IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.xxxx/ACCESS.2021.DOI

A Survey on Blockchain-based IoMT Systems: Towards Scalability

AMIRHOSSEIN ADAVOUDI JOLFAEI[1], SEYED FARHAD AGHILI[2], AND DAVE SINGELEE[2]

[1]Department of Computer Science, University of Luxembourg (e-mail: amirhossein.adavoudi@uni.lu)
[2]imec-COSIC KU Leuven, Kasteelpark Arenberg 10-bus 2452, 3001 Heverlee, Belgium (e-mail: seyedfarhad.aghili, dave.singelee@esat.kuleuven.be)

Corresponding author: Seyed Farhad Aghili (e-mail: seyedfarhad.aghili@esat.kuleuven.be).

This work was financed in part by the European Union's Horizon 2020 Research and innovation program, under grant agreement No. 826284 (ProTego)

ABSTRACT Recently, blockchain-based Internet of Medical Things (IoMT) has started to receive more attention in the healthcare domain as it not only improves the care quality using real-time and continuous monitoring but also minimizes the cost of care. However, there is a clear trend to include many entities in IoMT systems, such as IoMT sensor nodes, IoT wearable medical devices, patients, healthcare centers, and insurance companies. This makes it challenging to design a blockchain framework for these systems where scalability is a most critical factor in blockchain technology. Motivated by this observation, in this survey we review the state-of-the-art in blockchain-IoMT systems. Comparison and analysis of such systems prove that there is a substantial gap, which is the negligence of scalability. In this survey, we discuss several approaches proposed in the literature to improve the scalability of blockchain technology, and thus overcoming the above mentioned research gap. These approaches include on-chain and off-chain techniques, based on which we give recommendations and directions to facilitate designing a scalable blockchain-based IoMT system. We also recommended that a designer considers the well-known trilemma along with the various dimensions of a scalable blockchain system to prevent sacrificing security and decentralization as well. Moreover, we raise several research questions regarding benchmarking; addressing these questions could help designers determining the existing bottlenecks, leading to a scalable blockchain.

INDEX TERMS Internet of Medical Things (IoMT), Blockchain, Cloud, Scalability, Healthcare, Security

I. INTRODUCTION

The Internet of Things (IoT) is associated with the network of physical objects such as medical devices, Radio- Frequency IDentification (RFID) tags, home appliances, and vehicles [1]. There are a wide variety of IoT applications that can be divided into various domains such as healthcare, smart cities, retail, traffic, process automation, logistics, remote monitoring, and so on [2], [3].

Internet of Medical Things (IoMT) or Medical Internet of Things (MIoT) is the health customized version of IoT in which a doctor can measure various parameters of the patient's health such as heart rate, body temperature, and oxygen level remotely and immediately by means of different sensors placed in or on the patient's body [4]–[6]. An example of various environments and entities of IoMT is shown in Fig. 1. This figure shows how entities, including healthcare and emergency centers, medical devices, patients, and doctors can interact with each other via IoMT technology. Researchers have categorized an IoMT structure in different ways. In [7], for example, a healthcare system based on IoT primarily consists of three different components: cloud computing, IoT, and Wireless Body Area Network (WBAN). Besides, in [7], [8], the authors discussed an IoMT structure constituted of three layers, namely perception, network, and application, while in [9], five layers for IoMT are defined: perception, network, middleware, application, and business.

Remote monitoring enhanced clinical care, and physical and physiological assistance for patients are the major uses of an IoT healthcare system. An IoMT system improves the quality of care by real-time monitoring and minimizes the cost of care. It is worth noting that with the rising costs of drug and medical device development [7], the IoMT market has grown rapidly, increasing from 41.2 billion U.S. dollars in 2017 to an anticipated 158.1 billion U.S. dollars in 2022 [10].

Currently, in healthcare systems, devices such as sensors and wearables with wireless connectivity are communicating through a central device, generally called a gateway, which

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3117662, IEEE Access

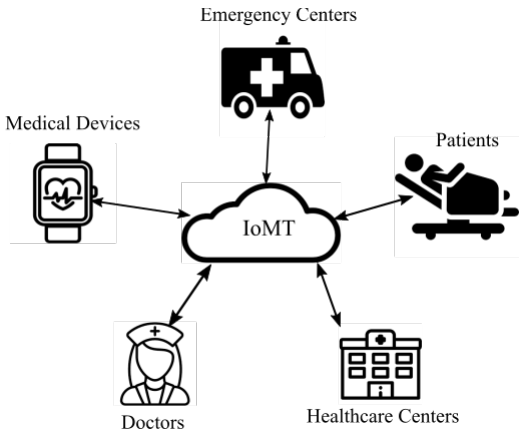

FIGURE 1. IoMT system environments.

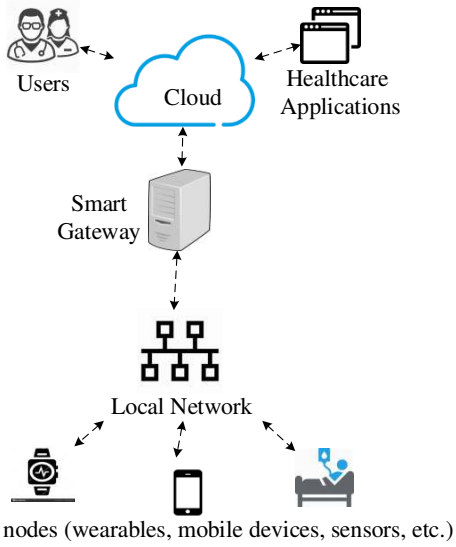

FIGURE 2. Cloud-based architecture of an IoMT application.

usually transmits the received data to the cloud [11]–[14]. The cloud-based architecture of an IoMT [11] is presented in Fig. 2. In this figure, IoT end nodes such as wearables, mobile devices, sensors, etc., send their real-time data to the gateway, and then the gateway decides whether to redirect the received data to a cloud or not. Users including patients, doctors, and healthcare applications receive the corresponding data from the cloud, and thus can monitor the end nodes online. Users can even access the data stored on the cloud anytime and from anywhere when they need it. The cloud-based architecture of an IoMT system includes several requirements such as mutual authentication, scalability, availability, access control, auditability of data, etc. A designer might consider some of these requirements depending on the desired IoMT application. However, a cloud-based IoMT system has several drawbacks concerning the availability of services, the privacy of users, security, interoperability, and data manipulation. The point of failure of the cloud server is one of the major drawbacks from which such systems suffer. That is, in case the cloud is down for whatever reason, the patients, doctors and medical staff are not able to connect to the cloud server, thus causing unavailability. In the following section, we discuss in detail the requirements and drawbacks of such a system.

Blockchain technology, which is a distributed ledger, can bring potential benefits to IoMT applications. Having a distributed architecture is one of the great benefits of blockchain technology, as it can solve a major problem, i.e., the point of failure of the cloud in IoMT applications. Moreover, blockchain technology offers additional merits, including smart contracts, security via data access management, tamper-proof recording, transparency, trustless consensus, and open architecture. Despite these benefits, several challenges exist regarding this technology, such as lack of standards and regulations, scalability, firmware and hardware vulnerabilities, lack of trusted authorities and data feeds, and challenges in smart contracts such as time-stamp dependence, dependence on the order of transactions, and call stack depth [15]–[17]. In [18], the authors summarized issues related to cloud-based and blockchain-based IoT applications. They noted that blockchain has the potential to provide security and protect against losses and risks and also helps preserve privacy. In contrast, the cloud has advantages in scaling the network and combating the forking issues of blockchain. The authors also mentioned that the issues of scalability, flexibility, latency, cost concerns, and energy consumption require more attention in Blockchain-based systems.

It is important to highlight that patients' data must be sent and received on time in blockchain-based IoMT applications, particularly in remote health monitoring applications, including emergency healthcare, wireless capsule endoscopy, telemedicine systems, and monitoring of aged patients. In these systems, patients' health data has to be sent and received in a timely manner so that doctors, nurses, and medical staff can remotely and real-time monitor patients and as a result, a correct and accurate diagnosis can be established. For example, in [19], patient data, namely Electroencephalography (EEG) and Electrocardiography (ECG) should be sent promptly for real-time monitoring. As another example, in [5], the heart rate data must be sent real-time for successful detection to detect sleep apnea.

A. MOTIVATION

More generally, there are two approaches for designing and implementing a framework for IoMT systems: i) cloud-based ii) blockchain-based. Several research reviews such as [5], [20], [21] have been published about designing cloud-based IoMT systems. However, cloud-based IoMT systems suffer from several drawbacks: centralized architecture, unavailability of services, etc [22]–[24]. Several research reviews [25]–[32] have been published regarding blockchain-

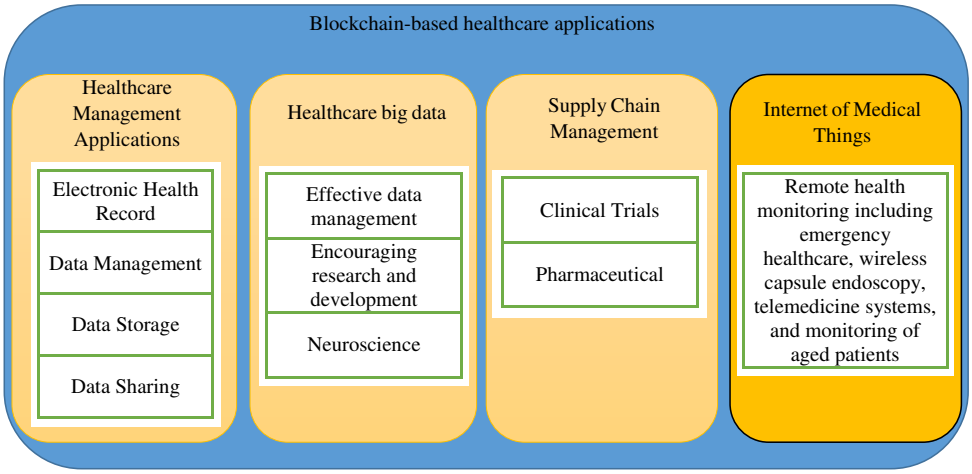

FIGURE 3. Blockchain-base healthcare applications.

based healthcare applications. These reviews aimed to cover and discuss all the relevant healthcare applications, i.e., healthcare management, supply chain management, healthcare big data, and IoMT applications. These applications and their related subcategories are shown in Fig. 3.

In work [33], the authors prepared a brief overview of the implementation of blockchain-based healthcare systems. The authors mentioned that these systems should consider scalability, security and privacy of data. However, their study does not review blockchain-based IoMT work and there are no structured approaches for the mitigation of the scalability limitations.

Blockchain-based IoMT domain itself includes the following key and widely used applications: remote health monitoring, emergency healthcare, wireless capsule endoscopy, telemedicine systems, and monitoring of aged patients. Moreover, several research studies [7], [21], [34]–[37] and surveys [8], [11], [38], [39] have been carried out with regard to the IoMT applications from the privacy and security point of view. But, based on our conducted literature review, none of these studies considered blockchain technology as a solution for bringing benefits, including distributed trust, integrity, transparency, traceability, etc. The state-of-the-art survey [3] investigated the impacts of various types of technologies on IoMT. These technologies include machine learning, edge/fog computing, big data, software defined networks, and blockchain. The authors also discussed how these technologies could improve the quality of service of IoMT systems. However, this survey did not focus on the blockchain-based IoMT systems, whereas our work fully considers such systems and gives directions concerning the scalability of blockchain-based IoMT systems. The survey [39], also just briefly mentioned that blockchain technology is a future research direction that can provide strong security and privacy protection.

The research studies [22], [31], [40]–[59] discussed blockchain-IoMT applications; however, none of the papers have focused on the scalability of the blockchain, which is a key factor in blockchain-based IoMT systems. We compared all the mentioned research work in various terms in sections V and VI.

In these systems, in fact, entities such as sensors and wearable devices are resource-constrained in terms of computational power, communication, and storage, which is in contrast to blockchain technology, which is resource-intensive in terms of computational and storage capacity. Additionally, more and more entities, including sensor nodes, IoT wearable medical devices, patients, private clinics, healthcare centers, enterprise research organizations, and insurance companies, are joining IoMT systems. On the other hand, the centralized communication model cannot satisfy the growing need for huge IoMT systems [24], [60]. Hence, conducting comprehensive and detailed research on the blockchain-based IoMT application that discusses the key factor, i.e., scalability and giving directions in this regard, is necessary.

B. CONTRIBUTION

This paper makes the following contributions:

- Studying the requirements and the drawbacks of cloud-based IoMT systems.
- Discussing the benefits that blockchain technology brings into IoMT systems and the major challenges which blockchain-based IoMT systems pose.
- Discussing various types of blockchain-based IoMT systems, including healthcare management, supply chain management, healthcare big data, and Internet of Medical Things applications.
- Reviewing and comparing the state-of-the-art blockchain-based IoMT systems in terms of various attributes, including the year when the paper is published, the authors, focus of study, architecture, benefits, problems

and challenges and evaluation.
- Analysing several state-of-the-art blockchain-based IoMT systems to prove the existence of a significant gap, which is the negligence of scalability.
- Presenting different approaches for improving the scalability of IoMT systems based on the current state-of-the-art works and discussing several design methods that can potentially lead to a scalable blockchain-based IoMT system.

C. ORGANIZATION

The survey is organized as follows. Section II presents the requirements and drawbacks of IoMT systems based on the cloud architecture. In this section, first, the requirements of such systems are discussed and then the drawbacks are elaborated. Section III generally discusses blockchain technology as a solution to overcome the drawbacks mentioned before: it first gives an introduction of blockchain technology, explains the merits of employing blockchain-based technologies for IoMT systems, and discusses the methodology applied to our study. Additionally, various healthcare applications based on blockchain technology are explained, namely healthcare management, healthcare big data, supply chain management, and IoMT applications. Section V provides a literature review of the state-of-the-art works concerned with blockchain-based IoMT systems. In Section VI the research gap is defined by considering the papers reviewed in Section V. Following that, Section VII first gives a brief introduction to the scalability. Then, we discuss various dimensions of the blockchain and compare two different approaches for designing scalable blockchains, and finally, several research directions and recommendations for the purpose of the scalability of blockchain-based IoMT applications are given in this section. The last Section VIII, concludes this survey.

II. CLOUD-BASED IOMT SYSTEMS

In this section, we discuss the requirements of a cloud-based IoMT system, including mutual authentication, scalability, availability, session unlinkability, access control, confidentiality, integrity, etc. We then explain the drawbacks of such systems, such as centralized architecture, unavailability of services, etc.

A. CLOUD-BASED IOMT SYSTEM REQUIREMENTS

Considering an IoMT system, a designer needs to satisfy the following requirements for a cloud-based architecture [11], [14], [34], [61].

- Scalability: As the entities participating in a network increase, it is significant to keep the quality of services such as latency, bandwidth, and jitter below a threshold level.
- Availability: All legitimate users, including physicians, nurses, and medical staff, must easily get access to the medical data collected by the sensors.
- Session unlinkability: An attacker should not be able to track a target user by linking across his/her sessions.
- Auditability of data: There might be trust issues between entities such as providers and the users, so auditability is an essential requirement in a cloud environment.
- Mutual authentication: Before establishing the session key and transferring information between two entities, they must be authenticated by each other.
- Access control: Doctors or nurses should only access part of the information defined by the policies. These policies are typically stored in the gateway.
- Confidentiality: Only legitimate users such as physicians are able to access patients' medical information.
- Integrity: The purpose of data integrity is to ensure that the data have not been modified during the transmission in any way.
- Entity privacy-preserving: The identity of each entity should not be learned from the transferred messages between entities.
- Energy consumption: The scheme designed for resource-constrained IoMT systems, including sensors, wearable devices, etc., should be efficient in terms of computation and communication.
- User-friendly: Reporting medical data should be easy and convenient for patients and doctors as well.

A designer could choose several of mentioned requirements so as to design his/her desired scenario.

