future internet

MDPI

Review

A Review on Blockchain for the Internet of Medical Things: Definitions, Challenges, Applications, and Vision

Gioele Bigini, Valerio Freschi and Emanuele Lattanzi *

Department of Pure and Applied Sciences, University of Urbino, Piazza della Repubblica 13, 61029 Urbino, Italy; g.bigini@campus.uniurb.it (G.B.); valerio.freschi@uniurb.it (V.F.)

* Correspondence: emanuele.lattanzi@uniurb.it

Received: 3 November 2020; Accepted: 23 November 2020; Published: 25 November 2020

Abstract: Nowadays, there are a lot of new mobile devices that have the potential to assist healthcare professionals when working and help to increase the well-being of the people. These devices comprise the Internet of Medical Things, but it is generally difficult for healthcare institutions to meet compliance of their systems with new medical solutions efficiently. A technology that promises the sharing of data in a trust-less scenario is the Distributed Ledger Technology through its properties of decentralization, immutability, and transparency. The Blockchain and the Internet of Medical Things can be considered as at an early stage, and the implementations successfully applying the technology are not so many. Some aspects covered by these implementations are data sharing, interoperability of systems, security of devices, the opportunity of data monetization and data ownership that will be the focus of this review. This work aims at giving an overview of the current state-of-the-art of the Blockchain-based systems for the Internet of Medical Things, specifically addressing the challenges of reaching user-centricity for these combined systems, and thus highlighting the potential future directions to follow for full ownership of data by users.

Keywords: DLT; blockchain; IPFS; internet of medical things; user-centric systems; consensus

1. Introduction

The market has always turned its attention towards the impact of innovation. Over the past 30 years, the technology moved such quick steps that many consolidated products and services have been replaced to provide better solutions. The role of computer science and engineering in this process is incontrovertible, forcing many industries to go along with it, often making it the company's core business, sometimes resulting in new products and services, but also new professions and improvements. In this fascinating context, the Digital Health sector is rising, in some ways, represented by the combination of computer science and healthcare to empower professionals and address the well-being of people with innovative systems.

The healthcare sector is already taking advantage of the introduction of digital technologies. However, there are some specific issues, as privacy and security issues that still needs attention: i.e., the sharing of information in a trust-less scenario. Particularly sensitive to this topic are the Internet of Medical Things (IoMT) solutions, those solutions that usually exploit devices like smartphones to increase the well-being of an individual. Nevertheless, what makes IoMT promising for the future is the scientific contribution that it could bring. In fact, while a patient sees a medical device as a solution to its problems, professionals

(i.e., doctors, researchers) can use it as a source of data to exploit in order to discover new diseases and treatments. Thus, imagining a world equipped with IoMT solutions, the crowd could build one of the most significant opportunities for healthcare: an interplanetary dataset representing all the clinical stories of the individuals from which to learn. However, as said previously, without firstly enabling a trusted context in a trust-less scenario would imply to neglect some potential risks: health data of an individual are considered sensitive, and they should be secured in any possible way [1].

A technology that seems promising a secure context in a trust-less scenario is the Distributed Ledger Technology (DLT). The technology is usually disclosed as capable of preserving three significant properties: decentralization, immutability, and transparency. These three features could not only give to health data the security it deserves, but also they could allow a shift in data ownership, giving to data creators full access power control over their data, basically shifting from a system-centric position (where the data are created by a user, owned by the provider of a service and the decisions over data are taken together with the provider) to a user-centric position (where the data are created by the user, owned by the user, and the decisions over data are totally up to himself). Advancements in this field often make use of distributed data storage services as the InterPlanetary File System (IPFS), with the attempt of decentralizing data management [2].

In this review, we will illustrate the advancements of the IoMT implementations combined with DLTs. Since we find out that those implementations could be still considered in the early stage of their real potential, we will first describe the state-of-the-art of the Internet of Medical Things, discussing the implementations proposed as capable of preserving privacy and security, finally labeling the proposed architectures regarding the ability to provide a user-centric system. Our final goal is to understand what is needed in order to go towards a user-centric solution for data management with respect to actual implementations.

This contribution is structured as follows: Section 1 contains the introduction; Section 2, the background over the IoMT; Section 3, our position compared to the other surveys; Section 4, the research papers analysis; Section 5, the discussion over user-centricity; Section 6, the future vision; Section 7, the conclusions.

2. Background

2.1. The Internet of Medical Things

A typical Internet of Things (IoT) infrastructure is made up of several devices connected to the Internet able to communicate with each other. More in general, any electronic device that has the capability of interfacing with and communicating with other nodes of the Internet can be considered part of the IoT network, i.e., smartphones.

The Internet of Medical Things (IoMT) envisions a network of medical devices and people, which use wireless communication to enable the exchange of healthcare data [3]. Thus, this specific context put into place significant issues in terms of privacy and security that need to be considered: health data are sensitive data that must be appropriately protected across the network.

If we consider Europe, all private companies and public bodies have been obliged to comply with the General Data Protection Regulation (GDPR). For what concerns health data handling, sources such as "genetic data", "biometric data", and "health data" must be managed carefully since these data are traced back to the sensitive category. Thus, they cannot be used without explicit consent unless for some cases (i.e., occupational medicine, health therapy, public interest). The same applies to data portability which places constraints on how data are shared [1].

Thus, we just highlighted how much privacy and security risks are vital factors to consider. When devices are, in fact, connected to the network for exchanging information, they represent a perfect

target to hit by malicious users. This kind of scenario should be prevented in the healthcare and so, regardless of the security problems related to the device itself (i.e., software and hardware weaknesses), the main threats are represented by the network used for sharing data. As a consequence, most of the implementations are usually forced to anonymize the information, definitely impacting on data exploitability, since anonymization forces the removal of personally identifiable information that has an impact on data integrity and thus quality [4].

