the blockchain.
- Step-7: The actions taken by a retailer are similar to Step-6.
- Step-8: Patients are encouraged to determine authenticity throughout the whole process as blockchain supply chain offers transparent information for verification to potential buyers.

4.1. Clinical Trials

Clinical trials in healthcare face many challenges, including personal data privacy, data sharing, and patient enrolment [109,110]. Blockchain technology has the potential to address these challenges.

It provides models for sharing clinical trial data that enable transparency and reproducibility securely [110,111]. Nugent et al. [112] proposed smart contracts on a private Ethereum network to address trust degradation and to strengthen data transparency on the clinical trials. The aim of this study was to improve the scientific credibility of findings from clinical trials, which could be undermined by problems such as missing data and selective publication. To enhance the capability of clinical trials and precision medicine, four new system components have been developed on top of the traditional blockchain by Shae and Tsai [113]. These consists of blockchain based distributed and parallel computing prototype for big data analytics; data management component for data integration; identity management component for privacy protection of IoT devices; and data sharing management component for collaborative research ecosystem [113]. In another study, Choudhury et al. [114] proposed a novel data management framework based on permission blockchain technology using smart contract. The aim of this research was to reduce the administrative burden, time, and effort of ensuring data integrity and privacy in multi-site Clinical trials. Benchoufi et al. [111] developed a consent workflow on top of clinical trial methodology. Their proof-of-concept protocol of blockchain, which is based on time stamping consent collection, includes smart contract enrollment. The historical traceability provides an opportunity to ensure verifiability and transparency of such extreme sensitive data, even when a full document is stored in a public storage, such as dedicated public website.

4.2. Pharmaceutical

Pharmaceutical companies are relentlessly trying to improve the quality of medicine as well as invent new medicine for diverse diseases. Such medicine is required to go through a long process ensuring patent protection, safety, efficacy, statistical validity and approval from regulatory authorities. Normally, this process takes many years, starting from discovery to commercialization, where clinical trials occupy a major part of the duration [115]. Consequently, such a long process is vulnerable to drug recall and counterfeit due to the lack of security and privacy [116]. This obstacle could be eliminated by using blockchain technology throughout the whole pharmaceutical process. We could reserve the privacy and ensure security by using blockchains distributed ledger, by ensuring that every trial event is recorded in the blockchian nodes which is tamper-proof. A private blockchain could be used to ensure that all pharmaceutical adhere to the preservation of patent protection. This can be done by using a smart contract that provides integrity, traceability and transparency [117,118]. According to a recent study [119], around sixty percent of pharmaceutical companies are either working or experimenting with blockchain, which reflects the potentials of blockchain in such industry. Counterfeit drugs are a global problem and challenge with outstanding risks to the general public and consumers [120,121]. Sylim et al. [120] developed a pharmacosurveillance blockchain system in a simulated network to test the feasibility of applying the technology and its principles in a pharmaceutical surveillance system. The aim was to improve the traceability of falsified drugs. The system resists conventional drug supply chain counterfeiting which is a significant issue to some Asian countries. In many ways, Gcoin, Global Governance Coin, provides a dynamic role to each of the nodes, including coin issuer, full node, miners, or normal node in a hierarchical relationship, which is used in drug SCM [120]. Tseng et al. [122] suggested a Gcoin blockchain as the base of the data flow of drugs to create transparent drug transaction data. This is shared amongst manufacturers, wholesalers, retailers, pharmacies, hospitals, and consumers. The recording of drug transactions can turn the drug supply chain from regulating (government audits) to surveillance (by every participant collaboratively). Additionally, the regulation model of the drug supply chain could be changed from the examination and inspection to the surveillance net model [122]. Over a decade, radio frequency identification (RFID) technology has been considered as a robust ownership preserver, however, out of the RFID trusted domain, such as the post supply chain network being vulnerable to be forged by cloning this identification. By leveraging the Ethereum platform and its wallet, such vulnerabilities could be eliminated throughout the whole supply chain line, starting from manufacturer to end customers [123]. Table 2 presents a summary of SCM mechanisms in blockchain technology.

Table 2. Comparison of the supply chain management mechanisms for healthcare in the blockchain.

Article	Blockchain Technology	Type of Data	Merits	Limitations
[112]	• Ethereum platform.	Clinical trial records	• Smart contract based on improving the transparency of clinical trials.	• Scalability can be a serious concern.
[113]	• Undefined.	Medical Records	• Better support precision medicine.	• Lack of coherence [89].
[114]	• Undefined.	Clinical trial records	• Monitoring and managing records in clinical trials.	• Cost of implementation is high.
[111]	• Proof-of-concept.	Clinical trial records	• Improve the transparency and processing of data enhancement and traceability of the consent protocol.	• The relation between the digital and the physical identities of patients is vague.
[120]	• Ethereum and Hyperledger Fabric platform. • Delegated proof-of-stake and practical byzantine fault tolerance. • Public blockchain.	Transaction records	• Enhancing the traceability of falsified drugs.	• The system is developed using simulated network. • There is no assurance of not tracking falsified drugs outside of official distribution chains.
[122]	• Gcoin platform (Consortium). • Proof-of-work. • Private blockchain.	Transaction records	• Creating transparent drug transaction data and shifting from regulating (government audits) to surveillance net.	• Operational cost is not discussed.
[123]	• Ethereum platform. • Proof-of-concept.	Transaction records	• Supply chain system for anti-counterfeits by using RFID technologies.	• Exposed to tracking attacks that monitor the movement of the RFID because electronic product codes are sent as a fixed value during the whole process and it would be possible for counterfeiters to copy the genuine product's tag [124,125].

4.3. Blockchain Use Cases in Supply Chain Management

Claims and Billing Management: Healthcare service has its own cost which already makes the whole industry worth a trillion dollars, and it is increasing rapidly [126]. The process of medical billing is an integral part of the healthcare sector. This is because, without billing, a proper service delivery cannot be ensured. This process starts from the time the patient is admitted to the hospital to the time it is checked-out. It involves several steps, such as check-in, confirming financial responsibility, coding and billing compliance, transmitting the claim, and receiving payment from insurance companies [127]. The entire billing scheme can be challenging as some of the fees are entirely covered by the patient's individual health insurance plan, or paid by the patient. One of the main issues in medical billing is excessive billing due to the lack of transparency and trust among doctors, patients, and insurance companies. Claims and billing in the healthcare sector are being continuously abused, but can be resolved or diminished by using a transparent system for every stakeholder. Blockchain can ensure such transparent system keeping everyone engaged in the whole process and removing mistrust among them [126].

Quality management: A drug is considered as counterfeit, if it contains improper ingredients, and traded with the intent to hide or imitate its provenance, authenticity or even effectiveness [128,129]. Furthermore, products and drug counterfeit greatly influence SCM [130]. Their performance in the pharmaceutical industry are competitive factors that disrupt the efficiency, authenticity and robust profitability in a particular healthcare industry enormously [131]. Customers are often unaware of the exact sources of the products they purchase and consume in a global marketplace [132]. Since this type of drug is malicious for a patient, it is a life-threatening issue around the world [133]. This also causes a threat to the reputation of the original pharmaceutical companies, making drug manufacturers and distributors invest a huge amount of money in countermeasures [128]. The study in [133] found that techniques such as spectroscopic and chromatographic are effective for detecting counterfeit because of their detection of active ingredients and image sample composition. However, they have their limitations as it relies on electromechanical apparatus, which increased the overhead cost. One way to solve these challenges is to have pharmaceutical manufacturers' information, including product serial numbers and package number on the blockchain, whereby pharmaceutical companies, drug manufacturers and customers could verify the authenticity of the data by connecting to the blockchain. This process ensures low-cost quality control, product registration, drug tracking, and drug counterfeit through the entire SCM process [131].

