2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain) | 978-1-6654-5198-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/IGETBLOCKCHAIN56591.2022.10087115

A systematic review of the use of blockchain in Internet of Medical Things

Madeleine B. P. Vega
Institute of Advanced Studies
University of São Paulo
São Paulo, Brazil
madeleinelbpv@gmail.com

Antonio M. Saraiva
Computer Engineering Department
University of São Paulo
São Paulo, Brazil
saraiva@usp.br

Marcos A. Simplicio Jr.
Computer Engineering Department
University of São Paulo
São Paulo, Brazil
mjunior@larc.usp.br

Bruno C. Albertini
Computer Engineering Department
University of São Paulo
São Paulo, Brazil
balbertini@usp.br

Roberto F. Silva
Institute of Advanced Studies
University of São Paulo
São Paulo, Brazil
Roberto.fray.silva@gmail.com

***Abstract*—International health organizations advocate for health care with greater quality and safety, reflecting population needs. However, current health services are inefficient, facing problems of inadequate treatment, human resources, infrastructure, and high costs. Digital health technologies play an increasingly important role in healthcare services such as remote care and vital signs monitoring. The Internet of Medical Things (IoMT), which is a customized version of the Internet of Things (IoT), is increasingly important as it interconnects different medical devices, sensors, patients, and doctors, among others. This brings several benefits in improving health services. Nevertheless, in the IoMT environment, there are several challenges to overcome. Blockchain technology, a distributed ledger, with its immutability, transparency, and anonymity features, is being used in IoMT to help overcome these challenges. In this paper, a systematic review was carried out to identify the research topics of blockchain application in IoMT, the challenges in IoMT, how blockchain helps to overcome them, and the maturity stage of those works. The review results allowed us to identify five research topics in which the main ones are authentication and intrusion detection. This review shows an overview of current research on this subject, giving the possibility of directing other research works, or optimizing the existing ones.**

Keywords*— *IoMT, Internet of Medical Things Blockchain, healthcare, remote health monitoring

I. Introduction

Rapid population growth creates significant challenges for improving health care. Current health services are inefficient, face problems as lack of adequate treatment, high costs, and lack of human and medical resources [1]. These problems in the health sector were evidenced in the Covid 19 pandemic. Thousands of people were quarantined and did not have adequate medical attention. Developing smart, efficient, and safe health systems for people's better quality of life are necessary. A vital contribution to developing smart healthcare systems comes from emerging technologies such as the Internet of Things (IoT), blockchain, and edge computing [2]. Internet of Medical Things (IoMT) is being progressively applied in healthcare to provide real-time services to patients and doctors. IoMT is a personalized version of IoT. The IoT consists of four layers: application, platform, network, and device services. The IoT platform is an interface to process data generated and collected from devices. This platform is a single point of failure factor. Another issue in IoT is privacy, as devices collect sensitive data from users [3]. Blockchain technology can help tackle these problems. Blockchain is a distributed digital ledger where transactions are visible to participants. Through a dynamic consent protocol, users can grant, deny or revoke access to data for different reasons according to their interests. [4]. In this work, a systematic review of the literature was carried out to identify the current research topics of blockchain use in IoMT, the challenges in IoMT, how blockchain helps to overcome them, and the research maturity stage. In this way, we can direct new research topics or improve existing ones.

II. Methodology

This systematic review of the literature aimed to identify the current research focus on using blockchain in the Internet of Medical Things (IoMT). The following steps were performed to achieve this objective: definition of research questions searches in the database, exclusion criteria, and data extraction.

A. Definition of research questions

Three research questions (RQ) were defined:

RQ1: What are the research topics in IoMT that use blockchain?

RQ2: What are the challenges in IoMT and how does blockchain helps to overcome them?

RQ3: What is the research maturity stage?

B. Searches in the database

The searches were carried out in the Scopus database, looking for the keywords (blockchain OR "block chain") AND ("internet of medical things" OR iomt) in the title, abstract and keywords search fields. We set the search period from 2009 to August 2022 because the first blockchain-related publication was associated to bitcoin in 2008. This search returned 95 papers. Only papers in scientific journals were considered.

C. Exclusion criteria

The title and abstract of the 95 papers were revised to exclude:

- Papers that use blockchain but do not belong to the Internet of Medical Things.
- Review or analysis papers of blockchain application in Internet of Medical Things.

We don't consider review or analysis papers because our work focused on researches that are being developed, either proposal or implementation, of the use of blockchain in IoMT.

As a result of this process, 47 papers were excluded, remaining 48.

