Is blockchain for Internet of Medical Things a panacea for COVID-19 pandemic?

Xuran Li [a], Bishenghui Tao [b], Hong-Ning Dai [c,*], Muhammad Imran [d], Dehuan Wan [e], Dengwang Li [a]

[a] *Shandong Key Laboratory of Medical Physics and Image Processing, School of Physics and Electronics, Shandong Normal University, Jinan, Shandong, China*
[b] *Faculty of Information Technology, Macau University of Science and Technology, Macau SAR, China*
[c] *Department of Computing and Decision Sciences, Lingnan University, Hong Kong SAR, China*
[d] *College of Applied Computer Science, King Saud University, Riyadh, Saudi Arabia*
[e] *Guangdong University of Finance, Guangzhou, China*

ARTICLE INFO

ABSTRACT

The outbreak of the COVID-19 pandemic has deeply influenced the lifestyle of the general public and the healthcare system of the society. As a promising approach to address the emerging challenges caused by the epidemic of infectious diseases like COVID-19, Internet of Medical Things (IoMT) deployed in hospitals, clinics, and healthcare centers can save the diagnosis time and improve the efficiency of medical resources though privacy and security concerns of IoMT stall the wide adoption. In order to tackle the privacy, security, and interoperability issues of IoMT, we propose a framework of blockchain-enabled IoMT by introducing blockchain to incumbent IoMT systems. In this paper, we review the benefits of this architecture and illustrate the opportunities brought by blockchain-enabled IoMT. We also provide use cases of blockchain-enabled IoMT on fighting against the COVID-19 pandemic, including the prevention of infectious diseases, location sharing and contact tracing, and the supply chain of injectable medicines. We also outline future work in this area.

© 2021 Elsevier B.V. All rights reserved.

1. Introduction

Since the year 2020, the whole world has been struggling to fight against the spread of the new coronavirus disease called SARS-CoV-2 (aka, COVID-19). COVID-19 is a dangerous respiratory infection that rapidly spreads from humans to humans. Even though many countries are sparing their efforts to slow down or control the outbreaks of COVID-19 and gradually restore regular lives, we still have a long way to go before the COVID-19 pandemic being fully solved. The widespread of the COVID-19 pandemic has led to an adverse influence on almost all aspects of human life and has also exposed the limitations on medical sources of the current healthcare systems.

Since the emergence of the COVID-19 pandemic, substantial efforts have been paid on exploiting technological advances to effectively fight against this disease. Among all these technologies, the Internet of Medical Things (IoMT) is one of the most promising approaches to help to prevent the widespread of this infectious disease [1,2]. IoMT is a

---

* Corresponding author.
 E-mail addresses: sdnulxr@sdnu.edu.cn (X. Li), 2009853YII30001@student.must.edu.mo (B. Tao), hndai@ieee.org (H.-N. Dai), dr.m.imran@ieee.org (M. Imran), wan_e@gduf.edu.cn (D. Wan), dengwang@sdnu.edu.cn (D. Li).

remote healthcare system, which is mainly composed of medical sensor devices, medical data servers, and professional medical staff (i.e., doctors, nurses, and so on). The medical sensor devices (including various biomedical sensors, RFID tags, and QR tags) collect the medical data of patients and then transmit the data to medical data servers. The authorized professional medical staff can then access the medical data, conduct an early diagnosis, and provide medical therapy measures. Meanwhile, IoMT can monitor the status of patients so as to provide professional medical support.

The wide adoption of IoMT systems to incumbent medical institutions and agencies brings potentials to address the COVID-19 pandemic. First, the time of waiting for an early diagnosis can be saved. The early diagnosis for COVID-19 is necessary since the contagiousness rate of COVID-19 is very high [3]. However, the medical resources (such as hospitals and doctors) are limited and the chances of early diagnosis for many patients are missed. When physiological data of a potential patient is collected by medical sensor devices, the professional medical staff can soon diagnose if the potential patient is infected. Second, monitoring patients with medical sensors can reduce the possibility of medical staff being infected. The possibility of direct contact between patients and medical staff can be minimized with IoMT-enabled remote healthcare service. Last but not least, limited medical resources can be saved. When a patient gets out of emergency status and only needs more rest for recovery, the medical staff can monitor this patient at given time intervals with the help of IoMT. The constrained medical resources (i.e., hospital beds, medical devices, and medical staff) can be saved for those patients in emergency status.

Though the adoption of IoMT is beneficial to combat COVID-19, there are some challenges to be solved before IoMT can be widely deployed. Due to the limited computing capability and battery capacity, complicated encryption algorithms are not feasible for most wearable or implanted medical sensor devices. Consequently, wireless data transmission of IoMT can be vulnerable to external attacks [4,5]. Since medical data contains sensitive personal information of patients, it is crucial to allow the authorized users to access the medical data while preserving the privacy of patients [6]. In addition, there are diverse types of medical sensor devices [7] and heterogeneous IoMT networks, thereby leading to the poor interoperability of IoMT.

One promising solution to the aforementioned challenges is integrating blockchain with IoMT [2,8,9]. The inherent nature of blockchain includes decentralization, trustworthiness, traceability, and transparency. Therefore, blockchain can potentially address the security, privacy, and interoperability challenges [10,11]. Firstly, the decentralized blockchain can protect the sensitive medical data of patients from being fully controlled by third-party entities. Secondly, the decentralization of blockchain can also avoid the single point of failure and mitigate the bottleneck at central servers due to the increasing number of medical sensor devices. Thirdly, blockchain-based IoMT can guarantee the security and traceability of IoMT data because the contents on the blockchain will not be controlled by any single entity, and the medical data as well as event logs stored on the blockchain are immutable [12]. Fourthly, the decentralized peer-to-peer (P2P) network architecture can help to process the heterogeneous IoMT data and improve the interoperability of IoMT.

The convergence of blockchain and IoMT may improve the security of IoMT, enhanced the privacy protection of IoMT data, and ameliorate the interoperability of IoMT systems. Hence, we explore the convergence of blockchain and IoMT in this paper. In particular, we propose a framework for integrating blockchain with IoMT, investigate the solutions of blockchain-enabled IoMT to tackle the COVID-19 pandemic, discuss the potential applications of blockchain-enabled IoMT, and outline future directions in blockchain-enabled IoMT. The main contributions of this paper are summarized as follows:

- We present the technical overview of blockchain and IoMT. Specifically, we introduce the blockchain structure, consensus algorithms, smart contract, and categories of blockchain systems.
- We propose a framework of integrating blockchain with IoMT and analyze the potentials brought by this framework. In particular, blockchain helps to improve the security of IoMT, enhance privacy protection of IoMT, and ameliorate the interoperability of IoMT systems.
- We provide use cases of blockchain-enabled IoMT in combating the COVID-19 pandemic, including the prevention of infectious diseases, location sharing and contact tracing, and the supply chain of injectable medicines.

The rest of this paper is organized as follows. Section 2 provides related studies in literature. Section 3 presents the technological review of blockchain and IoMT. Section 4 introduces an architecture of blockchain-enabled IoMT. The case studies of blockchain-enabled IoMT are provided in Section 5. The future directions are summarized in Section 6. Section 7 concludes this paper. Please refer to Fig. 1 for the organization of the entire paper.

2. Related work

The outbreak of the COVID-19 pandemic has brought severe influence on the whole world due to the high infectiousness of COVID-19. One of the potential solutions to address the COVID-19 pandemic is deploying IoMT across medical institutions as well as communities. The authors in [13] present a comparison between the traditional medical ecosystem and IoMT medical ecosystem and discuss the applications of IoMT systems in combating COVID-19 in different countries. In another work [14], a point-of-care diagnostics-based IoMT platform is proposed for patients infected by COVID-19. With this platform, the patients can dynamically monitor the disease status themselves and receiving medical support without spreading the virus. Meanwhile, the IoMT system for providing medical support to orthopedic patients with limited mobility during this COVID-19 pandemic environment is designed in [15]. However, most medical sensor devices in IoMT systems are limited in terms of computing capability and battery capacity. Moreover, there are heterogeneous
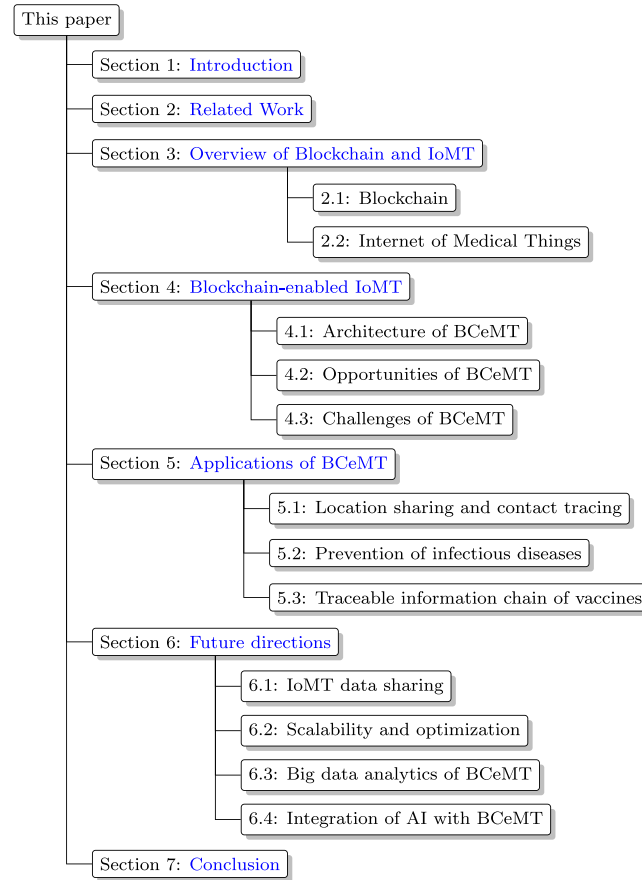
Fig. 1. Structural diagram of the paper.

types of medical sensor devices, leading to the complexity of the IoMT system. The main challenges of deploying the IoMT lie in 1) difficulty in assuring the security of patient's data and 2) the poor interoperability between medical sensor devices.