5. Internet of Medical Things

IoMT systems play a vital role in the development of health and medical information systems [134]. With IoMT technology, healthcare equipment such as heart monitor, body scanners, and wearable devices can gather, process and share data over the Internet in real time. For example, with the advancement of AI, healthcare providers, using the IoMT paradigm, can capture an image, identify malignant parts or even suspicious cells, and share such knowledge with those who have the right to access the information. The following sections elaborate mostly on the progress in healthcare IoT and smart medical devices in the AI arena. Figure 5 is an illustration of IoMT in blockchain.

- Step-1: In the realm of IoMT, the patient is the source of all data.
- Step-2: Medical IoT devices are normally either attached closely or remotely monitoring patients' body, consequently, generating large volume of data.
- Step-3: Data generated in step-2 are stored on blocks or on the cloud storage. AI will help blockchain to create intelligent virtual agents, which in turn can create new ledgers automatically. In case of sensitive medical data, where security is the first priority, decentralized AI system could help block chain to reach highest security [135].
- Step-4: Healthcare providers are the end users who seek access for a safe and sound care delivery which is authorized by the owner.

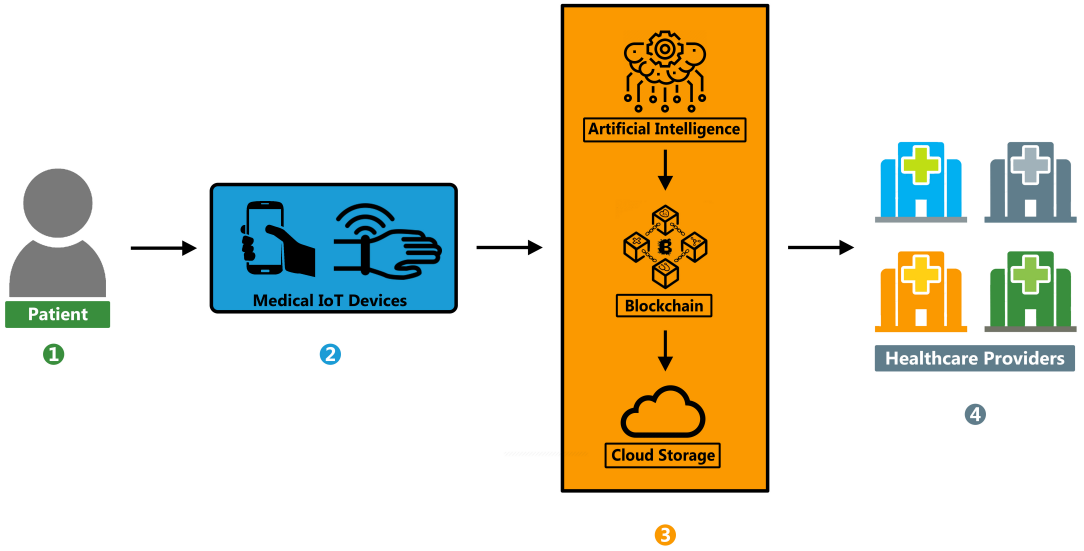

Figure 5. Internet of medical things (IoMT) in blockchain.

5.1. Healthcare IoT and Medical Devices

IoT is an association of computing devices having unique identifiers, capable of transferring data over a network using Internet protocol without any man-machine interactions. Such a powerful seamless interaction makes IoT play a crucial role in the healthcare system [136]. Wearable and medical devices are currently at the heart of IoMT [137]. One major constituent of IoMT in the healthcare industry is wireless body-area network (WBAN) systems. WBAN are becoming a significant enabling technology for a wide variety of applications, especially in medical and healthcare environments for remote monitoring of physiological parameters [138–141]. For instance, people can use IoT devices to remind them about appointments, changes in blood pressure, calories burnt and much more [142,143]. In the following discussion, we provide a review of current work on the integration of blockchain with IoMT.

Griggs et al. [144] introduced the integration of WBANs with blockchain smart contracts for a secured real-time patient monitoring and medical interventions system. The study proposes the integration of bockchain to execute smart contracts that would evaluate information collected by a patient's IoT healthcare devices based on customized threshold values. This is done to overcome the problem of logging transfer of data transactions in an IoT healthcare system. Rahman et al. [145] introduced an intelligent dyslexia analytics solution where a decentralized big data repository is used to store, and then share with healthcare communities, groups, and individuals using blockchain. Mobile Multimedia Health data is captured during dyslexia testing and stored in a decentralized big data repository, which can be shared for further clinical research and statistical analysis. Jo et al. [146] introduced structural health monitoring by using both IoT and blockchain technology. They proposed a novel system where locally centralized and globally decentralized distribution is activated by dividing them into edge and core network. Therefore, it enhances the efficiency and scalability of the blockchain system. Zhang et al. [57] introduced a model for using a securely PSN based healthcare. The primary challenge of this model is to ensure security while sharing data among PSN nodes. To address this problem, the authors developed two protocols. The first protocol designed is an improved version of IEEE802.15.6, which establishes secure links with unbalanced computational requirements for mobile devices and resources-limited sensor nodes. However, the second protocol used blockchain technique to share health data among PSN nodes. Ichikawa et al. [147] developed a framework tamper-resistant mobile Health system using blockchain technology, in order to ensure fidelity of records. The aim of this study was to develop a mobile health system for cognitive behavioral therapy for insomnia using a smartphone application.