D. *Data extraction*

In this step, the abstracts and, if necessary, the complete document of the 48 remaining papers were used to extract data that answer the research questions. The following stages of maturity were considered: a) architectural proposal, b) simulation or experiments, c) implementation and d) real life application, that is, prototype or implementation that is or will be used in a real case.

III. Results

A. *RQ1: What are the research topics in IoMT that use blockchain?*

The identified research topics were authentication, intrusion detection, federated/deep learning, task scheduling, verification/certification, and other topics. Fig. 1 shows the distribution of the 48 papers by research topics. Authentication and intrusion detection includes the most significant number of publications, 23% (11) and 21% (10), respectively, followed by task scheduling, 13% (6). Federate learning/deep learning and verification/certification concentrate the least significant number of publications, 8% (4) and 6% (3), respectively. Other topics are the documents that do not form a pattern and they concentrate 29% (14) of the publications.

In the authentication topic, 5 researches use blockchain to authenticate IoMT devices, and the other 6 use blockchain and physically unclonable function (PUF). A brief description of each of them follows: a) blockchain-based authentication and key management protocol for IoMT environment, called BAKMP-IoMT: the scheme uses private blockchain, the healthcare data are stored in a blockchain maintained by the cloud servers [5]. b) Decentralized framework for authentication and access control in IoMT based on smart contracts and interplanetary file systems (IPFS): the framework use consortium blockchain, on Ethereum Ropsten network, and proof of identity [6].

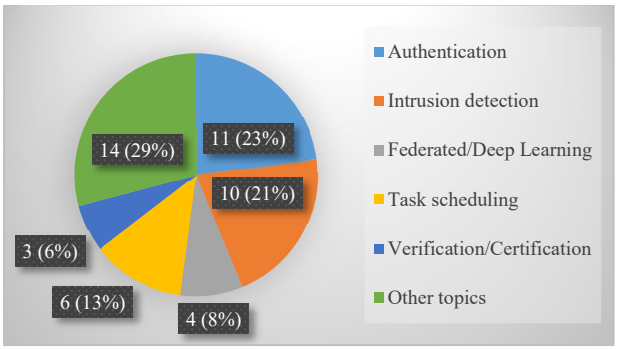

Fig. 1. Distribution of the selected 48 papers by research topics.

.

c) Framework based on blockchain and software guard extension (SGX) for a secure and trusted IoMT data analysis: the framework uses consortium blockchain to authenticate IoMT devices and for the IoMT data access control mechanism [7]. d) Three-layer framework, using blockchain and interplanetary file system (IPFS): the framework provides the authentication and authorization of patient and medical devices and the dissemination of patient and device information in the integrated blockchain network [8]. e) IoMT-Fog-Cloud architecture for a secure eHealth system the authentication scheme is based on context-aware CP-ABE (Ciphertext-Policy Attributed-Based Encryption) and blockchain [9]. f) Lightweight authentication protocol for wireless medical sensor networks (WMSNs) based on blockchain and physically unclonable functions (PUFs): the scheme supports dynamic identity updates per each authentication and key agreement [10]. g) Authentication scheme for IoMT devices based on smart contracts and PUF: the scheme is dedicated to solving the problem of copycat medical devices and securing the process of updating the firmware of these devices. The system is developed on a consortium blockchain [11]. h) The authors maintain that the work of the reference [10] authors have vulnerability issues and they propose a robust authentication protocol for wireless medical sensor networks (WMSN) based on smart contract and PUF [12]. i) Decentralized and scalable framework based on blockchain and PUFs for IoMT device authentication: the keys generated by PUFs are used to provide data encryption and device authentication. Smart contracts manage the access control. The framework is developed on Ethereum permissioned blockchain [13]. j) PUFchain 2.0, an IoMT security mechanism based on blockchain-assisted PUF for edge computing-drive smart healthcare: the PUF key is stored in a blockchain using blockchain consensus mechanism for IoMT device authentication [14]. k) Blockchain-assisted authentication framework for IoMT system in the fog computing architecture: the framework uses two authentication protocols, a PUF and an elliptic curve cryptography (ECC) [15].