One promising solution for addressing these challenges of the IoMT system is blockchain. The research [16] presents a blockchain-enabled framework for digital contact-tracing applications in the COVID-19 pandemic. In this framework, both the trust and privacy of users are guaranteed by the blockchain. Another research investigates enhancing the security and privacy of medical systems with blockchain in [17]. In this research, the blockchain and interplanetary file systems are utilized for constructing the security and privacy framework of IoMT. The authors in [18] investigate the performance improvement of the blockchain network and present the system architecture of utilizing blockchain in IoMT. They develop a smartphone app for the automation of medical records based on their proposed architecture. The integration of blockchain and IoMT is also investigated in [19]. In this research, a data-flow architecture is proposed for the integration of blockchain and IoMT, and the corresponding use cases are presented.

Considering the limitation of the storage capability of blockchain and the massive amount of physiological data collected from patients, the integration of cloud-assisted wireless body area network (WBAN) with blockchain in the smart medical system is investigated in studies [20–22]. In [20], a blockchain-enabled storage mechanism in the cloud-assisted WBAN is proposed. Meanwhile, the authors in [21] investigate a telecare medical information system, which is implemented in the cloud-assisted WBAN. To guarantee the security of patient health data, they also design the blockchain-based authentication protocol for this system. The work [22] investigates a cloud-assisted WBAN enabled remote patient monitoring system. In this system, they designed a lightweight consensus mechanism based on blockchain.

Different from the aforementioned researches, this paper proposes the framework of integrating blockchain with IoMT and analyzes the potential brought by this framework, especially in the context of COVID-19. In addition, we provide use cases of this framework in combating the COVID-19 pandemic, including the prevention of infectious diseases, location sharing and contact tracing, and the supply chain of injectable medicines. The comparison of the related studies with this paper is shown in Table 1.

Table 1
The comparison of related works with this work.

References	Main contributions	Blockchain	IoMT	Integrating blockchain with IoMT	Use cases in combating COVID-19
[13]	Presenting the architecture of the IoMT medical ecosystem and the applications of IoMT systems in combating COVID-19	×	✓	×	✓
[14]	Proposing a point-of-care diagnostics based IoMT platform for COVID-19 diagnosis and monitoring	×	✓	×	✓
[15]	Proposing the IoMT system for mobility restricted orthopedic patients during COVID-19 pandemic	×	✓	×	✓
[16]	Proposing a privacy-preserving framework for contact tracing based on the blockchain	✓	×	×	✓
[17]	Designing and implemented the security and privacy IoMT framework based on the blockchain and interplanetary file system	✓	✓	✓	×
[18]	Presenting a system architecture of integrated blockchain with IoMT and developed an app based on this architecture	✓	✓	✓	×
[19]	Proposing a data-flow architecture for the integration of blockchain and IoMT and presenting the use cases	✓	✓	✓	×
[20]	Proposing a blockchain-enabled storage mechanism in the cloud-assisted WBAN	✓	✓	✓	×
[21]	Designing the authentication protocol for the system integrating cloud-assisted WBAN with blockchain	✓	✓	✓	×
[22]	Proposing a blockchain-based lightweight consensus mechanism for a cloud-assisted WBAN enabled remote patient monitoring system	✓	✓	✓	×
This paper	Proposing a framework of integrating blockchain with IoMT and analyze the potentials brought by this framework, presenting use cases in combating the COVID-19 pandemic	✓	✓	✓	✓

3. Overview of blockchain and IoMT

This section presents a technical overview on both blockchain and IoMT.

3.1. Blockchain

In 2009, Nakamoto put forward Bitcoin, this brand new digital currency without any authoritative intermediary's coordination. In the system of Bitcoin, people who do not trust each other can directly make deal with this cryptocurrency [23]. In December 2013, a new blockchain-framework platform Ethereum was proposed by Buterin [24]. In addition to the built-in algorithms based on digital currency transactions, Ethereum also provides the Turing-complete programming language for the smart contract, which was the first applied to the blockchain.

The blockchain has a distinctive data structure. Information is encapsulated into every single block, and the blocks are sequentially combined into a chain. Block cipher is used to ensure that the data cannot be altered and forged. The system is decentralized, implying that there is no central node in the network of blockchain. Thus, any two nodes can trade with each other directly. Hence, blockchain networks mostly choose P2P protocol as the network transmission protocol. In this way, the blockchain system can be totally distributed so that the failures of a single point are tolerated.

The nodes in the blockchain network generally have key characteristics of equality, autonomy, distribution, and so on [25,26]. Moreover, as shown in Fig. 2, every node can freely join or depart from this system. During the information propagation, every single node always listens to the broadcasting messages in the network. Once a node receives a new transaction or block from neighbor peers, the broadcast message will be verified. The message includes a digital signature, proof of work, hash value, and so on. In order to prevent the invalid data from recording, only when the verification of the information has been to a consensus, the message would be encrypted and appended into the blockchain.

3.1.1. Blockchain structure

The structure of a blockchain is built as a connected block list. In this chain-like list, every single block has a hash pointing to the previous one. A correct (or confirmed) chain contains a complete block list and the transactions. It is available for every node to download and maintain the chain, implying that the blockchain system acts like a distributed public ledger. Fig. 3 presents an instance of the blockchain structure. Each block in a chain consists of a block body and a block header, with a hash pointer contained in the header pointing to its prior block, which is also called its parent
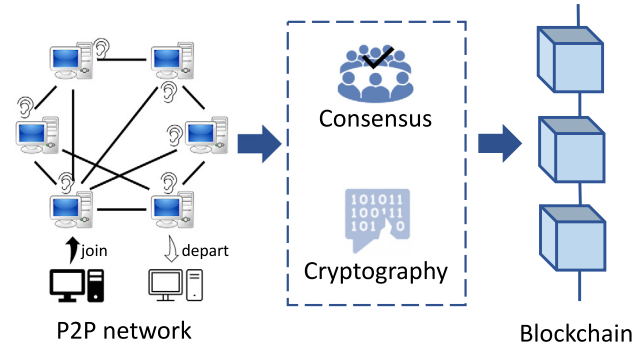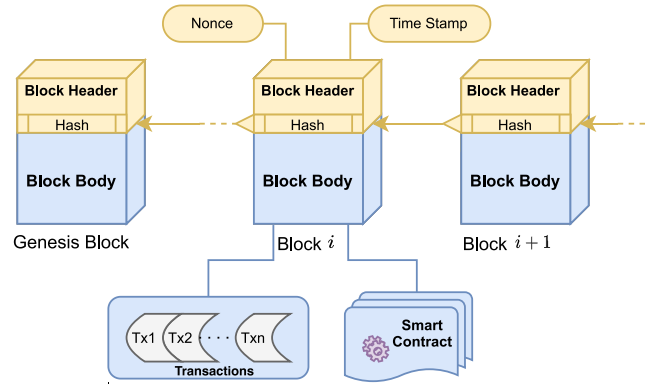
Fig. 2. Blockchain system.

Fig. 3. Blockchain structure.

Table 2
An example of block header components and description.

Components	Description
Block Version	Indicates which version of protocol and validation rules that the block defers to.
Merkle Tree Root Hash	The hash value of every transaction within the block.
Time Stamp	Current time as seconds in universal time since January 1, 1970.
nBits	Current hashing target in a compact format.
Nonce	Random number, usually starts with 0 and increases for every hash calculation.
Previous block hash	A 256-bit hash value of the previous block.

block. And the initial block which does not have any parent block is also called genesis block [25]. Some information for identification and marking will be stored in the block header, such as Nonce and Time Stamp. Meanwhile, the majority of complete data is stored in the block body, such as transaction data, smart contracts, etc.

A block contains a block header and a block body. Generally, as listed in Table 2, a block header includes a block version, Merkle tree root hash, timestamp, nBits, nonce, and the previous block hash [27]. It is worth mentioning that the information in the block cannot be modified by others with a hash pointer in the block header. The block body contains validated transactions as well as a transaction counter. Take the Bitcoin block as an example. The maximum size of a single block is defined as 1 MB and a transaction usually has a size of around 250 bytes. Thus, each block has a limit of 4,000 transactions. According to the real-time data of the Blockchain Explorer, the recent number of transactions of Bitcoin is about 2,000 transactions per block [28]. Moreover, the average Ethereum block size is between 20 to 30 KB mostly [29].

