Article

JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)

Vol.31; No.4.| 2023

Blockchain for the Internet of Medical Things (B-IoMT): Background, Architecture and Challenges

Qusay S. Alsaffar
Minister Office, Ministry of Higher Education and Scientific Research.
qusay_saffar@ mohesr.gov.iq , Baghdad, Iraq.
***Corresponding author email:** qusay_saffar@mohesr.gov.iq; mobile: +9647702969751

بلوكشين لأنترنيت الأشياء الطبية: الخلفية والمعمارية والتحديات (B–IoMT)

قصي سمير شاكر الصفار
مكتب الوزير، وزارة التعليم العالي والبحث العلمي، qusay_saffar@ mohesr.gov.iq ، بغداد، العراق

Accepted: 25 / 9 /2023 **Published:** 31 /12 /2023

ABSTRACT

Background:

Today blockchain and IoT technologies are being greatly used and exploited in several fields, particularly for Internet of Things healthcare. In healthcare systems, real-time sensory data can be obtained from patients and processed and analyzed by using IoT devices.

Materials and Methods:

The data that are aggregated from IoT are centrally computed, processed, and saved. Data centralization can lead to problems, potential tampering or manipulation, privacy evasion, and then failure. These serious problems can be solved by using blockchain through decentralization and IoT data storage. Therefore, blockchain and IoT technologies can be aimed to become a credible option for using IoT decentralization in healthcare systems.

This paper, firstly, introduces a brief explanation of blockchain. Secondly, it discusses the usage of blockchain of common consensus algorithms in the environment of health. Finally, the extent of the use of blockchain to support healthcare sector ecosystems and services. This paper explained the architecture of IoMT which is used for accessing, managing, and storing the data of healthcare.

Results:

Presenting a survey about studies and research that face the challenges of the Internet of Things and healthcare, and proposed solutions to save data from tampering.

Conclusion:

With the stringent protection standards in the healthcare industry, many studies have centered on the usage of blockchain in IoMT Stuff. The successful implementation of the IoMT, demands a lot of personalized, patient-centric treatment Internet of Medical Things that enhance affordability (reduced operating costs, cost-effective care), enhanced life quality, simplicity and ease of use.

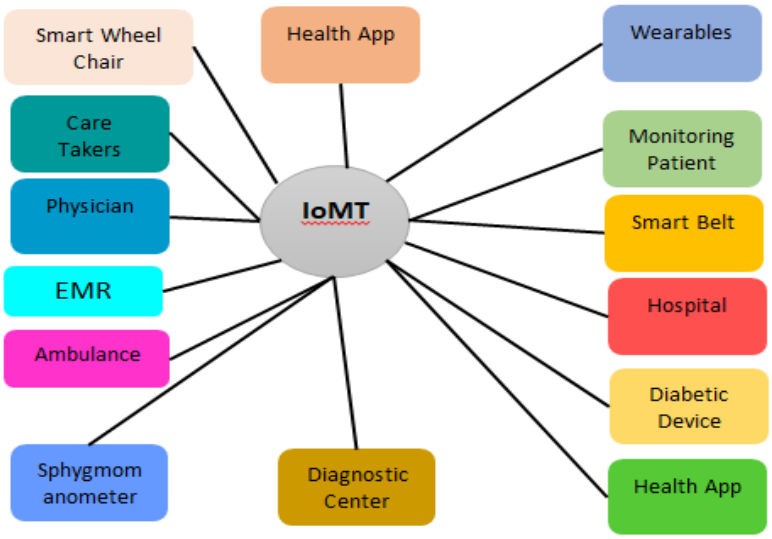
Keywords: Blockchain, Interment of Things (IoT), Consensus, Healthcare, Interment of Medical Things (IoMT).

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com
مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

INTRODUCTION

IoMT is a set of devices that provide a health service and they are connected to the internet. Essentially, the Internet of Things (IoT) is a connected infrastructure of healthcare systems like software applications, medical devices, and services as illustrated in Figure (1) Moreover, when among sensors and devices, healthcare organizations are able to make their workflow management and clinical operations more accurate and efficient observing of patient health from long distances [1],[2].



[Fig.1] Internet of Medical Things (IoMT) [3].

Along with the rapid increasing natural and advances of the security problems, the ways of securing IoMT have become a big challenge while the past security problems have become heavier. So, the privacy and security of IoMT is the core of researchers' interest [4],[5].

Different parties can receive a big amount of IoMT data after collecting them. The procedures should be made in a secure style. As a result of this large transformation, the methods of hackers are more prone and in need of immediate solutions to secure IoMT [6],[7].

In summary, the survey's major contributions can be summarized as follows: offering an overview of blockchain, discussing the use of blockchain of common consensus algorithms in the environment of health, using blockchain to support healthcare sectors ecosystems and services, this paper also explained the architecture of IoMT which are used for accessing, managing and storing the data of healthcare.

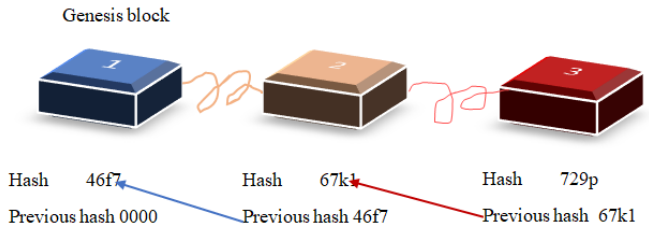
ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

BLOCKCHAIN TECHNOLOGY

Blockchain is designed as a P2P technology for sharing data computing and distributing. Blockchain allows the different parties to achieve various transactions in the network. Blockchain is a kind of data structure, that can store and track information from a huge number of devices in a decentralized paradigm[8].

Blockchain is a digital ledger that keeps the rising collection of data records and it is a tamper-proof. No centralized and no master is existing computer in the blockchain structure. The transactions is made among nodes by using a public key cryptography technology[9]. The shared ledger is used to store transactions. The chain of blocks is connected with each other cryptographically inside the ledger. It cannot remove or change blockchains that are recorded in ledger[10].

Proof-of- work is a puzzle that blockchain users must solve to put new data into blockchain. Genesis block is the first block. Each block includes hash number figure (2). The transaction can be viewed by participants. The actual contact cannot be seen by everyone. The private key protects actual contact [11].



[Fig 2] Blockchain Architecture[8]

There are various features that make blockchain technology used in Bitcoin. IoMT security problems can be solved ideally by applying the capabilities of the blockchain such that decentralized, security and autonomous[12]. There are a lot of strengths that contain in blockchain[13],[14]:

- Secure and Immutable: The blockchain is a digital ledger tamper-proof that nobody can modify the records that rises the precision of records.
- Decentralized Control: Means that no third party can access and no central data.
- Transparency of Data and Auditability: Blockchain stores all transactions that occurred and seen publicly to increase the auditability and trust.
- Distributed Information: Each node connected to the network stores a duplicate of record in blockchain, this process prevents central authority.
- Peer-to-Peer Transaction: A peer-to-peer connection has allowed by blockchain parties to avoid intermediary.
- Decentralized Consensus: The transactions is confirmed by every node in the network. This separates the notion of centralized protocol.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

STEPS OF BLOCKCHAIN WORK

In order to be added to the Blockchain, a block must meet the following requirements. [15],[16]:

- The transaction is requested by a node in the blockchain network.
- The members (nodes) view the request of transaction.
- The network nodes verify the request by using of algorithms then accept the transaction.
- The transaction is completed after the approval of the request by all nodes.
- Directly, after the transaction is done, the blockchain network receives a new block where it is immutable.
- The nodes add to the verified transaction with other transactions generating novel block of data.

The process of adding information to the blockchain means that the user must have a unique key and a public address to log in, then the user signs the transaction by using a private key. This information is very secure and it is copied thousands of times, if a hacker wants to make a modification, he/she needs more than 51% control of the nodes [17].