In the intrusion detection topic, 4 researches use blockchain for attack detection in the IoMT environment and 6 researches use blockchain and, deep learning, federated learning or machine learning. A brief description of each publication follows: a) blockchain-based trust management scheme based on Bayesian inference, to detect malicious insider nodes, for IoMT devices, particularly medical smartphone networks (MSNs) [16]. b) Blockchain-enabled task offloading and resource allocation scheme for the WVMT (Wireless virtual reality (VR)-enabled medical treatment) system. The task offloading and resource allocation are formulated as a Markov decision problem, and to maximize the long-term system reward is proposed a collective reinforcement learning [17]. c) Blockchain-assisted secure data management framework (BSDMF) and Proof of Activity protocol, which uses malicious code detection algorithm, for IoMT data security [18]. d) PoW (proof of work) consensus with crypto hash algorithm to protect the sensitive information of the patient from malware attack in the IoMT environment [19]. The authors maintain that the last strategies, to distinguish illegal elements in BTC-cryptocurrency, use artificial intelligence (AI) and just focuses on a restricted class of this elements. For overcome those limitations, it's proposed the identification of illegal activities on bitcoin blockchain for IoMT executing a troupe of choice trees for managed learning

[20]. e) Blockchain-based deep learning framework for fog computing-based 5G-enabled IoMT. The framework uses smart contracts-based proof of work to achieve the security and privacy, and deep learning scheme with a variational autoencoder (VAE) technique for privacy and bidirectional long short-term memory (BiLSTM) for intrusion detection [21]. f) Biserial correlative Miyaguchi-Preneel blockchain-based Ruzicka deep multilayer perceptive learning (BCMPB-RIDMPL) technique for malware detection in IoMT. The technique improves the malware detection through the choice of processes of feature selection, blockchain, and classification [22]. g) KNN (K-Nearest neighbour) machine learning algorithm with smart contract for authentication and identifying the dynamic time attack detection in the IoMT environment [23]. h) Framework for misbehaviour detection in lightweight IoMT devices based on blockchain and federated learning (FL): the FL is supported by two layers of bidirectional long-short term memory (BiLSTM) to help with misbehaviour detection [24]. i) Malware detection scheme in IoMT devices based on machine learning and blockchain. j) Fuzzy C means (FMC) clustering algorithm is used to extract relevant malwares, decision tree-based support vector machine (SVM) is used to classify real data from malware, and the malware data is stored in blockchain to ensure dynamic detection [25].

In the federated/deep learning topic, blockchain is used for data security. Those researches, briefly described, are: a) architecture for IoMT based on multi-agent system (MAS) to ensure the security of private data and the addition/modification of the used machine learning solutions. The proposal combines blockchain and federated learning [26]. b) Secure image transmission, and diagnosis model for the IoMT environment based on blockchain and deep learning. The model includes a few processes: data acquisition. encryption and decryption, hash values compression, and classification process [27]. c) Cross-cluster federated learning (CFL) framework, using cross-chain technique. Large cluster are divided into multiple small clusters for geographically distant areas, and organized with a blockchain-based FL (BFL). CPL connects multiple BFL clusters, and only a few aggregated updates are transmitted across clusters. CPL focuses on a cross-chain consensus protocol [28]. d) Deep learning-based model for bone cancer detection classification. The model uses IoMT transfer learning to reduce the training time, and the privacy and integrity of patient data are preserved by implementing blockchain, fog computing, and edge computing [29].

In the task scheduling topic, to minimize service or execution costs, 6 publications belong to the same first author and only one publication is by other authors. A brief description of each them follows: a) IoMT framework to minimize the application cost during offloading and scheduling in the blockchain-based fog-cloud network. The proposal uses blockchain-enable smart-contract cost-efficient scheduling algorithm framework (BECSAF) [30]. b) Novel multi-criteria aware system using deep reinforcement and blockchain network, which can adapt to any situations, such as dynamic changes in wireless communication values, resource availability, and failure of any resource during the process of applications [31]. c) Cost-efficient system for IoMT that is based on the cost-efficient service selection and execution and blockchain-enabled serverless network. The system uses a function-based task scheduling blockchain-enable framework (FTSB) [32]. d) Schemes for bio-inspired robotic in the blockchain-fog-cloud-based IoMT environment. The IoMT includes workflow application for ankle bio-inspired healthcare sensors and blockchain-enabled fog-cloud computing nodes [33]. e) Novel BECSAF (Blockchain-Enabled Cost-Efficient Scheduling Algorithm Framework) to minimize latency and execution cost in the IoMT systems [34]. f) IoMT system, which uses scheduling techniques in blockchain, to supply cost effective healthcare services [35].