3.1.2. Consensus algorithms

Various consensus algorithms are deployed to determine how to achieve agreement when verifying and recording new transactions and blocks. An efficient consensus mechanism needs to allow all participants to reach an agreement in a non-trusted environment and maintain the system under a good fault tolerance. There are different consensus algorithms in different platforms. As the first and the widest deployed consensus mechanism, the Proof of Work (PoW) introduced by the Bitcoin network assumes that all candidates take part in racing with their computing power, to find a required nonce value to construct the right block [23]. PoW guarantees a decentralized network and a public ledger system for trustless entities dealing with each other. However, PoW suffers from excessive power consumption.

Proof of Stake (PoS) can potentially overcome the drawbacks of PoW. The PoS comes from the concept that the more stake coins a node has, the higher chance it can fabricate the new block [30]. Therefore, nodes with more tokens are generally believed to be more inclined to maintain the security of the network in order to protect their own rights. PoS avoids a massive consumption of computing power, thereby being more energy-efficient than PoW. However, PoS still confronts the risk of attacks due to its low mining cost.

Delegated proof of stake (DPoS) is an extension of the PoS. This consensus protocol supports the users who have stakes to vote the delegate or witnesses, to build the blocks and chain, or change the parameters of the network. DPoS demonstrates better operational efficiency and double-spending attack protection. However, DPoS can result in a centralized network due to a limited number of selected delegates.

To protect the system from the attacks of potential malicious nodes, Hyperledger Fabric [31] utilizes the Practical byzantine fault tolerance(PBFT) [32]. In PBFT, replications among nodes reach consensus despite the failing or incorrect information propagation in the distributed network so as to enable the Byzantine faults tolerance. Moreover, after introducing the idea of voting nodes to record the transactions, delegated byzantine fault tolerance (DBFT) is implemented for saving communication consumption. In addition, Ripple protocol requires less trust to maintain the consensus with low latency, by utilizing collectively-trusted subnetworks from the larger network [33], thereby showing robustness when facing the Byzantine failures.

3.1.3. Smart contract

A smart contract is a protocol or a computing program deployed on the blockchain to automatically execute, control, or verify actions under the agreement between different parties. The conception of the smart contract was first proposed by Szabo in the 1996 [34] to reduce the requirement of trust, cost of enforcement, and exceptions of malicious attacks during the transaction. On top of the blockchain system, every user can call and interact with smart contracts to conduct various business activities, such as making transactions with others, receiving and sending messages, and voting activities [35]. Smart contracts share similar characteristics to the blockchain, such as distribution, decentralization, and immutability. Once a smart contract is deployed, no one can modify it, ensuring the security of transactions and systems. For an instance, Ethereum implements smart contracts in various computer languages like Solidity, Serpent, or LLL [36]. When a smart contract is called, it will run immediately in the content of an Ethereum Virtual Machine (EVM) on the decentralized network computers.

3.1.4. Categories of blockchain systems

The current blockchain systems can be categorized as public blockchains, private blockchains, and consortium blockchains. The access permission and network properties vary from different blockchain systems. we next briefly describe three typical blockchain systems.

Public Blockchains: Every user within a public blockchain system can freely take part in and interact with the blockchain. Blockchain-based cryptocurrency systems such as Bitcoin [23], Ethereum [24], and Litecoin have this mechanism. With no central node in charge of this decentralized and trustless network, the cryptography algorithm and consensus ensure the validity and integrity of data, thereby maintaining the fairness and equality of the system.

Private Blockchains: Unlike public blockchains, not anyone has access permission in private blockchain systems. Only authorized entities can access the on-chain data and initiate transactions, whereas the blockchain is essentially a centralized database. Private blockchains have generally been used for data confidentiality, authentication, and organization management of internal information.

Consortium Blockchains: As a combination of public blockchains and private blockchains, consortium blockchains have typically been under the control of some reign entities. The access mechanism is determined by manager nodes to decide who can join the network, initiate transactions, or participate in the consensus. Hyperledger Fabric [31], Quorum [37], and Corda [38] are the typical examples of consortium blockchains.

3.1.5. Summary

Blockchain technologies have various irreplaceable characteristics that are quite suitable for the application of the IoMT. For example, the immutability and traceability of blockchains can bring innovations to the data storage, security, and privacy protection of the IoMT. It makes the tracing and tracking of medical incidents more efficient while also avoiding privacy leakage and tampering attacks. Furthermore, nodes in the blockchain system can join and exit the system freely; this feature is very suitable for flexible connections of perception or actuation devices. Moreover, the application of smart contracts can provide new solutions for medical services and data management in IoMT, such as epidemic spread control, vaccination statistics, and medical equipment management.
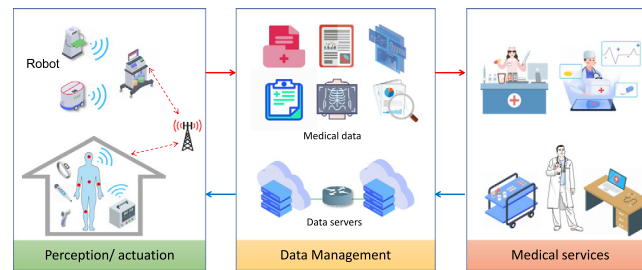
Fig. 4. Overview of IoMT.

Besides, among the various categories of blockchain systems, they have corresponding appropriate application scenarios. Due to the sensitivity of physiological data from patients, the private blockchain that a single group or multiple groups control (e.g., doctors, patients, administrators) is the most feasible type of blockchains for the IoMT applications. Besides, compared with public blockchains, private blockchains have better performance in scalability and flexibility. Patients' physiological data are not of high sensitivity for some scenarios, and the consortium blockchains may also be feasible.

In short, the integration of blockchain technology with the existing medical information system is a promising direction. Undeniably, it will also make new contributions to combat against COVID-19.

3.2. Internet of medical things

The system architecture and existing challenges of IoMT are presented in the following subsections.

3.2.1. System architecture of IoMT

The recently proposed IoMT-based medical system architecture usually consists of three layers [7,39]. As shown in Fig. 4, the three layers of IoMT architecture are composed of the data collection layer, the data management layer and the medical service layer.

Perception/Actuation layer: On the one hand, the perception/actuation layer collects the physiological data of patients and preprocess these physiological data with patients' privacy information. On the other hand, this layer can also enforce some actions on the IoMT. This layer is mainly composed of two types of devices: medical sensor/actuator devices and edge servers. Medical sensing devices are wearable or implanted biosensors, which are used to collect physiological data of patients, such as blood sugar, blood pressure, heart rate, electrocardiogram (ECG), electromyography (EMG) and electroencephalogram (EEG), etc. The medical sensor devices conduct the on-demand monitoring and collect the patient's physiological data at set intervals when the patients' physiological parameters are normal. When the patient's physiological parameters become abnormal or under the request of an authorized user (patient, doctor, nurse, etc.), the medical sensor devices will conduct continuous intensive monitoring of the patient.

After collecting the patients' physiological data, the medical sensor devices transmit the collected patient's physiological data to the edge servers. Edge servers may be gateways in the network, local base stations, or personal smart devices. The main function of edge servers is to preprocess the collected physiological data with various formats, eliminate the redundancy of the data, compress and encrypt these data. The edge servers can also conduct preliminary analysis and storage of the data, and generate alarming signals when physiological parameters become abnormal. When the edge servers complete the preliminary processing of the collected patients' physiological data, the data is uploaded to the data management layer through WiFi, LTE or 5G network.

Data management layer: In the data management layer, the patients' physiological data uploaded by edge servers are further processed, stored and analyzed on the data management equipment. The data management equipment in this layer needs to effectively manage and analyze the heterogeneous physiological data of patients, and classify the data according to the timeliness and the priority of the analysis task. In addition, the data management equipment needs to establish an efficient distributed storage mechanism for a large amount of data to support efficient data processing and analysis. In the scenario of intensive care, sudden disease detection and vital parameters monitoring, the real-time changes of physiological parameters such as heart rate and blood pressure reflect the health status of individuals. Therefore, these data need to be processed in a very short time, and then the analytical results on patients' physiological data should be rapidly returned to the medical professionals and the patient to deal with the emergencies.

Since the data management equipment needs to analyze patients' physiological data efficiently and rapidly, some recent studies employ cloud servers to conduct data processing, data storage and data analysis in this layer [40,41]. The cloud servers extract features of the collected physiological data and classify the data to help medical professionals (such as doctors) providing better medical service. In this way, medical professionals can obtain the processed data with the easy observed form, and provide prediction as well as treatment advice faster and better. With the permission of the patient, the algorithms and programs for the assessment of expected diagnosis and rehabilitation progress can be run

on the data management equipment. In this layer, access control mechanisms or identity authentication mechanisms are applied to ensure that only authorized entities can access patient's physiological data, so that data security and patients' privacy are protected. In addition, patients' information and related profiles will be anonymous before sharing data with other entities such as research centers.