TYPES OF THE BLOCKCHAIN

There are four types of blockchain are available [7],[18] and they are:

- Public Blockchains: A completely decentralized network are provided in the public blockchains, every node can share in the consensus process and get the content of the blockchain (e.g., Bitcoin and Ethereum).
- Private Blockchains: Devoted for single project resolutions and used to conserve route of data exchanges that happened several individuals or departments. Every member needs approval to enter the network and becomes as a known participant after joining.
- Consortium Blockchains: is a public and authorized network just for prerogative group. It is utilized as a reliably and auditable distributed synchronized database that conserves route of members data exchanges.
- Hybrid Blockchains: The advantages of public and private blockchains are merged in hybrid blockchains. The ledger is completely accessible by a public blockchain, while the ledger modifications can be controlled accessed by the private blockchain.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Table 1. Type of Blockchains

Properties	Private	Public	Consortium
Consensus Procedures	RAFT, PBFT	DPoS, PoW	PBFT
Nature	Controlled and Restricted	Open and decentralized	Controlled and Restricted
Participants	Identified and trusted	Anonymous and resilient	Identified and trusted
Immutability	Could be tampered	Infeasible to tamper	Could be tampered
Read/Write permission	permissioned	permission less	permissioned
Scalability	High	High	Low
Efficiency	High	Low	High
Transparency	High	Low	High
Transaction approval frequency	Short	Long (10 minutes or more)	Short
Example	Blockstack, Multichain, Bankchain	Ethereum, Bitcoin, Factom , Litecoin, Dash, Blockstream,	Hyperledger, R3, Ripple,

INTERNET OF MEDICAL THINGS

IoMT was created as a result of recent improvements in biosensors, medical devices, and communication technology[19]. It can be used in a variety of healthcare scenarios, including telemedicine, remote rehabilitation and pandemic quarantine. The IoMT which connects a variety of medical equipment and facilities healthcare institutions, has resulted in a large amount of heterogeneous medical data. Medical experts (such as doctors and nurses) can diagnose, identify, and treat patients using the enormous IoMT data by analyzing it[20],[21].

Although IoMT has the potential to provide both patients and medical practitioners with dependable and effective healthcare services, it also brings with it the following challenges[22]: 1) lack of interoperability between IoMT sectors; 2) security and privacy flaws in internet of medical things devices and systems. Internet of medical things systems are heterogeneous since they are made up of a variety of medical equipment, biomedical sensors, base stations and internet of things gateways. Meanwhile, the diversity of internet of medical things reflects the diversity of wireless protocols such as BLE, NFC, LoRa, LoWPAN, and NB-IoT. As a result of the variability of decentralized IoMT systems, Poor interoperability between systems, resulting in the establishment of a variety of information silos. As a result, transferring medical data between different medical facilities and institutions is complicated. Medical experts, on the other hand,

need to share medical knowledge, especially in the prevention and treatment of pandemic outbreaks like COVID-19[23].

Furthermore, IoMT is confronted with the growing security and privacy concerns[24]. The biological sensors and medical equipment with limited resources (e.g., poor processing capabilities and battery capacity) are vulnerable to malicious assaults such wiretapping, jammer, backdoor and worm attacks. In contrast to other types of IoT data, IoMT data is more sensitive to privacy. IoMT data, in particular, frequently necessitates outsourcing to faraway cloud servers maintained by third parties. The privacy of patients' data may be compromised during the collecting, processing and analysis of IoMT data, either purposefully or unintentionally.

BLOCKCHAIN IN INTERNET OF MEDICAL THINGS

The IoT is an expansion of Internet connection to the sensors and physical devices. Electronics that interconnected via internet can connect, contact and monitoring remotely[25]. Specified the hard requirements for IoT, blockchain seems to be quite convenient for: 1. Protecting the network from tampering those threats storing data. 2. Preparing a protected infrastructure including all devices in the network. The following discussion is about current models and e-healthcare based on the IoT[26]:

- The client–server model has been used currently in the IoT networks, where devices are authenticated, identified and interconnected through cloud servers need a huge amount of storage size and processing capability. Moreever, these devices are connected to internet, although close to each other. So, this model is convenient for small IoT networks. The cost of constructing a big number of links, preserving clouds and networking all devices, is important for great scale of IoT. Regardless of cost, depending on cloud servers makes the structure amenability to fail. Furthermore, IoT devices must be protected against information attacks or physical manipulation. Currently, the IoT devices are secured by some methods, but these methods are complex and not convenient for resource restricted internet of thing devices.
- A constructed P2P network blockchain that reduces the cost of setting and repairing of data centers and networking devices by providing storage requirements to all network devices. This communication model fixes failure problem. The cryptographic algorithms are used to process the privacy requirements for internet of things networks. It fixes another problem such that of the reliability in IoT networks by using tamper opposer ledgers.

Advantages of Blockchain IOMT – Healthcare

The combination of Blockchain and internet of medical things technologies allows not just for remote patient monitoring, but also to the centralized compilation and aggregation of clinical data (such as health insurance, entitlements, clinical trial data, administrative data, illness archives and health surveys) an expense method, allowing for self-governance and thus saving time and effort. Block chain is used to diagnose and treat diseases such as internal organ anomalies, cancer, and the proper use of sensory instruments like heartbeat sensors, as ingestible tablets, and more. Here are some of the benefits of Blockchain in the internet for medical things[27],[28],[29]:

- Collaboration aids the proper management and synchronization of distributed ledger technologies as well as the continuation of field innovation;

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

- Data provenance and integrity help medical centers cope with the growing number of users and devices they use to store and process data.
- Data protection guarantees the security of sensitive documents and information by preventing unauthorized users from accessing data and information.
- Monitoring aids in authorizing access to medical records, documenting transactions in a clear and transparent manner, and effort, saving time and money.
- Simplifying the process that reduces the amount of work required to protect sensitive information, resulting in an overall increase.

Applications of Blockchain for IoMT

According to several researchers, the advantages of integrating Blockchain techniques with medical care include computerized execution of programs, difference access control for various user groups and the improvement of health care legislation, logistics, distant data collection, the calibration of information or convergence, indexing, replication, and fault lenience.[11],[30],[31],[32].

The main aids for integrating blockchain technology in internet of medical things, health care applications and biomedical are consistent rules through smart contract, data access and monitoring, business model improvements, data storage, protection and data provenance, immutable audit trail, integrity of medical records, decentralized management, interoperable health data access, performance, robustness, availability, protection, and privacy in the medical supply chain, as well as cost-effectiveness, single patient recognition, source of single data, storage space, and value-based payment mechanisms. By combining blockchain technology for internet of think, it is possible to improve the of real-time proof.

Tracking and management of health assets in the supply chain based on the block chain: the immutability properties of the block chain help in the control of drug supply chains, making drug forgery more difficult. As a result, the block chain can be used in a variety of fields, including drug regulation and management. Block chain is used to monitor drug distribution to ensure that resources are following the supply chain pattern correctly. Cycling across all stages of the supply chain, for example, will aid in the fight against drug counterfeiters, as well as pharmaceutical product deviation and theft.

Management of health care information: in healthcare, for information management can use the block chain protocols to monitor transactions, as well as the process of transmitting electronic health records, with enhanced protection, privacy and data immutability. The block chain meets the requirements for bettering the security and quality of data transfer while also lowering energy costs. As consensus protocols progress, they can be used in resource-constrained devices (for example, internet of medical thing), as can light consensus protocols like SCP and PBFT[33]. The blockchain supports the exchange and storing of large amounts of health information.