2.2. Distributed Ledger Technology and Blockchain

The term "Blockchain" refers to a technology discussed by Stuart Haber and W. Scott Stornetta in 1991 ("How to time-stamp a digital document" [5]): a growing list of data structures, called blocks, connected and secured by cryptography. Conceptually, in the Blockchain, the distribution of information is guaranteed in a decentralized manner, therefore in the absence of a central entity, avoiding any tampering. Thus, Blockchain has been introduced as a technology able to provide decentralization, immutability, and transparency. An example of this is Bitcoin, released under the name of Satoshi Nakamoto [6] which depicts the first successful attempt to apply the technology and later Ethereum, the first Blockchain platform developed by Buterin et al. [7] that introduced smart contracts.

Blocks in the Blockchain can potentially contain any information in addition to the link of its previous block. This link is usually a Hash, a fixed-length "fingerprint" of the block that makes it unique. The first block of a Blockchain is called "Genesis Block", and it is used as the base for the entire chain, as shown in Figure 1.

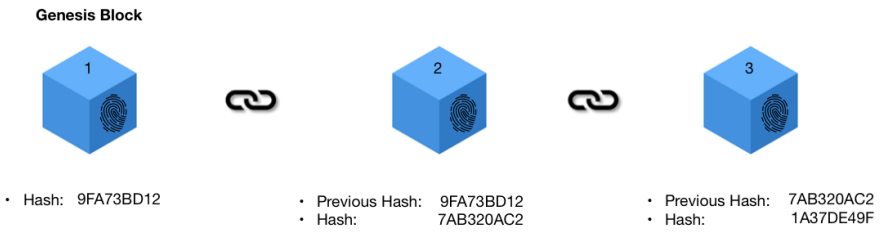

Figure 1. Blockchain technology example.

Blockchain is part of the family of Distributed Ledger Technologies (DLT): it simply implements specific features not considered by all DLTs implementations. In fact, DLT is the broader term to refer simply to distributed databases that are managed by various participants. An example of DLT different from the Blockchain is IBM Hyperledger [8].

In order to add more blocks to a Blockchain, the consensus between participants must be reached. One of the main differences between DLTs is usually the consensus: some DLTs offer full decentralized consensus between participants while others do not. Moreover, the same blocks constituting a DLT could be accessible or not, leading to "Permissioned" and "Permissionless" solutions.

Permissionless solutions (usually referred to as Public Blockchains) are based on avoiding establishing control by any central entity in the network. This means that, if the peers in the network trust the technology, the Blockchain constitutes a distributed network sharing a cryptographic secure, immutable ledger accessible to anyone. On the contrary, private blockchains are usually referred to as permissioned solutions, a kind of implementation restricted to a few network participants. This kind of implementation sacrifices decentralization for better control over the Blockchain itself. It can be useful in those cases in which there is a need of having only some actors participating in adding blocks to the network for various reasons.

Essential features to mention about Blockchain concerning other DLT solutions is the absence of a central entity. This means that, if peers in the network trust the technology, the Blockchain constitutes a distributed network, sharing a cryptographic secure, immutable ledger accessible to anyone. The ability to add blocks on the chain is guaranteed by a consensus protocol, a mechanism defined for the specific Blockchain through which the participants converge to reach consensus (i.e., the Proof-Of-Work consensus protocol [9]). On the contrary, DLT implementations different from Blockchain are usually restricted to a limited number of participants. It can be useful in those cases in which there is a need of having only some actors participating in adding blocks to the network, as well as able to read the blocks.

2.3. InterPlanetary File System

The InterPlanetary File System (IPFS) is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files [2]. The IPFS was born by looking to the data-sharing platforms of the past as Napster, large file distribution systems supporting over million of users.

Content published to IPFS is public by design, and, currently, IPFS does not provide a built-in solution for storing private data. Anyway, it is possible to store and transfer private data over IPFS through encryption and to create private networks of nodes. IPFS cannot guarantee data availability that means it is necessary to continuously save the published content on an IPFS node to reach availability and thus the node should always be online.

The main difference between a Centralized System and IPFS System architecture is shown in Figure 2. While in a centralized system architecture (Figure 2a), an uploader of content acts as a provider of content (maintaining it) and user nodes access the content. In an IPFS system architecture (Figure 2b), all user nodes act as a provider of content and so all the participants guarantee the maintenance.

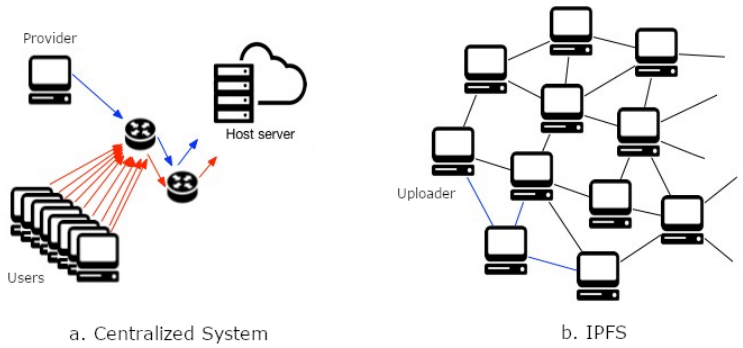

Figure 2. Centralized systems and IPFS.

Since the Blockchain needs distributed consensus between all the network nodes in order to add a new block, it will be expensive to store any data into the Blockchain. It is more efficient to store transactional data on the Blockchain while using IPFS as a storage medium. Adopting this architecture is hinted at by several research papers found. Moreover, a commercial example of Blockchain combined with IPFS implementation is Filecoin, a decentralized storage network designed to encourage nodes to save third-party content in return for some reward [10].

3. Comparison to Other Surveys

An increasing amount of works dealing with Blockchain and IoMT can be retrieved within the current scientific literature, specifically pointing out opportunities for overcoming the challenges posed by IoMT.