In the verification/certification topic, the publications are about batch verification, ciphertext authenticity verification and, search result certification. A brief description of them follows: a) large-scale batch verification scheme for Elliptic Curve Digital Signature Algorithm (ECDSA) for blockchain-enabled IoMT system, which identifies invalid signatures simultaneously, and also use two group testing algorithms, when the verification scheme returns a false result. Thus, the computing process is simplified and the overhead is reduced [36]. b) Blockchain-based profile matching framework in edge-based IoMT. KP-ABE (Key-policy attribute-based encryption) algorithm and smart contracts are used to achieve secure profile matching, and bloom filter based on many hash functions is designed to verify the authenticity of keyword ciphertext [37]. c) Blockchain-based framework for certifiable IoMT data search on smart medical systems, which are enabled to 5G and edge computing. A secure symmetric order-preserving encryption (OPE) technique is used for ensuring privacy during the search operation on an untrusted 5G Edge platform [38].

In other topics, publications that address different issues of blockchain used in IoMT were considered, and did not form a pattern. A brief description of each them follows: a) The authors perform an overview of blockchain technology and then propose an architecture for IoMT using blockchain to ensure the security of the data transmission across connected nodes [39]. b) Architecture for IoMT, which introduces the hybrid computing paradigm with the blockchain-based distributed data storage system to support low-latency services, also introduces the selective ring-based access control (SRAC), and patient anonymity and device authentication algorithms [40]. c) Decentralized health architecture, called BEdgeHealth, for data offloading and data sharing, which integrates blockchain, mobile-edge computing (MEC), smart contract, and IPFS in a distributed hospital network [41]. d) Blockchain-assisted secure data management framework (BSDMF) for IoMT-based health information. The BSDMF provides secure data management between personal servers and implantable devices and between cloud server and personal servers [42]. e) Multimodal secure data dissemination framework (MMSDDF) based on blockchain in IoMT. The proposal optimizes the data flow and secure patient data access control. The network of healthcare applications uses key blockchain [43]. f) IoMT and blockchain-based secured data sharing framework. The system uses IoMT devices interfaced with medical sensors to collect the patient vital parameters. A Markov chain model is used to monitor the patient medical states. Smart contracts accomplish the access control to patient data [44]. g) Blockchain-based fog computing architecture for IoMT. A security infrastructure into fog computing is provided using a block chain and the yet another consensus (YAC) protocol for storing and transferring IoMT data [45]. h) Medical cyber-physical system-enabled secure platform based on standard architecture, blockchain and IoMT. A proof of concept is presented, which captures

main vital signs from IoMT devices, where the data are secured in rest and during the transmission between associated nodes [46]. i) Model based on blockchain and, IoMT data of medical sensors and wearable devices, to detect stressful events of students [47]. Triple subject purpose-based access control (TS-PBAC) model to provide security and privacy-preserving in IoMT environment, the model is compatible with blockchain, and includes purpose and roles-based access control, policies of local differential privacy, and mutual evaluation of anonymous participants [48]. j) Private blockchain framework to store an individual physiological data of user in a distributed way. The system is implemented in a Raspberry Pi network, using proof of authority (PoA) consensus. Elliptic Curve Integrated Encryption Scheme is used to preserve the data confidentiality [49]. k) BIoMT, a blockchain hyperledger-fabric-enabled consortium serverless network platform for IoMT environment, to reduce the consumption of resources, such as computation, network and storage, and to provide an ecosystem more reliable. NuCypher Re-Encryption mechanism is used to protect the privacy of individual health transactions before sharing. [50]. l) Blockchain-based IoMT using consensus algorithm of Practical Byzantine Fault Tolerance with proof of work (PBFT-PoW) for secure data storage. The data are collected from wearable devices and stored in the cloud network [51]. m) FAITH, a Fast blockchain supported edge computing platform for healthcare 4.0 in IoMT. The platform is addressed for time-sensitive healthcare applications, blockchain and job orchestration are integrated to secure and accelerate the system [52].

B. *RQ2: What are the challenges in IoMT and how does blockchain helps to overcome them?*

The biggest challenges in the IoMT environment are security and privacy. Of the 48 publications, 22 focus on the security issue, 19 on security and privacy, and 7 on service or execution costs. The answer to RQ1 question shows how these challenges are faced using the blockchain, and in many cases, together with other disruptive technologies. Security and privacy are addressed through of authentication, intrusion detection, verification/certification and access control. Service or execution costs are faced mainly by task scheduling.

Fig 2 shows a co-occurrence network of keywords, generated from the 48 papers, using VOSViewer [53]. This network presents the keywords more used by the sampled set. Blockchain, security, iomt, internet of medical things and privacy are the words with the most weight, but we can also observe other words such as authentication, smart contracts, access control, malware detection, edge computing, among others, as well as the connections among them. Some words represent the challenges and other, the solutions for the IoMT environment. The word security is the most weight after the word blockchain, which shows that the biggest concern is related to security in IoMT and this challenge is faced using blockchain.