B. DRAWBACKS OF CLOUD-BASED IOMT SYSTEM

In this subsection, we discuss and summarize the major drawbacks of the IoMT based on the cloud architecture. In cloud-based architecture, the IoMT nodes typically send and receive data to/from a centralized third-party, i.e., cloud. Hence, the IoMT system elements such as doctors and patients rely on this centralized trusted party [58]. The state-of-the-art security frameworks use centralized architecture, which is not well suited for IoMT due to the large distributed scale of IoMT networks and single point of failure. In addition, security and privacy are major challenges in IoMT in which devices are resource-limited and cannot afford the high resource requirements of traditional heavyweight security algorithms [43].

The authors in [62], discuss the limitations of using conventional cryptographic primitives and access control models to address security and privacy issues in the cloud-based environment. Moreover, the authors highlight the fact that the privacy and integrity of healthcare data must be protected from unauthorized access attempts from inside the network or ecosystem, e.g., employees of the healthcare provider or cloud service provider.

The authors in [22] state that patients' data are usually stored in the cloud in healthcare applications, which makes it difficult for the users to have enough control over their data. However, it is the entity's right to know where and how his/her data has been stored, and who can access his/her data due to the General Data Protection Regulation(GDPR) [63]. The GDPR framework sets rules and policies for the collec-

tion and processing of personal data. These data concerns individuals are living in European Union (EU) [64][1].

In [44], the authors describe IoMT applications and platforms' dependency on a cloud that compromises security. The authors in [23] state: "Even if the unprecedented economic and engineering challenges are resolved, cloud servers will remain a bottleneck and point of failure that can disrupt the entire network," which encourages researchers to gain benefit from distributed architectures such as blockchain technology to address the drawbacks mentioned so far.

According to [24], users' privacy is particularly at risk when sensitive medical data are managed by centralized companies, which can make illegitimate use of them, and the centralized control of IoMT devices makes the central unit target of the attacks. In addition, much of the cost of IoMT systems is related to central servers, infrastructure, maintenance, and networking equipment; the total cost of an IoMT system increases exponentially as the number of IoMT devices increases [66].

To sum up, the challenges and drawbacks of IoMT cloud-based architecture could be categorized as the following [24].

- Centralized architecture: The state-of-the-art security mechanisms for IoMT are highly centralized. The entire network operation relies on cloud servers, which creates a single point of failure as well as a bottleneck. These centralized mechanisms are not well suited for IoMT applications due to low scalability and the high cost of central servers and maintenance.
- Unavailability of service: Cloud servers are sometimes down because of cyberattacks, such as software bugs, power, cooling, and so forth. Moreover, cloud services may be down due to force majeure or routine maintenance.
- Privacy of users: Privacy of users like patients and doctors may not be well protected as required, as the cloud is a third-party that lacks trust [58].
- Security: The centralized nature of the cloud might lead to security risks. IoMT nodes are vulnerable to various malicious attacks, including distributed denial-of-service (DDoS) attacks, data-stealing, hacking, and remote hijacking [24].
- Interoperability: Interoperability is the process of sharing and transferring data among different sources. Many medical records are generated daily and are stored in a centralized location at different hospitals; thus due to the centralized nature of the health record storage system, these records end up fragmented. Thus, in the cloud-based system, centralized data authorities must guarantee a reliable database in an untrusted network [26].
- Data manipulation: Patients' sensitive data might be manipulated and can be used inappropriately.

[1]Each part of the world opted for a different approach to data protection. For instance, the US follows the Health Insurance Portability and Accountability Act (HIPAA), a set of standards created to secure protected health information [65].

III. BLOCKCHAIN AS A SOLUTION

In this section, we elaborate on blockchain's merits that help us overcome the drawbacks mentioned in the previous section. What is worth mentioning is the limitation of the blockchain, such as scalability and energy consumption, that should be made taking into account. At the end of this section and later in sections V and VI, we will discuss the issues of combining the blockchain and IoT. Moreover, in Section VII, we will explain different approaches and perspectives about designing a scalable blockchain system in the context of IoMT.

According to the research studies discussed in Section II, most of the current IoMT ecosystems depend on communication and control models based on a central cloud server. This model has connected generic computing devices and continues to support small-scale IoT networks. However, the centralized communication model cannot satisfy the growing need for huge IoT systems [24], [60].

Blockchain technology has a multitude of benefits that can be utilized in an IoMT system. With blockchain, for example, people are not required to entrust IoMT data produced by their devices to centralized companies. Instead, data could be safely stored in different peers (i.e., a node of the blockchain network that has its own copy of the chain), and the blockchain could guarantee their authenticity and prevent unauthorized access [24].

The authors in [44]contributed by presenting a secure mechanism to provide integrity of data, confidentiality, and authenticity in IoMT employing blockchain technology. However, due to the enormous size of the personal healthcare records (PHRs) and the consequent increase in the size of the entire blockchain, their mechanism suffers from the storage problem. A blockchain-based architecture of an IoMT system is shown in Fig. 4 [44]. This figure illustrates that medical practitioners can upload the patient's reports to the block of a distributed ledger and later doctors or caretakers will be able to monitor those reports remotely. In addition, the real-time data sent by body sensors can be observed remotely by an authorized doctor or a caretaker.

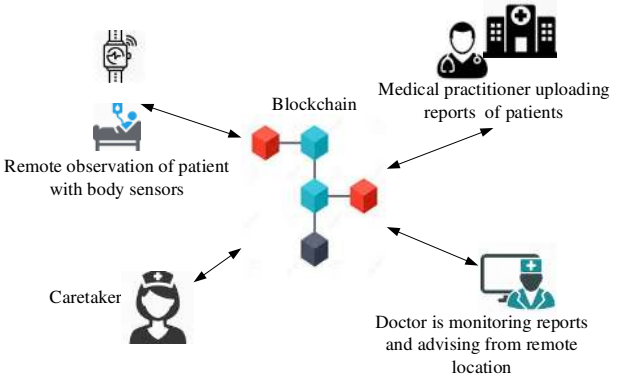

FIGURE 4. Blockchain-based IoMT architecture.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3117662, IEEE Access

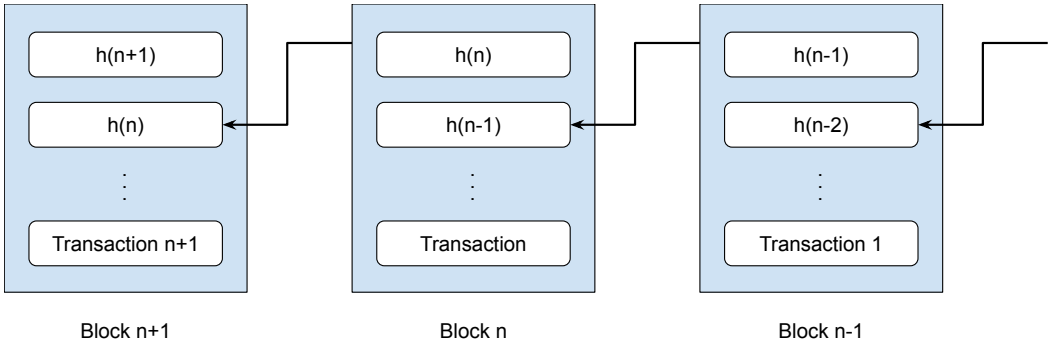

FIGURE 5. Block forms in the blockchain technology.

A. BLOCKCHAIN TECHNOLOGY

According to statistics, spending on blockchain solutions worldwide increases from 2.9 billion U.S. dollars in 2019 to 12.4 billion U.S. dollars in 2022 [33]. Coined in 2008, blockchain enables its users to have transactions without involving a third party [68]. In other words, blockchain is a distributed decentralized ledger to which data can only attach and data is always persistent. All of the stored data forms in blocks and a network of peer-to-peer nodes share the copy of the blockchain (see Figure 5). Each block typically includes two parts, namely the block header and the block body. Before committing to the chain, each block is checked in terms of both completeness and correctness, and the defined consensus protocol provides validation and security for the stored data. The consensus protocols are categorized in two quorum and deterministic groups [69]: the quorum protocols such as proof of work (PoW) [70], [71] analyze the resources intensive behavior and deterministic protocols such as proof of luck (PoL) [72] use pseudo-randomness for identifying the block.

There are various types of blockchain, namely public, private and permissioned. Anyone can join the network in the public blockchain, access the blocks, and even read, write and store blocks, and execute consensus protocol such as Bitcoin and Ethereum [73], [74]. However, in Private blockchain, only an entity which is trusted by other users in the network can control, read and write transactions to the blockchain [75]. Finally, permissioned blockchain is a hybrid of the public and private blockchain. Considering the permissioned blockchain, a few selected nodes are predetermined to be involved in transaction and each entity can grant the permission of reading or writing to other entities [67]. In Table 1, these types of blockchains are compared.

Smart Contract: In blockchain technology, smart contracts written as program codes are self-executing contracts allowing transactions to be conducted between untrusted or anonymous parties without a central authority. A smart contract can be called for the network members who are aware of the transaction address. Smart contracts provide a great deal of confidence as the blockchain has the property of irremovability. Ethereum [76] is one of the well-known blockchains, the largest platform for smart contracts [77]. More information regarding smart contracts is presented in [78]. In this work, the authors explained the criteria regarding the infrastructure of smart contracts.

In the next subsection, we discuss the benefits of blockchain technology for IoMT systems [24], [31], [32], [44].

B. BENEFITS OF EMPLOYING BLOCKCHAIN-BASED TECHNOLOGIES FOR IOMT SYSTEMS

In the following, the merits of using blockchain technologies, including distributed ledger, smart contracts, security,tamper-proof, transparency, trustless consensus, and open architecture, are discussed.

- Distributed architecture: The distributed nature of the blockchain ensures that there is no single point of failure or single point of attack in the system.
- Smart contracts: Smart contracts can be used where certain rule-based methods are created for patients' data access. Here, permissions can be granted to certain health organizations. In IoMT applications, smart contracts may be used to set the rules of the application, automate processes, and enable seamless communications and

TABLE 1. Comparison between public, private and permissioned blockchains and centralized database properties [67]

Feature	Public	Private	Permissioned	Centralized
Speed	Slow	Fast	Fast	Slow
Identity	Anonymous	Known	Anonymous	Known
Traceability	Yes	Restricted	Yes	No
Participation	Anyone	Permitted entities	Permitted entities	Limited
Write/Read Permissions	Granted/ Granted	Restricted/ Restricted	Restricted/ Granted	Restricted/ Granted

transactions between IoMT devices and other entities, including patients, healthcare providers, and doctors.
- Security via data access management: Only authorized entities like doctors, medical staff, etc., can get access to a patients' record information based on the policies sets defined by the legitimate administrator.
- Tamper-proof recording: Any unauthorized alteration in patients' medical data can be detected trivially. For example, altering or modifying data from clinical trials fraudulently can be eradicated.
- Transparency: Since every recorded data in a block is publicly available to be seen by all network peers, and the stored data cannot be modified, this provides transparency. For example, each transaction between drug manufacturers, pharmacists, and patients can be traced to verify and protect important drug information for tackling issues such as counterfeit drugs. This will lead to drug traceability.
- Trustless consensus: Blockchain-based IoMT applications are based on distributed consensus, which eliminates the necessity to use trusted intermediaries such as financial institutions and central banks.
- Open Architecture: Open architecture is a technology infrastructure with specifications that are made public by its designers. This includes officially approved standards as well as privately designed architectures [79].

Industry Trends in Blockchain: According to Statista (2021), forecasts suggest that spending on blockchain solutions will continue to grow in the coming years, reaching nearly 19 billion U.S. dollars annually by 2024 [80]. Factors driving the blockchain market include [32] privacy and security of protected health information such as Confidentiality, Integrity and Availability (CIA), limited access to health data, fraud and abuse detection, inconsistent rules and permissions for accessing patient data, lack of interoperability as a consequence of non-compatibility between systems, trackability and verifiability. Regarding the CIA property, it is important to emphasize that since the data stored in the blocks are signed, blockchain can offer strong Integrity protection. Also, it is nearly impossible to change the data in a block due to linking via hashes and the consensus requirement. Moreover, because a distributed architecture is used and a full copy of the data is located in all nodes, a high level of availability is provided by design. However, confidentiality is typically low by default since blockchain requires the transaction data to be visible and verifiable by design. Therefore, the blockchain implementation does not enforce confidentiality aspects as strongly as it enforces the integrity and availability of the data. Thus, If a high level of confidentiality is required, the system should provide additional protection, such as application-level encryption or other means where (sensitive) data is not directly readable by unauthorized nodes, which is out of the scope of this survey.

C. SCALABILITY OF BLOCKCHAIN

Blockchain is a decentralized database that facilitates auditable and transparent management of data by means of an immutable and append-only data structure [81], [82]. It is implemented as a linked list where pointers are cryptographic hash ones and every block contains a hash of the previous block [83]. A serious concern of blockchain is the scalability problem which has been discussed in [81], [84]–[87]. Several papers [29], [88]–[91] specifically discuss the scalability problem faced by current blockchain-based IoT applications. The paper [17] states that the scalability problem is caused by inefficient blockchain structures and consensus mechanisms.

Bitcoin, for example, takes about 10min to confirm transactions, with maximum throughput 7 transactions/sec. Meanwhile, mainstream payment-processing companies like Visa have a high throughput of about 24,000 transactions/ sec [81], [85]. Blockchain scalability is concerned with the following metrics [81], [85]:

- Maximum throughput is defined as the maximum number of transactions that the blockchain can confirm and this rate is limited by the inter-block time and the maximum block size.
- Latency is defined as the amount of time for a transaction to confirm. Additionally, several other metrics such as bootstrap time, cost per confirmed transaction (CPCT) are discussed in [85].

IV. HEALTHCARE APPLICATIONS

In this section, we explain our methodology and then explore various blockchain-based healthcare applications.

A. OUR METHODOLOGY

This section will research various blockchain-based healthcare applications and explain our focus and references used in this survey. Blockchain technology has a wide range of applications [17], [112]–[114], including finance, notary services, management of personal data, insurance, industrial sector, automotive and mobility, healthcare, education, government, software, IoT, sharing economy, etc.

Healthcare applications based on the blockchain itself can be categorized into four different main groups, including healthcare management, healthcare big data, supply chain management, and Internet of Medical Things applications which are summarized in Table 2.

In the following subsections, we first explore all these applications, and later in the literature review section, we concentrate on the blockchain-based IoMT application to narrow down the scope of our research. We elaborate specifically on this application and conduct a comprehensive review of the state-of-the-art research in this regard. This research review is carried out by reviewing recent articles published from the years 2017 to 2021. The following features are considered when comparing the literature:

- Focus of study: This attribute indicates the research work has been carried out from what point of view.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3117662, IEEE Access

TABLE 2. Relevant references of blockchain-base healthcare applications

References	Blockchain-based Healthcare Applications	Sub categories
[92]–[101]	Healthcare Management Applications	Electronic Health Record, Data Management, Data Storage, Data Sharing
[29], [27], [102]	Healthcare big data	Effective data management, Encouraging research and development, Neuroscience
[25], [103]–[106]	Supply Chain Management	Clinical Trials, Pharmaceutical
[7], [11], [27], [34], [38], [54]–[59], [107]–[111]	Internet of Medical Things (IoMT)	Remote health monitoring (emergency healthcare, wireless capsule endoscopy, telemedicine systems, and monitoring of aged patients)

- AI: This attribute shows that the research study benefits of AI technology.
- Benefits: This feature highlights the benefits of the proposed model.
- Problems and Challenges: It discusses the problems and issues that the related work currently faces or might face in the future. Studying this feature carefully will help us distinguish the research gaps among the reviewed studies.
- Evaluation: This attribute has two values: “Yes" indicates that the authors have carried out related experiments to evaluate their proposed model, while “No" means no experimental study has been conducted for evaluation.

B. HEALTHCARE MANAGEMENT APPLICATIONS

Electronic Health Records (EHRs), data management, data storage, and data sharing are the major applications that fall into this category [28].

a: Electronic Health Records

EHRs are digital forms of patient records collected from the start of treatment until the patient is cured. This information is gathered by medical institutes such as hospitals, insurance companies, etc [115]. Fig. 6 shows that EHRs include medications, sound and image files, X-ray images, diagnosis records, etc.