We started getting the literature in the following databases: IEEE Xplore Digital Library; Wiley Online Library; ACM Digital Library; MDPI; Springer; Scopus. We used the keywords "Blockchain" AND "Internet of Medical Things", and 41 different research publications have been found. The findings show that the field does not appear to be so investigated, thus confirming that the Internet of Medical Things, coupled with Blockchain, leaves room for more attention, research and studies in the healthcare broader context.

We adopt the following methodology to divide the literature. First of all, we discriminated the surveys from the scientific papers to understand the issues addressed, with the attempt to reach an understanding of the advancements in the IoMT. Lately, we look to research papers trying to identify the most investigated topics, understanding the technologies used and how they could allow user-centricity. Finally, we tried to understand which of these papers proposed implementations that were user-centric.

Out of these 41 publications, 21 are surveys that discuss several challenges and opportunities posed by Blockchain integration on the Internet of Medical Things. Since this work would like to give a different position for the future with respect to other surveys, we decided to first divide surveys papers from research papers, discussing the first one in this section. Later on, in Section 4, we will discuss the research papers found, finally leading to our contribution in Section 5.

We associate papers in Table considering the kind of survey: some consider talking about the IoMT in a more informative way, and others prefer to summarize specific topics. In contrast, others finally prefer to give a view over real implementations. Thus, they belong to: General (Table 1), if they broadly analyze the IoMT area; Topic Focused, if they give an overall comprehension over a specific topic (Table 2); Implementation Focused, if they try to sum up practical implementations and frameworks (Table 3).

Table 1. General Reviews.

Survey	Papers
General	Pilkington [11] Borovska [12] Mackey et al. [13] Agbo et al. [14]

Table 2. Topic Focused Reviews.

Survey	Domain	Papers
Topic Focused	Privacy and Security	Nanayakkara et al. [15] Neshenko et al. [16] Seliem and Elgazzar [17]
	Data Management	Banerjee et al. [18]
	Frameworks for Blockchain-Based IoMT	Fernández-Caramés and Fraga-Lamas [19] Al-Turjman et al. [3] Pavithran et al. [20] Chukwu and Garg [21]

Table 3. Implementation Focused Reviews.

Survey	Domain	Papers
Implementation Focused	Scalability	Mazlan et al. [22]
	Data Management and Interoperability	Zhang et al. [23] Saha et al. [24]
	Healthcare Sector	Hussien et al. [25] Hölbl et al. [26] Zubaydi et al. [27] Khezr et al. [28]
	Industrial Sector	Al-Megren et al. [29] Ahram et al. [30]

3.1. General

Pilkington [11] and Borovska [12] addressed the growing segment of the Internet of Medical Things providing reflections on how the devices could contribute to generate big data, potentially leading to new medical solutions thanks to the application of machine learning techniques. In their view, the intersection of big data analytics and precision medicine can be promising for detecting diseases in the future. They examined the Blockchain technology as a medium for healthcare data management in general, considering the shortcomings of private and centralized organizations, analyzing the transformative role of Blockchain for the management of electronic health records.

Mackey et al. [13] and Agbo et al. [14] discussed the role of Blockchains in facilitating data management, provenance, and security, resulting in its potential to transform healthcare. They recognized that Blockchain is not only about cryptocurrencies, but could be helpful in other sectors, i.e., healthcare. For example, the use of Blockchain for privacy reasons on electronic health records, or for enabling credentials and licensing of medical professionals, or for advance in biomedical engineering. They also showed several examples of solutions based on Blockchain in healthcare application scenarios, which, however, generally lack adequate prototype implementations. Hence, they highlighted the state-of-the-art in the development of Blockchain applications for healthcare, concluding that there is still need for more research in the field to improve and evaluate the impact of the adoption of this technology.

3.2. Topic Focused

The reviews from Nanayakkara et al. [15], Neshenko et al. [16], Seliem and Elgazzar [17] consider several threats and risks related to the IoMT. They focused on the analysis of articles in order to discover privacy, security, cost, and performance issues, highlighting present frameworks and implementations. Their investigation concludes that Blockchain could be used to solve the trust, security and privacy issues without sacrificing performances.

Other researchers as Banerjee et al. [18] focused on data management for the IoMT. Specifically, they considered the proposals of keeping track of the health datasets on the Blockchain as a way of sharing data. Avoiding the sharing of information directly on the Blockchain makes sense because it is difficult to store data in the blocks since the technology itself could not scale efficiently in size.

Other authors surveyed frameworks for the Internet of Medical Things combined with Blockchain. Fernández-Caramés and Fraga-Lamas [19], Al-Turjman et al. [3], Pavithran et al. [20], and Chukwu and Garg [21] focus the attention on summarizing frameworks in order to identify components and design elements for new implementations, along with usual development plans.

3.3. Implementation Focused

Mazlan et al. [22] are the only researchers found addressing the scalability problems that public Blockchains pose. It is worth noticing that they find out that generally the choice to tackle with scalability is by making two kinds of choices: storage optimization or redesign of the entire Blockchain, both of them significative development obstacles.

Zhang et al. [23] and Saha et al. [24] summarize the existing Blockchain-based systems and applications, classifying them by traceability and data security protection and trying to understand opportunities and challenges for the development in the industry. They also analyzed the ability of Blockchain systems to support data integrity, reliability, and the capability to address security issues in the cloud.

For what concerns the use cases in the healthcare domain, Hussien et al. [25], Hölbl et al. [26], Zubaydi et al. [27] and Khezr et al. [28] conducted their reviews by analyzing the use of Blockchain in healthcare applications and putting them into a coherent taxonomy. Their work provides insights on the increasing number of studies related to the adoption of Blockchain technology, looking for several motivations as data sharing and security issues.