C. *RQ3: What is the research maturity stage?*

Fig. 3 shows the maturity stage of the 48 researches. We can see that 73% (35) are in the simulation or experiments stage, 25% (12) are in the implementation stage, 2% (1) are in the architectural proposal stage, and there is no real-life application publication.

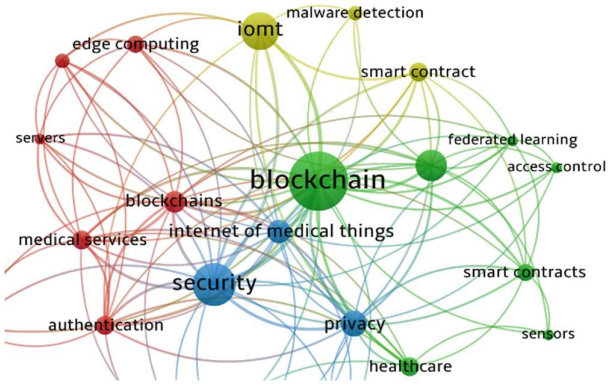

Fig. 2. Co-occurrence Network of keywords from the selected 48 papers.

To better observe the maturity stage of the researches, Fig. 4 shows the number of publications per year and maturity stage. In 2019 there was the first publication. It is the one that is in the architecture proposal stage. In 2020, there were two publications. They are in the simulation or experiments stage. In 2021 there was a considerable increase, 23 publications, 16 on which are in the simulation or experiments stage and 7 are in the implementation stage. And until August of 2022 there were already 22 publications, 17 on which are in the simulation or experiments stage and 5 are in the implementation stage. These data show that researches in this field are at an early stage and they are recent.

IV. Discussion

The systematic review results revealed that research is more focused on using blockchain for authentication and intrusion detection in the IoMT environment. There are few pieces of research concerning execution cost and cost of services. There is also a lack of research on case studies. For now, attention is focused on solving security and privacy challenges.

The results also show that research on blockchain usage in IoMT is recent and at an early stage. The number of publications has grown enormously since 2021. Perhaps this increase is related to the Covid 19 pandemic as, with isolation, remote medical care has become necessary. This sudden increase in publications also shows that blockchain has aroused great expectations of its use in IoMT.

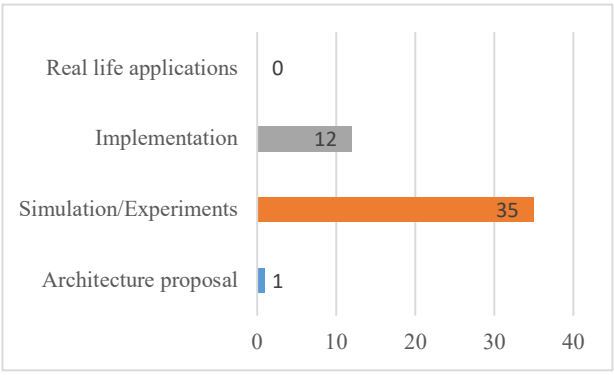

Fig. 3. Number of publications by maturity stage.

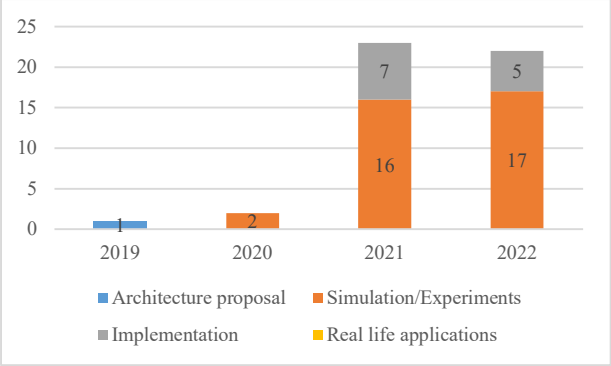

Fig. 4. Number of Publications per year (2022, publications until August) and maturity stage.

Several literature reviews on the use of blockchain in IoMT were carried out focusing on: privacy and security [54], blockchain scalability issues in the IoMT environment [55], and security of IoMT edge networks to healthcare monitoring [56]. This systematic review, on the other hand, highlights the research topics of blockchain use in the IoMT environment, the challenges in IoMT and how the blockchain is used to face these issues. In addition, it also presents a brief description of each of the publications and shows the maturity stage of researches.