Medical service layer: The medical service layer aims to provide users with basic visual data analysis results. The visualized data are used to generate reports and send them to healthcare participants (including doctors, patients, and nursing staff) involved in clinical observation, patient diagnosis, and intervention processes. Medical personnel (such as doctors) with appropriate authentication and authorization credentials can access the reports on patient's physiological data and provide medical advice to patients timely.

The medical professionals can track designated patients and access the reports based on the daily activities of patients. On the one hand, through real-time analysis, the changes in patients' physiological parameters can be detected immediately to avoid sudden diseases. When the patient's physiological parameters become abnormal, the medical service equipment sends a notification alarm to the nursing staff for further treatment advice. Then the medical professionals could guard against risk and initiate the necessary action plan to deal with emergencies such as heart attack, falls, etc. On the other hand, through long-term monitoring and analysis of patient physiological data, the medical professionals can track the health status of patients' daily life and predict some potential health risks, such as obesity and hypertension. In addition, considering the physiological characteristics of individuals, individual treatment simulations can be carried out to assess the health risk and design the best medical plan.

3.2.2. Challenges in IoMT

The advent of IoMT still confronts the following challenges.

Absence of interoperability: There are a variety of medical sensor devices in the data collection layer of IoMT, where the medical sensor devices are different in computing capability, memory, energy supply and embedded software. The data formats of collected patient's physiological data vary from device to device, consequently resulting in the difficulty of managing the data in the data management layer.

Another reason caused the poor interoperability lies in the heterogeneity of wireless/wired protocols. When the patient's physiological data is collected, the medical sensor devices transmit the collected data to edge servers. During this transmission process, different wireless protocols are employed. For some powerful wearable medical sensor devices, the protocols like WiFi, NB-IoT and Bluetooth Low Energy (BLE) are utilized. The protocols like Near-field communication (NFC), Radio Frequency Identification (RFID) are employed for medical sensor devices implanted into the patient's body. The poor interoperability across different IoMT systems will result in the difficulty of medical information exchange in different medical institutions.

Privacy and security: The leakage of patients' sensitive physiological information may lead to serious problems to patients. However, most medical sensor devices in the data collection layer are resource-constrained. The limitations of computing power, memory, energy supply in medical sensor devices also result in the infeasibility of traditional complicated encryption mechanisms. The patient's sensitive physiological data from medical sensor devices to edge serves may be wiretapped by illegal devices.

To protect the privacy of patients' sensitive information in the data management layer and health service layer, various access control mechanisms and identity authentication mechanisms are designed [4]. However, the data storage of patients' sensitive physiological data still relies on the third party, where the bugs on information leakage may exist in the data server. Consequently, data storage or cloud services providers may mistakenly or intentionally release patients' privacy-sensitive data.

4. Blockchain-enabled IoMT

In this section, we propose an architecture for incorporating blockchain into IoMT systems, namely BCeMT, and investigate the benefits as well as challenges of BCeMT.

4.1. Architecture of blockchain-enabled IoMT

The convergence of blockchain and IoMT can ameliorate the interoperability of IoMT systems, significantly improve the security of IoMT, and enhance the privacy protection of IoMT [2]. Fig. 5 depicts a system architecture of BCeMT. In this architecture, the blockchain layer is essentially serving for the entire IoMT, i.e., covering the perception/actuation layer, data management, and medical services layer.

In this architecture, the blockchain is serving as a crucial infrastructure connecting different layers of IoMT. Blockchains are endowed with cryptographic schemes (i.e., digital signature and public encryption), P2P networks, distributed consensus, smart contracts, and a chain of blocks. Consequently, the blockchain can ensure a certain security of IoMT. The employment of the authentication [42], homomorphic obfuscations, and group signature [43] to blockchains can further protect the data privacy of IoMT. Moreover, the overlaid P2P networks in blockchain systems can connect different sectors in IoMT together so as to improve the interoperability across the entire IoMT.
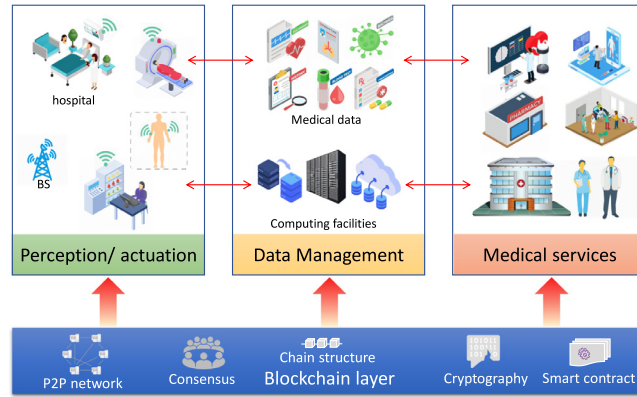
Fig. 5. System architecture of BCeMT.

4.2. Opportunities of BCeMT

BCeMT can overcome challenges of IoMT and offer the following opportunities to enhance IoMT.

4.2.1. Interoperability improvement

The introduction of blockchain to IoMT can essentially connect fragmented sectors of IoMT together via the overlaid P2P network, which is a crucial part of blockchain systems. Thereafter, different IoMT sectors, such as medical centers, clinics, hospitals, and homes can be connected together to offer a ubiquitous Internet service across the entire IoMT [44]. Therefore, the interoperability across different healthcare sectors has been improved.

In addition, this novel architecture can also help to collect, preprocess, and store diverse IoMT data. During this process, heterogeneous IoMT data can be converted, transformed, encrypted, compressed, and stored in blockchain (i.e., on-chain data) [45]; alternatively IoMT data can be saved in an off-chain fashion, in which only hashes of IoMT data are stored in blockchain [46]. Consequently, the interoperability of IoMT has also been greatly improved.

4.2.2. Privacy preservation of IoMT data

To preserve the privacy of patients, only authorized users are allowed to access the sensitive medical data of patients. The research [48] proposed an attribute-based access control scheme to address the privacy issues of patients' Electronic health record (EHR) data in the blockchain-based e-health system. In this scheme, the attribute assignments and delegation control are managed by the blockchain in a lightweight style. Meanwhile, the research [47] proposed a permissioned blockchain-enabled framework and an access control scheme to protect the privacy of patients' EHR data. In their framework, the distributed proxy re-encryption method and the corresponding re-encryption contract are utilized. With the proxy re-encryption method, keys as well as small encrypted records can be stored on the blockchain.

Due to the limited storage capacity of IoMT, the lightweight cryptographic operations in BCeMT are investigated. Particularly, the authors of [49] designed a private blockchain-based access control mechanism for the applications of IoMT. The privacy preservation of this mechanism is achieved by the elliptic curve cryptography (ECC) enabled signature approach. Moreover, in [50], a blockchain-based data access mechanism is proposed to guarantee that medical data accessibility is controlled by the patients. In this mechanism, the lightweight public key cryptographic operations are conducted with ECC cryptographic function. The work [51] proposed a platform to protect the privacy of patients' EHR data by storing the sensitive information on the blockchain. In this platform, the ECC cryptographic function is applied to achieve the pseudonymity of patients.

In addition to access control schemes, attribute-based signature mechanisms can be utilized to preserve the privacy of patients. In particular, in [52], the authors designed an attribute-based signature mechanism for a blockchain-based EHR system. To ensure the anonymity of patients and immutability of data in EHRs, this mechanism introduced multiple authorities. Another attribute-based signature scheme in a blockchain-based EHR system is proposed in [53]. While in this mechanism, the attributes are revocable by utilizing the KUNodes algorithm, and therefore the identity privacy of users (both patients and doctors) is protected.

Utilizing more than one blockchain is another possible solution to deal with the privacy leakage problem of IoMT. The research [54] proposed a privacy-preserving framework enabled by two blockchains for the smart healthcare system. In this framework, one blockchain is used for publishing data and the other is used for fine-grained access control, while the medical data is stored in a file system. In this way, neither the patients' medical data nor the doctors' diagnoses will be tampered. The authors in [55] proposed another two-blockchains enabled privacy-preserving framework. In this framework, a permissioned blockchain is applied to store the medical data as well as patients' personal information, and

Table 3
Applying blockchain technique for privacy preserving of IoMT.