Finally, Al-Megren et al. [29] and Ahram et al. [30] investigated the Internet of Things, healthcare, supply chain management, and the public administration sector. For each sector, they described the use cases in which an attempt is made to implement Blockchain solutions. They found out the growing maturity, benefits, and challenges of Blockchain technology underlining the need for further investigations at that time, for all the sectors involved.

3.4. Our Position

The surveys analyzed seem not to focus on the user-centricity in the IoMT. We think that an aspect that should be more reviewed and investigated is the ability of these combined systems (Blockchain and IoMT) to enable users to have full control over their data with no authority in the middle. This does not merely mean ensuring privacy and security but also to provide systems and mechanisms to data owners to manage their data across the network entirely. In this review, we would like to focus on an essential aspect of the Internet of Medical Things: User-centricity. We think this aspect is vitally important for future implementations since health data are sensitive data that could enable personalized medicine. The surveys found are generally focused on finding best practices, identifying challenges and frameworks without focusing on patient-centricity. For this reason, we will go through the research papers found to understand how to move towards an idea of Blockchain-based implementations in which the solution for data management in IoMT should enable User-centricity, which means enabling users to own and control their data.

4. Research Papers Review

IoMT implementations combined with Blockchain are not so many and indeed they should need more investigations. In Section 3.4 "Our Position", we talked about the methodology used for searching the papers and described all the analyzed surveys found. In this section, we are going to discuss, based on the background provided in the previous section, all the remaining research papers found.

In Table 4, we highlighted applicative research paper to give a more precise overview of practical implementations. The ones not applicative are considered theoretical. For each paper, either theoretical or applicative, we extract the used Blockchain implemented, in terms of permissioned and permissionless, and we assigned the relative area of focus. We identified that there are four specific topics: Blockchain Design, if the research is oriented on suggesting the architecture of a Blockchain-based healthcare solution; Data sharing, if they focus on data management and sharing of data; Blockchain for Security, if they focus

on the usage of the Blockchain for increasing security in various domains; Data Crowdsourcing, if they focus on the use of Blockchain for crowdsourcing solutions.

Table 4. Research papers classification.

Topic	Authors	DLT	Applicative
Blockchain Design	Shae and Tsai [31]	Permissioned	
	Bhawiyuga et al. [32]	Permissioned	
	Chakraborty et al. [33]	Permissioned Permissionless	
	Srivastava et al. [34]	Permissioned Permissionless	
Data Sharing	Angeletti et al. [35]	Permissioned	
	Abdellatif et al. [36]	Permissioned	
	Dilawar et al. [37]	Permissionless	
	Jiang et al. [38]	Permissioned Permissionless	×
	Xu et al. [39]	Permissioned Permissionless	×
	Wang et al. [40]	Permissioned	×
	Dey et al. [41]	Permissioned	×
	Azbeg et al. [42]	Permissioned	×
	Nguyen et al. [43]	Permissioned	×
	Nguyen et al. [44]	Permissioned	×
Blockchain for Security	Dwivedi et al. [45]	Not Specified	
	Meng et al. [46]	Not Specified	
	Alblooshi et al. [47]	Permissioned	×
	Srivastava et al. [48]	Not Specified	
Data Crowdsourcing	Fernández-Caramés et al. [49]	Permissionless	×
	Rupasinghe et al. [50]	Permissioned Permissionless	×

4.1. Theoretical Research Papers

Theoretical research papers focused mainly on three big groups: Blockchain Design, frameworks design for building a solution for healthcare data management; Data sharing, approaches, and methodologies to share data safely in the network; Blockchain for Security, research that exploits Blockchain as a medium for systems security, i.e., security of mobile devices.

For each paper, we looked to the Blockchain used, but, specifically for the research papers in the Blockchain for Security section, it has not been possible to retrieve the type of Blockchain, since it is not specified.

Thus, Shae and Tsai [31], Bhawiyuga et al. [32], and Chakraborty et al. [33] focused their attention identifying components needed for Data Management in a way that different participants could safely access data.

Other researchers as Angeletti et al. [35], Abdellatif et al. [36] and Dilawar et al. [37] put their focus on data access architectures and mechanisms, looking to different opportunities in private and public

Blockchains solutions, as well as the use of smart contracts. In their visions, we need privacy-preserving applications where users can safely share their personal data.

For what concerns Blockchain for Security section, Dwivedi et al. [45], Meng et al. [46], Alblooshi et al. [47], and Srivastava et al. [48] agree on the fact the IoMT is intensive data domain with a continuous growing rate that must be secured because of a large amount of sensitive data. They see in Blockchain a possible solution since it is a tamper proved digital ledger able to ensure communication between non-trusting parties and no central authority. They addressed problems of safe data transmission, even proposing advanced cryptographic primitives in order to make devices more secure and anonymous over a Blockchain-based network.

4.2. Applicative Research Papers

For what concern applicative research papers, we saw that the majority of the implementations use a Permissioned Blockchain, and they are most of all focused on the data-sharing issue for healthcare with some exceptions.

Wang et al. [40], Dey et al. [41], Azbeg et al. [42], Nguyen et al. [43], and Nguyen et al. [44] focus on the safe sharing of healthcare data and data management. They specifically focus on cloud-based IoMT solutions finding in the Blockchain a system for data sharing between devices through the help of smart contracts.

Jiang et al. [38], Xu et al. [39], and Srivastava et al. [48] built their solutions on a combination of Permissioned and Permissionless Blockchains to reach a better decentralization and data management.

Some researchers also focus on the hypothesis that the Blockchain can be used for crowdsourcing monetization. Fernández-Caramés et al. [49] and Rupasinghe et al. [50] built solutions using permissionless and Permissioned Blockchain and smart contracts for achieving this goal.

Finally, Alblooshi et al. [47] gave a solution for securing IoMT device ownership. This kind of solution leverages totally on smart contracts, managing the ownership of IoMT devices with no trusted third party.