5.2. Healthcare IoT Infrastructure and Data Security

Healthcare Information and Communication Technology (ICT) infrastructure consists of many networks and IoT devices, including terminals, sensor, diagnostic tools, wireless access points, etc. This infrastructure enables many healthcare systems such as wearable devices and remote monitoring services to transmit and share data about the patient's critical conditions with caregivers. During the transmission process, data traverse through unknown communication networks (e.g., Wide Area Networks) which might be vulnerable to security and privacy breaches. Indeed, there are many cases (e.g., Three Phishing attacks costs 20,000 patient's personal data breach at Catwaba Valley Medical Center in North Carolina [148]) where malicious attackers are relentlessly trying to discover any acute weakness to penetrate the healthcare network and compromise the service provider's valuable information. To address the above-mentioned security challenges in healthcare IoT, researchers are exploring various techniques to protect users' data from unlawful penetration. For example, Nikoloudakis et al. in [149] proposed a software defined network which virtualizes the traditional network infrastructure into several abstraction levels to build a resistance mechanism against malicious attack. The authors also suggested a fog computing architecture that assesses vulnerabilities of existing and newly added hardware into the healthcare IoT using OpenVAS framework. The main shortcoming of the proposed model is that the average assessment period of a single device is around 7 min and 21 s, which is too long and raises serious concern regarding the scalability of the system. This issue could be addressed by using blockchain-based Ethereum platform since block mining time is 10–15 s. Other research by Nausheen and Begum in [150] proposed a different solution based on application hardening such as code obfuscation and application program interface(APIs) to protect key logic and mobile applications, respectively. The study suggests the addition of a defense layer against reverse engineering by return oriented programming and check summing techniques. Although the security protection of implanted medical devices gadgets is well assisted in this study, heterogeneous technologies are required to integrate for a cumulative efficiency, but at the expense of increased complexity to the whole system. In order to enhance the Intrusion Detection Systems (IDSs) in IoT networks, the authors in [151] introduced Adaptively Supervised and Clustered Hybrid (ASCH-IDS) technique which classifies potential intruders from aggregated sensory data. A dissimilar proportion of aggregated sensory traffic is fed into two detection subsystems: Anomaly detection (ADSs) and Misuse detection (MDSs) for better performance. Interestingly, when the proportion adjustment increases the system performs well, and it shows the highest accuracy in terms of Sensitivity and Specificity when sensory data proportion on misuse detection is 0:25%. This process indicates an increased detected rate. Furthermore, the same authors in [152] employ Restricted Boltzmann Machine-based Clustered IDS (RBC-IDS), a deep learning-based methodology to monitor critical infrastructure for potential intruders using three hidden layers which shows increased accuracy of 99.91% compared to 99.80% in the previous study. However, the overhead cost of this new experiment is double the previously proposed model. As the self-driving autonomous vehicle is shaping the current transportation system gradually, its use in healthcare is indispensable, especially, in the healthcare SCM. Aloqaily et al. [153] introduced an intrusion detection mechanism to resist attack such as Denial of Service, Probe, Remote to user, etc. The authors proposed deep belief network for data dimension reduction, and decision tree using ID3 algorithm for intrusion classification. The detection accuracy of the systems is 99.92% which is quite high; however, the false negative rate is 1.53%. The result means approximately three intrusion attacks could penetrate the system for every 200 user sessions. In an effort to reduce the security vulnerability of RFID in healthcare IoT infrastructure, Catarinucciet et al. [154] proposed a smart hospital system that consist of hybrid-sensing network exploiting constrained application protocol, IoT smart gateway, and a user interface to provide third-parties the ability to empower patients with health monitoring system. However, the collected data from the IoT devices is stored in a central database which is prone to be forged. This could be addressed by using decentralized ledger such as blockchain since data blocks are replicated to distributed network nodes for enhanced transparency. Parallel to the above work, Robereto Saia [155,156] proposed a novel approach for the

internet of entities which integrates Mobile and IoT networks into two main components: entities such as the user devices and a tracker that facilitates the transmission of information to the blockchain. The proposed architecture is a blend of Wireless and blockchain networks which can be used for healthcare services, but a proper implementation of such a large and complex network may unlock potential limitations; for example, computational overhead optimization of blockchain might be difficult [155,156]. Esposito et al. [157] explored healthcare data security and privacy by introducing different forms of data structure in the blockchain. However, due to the overhead complexity of storing large volume of health data in the blockchain, the study uses only the hash of data as transaction. However, this alone cannot ensure data security. Reducing the overhead of Blockchain implementation in healthcare small area networks is a challenging prospect since adding blocks in the chain following mainstream cryptographic mining algorithms such as PoW requires enormous computational power. To address such challenge, Dorri et al. in [158,159] proposed a novel lightweight architecture for networks comprising numerous IoT devices. A local computer is used as a Miner and a number of IoT devices are clustered together such that one is selected as a cluster head to reduce access verification using policy header. This scheme allows for the policy header to contain updated Access control list that is administered by network operator. In addition, this study used a shared overlay network where many data owners are permitted to insert data into the blocks which is controlled by single admin. However, this may lead to lack of trustworthiness among users. In the review paper of Khan and Salah [160], several security and privacy vulnerabilities in the current IoT ecosystem were identified for further research including protection during updating software of billions of IoT devices (healthcare, for instance) where blockchain could be used to enhance security. Protecting healthcare critical IoT infrastructure and sensitive data may eliminate potential security and privacy issues, for example, in mid-2016 3.62 million patients' data including personal information, social security number, and credit card numbers were compromised in Banner Health, Arizona [161]. According to the above discussion, we can infer that although conventional security systems is providing enhanced security, complete tamper proof systems cannot be ensured. Blockchain is considered by many as a potential solution among other state-of-the-art technologies to be implemented in a small and medium scale healthcare IoT systems.

5.3. Artificial Intelligence

Blockchain technologies get increasingly powerful and robust, as they become coupled with AI in various real-word healthcare solutions [162]. Machine learning and deep learning are the main driving ingredients for AI domain, which is also relentlessly improving the advancement of automation. The more data we feed to the machine, the more the ability a machine will gain to classify or predict patterns accurately [163]. Kuo and Ohno-Machado [164] introduced ModelChain framework based on blockchain technology. This framework utilizes a private blockchain to enable multiple institutions to contribute health data to train a machine-learning model improve care without disclosing their health records [164]. Such a framework increases the security and robustness of the distributed privacy-preserving health care predictive modeling across multiple institutions. Wang et al. [165] proposed a blockchain based parallel healthcare system (PHS), including artificial systems, computational experiments and parallel execution (ACP). The ACP focused mainly on representing a patient's diagnosis, condition, and treatment process [165]. A consortium blockchain is added with the PHS to link hospitals, patients, health governing body and related communities [165]. The summary of benefits and limitations of the IoMT in blockchain technology is shown in Table 3.

Table 3. Comparison of the internet of medical things mechanisms for healthcare in the blockchain.

Article	Blockchain Technology	Type of Data	Merits	Limitations
[144]	• Ethereum platform. • Proof-of-concept. • Public blockchain.	Sensor data	• Integration of WBAN using smart contracts for securely automated patient monitoring.	• Inefficient data ingestion.
[145]	• Ethereum and Hyperledger platform. • Private blockchain.	Multimedia IoT data	• Dyslexia diagnosis data can be shared securely with mobile medical practitioners.	• High upload time.
[146]	• Ethereum platform. Proof-of-work. • Private blockchain.	Sensor data	• Ensuring transparency, data security, and data storage by using a PoW consensus mechanism.	• Security risks for real-time monitoring because of faster block-time.
[147]	• Hyperledger Fabric platform.	EHR and sensor data	• Robust against network fault such as distributed node down.	• Vulnerable to attack.
[155]	• Public blockchain.	Sensor data	• Ensuring anonymity and immutability. • Log activity of entity and object.	• Computational overhead is high.
[156]	• Public blockchain.	Sensor data	• Robust localization security of sensor devices in a wireless network.	• Implementation of blockchain in such a large and complex network will eventually be vulnerable to malicious attack.
[157]	• Undefined.	EMR, EHR, and PHR	• Storage and mining overhead are reduced.	• Vulnerable to security and privacy.
[159]	• Public blockchain.	Sensor data	• Reduced validation time by using Cluster Head.	• Lack of transparency and trustworthiness.
[164]	• Proof-of-information. • Private blockchain.	Medical records	• Enhanced privacy in medical health prediction model.	• Vulnerable to attack [166].
[165]	• Proof of stake. • Private blockchain.	Medical records	• Artificial healthcare systems.	• Limited treatment scenarios are included.