References	Blockchain type	Design objectives	Main contributions	Methods
[47]	Permissioned	Protecting the privacy of patients' EHR data	Access control scheme with proxy re-encryption method	Storing keys and encrypted records on the blockchain
[48]	Not mentioned	Addressing the privacy issues of patients' EHR data	Attribute based access control scheme	Managing the attribute assignments and delegation control with blockchain
[49]	Private	Preserving the privacy of patients	Access control mechanism	ECC-enabled signature scheme
[50]	Private or permissioned	Medical data accessibility is controlled by the patient	Data accessibility mechanism	Lightweight public key cryptographic operations
[51]	Permissioned	Protect the privacy of patients' EHR data	A platform to store the sensitive personal information on blockchain	ECC cryptographic function is applied to achieve the pseudonymity of patients
[52]	Not mentioned	Ensuring the anonymity of patients and immutability of data in EHRs	Attribute-based signature mechanism	Introducing multiple authorities to this system and sharing pseudorandom function seed in every two authorities and keep secretly
[53]	Permissioned	Privacy preservation both patients and doctors	Attribute-based signature scheme	Utilizing the KUNodes algorithm for revocation
[54]	Public	Protecting both patients' medical data and the doctors' diagnoses	A two blockchains enabled privacy preserving framework	One blockchain used for sharing data and the other used for fine-grained access control
[55]	Permissioned and permission-less	Protecting the privacy of patients during the medical data sharing process	A framework consists of two blockchains	A permissioned blockchain stores the medical data and patients' personal information, and send the medical data to the permission-less blockchain at set intervals
[56]	Permissioned	Allowing patients to selectively share the medical data	An App for BCeMT	The access control list of medical data is generated according to the settings and operations of patients
[57]	Private	Ensuring patients to manage their own medical data by themselves	An App for BCeMT	Integrating the traditional database with gateway, and blockchain helps to store medical data

periodically anchors the medical data to a permission-less blockchain. Medical data sharing is enabled and the privacy of patients is protected.

Some researches focus on designing Applications (Apps) to make sure that patients could manage their own medical data by themselves. In [56], the authors designed a mobile App in a permissioned blockchain-enabled medical data sharing system. With this App, the patients shall selectively share the medical data according to the necessity of their own judgment. The research [57] proposed another App based on an architecture that integrating the traditional database with the gateway. In this architecture, the blockchain helps to store medical data and patients are clearly aware of the usage of medical data.

A summary of the researches on utilizing blockchain technique to preserve the privacy of patients in IoMT is given in Table 3.

4.2.3. Security assurance of IoMT

To protect the sensitive medical data of IoMT from being wiretapped, the medical data is required to be encrypted before the transmission and retrieval process. In [9], the authors designed an authenticated key management protocol for a BCeMT environment with lightweight cryptographic operations. Specifically, the one-way cryptographic hash function and bitwise XOR operations are applied to conduct the lightweight cryptographic operations for computing resources limited medical sensor devices. Their protocol helps to protect the security of patient's medical data, and the security performance of this protocol is verified by the tool AVISPA. The work [58] proposed a lightweight decentralized authentication scheme for patients in distributed IoMT with a public blockchain. In this authentication scheme, the symmetric key encryption algorithm ARX is utilized to conduct lightweight encryption operations on the data of medical sensor devices.

The smart contract can be utilized to help secure the blockchain-based IoMT. The authors in [59] proposed a blockchain-enabled framework to ensure the security of medical data. In this framework, two smart contracts are applied to securely share and store the medical data individually, and a graph neural network based trust model is used to detect the malicious nodes. The proxy re-encryption method is utilized in their scheme so that patients shall dynamically provide or revoke the permissions of their medical data access. Meanwhile, in [60], the authors introduced the process of securing medical data with smart contract in a blockchain-enabled remote healthcare system.

In some cases, the volume of medical data is too large to be stored in the blockchain, so that only the vital part of the data will be stored on the blockchain. In [61], the authors proposed a BCeMT system to protect the patients' sensitive information security in the medical image retrieval process. The feature vectors of each image are extracted and encrypted

Table 4
Applying blockchain technique for security assurance of IoMT.

References	Blockchain type	Design objective	Main contributions	Methods
[9]	Public	Protecting the security of patients' medical data in BCeMT	Authenticated key management protocol	One-way cryptographic hash function and bitwise XOR operations
[58]	Public	Protecting the security of patients' medical data in BCeMT	Lightweight decentralized authentication scheme	Lightweight symmetric key encryption algorithm ARX
[59]	Consortium	Ensure the security of medical data	A BCeMT framework	Two smart contracts are utilized to securely share and store the medical data individually
[60]	Not mentioned	Protect patients' personal and information and medical data	A remote medical system based on blockchain	Securing medical data with smart contract
[61]	Not mentioned	Protect the patients' sensitive information security in the medical image retrieval process	A BCeMT system for medical image retrieval process	Storing the extracted and encrypted feature vectors of each image into the blockchain
[62]	Not mentioned	Ensuring the patients to control their identity information by themselves in medical images sharing process	A BCeMT framework for medical image retrieval process	Identities of patients are stored on the blockchain as randomly-generated public keys
[63]	Public	Securing the medical data sharing system	A blockchain enabled medical framework	Utilizing the patients' digital medical identities to encrypt the to be shared medical data

before storing them in the blockchain. The integrity and accuracy of encrypted image features will be verified by miners with a hash signature when the information is uploading to the blockchain. Another research [62] also utilizes blockchain technology to protect the patients' sensitive information in medical images. In this research, the identities of patients are stored on the blockchain as randomly generated public keys, and the patients' identity information is controlled by themselves in medical image sharing.

In [63], the authors proposed a blockchain-enabled framework for securing the medical data sharing system. In this framework, the patients' digital medical identities are utilized to encrypt the medical content to be shared and the security of medical data is enhanced. Based on this framework, a case study of decentralized App for sharing medical data is demonstrated.

A summary of the researches on utilizing blockchain techniques to protect the security of patients' data in IoMT is given in Table 4.

4.3. Challenges of BCeMT

Although the BCeMT architecture brings a number opportunities, there are still a few challenges that remain to be addressed before BCeMT can be practically adopted.

4.3.1. Resource constraints

Storage and computation capability constraints may limit the widespread applications of BCeMT architecture. On one hand, a massive amount of physiological data may be generated from the IoMT network, thereby posing stringent requirements on high storage and computation capability. Moreover, the chain in the blockchain network has kept growing and each node stores a replica of the entire chain. On the other hand, the processing ability of each node in the blockchain network is also limited [45].

One potential solution to this challenge is to introduce cloud services into this architecture. In this way, we can upload a large amount of less privacy-sensitive data to the remote clouds while storing the sensitive data (e.g., the sensitive private information of patients) at the blockchain. Processing most medical data on the clouds will also release the computation burden at nodes in the blockchain.

4.3.2. Governance issues

The current emerged private and permissioned blockchain applications are granted "write" permissions to a predefined peer or set of peers [64]. In the sensitive healthcare domain, the legal regulations on the BCeMT are required to explicitly define the nodes, users, peers and validators of the blockchain.

For governance, only participating hospitals and institutions, as well as selected patients who are permissioned, are included in the blockchain network [65]. The adoption of BCeMT architecture needs to be backed by legal instruments.

5. Applications of BCeMT

BCeMT can potentially address the crisis caused by the COVID-19 epidemic. We list several possible applications of BCeMT in tackling the COVID-19 crisis.
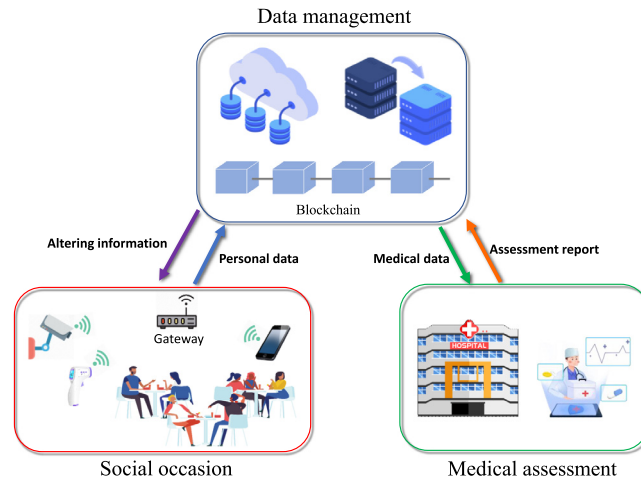
Fig. 6. Location sharing and contact tracing.

5.1. Location sharing and contact tracing

According to recent studies [66,67], there are two main transmission pathways of the COVID-19 virus. The first is the direct human-to-human transmission through respiratory droplets from the coughing, sneezing or even breathing of patients. The second is an indirect pathway through touching the staff surface infected by patients. Therefore, obtaining the location information of patients and tracing their close contacts are vital to prevent the transmission of the COVID-19 virus. However, the conventional information-sharing methods may lead to privacy leakage and the patients may lose control of their personal data.

The blockchain-based IoMT may solve this problem with the decentralized architecture and unforgeability characteristic. As shown in Fig. 6, the potential patients and general public in the social occasion first upload the location and medical information to the blockchain-based database, where the patients' information pseudonymity can be achieved by cryptographic functions [51]. Next, the authenticated medical centers will obtain the medical data and conduct the COVID-19 assessment. If the assessment result is positive, the blockchain-based database will connect to the medical center for medical support and inform the gateway on social occasions to generate the alarming signal to warn the general public. Privacy preservation can be achieved with the location sharing scheme [68] and the transparency feature of blockchain may guarantee the unforgeability of contact traceability.