5. A User-Centric Perspective for the Internet of Medical Things

From the analysis we did in the previous section, we saw that the majority of research papers prefer to use Permissioned solutions instead of permissionless ones. This interesting fact is probably related to the opportunity represented by a permissioned and private model that offers a more flexible ledger in terms of authority. The reason to implement this model is mainly related to the possibility of keeping control of the Blockchain by a restricted number of participants, usually referred to as a consortium. However, this model is risky and it sacrifices decentralization and immutability: the consortium could have the concrete potential to modify the ledger. This consideration is particularly important for those implementations that try to reach user-centricity because if a ledger could be changed by a restricted group of participants (without considering tampering), it could not be defined as a user-centric system. Thus, this problem posed some questions to researchers that probably encouraged the introduction of decentralized storages combined with Blockchain (as IPFS) not only for scalability reasons but also for security because they constitute two different technologies.

A user-centric system is a system where users have more control and flexibility with respect to ordinary systems. In the healthcare domain, this means that patients could be able to manage and own their data entirely, making it live in their personal devices or their preferred locations.

In this section, we will assess three more things out of the type of Blockchain for what concerns implementations: if the consensus is decentralized or restricted to a limited number of participants, if they mentioned user-centricity and which of them is finally user-centric. In order to classify the implementations, we considered the type of DLTs, the consensus and so, the strength of the solution proposed in terms of

user-centricity which is the ability of the user to control its data. Results are shown in Table 5 and, in this section, we are going to discuss each paper.

Table 5. Evaluation of user-centricity in research papers labeled as Applicative. User-centricity is the ability of the user to own its data without the risk of tampering or loose power by consortiums decisions.

Authors	Consensus	Mention Centricity	User-centric
Jiang et al. [38]	Restricted	No	No
Xu et al. [39]	Decentralized	Yes	Yes
Wang et al. [40]	No Consensus	No	No
Dey et al. [41]	Restricted	No	No
Azbeg et al. [42]	Restricted	No	No
Nguyen et al. [43]	Decentralized	No	No
Nguyen et al. [44]	Decentralized	Yes	Yes
Alblooshi et al. [47]	Decentralized	No	Yes
Fernández-Caramés et al. [49]	Decentralized	No	Yes
Rupasinghe et al. [50]	Decentralized	Yes	Yes

Jiang et al. [38] propose a platform named BlocHIE, based on Blockchain, for data sharing between individuals employing two Blockchains: EMR-Chain, for medical institutions; PHD-Chain, for individuals. Both institutions and individuals can submit and share healthcare data. They handle healthcare data through the combination of off-chain storage and on-chain transactions. The off-chain storage is achieved by storing the data in the distributed databases of the hospitals while the on-chain verification is achieved by including the hash value of each medical record in the transaction. Because medical institutions usually submit very privacy-sensitive data as medical reports and treatments (because of healthcare professionals) while individuals are more prone to submit a massive amount of data (because of data generated by IoMT devices), such kind of approach provides from one side a centralized solution where institutions can keep control over user data and to the other side a decentralized solution for data provenance. The whole system could not be considered user-centric but could solve the problem of data management in a healthcare environment.

Xu et al. [39] propose Healthchain, a large-scale health data management scheme based on Blockchain where users have full control of their data as well as access policies. The system uses two Blockchains, namely Userchain, a public Blockchain used to publish users' data, and Doccchain, a private Blockchain of healthcare institutions used to publish doctors diagnoses. For the researchers, this scheme should ensure the design goals of supporting large-scale IoT devices, reaching a high efficiency, and creating a real-time online diagnosis system, which could preserve privacy, ensure accountability and, finally, manage permissions. It is composed of five entities: the IoMT Devices; the User Nodes, able to manage one or more IoT devices aggregating, encrypting, and sending data to the storage node; the Doctor Nodes that are doctors or companies providing healthcare services; the Accounting Node: a particular node maintained by the consortium to verify whether the transactions from doctor nodes are correct and valid; Storage Nodes, IPFS-based systems maintained by the consortium that collaboratively store complete encrypted users ' IoMT data and encrypted doctors' diagnoses in a distributed manner. IoMT devices send health data to the User Nodes that encrypt the data forwarding them to an IPFS storage that takes care of the transaction to the Userchain. The Doctor Node is then able to give real-time online diagnoses readable

by the patients reading the Docchain. The ability to have control over data by the user is significant and goes towards a user-centric solution.

Wang et al. [40] proposes a Blockchain-based eHealthcare system using Hyperledger Fabric interoperating with wireless body area networks (WBAN) which use the WBAN to network the devices of the patients and the Blockchain technology. Hyperledger Fabric provides a private, permissioned network where participants trust each other. The actors of such a system are: patients, doctors, healthcare institutions, and suppliers. The workflow of the proposal is the following: the patients transmit the data collected through the WBAN from the sensors to the centralized devices. The devices wait for the instructions by the centralized device that later generates the final record of information to submit to the Blockchain, in order to update the physical data of the patients. In this kind of architecture, the data are effectively kept safe: healthcare professionals get access only to the records of their patients. Anyway, in this implementation, Hyperledger Fabric does not require any consensus mechanism at all making it challenging to know if the ledger has been tampered with, leading to a less secure system. In this solution, the data management layer does not seem to allow secure control over data, and so we cannot say it is user-centric.

Dey et al. [41] propose a Blockchain-based system named Healthsense where a sensor collects real-time data of a patient's medical condition and stores it in the Blockchain for later use with smart contracts. The solution makes use of IPFS for off-chain storage, and, through a smart contract, the sensor is put in communication with the Blockchain. In some way, this allows IoMT devices to find each other and begin trading data off-chain autonomously or with the platform. Anyway, researchers' architecture does not specify any consensus model, and, eventually, it will be restricted since it is thought to work specifically for hospitals.