5.4. Blockchain Use Cases in the Internet of Medical Things

Lack of Standardization: The acceleration of the healthcare industry towards adopting state-of-the-art IoMT technology is enormous. In addition to healthcare providers on premise medical devices, IoMT unlocks the facility of medical services to be accessed ubiquitously to guide patients invariably. This is also the building blocks of telehealth surveillance applications as wireless devices are associated with capturing bio-signals. Therefore, tamperproof transmission of medical data is very substantial [167]. This problem results from the high heterogeneity in communication protocols, medical devices and platforms, which could be termed as lack of standardization among IoMT manufacturers. Therefore, protecting such variable standardized transmission medium is difficult in the current perspective [168]. State-of-the-art technology, such as blockchain, could be applied to resist unauthorized access during data transmission over an unknown network as a diverse communication standard of a system does not affect blockchain's performance. Furthermore, tampering even a blockchain data block requires enormous computation power and consensus (51%) among its mining nodes before broadcasting to the whole network to add in the chain.

6. Conclusions

The blockchain technology is gaining significant attention from individuals, as well as organizations of nearly all kinds and dimensions. It is capable of transforming the traditional industry with its features, which include decentralization, anonymity, persistency, and auditability [32,169,170]. The blockchain technology is expected to reshape the healthcare ecosystem. Not only the process will be transparent and secure, but also the quality of healthcare will be increased at a lower cost. In this paper, we discussed various blockchain applications in the healthcare industry and identified the major research initiatives as well as future research opportunities. Specifically, we presented current research on health data management and how blockchain will empower patients and stream line the sharing process of health data. We found that there is a consensus among researchers that, with blockchain technology, patient data will be truly owned and controlled by the rightful owner of the data, i.e., the patient. The blockchain allows for health records to be time-stamped so that no one can tamper with them after becoming part of the distributor ledger. The patients will have the right to decide who can and cannot access their data and for what purpose. However, there are still several open challenges that require further investigation. For example, cross-border sharing of health data where different and often conflicting jurisdictions exist may hinder the benefit of blockchain's data sharing. Indeed, the expectation of individual's privacy varies from one country to another based on the government regulations. Therefore, future research on regulation, standardization, and cross-border health data retrieving policies including retention and usage intention are duly urgent. Another potential problem that is under-researched is the capability of the blockchain to store and process massive data access transactions in a timely manner. As the volume of transactions increases, the delay of mining blocks in private or public blockchain's will increase exponentially. Therefore, there is a need for innovative mechanisms and algorithms to minimize the mining delays. Furthermore, we discussed current research of blockchain on healthcare SCM. In particular, the applicability of blockchain to address trust degradation and to strengthen data transparency on the clinical trials. Several researchers propose the use of blockchain to improve the scientific credibility of findings from clinical trials, which could be undermined by problems such as missing data and selective publication. We also discussed the issue of tracking drugs; it is clear that blockchain technology will be an indispensable tool for pharmacist and healthcare providers to properly and timely authenticate the flow of legitimate drugs and their delivery to the patients. However, further research on robust tracking mechanisms that monitor the registration of the products is needed. Current tracking systems that rely on RFIDs and Barcodes are not immune from tampering since these codes are sent as fixed values in the supply chain process which can be modified/copied by counterfeiters. Other cases such as billing and payment management were presented in this paper as future research issues. Claims and billing in the healthcare sector are being continuously abused, but can be resolved or diminished by using a transparent system such as

blockchain. Finally, we presented the application of blockchain in IoMT. Healthcare systems of the 21st century will consist of various devices connecting patients (e.g., remote healthcare services, wearable devices, etc.) with their caregivers. These systems generate data continuously and can be subject to malicious attacks while in transmission at various levels of the underlying communication network. In this paper, we discussed several research studies that propose tamper-resistant systems using blockchain technology to ensure the fidelity of health data. The main problem that we believe it needs attention from researchers is how the blockchain will operate in complex and diverse communication systems. The IoMT delivery system will be using communication networks owned by different service providers with different data access control policies. For the blockchain technology to work in such an environment, we need research that investigates blockchain mechanisms that promote single global access policy for the whole network. Furthermore, since the network consists of nodes and computers that are spatially separated, there is a need for synchronization mechanisms to identify the order of block additions. We also suggest further research on innovative solutions that promote blockchain as a service that allows various parties (networks, devices, users, etc.) of the IoMT paradigm to access basic coherent blockchain infrastructures.

Author Contributions: Conceptualization, S.K., M.M., A.Y. and R.B.; writing of the original draft preparation, S.K.; supervision, A.Y. and R.B.; writing of review and editing, S.K., M.M., A.Y. and R.B.

Funding: This research received no external funding.

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

Abbreviations

The following abbreviations are used in this manuscript:

EHR	Electronic health record
PHR	Personal health record
R&D	Research and development
PoW	Proof-of-work
SCM	Supply chain management
P2P	Peer to peer
QoE	Quality of experience
IoMT	Internet of medical things
EMR	Electronic medical record
WBAN	Wireless body-area network
HGD	Healthcare data dateway
RFID	Radio frequency identification
IoT	Internet of things
AI	Artificial intelligence
PHS	Parallel healthcare system
PSN	Pervasive social network
IDS	Intrusion detection system
API	Application program interface
ICT	Information and communication technology

References

1. Michael, J.; Cohn, A.; Butcher, J.R. BlockChain Technology. 2018. Available online: https://www.steptoe.com/images/content/1/7/v3/171269/LIT-FebMar18-Feature-Blockchain.pdf (accessed on 20 March 2019).
2. Lee, J.H.; Pilkington, M. How the Blockchain Revolution Will Reshape the Consumer Electronics Industry [Future Directions]. *IEEE Consum. Electron. Mag.* **2017**, *6*, 19–23. [CrossRef]
3. Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where is current research on blockchain technology?—A systematic review. *PLoS ONE* **2016**, *11*, e0163477. [CrossRef] [PubMed]