5.2. Prevention of infectious diseases

As indicated in [69], keeping a social distance is an effective way to prevent the outbreaks of infectious diseases like COVID-19. BCeMT can offer a solution to social-distancing measures. For example, as shown Fig. 7, sensors as well as cameras can detect, identify, and count the number of customers in a restaurant, consequently offering early warnings of an overcrowded environment. Moreover, [70] shows that the increment of air ventilation in a crowded environment can also diminish the aerosol transmission of coronavirus. The controller of a ventilation fan or an air conditioner can dynamically adjust the ventilation volume according to the crowd density which can be obtained by cameras and ambience sensors. The ventilation fans or central air conditioning systems can be shut down or reduced airflow for the sparse crowd so as to save energy consumption.

The outbreaks of COVID-19 also result in overcrowded hospitals. It becomes extremely important to improve air filtration inwards or emergency rooms in a hospital. In addition, it is also crucial to ensure the functioning of exhaust fans in restroom facilities of a hospital so as to reduce the air transmission risk of coronavirus. However, it is laborious for technicians to troubleshoot every fan and air conditioner in the entire ventilation system. In addition, it can also cause health risks for technicians to manually check the ventilation system due to the contaminated surfaces and filters [71]. In this case, the wide proliferation of diverse sensors and actuators (like controllers of fans) in IoMT can offer a solution to this emerging issue. On the one hand, sensors can report the possible faults of fans and abnormal functioning of the ventilation system. On the other hand, actuators of fans can dynamically adjust airflow volumes as shown in Fig. 7.

5.3. Traceable information chain of COVID-19 vaccines

Undoubtedly, vaccines play an indispensable role in the control of the COVID-19 epidemic. Researchers around the world have invested enormous effort in vaccine development, testing, and mass production as soon as possible to fight
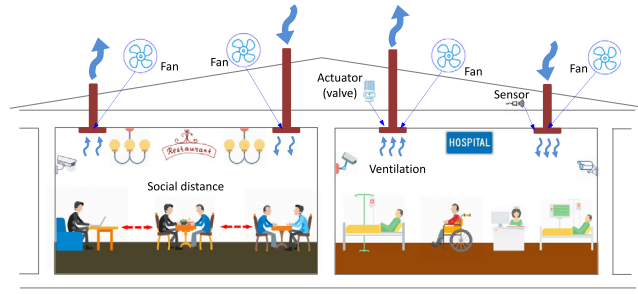
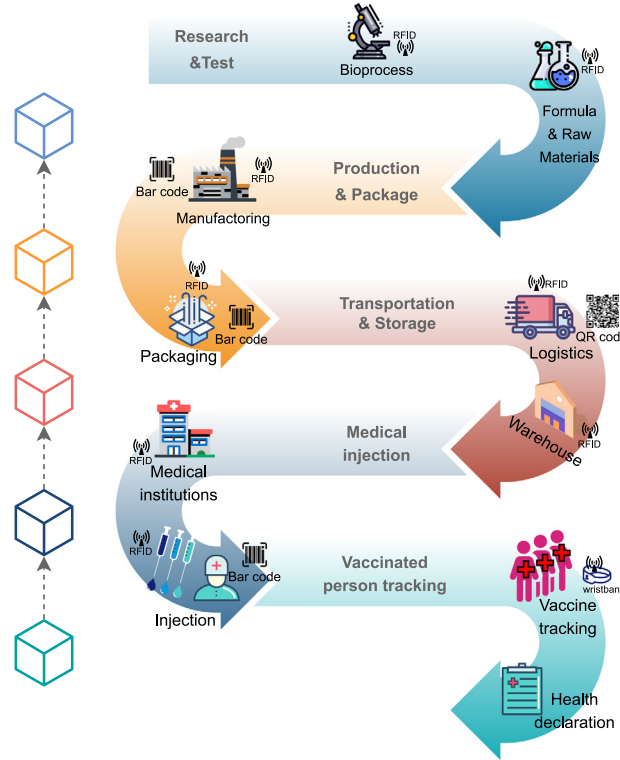**Fig. 7.** Prevention of infectious diseases.

Fig. 8. Supply chain of injectable medicines.

against the spread of the virus. Due to the huge demand for this vaccine, we can reasonably speculate that there will be many problems in the mass production and distribution of injections, such as quality control, transportation, and storage safety. In fact, some suspected adverse reactions after injection have also been found in existing tests and injection results [72]. Therefore, it is necessary to design and build a vaccine supply chain system based on the blockchain to ensure the quality, safety, and traceability of the vaccine. When a problem occurs, this vaccine-tracing system can quickly trace back and locate the source of the problem. In addition, due to massive COVID-19 vaccine production, the production of other vaccines may also be affected due to excessive production lines, raw materials, and manpower requirements. The system combined with IoMT can also provide data support for the rational distribution of productivity.

The immutability and security of the blockchain are suitable for data recording and storage in the injectable medical supply chain. As shown in Fig. 8, from vaccine research and testing to follow-up observation of vaccine injections, and health declaration, information can be collected and recorded on the chain. In the operation and maintenance, various IoMT devices can evolve, such as sensors, Radio Frequency Identification (RFID) tags, bracelets, etc [2]. In the IoMT blockchain system as illustrated in Fig. 8, vaccine information at different stages will be encapsulated on the chain, including the results of research and testing, the source of production materials, process factories, transportation logistics and storage warehouse information, hospitals and medical staffs, the follow-up symptom observation after the injection. Among them, RFID tags, Quick Response tags (QR tags), Bar code tags, and sensors can ensure that information recording

is more efficient and non-falsifiable. The patients after vaccine injections can declare their health status regularly during the observation period, thereby ensuring the subsequent collection of injections more complete.

6. Future directions

Although BCeMT has the great potential to address the COVID-19 crisis, there are a number of issues to be tackled. We discuss the open issues as follows.

6.1. Legislation and incentives of IoMT data sharing

Although BCeMT is promising in fostering interoperability of IoMT systems, offering privacy preservation of IoMT data, and guaranteeing the security of IoMT systems, incumbent medical institutions, organizations and the public have their concerns or misgivings to share IoMT data. The first reason is the absence of regulations and the legislation of medical data [73]. Secondly, another obstacle in medical data sharing lies in patients' concerns on how their medical data is shared and exploited [74].

To dispel the public's misgivings of IoMT data sharing, there are several working directions in the future. Firstly, substantial legislative efforts are necessary to be made to regulate IoMT data sharing and data governance. Clear definitions and regulations on how to share IoMT data, which part of IoMT data to be shared, and which party to use IoMT data. During this process, blockchain may also serve a crucial role in promoting the regulations and standardization of IoMT data sharing. For example, traceable blockchain can make the data-sharing process be fully traceable so as to improve the transparency of data sharing and governance. Secondly, blockchain can play as a catalyst for data sharing. For example, built-in incentive/pricing mechanisms of blockchain can be adopted to encourage the public or patients to share their medical data. Medical and research agencies can pay for the shared IoMT data. It is worth mentioning that data privacy protection mechanisms are still necessary for medical data sharing.

6.2. Scalability and optimization of blockchain

The emerging BCeMT also poses stringent requirements on blockchains in terms of throughput and storage. Thus, the scalability, throughput efficiency, and modularity of blockchains will become valuable research directions in the future.

Both the scalability and throughput efficiency of the blockchain have received extensive attention [44]. The massive IoMT data may overload the existing blockchain systems. There are several possible solutions to this issue. 1) *Adopting new blockchain data storage method*, for example, the combination of on-chain and off-chain data storage can avoid the problem of huge on-chain data redundancy and difficulty to synchronize. 2) *Efficiency of consensus algorithms*, we can adjust existing consensus algorithms after finding the best performance consensus parameters, such as encryption algorithm, block size, block interval, etc. 3) *hybrid blockchain type*, a flexible consortium chain integrating the private chain or public chain may possibly increase the transaction volume per unit time.

Moreover, the modularity of blockchains can also offer a flexible manner to disassembling and reconstructing blockchain systems so as to support diverse applications (especially for COVID-19) without affecting the security of blockchain data. The modularity can be achieved by designing suitable smart contract deployment plans.

6.3. Privacy-preserving big data analytics of BCeMT

In the IoMT system, a large amount of medical data will be continuously collected by the medical sensor devices. With the help of big data technology, the collected medical data in IoMT may be utilized more effectively and efficiently in disease prediction and other applications. However, one of the main obstacles in utilizing the medical data with big data technique is the requirement of patients' privacy protection [75].

The adoption of blockchain to IoMT systems is a promising solution to solve the privacy problem of medical data in IoMT. The BCeMT system can preserve the privacy of patients and remove the obstacle of utilizing medical data with big data. In particular, the integration of attribute-based encryption [76] and blockchains can achieve data analysis on encrypted data [77]. In the future, the implementation of big data techniques in BCeMT systems can further extract useful information while preserving data privacy.

6.4. Integration of AI with BCeMT

Artificial intelligence, especially advances in machine learning (ML) and deep learning (DL) may potentially improve the service quality of the IoMT system. The intelligent services empowered by ML/DL may make up for the absence of medical resources. The massive IoMT data can be used to train ML/DL models so as to obtain reliable prediction models with high accuracy [78]. Once a reliable disease prediction model with high accuracy is built for the IoMT system, the spread of infectious diseases such as COVID-19 will be significantly inhibited.