Storage and secure sharing of health care data: both stakeholders in the medical care industry are required to secure exchange patient medical data. To make informed health-care choices, it is important to exchange unaltered data related to patients. The rapid development of blockchain means that health data can be shared and stored on the Block chain in safe, an absolute and consistent manner. The consensus protocol is the primary protocol involved in the network confidence building processes. It aids in the exchange of patient data, image sharing, and security

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

logs in healthcare systems, health-care information management, patient monitoring with personal sensors, patient monitoring with restricted sensors and reliability.

Security and privacy in blockchain for IOMT: In blockchain, there are a number of privacy issues that need to be addressed, according to[27] is identity protection protecting the user's private identity while keeping it separate from the transaction, and (ii) Transaction protection entails preventing unauthorized users from accessing the transaction's contents.

Blockchain Consensus Algorithms in Healthcare - IoMT

The smart contract is a part of the code that is used to modify, access and manage the ledger, it is a computer protocol. The smart contract is a facility to approval for all blockchain nodes. There is different cryptocurrency that contains consensus algorithms. The paper selected a group of consensus algorithms that can be used in e-healthcare service [34],[35],[36]:

Proof of Work (POW): The proof of work is highly sophisticated computationally where blockchain is been what it is. PoW is a technique to define the selected nodes in the network. To perform, one will win rewards, it must achieve computational challenge, so the operation is difficult. The main purpose of the PoW is to avoid cyber-attacks. Attacker can easily make DoS if blockchain without PoW, and fill up the network with blocks. This will lead the network crowding and all peers want to achieve additional job to get a correct block among millions fake blocks. In addition, to make PoW hard to solve and easy to verify, it must be asymmetric task. A miner must solve the hash puzzle, so he must spend more time, while the other miners can instantly and easily in the network verify the solution[37]. The hash function begins from sequential 0, this number is added conforming to the puzzle difficulty. Anyone can achieve PoW that regarded hash function. The hash problem can be solved by any device. This features of PoW are regarded a standard system[34] .

Proof of Stake (PoS): Some peers are not regarded for the mining operation, because these nodes do not contain the primary needed requirements, where, nodes attempt to solve the problem in PoW. Moreover, the process of adding new blocks in PoW is difficult to modify a previous block. This indicates the flexibility and security for the blockchain.

Delegated Proof of Stake (DPoS): This type is represented as democratic. It makes cost trend centralization and faster transaction. The consensus for expose and voting out attacker are existing. So, DPoS can apply in e-healthcare systems with high likelihood.

LPoS: It is abbreviation are Leased proof of stake, the problem of centrality in the PoS can be solved in LPoS, the nodes with the lease contract and less balances can be enabled, and participates the reward with riches owner. When applying this type of algorithm the research enhanced the quality e-health service.

Proof of Importance (PoI): PoI enhanced over PoS. It regarded nodes reputation plus nodes evenness. This network is more productive. This type of algorithm is recommended to utilize in e-healthcare services to assist patients for making a decision.

Practical Byzantine Fault Tolerance (PBFT): The nodes share in the voting operation for adding new block. The nodes must be more 2/3 consensus. This algorithm is best than PoW and PoS and considered economical and appropriate for private blockchains. While this algorithm has less leniency against fabricated nodes. This type is favorite for e-health services utilization.

Delegated Byzantine Fault Tolerance (dBFT): The PBFT has improved to be dBFT. Peers are selected as envoy of another node. So, the e-healthcare services may not totally execute upon get benefit of dBFT in the IoT blockchain system.

Proof of Capacity (PoC): The PoW has improved to be PoC. It is necessary to store enormous data to mine the following blocks of another nodes. but it is not convenient for IoT. Also, this algorithm is not recommended for e-health services.

Proof of Activity (PoA): This type is mixed between PoW and PoS. First the PoW is executed. Then the transaction is placed into the header of miner after a PoS by the set of validators that they signed together. It is not convenient for the IoT because long latency, So, it is a bad option for e-healthcare.

Proof of Burn (PoB): It means to transmit coins to an irrecoverable address. Additional burnt coins prefer to be mined. This type is suitable for cryptocurrency but not suitable for IoT because it is conditioned presence financial framework combustion of coins. As a result of burning methods randomly, this type is not convenient for e-healthcare systems.

Proof of Elapsed Time (PoET): It proposed by Intel and it enhanced over PoW with a very small energy consumption. The waiting time detects the winning miner and it is selected in random way. The SGX is regarded suitable for IoT. It is quite particular for the SGX environment, it is suitable for e-healthcare.

Stellar Consensus Protocol (SCP): The PBFT has improved to be SCP. The SCP contains two phases: candidate protocol and voting protocol. So, the SCP is considered a perfect option for DAPP to scope IoT healthcare service.

Table 2: Comparison of consensus algorithms for internet of things-based healthcare

	IoT Compliant	Constrained	Energy	Popularity	Accessibility	example	Health Support
PoW	No	No	Very High	Very High	Open	Bitcoin	Medium
PoS	Partial	No	Med	Very High	Open	Etherium	High
DPoS	Partial	Partial	Med	Med	Open	Bitshare	High
LPoS	Partial	Partial	Med	Med	Open	Waves	High
PoI	No	No	Med	Med	Open	NEM	High
PBFT	No	No	Low	Low	Prop	Hyperledger	High
dBFT	No	No	Low	Low	Prop	NEO	LOW
PoC	No	No	Low	Low	Open	Burstcoin	Low
PoA	No	No	Med	Low	Prop	Bitcoin	Low
PoB	No	No	High	Low	Prop	Slimcoin	Low
PoET	Yes	Yes	High	Low	Prop	Sawtooth	High
SCP	Partial	No	Med	Low	Prop	Stellar	High

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Architecture of the Healthcare Monitoring

The scenario depicts a remote healthcare management system for patients who are not in hospitals and are monitored by a health team. To this end, they presume that every patient is fit with sensors that can continuously calculate a predefined set of parameters related to a person's medical status (such body temperature, heart rate, oxygen saturation, blood pressure, etc...). Other wearable sensors could be mounted in the patient's home to track his/her immediate surroundings and try for the monitoring of a person's activity as well as incidents such as falls. The data collected by means of wearable technology and other home wearable sensors is sent to a remote database system on a regular basis. A live monitoring system takes over at that time to examine the data and raise alarms if abnormalities are detected, allowing clinicians to take action remotely. This information is often saved in order to keep track of all the accidents that might occur, and it can be useful to doctors who are monitoring the patients' health status. All of the transactions among the various parts of our scenario include a highly confidential personal information. It is self-evident that these medical records should be kept private and accessible only to a small number of people in a global framework which ensures non-repudiation. To meet this entire criterion, they created a blockchain-based architecture to remotely track the patient's condition. Figure (3) shows the architecture, which is made up of two blockchains, medical devices and a monitoring system.