4. Yaeger, K.; Martini, M.; Rasouli, J.; Costa, A. Emerging Blockchain Technology Solutions for Modern Healthcare Infrastructure. *J. Sci. Innov. Med.* **2019**, *2*. [CrossRef]
5. Gaggioli, A. Blockchain Technology: Living in a Decentralized Everything. *Cyberpsychol. Behav. Soc. Netw.* **2018**, *21*, 65–66. [CrossRef]
6. Macrinici, D.; Cartofeanu, C.; Gao, S. Smart contract applications within blockchain technology: A systematic mapping study. *Telemat. Inform.* **2018**, *35*, 2337–2354. [CrossRef]
7. Smart Contracts. Available online: https://blockchainhub.net/smart-contracts/ (accessed on 12 March 2019).
8. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **2019**, *100*, 143–174. [CrossRef]
9. Treleaven, P.; Brown, R.G.; Yang, D. Blockchain Technology in Finance. *Computer* **2017**, *50*, 14–17. [CrossRef]
10. Fanning, K.; Centers, D.P. Blockchain and its coming impact on financial services. *J. Corporate Account. Financ.* **2016**, *27*, 53–57. [CrossRef]
11. Pilkington, M. 11 Blockchain technology: Principles and applications. In *Research Handbook on Digital Transformations*; Edward Elgar: Cheltenham, UK, 2016; p. 225.
12. Ayed, A.B. A conceptual secure blockchain-based electronic voting system. *Int. J. Netw. Secur. Its Appl.* **2017**, *9*, 1–9.
13. Foroglou, G.; Tsilidou, A.L. Further applications of the blockchain. In Proceedings of the 12th Student Conference on Managerial Science and Technology, Athens, Greece, 14 May 2015.
14. Yang, R.; Yu, F.R.; Si, P.; Yang, Z.; Zhang, Y. Integrated blockchain and edge computing systems: A survey, some research issues and challenges. *IEEE Commun. Surv. Tutor.* **2019**. [CrossRef]
15. Lin, I.C.; Liao, T.C. A Survey of Blockchain Security Issues and Challenges. *IJ Netw. Secur.* **2017**, *19*, 653–659.
16. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*; BN Publishing: La Vergne, TN, USA, 2008.
17. Rawal, V.; Mascarenhas, P.; Shah, M.; Kondaka, S.S. *White Paper: Blockchain for Healthcare an Opportunity to Address Many Complex Challenges in Healthcare*; CitiusTech: Princeton, NJ, USA, 2017.
18. Engelhardt, M.A. Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. *Technol. Innov. Manag. Rev.* **2017**, *7*, 22–34. [CrossRef]
19. Mead, C.N. Data interchange standards in healthcare it-computable semantic interoperability: Now possible but still difficult. do we really need a better mousetrap? *J. Healthc. Inf. Manag.* **2006**, *20*, 71.
20. Iroju, O.; Soriyan, A.; Gambo, I.; Olaleke, J. Interoperability in healthcare: Benefits, challenges and resolutions. *Int. J. Innov. Appl. Stud.* **2013**, *3*, 262–270.
21. Al Ridhawi, I.; Aloqaily, M.; Kotb, Y.; Al Ridhawi, Y.; Jararweh, Y. A collaborative mobile edge computing and user solution for service composition in 5G systems. *Trans. Emerg. Telecommun. Technol.* **2018**, *29*, e3446. [CrossRef]
22. Al Ridhawi, I.; Aloqaily, M.; Kantarci, B.; Jararweh, Y.; Mouftah, H.T. A continuous diversified vehicular cloud service availability framework for smart cities. *Comput. Netw.* **2018**, *145*, 207–218. [CrossRef]
23. Cardoso, L.; Marins, F.; Portela, F.; Santos, M.; Abelha, A.; Machado, J. The next generation of interoperability agents in healthcare. *Int. J. Environ. Res. Public Health* **2014**, *11*, 5349–5371. [CrossRef]
24. Gordon, W.J.; Catalini, C. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 224–230. [CrossRef]
25. Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G. Applying software patterns to address interoperability in blockchain-based healthcare apps. *arXiv* **2017**, arXiv:1706.03700.
26. 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]
27. 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.
28. 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]
29. Sharma, R. *Blockchain in Healthcare*; FCCCO: Ontario, ON, Canada, 2018.

30. 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] [PubMed]
31. Peter, H.; Moser, A. Blockchain-applications in banking & payment transactions: Results of a survey. In Proceedings of the 14th International Scientific Conference Pt, European Financial Systems, Brno, Czech Republic, 26–27 June 2017; Volume 2, pp. 141–149.
32. Zheng, Z.; Xie, S.; Dai, H.N.; Wang, H. *Blockchain Challenges and Opportunities: A Survey*; Work Paper; Inderscience Publishers: Geneva, Switzerland, 2016.
33. Beck, R.; Avital, M.; Rossi, M.; Thatcher, J.B. Blockchain technology in business and information systems research. *Bus. Inf. Syst. Eng.* **2017**, *59*, 381–384. [CrossRef]
34. Cai, C.W. Disruption of financial intermediation by FinTech: A review on crowdfunding and blockchain. *Account. Financ.* **2018**, *58*, 965–992. [CrossRef]
35. Conoscenti, M.; Vetro, A.; De Martin, J.C. Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6.
36. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.
37. Banerjee, M.; Lee, J.; Choo, K.K.R. A blockchain future for internet of things security: A position paper. *Dig. Commun. Netw.* **2018**, *4*, 149–160. [CrossRef]
38. Fernández-Caramés, T.M.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* **2018**, *6*, 32979–33001. [CrossRef]
39. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet Things J.* **2018**. [CrossRef]
40. Zhang, C.; Wu, J.; Long, C.; Cheng, M. Review of existing peer-to-peer energy trading projects. *Energy Procedia* **2017**, *105*, 2563–2568. [CrossRef]
41. Chitchyan, R.; Murkin, J. Review of blockchain technology and its expectations: Case of the energy sector. *arXiv* **2018**, arXiv:1803.03567.
42. Ølnes, S.; Ubacht, J.; Janssen, M. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Gov. Inf. Q.* **2017**, *34*, 355–364.
43. Hou, H. The application of blockchain technology in E-government in China. In Proceedings of the IEEE 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, 31 July–3 August 2017; pp. 1–4.
44. Alketbi, A.; Nasir, Q.; Talib, M.A. Blockchain for government services—Use cases, security benefits and challenges. In Proceedings of the IEEE 2018 15th Learning and Technology Conference (L&T), Jeddah, Saudi Arabia, 25–26 February 2018; pp. 112–119.
45. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gen. Comput. Syst.* **2017**, in press. [CrossRef]
46. Conti, M.; Kumar, E.S.; Lal, C.; Ruj, S. A survey on security and privacy issues of bitcoin. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3416–3452. [CrossRef]
47. Joshi, A.P.; Han, M.; Wang, Y. A survey on security and privacy issues of blockchain technology. *Math. Found. Comput.* **2018**, *1*, 121–147. [CrossRef]
48. Mettler, M. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–16 September 2016; pp. 1–3.
49. Kuo, T.T.; Kim, H.E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inform. Assoc.* **2017**, *24*, 1211–1220. [CrossRef] [PubMed]
50. Stagnaro, C. White Paper: Innovative Blockchain Uses in Health Care. Available online: https://www.freedassociates.com/ (accessed on 24 April 2019).
51. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]
52. Radanović, I.; Likić, R. Opportunities for Use of Blockchain Technology in Medicine. *Appl. Health Econ. Health Policy* **2018**, *16*, 583–590. [CrossRef]