V. Conclusions

This systematic review highlights five research topics on blockchain use in IoMT: authentication, intrusion detection, federated/deep learning, task scheduling, and verification/certification. The topics that concentrate the most significant number of research are authentication and intrusion detection, and there are few pieces of research related to the cost of services and execution. The biggest challenges in the IoMT environment are security and privacy, and blockchain addresses these challenges. The review also shows that this research field is at an early stage. The most significant number of research is in the simulation or experiments stage. The first publication was in 2019. In 2021 and 2022, the publications suddenly increased, which shows a high expectation of using blockchain in IoMT. Thus, this review reveals an overview of current research on blockchain use in IoMT, which may allow directing other research or improving existing ones.

Acknowledgment

This study was supported by the UBRI (University Blockchain Research Initiative) of Ripple company via Silicon Valley Community Foundation.

References

[1] S. Ramzan, A. Aqdus, V. Ravi, D. Koundal, R. Amin, and M. A. Al, "Healthcare applications using blockchain technology : motivations and challenges," *IEEE Trans. Eng. Manag.*, in press.

[2] A. A. Abdellatif, A. Z. Al-Marridi, A. Mohamed, A. Erbad, C. F. Chiasserini, and A. Refaey, "SsHealth: toward secure, blockchain-enabled healthcare systems," *IEEE Netw.*, vol. 34, no. 4, pp. 312–319, 2020.

[3] S. Jeong, J. H. Shen, and B. Ahn, "A study on smart healthcare monitoring using IoT based on blockchain," *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021.

[4] H. Al-Aswad, W. M. El-Medany, C. Balakrishna, N. Ababneh, and K. Curran, "BZKP: blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation," *Arab J. Basic Appl. Sci.*, vol. 28, no. 1, pp. 154–171, 2021.

[5] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. 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. 95956–95977, 2020.

[6] 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," *J. Supercomput.*, vol. 77, no. 8, pp. 7916–7955, 2021.

[7] Y. Gao, H. Lin, Y. Chen, and Y. Liu, "Blockchain and SGX-enabled edge-computing-empowered secure IoMT data analysis," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15785–15795, 2021.

[8] A. Mehbodniya, R. Neware, S. Vyas, M. R. Kumar, P. Ngulube, and S. Ray, "Blockchain and IPFS integrated framework in bilevel fog-cloud network for security and privacy of IoMT devices," *Comput. Math. Methods Med.*, vol. 2021, 2021.

[9] B. Annane, A. Alti, and A. Lakehal, "Blockchain based context-aware CP-ABE schema for internet of medical things security," *Array*, vol. 14, no. February, p. 100150, 2022.

[10] W. Wang *et al.*, "Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8883–8891, 2022.

[11] R. Akkaoui, "Blockchain for the management of internet of things devices in the medical Industry," *IEEE Trans. Eng. Manag.*, vol. PP, pp. 1–12, 2021.

[12] S. Yu and Y. Park, "A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions," *IEEE Internet Things J.*, vol. 4662, no. c, pp. 1–15, 2022.

[13] K. P. Satamraju and B. Malarkodi, "A decentralized framework for device authentication and data security in the next generation internet of medical things," *Comput. Commun.*, vol. 180, no. August, pp. 146–160, 2021.

[14] V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: hardware-assisted robust blockchain for sustainable simultaneous device and data Security in smart healthcare," *SN Comput. Sci.*, vol. 3, no. 5, 2022.

[15] X. Jia, M. Luo, H. Wang, J. Shen, and D. He, "A Blockchain-assisted privacy-aware authentication scheme for internet of medical things," *IEEE Internet Things J.*, pp. 1–13, 2022.

[16] W. Meng, W. Li, and L. Zhu, "Enhancing medical smartphone networks via blockchain-based trust management against insider attacks," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1377–1386, 2020.

[17] P. Lin, Q. Song, F. R. Yu, D. Wang, and L. Guo, "Task offloading for wireless VR-enabled medical treatment with blockchain security using collective reinforcement learning," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15749–15761, 2021.

[18] R. Rajadevi, K. Venkatachalam, M. Masud, M. A. AlZain, and M. Abouhawwash, "Proof of activity protocol for IoMT data security," *Comput. Syst. Sci. Eng.*, vol. 44, no. 1, pp. 339–350, 2023.