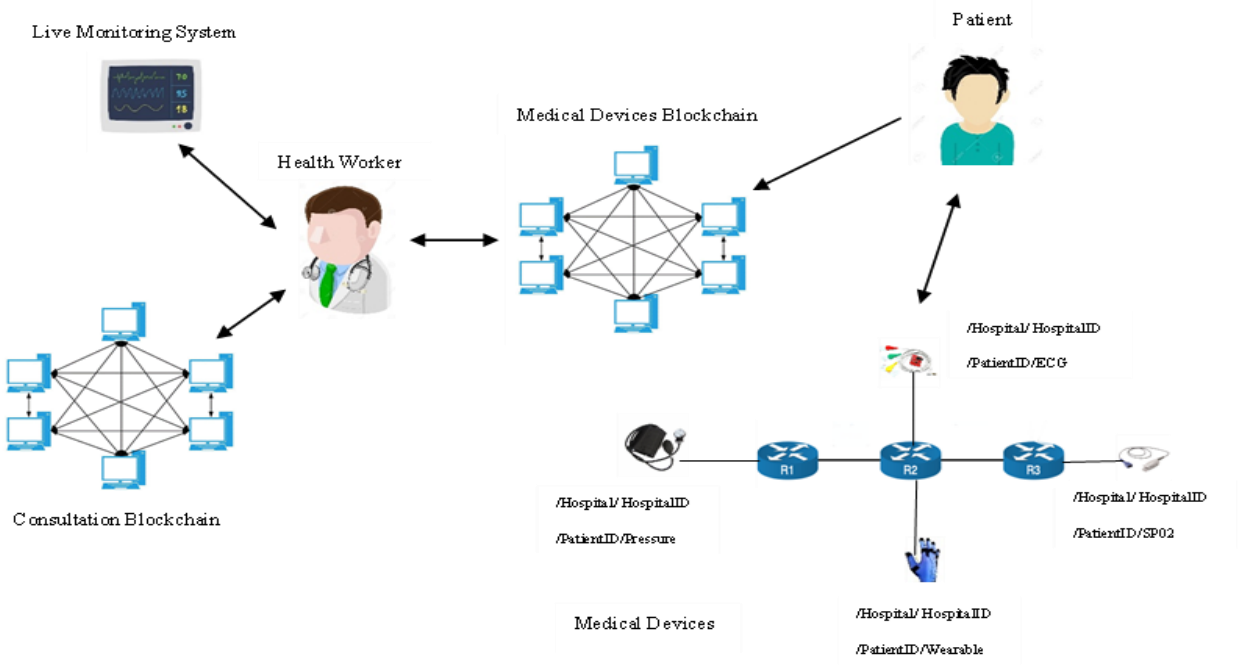


Fig [3]: Healthcare Monitoring Architecture [8]

Medical Devices Blockchain: Every patient is tracked by a series of medical devices in the designed architecture. These medical devices modify the collect of data that has been saved in a blockchain for medical devices. As a result, one medical device blockchain is optimized for each patient. A portion of the medical devices blockchain is represented by the smart contract. In the following part, how to use a smart contract is presented.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Consultation Blockchain: it is depicted in the designed architecture is one-of-a-kind, containing all of the patient's records' history. This blockchain is shared among hospitals and contains patient records. As a result, exchanging medical reports between hospitals and health workers becomes simpler and more convenient. The researcher chose to distinguish those two blockchains in proposed case because each one serves a distinct function. The data collected by the sensors must be kept for the duration of the procedure, and medical records must be accessible at all times in the patient's life.

Live Monitoring System: This is the body which manipulates and analyzes data on a continuous basis. It is primarily used to send a warning to the doctor (if necessary) in the event of an emergency.

Medical Devices: The Named Data Networking (NDN) paradigm is used to retrieve data from patient sensors and store it in the medical devices blockchain. To put it another way, A hierarchy is created a hierarchy to enable medical devices to communicate with one another.

Health Worker: He/She may be a nurse, doctor, anesthetist, and etc. He/She is a member of the medical equipment blockchain as well as the consultation blockchain. He can simulate data from the medical devices blockchain with the live monitoring system, and he can imagine or upgrade data with the consultation blockchain.

Patient: Patient is a blockchain server for health devices. It gathers information from medical equipment and sends it to the health equipment blockchain for storage.

Challenges of IoMT- Blockchain

Blockchain technologies are unquestionably beneficial to the IoMT in terms of stability. Present and future research in this field is based on scalability and interoperability issues. The lack of guidelines for designing healthcare apps based on blockchain technology is revealed by the interoperability issue[38],[39]. As a result, the various established applications will be unable to communicate with one another. Furthermore, when dealing with vast volumes of medical data, in blockchain-based healthcare systems, scalability is a big issue [8]. Due to the large volume of healthcare data, storing it on-chain or on blockchain is not feasible, as this would result in substantial performance degradation. There is also a latency problem in a blockchain-based system due to transaction processing rate and off-chain data load. Finally, smart contracts could be vulnerable to hackers due to the immutability of the blockchain and the self-execution of code. However, due to the conflicting specifications in these two technologies, combining both technologies is not easy and presents many challenges[27],[8],[40]:

- **Processing:** The sophisticated cryptography and Mining operation in blockchain technology require much resources and a large computation and high-power utilization where cannot be provided in IoMT resource-limited that today suffer from resource limitation and power restriction.
- **Storage:** An enormous amount of data with great flow are generated by IoMT devices. Blockchain must save and process these data to guarantee the integrity that construct an important challenge. To give a distributed storage, blockchains technology depend on their nodes where IoMT devices cannot provide this facility because of the restricted storage abilities.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

- **Mobility:** The infrastructure of blockchain is constructed as fixed network. However, the implantable/wearable devices are in mobility at any time that continually variety the network topology.
- **Real Time:** It must provide a real time and instant latency for IoMT applications, while, it is time consuming to create a block. In Bitcoin it requires 10 minutes to create a1MB of block. It is challenging time to construct a block regarding to real time requirement.
- **Traffic Overhead:** A significant overhead traffic is created synchronically when nodes generate blocks and connect continuously. The IoT devices cannot provide this facility due to the limitation of bandwidth.

Blockchain-Based Approaches in IoMT

In this section, the most current studies which has been used blockchain in conjunction with internet of medical thing. The research will be surveyed these studies based on the most widely used method for integrating blockchain into IoMT.

Ethereum-Based Contributions

In [41], proposed an authorized blockchain that relies on architecture that was proposed to provide monitoring and remote protection for patients. Ethereum has been exploited to send warnings to patients and healthcare, this facility is executed by analyzing data and using smart contract. Practical Byzantine Fault Tolerance (PBFT) was proposed instead of PoW consensus.

IoMT devices are employed to prevent the progress and monitor a neurological disorder, it is developed by cloud-based [42]. Cloud computing secures the exchange operation, it processes and stores IoMT data. Blockchain network provides the ability for users to share data in the healthcare system, it deploys Ethereum. The smart contract controls cloud data where users can access these data.

In [43] There is an architecture that relies on a private Ethereum, it is used to implement smart contract and organizes the demands of devices and users. Interplanetary File System (IPFS) has been used for data storage. This file system stores patient health records and devices' technical information. The consensus mechanism is executed by the smart contract. A proof of medical stack (PoMS) secures smart contracts from malicious attacks and it has been proposed instead of (PoS). (PoMS) supplies a huge of medical information to the stakeholders, these information are tokens to a block's creation and validation. In [44] a private blockchain has been utilized to organize medical data. Ethereum smart contracts are exploited to organize data access, these data are related to parties such as (research organizations, doctors, hospitals, patients and other stakeholders). The permissions, data integrity, metadata and record ownership within medical records smart representations that are included in the smart contract. The data and medical records are protected and stored in an external server by using a blockchain to secure the record's cryptographic hash.

Modified Consensus Protocol

In [45], the research introduced a consortium blockchain-based architecture for securely recording data provided by IoMT while maintaining the patient privacy. A patient agent software (PA) is used to define blockchain capabilities in the proposed architecture. For tamper-proof keeping of huge amounts of health data, it runs on a public cloud, and for light-weight functions, it runs on an edge computing network. The researcher proposes an updated PoS consensus, in

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

which a leader is chosen to validate and create blocks for a group of nodes. Smart contracts are being used to deal with health data in a number of ways, triggering alerts for some accidents, including filtering clinically useless information, migrating data to cloud if necessary, and classifying information. In terms of energy consumption and block generation time, the authors state that the modified PoS is more efficient than PoS.

In [46] the blockchain-based consortium architecture was proposed. To denote blockchain functionalities, the authors generated a patient agent program (PA) that is implemented on the edge computing platform. Smart contracts were used to handle health data in a variety of ways, such filtering medically useless information, creating alerts for specific events, drifting information to the cloud if necessary, and classifying data. According to the researcher, the adapted proof of stake is much more effective than the PoS in terms of energy consumption and block generation time.