53. Siyal, A.; Junejo, A.; 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]
54. 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]
55. Roehrs, A.; da Costa, C.A.; da Rosa Righi, R. OmniPHR: A distributed architecture model to integrate personal health records. *J. Biomed. Inform.* **2017**, *71*, 70–81. [CrossRef]
56. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.
57. Zhang, J.; Xue, N.; Huang, X. A secure system for pervasive social network-based healthcare. *IEEE Access* **2016**, *4*, 9239–9250. [CrossRef]
58. 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]
59. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef] [PubMed]
60. Saraf, C.; Sabadra, S. Blockchain platforms: A compendium. In Proceedings of the 2018 IEEE International Conference on Innovative Research and Development (ICIRD), Bangkok, Thailand, 11–12 May 2018; pp. 1–6.
61. Ethereum. Available online: https://www.ethereum.org/ (accessed on 20 March 2019).
62. Ripple. Available online: https://ripple.com/ (accessed on 20 March 2019).
63. Hyperledger. Available online: https://www.hyperledger.org/ (accessed on 20 March 2019).
64. Dimitrov, D.V. Blockchain Applications for Healthcare Data Management. *Healthc. Inform. Res.* **2019**, *25*, 51–56. [CrossRef] [PubMed]
65. Panesar, A. *Machine Learning and AI for Healthcare: Big Data for Improved Health Outcomes*; Springer: Emeryville, CA, USA, 2019.
66. Frost, J.H.; Massagli, M.P. Social uses of personal health information within PatientsLikeMe, an online patient community: What can happen when patients have access to one another's data. *J. Med. Internet Res.* **2008**, *10*, e15. [CrossRef] [PubMed]
67. Castaldo, L.; Cinque, V. Blockchain-based logging for the cross-border exchange of ehealth data in europe. In *International ISCIS Security Workshop*; Springer: Cham, Switzerland, 2018; pp. 46–56.
68. Hien, D.T.T.; Hien, D.H.; Pham, V.H. A survey on opportunities and challenges of Blockchain technology adoption for revolutionary innovation. In Proceedings of the ACM Ninth International Symposium on Information and Communication Technology, Danang City, Vietnam, 6–7 December 2018; pp. 200–207.
69. Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5.
70. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* **2018**. [CrossRef]
71. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. Medblock: Efficient and secure medical data sharing via blockchain. *J. Med. Syst.* **2018**, *42*, 136. [CrossRef]
72. Ji, Y.; Zhang, J.; Ma, J.; Yang, C.; Yao, X. BMPLS: Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems. *J. Med. Syst.* **2018**, *42*, 147. [CrossRef]
73. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient Healthcare Data Sharing via Blockchain. *Appl. Sci.* **2019**, *9*, 1207. [CrossRef]
74. Vo, H.T.; Kundu, A.; Mohania, M.K. *Research Directions in Blockchain Data Management and Analytics*; EDBT: Lisbon, Portugal, 2018; pp. 445–448.
75. Zhu, L.; Wu, Y.; Gai, K.; Choo, K.K.R. Controllable and trustworthy blockchain-based cloud data management. *Future Gen. Comput. Syst.* **2019**, *91*, 527–535. [CrossRef]
76. Genestier, P.; Zouarhi, S.; Limeux, P.; Excoffier, D.; Prola, A.; Sandon, S.; Temerson, J.M. Blockchain for consent management in the ehealth environment: A nugget for privacy and security challenges. *J. Int. Soc. Telemed. eHealth* **2017**, *5*, GKR-e24.
77. Zhang, R.; Liu, L. Security models and requirements for healthcare application clouds. In Proceedings of the 2010 IEEE 3rd International Conference on cloud Computing, Miami, FL, USA, 5–10 July 2010; pp. 268–275.

78. Wang, H.; Song, Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. *J. Med. Syst.* **2018**, *42*, 152. [CrossRef]
79. Al Omar, A.; Bhuiyan, M.Z.A.; Basu, A.; Kiyomoto, S.; Rahman, M.S. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Gen. Comput. Syst.* **2019**, *95*, 511–521. [CrossRef]
80. Kaur, H.; Alam, M.A.; Jameel, R.; Mourya, A.K.; Chang, V. A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. *J. Med. Syst.* **2018**, *42*, 156. [CrossRef]
81. Li, X.; Huang, X.; Li, C.; Yu, R.; Shu, L. EdgeCare: Leveraging Edge Computing for Collaborative Data Management in Mobile Healthcare Systems. *IEEE Access* **2019**, *7*, 22011–22025. [CrossRef]
82. Wang, S.J.; Middleton, B.; Prosser, L.A.; Bardon, C.G.; Spurr, C.D.; Carchidi, P.J.; Kittler, A.F.; Goldszer, R.C.; Fairchild, D.G.; Sussman, A.J. A cost-benefit analysis of electronic medical records in primary care. *Am. J. Med.* **2003**, *114*, 397–403. [CrossRef]
83. Miller, R.H.; Sim, I. Physicians' use of electronic medical records: barriers and solutions. *Health Affairs* **2004**, *23*, 116–126. [CrossRef]
84. Terry, A.L.; Thorpe, C.F.; Giles, G.; Brown, J.B.; Harris, S.B.; Reid, G.J.; Thind, A.; Stewart, M. Implementing electronic health records: Key factors in primary care. *Can. Fam. Phys.* **2008**, *54*, 730–736.
85. Chen, Y.; Ding, S.; Xu, Z.; Zheng, H.; Yang, S. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. *J. Med. Syst.* **2018**, *43*, 5. [CrossRef]
86. Guo, R.; Shi, H.; Zhao, Q.; Zheng, D. Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems. *IEEE Access* **2018**, *776*, 1–12. [CrossRef]
87. Hussein, A.F.; ArunKumar, N.; Ramirez-Gonzalez, G.; Abdulhay, E.; Tavares, J.M.R.; de Albuquerque, V.H.C. A Medical Records Managing and Securing Blockchain Based System Supported by a Genetic Algorithm and Discrete Wavelet Transform. *Cognit. Syst. Res.* **2018**, *52*, 1–11. [CrossRef]
88. Rivest, R. *The MD5 Message-Digest Algorithm*; Technical Report; RFC Editor: Marina del Rey, CA, USA, 1992. [CrossRef]
89. Yang, J.; Onik, M.M.H.; Lee, N.Y.; Ahmed, M.; Kim, C.S. Proof-of-Familiarity: A Privacy-Preserved Blockchain Scheme for Collaborative Medical Decision-Making. *Appl. Sci.* **2019**, *9*, 1370. [CrossRef]
90. Zhang, X.; Poslad, S. Blockchain support for flexible queries with granular access control to electronic medical records (EMR). In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.
91. Zhang, X.; Poslad, S.; Ma, Z. Block-Based Access Control for Blockchain-Based Electronic Medical Records (EMRs) Query in eHealth. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, UAE, 9–13 December 2018; pp. 1–7.
92. Sharples, M.; Domingue, J. The blockchain and kudos: A distributed system for educational record, reputation and reward. In *European Conference on Technology Enhanced Learning*; Springer: Cham, Switzerland, 2016; pp. 490–496.
93. Devine, P. Blockchain Learning: Can Crypto-Currency Methods Be Appropriated to Enhance Online Learning? In Proceedings of the ALT Online Winter Conference, Manchester, UK, 7–10 December 2015.
94. Funk, E.; Riddell, J.; Ankel, F.; Cabrera, D. Blockchain technology: A data framework to improve validity, trust, and accountability of information exchange in health professions education. *Acad. Med.* **2018**, *93*, 1791–1794. [CrossRef] [PubMed]
95. Benna, I.I. Optimizing Health, Education and Governance Delivery Through Blockchain. In *Optimizing Regional Development Through Transformative Urbanization*; IGI Global: Hershey, PA, USA, 2019; pp. 24–47.
96. Hoy, M.B. An introduction to the Blockchain and its implications for libraries and medicine. *Med. Ref. Serv. Q.* **2017**, *36*, 273–279. [CrossRef] [PubMed]
97. Iezzoni, L.I. Assessing quality using administrative data. *Ann. Internal Med.* **1997**, *127*, 666–674. [CrossRef]
98. Alonso, S.G.; Arambarri, J.; López-Coronado, M.; de la Torre Díez, I. Proposing New Blockchain Challenges in eHealth. *J. Med. Syst.* **2019**, *43*, 64. [CrossRef]
99. DesRoches, C.M.; Campbell, E.G.; Rao, S.R.; Donelan, K.; Ferris, T.G.; Jha, A.; Kaushal, R.; Levy, D.E.; Rosenbaum, S.; Shields, A.E.; et al. Electronic health records in ambulatory care—A national survey of physicians. *N. Engl. J. Med.* **2008**, *359*, 50–60. [CrossRef]
100. Bahga, A.; Madisetti, V.K. A cloud-based approach for interoperable electronic health records (EHRs). *IEEE J. Biomed. Health Inform.* **2013**, *17*, 894–906. [CrossRef] [PubMed]