Azbeg et al. [42] proposes a platform architecture based on a Permissioned Blockchain for diabetes self-management. The researchers said that integrating Blockchain with low power devices, such as the ones used for diabetes monitoring is a difficult task. The way they reached this goal was by registering each new device in the Blockchain by its owner, the one able to permit to access the Blockchain. Thus, the system is composed of the devices, the Blockchain, and the medical institutions (that maintains the Blockchain). The connection to the Blockchain is realized through a gateway (a smartphone) able to encrypt and route information to an off-chain IPFS database which can be accessed by authorized physicians and healthcare teams. The healthcare institutions are actually the full nodes of the network: they store pointers to data, validate transactions, and create new blocks as other similar centralized solutions, leading to a potential system-centric solution rather than user-centric.

Nguyen et al. [43] proposed a system for data sharing combined with a Blockchain network as a reliable data exchange among healthcare users. It is composed of a wearable sensor device, a mobile gateway, and a cloud server. They used the Ethereum Blockchain platform for the Blockchain network and design smart contracts to control user access on the cloud. Anyway, using the cloud as a storage is a risky solution and needs to be owned by someone, usually a central authority. Moreover, the system is more focused on secure sharing rather than preserving ownership. For this reason, in Nguyen et al. [44], they substitute the cloud storage with the IPFS, going towards a user-centric system.

Alblooshi et al. [47] used smart contracts to manage the ownership of IoMT devices with no trusted third-party. The proposed system consists of five key components: patient, manufacturer, and two smart contracts (one for the IoMT device and one owned by the manufacturer) and the healthcare provider. Basically the patient, which is the owner of the IoT Device, can set the rules and conditions on the IoMT device smart contract for device management. The healthcare provider includes professionals who are interested in knowing, owning, or transferring the ownership of the device. This kind of solution leverages totally on smart contracts, potentially even in a permissionless Blockchain, but anyway it is not thought to

handle health data. At the same time, it is user-centric, since all the decisions made are handled by the user that could exit the system at any time.

Fernández-Caramés et al. [49] proposed a system for monitoring patients remotely and warning them about potentially dangerous situations. It uses smartphones to collect information and sends them to a remote cloud. In order to exchange data between healthcare parties, the system includes the deployment of a decentralized storage system that receives, processes, and stores the collected data and provides a cryptocurrency as an incentive for participation. The architecture consists in an interface for users that allows the access of the stored information: a decentralized storage system that replicates the collected information and distributes it automatically among multiple nodes; and a distributed ledger that uses smart contracts in order to reward participation. This kind of approach is interesting and goes towards data crowdsourcing with Blockchain that should be user-centric by design.

Rupasinghe et al. [50] proposes a conceptual Blockchain-based fall prediction model using smart contracts and the FHIR (Fast Healthcare Interoperability Resources) standard protocol. They identify four roles: person under care, primary care provider (or long-term provider), secondary care provider (or short term providers), and temporary caregiver. Each of these entities is maintaining their electronic health record management systems and can be considered as data sources for the final prediction model. The architecture is based on a Permissioned and private Blockchain that leverage smart contracts for accessibility, creating different access levels based on each user category, leading to a user-centric solution.

6. Future Directions

As mentioned throughout this review, the possibility of freely sharing sensitive information between professionals and health institutions would allow a step forward for personalized medicine, taking advantage of the most advanced machine learning techniques that computer science is offering.

We saw that there are different ways of thinking on how to share data on the Blockchain: storing data in its blocks (but very difficult actually due to scalability issues); exploiting data provenance, by basically storing positions of data in the Blockchains instead of data itself; and using distributed storages combined with the Blockchain, thus using them as off-chain storage. In each of the solutions, there is a potential to never move data across the network that could be simply accessed and used.

The review focused on the ability of Blockchain of creating specific solutions able to enable the user to be the true owner of their data. At the moment, what is evident is the increasing interest in user-centric solutions even when it is not the goal of the research. Several solutions are trying to increase the level of ownership of users over their data, but the problem of creating a full decentralized user-centric system for health data remains. The usage of permissioned solutions owned by healthcare institutions is sometimes ambiguous, maybe enabling users on managing their data but finally forcing them to accept consortium rules over data management. Moreover, this specific problem affecting security in Permissioned solutions also has an impact on the usage of decentralized storages that risk being wasted since they lose their value. If the Blockchain risks being compromised by participants, then the solutions fail to deliver immutability and even if user data are on decentralized storage, they will not be able to guarantee a user-centric system. Several implementations underline this.

Finding a solution to this problem, maybe through hybrid implementations between Permissioned and Permissionless implementations, could be even more impressive when these networks can reward the participants making them able to be active contributors to a community with their data as the one of healthcare. This vision also settles very well with a concept that has been found in one review only: rewards for data contribution. As said previously, whenever an individual uses an IoMT system or an IoT device, it is never rewarded for the contribution it makes. Typically, individuals pay to get professional help, but their contribution is higher than the performance received. In fact, in principle, they contribute to

enhancing scientific knowledge. In an increasingly Blockchain-enabled world, the Internet of Blockchains could definitely enable data sharing and data crowdsourcing.

However, we would need to move the architectures from a system-centric perspective, where a user is the consumer of the application, to a user-centric perspective, where the user is more than a consumer but an active participant. It could be exciting having a solution in which each user physically owns data, for example, on a small device in their home or their smartphones. If these devices act as safe, decentralized storage, then every unknown entity could access easily the data stored in it, respecting rules posed by the users that are owners of what they share.

7. Conclusions

Wellbeing is the foundation for the lifestyle of a healthy individual and managing medical data could help users on better achieving the goal.

In the past, the need for a large amount of data and privacy issues was weaker: the traditional method for data collection was through recordings on paper, medical science was not supported by existing technology, and there was no large amount of data available to use, leading to no explanation for several diseases. With mobile devices, it is now possible to collect a massive amount of data that could be used to deliver and discover new solutions and treatments. By introducing the Internet of Medical Things, potentially any data collected by a user could be exploited with a specific goal.