[19] R. Punithavathi, K. Venkatachalam, M. Masud, M. A. Alzain, and M. Abouhawwash, "Crypto hash based malware detection in IoMT framework," *Intell. Autom. Soft Comput.*, vol. 34, no. 1, pp. 559–574, 2022.

[20] A. Kumar, K. Abhishek, P. Nerurkar, M. R. Khosravi, M. R. Ghalib, and A. Shankar, "Big data analytics to identify illegal activities on bitcoin blockchain for IoMT," *Pers. Ubiquitous Comput.*, 2021.

[21] M. A. Almaiah, A. Ali, F. Hajjej, M. F. Pasha, and M. A. Alohali, "A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things," *Sensors*, vol. 22, no. 6, 2022.

[22] A. S. Alotaibi, "Biserial miyaguchi–preneel blockchain-based ruzicka-indexed deep perceptive learning for malware detection in iomt," *Sensors*, vol. 21, no. 21, 2021.

[23] Y. D. Al-Otaibi, "K-nearest neighbour-based smart contract for internet of medical things security using blockchain," *Comput. Electr. Eng.*, vol. 101, no. January, p. 108129, 2022.

[24] S. Rahmadika, P. V. Astillo, G. Choudhary, D. G. Duguma, V. Sharma, and I. You, "Blockchain-based privacy preservation scheme for misbehavior detection in lightweight IoMT devices," *IEEE J. Biomed. Heal. Informatics*, vol. XX, no. Xx, pp. 1–12, 2022.

[25] A. M. Hilal *et al.*, "Malware detection using decision tree based SVM classifier for IoT," *Comput. Mater. Contin.*, vol. 72, no. 1, pp. 713–726, 2022.

[26] D. Połap, G. Srivastava, and K. Yu, "Agent architecture of an intelligent medical system based on federated learning and blockchain technology," *J. Inf. Secur. Appl.*, vol. 58, no. February, p. 102748, 2021.

[27] B. A. Y. 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," *Pers. Ubiquitous Comput.*, 2021.

[28] H. Jin, X. Dai, J. Xiao, B. Li, H. Li, and Y. Zhang, "Cross-cluster federated learning and blockchain for internet of medical things," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15776–15784, 2021.

[29] M. U. Nasir, S. Khan, S. Mehmood, M. A. Khan, A. u. Rahman, and S. O. Hwang, "IoMT-based osteosarcoma cancer detection in histopathology images using transfer learning empowered with blockchain , fog computing , and edge computing," *Sensors (Switzerland)*, vol. 22, no. 14, 2022.

[30] A. Lakhan *et al.*, "Smart-contract aware ethereum and client-fog-cloud healthcare system," *Sensors*, vol. 21, no. 12, pp. 1–21, 2021.

[31] A. Lakhan, M. A. Mohammed, S. Kozlov, and J. J. P. C. Rodrigues, "Mobile-fog-cloud assisted deep reinforcement learning and blockchain-enable IoMT system for healthcare workflows," *Trans. Emerg. Telecommun. Technol.*, no. August, pp. 1–17, 2021.

[32] A. Lakhan *et al.*, "Cost-efficient service selection and execution and blockchain-enabled serverless network for internet of medical things," *Math. Biosci. Eng.*, vol. 18, no. 6, pp. 7344–7362, 2021.

[33] A. lakhan, M. A. Mohammed, D. A. Ibrahim, and K. H. Abdulkareem, "Bio-inspired robotics enabled schemes in blockchain-fog-cloud assisted IoMT environment," *J. King Saud Univ. - Comput. Inf. Sci.*, in press.

[34] A. Lakhan, M. A. Mohammed, M. Elhoseny, M. D. Alshehri, and K. H. Abdulkareem, "Blockchain multi-objective optimization approach-enabled secure and cost-efficient scheduling for the internet of medical things (IoMT) in fog-cloud system," *Soft Comput.*, vol. 26, no. 13, pp. 6429–6442, 2022.

[35] G. Ravikumar, K. Venkatachalam, M. Masud, and M. Abouhawwash, "Cost efficient scheduling using smart contract cognizant ethereum for IoMT," *Intell. Autom. Soft Comput.*, vol. 33, no. 2, pp. 865–877, 2022.

[36] H. Xiong *et al.*, "On the design of blockchain-based ECDSA with fault-tolerant batch verification protocol for blockchain-enabled IoMT," *IEEE J. Biomed. Heal. Informatics*, vol. 26, no. 5, pp. 1977–1986, 2022.