In [32], three important features of EHRs systems that can be improved by employing blockchain are discussed. These features are as follows:

- Immutability via unique hash value: The data of a block can be verified using the corresponding unique hash value stored to the next block. The hash value is computed by applying a hash function such as SHA256 to a message; this value is used for checking the integrity of the corresponding message.
- Security via data access management: Only authorized users may access record information since each hash may contain particular user permissions for patients, nurse, device, etc.
- Interoperability via version control: Since everyone who has the related responsibility and role, they can append information to the record avoiding issues such as inconsistent or duplicate records.

b: Data Management

Blockchain can enable secure data management or improve the security level in an application such as healthcare [92]. MedRec [98] is a new record management system employing blockchain technology to handle electronic medical records (EMRs). This system provides patients with immutable records and easy access to their medical data from healthcare centers. MedRec makes patient data sharing possible and incentivizes public health authorities, medical researchers, etc., to be involved in the network as “miners”. This helps researchers to sustain the system.

c: Data Storage

In [95], the authors proposed a framework named BlockCloud by combining the blockchain and cloud technologies to enhance the applications in healthcare environments. This framework is proposed for storing and managing EHRs in a cloud environment while it considers the security as well as the accuracy that results from the key feature of blockchain, i.e., tamper-proof digital ledger [44].

d: Data Sharing

Sharing healthcare records might happen, for instance, between a patient and a doctor at their first meeting, among doctors, or sharing could happen between a patient and an insurance company or a research center. Blockchain technol-

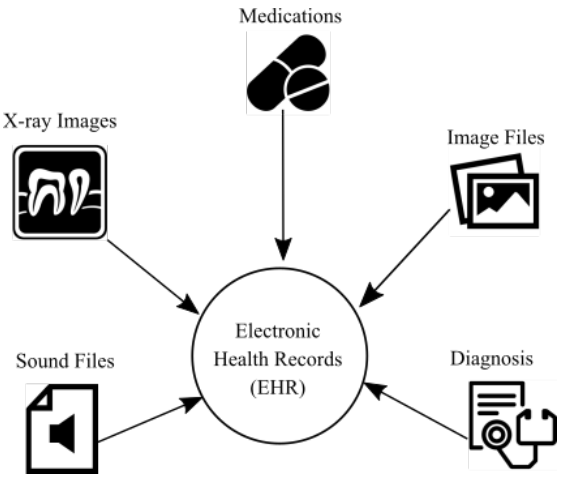

FIGURE 6. Electronic Health Records (EHRs)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3117662, IEEE Access

ogy can enable a secure and convenient sharing mechanism of EHRs [97]. An App called Healthcare Data Gateway (HGD) [99] based on the blockchain provides a patient with owning, controlling and sharing their health information securely and easily without sacrificing privacy, which makes the healthcare systems smarter while keeping patients' data private.

C. HEALTHCARE BIG DATA

Effective data management, encouraging research and development, and neuroscience are relevant applications that can be grouped under this category [29].

a: Effective Data Mining

These days, thanks to technologies, including deep learning, artificial intelligence (AI), and neural networks, data mining has become practical due to access to big data [29]. Researchers could convert the previously healthcare data to information that has more meaning, and further, the information can be transformed into knowledge by processing this huge amount of information. The obtained knowledge, in fact, embodies relevant and useful information that later, stakeholders can gain benefit from the provided knowledge. These stakeholders might include patients, producers of healthcare data, insurance companies, providers such as medical centers, hospitals, and finally, analyzers or researchers [29].

b: Encouraging Research and Development

Currently, large healthcare data such as biomedical and genomics information are analyzed by researchers to improve research and development in these areas. On the other hand, this information might be fake or manipulated by malicious users, which affects the quality of research. Blockchain in this domain plays a crucial part in providing trust, integrity and transparency, which are key elements of blockchain technology. These elements assure the stakeholders that the provided knowledge is trustable and can be referred to by entities such as analyzers, patients, medical staff, etc., and encourage all aforementioned stakeholders to share their healthcare data by employing blockchain technology [29].

c: Neuroscience

Neural devices [27] are equipped with computing chips, sensitive sensors, and wireless communication and can detect the current mental state of a person with the help of the data in relation to their brain activity. These data can be used further to analyze the patterns of brain activity and translate them into commands for controlling external devices such as drones, robotic arms, smart appliances, etc. The analysis of the brain activity is based on the machine learning algorithms that are being fed with a huge amount of accurate and trustable data. Blockchain, in this application, can demonstrate its great potential by providing a fundamental infrastructure in which the brain data can be stored while its privacy, accuracy, and transparency are guaranteed [102].

D. SUPPLY CHAIN MANAGEMENT

In this subsection, we focus on two important supply chain management applications, including Pharmaceutical and Clinical Trials.

a: Pharmaceutical

In the pharmaceutical supply chain, medications pass many stages, including suppliers of raw materials, manufacturers, medical organizations, wholesalers, retailers, and patients. Blockchain enables managing such a complex and lengthy supply chain by ensuring transparency in the processes and procedures in those stages. In case of the need to recall medicines if any problem causes, blockchain can help the related authorities choose a proper reaction [103]. In [104], the authors suggested the Gcoin blockchain to make a secure, transparent, and consensus driven drug supply ecosystem. The Gcoin blockchain can track every medicine by its identification, and only one identification is assigned to every medicine. Hence, every drug can only be sold once from one address to another, preventing the double spending of drugs. Using the Gcoin blockchain system, the overall costs in the drug supply chain could be decreased due to the improvement of information exchange.

b: Clinical Trials

Since Blockchain allows for sharing, tracking, protecting data, it can impact clinical research globally. It is a step toward better transparency by improving trust among research communities and between patients and research communities [106]. The authors in [105] demonstrated that transparency of data management in clinical trials could be improved using the smart contracts running on the Ethereum blockchain. Smart contracts, in fact, can act as trusted administrators that enhance the transparency of data reporting in clinical trials by preventing all aspects of data from manipulation. These aspects of data include clinical measurements, trial registration, and subject registration.

E. INTERNET OF MEDICAL THINGS

Internet of Medical Things (IoMT) is the focus of study in our research review, and remote health monitoring is one of the major IoMT's applications. This subsection discusses remote health monitoring, emergency healthcare, wireless capsule endoscopy, telemedicine systems, and monitoring of aged patients. In the rest of this section, we briefly explain the security and privacy aspect of IoMT systems. Finally, in the literature review section, we discuss in detail all the relevant state-of-the-art works that fall under this category.

a: Remote Health Monitoring

One of the major and important building blocks of the modern healthcare system is IoMT [11]. The IoMT is a system of medical sensors and applications offering better and more healthcare services including the detection and prevention of diseases [34]. Researchers are gaining the benefit of wearable

sensors such as mosquito, conductivity, contact temperature sensors, etc. In order to enhance remote monitoring and to make an early and comprehensive diagnosis of chronic diseases. These sensors record useful body parameters such as heart rate (BPM), temperature, and breath acetone [7]. Remote health monitoring itself can be divided into several subcategories [34], including emergency healthcare, wireless capsule endoscopy, telemedicine systems, and monitoring of aged patients. These subcategories are introduced as follows:

- Emergency healthcare: Physicians can monitor emergency patients, for example, the ones with cardiovascular diseases, particularly heart attacks using intelligent sensors-based devices. These devices help doctors to provide efficient treatment remotely in an emergency [34], [108].
- Wireless capsule endoscopy: Wireless capsule endoscopy (WCE), which is a subset of Tele-monitoring, is an imaging system that benefits from a capsule-shaped tiny camera. This capsule presents the interior view of the patient's intestine through the high resolution and clear punctures sent by high-quality camera sensors [34], [109].
- Telemedicine systems: [34] Telemedicine is an IoMT emerging medical technology that provides quality healthcare services to remote locations. This technology enables a physician to diagnose a patient at any place and any time, so there is no need for patients to visit a doctor in person or to visit an emergency room [110], [111].
- Monitoring of aged patients: Healthcare and monitoring of the aged patients has become the latest research problem that needs further investigation. Elderly people suffering from Alzheimer's Disease (AD), dementia, linguistic impairment, hearing disorders, or other health problems require a health-monitoring system. IoMT provides the aged patients with real-time and accurate monitoring using the sensors and wearable devices attached to patients' body. These sensors send information to the corresponding healthcare centers, and then the IoMT-based healthcare monitoring applications located in these centers help aged individuals to receive information about their health status. The elderly patients are able to receive services provided by the centers from the comfort of their homes [34], [38], [107].

b: IoMT Security and Privacy

In this subsection, we provide a brief overview of the security and privacy aspects of IoMT systems. Authors in [7] have reviewed the challenges of IoT healthcare devices using the data collected from 35 peer-reviewed articles. This paper identified various IoMT challenges, including security and privacy issues, network issues, data issues, hardware and software issues, etc. They found that the security and privacy issue is by far the most serious and significant challenge among other challenges. The authors reached the conclusion that healthcare manufacturers and information security specialists should provide integrity and confidentiality of the users' information. The research review [11] conducted extensive research by reviewing 30 articles regarding healthcare security and privacy issues. The authors compared different types of security threats to each other using a bar chart. These threats include abuse of services, collusion, data breaches, data tampering, data theft, etc. The authors concluded that IoMT applications are threatened mainly through unauthorized access and data breaches. They also mentioned that impersonations and data tampering are the subsequent serious threats that jeopardize IoMT applications' security and privacy. They recommend that further study with more focus on access control is needed. The survey [39] presented different levels for healthcare systems and then discussed the security and privacy for each level individually.

- Data level: This level is discussed in the context of the General Data Protection Regulation (GDPR) [64] and the Health Insurance Portability and Accountability Act (HIPAA) [39]. This level itself consists of three different aspects: confidentiality, integrity, and availability. Regarding confidentiality, collection, storage, and exchange of patient's data must comply with regulations such as GDPR and HIPPA. With regard to integrity, article 5(d) of the GDPR says that the data of patients should be kept accurate and up to date. Based on article 32 of the GDPR, security measures should be adapted so that patients can get access to their data on time.
- Sensor level: The security methods employed in this level are needed to be lightweight in terms of computation and communication. Sensors are required to be tamper-proof so that an attacker cannot reprogram the IoMT devices. Additionally, a real-time intrusion detection mechanism should be provided for sensors to leave and rejoin the environment where patients are located. Sensors should be capable of self-healing, i.e., recover themselves after being attacked in a network. Over-the-air programming can be used for self-healing mechanisms, i.e., updating security policies for the network to prevent attacks by malicious users. Finally, mechanisms must be used for users joining and leaving a network. Previous messages cannot be read by the newly joined users, while the future data must not be read by the users leaving the network.
- Personal server level: Before sending the health data to the medical server, it is generally stored in the personal server (i.e., a smartphone). The personal server must establish a secure channel between itself and an IoMT device. Moreover, the patient health data stored on the personal server should be accessed by the medical staff, patients and legitimate users; thus effective authentication methods such as lightweight identity authentication proposed in [116] are required in this respect.
- Medical server level: For getting access to the patients' data, effective access control methods should be developed. These methods should be capable of updating the

policy sets effectively. An effective Key management mechanism for key distribution in IoMT applications is vital. These mechanisms generally make use of symmetric key cryptography as they are more appropriate for resource-constrained IoMT devices.

The authors in [39] refer to blockchain technology as a future research direction. They state that blockchain can provide privacy protection and strong security to the IoMT healthcare systems and exemplify MedRec [98] for securing EHRs, permission management, and medical data access.

In [21], the authors state that the lack of security awareness among patients, doctors, medical staff, etc., can make an IoMT system vulnerable to potential attacks which cause actual bodily harm and threaten the patients' lives. The authors, hence, developed an IoMT Security Assessment Framework called IoMT-SAF, which is web-based and covers necessary security measures by recommending a detailed list of assessment attributes, i.e., 260 questions. These questions or attributes are grouped in different categories, including web security, software security, privacy, physical security attributes, etc. This helps IoMT adopters to enforce security based on their security goals which differ depending on the scenario. The survey [8] discusses the security and privacy challenges that include five different aspects: data encryption, access control, trusted third party auditing, data search, and data anonymization, which are explained in the following.

Data encryption: Since nodes like sensors in IoMT applications have limited resources, it is important to use lightweight cryptographic algorithms to provide confidentiality without sacrificing real-time and continuous remote monitoring. In addition, key management protocols play a major part in such applications.

Access control: By defining intended policies, only authorized entities like patients, doctors and medical staff can get access to their corresponding resources and unauthorized users prevent accessing data that is not related to them. The authors mentioned three kinds of encryption methods that are used in access control: attribute-based encryption, symmetric key encryption, and asymmetric key encryption.

Trusted third party: IoMT applications that tend to store health information to the cloud are vulnerable to data corruption since cloud servers are generally not fully trusted. Supervised machine learning methods, including support vector machine, and logistic regression as well as unsupervised approaches enable the accountability of the service providers.

Data search: Typically, before outsourcing the sensitive healthcare data to the cloud server, they must be encrypted to provide the users' privacy. Thus, users can make use of different methods to search over encrypted data. These methods include searchable symmetric encryption and public-key encryption with keyword search.

Data anonymization: Patient's sensitive healthcare information can be categorized as follows: (i) Explicit identifiers: These identifiers such as a name, ID number, and phone number show a patient, (ii) Quasi-identifiers: The identifiers like birth data, address, and age can indicate a patient uniquely and (iii) Privacy attributes: These attributes refer to the sensitive information of patients including income and illness.

The authors in [8], introduced data anonymous method, and random perturbation approach such as k-anonymity, l-diversity, etc., to overcome these challenges. In [37], the authors presented a taxonomy of the security and privacy challenges to promote awareness among stakeholders so that they can identify the potential attacks in IoMT applications. In this research study, the authors cataloged the security and privacy issues in such applications based on the following taxonomies:

- IoMT Layers: The authors in [37] introduced a five-layered architecture consisting of perception, network, middleware, application, and business. The perception layer acquires data, e.g., heart rate, oxygen level, etc., via equipment such as wearable, implantable, ambient, and stationary devices. Side-channel, tag cloning, tampering devices, etc., are the potential attacks for this layer. The network layer is responsible for the delivery, discovery, and routing of the content toward the destination. Various types of potential attacks which are concerned with this layer include eavesdropping, replay, man-in-the-middle, rogue access, denial of service, and sinkhole. The control of filtering and collecting the received data from devices such as sensors and providing access control is related to the middleware layer. Cross-Site request forgery, session hijacking, and cross-site scripting fall into this layer. The application layer provides users with an interface where users connect to the IoMT devices. SQL injection, Account hijacking, Ransomware, etc., are the potential attacks that belong to this layer. The business layer is responsible for obtaining knowledge from the collected IoMT data. Attacks in this layer might cause information disclosure, deception, etc.
- Intruder Type: It indicates the attackers'capabilities with regard to resources and skills needed to perform attacks.
- Compromise Level: This category identifies which part of the IoMT environment (i.e., user, system/application, hardware) has been violated.
- Attack Impact: Attack impact indicates how important the risk of an attack is.
- Attack Method: Attack method catalogs IoMT attacks regarding the methods used to penetrate a system.
- CIA Compromise: This categorizes attacks in relation to the CIA components, i.e., confidentiality, integrity, and availability.
- Attack Origin: Based on the starting point, attacks can be cataloged.
- Attack Level: It includes passive attacks in which an attacker performs an attack for launching active attacks on the system. Active attacks compromise the system using the information collected from passive attacks.
- Attack Difficulty: This categorizes attacks on an IoMT

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3117662, IEEE Access

application based on how difficult the attacks are.

V. BLOCKCHAIN-BASED IOMT

The methodology subsection explained four categories of healthcare applications, namely healthcare management, healthcare big data, supply chain management, and IoMT applications. In this section, we focus on blockchain-based IoMT applications and elaborate on them.