101. Lee, S.M.; Lee, D.; Schniederjans, M.J. Supply chain innovation and organizational performance in the healthcare industry. *Int. J. Oper. Prod. Manag.* **2011**, *31*, 1193–1214. [CrossRef]
102. Dehgani, R.; Jafari Navimipour, N. The impact of information technology and communication systems on the agility of supply chain management systems. *Kybernetes* **2019**. [CrossRef]
103. Kim, C.; Kim, H.J. A study on healthcare supply chain management efficiency: Using bootstrap data envelopment analysis. *Health Care Manag. Sci.* **2019**, 1–15. [CrossRef]
104. Clauson, K.A.; Breeden, E.A.; Davidson, C.; Mackey, T.K. Leveraging blockchain technology to enhance supply chain management in healthcare. *Blockchain Healthc. Today* **2018**. . [CrossRef]
105. World Health Organisation. *WHO Global Surveillance and Monitoring System for Substandard and Falsified Medical Products*; World Health Organisation: Geneva, Switzerland, 2017.
106. Jayaraman, R.; AlHammadi, 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.
107. Dujak, D.; Sajter, D. Blockchain Applications in Supply Chain. In *SMART Supply Network*; Springer: Cham, Switzerland, 2019; pp. 21–46.
108. Narayanaswami, C.; Nooyi, R.; Raghavan, S.G.; Viswanathan, R. Blockchain Anchored Supply Chain Automation. *IBM J. Res. Dev.* **2019**. [CrossRef]
109. Isojarvi, J.; Wood, H.; Lefebvre, C.; Glanville, J. Challenges of identifying unpublished data from clinical trials: Getting the best out of clinical trials registers and other novel sources. *Res. Synth. Methods* **2018**, *9*, 561–578. [CrossRef]
110. Benchoufi, M.; Ravaud, P. Blockchain technology for improving clinical research quality. *Trials* **2017**, *18*, 335. [CrossRef] [PubMed]
111. Benchoufi, M.; Porcher, R.; Ravaud, P. Blockchain protocols in clinical trials: Transparency and traceability of consent. *F1000Research* **2017**, *6*, 66. [CrossRef] [PubMed]
112. Nugent, T.; Upton, D.; Cimpoesu, M. Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research* **2016**, *5*, 2541. [CrossRef]
113. Shae, Z.; Tsai, J.J. On the design of a blockchain platform for clinical trial and precision medicine. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017; pp. 1972–1980.
114. Choudhury, O.; Fairoza, N.; Sylla, I.; Das, A. A Blockchain Framework for Managing and Monitoring Data in Multi-Site Clinical Trials. *arXiv* **2019**, arXiv:1902.03975.
115. Schöner, M.M.; Kourouklis, D.; Sandner, P.; Gonzalez, E.; Förster, J. *Blockchain Technology in the Pharmaceutical Industry*; Frankfurt School Blockchain Center: Frankfurt, Germany, 2017.
116. Marucheck, A.; Greis, N.; Mena, C.; Cai, L. Product safety and security in the global supply chain: Issues, challenges and research opportunities. *J. Oper. Manag.* **2011**, *29*, 707–720. [CrossRef]
117. Xu, X.; Lu, Q.; Liu, Y.; Zhu, L.; Yao, H.; Vasilakos, A.V. Designing blockchain-based applications a case study for imported product traceability. *Future Gen. Comput. Syst.* **2019**, *92*, 399–406. [CrossRef]
118. Westerkamp, M.; Victor, F.; Kupper, A. Tracing manufacturing processes using blockchain-based token compositions. *Dig. Commun. Netw.* **2019**, in press. [CrossRef]
119. 60 of Pharma Companies Using or Trying Blockchain Survey. Available online: https://pharmaphorum.com/news/60-of-pharma-companies-using-or-trying-blockchain-survey/ (accessed on 12 March 2019).
120. 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]
121. Mackey, T.K.; Liang, B.A. The global counterfeit drug trade: Patient safety and public health risks. *J. Pharm. Sci.* **2011**, *100*, 4571–4579. [CrossRef] [PubMed]
122. Tseng, J.H.; Liao, Y.C.; Chong, B.; Liao, S.w. Governance on the Drug Supply Chain via Gcoin Blockchain. *Int. J. Environ. Res. Public Health* **2018**, *15*, 1055. [CrossRef] [PubMed]
123. Toyoda, K.; Mathiopoulos, P.T.; Sasase, I.; Ohtsuki, T. A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. *IEEE Access* **2017**, *5*, 17465–17477. [CrossRef]