Modified Cryptographic Technique:

In [47] , a proposed blockchain-based structure appropriate for internet of medical thing devices. To allow nodes to join in the network it must be certificated then send a transaction. The POW consensus protocol has removed by authors. To handle with the high size created by internet of medical thing devices, it collects encrypted information into blocks and save the connected blocks in cloud. To enable the tamper proof storage the blockchain stores hashes of blocks. For the user authenticity and anonymity, they utilize a low of weight facility-keeping loop signature structure that permits a set of nodes to take part in data signature. Therefore, to ensure data security and integrity through the storing and transmitting, they utilized dual encryption technique and the digital signature. The lightweight ARX algorithms are used to encrypt the data then the receiver's public key is used to encrypt the key. The Diffie-Hellman used a key exchange algorithm to protect public key transmission. To avoid network delay and scalability, nodes are regulated in clusters. A hash blocks is verified and stored by a cluster head, controls inter connection between nodes and verifying digital signatures.

Without Any Technical Specifications, a General Blockchain Concept is Propose

MedChain [48] is an association, blockchain structure proposed to meet problems regarding the activity of sharing data created from sensors. This consists of dealing with time-sets data flows, medical data control immutable and mutable, granting sharing, an active storage and critical data. The MedChain network contains two subnetworks: first: Blockchain decentralized network to save immutable data containing session, operation, data digest and user's identity. Second: P2P decentralized network to save mutable information are enabling information request containing the description of session and data.

Blockchain-internet of medical things [49] is a blockchain-based architecture that is lightweight and tailored to overcome security and privacy issues when developing IoMT systems. There are four layers to the proposed architecture: (1) providing decentralization, the device layer, which is made up of internet of medical things modules, employs the identity-based credential (IBC) method and the Elliptic Curve Cryptography key establishment protocol., (2) The facilitating layer is used to manage internet of medical thing devices and give them a specific identity based on their characteristics, (3) Cloud computing layer for anonymizing data and storing it anonymously, and (4) Cluster layer for grouping multiple organizations such as medical facilities, cloud servers and service providers into clusters. To reduce network overhead and latency, cluster is led by a cluster who is in charge of contact with other cluster heads. There are no technical specifics in this work. It has not been applied or tested.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

In [50] proposes a blockchain-based framework for sending and storing large quantities of sensitive data generated by internet of medical things in a safe manner.

Discussion and Open Issues

Despite the fact that the incorporation of internet of medical things and blockchain technologies ensures continuous control, enhanced quality of life, relaxed management, comfortable, in real-time, optimal disease control and prevention, reduced operating costs, ease of use, and calmness, there are still many challenges to be addressed. Furthermore, issues such as the necessity of constrained devices in health care applications must be addressed.

Table 3 shows how current contributions that have incorporated blockchain into IoMT are classified. The largest of the suggested policies are private blockchain used and based Ethereum framework due for the accounting flexibility provided by smart contract deployment. While combining blockchain with internet of medical things, several problems have been addressed. The majority of works [42] proposed off-chain storage for storing large IoMT data: Because of its distributed data structure, IPFS has been suggested in some studies [51],[43]. Other studies [42],[44],[45],[47],[49] and [52] used cloud computing to save encrypted information while maintaining a blockchain hash references. Such approaches do not ensure immutability that is a key aspect of blockchain. From the real world, if information has been changed or tampered with, the hash stored in the blockchain will detect it, but it will not be retrieved since it is just saved for the cloud computing (storage is centralized). Other research suggested on-chain storage out of elaborating on the technical details of dealing for a massive amount of information streams produced by internet of medical things devices. Healthcare applications, on the contrary, necessitate real-time in answer, a protocol for rapid consensus. IoMT, on the other hand, are limited devices that generate a large amount of data. To satisfy IoMT criteria, the majority of the studies [44],[53] have eliminated the consensus protocol. Smart contracts are used by some authors [43] to self-verify and self-execute transactions. A lightweight consensus process protects these smart contracts. Others [41],[45],[10] suggested a new consensus protocol: authors in[13],[15] adapted the PoS protocol to IoMT specifications, while others [43],[45] grouped nodes into clusters and selected a template for each cluster to manage node-to-node transactions, construct blocks and validate,. To preserve patient privacy, other studies [45],[47] lightweight privacy-preserving techniques, such as the ring signature method, have been suggested.

A lot of issues have been investigated, and related solutions for information (such as security) in the internet of medical things, blockchain, and cloud computing have been suggested. However, there is a gap that can be seen as an incentive for finding the best technological solutions. Like a lacuna the issue of a lack of standards has yet to be addressed. In literatures,[54],[55],[56],[57],[58],[59] are a few worth noting, as are the pertinent principles of privacy preservation. The majority of block chain research in the IoMT is solely based on anonymity, concealment, data integrity, and authentication. However, it does not address the issues that arise from the large amounts of data generated by resource-constrained internet of medical things devices.

Another factor that confirmed the results of this study is that patients are often hesitant to visit hospitals for fear of contracting illnesses. As a result, the smart-based health service was effective to use during COVID-19[60]. The health and environmental conditions of patients at homes are subsequently measured basis using the IoT system, according to the[61].Therefore, The development of such applications is not possible outside of legislative frameworks that mandate risk management as well as the integration of such tools and applications to improve patient and healthcare worker safety according to [62],[63]. Moreover, The study[64] highlighted the close

cooperation amongst COVID-19 researchers, particularly between US and China. Obesity, smoking, exercise, inflammation, and other factors linked to COVID-19 prevalence were all frequent COVID-19 risk factors. One of the research investigations, on the other hand, looked into the potential dangers of integrating low-memory and low-cost gadgets into critical care units.

Table 3 Current researches for IOMT using blockchain

#Ref	Use Case	Types	Framework	Storages	consensus	Smart Contract	Digital signature
[45]	Manage Internet of Medical things data	Consortium	No mentioned	Off-chain (cloud)	Cluster head verifies and adds blocks	Analysis and manage data	Ring signature
[44]	Manage Internet of Medical things data	Private	Ethereum	external server (off chain)	No mentioned	Health history visualized in a smart way	No mentioned
[65]	Manage Internet of Medical things data	Public	Ethereum	IPFS (Off chain)	No mentioned	Organize interactions between patients and their data, as well as between doctors and patients.	No mentioned
[43]	Manage Internet of Medical things data	Private	Ethereum	Off-chain (IPFS)	PoS	Manage access control	No mentioned
[48]	Manage Internet of Medical things data	Consortium	No mentioned	On-chain	BFTSMaRt	No mentioned	No mentioned
[49]	Manage Internet of Medical things data	Private	No mentioned	Off-chain(cloud)	No mentioned	No mentioned	No mentioned
[3]	Manage Internet of Medical things data	Private	Ethereum	No mentioned	PoW	No mentioned	No mentioned
[50]	Manage Internet of Medical things data	No mentioned	No mentioned	Hybrid	No mentioned	No mentioned	No mentioned
[41]	Remote patient monitoring	Private	Ethereum	On chain	PBFT	Analyze information and communicate any changes to patients and healthcare providers.	No mentioned