The authors in [40], first describe the blockchain, its advantages and applications, and then elaborates on different protocols, namely InterPlanetary File System (IPFS), IoT, Message Queuing Telemetry Transport (MQTT), and REST. IPFS, a peer-to-peer network, is a hypermedia distributed protocol that provides a method for sharing and storing files. The hash of the stored files is generated using cryptography and will be used for the identification of files. MQTT is a lightweight, Publish/Subscribe protocol, open-source protocol for connecting the resource-limited objects in IoT. MQTT is lightweight because it reduces the number of messages sent to the Internet by means of a server named broker. REpresentational State Transfer (REST) is an alternative to the XML-based SOAP (Simple Object Access Protocol). SOAP is a messing protocol for exchanging information among the nodes. REST is more lightweight, simpler, and easier to use compared to SOAP. The authors in [40] state that Server/Client-based IoT applications are a single point of failure; security in this model is lax since the health data might be modified maliciously and also the communications between the nodes are not secure. Hence, the authors presented a model for medical applications via IoT, IPFS, MQTT, REST and blockchain technology to overcome the aforementioned failure. However, the proposed model is not efficient compared to the Server/Client model in terms of energy and response time. In fact, mining data is an intensive resource-consuming process, and in the proposed model, it takes the IoMT devices a little more time to perform their tasks than that in the Server/Client model.

In [41], for the Dyslexia diagnosis and treatment purpose, a new framework based on the blockchain and IoT has been presented. The patinas securely send their movements of eye, hand, and stylus using the smartphone to a nearby MEC node, which makes use of auto-grading algorithms in order to detect dyslexic patterns. To do so, these algorithms analyze the multimedia (eye tracking, audio, video, and text) IoT data received by the patients and save the result in blockchain and off-chain in which the information is stored outside of the blockchain. The data stored on the blockchain can further be shared with medical practitioners for the purpose of manual analysis. These data are also helpful for quality assurance, statistical analysis, and clinical research. This framework ensures the security and anonymity of the patients diagnosed as dyslexic. The authors intend to propose solutions to decrease the delay of sending the multimedia data as future work.

The research study [42] states that insider attacks can pose serious threats to an IoMT and a medical smartphone network (MSN). Users who are using smartphones in healthcare organizations constitute an MSN, which is a type of IoMT. Smartphones provide patients with user-friendly applications to inform doctors about their health conditions and also manage their data, reduce cost, etc. An insider attacker can compromise a node in MSN and then from this node can launch other attacks such as scanning, spoofing attack, etc. The authors of [42], in their prior research [117], designed a model that benefited from Bayesian inference [118] to detect untrustworthy nodes in an MSN and used intrusion detection systems (IDS) to defeat insider attacks. They also adopted a central server for trust computation and decision making. The authors in [42] presented a two-layer architecture (MSN layer, Chain layer) which is based on their previous published work [119]. The MSN layer is based on their previous work for communication between nodes and the central server, so there is no need for designing a new infrastructure that can cost a fortune. In fact, the new approach can take advantage of the existing old infrastructure in health organizations. The Chain layer is a consortium blockchain in which users can upload features of malicious or unwanted packets. The authors claim that using this scheme, firstly, user can quickly upload their blacklist by checking the blockchain, and secondly, more powerful users in MSNs can examine their traffic status with a potentially abnormal user. However, the authors state that their scheme has several drawbacks; for instance, it is not resistant to external attacks such as Denial-of-service (DoS), or their scheme suffers from intensive resource-consuming of blockchain. They also mention that the central server could be the target of attackers. In work [120], the authors also mentioned that using Consortium Blockchain can provide higher scalability and transaction privacy. However, this work also lacks a literature review and does not propose any mitigation for the scalability limitations.

The work [43] introduced an architecture called BIoMT to provide security and privacy. The authors state that their proposed framework has lower overhead in terms of power consumption and network communications. Their architecture consists of the following layers:

- Device layer: Devices such as sensors, wearables devices, smartphones, etc., constitutes this layer. These devices gather information from users who are inside or outside a medical facility. Two schemes are combined in this layer for a key establishment mechanism: Elliptic Curve Cryptography (ECC) and identity-based credential (IBC). Transactions are encrypted with the help of ECC. In this work, a key establishment mechanism for IoMT devices is provided by combining ECC and IBC.
- Facility layer: It contains the bolster that is responsible for managing the IoMT devices.The bolster includes two elements: (i) local blockchain, which provides the authorized users with adding/removing devices via creating/deleting transactions. (ii) Local storage where users' data can be stored. This layer also runs different types of algorithms.

- Cloud layer: This layer offers support such as storage and computational to the cluster layer.
- Cluster layer: It includes several entities such as cloud servers, service providers, and medical facilities.

The authors of [43], with the help of the AVISPA tool, checked the security of their framework against different attacks such as inventory, replay, and man-in-the-middle, and they also described how their framework provides fundamental security features, including authentication, confidentiality, integrity, availability, and user control. The authors evaluated the performance, such as end-to-end delay and energy consumption, but they did not describe the methods used for this evaluation. They also did not describe in detail how they performed the security analysis.

In [44], the authors mentioned that the cloud servers are not fully honest as they can modify or remove patients' health data. They state that blockchain-based IoMT is superior to cloud-based IoMT in terms of security and privacy. Blockchain, in fact, provides the transparency and auditability security features that are key factors in IoMT applications. The authors, hence, took advantage of blockchain technology and made a contribution by proposing two algorithms to provide integrity, authenticity, and confidentiality in an IoMT application. The first algorithm fetches a patient's EHRs from a database, and the second algorithm attaches the obtained EHRs to a block and next adds the resulted block to the blockchain. To add the block, medical practitioners must make a connection to the blockchain. However, their scheme suffers from large-size EHRs that cannot be fitted to the block of a public blockchain. The authors suggest that to address this problem, an off-chain approach could be adopted. In this approach, the huge amount of health data is stored in a traditional database instead of in a block of the blockchain, and only the hash of the health data will be stored in the blockchain for users' authentication.

In [22], the authors pointed out that combining blockchain and IoT has two major challenges: (i) Network overhead: This is caused by adding a block to the blockchain as well as broadcasting the transactions to all the miners in a network. The miners, in fact, first check the validity of the new transactions and then add them to the blockchain. (ii) Low throughput: considering the scale of IoT applications, the number of transactions that can be stored on the blockchain is limited. In this study, the authors presented a blockchain-based access control architecture. Blockchain is used for storing the hash of patients' data and patients' access policies as well. They improved the efficiency of the blockchain in the context of IoMT as follows: (i) To reduce the data redundancy, miners are clustered, and to reduce the network overhead, the size of the transaction is reduced. (ii) To provide security and privacy, the patients' data are stored in a location that is close to them. The authors benefited from Practical Byzantine Fault Tolerance (PBFT) [121] to reduce network cost in terms of processing and bandwidth and to enhance network efficiency and security. In this architecture, users can define access policies for their data. To do so, users send their policies to miners of a cluster in the form of a transaction. They finally analyzed the security of their scheme against several attacks, including appending, Dos, distributed DoS, modification attack, public Blockchain modification, 51% attack. However, the authors did not perform any experiments to evaluate the performance of their architecture.

In [31], the authors proposed a comprehensive approach for the integration of the blockchain and the healthcare domain. They aimed at overcoming the current blockchain's limitations and drawbacks. Their approach tries to consider the issues of security, privacy, scalability, interoperability, and regularity. This approach will help designers find the answers to the following questions when designing a blockchain-based healthcare system:

- How to provide access control for the authenticated entities to get access to their related health data, and meanwhile preserving the patient's privacy.
- How to guarantee the security of the patients interacting with the system.
- How to lift the sanctions imposed by the regulatories and how to ensure the ethical use of health data.
- How to get access to different types of data from several healthcare institutions with the help of a single system.

The authors used a permissioned blockchain that provides access control for specific authenticated users. Not only does the permissioned blockchain improve the security and network performance, but also it reduces the cost and process for the parties who are not taking part in the mining process. Ellipticcurve cryptography (ECC) [122], in this approach, is used to ensure security. This algorithm consumes less processing and provides high-speed transfer of data due to the shorter size of the key. The QuorumChain [123] consensus algorithm is employed in this approach, which works based on the majority voting. In the case that IoT devices participate in a network, the authors recommended the PBFT as a consensus algorithm since it reduces the energy consumption for resource-constrained IoT devices. However, although the PBFT algorithm can converge fast and efficiently, it suffers from the scalability issue, i.e., only a limited number of IoT devices can participate in this consensus algorithm.

A blockchain-based IoMT model is proposed in [45] that consists of five important segments: the Blockchain Network, Cloud Storage, Healthcare Providers, Smart Contracts and Patients. The authors used remote patient monitoring as a scenario to present their idea. To reduce the delay as well as the network overhead, clusters, a group of nodes, are used in this model. The authors pointed out that combining the blockchain and IoT has several issues that are discussed in the following:

- Resource limitations: The process of mining in the blockchain is resource-intensive both computationally and in terms of memory storage, which is in contrast to IoMT devices with limited resources.
- Bandwidth limitations: For transaction validation, many massages must be broadcast by nodes in the blockchain,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3117662, IEEE Access

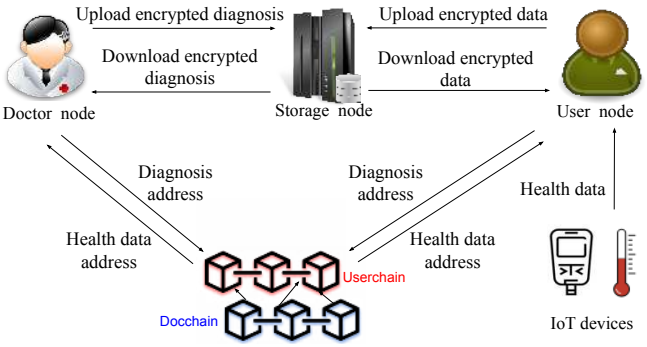

FIGURE 7. Healthchain system model proposed in [46].

while IoMT devices have limited bandwidth.

- Connectivity limitations: Devices in the blockchain must always connect to the blockchain and participate in the predefined protocol. This makes an IoMT device vulnerable to security attacks.
- Memory limitations: Storing all the health information sent by all the nodes in the network is a serious challenge regarding IoMT devices with limited storage capacity.

To address the memory limitations, wearable devices do not always send health information to the network with the help of smart contracts. A smart contract permits a user to run a script in a blockchain in a verifiable way without a trusted party. In this model, a smart contract decides when to send the relevant information of a patient to the network. Even by using smart contracts, a user can grant/deny permission to access their own information. In the proposed model, for example, when the glucose level of a patient reaches a threshold, a pre-defined smart contract will send the relevant data along with an alert to the network. If a healthcare organization like a hospital requires a patient's alert, the smart contract will send the alert to the cloud server, and simultaneously the hash of the data will be saved on the blockchain.

In [46], the authors proposed a Blockchain-based smart healthcare system called "Healthchain" that provides patients with storing their large-scale health data securely on the storage. The Healthchain proposed in [46] is comprised of five different layers, including data, network, consensus, incentive and application layers. Figure 7 demonstrates the components of Healthchain, which are as follows.

- IoT devices: These devices do not interact directly with the blockchain, and each device is associated exactly with only one user node.
- User nodes: Each user node collects health data from one or more IoT devices, which encrypts the data and sends it to a storage node. User nodes with higher computation power are involved in the mining process.
- Doctor nodes: A doctor can be a real doctor or an analyzer that is based on AI. Doctor nodes make a diagnosis based on the health data received from IoT devices.
- Accounting node: The consortium deploys the accounting node. This node is responsible for validating the doctors' transactions.
- Storage nodes: These nodes jointly store encrypted patients' health data and encrypted doctors' diagnosis distributively. Each storage node is based on IPFS, which enables storing a huge amount of data in a distributed manner with high efficiency.
- Userchain: It is a public blockchain that anyone can join in order to read and send transactions. A series of Ublocks constitute the Userchain that functions based on Proof of Work.
- Docchain: It is a consortium blockchain consisting of Dblocks for publishing doctors' diagnosis. Diagnosis transactions can only be generated by legitimate doctors. These transactions can be added to this blockchain by accounting nodes using the PBFT consensus algorithm.

The authors aimed to achieve the following design goals: the process of a high volume of data of large-scale IoT devices, patients' health data and doctors' diagnosis should be uploaded in time, no adversary should be able to get access to user's sensitive health data, a mechanism should be provided to audit whether the doctors' diagnosis is tampered with, and at any time a user should deny the right of a doctor to get access to their health data. The authors performed security analysis to ensure the design goals and finally carried out a performance evaluation. However, the authors did not focus on how to share and evaluate the EMRs transmitting processes. To this end, the authors in [124] proposed a novel EMRs data management and trading system, also called "Healthchain" based on consortium blockchain technology. The authors proposed a blockchain-based system in which patients can access EMRs in different organizations, and the EMRs can be traded among other users easily. In [125], the authors proposed a blockchain-based healthcare data management system again called "HealthChain." This system is based on two kinds of blockchains: i) Private Blockchain: for intra-regional communication and, ii) Consortium Blockchain: for inter-regional communication. The authors claimed their proposed system provides a secure healthcare record management system with scalability and low storage space.

The authors in [47] described a fine-grained authorization framework that is based on smart contracts and blockchain, whose main goal is to control the access of users to medical data and devices. The private blockchain ecosystem is authenticated by a proof-of-medical-stake consensus mechanism [126] that is suitable for medical applications.

The authors in [48] introduced a model to provide security and privacy to a remote monitoring system. To this end, they benefited from different cryptographic techniques, including ARX encryption scheme [127], ring signatures [128], and Diffie-Hellman key exchange [129]. The proposed model includes the following layers:

- Overlay network: This network contains different devices such as a tablet, computer, smartphone, etc. The overlay network is grouped into many clusters in order to prevent delay and to increase network scalability. Each cluster consists of one cluster head which is a unique public key.
- Cloud storage: Patients' health data are stored in the cloud servers in place of the blockchain. The health data is encrypted with the user's public key and then will be stored in identical blocks with a unique block number.
- Healthcare provider: As soon as the health providers receive an alert from a network, they provide the patient with medical treatment. The patient themselves are able to give and revoke data access from entities such as an insurance company or medical staff.
- Smart contracts: Using smart contracts, a condition in relation to a patient can be set. For example, when the blood pressure reaches a defined threshold, an alert will be sent to a legitimate entity or healthcare provider. The smart contract will also save the alert over a cloud server so that authorized entities get access to it later.
- Patient equipped with IoT devices: The patients send their health information to devices like a tablet or smartphone for formatting purposes. Later, the information, including one or more parameters such as blood pressure will be sent to the corresponding smart contract to check whether the received parameters meet the threshold values or not.

The proposed model uses a type of lightweight symmetric algorithm named ARX to provide confidentiality for patients' data. The model also supports authentication by means of a digital signature. A ring signature is used, which allows to signer data anonymously. This model, however, lacks security and performance evaluation, which the authors consider as future work.

In [49], an access control model named MDPAC for the purpose of security is proposed. This model enables legitimate entities to get access to health data and guarantees communication among patients and doctors in a private, secure, and efficient manner. This model, in fact, gives permission to the administrators to assign users to the roles, permissions to the roles, and accordingly the actions to resources and objects. This access control model operates based on the Role-based access control (RBAC) model and enables the patients to access the health data by means of the IoT. The authors evaluated their work and claim that their model is more efficient in terms of running time compared to the state-of-the-art algorithms.

The authors in [50] described the typical scenarios of medical image retrieval based on blockchain for providing privacy, including privacy disclosure, data tampering, and data forgery, and then they explained various requirements of medical image retrieval.

- privacy protection: As medical images are sensitive, the identification of the patients should not be revealed.
- scalability: The system should support the rapid growth of the participants involving in the system.
- reliability: The image data should always be available and protected from being deleted or tampered with.

The authors in this paper presented a layered model which includes the following layers:

- Application layer: In this layer, suitable scenarios can be expanded to data modeling in the future.
- Service layer: This layer provides key functionalities of similarity measurement and image retrieval based on the publicly encrypted image features.
- Transaction layer: This layer includes three main components, namely image feature extraction, image feature encryption, and transaction generation.
- Physical layer: Various roles are defined in this layer, namely hospital, third party, regulatory authority, image retrieval service, and miner.

Finally, the authors evaluated their model, which shows it guarantees the privacy and it is resistant to potential threats. They also evaluated their model in terms of performance.

The authors in [51] introduced a preliminary model by employing a newly designed protocol named GHOSTDAG that benefits from smart contracts in order to monitor patients remotely. GHOSTDAG, which is introduced in [130]. is recognized by its both throughput and security. This protocol made use of a directed acyclic graph (DAG). The components of the GHOSTDAG model presented in 8 are as follows.