124. Sidorov, M.; Ong, M.T.; Sridharan, R.V.; Nakamura, J.; Ohmura, R.; Khor, J.H. Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains. *IEEE Access* **2019**, *7*, 7273–7285. [CrossRef]
125. Pun, H.; Swaminathan, J.M.; Hou, P. *Blockchain Adoption for Combating Deceptive Counterfeits*; SSRN: New York, NY, USA, 2018.
126. Dhillon, V.; Metcalf, D.; Hooper, M. *Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make It Work for You*; Springer: Emeryville, CA, USA, 2017.
127. Course 2: The Medical Billing Process. Available online: https://www.medicalbillingandcodingonline.com/medical-coding-for-billers/ (accessed on 12 March 2019).
128. Counterfeit Medications. Available online: https://en.wikipedia.org/wiki/Counterfeit_medications (accessed on 14 March 2019).
129. Deisingh, A.K. Pharmaceutical counterfeiting. *Analyst* **2005**, *130*, 271–279. [CrossRef]
130. Zhu, Q.; Kouhizadeh, M. Blockchain Technology, Supply Chain Information, and Strategic Product Deletion Management. *IEEE Eng. Manag. Rev.* **2019**, *47*, 36–44. [CrossRef]
131. Plotnikov, V.; Kuznetsova, V. The Prospects for the Use of Digital Technology "Blockchain" in the Pharmaceutical Market. In *MATEC Web of Conferences*; EDP Sciences: Ho Chi Minh, Vietnam, 2018; Volume 193, p. 02029.
132. Montecchi, M.; Plangger, K.; Etter, M. It's real, trust me! Establishing supply chain provenance using blockchain. *Bus. Horiz.* **2019**, in press. [CrossRef]
133. Kumar, R.; Agarwal, A.; Shubhankar, B. Counterfeit Drug Detection: Recent Strategies and Analytical Perspectives. *Int. J. Pharma Res. Health Sci.* **2018**, *6*, 2351–2358.
134. Chiuchisan, I.; Costin, H.N.; Geman, O. Adopting the internet of things technologies in health care systems. In Proceedings of the 2014 International Conference and Exposition on Electrical and Power Engineering (EPE), Iasi, Romania, 16–18 October 2014; pp. 532–535.
135. Decentralized AI: Blockchain's Bright Future. Available online: https://espeoblockchain.com/blog/decentralized-ai-benefits/ (accessed on 20 March 2019).
136. Moosavi, S.R.; Gia, T.N.; Rahmani, A.M.; Nigussie, E.; Virtanen, S.; Isoaho, J.; Tenhunen, H. SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Comput. Sci.* **2015**, *52*, 452–459. [CrossRef]
137. Haghi, M.; Thurow, K.; Stoll, R. Wearable devices in medical internet of things: Scientific research and commercially available devices. *Healthc. Inform. Res.* **2017**, *23*, 4–15. [CrossRef]
138. Yuce, M.R. Implementation of wireless body area networks for healthcare systems. *Sens. Actuators Phys.* **2010**, *162*, 116–129. [CrossRef]
139. Crosby, G.V.; Ghosh, T.; Murimi, R.; Chin, C.A. Wireless body area networks for healthcare: A survey. *Int. J. Ad Hoc Sens. Ubiquitous Comput.* **2012**, *3*, 1. [CrossRef]
140. Rani, A.A.V.; Baburaj, E. Secure and intelligent architecture for cloud-based healthcare applications in wireless body sensor networks. *Int. J. Biomed. Eng. Technol.* **2019**, *29*, 186–199. [CrossRef]
141. Elhayatmy, G.; Dey, N.; Ashour, A.S. Internet of Things based wireless body area network in healthcare. In *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*; Springer: Cham, Switzerland, 2018; pp. 3–20.
142. Zanjal, S.V.; Talmale, G.R. Medicine reminder and monitoring system for secure health using IOT. *Procedia Comput. Sci.* **2016**, *78*, 471–476. [CrossRef]
143. Dimitrov, D.V. Medical internet of things and big data in healthcare. *Healthc. Inform. Res.* **2016**, *22*, 156–163. [CrossRef]
144. 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] [PubMed]
145. Rahman, M.A.; Hassanain, E.; Rashid, M.M.; Barnes, S.J.; Hossain, M.S. Spatial Blockchain-Based Secure Mass Screening Framework for Children With Dyslexia. *IEEE Access* **2018**, *6*, 61876–61885. [CrossRef]
146. Jo, B.; Khan, R.; Lee, Y.S. Hybrid Blockchain and Internet-of-Things Network for Underground Structure Health Monitoring. *Sensors* **2018**, *18*, 4268. [CrossRef]
147. Ichikawa, D.; Kashiyama, M.; Ueno, T. Tamper-resistant mobile health using blockchain technology. *JMIR mHealth uHealth* **2017**, *5*, e111. [CrossRef]

148. 3 Phishing Hacks Breach 20,000 Catawba Valley Patient Records. Available online: https://www.healthcareitnews.com/news/3-phishing-hacks-breach-20000-catawba-valley-patient-records (accessed on 20 April 2019).
149. Nikoloudakis, Y.; Pallis, E.; Mastorakis, G.; Mavromoustakis, C.X.; Skianis, C.; Markakis, E.K. Vulnerability assessment as a service for fog-centric ICT ecosystems: A healthcare use case. *Peer-to-Peer Netw. Appl.* **2019**, 1–9. [CrossRef]
150. Nausheen, F.; Begum, S.H. Healthcare IoT: Benefits, vulnerabilities and solutions. In Proceedings of the 2018 IEEE 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 19–20 January 2018; pp. 517–522.
151. Otoum, S.; Kantarci, B.; Mouftah, H. Adaptively supervised and intrusion-aware data aggregation for wireless sensor clusters in critical infrastructures. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.
152. Otoum, S.; Kantarci, B.; Mouftah, H.T. On the Feasibility of Deep Learning in Sensor Network Intrusion Detection. *IEEE Netw. Lett.* **2019**. [CrossRef]
153. Aloqaily, M.; Otoum, S.; Al Ridhawi, I.; Jararweh, Y. An intrusion detection system for connected vehicles in smart cities. *Ad Hoc Netw.* **2019**, in press. [CrossRef]
154. Catarinucci, L.; De Donno, D.; Mainetti, L.; Palano, L.; Patrono, L.; Stefanizzi, M.L.; Tarricone, L. An IoT-aware architecture for smart healthcare systems. *IEEE Internet Things J.* **2015**, *2*, 515–526. [CrossRef]
155. Saia, R. Internet of Entities (IoE): A Blockchain-based Distributed Paradigm to Security. *arXiv* **2018**, arXiv:1808.08809.
156. Saia, R.; Carta, S.; Recupero, D.; Fenu, G. Internet of Entities (IoE): A Blockchain-based Distributed Paradigm for Data Exchange between Wireless-based Devices. In Proceedings of the 8th International Conference on Sensor Networks (SENSORNETS 2019), Prague, Cxech Republic, 26–27 January 2019.
157. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.K.R. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [CrossRef]
158. Dorri, A.; Kanhere, S.S.; Jurdak, R. Blockchain in internet of things: Challenges and solutions. *arXiv* **2016**, arXiv:1608.05187.
159. Dorri, A.; Kanhere, S.S.; Jurdak, R. Towards an optimized blockchain for IoT. In Proceedings of the ACM Second International Conference on Internet-of-Things Design and Implementation, Pittsburgh, PA, USA, 18–21 April 2017; pp. 173–178.
160. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gen. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
161. Top 10 Biggest Healthcare Data Breaches of All Time. Available online: https://www.healthcareitnews.com/news/3-phishing-hacks-breach-20000-catawba-valley-patient-records (accessed on 20 April 2019).
162. 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] [PubMed]
163. Mamoshina, P.; Ojomoko, L.; Yanovich, Y.; Ostrovski, A.; Botezatu, A.; Prikhodko, P.; Izumchenko, E.; Aliper, A.; Romantsov, K.; Zhebrak, A.; et al. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget* **2018**, *9*, 5665. [CrossRef]
164. Kuo, T.T.; Ohno-Machado, L. ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks. *arXiv* **2018**, arXiv:1802.01746.
165. 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]
166. Qiu, J.; Liang, X.; Shetty, S.; Bowden, D. Towards Secure and Smart Healthcare in Smart Cities Using Blockchain. In Proceedings of the 2018 IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA, 16–19 September 2018; pp. 1–4.
167. Pirbhulal, S.; Wu, W.; Li, G. A Biometric Security Model for Wearable Healthcare. In Proceedings of the 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, 17–20 November 2018; pp. 136–143.
168. Internet of Medical Things (IoMT)—The Future of Healthcare. Available online: https://igniteoutsourcing.com/healthcare/internet-of-medical-things-iomt-examples/ (accessed on 20 March 2019).

169. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
170. Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; Santamaría, V. Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet* **2018**, *10*, 20. [CrossRef]