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

[47]	Remote patient monitoring	Private	No mentioned	Off chain (cloud)	Blocks are checked and added by the cluster head.	Analyze internet of medical thinkg data and keep track of the patients' health.	Lightweight ring signature
[66]	Remote monitoring of diabetes patients	No mentioned	Ethereum	No mentioned	No mentioned	Manage access control	No mentioned
[39]	Remote patient monitoring	Private	Ethereum	Off-chain (cloud)	No mentioned	send a warning to the appropriate individual, as well as storing the abnormal data in the cloud	Lightweight ring signature
[42]	Remote patient monitoring	Private	Ethereum	Off-chain(cloud)	No mentioned	Manage access control	No mentioned
[51]	Electronic medical records	Private	Ethereum	Off chain	No mentioned	Support a clinician framework that makes medical records clear and open.	No mentioned
[67]	Electronic medical records	Private	Specific	Off-chain	No mentioned	PHR is a distribution of responsibilitie s that proposes latency solutions.	No mentioned
[68]	Electronic medical records	Private	Ethereum	Hybrid	No mentioned	Suggests a blockchain-based EMR technology that complies with ONC standards.	No mentioned
[69]	Electronic medical records	Private	Proprietary	Hybrid	No mentioned	A healthcare system for both on chain verification and off chain storage	No mentioned

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

[70]	Pharmaceutical supply chain	Private	Hyperledger Fabric	On-chain	No mentioned	Create a pharmaceutical supply chain that is stable, immutable, and traceable.	No mentioned
[71]	Pharmaceutical supply chain	Private	Hyperledger Fabric	On-chain	No mentioned	access control lists	No mentioned
[72]	Pharmaceutical supply chain	Private	Ethereum	Off-chain	No mentioned	No mentioned	No mentioned
[73]	Health insurance claims	Private	Ethereum	Off-chain	No mentioned	Proposes a medical insurance storage system based on blockchain technology.	No mentioned

Conclusion and Future Work

With the stringent protection standards in the healthcare industry, many studies have centered on the usage of blockchain in IoMT Stuff. The successful implementation of the IoMT, demands for a lot of personalized, patient-centric treatment Internet of Medical Things that enhances affordability (reduced operating costs, cost effective care), enhancing life quality, simplicity and ease of use. In this paper, blockchain technology was used to secure protection for IOMT, a review of the weak points in protecting devices of IOT. A comparison of consensus algorithms of internet of things-based healthcare. For increasing data patients' real-time monitoring and prevention the network crowded the NDN is provided in this paper. A survey of the studies most used for integrating blockchain into IOMT. Classify the current contributions that incorporate the blockchain into IOMT.

Future research should focus on the following topics: Consensus algorithms need a lot of computational resources, which the IoMT cannot afford. The time taken to support blocks is not consistent with IoMT-QoS; the identity-based network layer's threats are yet to be overcome.

Conflict of interests.

There are non-conflicts of interest.

References

[1] P. Lade, R. Ghosh, and S. Srinivasan, 'Manufacturing analytics and industrial Internet of Things', IEEE Intell. Syst., vol. 32, no. 3, pp. 74–79, 2017, doi: 10.1109/MIS.2017.49.

[2] S. Chakraborty, S. Aich, and H. C. Kim, 'A Secure Healthcare System Design Framework using Blockchain Technology', Int. Conf. Adv. Commun. Technol. ICACT, vol. 2019-Febru, pp. 260–264, 2019, doi: 10.23919/ICACT.2019.8701983.

[3] 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, doi: 10.14569/IJACSA.2019.0100110.

[4] A. D. Dwivedi, L. Malina, P. Dzurenda, and G. Srivastava, 'Optimized blockchain model for internet of things based healthcare applications', 2019 42nd Int. Conf. Telecommun. Signal Process. TSP 2019, pp. 135–139, 2019, doi: 10.1109/TSP.2019.8769060.

[5] G. S. Ramachandran and B. Krishnamachari, 'Blockchain for the IoT: Opportunities and challenges', arXiv, no. May, 2018.

[6] J. J. P. C. Rodrigues et al., 'Enabling Technologies for the Internet of Health Things', IEEE Access, vol. 6, no. January, pp. 13129–13141, 2018, doi: 10.1109/ACCESS.2017.2789329.

[7] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, 'Security and Privacy in the Medical Internet of Things: A Review', Secur. Commun. Networks, vol. 2018, 2018, doi: 10.1155/2018/5978636.

[8] O. Attia, I. Khoufi, A. Laouiti, and C. Adjih, 'An IoT-Blockchain architecture based on hyperledger framework for healthcare monitoring application', 2019 10th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2019 - Proc. Work., pp. 19–23, 2019, doi: 10.1109/NTMS.2019.8763849.

[9] D. A. Noby and A. Khattab, 'A survey of blockchain applications in IoT systems', Proc. - ICCES 2019 2019 14th Int. Conf. Comput. Eng. Syst., pp. 83–87, 2019, doi: 10.1109/ICCES48960.2019.9068170.

[10] L. Ismail, H. Materwala, and S. Zeadally, 'Lightweight Blockchain for Healthcare', IEEE Access, vol. 7, no. October, pp. 149935–149951, 2019, doi: 10.1109/ACCESS.2019.2947613.

[11] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, 'MedRec: Using blockchain for medical data access and permission management', Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016, pp. 25–30, 2016, doi: 10.1109/OBD.2016.11.

[12] H. Halpin and M. Piekarska, 'Introduction to security and privacy on the blockchain', Proc. - 2nd IEEE Eur. Symp. Secur. Priv. Work. EuroS PW 2017, pp. 1–3, 2017, doi: 10.1109/EuroSPW.2017.43.

[13] K. P. Satamraju and B. Malarkodi, 'A secured and authenticated internet of things model using blockchain architecture', Proc. 2019 TEQIP - III Spons. Int. Conf. Microw. Integr. Circuits, Photonics Wirel. Networks, IMICPW 2019, pp. 19–23, 2019, doi: 10.1109/IMICPW.2019.8933275.

[14] S. Velliangiri and P. Karthikeyan Karunya, 'Blockchain technology: Challenges and security issues in consensus algorithm', 2020 Int. Conf. Comput. Commun. Informatics, ICCCI 2020, 2020, doi: 10.1109/ICCCI48352.2020.9104132.

[15] P. P. Ray, D. Dash, K. Salah, and N. Kumar, 'Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases', IEEE Syst. J., pp. 1–10, 2020, doi: 10.1109/jsyst.2020.2963840.

[16] B. I. Hameed, 'Blockchain and cryptocurrencies technology: A survey', Int. J. Informatics Vis., vol. 3, no. 4, pp. 355–360, 2019, doi: 10.30630/joiv.3.4.293.

[17] H. M. Hussien, S. M. Yasin, S. N. I. Udzir, A. A. Zaidan, and B. B. Zaidan, 'A Systematic Review for Enabling of Develop a Blockchain Technology in Healthcare Application: Taxonomy, Substantially Analysis, Motivations, Challenges, Recommendations and Future Direction', J. Med. Syst., vol. 43, no. 10, 2019, doi: 10.1007/s10916-019-1445-8.

[18] A. A. Monrat, O. Schelén, and K. Andersson, 'A survey of blockchain from the perspectives of applications, challenges, and opportunities', IEEE Access, vol. 7, pp. 117134–117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

[19] M. Simic, G. Sladic, and B. Milosavljević, 'A Case Study IoT and Blockchain powered A Case Study IoT and Blockchain powered Healthcare', 8th PSU-UNS Int. Conf. Eng. Technol., no. June, 2017.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

[20] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, 'Blockchain technology in healthcare: A comprehensive review and directions for future research', Appl. Sci., vol. 9, no. 9, pp. 1–28, 2019, doi: 10.3390/app9091736.

[21] F. Alshehri and G. Muhammad, 'A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare', IEEE Access, vol. 9, pp. 3660–3678, 2021, doi: 10.1109/ACCESS.2020.3047960.

[22] Y. A. Qadri, A. Nauman, Y. Bin Zikria, A. V. Vasilakos, and S. W. Kim, 'The Future of Healthcare Internet of Things: A Survey of Emerging Technologies', IEEE Commun. Surv. Tutorials, vol. 22, no. 2, pp. 1121–1167, 2020, doi: 10.1109/COMST.2020.2973314.