- Patient: Patients can grant access to their desired entity to receive medical treatment. Patients are able to revoke access or even set a time for giving and revoking access.
- Hospitals: These institutions can ask a patient to grant access to his/her medical history and health data. These institutions can provide medical treatment upon receiving an alert from a smart device attached to a patient.
- RPM devices: These devices send health information collected from a patient to a smart device such as a smartphone.
- GHOSTDAG blockchain: The model proposed in [51] benefits from a private and a public blockchain that is based on GHOSTDAG. The private blockchain stores the alerts that are issued by smart contracts.
- Authorized entities: A patient is able to share his/her health data with stakeholders such as insurance companies, family members, etc.

The authors stated that their model needs a simulation environment to measure the performance of the protocol. Additionally, their model requires mathematical methods to ensure the security of the protocol.

The research work [52] presented an architecture for the purpose of automatic assessment and real-time estimation of neurological disorders. This architecture profits from the blockchain to share the patients' data with healthcare providers, including treating physicians and doctors. This architecture includes three key parts as follows:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3117662, IEEE Access

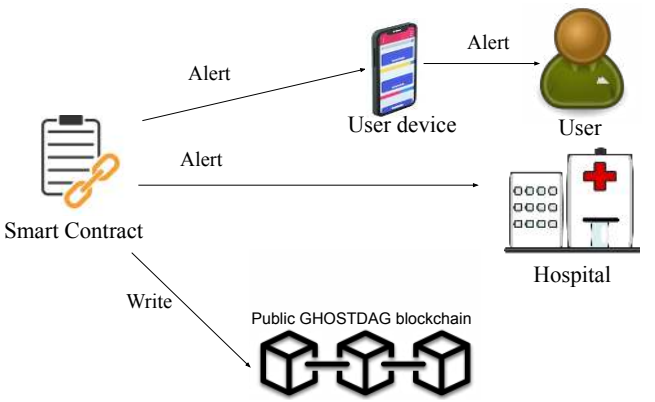

FIGURE 8. GHOSTDAG system model.

- Wearable sensor device: This part benefits from a sensor network that records the complex movements of patients' body with the help of a tri-axial gyroscope and tri-axial accelerometer.
- Mobile gateway: Before sending the data collected by the sensors to the cloud server, they are stored temporarily in the gateway. An Android phone is used as a mobile gateway that provides a real-time visualization.
- Cloud server: The Amazon Web Services (AWS) is used as the main cloud platform. It consists of different cloud services, including AWS IoT, Amazon Elastic Compute Cloud, AWS Lambda, and AWS Simple Storage Service. This platform has shown its potential in the context of healthcare.

The authors employed the Ethereum blockchain platform for the sake of data sharing and access control (using smart contracts) as well. They evaluated the performance of their proposed system in terms of record data, process data, view historical data, and data sharing. The authors claimed that the integration of their system with blockchain brings flexibility, availability, low-cost service, and reliability.

The paper [47], introduced a novel EHRs sharing architecture with the help of blockchain and IPFS for a healthcare system. In order to enhance the security of EHRs sharing, they employed smart contracts that provide a trustworthy access control mechanism. The proposed system is based on a mobile cloud platform in which the patients' data are collected from a set of local gateways. These data, then, are stored on a cloud for the purpose of data sharing with healthcare providers. The EHRs also can be gathered from wearable body sensors with the help of a mobile application on the patients' smartphone. They have also proposed a cloud blockchain network for the sake of data sharing. This blockchain is based on Ethereum and its main components are as follows:

- EHRs manager: This component controls the transactions of all the users on the blockchain network, thus playing a crucial role in data sharing framework.
- Admin: The operations and transactions on the cloud are managed by this component and it is responsible for adding, revoking, and changing access permissions.
- Smart contracts: It is deemed to be core software in the proposed healthcare platform. Users by means of the contract address can interact with smart contracts. Smart contracts define access control using all legitimate operations.
- Decentralized storage: The IPFS provides a decentralized peer-to-peer file system to provide a file sharing platform in the blockchain network. Users can store their data on distributed storage nodes to avoid a single point of failure. In the proposed architecture, the health data are encrypted and then stored in IPFS nodes.

The design goals of the proposed architecture are as follows:

- Only authorized users should be authenticated by the system and get access to EHRs.
- The system should provide lightweight access control using smart contracts to prevent high network latency and to support fast data access.
- The system should support the following features: system integrity, high security levels, data privacy and flexibility to mobile users.

The authors finally evaluated their system in terms of network overheads and access control.

The authors in [57] introduced a blockchain-based architecture to overcome the drawbacks concerning the blockchain-based and cloud-centric IoMT healthcare systems. These drawbacks include high latency, high storage cost and single point of failure. Additionally, the presented model in [57] provides security, privacy, traceability, availability, and anonymity features. Data security and privacy is achieved by the selective ring based access control (SRAC) and other cryptography methods. The model benefits from smart contracts to automate medical alerting and services. The proposed model includes the following three layers:

- Data producer: This layer is responsible for patient's device registration. It then sends the patients' encrypted data to the respective edge computer. Employing edge devices as a proxy makes the scheme suitable for constrained devices.
- Hybrid computing: This layer consists of several components: Distributed Data Storage System (DDSS), blockchain management, cloud computing, edge computing, and access control. This distributed computing layer offers data processing and analysis followed by decision making.
- Data consumer:This layer includes actuators, service provider terminals, emergency alerting systems, and more. Nodes act according to the decisions received from the middle layer.

Finally, they have analyzed their models which reveals that it meets the security and privacy requirements. Besides, the experimental analysis shows that the proposed model

needs less storage and the response time is in the order of milliseconds.

To address the problems of the current IoMT systems, such as centralization of patient sensitive information, the paper [58] presented a distributed framework based on the blockchain and IPFS technology to handle the issues. The IPFS cluster node not only ensures the security and authentication of the IoMT devices but also provides secure storage management. The presented model includes two main parts: i) patients and medical devices are authenticated and authorized and ii) to guarantee the privacy of the patient sensitive information, data are stored in a blockchain. This framework has three types of communications, including i) medical-device-to-IPFS cluster node communication, which is responsible for registering the patients and their medical devices and authenticating the medical devices, ii) IPFS cluster node-to-smart contracts communication, which offers authentication and authorization of the medical devices also their data mapping for ensuring privacy in the blockchain network, and iii) smart contracts-to-blockchain network communication, which disseminates the information into the blockchain network after authentication and authorization. The authors informally proved that their proposed model is secure against various attacks, including spoof attack, Sybil attack, replay attack. They also evaluated their work in terms of execution time and gas consumption and demonstrated that their framework is efficient in terms of security and privacy. This evaluation is carried out in an Ethereum Ropsten network with 25 peers. Although the introduced model has several advantages, including a decentralized system, a registration-based security model, and access control, it takes more computational time to maintain more devices and building a distributed cluster. Hence, the authors plan to extend their model so as to support a large number of agents (peers).

The authors in [54] presented BAKMP-IoMT, with the help of blockchain which provides authentication key agreement protocol for IoMT environment. This secure key agreement protocol is between implantable medical devices and personal servers and between personal servers and cloud servers. The authors proved the security of their model formally and informally. For the formal security verification, they used an accepted automated software validation tool called AVISPA. They demonstrated that their proposed protocol is secure against various attacks such as replay attack, man-in-the-middle attack, impersonation attack and showed that BAKMP-IoMT provides two important security features: anonymity and untraceability. However, this work lacks the scalability property. BAKMP-IoMT is compared with other similar work, which shows that it has less communication and communication overhead concerning the authentication and key management phase, and it performs better in terms of security and functionality features.

Authors in [55] discussed that the IoMT devices could be used to collect massive medical and healthcare data for diagnosing and identifying COVID-19. Hence, the paper aims at the integration of blockchain and IoMT to handle the COVID-19 crisis. In this paper, to tackle the COVID-19 crisis, several solutions provided by blockchain-enabled IoMT are presented: tracing the pandemic origin, quarantining and social distancing, smart hospital, medical data provenance, and remote healthcare and telemedicine. These solutions benefit from various IoMT devices, including heat sensors, nucleic acid test, wristband sensor, tags, and Wearable body sensors. The provided solutions also take advantage of blockchain technology to provide traceability, immutability, privacy protection, and authentication.

The paper [56] took advantage of blockchain, AI, and privacy-preserving federated learning framework in the context of IoMT. Federated learning is a machine learning approach where the final goal is to learn a centralized model while training data are stored on remote devices such as IoMT devices or hospitals [131]. The architecture consists of several parts, including the global model: this model is offered by a medical center or a company and it is a prebuilt machine learning model, local model: this model is trained on a local medical device, IoT medical devices, and the blockchain. Then, the proposed architecture is evaluated using medical images data.

Also, the paper [59] proposed a novel blockchain-based deep learning for secure image transmission. This scheme uses a deep belief network (DBN) algorithm for the classification process to diagnose the existence of the disease in the IoMT environment. In general, the scheme includes data collection, secure transaction, hash value encryption, and data classification. As mentioned in Figure 9 in this scheme, first, IoT gadgets collect the patient details, then the hybridization of grasshopper with fruit fly optimization (GOFFO) algorithm with ECC is used for secret image transmission. In this scheme, the authors encrypt and compress the hash values in blockchain employing the Neighborhood Indexing Sequence with Burrow Wheeler Transform (NISBWT) technique. Finally, the DBN model is used for the classification process. The performance evaluation of the model, along with the sensitivity, specificity and accuracy are also discussed in [59].

In [132], the authors proposed a novel blockchain-based data management framework called BSDMF for the secure exchange of patient data in IoMT systems. They claimed that BSDMF could enhance scalability. The experimental results of their proposed framework achieved a high accuracy ratio and less response time compared to other popular methods. However, they had a maximum of 100 IoT nodes in their experiments, with this limited number of nodes it cannot be concluded that the scheme is scalable. Moreover, the authors considered only the response time factor to conclude that their scheme is scalable, which is also not enough and they should take other factors to account (cf. Section VII). In [133], the authors also proposed a blockchain-based authentication scheme dedicated to IoMT devices. Their proposed authentication scheme was implemented on Ethereum. The authors evaluated their scheme regarding its computation

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3117662, IEEE Access

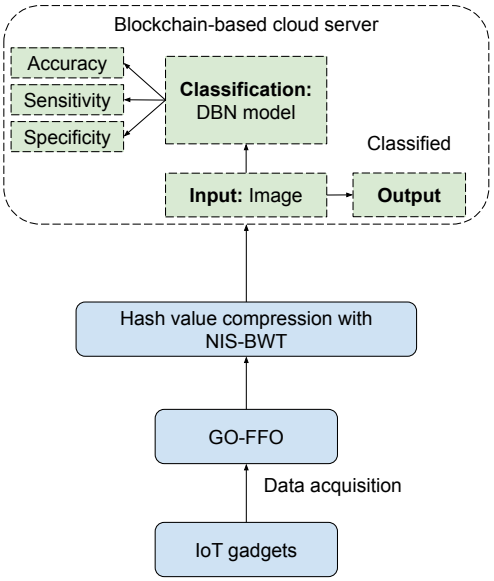

FIGURE 9. Architecture of the scheme proposed in [59].

and communication costs, and they also formally proved the scheme's security using the ProVerif tool. The authors claimed that their scheme is also scalable just because it is based on the proof of authority (PoA) consensus mechanism. However, we will explain later that several dimensions can directly or indirectly affect the scalability of the blockchain (cf. Figure 10).

VI. ANALYSIS OF DATA, RESULTS AND RESEARCH GAP

This section summarizes all the studies discussed in Section V in Table 3 regarding the following attributes.

- Year: This column shows the year when the paper is published.
- Authors: The name of the first author is shown in this column.
- Focus of study: The main aim and focus of the paper discussed in the Section V is given in this column.
- AI: This attribute shows that the review study has used AI in their system.
- Benefits: The main benefits of the discussed model or architecture in the paper is shown under this attribute.
- Problems and challenges: The research gap, problems, and challenges of the papers are shown in this column.
- Evaluation: It shows whether or not the model presented in the papers is evaluated in terms of the performance, communication or computation overhead, storage, etc.

Based on the review of the papers discussed in Section V and the analysis of the data shown in Table 3, we conclude the following results:

The main focus of almost all the studies [22], [31], [40]–[44], [48]–[51], [53]–[58], [133] is relevant to security and privacy, whereas the works [45], [47], [52], [59], [132] only focused on the security, not the privacy, issues.

Although all the works summarized in Table 3 inherit the benefits of the blockchain technology; however, commonly, the studies [22], [41], [54] discussed mainly the anonymity property in blockchain-based IoMT applications.

In terms of the benefits of the models summarized in Table 3, apart from the security and privacy issues, several studies considered access control which is an important feature in blockchain-based IoMT systems. These studies are as follows: [22], [45], [57], [58]. The papers [43], [47]–[49], [52], [53] also considered the access control property, although this property is not the main focus of these studies.

The authors in the papers [22], [40], [41], [44], [55] took into account the immutability property of the blockchain, and confidentiality is mainly discussed in works [40], [43], [44]. A few of the research works considered artificial intelligence [56], [59].

Analysis of the data presented in the column problems and challenges of Table 3 confirms a substantial gap in all the papers, which is the negligence of scalability of the blockchain regarding IoMT applications. Although the paper [51] considered the scalability factor, it is not the main focus of the study, and, additionally, the proposed scheme is not evaluated by the authors.

What is also worth mentioning is the metrics to benchmark the blockchain usage model. There are several benchmarking tools for performance analysis of blockchain platforms, such as BlockBench [134], Hyperledger Caliper [135], DAGbench [136], BCTMark [137] and BBB [138], [139]. However, only BlockBench and DAGbench provide scalability metrics [140]. BlockBench is developed to evaluate the performance of private blockchain-based systems. In [134], the authors use BlockBench to analyze the performance of private blockchain platforms such as Ethereum, Parity, Fabric, and Quorum. DAGbench is a framework for benchmarking a DAG DLTs like IOTA [136].

A. RESEARCH GAP

Scalability is one of the significant problems that current blockchain-based IoMT applications face, causing slow transaction validation, high transaction fees, high storage memory requirements, and long synchronization times [17], [26]. Hence, scalability is an essential factor that needs more research and direction. To this end, in the rest, we will explain different approaches to design scalable blockchain-based IoMT systems. As an example, we will discuss that it is essential for a designer to sufficiently understand the dimensions that can directly or indirectly affect the scalability of blockchain, including the consensus algorithm, ledger structure, etc. Also, considering the two approaches, on-chain, and off-chain, will help designers use a blockchain structure that fits their desired application's objectives. Also, to distinguish the bottlenecks of the proposed scalable blockchain system, designers must consider benchmarking their proposal.