Though the IoMT system continuously provides medical data, different medical institutes need to share the encrypted medical data to obtain more data so to improve the performance of their prediction model. In this case, a large number of computational operations are required. Thus, distributed computing is a solution [79]. In the BCeMT system, the architecture is distributed and the blockchain-based encryption operations ensure the security and privacy of medical data. In the future, task decomposition across the entire BCeMT system will be further investigated.

7. Conclusion

In this article, we explore the application of blockchain-enabled IoMT (BCeMT) to fight against the COVID-19 pandemic. We first present a technical overview of blockchain and IoMT. We also summarize the challenges on privacy, security, and interoperability of incumbent IoMT systems. We then present the architecture of BCeMT and elaborate on the opportunities brought by BCeMT. We discuss the benefits of this architecture, including the security improvement of IoMT, privacy protection assurance of IoMT, and the interoperability amelioration of IoMT systems. We next provide several use cases of BCeMT on combating the COVID-19 pandemic. The applications of BCeMT include the prevention of infectious diseases, location sharing and contact tracing, and the supply chain of injectable medicines. Finally, we outline the future directions of BCeMT.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

References

[1] A.H. Mohd Aman, W.H. Hassan, S. Sameen, Z.S. Attarbashi, M. Alizadeh, L.A. Latiff, Iomt amid covid-19 pandemic: Application, architecture, technology, and security, J. Netw. Comput. Appl. (2020) 102886.

[2] H.-N. Dai, M. Imran, N. Haider, Blockchain-enabled internet of medical things to combat COVID-19, IEEE Internet Things Mag. 3 (3) (2020) 52–57, http://dx.doi.org/10.1109/IOTM.0001.2000087.

[3] H. Habibzadeh, K. Dinesh, O. Rajabi Shishvan, A. Boggio-Dandry, G. Sharma, T. Soyata, A survey of healthcare internet of things (hiot): A clinical perspective, IEEE Internet Things J. 7 (1) (2020) 53–71.

[4] Y. Sun, F. Lo, B. Lo, Security and privacy for the internet of medical things enabled healthcare systems: A survey, IEEE Access 7 (2019) 183339–183355.

[5] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R.U. Rasool, W. Dou, Complementing iot services through software defined networking and edge computing: A comprehensive survey, IEEE Commun. Surv. Tutor. 22 (3) (2020) 1761–1804.

[6] M. Shen, Y. Deng, L. Zhu, X. Du, N. Guizani, Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach, IEEE Netw. 33 (5) (2019) 27–33.

[7] X. Li, H.-N. Dai, Q. Wang, M. Imran, D. Li, M.A. Imran, Securing internet of medical things with friendly-jamming schemes, Comput. Commun. 160 (2020) 431–442, http://dx.doi.org/10.1016/j.comcom.2020.06.026.

[8] P.P. Ray, D. Dash, K. Salah, N. Kumar, Blockchain for iot-based healthcare: Background, consensus, platforms, and use cases, IEEE Syst. J. (2020) 1–10, Early Access.

[9] N. Garg, M. Wazid, A.K. Das, D.P. Singh, J.J.P.C. Rodrigues, Y. Park, Bakmp-iomt: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment, IEEE Access 8 (2020) 95956–95977.

[10] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, M. Imran, Securing iots in distributed blockchain: Analysis, requirements and open issues, Future Gener. Comput. Syst. 100 (2019) 325–343.

[11] J. Wan, J. Li, M. Imran, D. Li, Fazal-e-Amin, A blockchain-based solution for enhancing security and privacy in smart factory, IEEE Trans. Ind. Inf. 15 (6) (2019) 3652–3660.

[12] M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of blockchains in the internet of things: A comprehensive survey, IEEE Commun. Surv. Tutor. 21 (2) (2019) 1676–1717.

[13] A.H. Mohd Aman, W.H. Hassan, S. Sameen, Z.S. Attarbashi, M. Alizadeh, L.A. Latiff, IoMT amid COVID-19 pandemic: Application, architecture, technology, and security, J. Netw. Comput. Appl. 174 (2021) 102886, http://dx.doi.org/10.1016/j.jnca.2020.102886.

[14] T. Yang, M. Gentile, C.-F. Shen, C.-M. Cheng, J. Arada, Combining point-of-care diagnostics and internet of medical things (iomt) to combat the covid-19 pandemic, Diagnostics 10 (2020) http://dx.doi.org/10.3390/diagnostics10040224.

[15] R. Pratap Singh, M. Javaid, A. Haleem, R. Vaishya, S. Ali, Internet of medical things (iomt) for orthopaedic in covid-19 pandemic: Roles, challenges, and applications, J. Clin. Orthop. Trauma 11 (4) (2020) 713–717, http://dx.doi.org/10.1016/j.jcot.2020.05.011.

[16] P.V. Klaine, L. Zhang, B. Zhou, Y. Sun, H. Xu, M. Imran, Privacy-preserving contact tracing and public risk assessment using blockchain for covid-19 pandemic, IEEE Internet Things Mag. 3 (3) (2020) 58–63, http://dx.doi.org/10.1109/IOTM.0001.2000078.

[17] R. Kumar, 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. (2021) 1–40.

[18] F. Alam Khan, M. Asif, A. Ahmad, M. Alharbi, H. Aljuaid, Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development, Sustainable Cities Soc. 55 (2020) 102018.

[19] P.P. Ray, D. Dash, K. Salah, N. Kumar, Blockchain for iot-based healthcare: Background, consensus, platforms, and use cases, IEEE Syst. J. 15 (1) (2021) 85–94, http://dx.doi.org/10.1109/JSYST.2020.2963840.

[20] Y. Ren, Y. Leng, F. Zhu, J. Wang, H.J. Kim, Data storage mechanism based on blockchain with privacy protection in wireless body area network, Sensors 19 (10) (2019) 2395.

[21] S. Son, J. Lee, M. Kim, S. Yu, A.K. Das, Y. Park, Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain, IEEE Access 8 (2020) 192177–192191, http://dx.doi.org/10.1109/ACCESS.2020.3032680.

[22] M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, A decentralized patient agent controlled blockchain for remote patient monitoring, in: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob, 2019, pp. 1–8, http://dx.doi.org/10.1109/WiMOB.2019.8923209.

[23] S. Nakamoto, Bitcoin: A Peer-To-Peer Electronic Cash System, Tech. rep. Manubot, 2019.

[24] G. Wood, et al., Ethereum: A secure decentralised generalised transaction ledger, Ethereum Proj. Yellow Pap. 151 (2014) (2014) 1–32.