[23] H. N. Dai, M. Imran, and N. Haider, 'Blockchain-enabled internet of medical things to combat COVID-19', arXiv, no. August, 2020, doi: 10.1109/iotm.0001.2000087.

[24] M. Monti and S. Rasmussen, 'RAIN: A Bio-Inspired Communication and Data Storage Infrastructure', Artif. Life, vol. 23, no. 4, pp. 552–557, 2017, doi: 10.1162/ARTL_a_00247.

[25] K. Wilber, S. Vayansky, N. Costello, D. Berdik, and Y. Jararweh, 'A survey on blockchain for healthcare informatics and applications', 2020 7th Int. Conf. Internet Things Syst. Manag. Secur. IOTSMS 2020, 2020, doi: 10.1109/IOTSMS52051.2020.9340232.

[26] K. Taylor, A. Sanghera, M. Steedman, and M. Thaxter, 'Medtech and the Internet of Medical Things: How Connected Medical Devices are Transforming Health Care', Deloitte Cent. Heal. Solut., no. July, pp. 1–56, 2018, [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf.

[27] J. Indumathi et al., 'Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly, Unflappable, Unblemished, Unlimited Health Care Services (BC IoMT U6HCS)', IEEE Access, vol. 8, pp. 216856–216872, 2020, doi: 10.1109/ACCESS.2020.3040240.

[28] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, 'A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures', IEEE Access, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[29] J. Al-Jaroodi, N. Mohamed, and E. AbuKhousa, 'Health 4.0: On the Way to Realizing the Healthcare of the Future', IEEE Access, vol. 8, pp. 211189–211210, 2020, doi: 10.1109/ACCESS.2020.3038858.

[30] R. Jayaraman, K. Saleh, and N. King, 'Improving opportunities in healthcare supply chain processes via the internet of things and blockchain technology', Int. J. Healthc. Inf. Syst. Informatics, vol. 14, no. 2, pp. 49–65, 2019, doi: 10.4018/IJHISI.2019040104.

[31] D. B. Murphy, 'and Electronic', Imaging, vol. 83, no. 991, pp. 569–77, 2001, [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/20701335.

[32] A. Sharma, Sarishma, R. Tomar, N. Chilamkurti, and B. G. Kim, 'Blockchain based smart contracts for internet of medical things in e-healthcare', Electron., vol. 9, no. 10, pp. 1–14, 2020, doi: 10.3390/electronics9101609.

[33] I. Makhdoom, M. Abolhasan, and W. Ni, 'Blockchain for IoT: The Challenges and a Way Forward', no. July, pp. 594–605, 2018, doi: 10.5220/0006905605940605.

[34] M. Salimitari and M. Chatterjee, 'A survey on consensus protocols in blockchain for IoT networks', arXiv, pp. 1–15, 2018.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

[35] T. Ali Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, 'A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations', IEEE Access, vol. 7, pp. 176838–176869, 2019, doi: 10.1109/ACCESS.2019.2957660.

[36] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, 'Blockchain challenges and opportunities: a survey', Int. J. Web Grid Serv., vol. 14, no. 4, p. 352, 2018, doi: 10.1504/ijwgs.2018.10016848.

[37] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, 'A systematic review of the use of blockchain in healthcare', Symmetry (Basel)., vol. 10, no. 10, 2018, doi: 10.3390/sym10100470.

[38] J. Yang, H. Bi, Z. Liang, H. Zhou, and H. J. Yang, 'A Survey on Blockchain: Architecture, Applications, Challenges, and Future Trends', Proc. - IEEE Congr. Cybermatics 2020 IEEE Int. Conf. Internet Things, iThings 2020, IEEE Green Comput. Commun. GreenCom 2020, IEEE Cyber, Phys. Soc. Comput. CPSCom 2020 IEEE Smart Data, SmartD, pp. 749–754, 2020, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics50389.2020.00129.

[39] G. Srivastava, J. Crichigno, and S. Dhar, 'A Light and Secure Healthcare Blockchain for IoT Medical Devices', 2019 IEEE Can. Conf. Electr. Comput. Eng. CCECE 2019, 2019, doi: 10.1109/CCECE.2019.8861593.

[40] R. Ben Fekih and M. Lahami, Application of Blockchain Technology in Healthcare: A Comprehensive Study, vol. 12157 LNCS. Springer International Publishing, 2020.

[41] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, 'Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring', J. Med. Syst., vol. 42, no. 7, 2018, doi: 10.1007/s10916-018-0982-x.

[42] D. C. Nguyen, K. D. Nguyen, and P. N. Pathirana, 'A Mobile Cloud based IoMT Framework for Automated Health Assessment and Management', Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. EMBS, pp. 6517–6520, 2019, doi: 10.1109/EMBC.2019.8856631.

[43] V. Malamas, T. Dasaklis, P. Kotzanikolaou, M. Burmester, and S. Katsikas, 'A forensics-by-design management framework for medical devices based on blockchain', Proc. - 2019 IEEE World Congr. Serv. Serv. 2019, pp. 35–40, 2019, doi: 10.1109/SERVICES.2019.00021.

[44] A. Khatoon, 'A blockchain-based smart contract system for healthcare management', Electron., vol. 9, no. 1, 2020, doi: 10.3390/electronics9010094.

[45] M.A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, 'Blockchain leveraged decentralized IoT eHealth framework', Internet of Things, vol. 9, no. May, p. 100159, 2020, doi: 10.1016/j.iot.2020.100159.

[46] M.A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, 'Continuous Patient Monitoring with a Patient Centric Agent: A Block Architecture', IEEE Access, vol. 6, pp. 32700–32726, 2018, doi: 10.1109/ACCESS.2018.2846779.

[47] A.D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, 'A decentralized privacy-preserving healthcare blockchain for IoT', Sensors (Switzerland), vol. 19, no. 2, pp. 1–17, 2019, doi: 10.3390/s19020326.

[48] B. Shen, J. Guo, and Y. Yang, 'MedChain: Efficient healthcare data sharing via blockchain', Appl. Sci., vol. 9, no. 6, 2019, doi: 10.3390/app9061207.

[49] M. Seliem and K. Elgazzar, 'BIoMT: Blockchain for the internet of medical things', 2019 IEEE Int. Black Sea Conf. Commun. Networking, BlackSeaCom 2019, pp. 2019–2022, 2019, doi: 10.1109/BlackSeaCom.2019.8812784.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

[50] M. A. Uddin, A. Stranier, I. Gondal, and V. Balasubramanian, 'A patient agent to manage blockchains for remote patient monitoring', Stud. Health Technol. Inform., vol. 254, no. April, pp. 105–115, 2018, doi: 10.3233/978-1-61499-914-0-105.

[51] L. Hongwei, W. Xinhui, and L. Sanyang, 'Feasible direction algorithm for solving the SDP relaxations of quadratic {-1, 1} programming problems', Optim. Methods Softw., vol. 19, no. 2, pp. 125–136, 2004, doi: 10.1080/10556780410001647203.

[52] R. Singh, 'A Proposal for Mobile E-Care Health Service System Using IOT for Indian Scenario', J. Netw. Commun. Emerg. Technol. www.jncet.org, vol. 6, no. 1, pp. 21–23, 2016, [Online]. Available: www.jncet.org.

[53] C. Agbo, Q. Mahmoud, and J. Eklund, 'Blockchain Technology in Healthcare: A Systematic Review', Healthcare, vol. 7, no. 2, p. 56, 2019, doi: 10.3390/healthcare7020056.

[54] M. Kuttikrishnan, I. Jeyaraman, and M. Dhanabalachandran, 'An Optimised Intellectual Agent Based Secure Decision System for Health Care', Int. J. Eng. Sci. Technol., vol. 2, no. 8, pp. 3662–3675, 2010.