TABLE 3. Summary of review of blockchain-based IoMT literature

Num	Authors	Focus of study	AI	Benefits	Problems and challenges	Evaluation
1	Dey et al. 2017 [40]	Security, Privacy	No	Transparency, Tamper-proof ledger, Confidentiality	Scalability is not addressed, No access control, Resource-intensive, High response time	No
2	Rahman et al. 2018 [41]	Security, Privacy	No	Security, Anonymity, Tamper-proof ledger	Scalability is not addressed, No access control	Yes
3	Meng et al. 2019 [42]	Security, Privacy	No	Detection of malicious nodes	Scalability is not addressed, No access control, Resource-intensive, Vulnerable to DoS attack, Centralized server is vulnerable	Yes
4	Seliem et al. 2019 [43]	Security, Privacy	No	Lightweight, authentication, confidentiality,integrity, availability, and user control, security analysis	Scalability is not addressed, No detailed evaluation and no detailed security analysis	Yes
5	Dilawar et al. 2019 [44]	Security, Privacy	No	Confidentiality, authenticity, integrity, tamper-proof ledger	Scalability is not addressed, No access control, Storage Problem	No
6	Zubaydi et al. 2019 [31]	Review of consensus algorithms, Security, Performance	No	Low energy consumption, Authentication, Verification, Low-latency storage	Scalability is not addressed	No
7	Hossein et al. 2019 [22]	Security, Privacy, Access control	No	Access control, immutability, anonymity	Scalability is not addressed, PBFT is used	No
8	Dwivedi et al. 2019 [45]	Security	No	Privacy, Security	Scalability is not addressed	No
9	Xu et al. 2019 [46]	Security, Access control	No	Security, Access control, Privacy, Support Large data	Scalability is not addressed	Yes
10	Malamas et al. 2019 [47]	Security	No	Access control, Privacy	Scalability is not addressed	No
11	Srivastava et al. 2019 [48]	Security, Privacy	No	Security, Privacy, Access control	Scalability is not addressed	No
12	Habib et al. 2019 [49]	Security, Privacy	No	Access control, Privacy	Scalability is not addressed	Yes
13	Shen et al. 2019 [50]	Security, Privacy	No	Privacy	Scalability is not addressed	Yes
14	Srivastava et al. 2019 [51]	Security, Privacy	No	Security, high-throughput, reliable RPM system	No security analysis, No comparitive analysis	No
15	Nguyen et al. 2019 [52]	Security	No	Security, Access control, Availability, Reliability	Scalability is not addressed	Yes
16	Nguyen et al. 2019 [53]	Security, Privacy	No	Security, Privacy, Access control	Scalability is not addressed	Yes
17	NEHA et al. 2020 [54]	Security, Privacy	No	Security, Privacy, Anonymity, Untraceability	Scalability is not addressed	Yes
18	Hong-Ning et al. 2020 [55]	Security, Privacy	No	Security, Privacy, immutability, traceability	Scalability is not addressed	Yes
19	Dawid et al. 2020 [56]	Security, Privacy	No	Privacy and AI, federated learning	Scalability is not addressed	Yes
20	Egala et al. 2021 [57]	Security, Privacy, Access control	No	Security, Privacy, Access control, Low storage and Low response time	Scalability is not addressed	Yes
21	Randhir et al. 2021 [58]	Security, Privacy, Access control	No	Security, Privacy, Access control	Scalability is not addressed	Yes
22	Alqaralleh et al. 2021 [59]	Security	Yes	Security, Data classification	Scalability is not addressed	Yes
23	Abbas et al. 2021 [132]	Security	No	Security, High accuracy ratio, Less response time	Only the response time is intended for scalability	Yes
24	Akkaoui 2021 [133]	Security, Privacy	No	Security, Anonymity, Integrity	Only the consensus protocol is intended for scalability	Yes

VII. RESEARCH DIRECTIONS FOR SCALABILITY

In this section, different approaches and perspectives in relation to the design of a scalable blockchain system in the context of IoMT will be discussed. These approaches and views will aid us in finding a workable, effective solution for the research gap discussed before. In addition, this section will describe benchmarking of blockchain systems, which is essential for the experimental evaluation of any proposed models.

A. VARIOUS DIMENSIONS OF THE BLOCKCHAIN

In order to design a full-fledged scalable blockchain system, it is vital to carefully consider all aspects of such a system. Gaining a deep understanding of such aspects will help a designer decide whether or not to choose a specific feature for the intended system and decide how to carry out reasonable trade-offs. Furthermore, a full understanding of these aspects and trade-offs will help a designer not to sacrifice some important metrics such as security and performance metrics to achieve scalability. This can impact the quality of the overall system. These dimensions are suggested by academic literature and industrial products developing and using blockchain. In the following, we introduce dimensions that can directly or indirectly affect the scalability of blockchains (see Figure 10).

- Fundemental properties of blockchain: Five properties in [141] have been introduced: immutability, non-repudiation, integrity, transparency, and equal rights, which are as follows.
  - Immutability: The data stored on each block of the blockchain cannot be modified.
  - Integrity: If just one bit of the data stored on a block changes, this change is easily detectable by means of cryptographic primitives such as hash functions.
  - Transparency: Since every data stored in a block is publicly available to everyone, and the stored data cannot be modified, this provides transparency.
  - Non-repudiation: Using the cryptographic tools including sign techniques, non-repudiation is provided.
  - Equal rights: This property provides equal rights for each participant for accessing and manipulating the blockchain.

  A designer should be familiar with the five important properties introduced above.
- Permission: The two types of permissions are as follows.
  - Permissioned blockchain: By permissioned blockchain, we mean that a user must have permission to start a transaction, to join a network, or to mine. This type of blockchain is appropriate for regulated industries; for example, banks must provide users with real-world identity to meet the Know Your Customer (KYC).
  - Permission-less blockchain: This type of blockchain is totally open in the sense that the users can join a network at any time, mine blocks, and validate transactions.

  There are often trade-offs between these two types, including transaction processing rate, which is a metric of scalability [81], censorship resistance, cost, reversibility, and flexibility in changing the network rules.
- Decentralization: Decentralization lifts the burden of responsibility from an authority or a central location [141]. The spectrum of decentralization, from fully centralized to fully decentralized, is discussed as follows:
  - Fully centralized: All the users are reliant on only one central authority; e.g., the governments, courts within a jurisdiction, and such a system is a single point of failure.
  - Partially centralized and partially decentralized: There are several providers which the users can rely on. In case that a provider fails, the users can switch to other alternative providers.
  - Fully decentralized: Such systems include permission-less public blockchains, e.g., Bitcoin and Ethereum.
- Deployment: There are different types of deployment: public blockchain, consortium/community blockchain, and private blockchain.
  - Public blockchain: It is accessible by anyone in the network; most digital currencies use the public blockchain. Although such a public blockchain offers better auditability and transparency, it sacrifices performance which is a crucial factor in some real-time applications.
  - Consortium/community blockchain: It is typically used by several organizations and the right to read the blockchain is granted to the public or granted to particular participants.
  - Private blockchain: Since the network is controlled and hosted by just a single organization, private blockchains are the most flexible in terms of configuration.
- Consensus protocol: The consensus protocol impacts scalability and security. In [141] two protocols, namely Bitcoin-NG and Red Belly blockchain(RBBC), have been introduced, which improve scalability. Also, certain protocols, including PoW, proof-of-retrievability (PoR), PoS, Practical Byzantine Fault Tolerance (PBFT) presented that impact security. More details about consensus algorithms are presented in [142]. In this work, the authors classify consensus algorithms into two categories: Proof-Based and Vote-based.
- Blockchian configuration: Blockchain configuration impacts the scalability and it is associated with the number/complexity of transactions in a block and the rate at which the transactions are produced. If we shorten

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3117662, IEEE Access

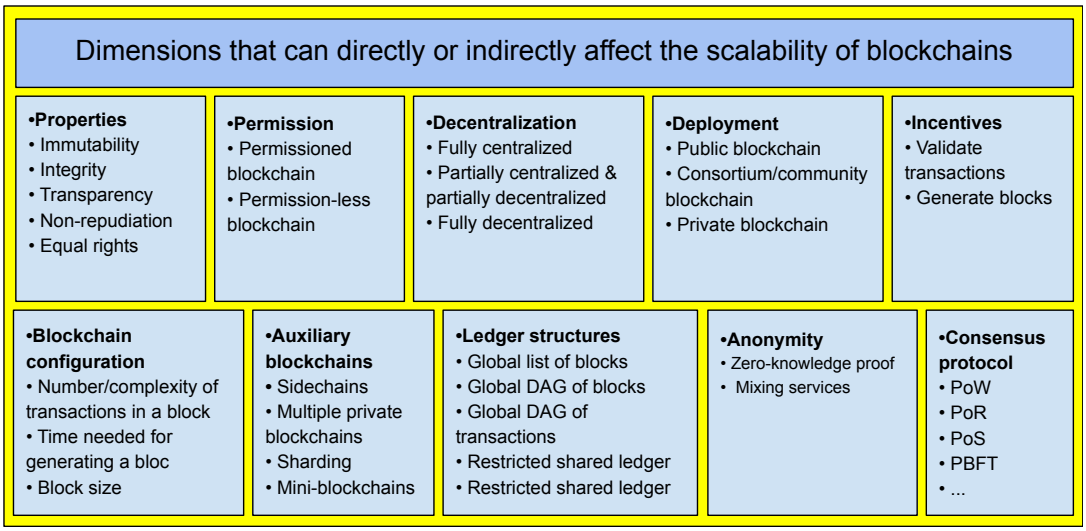

FIGURE 10. Dimensions that can directly or indirectly affect the scalability of blockchain.

the time needed for generating a block, it will reduce latency and increase throughput; however, the shorter the interblock time is, the more forks will be caused. Blockchain configuration also concerns the block size of a block. If a block includes more transactions, the throughput will be increased.

- Auxiliary blockchains: A blockchain could be combined with or built on an existing blockchain, which forms an auxiliary blockchain. This type of blockchain can be used to improve scalability. In [141], sidechains, multiple private blockchains, sharding, and mini-blockchains are introduced as options for scalability.
- Ledger structures: The ledger structure can be categorized as follows:
  - -- Global list of blocks: For example, transactions in Bitcoin are stored on a single chain of blocks.
  - -- Global directed acyclic graph (DAG) of blocks: For instance, the logical view of transactions recorded in Hashgraph [143] is based on DAG.
  - -- Global DAG of transactions: For example, IOTA [144] individual transactions also are based on DAG.
  - -- Restricted shared ledgers: Systems including Hyperledger Fabric [145] and Corda [146] consist of many small ledgers which are shared only among authorized parties to view the transactions stored in those small ledgers.
- Anonymity: In [141], two methods are mentioned for enabling private payment without disclosing the parties or the amount involved: zero-knowledge proof construction and mixing services.
- Incentives: Incentives are paid to make miners join the network, validate transactions, generate blocks, and might execute smart contract functions correctly.

Scalability-aware Recommendation

Now, we present a research direction that helps facilitate the design of a scalable blockchain. There is a well-known trilemma that states it is possible to choose only two out of the three following features: scalability, decentralization, and security [147]. Hence, according to the intended system conditions and requirements of the application, a designer should consider the most relevant dimensions for their application among the ones discussed above. This will assist the designer in balancing the scalability against both decentralization and security. Keeping in mind all these dimensions and the mentioned trilemma prevent a designer from sacrificing either security or decentralization in the process of designing.

B. ON-CHAIN APPROACH VS. OFF-CHAIN APPROACH

In [81], two different approaches to design scalable blockchains have been mentioned: off-chain solutions and on-chain solutions. On-chain approaches change the blockchain design in order to support high scalability, whereas off-chain solutions such as sidechains cause frequent transactions to occur over low-tier blockchain instances that are paralleled to and supported by the main blockchain. In this subsection, on-chain and off-chain approaches are discussed [81], [148]. By gaining a sufficient understanding of these approaches, designers of the blockchain can get an intuition of the different structures of a blockchain system. This intuition, for example, would help a designer to combine some parts of the mentioned structures in a way in order to design a scalable blockchain-based IoMT system. In this subsection, we first discuss various types of on-chain approaches and then we explain the off-chain approaches.

a: On-chain Approaches

Major on-chain solutions are discussed in the following:

- Specific consensus mechanisms: The design of new consensus mechanisms that is suitable for IoMT appli-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3117662, IEEE Access

cations is one approach to improve scalability. IoMT devices are resource-constrained in terms of computing power and storage factors. These factors are key considerations for the design of consensus algorithms in the context of IoMT. The authors in [17] summarized several consensus algorithms for blockchain-based IoT systems (see Table 4). As mentioned in Table 4, PoS, FBA and dBFT are scalable. In PoS, the goal is to reduce the processing required to create a block; however, one of the problems with PoS in the IoT is that it can lead to the consolidation of consensus across few nodes, creating a single point of attack, somewhat centralizing trust, and limiting scalability. Moreover, as far as we know, there is no blockchain for IoT using the PoS consensus. FBA is also scalable, but it needs the trusted nodes, which is a challenge for designing the system. Finally, dBFT also can solve the problem of scaling consensus algorithms by reducing the number of nodes that perform consensus. However, as elected nodes are unreliable in dynamic IoT scenarios, it can still cause a problem. A designer should consider three factors for the adoption of the consensus algorithm: the architecture of the system, the intended attack vector, and the hardware requirements [149].

- Sharding: A major solution to design a scalable blockchain is sharding [86], [87], [150]. Sharding splits the overheads of processing among several smaller groups of nodes that work parallelly in order to maximize performance, while they require considerably lower communication overhead.
- DAG-based distributed ledger structures: Directed Acyclic Graph (DAG) structure makes it possible to append concurrently several blocks to the network [151]. IOTA cryptocurrency system [144], for example, makes use of a DAG structure [88].
- Parallel blockchain extension: In this solution, leaders coordinate with other nodes to achieve consensus. They extend in different parallel parts of the blockchain (a graph of transactions). In the framework proposed by [152], each transaction validates two previous transactions, i.e., its parents.
- Multiple blocks per leader: Bitcoin-NG [84] is much like bitcoin that serializes transactions while allowing for better bandwidth and latency performance without sacrificing other factors. The leader, in fact, can unilaterally append several transactions to the blockchain during its epoch.
- Collective leaders: This solution makes use of several leaders to decide quickly and collectively whether or not a block should be inserted into the blockchain [153].

b: Our Recommendation on On-chain Solutions

Reasonable combining of some of these themes which are mentioned above would lead us to propose a new scalable protocol without sacrificing security and performance, which could be applied in IoMT systems. For example, the idea of parallel blockchain extension [152] can be merged with Sharding schemes so that the blockchain exists as partially connected trees on separated shards.

c: Off-chain Approaches

Sidechains which are a type of off-chain approach, have been heralded as the key enabler of blockchain scalability and interoperability [154]. Sidechains can be used to off-load the load of a blockchain in terms of transaction processing. Two types of sidechains are as follows:

- Two blockchains can be the sidechains of the other and they are treated as equals.
- The sidechain can be a child of an existing blockchain named the mainchain.

Note: Given that the two chains are secure as individual blockchains, a secure sidechain protocol construction allows this security to be carried on to cross-chain transfers [154].

Sidechain Related Works: In [154] a sidechain construction has been presented that is suitable for Proof-of-Stake sidechain systems. It is shown that this scheme can be adapted for other protocols such as Ouroboros [155], Ouroboros Genesis [156], Snow White [157], and Algorand [158]. The authors in [154] proved that their construction is secure by means of the standard cryptographic assumptions. Cross-chain certification is the important technique used in this study, which is facilitated by a novel cryptographic primitive called ad-hoc threshold multisignatures (ATMS). The work [159] is another construction about sidechain allowing communication between Proof-of-Work blockchains without trusted intermediaries. Non-Interactive Proofs of Proof-of-Work (NIPoPoWs) is used as a cryptographic primitive in this paper. Moreover, pigged sidechains [148] enables bitcoins and other ledger assets to be transferred between multiple blockchains. They refer to interoperable blockchains as pegged sidechains. In a two-way peg scheme, a simplified payment verification proof (SPV) is used.

d: Our Recommendation on Off-chain Solutions

Among the mentioned studies, [160] and [161] are provably secure and they made use of PoS and PoW as consensus algorithms, respectively; hence, one approach can be to design a provably secure sidechain construction for IoMT secure consensus protocols with enhanced features.

To conclude this subsection, it is important for a designer to sufficiently understand the dimensions of a blockchain system, including the consensus algorithm, ledger structure, etc. Furthermore, keeping in mind the two approaches, on-chain and off-chain, will help designers to consider a blockchain structure that fits their desired application's objectives.