We examined in this work the contributions of the Blockchain to IoMT applications, focusing on the current challenges and vision for the future. The review aimed in particular at summarizing surveys and research papers that attempt to understand the state of the industry from a practical point of view and which are the related problems that currently act as barriers for a subsequent step towards user-centricity.

Several papers have been investigated focusing on their approaches with Blockchain to go towards a user-centric system. Looking to the solutions proposed, what DLTs are underlining is that they could bring a new way of handling privacy and security in the healthcare context, as well as making the sharing of information between different institutions easier. Through the achievement of specific goals as user-centricity, security, scalability, and interoperability, the Blockchain can be the driving technology through which to develop lasting and independent platforms for data sharing that can give value to privacy and contributions.

Author Contributions: Conceptualization, G.B. and E.L.; methodology, G.B. and E.L.; investigation, G.B.; writing—original draft preparation, G.B.; writing—review and editing, G.B., V.F., and E.L.; visualization, G.B., V.F., and E.L.; supervision, E.L.; project administration, E.L.; funding acquisition, V.F., and E.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Regione Marche with DDPF n. 1189 and by the Department of Pure and Applied Sciences, University of Urbino.

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

Abbreviations

The following abbreviations are used in this manuscript:

DLT	Distributed Ledger Technology
GDPR	General Data Protection Regulation
IoMT	Internet of Medical Things
IoT	Internet of Things
IPFS	Inter Planetary File System
WBAN	Wireless Body Area Network

References

1. European Commission. Complete Guide to GDPR Compliance. 2016. Available Online: https://gdpr.eu (accessed on 25 November 2020).
2. Benet, J. Ipfs-content addressed, versioned, p2p file system. *arXiv* **2014**, arXiv:1407.3561.
3. Al-Turjman, F.; Nawaz, M.H.; Ulusar, U.D. Intelligence in the Internet of medical things era: A systematic review of current and future trends. *Comput. Commun.* **2020**, *150*, 644–660.
4. Mostert, M.; Bredenoord, A.L.; Biesaart, M.C.; Van Delden, J.J. Big Data in medical research and EU data protection law: Challenges to the consent or anonymise approach. *Eur. J. Hum. Genet.* **2016**, *24*, 956–960.
5. Haber, S.; Stornetta, W.S. How to time-stamp a digital document. In *Conference on the Theory and Application of Cryptography*; Springer: Berlin, Germany, 1990; pp. 437–455.
6. Nakamoto, S. Bitcoin P2P e-cash paper. *Cryptogr. Mail. List.* **2008**, *31*, 2008.
7. Buterin, V. A next-generation smart contract and decentralized application platform. *White Pap.* **2014**, *3*, Available online: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf (accessed on 25 November 2020).
8. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.
9. Back, A. Hashcash—a denial of service counter-measure, 2002, Available online: ftp://sunsite.icm.edu.pl/site/replay.old/programs/hashcash/hashcash.pdf (accessed on 25 November 2020).
10. Filecoin. A Decentralized Storage Network Designed to Store Humanity's Most Important Information. 2017. Available online: https://filecoin.io (accessed on 25 November 2020).
11. Pilkington, M. Can blockchain improve healthcare management? Consumer medical electronics and the IoMT. *Consum. Med. Electron. IOMT* Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3025393 (accessed on 24 August 2017).
12. Borovska, P. Big Data Analytics and Internet of medical Things Make Precision Medicine a Reality. *Int. J. Internet Things Web Serv.* **2018**, *3*, 24–31.
13. 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.
14. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain technology in healthcare: A systematic review. *Healthcare* **2019**, *7*, 56.
15. Nanayakkara, N.; Halgamuge, M.; Syed, A. Security and Privacy of Internet of Medical Things (IoMT) Based Healthcare Applications: A Review. In Proceedings of the 262nd The IIER International Conference, Istanbul, Turkey, 6 November 2019.
16. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 2702–2733.
17. Seliem, M.; Elgazzar, K. BIoMT: Blockchain for the internet of medical things. In *2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*; IEEE: New York, NY, USA, 2019; pp. 1–4.
18. Banerjee, M.; Lee, J.; Choo, K.K.R. A blockchain future for internet of things security: a position paper. *Digit. Commun. Netw.* **2018**, *4*, 149–160.
19. 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.
20. Pavithran, D.; Shaalan, K.; Al-Karaki, J.N.; Gawanmeh, A. Towards building a blockchain framework for IoT. *Clust. Comput.* **2020**, pp. 1–15.
21. Chukwu, E.; Garg, L. A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations. *IEEE Access* **2020**, *8*, 21196–21214.