[55] A. Devibala, 'A Survey on Security Issues in Iot for Blockchain Healthcare', Proc. 2019 3rd IEEE Int. Conf. Electr. Comput. Commun. Technol. ICECCT 2019, pp. 1–7, 2019, doi: 10.1109/ICECCT.2019.8869253.

[56] V. Vasudevan, N. Sivaraman, S. S. Kumar, R. Muthuraj, J. Indumathi, and G. V. Uma, 'A comparative study of SPKI/SDSI and K-SPKI/SDSI systems', Inf. Technol. J., vol. 6, no. 8, pp. 1208–1216, 2007, doi: 10.3923/itj.2007.1208.1216.

[57] Chao-Hsi Huang and Kung-Wei Cheng, 'RFID Technology Combined with IoT Application in Medical Nursing System', Bull. Networking, Comput. Syst. Softw., vol. 3, no. 1, pp. 20–24, 2014, [Online]. Available: http://bncss.org/index.php/bncss/article/view/31.

[58] S. Y. Ge, S. M. Chun, H. S. Kim, and J. T. Park, 'Design and implementation of interoperable IoT healthcare system based on international standards', 2016 13th IEEE Annu. Consum. Commun. Netw. Conf. CCNC 2016, pp. 119–124, 2016, doi: 10.1109/CCNC.2016.7444743.

[59] G. Matar, J. M. Lina, J. Carrier, A. Riley, and G. Kaddoum, 'Internet of Things in sleep monitoring: An application for posture recognition using supervised learning', 2016 IEEE 18th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2016, pp. 0–5, 2016, doi: 10.1109/HealthCom.2016.7749469.

[60] A. Alexandru, D. Coardos, and E. Tudora, 'Iot-based healthcare remote monitoring platform for elderly with fog and cloud computing', Proc. - 2019 22nd Int. Conf. Control Syst. Comput. Sci. CSCS 2019, pp. 154–161, 2019, doi: 10.1109/CSCS.2019.00034.

[61] N. El-Rashidy, S. El-Sappagh, S. M. R. Islam, H. M. El-Bakry, and S. Abdelrazek, 'End-to-end deep learning framework for coronavirus (COVID-19) detection and monitoring', Electron., vol. 9, no. 9, pp. 1–25, 2020, doi: 10.3390/electronics9091439.

[62] A. Coronato and A. Cuzzocrea, 'An Innovative Risk Assessment Methodology for Medical Information Systems', IEEE Trans. Knowl. Data Eng., vol. 13, no. 9, 2020, doi: 10.1109/TKDE.2020.3023553.

[63] M. Hamer, C. R. Gale, M. Kivimäki, and G. D. Batty, 'Overweight, obesity, and risk of hospitalization for COVID-19: A community-based cohort study of adults in the United Kingdom', Proc. Natl. Acad. Sci. U. S. A., vol. 117, no. 35, pp. 21011–21013, 2020, doi: 10.1073/pnas.2011086117.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

[64] P. Radanliev et al., 'COVID-19 What Have We Learned? The Rise of Social Machines and Connected Devices in Pandemic Management Following the Concepts of Predictive, Preventive and Personalised Medicine', SSRN Electron. J., pp. 311–332, 2020, doi: 10.2139/ssrn.3692585.

[65] J. Singh, 'and Electronic', Imaging, vol. 68, no. December, pp. 515–524, 1994.

[66] M. Saravanan, R. Shubha, A. M. Marks, and V. Iyer, 'SMEAD: A secured mobile enabled assisting device for diabetics monitoring', 11th IEEE Int. Conf. Adv. Networks Telecommun. Syst. ANTS 2017, pp. 1–6, 2018, doi: 10.1109/ANTS.2017.8384099.

[67] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, 'OmniPHR: A distributed architecture model to integrate personal health records', J. Biomed. Inform., vol. 71, pp. 70–81, 2017, doi: 10.1016/j.jbi.2017.05.012.

[68] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, 'FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data', Comput. Struct. Biotechnol. J., vol. 16, pp. 267–278, 2018, doi: 10.1016/j.csbj.2018.07.004.

[69] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, 'Blochie: A blockchain-based platform for healthcare information exchange', Proc. - 2018 IEEE Int. Conf. Smart Comput. SMARTCOMP 2018, no. May 2019, pp. 49–56, 2018, doi: 10.1109/SMARTCOMP.2018.00073.

[70] R. Raj, N. Rai, and S. Agarwal, 'Anticounterfeiting in Pharmaceutical Supply Chain by establishing Proof of Ownership', IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON, vol. 2019-Octob, no. December 2019, pp. 1572–1577, 2019, doi: 10.1109/TENCON.2019.8929271.

[71] S. R. Bryatov and A. A. Borodinov, 'Blockchain technology in the pharmaceutical supply chain: Researching a business model based on Hyperledger Fabric', CEUR Workshop Proc., vol. 2416, pp. 134–140, 2019, doi: 10.18287/1613-0073-2019-2416-134-140.

[72] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, 'Blockchains everywhere - A use-case of blockchains in the pharma supply-chain', Proc. IM 2017 - 2017 IFIP/IEEE Int. Symp. Integr. Netw. Serv. Manag., pp. 772–777, 2017, doi: 10.23919/INM.2017.7987376.

[73] L. Zhou, L. Wang, and Y. Sun, 'MIStore: a Blockchain-Based Medical Insurance Storage System', J. Med. Syst., vol. 42, no. 8, 2018, doi: 10.1007/s10916-018-0996-4.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

الخلاصة

المقدمة:

يتم اليوم استخدام تقنيات Blockchain وIoT بشكل كبير واستغلالها في العديد من الحقول. خاصة فيما يتعلق بالرعاية الصحية لإنترنت الأشياء. في أنظمة الرعاية الصحية، يمكن الحصول على البيانات الحسية في الوقت الفعلي من المرضى ومعالجتها وتحليلها باستخدام أجهزة إنترنت الأشياء.

طرق العمل:

البيانات التي يتم تجميعها من إنترنت الأشياء يتم حسابها ومعالجتها وحفظها بشكل مركزي. يمكن أن تؤدي مركزية البيانات إلى مشاكل، من المحتمل أن تؤدي إلى العبث أو التلاعب، والتهرب من الخصوصية ثم الفشل. يمكن حل هذه المشكلات الخطيرة باستخدام Blockchain من خلال اللامركزية وتخزين بيانات إنترنت الأشياء. لذلك، يمكن دمج تقنيات Blockchain وIoT لتصبح خيارًا موثوقًا به لاستخدام لامركزية إنترنت الأشياء في أنظمة الرعاية الصحية.

هذه الورقة، أولاً، تقدم شرحًا موجزًا عن Blockchain. ثانيًا، مناقشة استخدام Blockchain لخوارزميات الإجماع الشائعة في البيئة الصحية. أخيرًا، استخدام Blockchain لدعم النظم البيئية والخدمات في قطاع الرعاية الصحية. وضحنا أيضًا بنية IoMT التي تُستخدم للوصول إلى بيانات الرعاية الصحية وإدارتها وتخزينها.

النتائج:

تقديم دراسة حول الدراسة الحالية التي تواجه تحديات في إنترنت الأشياء والرعاية الصحية، والحلول المقترحة لحفظ البيانات بعيداً عن العبث.

الاستنتاجات:

لزيادة مراقبة البيانات في الوقت الحقيقي الخاصة بالمرضى والوقاية من ازدحام الشبكة يتم توفير NDN لحل هذه المشكلة. تقديم دراسة استقصائية للبحوث الأكثر استخدامًا لدمج blockchain في IOMT. تصنيف المساهمات الحالية التي تدمج blockchain في IOMT.

الكلمات المفتاحية: Blockchain, انترنيت الأشياء (IoT), التوافق, الرعاية الصحية, انترنيت الأشياء الطبية (IOMT).

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com