C. BENCHMARKING OF BLOCKCHAIN SYSTEMS

After designing a scalable blockchain system, it must be benchmarked. This can help a designer to distinguish the bottlenecks correctly, and, therefore, he/she can apply rea-

TABLE 4. Consensus algorithms for blockchains in IoT

Consensus algorithm	Deployment	Permission	Benefits	Drawbacks
PoS [162]	Public	Permissionless	Scalable, lower power consumption	Overload in few nodes can impact in the operation of the blockchain
FBA [163]	Private or Consortium	Permissioned	Scalable and less hardware/energy requirements	It is required that "important" nodes are trusted
dBFT [164]	Private or Consortium	Permissioned	Scalable and less hardware/energy requirements	Problems in dynamic scenarios
PoW [165]	Public	Permissionless	Few messages exchanged to achieve consensus	High energy and computing consumption
PoSpace [166]	Public	Permissionless	Lower power consumption	Requires high amount of memory/storage
PBFT [167]	Private or Consortium	Permissionless	Less hardware/energy requirements	Not scalable
IBFT [168]	Private or Consortium	Permissionless	Less hardware/energy requirements	Not scalable, produces empty blocks
RAFT [164]	Private or Consortium	Permissionless	Less hardware/energy requirements	Not scalable, serialization of requests

sonable trade-offs to solve the bottlenecks. In order to benchmark a system, appropriate abstraction layers need to be adapted as this will impact the way a blockchain system is benchmarked. As discussed in [82], the authors have refined the layers they adapted in the design stage to benchmark each layer individually. These layers are distributed ledger, cryptography, consensus and smart contracts. This paper shows several trade-offs in the design space. These layers are: Cryptography, Smart contract, Consensus, and Distributed ledger. In [82], all the above-mentioned layers are benchmarked using BLOCKBENCH framework [134], resulting in gaining insights into the design trade-offs and bottlenecks. Specifically, five important metrics are used for benchmarking: scalability, latency, throughput, fault tolerance, and security metrics. To sum up, the authors in [82] abstracts the blockchain system in a way so that they can explore the trade-offs and bottlenecks using the four mentioned layers.

Scalability-aware Recommendation

In order to benchmark a designed blockchain system, the following research questions should be taken into account:

- What layers ought to be chosen in order to design a scalable blockchain system according to the blockchain features and requirements? To be more precise, what abstraction layers need to be considered? It is worth mentioning that due to the selected layers, the designer will only focus on the abstraction layer such as consensus protocols, cryptographic algorithms, ledger structure and so forth, which in turn impacts the scalability.
- What benchmark frameworks will be matched our chosen layers? Is it be possible to customize some existing frameworks or should they be developed from scratch?
- It should be considered that scalability is not a singular well-defined metric of a blockchain system. To be more precise, scalability captures the tension between various performances and security metrics [85]. Therefore, this raises another question: what metrics should be selected in the evaluation process of the scalable blockchain system and how do these metrics have to be evaluated?
- After the evaluation of the blockchain system, tuning of the system to achieve the maximum scalability using hyperparameter optimization techniques, such as Bayesian optimization would be necessary, thus raises this question: in order to achieve optimum scalability, which parameters of the designed blockchain system should be configured? And to what extent can these parameters be pushed without sacrificing security or other important metrics?

Further metrics can be of interest and they can be research questions. For example, the cost could be a noticeable metric, and how this metric would be defined with respect to a specific blockchain system is a question.

VIII. CONCLUSION

In this survey, we first described the cloud-based IoMT system and its drawbacks, among which (i) the single point of failure, (ii) security and (iii) privacy threats are the most important issues of such systems. Then, we gave an introduction to blockchain technology and elaborated on the benefits of this technology for IoMT systems. We discussed how IoMT systems could reap the benefits of blockchain technology, including distributed ledger, transparency, tamper-proof ledger to overcome those drawbacks. A taxonomy of healthcare applications is demonstrated in this survey. These applications are categorized into four groups, namely healthcare management, healthcare big data, supply chain management, and IoMT. In this survey, we focused on the IoMT application and conducted a comprehensive review of the state-of-the-art of blockchain-based IoMT systems. We considered 24 articles in the corresponding domain. By comparing and analyzing these studies, we identified an important research gap which is scalability. This gap is a major concern that should be taken into account by researchers when designing such systems. Finally, we considered two approaches to solve scalability, i.e., either on-chain and off-chain-based solutions, and presented several research directions which could guide researchers through designing scalable blockchain-based IoMT systems.

REFERENCES

[1] M. Thibaud, H. Chi, W. Zhou, and S. Piramuthu, "Internet of Things (IoT) in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review," *Decision Support Systems*, vol. 108, pp. 79–95, 2018.

[2] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Computer Networks*, vol. 144, pp. 17–39, 2018.

[3] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The future of healthcare internet of things: a survey of emerging technologies," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1121–1167, 2020.

[4] A. H. Sodhro, S. Pirbhulal, and A. K. Sangaiah, "Convergence of iot and product lifecycle management in medical health care," *Future Generation Computer Systems*, vol. 86, pp. 380–391, 2018.

[5] L. Haoyu, L. Jianxing, N. Arunkumar, A. F. Hussein, and M. M. Jaber, "An iomt cloud-based real time sleep apnea detection scheme by using the spo2 estimation supported by heart rate variability," *Future Generation Computer Systems*, vol. 98, pp. 69–77, 2019.

[6] A. Nayyar, V. Puri, and N. G. Nguyen, "Biosenhealth 1.0: A novel internet of medical things (iomt)-based patient health monitoring system," in *International Conference on Innovative Computing and Communications*. Springer, 2019, pp. 155–164.

[7] I. Jayatilleka and M. N. Halgamuge, "Internet of things in healthcare: Smart devices, sensors, and systems related to diseases and health conditions," in *Real-Time Data Analytics for Large Scale Sensor Data*. Elsevier, 2020, pp. 1–35.

[8] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and privacy in the medical internet of things: a review," *Security and Communication Networks*, vol. 2018, 2018.

[9] F. Alsubaei, A. Abuhussein, and S. Shiva, "An overview of enabling technologies for the internet of things," *Internet of Things A to Z: Technologies and Applications*, pp. 77–112, 2018.

[10] "Reimagining the patient-centric clinical trial with iomt," https://www.iconplc.com/insights/patient-centricity/reimagining-patient-centricity-with-the-iomt/, 2019.

[11] S. P. Amaraweera and M. N. Halgamuge, "Internet of things in the healthcare sector: Overview of security and privacy issues," in *Security, Privacy and Trust in the IoT Environment*. Springer, 2019, pp. 153–179.

[12] M. Jayaratne, D. Nallaperuma, D. De Silva, D. Alahakoon, B. Devitt, K. E. Webster, and N. Chilamkurti, "A data integration platform for patient-centered e-healthcare and clinical decision support," *Future Generation Computer Systems*, vol. 92, pp. 996–1008, 2019.

[13] A. A. Mutlag, M. K. A. Ghani, N. a. Arunkumar, M. A. Mohamed, and O. Mohd, "Enabling technologies for fog computing in healthcare iot systems," *Future Generation Computer Systems*, vol. 90, pp. 62–78, 2019.

[14] E. Marin, M. A. Mustafa, D. Singelée, and B. Preneel, "A privacy-preserving remote healthcare system offering end-to-end security," in *International Conference on Ad-Hoc Networks and Wireless*. Springer, 2016, pp. 237–250.

[15] P. Asuquo, C. Ogah, W. Hathal, and S. Bao, "Blockchain meets cybersecurity: Security, privacy, challenges, and opportunity," in *Advanced Applications of Blockchain Technology*. Springer, 2020, pp. 115–127.

[16] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266–2277, 2019.

[17] S. Kim and G. C. Deka, *Advanced applications of blockchain technology*. Springer, 2020.

[18] R. A. Memon, J. P. Li, J. Ahmed, M. I. Nazeer, M. Ismail, and K. Ali, "Cloud-based vs. blockchain-based iot: a comparative survey and way forward," *Frontiers of Information Technology & Electronic Engineering*, vol. 21, no. 4, pp. 563–586, 2020.

[19] A. A. Abdellatif, M. G. Khafagy, A. Mohamed, and C.-F. Chiasserini, "Eeg-based transceiver design with data decomposition for healthcare iot applications," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3569–3579, 2018.

[20] F. Qureshi and S. Krishnan, "Wearable hardware design for the internet of medical things (iomt)," *Sensors*, vol. 18, no. 11, p. 3812, 2018.

[21] F. Alsubaei, A. Abuhussein, V. Shandilya, and S. Shiva, "Iomt-saf: Internet of medical things security assessment framework," *Internet of Things*, vol. 8, p. 100123, 2019.

[22] K. M. Hossein, M. E. Esmaeili, T. Dargahi *et al.*, "Blockchain-based privacy-preserving healthcare architecture," in *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*. IEEE, 2019, pp. 1–4.

[23] A. Banafa, "Iot and blockchain convergence: benefits and challenges," *IEEE Internet of Things*, 2017. [Online]. Available: http://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html

[24] A. Erdem, S. Ö. Yildirim, and P. Angin, "Blockchain for ensuring security, privacy, and trust in iot environments: The state of the art," in *Security, Privacy and Trust in the IoT Environment*. Springer, 2019, pp. 97–122.

[25] E. J. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," *ACM Computing Surveys (CSUR)*, vol. 53, no. 2, pp. 1–27, 2020.

[26] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *Journal of Network and Computer Applications*, vol. 135, pp. 62–75, 2019.

[27] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives," *Cryptography*, vol. 3, no. 1, p. 3, 2019.

[28] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Applied Sciences*, vol. 9, no. 9, p. 1736, 2019.

[29] M. M. H. Onik, S. Aich, J. Yang, C.-S. Kim, and H.-C. Kim, "Blockchain in healthcare: Challenges and solutions," in *Big Data Analytics for Intelligent Healthcare Management*. Elsevier, 2019, pp. 197–226.

[30] T. Hardin and D. Kotz, "Blockchain in health data systems: A survey," in *2019 sixth international conference on internet of things: Systems, management and security (IOTSMS)*. IEEE, 2019, pp. 490–497.

[31] H. D. Zubaydi, Y.-W. Chong, K. Ko, S. M. Hanshi, and S. Karuppayah, "A review on the role of blockchain technology in the healthcare domain," *Electronics*, vol. 8, no. 6, p. 679, 2019.

[32] K. Rabah, "Challenges & opportunities for blockchain powered healthcare systems: A review," *Mara Research Journal of Medicine and Health Sciences*, vol. 1, no. 1, pp. 45–52, 2017.

[33] R. M. Aileni and G. Suciu, "Iomt: A blockchain perspective," in *Decentralised Internet of Things*. Springer, 2020, pp. 199–215.

[34] S. Pirbhulal, O. W. Samuel, W. Wu, A. K. Sangaiah, and G. Li, "A joint resource-aware and medical data security framework for wearable healthcare systems," *Future Generation Computer Systems*, vol. 95, pp. 382–391, 2019.

[35] F. Alsubaei, A. Abuhussein, and S. Shiva, "A framework for ranking iomt solutions based on measuring security and privacy," in *Proceedings of the Future Technologies Conference*. Springer, 2018, pp. 205–224.

[36] G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, "Internet of medical things (iomt): applications, benefits and future challenges in healthcare domain," *J Commun*, vol. 12, no. 4, pp. 240–7, 2017.

[37] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the internet of medical things: taxonomy and risk assessment," in *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*. IEEE, 2017, pp. 112–120.

[38] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of security and privacy for the internet of medical things (iomt)," in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, 2019, pp. 457–464.

[39] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and privacy for the internet of medical things enabled healthcare systems: A survey," *IEEE Access*, vol. 7, pp. 183 339–183 355, 2019.

[40] T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre, "Healthsense: A medical use case of internet of things and blockchain," in *2017 International conference on intelligent sustainable systems (ICISS)*. IEEE, 2017, pp. 486–491.

[41] M. A. Rahman, E. Hassanain, M. M. Rashid, S. J. Barnes, and M. S. Hossain, "Spatial blockchain-based secure mass screening framework for children with dyslexia," *IEEE Access*, vol. 6, pp. 61 876–61 885, 2018.

[42] W. Meng, W. Li, and L. Zhu, "Enhancing medical smartphone networks via blockchain-based trust management against insider attacks," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1377–1386, 2019.

[43] M. Seliem and K. Elgazzar, "Biomt: Blockchain for the internet of medical things," in *2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*. IEEE, 2019, pp. 1–4.

[44] N. Diawar, M. Rizwan, F. Ahmad, and S. Akram, "Blockchain: Securing internet of medical things (iomt)," *International Journal Of Advanced Computer Science and Applications*, pp. 82–89, 2019.

[45] A. D. Dwivedi, L. Malina, P. Dzurenda, and G. Srivastava, "Optimized blockchain model for internet of things based healthcare applications," *arXiv preprint arXiv:1906.06517*, 2019.

[46] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8770–8781, 2019.

[47] V. Malamas, T. Dasaklis, P. Kotzanikolaou, M. Burmester, and S. Katsikas, "A forensics-by-design management framework for medical devices based on blockchain," in *2019 IEEE World Congress on Services (SERVICES)*, vol. 2642. IEEE, 2019, pp. 35–40.

[48] G. Srivastava, J. Crichigno, and S. Dhar, "A light and secure healthcare blockchain for iot medical devices," in *2019 IEEE Canadian conference of electrical and computer engineering (CCECE)*. IEEE, 2019, pp. 1–5.

[49] M. A. Habib, C. N. Faisal, S. Sarwar, M. A. Latif, F. Aadil, M. Ahmad, R. Ashraf, and M. Maqsood, "Privacy-based medical data protection against internal security threats in heterogeneous internet of medical things," *International Journal of Distributed Sensor Networks*, vol. 15, no. 9, p. 1550147719875653, 2019.

[50] M. Shen, Y. Deng, L. Zhu, X. Du, and N. Guizani, "Privacy-preserving image retrieval for medical iot systems: A blockchain-based approach," *IEEE Network*, vol. 33, no. 5, pp. 27–33, 2019.

[51] G. Srivastava, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "Data sharing and privacy for patient iot devices using blockchain," in *International Conference on Smart City and Informatization*. Springer, 2019, pp. 334–348.

[52] D. C. Nguyen, K. D. Nguyen, and P. N. Pathirana, "A mobile cloud based iomt framework for automated health assessment and management," in *2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. IEEE, 2019, pp. 6517–6520.

[53] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure ehrs sharing of mobile cloud based e-health systems," *IEEE Access*, 2019.

[54] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. Rodrigues, and Y. Park, "Bakmp-iomt: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment," *IEEE Access*, vol. 8, pp. 95 956–95 977, 2020.

[55] H.-N. Dai, M. Imran, and N. Haider, "Blockchain-enabled internet of medical things to combat covid-19," *IEEE Internet of Things Magazine*, vol. 3, no. 3, pp. 52–57, 2020.

[56] D. Połap, G. Srivastava, A. Jolfaei, and R. M. Parizi, "Blockchain technology and neural networks for the internet of medical things," in *IEEE INFOCOM 2020-IEEE conference on computer communications workshops (INFOCOM WKSHPS)*. IEEE, 2020, pp. 508–513.

[57] B. S. Egala, A. K. Pradhan, V. R. Badarla, and S. P. Mohanty, "Fortified-chain: A blockchain based framework for security and privacy assured internet of medical things with effective access control," *IEEE Internet of Things Journal*, 2021.

[58] R. Kumar and R. Tripathi, "Towards design and implementation of security and privacy framework for internet of medical things (IoMT) by leveraging blockchain and IPFS technology," *The Journal of Supercomputing*, pp. 1–40, 2021.

[59] B. A. Alqaralleh, T. Vaiyapuri, V. S. Parvathy, D. Gupta, A. Khanna, and K. Shankar, "Blockchain-assisted secure image transmission and diagnosis model on internet of medical things environment," *Personal and Ubiquitous Computing*, pp. 1–11, 2021.

[60] P. Angin, M. B. Mert, O. Mete, A. Ramazanli, K. Sarica, and B. Gungoren, "A blockchain-based decentralized security architecture for iot," in *International Conference on Internet of Things*. Springer, 2018, pp. 3–18.

[61] S. F. Aghili, H. Mala, M. Shojafar, and P. Peris-Lopez, "Laco: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in iot," *Future Generation Computer Systems*, vol. 96, pp. 410–424, 2019.

[62] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018.

[63] I. P. Team, *EU general data protection regulation (GDPR): an implementation and compliance guide*. IT Governance Ltd, 2017.

[64] M. Rhahla, T. Abdellatif, R. Attia, and W. Berrayana, "A gdpr controller for iot systems: application to e-health," in *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. IEEE, 2019, pp. 170–173.

[65] R. Nosowsky and T. J. Giordano, "The health insurance portability and accountability act of 1996 (hipaa) privacy rule: implications for clinical research," *Annu. Rev. Med.*, vol. 57, pp. 575–590, 2006.