22. Mazlan, A.A.; Daud, S.M.; Sam, S.M.; Abas, H.; Rasid, S.Z.A.; Yusof, M.F. Scalability Challenges in Healthcare Blockchain System—A Systematic Review. *IEEE Access* **2020**, *8*, 23663–23673.
23. Zhang, J.; Zhong, S.; Wang, J.; Wang, L.; Yang, Y.; Wei, B.; Zhou, G. A Review on Blockchain-Based Systems and Applications. In *International Conference on Internet of Vehicles*; Springer: Berlin, Germany, 2019; pp. 237–249.
24. Saha, A.; Amin, R.; Kunal, S.; Vollala, S.; Dwivedi, S.K. Review on "Blockchain technology based medical healthcare system with privacy issues". *Secur. Priv.* **2019**, *2*, e83.
25. Hussien, H.; Yasin, S.; Udzir, S.; Zaidan, A.; Zaidan, B. A Systematic Review for Enabling of Develop a Blockchain Technology in Healthcare Application: Taxonomy, Substantially Analysis, Motivations, Challenges, Recommendations and Future Direction. *J. Med. Syst.* **2019**, *43*, 320.
26. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A systematic review of the use of blockchain in healthcare. *Symmetry* **2018**, *10*, 470.
27. Zubaydi, H.D.; Chong, Y.W.; Ko, K.; Hanshi, S.M.; Karuppayah, S. A review on the role of blockchain technology in the healthcare domain. *Electronics* **2019**, *8*, 679.
28. Khezr, S.; Moniruzzaman, M.; Yassine, A.; Benlamri, R. Blockchain technology in healthcare: A comprehensive review and directions for future research. *Appl. Sci.* **2019**, *9*, 1736.
29. Al-Megren, S.; Alsalamah, S.; Altoaimy, L.; Alsalamah, H.; Soltanisehat, L.; Almutairi, E.; others. Blockchain use cases in digital sectors: A review of the literature. In *Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*; IEEE: New York, NY, USA, 2018; pp. 1417–1424.
30. Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In *Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON)*; IEEE: New York, NY, USA, 2017; pp. 137–141.
31. 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)*; IEEE: New York, NY, USA, 2017; pp. 1972–1980.
32. Bhawiyuga, A.; Wardhana, A.; Amron, K.; Kirana, A.P. Platform for Integrating Internet of Things Based Smart Healthcare System and Blockchain Network. In *Proceedings of the 2019 6th NAFOSTED Conference on Information and Computer Science (NICS)*; IEEE: New York, NY, USA, 2019; pp. 55–60.
33. Chakraborty, S.; Aich, S.; Kim, H.C. A secure healthcare system design framework using blockchain technology. In *Proceedings of the 2019 21st International Conference on Advanced Communication Technology (ICACT)*; IEEE: New York, NY, USA, 2019; pp. 260–264.
34. Srivastava, G.; Crichigno, J.; Dhar, S. A light and secure healthcare blockchain for iot medical devices. In *Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*; IEEE: New York, NY, USA, 2019; pp. 1–5.
35. Angeletti, F.; Chatzigiannakis, I.; Vitaletti, A. The role of blockchain and IoT in recruiting participants for digital clinical trials. In *Proceedings of the 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*; IEEE: New York, NY, USA, 2017; pp. 1–5.
36. Abdellatif, A.A.; Al-Marridi, A.Z.; Mohamed, A.; Erbad, A.; Chiasserini, C.F.; Refaey, A. ssHealth: Toward Secure, Blockchain-Enabled Healthcare Systems. *IEEE Netw.* **2020**, *34*, 312–319.
37. Dilawar, N.; Rizwan, M.; Ahmad, F.; Akram, S. Blockchain: Securing Internet of Medical Things (IoMT). *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 82–89.
38. Jiang, S.; Cao, J.; Wu, H.; Yang, Y.; Ma, M.; He, J. Blochie: A blockchain-based platform for healthcare information exchange. In *Proceedings of the 2018 IEEE International Conference on Smart Computing (Smartcomp)*; IEEE: New York, NY, USA, 2018; pp. 49–56.
39. Xu, J.; Xue, K.; Li, S.; Tian, H.; Hong, J.; Hong, P.; Yu, N. Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. *IEEE Internet Things J.* **2019**, *6*, 8770–8781.
40. Wang, J.; Han, K.; Alexandridis, A.; Chen, Z.; Zilic, Z.; Pang, Y.; Jeon, G.; Piccialli, F. A blockchain-based eHealthcare system interoperating with WBANs. *Future Gener. Comput. Syst.* **2020**, *110*, 675–685.

41. Dey, T.; Jaiswal, S.; Sunderkrishnan, S.; Katre, N. HealthSense: A medical use case of Internet of Things and blockchain. In *Proceedings of the 2017 International Conference on Intelligent Sustainable Systems (ICISS)*; IEEE: New York, NY, USA, 2017, pp. 486–491.
42. Azbeg, K.; Ouchetto, O.; Andaloussi, S.J.; Fetjah, L.; Sekkaki, A. Blockchain and IoT for security and privacy: A platform for diabetes self-management. In *Proceedings of the 2018 4th International Conference on Cloud Computing Technologies and Applications (Cloudtech)*; IEEE: New York, NY, USA, 2018, pp. 1–5.
43. Nguyen, D.C.; Nguyen, K.D.; Pathirana, P.N. A mobile cloud based iomt framework for automated health assessment and management. In *Proceedings of the 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*; IEEE: New York, NY, USA, 2019; pp. 6517–6520.
44. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for secure EHRs sharing of mobile cloud based e-Health systems. *IEEE Access* **2019**, *7*, 66792–66806.
45. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* **2019**, *19*, 326.
46. Meng, W.; Li, W.; Zhu, L. Enhancing Medical Smartphone Networks via Blockchain-Based Trust Management Against Insider Attacks. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1377–1386. .
47. Alblooshi, M.; Salah, K.; Alhammadi, Y. Blockchain-based ownership management for medical IoT (MIoT) devices. In *Proceedings of the 2018 International Conference on Innovations in Information Technology (IIT)*; IEEE: New York, NY, USA, 2018; pp. 151–156.
48. Srivastava, G.; Parizi, R.M.; Dehghantanha, A.; Choo, K.K.R. Data sharing and privacy for patient iot devices using blockchain. In *Proceedings of the International Conference on Smart City and Informatization*; Springer: Berlin, Germany, 2019; pp. 334–348.
49. Fernández-Caramés, T.M.; Froiz-Míguez, I.; Blanco-Novoa, O.; Fraga-Lamas, P. Enabling the internet of mobile crowdsourcing health things: A mobile fog computing, blockchain and IoT based continuous glucose monitoring system for diabetes mellitus research and care. *Sensors* **2019**, *19*, 3319.
50. Rupasinghe, T.; Burstein, F.; Rudolph, C.; Strange, S. Towards a blockchain based fall prediction model for aged care. In Proceedings of the Australasian Computer Science Week Multiconference, Sydney, NSW, Australia, 29–31 January 2019; pp. 1–10.