[37] X. Nie, A. Zhang, J. Chen, Y. Qu, and S. Yu, "Blockchain-empowered secure and privacy-preserving health data sharing in edge-based IoMT," *Secur. Commun. Networks*, vol. 2022, no. 1, 2022.

[38] M. S. Rahman, A. Alabdulatif, and I. Khalil, "Privacy aware internet of medical things data certification framework on healthcare blockchain of 5G edge," *Comput. Commun.*, vol. 192, no. May, pp. 373–381, 2022.

[39] N. Dilawar, M. Rizwan, F. Ahmad, and S. Akram, "Blockchain: securing internet of medical things (IoMT)," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 1, pp. 82–89, 2019.

[40] B. S. Egala, A. K. Pradhan, V. 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 Things J.*, vol. 8, no. 14, pp. 11717–11731, 2021.

[41] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "BEdgeHealth: a decentralized architecture for edge-based IoMT networks using blockchain," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11743–11757, 2021.

[42] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, "Correction to: blockchain-assisted secured data management framework for health information analysis based on internet of medical things (Personal and Ubiquitous Computing, (2021), 10.1007/s00779-021-01583-8)," *Pers. Ubiquitous Comput.*, in press.

[43] R. Arul, Y. D. Al-Otaibi, W. S. Alnumay, U. Tariq, U. Shoaib, and M. D. J. Piran, "Multi-modal secure healthcare data dissemination framework using blockchain in IoMT," *Pers. Ubiquitous Comput.*, in press.

[44] M. Z. U. Rahman, S. Surekha, K. P. Satamraju, S. S. Mirza, and A. Lay-Ekuakille, "A collateral sensor data sharing framenwork for decentralized healthcare systems," *IEEE Sens. J.*, vol. 21, no. 24, pp. 27848–27857, 2021.

[45] M. AI Duhayyim *et al.*, "Integration of fog computing for health record management using blockchain technology," *Comput. Mater. Contin.*, vol. 71, no. 2, pp. 4135–4149, 2022.

[46] M. Elsayeh, K. A. Ezzat, H. El-Nashar, and L. N. Omran, "Cybersecurity architecture for the internet of medical things and connected devices using blockchain," *Biomed. Eng. - Appl. Basis Commun.*, vol. 33, no. 2, pp. 1–14, 2021.

[47] N. Ersotelos *et al.*, "Blockchain and iomt against physical abuse: bullying in schools as a case study," *J. Sens. Actuator Networks*, vol. 10, no. 1, 2021.

[48] G. Wu, S. Wang, Z. Ning, and J. Li, "Blockchain-enabled privacy-preserving access control for data publishing and sharing in the internet of medical things," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8091–8104, 2022.

[49] D. Mohan, L. Alwin, P. Neeraja, K. D. Lawrence, and V. Pathari, "A private ethereum blockchain implementation for secure data handling in internet of medical things," *J. Reliab. Intell. Environ.*, in press.

[50] A. A. Khan, A. A. Wagan, A. A. Laghari, A. R. Gilal, I. A. Aziz, and B. A. Talpur, "BIoMT : a state-of-the-art consortium serverless network architecture for healthcare system using blockchain smart contracts," *IEEE Access*, vol. 10, no. August, pp. 78887–78898, 2022.

[51] D. Palanikkumar, A. Fahad Alrasheedi, P. Parthasarathi, S. S. Askar, and M. Abouhawwash, "Hybrid smart contracts for securing IoMT data," *Comput. Syst. Sci. Eng.*, vol. 44, no. 1, pp. 457–469, 2023.

[52] Z. Ming, M. Zhou, L. Cui, and S. Yang, "FAITH: a fast blockchain-assisted edge computing platform for healthcare applications," *IEEE Trans. Ind. Informatics*, vol. 3203, no. c, pp. 1–10, 2022.

[53] N. J. van Eck and L. Waltman, "VOSviewer manual version 1.6.16," *Univeristeit Leiden*, unpublished.

[54] T. Vaiyapuri, A. Binbusayyis, and V. Varadarajan, "Security, privacy and trust in iomt enabled smart healthcare system: a systematic review of current and future trends," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 2, pp. 731–737, 2021.

[55] A. Adavoudi Jolfaei, S. F. Aghili, and D. Singelee, "A survey on blockchain-based iomt systems: towards scalability," *IEEE Access*, vol. 9, pp. 148948–148975, 2021.

[56] F. Pelekoudas-Oikonomou *et al.*, "Blockchain-based security mechanisms for IoMT edge networks in IoMT-based healthcare monitoring systems," *Sensors*, vol. 22, no. 7, 2022.