[66] A. Zaslavsky, C. Perera, and D. Georgakopoulos, "Sensing as a service and big data," *arXiv preprint arXiv:1301.0159*, 2013.

[67] J. Bell, T. D. LaToza, F. Baldmitsi, and A. Stavrou, "Advancing open science with version control and blockchains," in *Proceedings of the 12th International Workshop on Software Engineering for Science*. IEEE Press, 2017, pp. 13–14.

[68] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[69] B. MacKenzie, R. I. Ferguson, and X. Bellekens, "An assessment of blockchain consensus protocols for the internet of things," in *2018 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*. IEEE, 2018, pp. 183–190.

[70] M. Jakobsson and A. Juels, "Proofs of work and bread pudding protocols," in *Secure information networks*. Springer, 1999, pp. 258–272.

[71] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems (TOCS)*, vol. 20, no. 4, pp. 398–461, 2002.

[72] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol," in *proceedings of the 1st Workshop on System Software for Trusted Execution*, 2016, pp. 1–6.

[73] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in *2017 19th international conference on advanced communication technology (ICACT)*. IEEE, 2017, pp. 464–467.

[74] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in *IEEE EUROCON 2017-17th International Conference on Smart Technologies*. IEEE, 2017, pp. 763–768.

[75] W. Xin, T. Zhang, C. Hu, C. Tang, C. Liu, and Z. Chen, "On scaling and accelerating decentralized private blockchains," in *2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids)*. IEEE, 2017, pp. 267–271.

[76] V. Buterin, "Ethereum white paper," *GitHub repository*, vol. 1, pp. 22–23, 2013.

[77] T. Hu, X. Liu, T. Chen, X. Zhang, X. Huang, W. Niu, J. Lu, K. Zhou, and Y. Liu, "Transaction-based classification and detection approach for Ethereum smart contract," *Information Processing & Management*, vol. 58, no. 2, p. 102462, 2021.

[78] I. Mokdad and N. M. Hewahi, "Empirical evaluation of blockchain smart contracts," in *Decentralised Internet of Things*. Springer, 2020, pp. 45–71.

[79] "Open architecture," https://www.gartner.com/en/information-technology/glossary/open-architecture, 2020.

[80] "Worldwide spending on blockchain solutions from 2017 to 2024," https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/, 2021.

[81] S. Bano, M. Al-Bassam, and G. Danezis, "The road to scalable blockchain designs," *USENIX; login: magazine*, 2017.

[82] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.

[83] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. bft replication," in *International workshop on open problems in network security*. Springer, 2015, pp. 112–125.

[84] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol," in *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, 2016, pp. 45–59.

[85] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer *et al.*, "On scaling decentralized blockchains," in *International Conference on Financial Cryptography and Data Security*. Springer, 2016, pp. 106–125.

[86] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 17–30.

[87] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 583–598.

[88] S. Popov, O. Saa, and P. Finardi, "Equilibria in the tangle," *Computers & Industrial Engineering*, vol. 136, pp. 160–172, 2019.

[89] A. S. Sani, D. Yuan, W. Bao, P. L. Yeoh, Z. Y. Dong, B. Vucetic, and E. Bertino, "Xyreum: A high-performance and scalable blockchain for iiot security and privacy," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2019, pp. 1920–1930.

[90] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Lsb: A lightweight scalable blockchain for iot security and anonymity," *Journal of Parallel and Distributed Computing*, vol. 134, pp. 180–197, 2019.

[91] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4650–4659, 2018.

[92] L. Zhu, Y. Wu, K. Gai, and K.-K. R. Choo, "Controllable and trustworthy blockchain-based cloud data management," *Future Generation Computer Systems*, vol. 91, pp. 527–535, 2019.

[93] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable cities and society*, vol. 39, pp. 283–297, 2018.

[94] A. Mense and L. Athanasiadis, "Concept for sharing distributed personal health records with blockchains," in *Data, Informatics and Technology: An Inspiration for Improved Healthcare*. IOS Press, 2018, pp. 7–10.

[95] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment," *Journal of medical systems*, vol. 42, no. 8, p. 156, 2018.

[96] J. Cunningham and J. Ainsworth, "Enabling patient control of personal electronic health records through distributed ledger technology," *Stud Health Technol Inform*, vol. 245, pp. 45–48, 2018.

[97] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 2017, pp. 1–5.

[98] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd International Conference on Open and Big Data (OBD)*. IEEE, 2016, pp. 25–30.

[99] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, no. 10, p. 218, 2016.

[100] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *Journal of medical systems*, vol. 43, no. 1, pp. 1–9, 2019.

[101] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Medibchain: A blockchain based privacy preserving platform for healthcare data," in *International conference on security, privacy and anonymity in computation, communication and storage*. Springer, 2017, pp. 534–543.

[102] M. Swan, "Blockchain thinking: The brain as a decentralized autonomous corporation [commentary]," *IEEE Technology and Society Magazine*, vol. 34, no. 4, pp. 41–52, 2015.

[103] D. Dujak and D. Sajter, "Blockchain applications in supply chain," in *SMART supply network*. Springer, 2019, pp. 21–46.

[104] J.-H. Tseng, Y.-C. Liao, B. Chong, and S.-w. Liao, "Governance on the drug supply chain via gcoin blockchain," *International journal of environmental research and public health*, vol. 15, no. 6, p. 1055, 2018.

[105] T. Nugent, D. Upton, and M. Cimpoesu, "Improving data transparency in clinical trials using blockchain smart contracts," *F1000Research*, vol. 5, 2016.

[106] M. Benchoufi and P. Ravaud, "Blockchain technology for improving clinical research quality," *Trials*, vol. 18, no. 1, p. 335, 2017.

[107] J. Padikkapparambil, C. Ncube, K. K. Singh, and A. Singh, "Internet of things technologies for elderly health-care applications," in *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach*. Elsevier, 2020, pp. 217–243.

[108] A. H. Sodhro, A. K. Sangaiah, S. Pirphulal, A. Sekhari, and Y. Ouzrout, "Green media-aware medical iot system," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 3045–3064, 2019.

[109] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, "A privacy-preserving cryptosystem for IoT E-healthcare," *Information Sciences*, vol. 527, pp. 493–510, 2020.

[110] M. Irfan and N. Ahmad, "Internet of medical things: Architectural model, motivational factors and impediments," in *2018 15th Learning and Technology Conference (L&T)*. IEEE, 2018, pp. 6–13.

[111] M. Hossain, S. R. Islam, F. Ali, K.-S. Kwak, and R. Hasan, "An internet of things-based health prescription assistant and its security system design," *Future generation computer systems*, vol. 82, pp. 422–439, 2018.

[112] V. Gatteschi, F. Lamberti, and C. Demartini, "Blockchain technology use cases," in *Advanced Applications of Blockchain Technology*. Springer, 2020, pp. 91–114.

[113] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.

[114] I. Radanović and R. Likić, "Opportunities for use of blockchain technology in medicine," *Applied health economics and health policy*, vol. 16, no. 5, pp. 583–590, 2018.

[115] A. Kumar and R. Kumar, "Privacy preservation of electronic health record: Current status and future direction," in *Handbook of Computer Networks and Cyber Security*. Springer, 2020, pp. 715–739.

[116] H. Luo, W. Chen, C. Chen, Y. Yang, Y. Zhang, and Y. Wu, "Analysis of a multichannel lightweight identity authentication method," in *2019 IEEE 19th International Conference on Communication Technology (ICCT)*. IEEE, 2019, pp. 1285–1290.

[117] W. Meng, W. Li, Y. Wang, and M. H. Au, "Detecting insider attacks in medical cyber–physical networks based on behavioral profiling," *Future Generation Computer Systems*, vol. 108, pp. 1258–1266, 2020.

[118] Y. L. Sun, W. Yu, Z. Han, and K. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 305–317, 2006.

[119] W. Meng, W. Li, Y. Xiang, and K.-K. R. Choo, "A bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks," *Journal of Network and Computer Applications*, vol. 78, pp. 162–169, 2017.

[120] K. A. Kumari, R. Padmashani, R. Varsha, and V. Upadhayay, "Securing internet of medical things (iomt) using private blockchain network," in *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*. Springer, 2020, pp. 305–326.

[121] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2018.

[122] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.

[123] C. Cachin and M. Vukolić, "Blockchain consensus protocols in the wild," *arXiv preprint arXiv:1707.01873*, 2017.

[124] C. Li, M. Dong, J. Li, G. Xu, X. Chen, and K. Ota, "Healthchain: Secure emrs management and trading in distributed healthcare service system," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7192–7202, 2020.

[125] T. A. Rahoof and V. Deepthi, "Healthchain: A secure scalable health care data management system using blockchain," in *International Conference on Distributed Computing and Internet Technology*. Springer, 2020, pp. 380–391.

[126] F. Ellouze, G. Fersi, and M. Jmaiel, "Blockchain for internet of medical things: A technical review," in *International Conference on Smart Homes and Health Telematics*. Springer, 2020, pp. 259–267.

[127] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The simon and speck lightweight block ciphers," in *Proceedings of the 52nd Annual Design Automation Conference*, 2015, pp. 1–6.

[128] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2001, pp. 552–565.

[129] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based iot ecosystem using attribute-based encryption," in *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE, 2017, pp. 1–6.

[130] Y. Sompolinsky and A. Zohar, "Phantom, ghostdag," 2020. [Online]. Available: https://eprint.iacr.org/2018/104.pdf

[131] J. Konečnỳ, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," *arXiv preprint arXiv:1610.05492*, 2016.

[132] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, "Blockchain-assisted secured data management framework for health information analysis based on internet of medical things," *Personal and Ubiquitous Computing*, pp. 1–14, 2021.

[133] R. Akkaoui, "Blockchain for the management of internet of things devices in the medical industry," *IEEE Transactions on Engineering Management*, pp. 1–12, 2021.
[134] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "Blockbench: A framework for analyzing private blockchains," in *Proceedings of the 2017 ACM International Conference on Management of Data*. ACM, 2017, pp. 1085–1100.
[135] IBM, "Blockchain performance benchmarking for hyperledger besu, hyperledger fabric, ethereum and fisco bcos networks," in *White Paper*, 2018.
[136] Z. Dong, E. Zheng, Y. Choon, and A. Y. Zomaya, "Dagbench: A performance evaluation framework for dag distributed ledgers," in *2019 IEEE 12th International Conference on Cloud Computing (CLOUD)*. IEEE, 2019, pp. 264–271.
[137] D. Saingre, T. Ledoux, and J.-M. Menaud, "Bctmark: a framework for benchmarking blockchain technologies," in *2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA)*. IEEE, 2020, pp. 1–8.
[138] X. Duan, H. Pan, L. Tseng, and Y. Wu, "Bbb: make benchmarking blockchains configurable and extensible," in *2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC)*. IEEE, 2019, pp. 61–611.
[139] H. Pan, X. Duan, Y. Wu, L. Tseng, M. Aloqaily, and A. Boukerche, "Bbb: A lightweight approach to evaluate private blockchains in clouds," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*. IEEE, 2020, pp. 1–6.
[140] C. Lal and D. Marijan, "Blockchain testing: Challenges, techniques, and research directions," *arXiv preprint arXiv:2103.10074*, 2021.
[141] X. Xu, I. Weber, and M. Staples, "Varieties of blockchains," in *Architecture for Blockchain Applications*. Springer, 2019, pp. 45–59.
[142] R. Bhardwaj and D. Datta, "Consensus algorithm," in *Decentralised Internet of Things*. Springer, 2020, pp. 91–107.
[143] "Hashgraph," https://www.hederahashgraph.com/.
[144] "IOTA," http://www.iota.org/.
[145] C. Cachin *et al.*, "Architecture of the hyperledger blockchain fabric," in *Workshop on distributed cryptocurrencies and consensus ledgers*, vol. 310, no. 4. Chicago, IL, 2016.
[146] M. Benji and M. Sindhu, "A study on the corda and ripple blockchain platforms," in *Advances in Big Data and Cloud Computing*. Springer, 2019, pp. 179–187.
[147] M. Liu, F. R. Yu, Y. Teng, V. C. Leung, and M. Song, "Performance optimization for blockchain-enabled industrial internet of things (iiot) systems: A deep reinforcement learning approach," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3559–3570, 2019.
[148] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, "Enabling blockchain innovations with pegged sidechains," *URL: http://www.opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*, 2014.
[149] V. Dedeoglu, R. Jurdak, A. Dorri, R. Lunardi, R. Michelin, A. Zorzo, and S. Kanhere, "Blockchain technologies for iot," in *Advanced Applications of Blockchain Technology*. Springer, 2020, pp. 55–89.
[150] M. Zamani, M. Movahedi, and M. Raykova, "Rapidchain: scaling blockchain via full sharding," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2018, pp. 931–948.
[151] L. Cui, S. Yang, Z. Chen, Y. Pan, M. Xu, and K. Xu, "An efficient and compacted dag-based blockchain protocol for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4134–4145, 2019.
[152] X. Boyen, C. Carr, and T. Haines, "Blockchain-free cryptocurrencies: A framework for truly decentralised fast transactions," Cryptology ePrint Archive, Report 2016/871, Tech. Rep., 2016.
[153] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*, 2016, pp. 279–296.
[154] P. Gaži, A. Kiayias, and D. Zindros, "Proof-of-stake sidechains," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 139–156.
[155] B. David, P. Gaži, A. Kiayias, and A. Russell, "Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2018, pp. 66–98.
[156] C. Badertscher, P. Gaži, A. Kiayias, A. Russell, and V. Zikas, "Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2018, pp. 913–930.
[157] I. Bentov, R. Pass, and E. Shi, "Snow white: Provably secure proofs of stake." *IACR Cryptology ePrint Archive*, vol. 2016, p. 919, 2016.
[158] J. Chen and S. Micali, "Algorand," *arXiv preprint arXiv:1607.01341*, 2016.
[159] A. Kiayias and D. Zindros, "Proof-of-work sidechains," in *International Conference on Financial Cryptography and Data Security*. Springer, 2019, pp. 21–34.
[160] P. Gazi, A. Kiayias, and D. Zindros, "Proof-of-stake sidechains," in *IEEE Symposium on Security & Privacy*, 2019.
[161] A. Kiayias and D. Zindros, "Proof-of-work sidechains," Cryptology ePrint Archive, Report 2018/1048, Tech. Rep., 2018.
[162] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published paper, August*, vol. 19, 2012.
[163] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," *Stellar Development Foundation*, vol. 32, 2015.
[164] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, 2017, pp. 2567–2572.
[165] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 3–16.
[166] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in *Annual Cryptology Conference*. Springer, 2015, pp. 585–605.
[167] M. Castro, B. Liskov *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, no. 1999, 1999, pp. 173–186.
[168] A. Baliga, I. Subhod, P. Kamat, and S. Chatterjee, "Performance evaluation of the quorum blockchain platform," *arXiv preprint arXiv:1809.03421*, 2018.

AMIRHOSSEIN ADAVOUDI JOLFAEI is currently doing his PhD under the Department of Computer Science, University of Luxembourg. He received his M.S. degree at University of Isfahan in 2017. His main research interests include lightweight security protocols, privacy-preserving in vehicular sensor networks, secure computation, WSNs security.

SEYED FARHAD AGHILI received his Ph.D. degree in Information Technology Engineering from Faculty of Computer Engineering, University of Isfahan in 2019. He received his M.S. degree in Electrical Engineering from Shahid Rajaee Teacher Training University (SRTTU) in 2013. He is currently a Post Doctoral Research Fellow, COSIC, KU Leuven, Belgium. In July 2018, he joined to SPRITZ Security & Privacy Research Group at the University of Padua as a visiting Ph.D. researcher. From April 2019 to January 2020, he was an exchange Ph.D. student at Computer Networks and Telematics, Institute of Computer Science, Faculty of Engineering, University of Freiburg. His current research interest includes RFID and IoT systems security.

DR. IR. DAVE SINGELÉE received the Master's degree of Electrical Engineering and a PhD in Applied Sciences in 2002 and 2008 respectively, both from KU Leuven (Belgium). He is currently an industrial research manager (IOF) at the research group COSIC. His main research interests are cryptography, security and privacy of wireless communication networks, key management, distance bounding, cryptographic authentication protocols, and security solutions for medical devices.