[25] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: A survey, Int. J. Web Grid Serv. 14 (4) (2018) 352–375.
[26] S. Hakak, W.Z. Khan, G.A. Gilkar, M. Imran, N. Guizani, Securing smart cities through blockchain technology: Architecture, requirements, and challenges, IEEE Netw. 34 (1) (2020) 8–14.
[27] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in: 2017 IEEE International Congress on Big Data, BigData congress, IEEE, 2017, pp. 557–564.
[28] D. Koops, Predicting the confirmation time of bitcoin transactions, 2018, arXiv:1809.10596, arXiv preprint. URL https://arxiv.org/abs/1809.10596.
[29] S. Rouhani, R. Deters, Performance analysis of ethereum transactions in private blockchain, in: 2017 8th IEEE International Conference on Software Engineering and Service Science, ICSESS, IEEE, 2017, pp. 70–74.
[30] G.-T. Nguyen, K. Kim, A survey about consensus algorithms used in blockchain., Journal of Information Processing Systems 14 (1) (2018).
[31] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, et al., Hyperledger fabric: a distributed operating system for permissioned blockchains, in: Proceedings of the thirteenth EuroSys conference, 2018, pp. 1–15.
[32] M. Castro, B. Liskov, et al., Practical byzantine fault tolerance, in: OSDI, Vol. 99, 1999, pp. 173–186.
[33] D. Schwartz, N. Youngs, A. Britto, et al., The ripple protocol consensus algorithm, in: Ripple Labs Inc White Paper, Vol. 5, No. 8, 2014.
[34] N. Szabo, Smart contracts: building blocks for digital markets, EXTROPY:, J. Transhumanist Thought (16) 18 (2) (1996).
[35] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, M. Imran, An overview on smart contracts: Challenges, advances and platforms, Future Gener. Comput. Syst. 105 (2020) 475–491.
[36] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, F.-Y. Wang, An overview of smart contract: architecture, applications, and future trends, in: 2018 IEEE Intelligent Vehicles Symposium (IV), IEEE, 2018, pp. 108–113.
[37] J.M. Chase, Quorum whitepaper, 2016.
[38] R.G. Brown, J. Carlyle, I. Grigg, M. Hearn, Corda: an introduction, R3 CEV, 2016, p. 15.
[39] Y.A. Qadri, A. Nauman, Y.B. Zikria, A.V. Vasilakos, S.W. Kim, The future of healthcare internet of things: A survey of emerging technologies, IEEE Commun. Surv. Tutor. 22 (2) (2020) 1121–1167.
[40] J.H. Abawajy, M.M. Hassan, Federated internet of things and cloud computing pervasive patient health monitoring system, IEEE Commun. Mag. 55 (1) (2017) 48–53.
[41] R. Cao, Z. Tang, C. Liu, B. Veeravalli, A scalable multicloud storage architecture for cloud-supported medical internet of things, IEEE Internet Things J. 7 (3) (2020) 1641–1654.
[42] Y. Wu, H.-N. Dai, H. Wang, K.-K.R. Choo, Blockchain-based privacy preservation for 5G-enabled drone communications, IEEE Netw. 35 (1) (2021) 50–56, http://dx.doi.org/10.1109/MNET.011.2000166.
[43] S. Zhang, J. Lee, A group signature and authentication scheme for blockchain-based mobile-edge computing, IEEE Internet Things J. 7 (5) (2020) 4557–4565, http://dx.doi.org/10.1109/JIOT.2019.2960027.
[44] Y. Wu, H.N. Dai, H. Wang, Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0, IEEE Internet Things J. 8 (4) (2021) 2300–2317, http://dx.doi.org/10.1109/JIOT.2020.3025916.
[45] H.-N. Dai, Z. Zheng, Y. Zhang, Blockchain for internet of things: A survey, IEEE Internet Things J. 6 (5) (2019) 8076–8094.
[46] J. Eberhardt, S. Tai, On or off the blockchain? insights on off-chaining computation and data, in: European Conference on Service-Oriented and Cloud Computing, Springer, 2017, pp. 3–15.
[47] G.G. Dagher, J. Mohler, M. Milojkovic, P.B. Marella, Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, Sustainable Cities Soc. 39 (2018) 283–297.
[48] H.S. Gardiyawasam Pussewalage, V.A. Oleshchuk, Blockchain based delegatable access control scheme for a collaborative e-health environment, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1204–1211.
[49] S. Saha, A.K. Sutrala, A.K. Das, N. Kumar, J.J.P.C. Rodrigues, On the design of blockchain-based access control protocol for iot-enabled healthcare applications, in: ICC 2020 - 2020 IEEE International Conference on Communications, ICC, 2020, pp. 1–6..
[50] V. Ramani, T. Kumar, A. Bracken, M. Liyanage, M. Ylianttila, Secure and efficient data accessibility in blockchain based healthcare systems, in: 2018 IEEE Global Communications Conference, GLOBECOM, 2018, pp. 206–212.
[51] A.A. Omar, M.Z.A. Bhuiyan, A. Basu, S. Kiyomoto, M.S. Rahman, Privacy-friendly platform for healthcare data in cloud based on blockchain environment, Future Gener. Comput. Syst. 95 (2019) 511–521.
[52] R. Guo, H. Shi, Q. Zhao, D. Zheng, Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems, IEEE Access 6 (2018) 11676–11686.
[53] Q. Su, R. Zhang, R. Xue, P. Li, Revocable attribute-based signature for blockchain-based healthcare system, IEEE Access 8 (2020) 127884–127896.
[54] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, N. Yu, Healthchain: A blockchain-based privacy preserving scheme for large-scale health data, IEEE Internet Things J. 6 (5) (2019) 8770–8781.
[55] T. Zhou, X. Li, H. Zhao, Med-ppphis: Blockchain-based personal healthcare information system for national physique monitoring and scientific exercise guiding, J. Med. Syst. 43 (9) (2019) 1–23.
[56] X. Liang, J. Zhao, S. Shetty, J. Liu, 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, 2017, pp. 1–5.
[57] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control, J. Med. Syst. 40 (218) (2016).
[58] A. Yazdinejad, G. Srivastava, R.M. Parizi, A. Dehghantanha, K.K.R. Choo, M. Aledhari, Decentralized authentication of distributed patients in hospital networks using blockchain, IEEE J. Biomed. Health Inf. 24 (8) (2020) 2146–2156.
[59] Z. Wang, N. Luo, P. Zhou, Guardhealth: Blockchain empowered secure data management and graph convolutional network enabled anomaly detection in smart healthcare, J. Parallel Distrib. Comput. 142 (2020) 1–12.
[60] H.L. Pham, T.H. Tran, Y. Nakashima, A secure remote healthcare system for hospital using blockchain smart contract, in: 2018 IEEE Globecom Workshops, GC Wkshps, 2018, pp. 1–6.
[61] M. Shen, Y. Deng, L. Zhu, X. Du, N. Guizani, Privacy-preserving image retrieval for medical iot systems: A blockchain-based approach, IEEE Netw. 33 (5) (2019) 27–33.
[62] V. Patel, A framework for secure and decentralized sharing of medical imaging data via blockchain consensus, Health Inf. J. 25 (4) (2019) 1398–1411.
[63] P. Zhang, J. White, D.C. Schmidt, G. Lenz, S.T. Rosenbloom, Fhirchain: Applying blockchain to securely and scalably share clinical data, Comput. Struct. Biotechnol. J. 16 (2018) 267–278.
[64] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with iot. challenges and opportunities, Future Gener. Comput. Syst. 88 (NOV.) (2018) 173–190.
[65] T.K. Mackey, T.T. Kuo, B. Gummadi, K.A. Clauson, G. Church, D. Grishin, K. Obbad, R. Barkovich, M. Palombini, 'fit-for-purpose?' – challenges and opportunities for applications of blockchain technology in the future of healthcare, BMC Med. 17 (1) (2019).
[66] K. Al Huraimel, M. Alhosani, S. Kunhabdulla, M.H. Stietiya, SARS-CoV-2 In the environment: Modes of transmission, early detection and potential role of pollutions, Sci. Total Environ. 744 (2020) 140946.

[67] M. Kumar, K. Taki, R. Gahlot, A. Sharma, K. Dhangar, A chronicle of sars-cov-2: Part-i - epidemiology, diagnosis, prognosis, transmission and treatment, Sci. Total Environ. 734 (2020) 139278.

[68] J. Yaxian, Z. Junwei, M. Jianfeng, Y. Chao, Y. Xin, Bmpls: Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems, J. Med. Syst. 42 (8) (2018) 1–13.

[69] J.A. Lewnard, N.C. Lo, Scientific and ethical basis for social-distancing interventions against covid-19, Lancet. Infect. Dis. 20 (6) (2020) 631.

[70] J. Lu, J. Gu, K. Li, C. Xu, W. Su, Z. Lai, D. Zhou, C. Yu, B. Xu, Z. Yang, Covid-19 Outbreak associated with air conditioning in restaurant, Guangzhou, China, 2020, Emerg. Infect. Diseases 26 (7) (2020) 1628.

[71] V.A. Mouchtouri, M. Koureas, M. Kyritsi, A. Vontas, L. Kourentis, S. Sapounas, G. Rigakos, E. Petinaki, S. Tsiodras, C. Hadjichristodoulou, Environmental contamination of sars-cov-2 on surfaces, air-conditioner and ventilation systems, Int. J. Hyg. Environ. Health 230 (2020) 113599, http://dx.doi.org/10.1016/j.ijheh.2020.113599, URL http://www.sciencedirect.com/science/article/pii/S1438463920305459.

[72] S.P. Kaur, V. Gupta, COVID-19 Vaccine: A comprehensive status report, Virus Res. 288 (2020) 198114, http://dx.doi.org/10.1016/j.virusres.2020.198114, URL http://www.sciencedirect.com/science/article/pii/S0168170220310212.

[73] R. Milne, K.I. Morley, H. Howard, E. Niemiec, D. Nicol, C. Critchley, B. Prainsack, D. Vears, J. Smith, C. Steed, et al., Trust in genomic data sharing among members of the general public in the UK, USA, Canada and Australia, Hum. Genet. 138 (11) (2019) 1237–1246.

[74] J. Kim, H. Kim, E. Bell, T. Bath, P. Paul, A. Pham, X. Jiang, K. Zheng, L. Ohno-Machado, Patient perspectives about decisions to share medical data and biospecimens for research, JAMA Netw. Open 2 (8) (2019) e199550, http://dx.doi.org/10.1001/jamanetworkopen.2019.9550.

[75] S. Shi, D. He, L. Li, N. Kumar, M.K. Khan, K.-K.R. Choo, Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey, Comput. Secur. 97 (2020) 101966.

[76] K. Zhang, J. Long, X. Wang, H. Dai, K. Liang, M. Imran, Lightweight searchable encryption protocol for industrial internet of things, IEEE Trans. Ind. Inf. (2020) 1.

[77] W. Liang, Y. Fan, K.C. Li, D. Zhang, J.L. Gaudiot, Secure data storage and recovery in industrial blockchain network environments, IEEE Trans. Ind. Inf. 16 (10) (2020) 6543–6552, http://dx.doi.org/10.1109/TII.2020.2966069.

[78] M. Zhao, et al., SEENS: Nuclei segmentation in pap smear images with selective edge enhancement, Future Gener. Comput. Syst. 114 (2021) 185–194, http://dx.doi.org/10.1016/j.future.2020.07.045, URL https://www.sciencedirect.com/science/article/pii/S0167739X20304271.

[79] H.-N. Dai, Y. Wu, M. Imran, H. Wang, N. Haider, Blockchain-empowered edge intelligence for internet of medical things against COVID-19, IEEE Internet Things Mag. (2021) 1–8.