Cluster Computing
https://doi.org/10.1007/s10586-024-04357-y

IoT-based eHealth using blockchain technology: a survey

Aya H. Allam[1] · Ibrahim Gomaa[2] · Hala H. Zayed[1,3] · Mohamed Taha[1]

Received: 26 October 2023 / Revised: 13 January 2024 / Accepted: 10 February 2024
© The Author(s) 2024

Abstract
The eHealth sector has witnessed significant growth due to technological advancements, facilitating care delivery in patients' homes and moving away from traditional hospital settings. Blockchain and the Internet of Things (IoT) play pivotal roles in enhancing healthcare services, offering features such as remote patient monitoring, streamlined electronic medical record (EMR) management, drug traceability, and effective disease control, particularly during events like the COVID-19 pandemic. The growing utilization of IoT devices brings about security challenges, including concerns related to data integrity and device authentication. This paper proposes the integration of blockchain technology as a robust solution. Leveraging its decentralized and tamper-resistant features, blockchain establishes trust among diverse IoT devices, ensuring the integrity of IoT data. Additionally, smart contracts enhance device authentication, fortifying overall security by addressing vulnerabilities associated with centralization. Regarding the management of eHealth, this survey begins with an overview of the industry, highlighting IoT-related challenges in healthcare. It explores various IoT applications in eHealth and discusses how blockchain can effectively address obstacles in healthcare management through IoT. Notably, the paper provides insights into examining consensus algorithm parameters within blockchain systems, clarifying the methodology used to assess and optimize these critical components. The survey extends to a thorough review of existing research on integrating blockchain-based IoT in eHealth. Finally, it presents an overview of challenges and potential solutions for implementing blockchain-based IoT in the eHealth sector. This comprehensive survey aims to empower stakeholders by providing insights to enhance patient care in this dynamic and evolving field.

Keywords IoT · Healthcare · Blockchain · Security · COVID-19

1 Introduction

Today, global healthcare spending could exceed $10 trillion [1]. Healthcare is a vital field that impacts the global population and plays an important role in the advancement of nations. As a result, eHealth systems have contributed greatly to most government initiatives worldwide, and industry spending increased by 4.1% per year globally between 2017 and 2021 [2].

IoT technology has greatly impacted the healthcare sector and led to significant growth in recent years. The eHealth industry has been significantly improved by integrating IoT into various applications such as EMR management, disease prediction, remote patient monitoring, and drug traceability [3]. In healthcare systems, data collected by IoT sensors play a critical role [4]. Remote patient monitoring is very prevalent these days, and protecting the privacy of enormous volumes of data is a major challenge with such systems [5]. These issues can be

✉ Aya H. Allam
aya.allam@fci.bu.edu.eg

Ibrahim Gomaa
igomaa@nti.sci.eg

Hala H. Zayed
hala.zayed@eui.edu.eg

Mohamed Taha
mohamed.taha@fci.bu.edu.eg

[1] Computer Science Department, Faculty of Computer and Artificial Intelligence, Benha University, Benha, Egypt

[2] National Telecommunication Institute (NTI), Cairo, Egypt

[3] Faculty of Engineering, Egypt University of Informatics, Cairo, Egypt

Published online: 04 April 2024

solved with several technologies, such as Mobile Edge Computing (MEC), Fog Computing, and Blockchain [6]. Blockchain technology is being explored as a potential solution for addressing security challenges. This has led to increased interest in using blockchain to safeguard sensitive data [3]. Integration of IoT-based eHealth systems using blockchain technology is presented in lots of research, and many challenges are faced in this integration. This article reviews and analyzes integration frameworks of Blockchain-based IoT in the healthcare industry. Moreover, the work also identifies key challenges that impede blockchain adoption in healthcare applications utilizing IoT architectures.

1.1 Search methodology

This study delves into blockchain-based research papers Related to Healthcare, IoT, and Blockchain published between 2015 and 2023.

1.1.1 Search strategy

The search space for this study was defined by utilizing various scientific databases, including Google Scholar, ResearchGate, IEEE, Science Direct, Elsevier, Springer, ACM, MDPI, Wiley, and Hindawi.

1.1.2 Search criteria

To achieve a comprehensive understanding of the subject and address the research questions, specialized search keywords were employed. The selected papers were identified using the search keywords ("HER" OR "Healthcare" OR "EMR" OR "Electronic Health Record" OR "Electronic Medical Record") AND ("IoT" OR "Internet of Things") AND "Blockchain."

1.1.3 Paper selection process

Following the defined search strategy and criteria as shown in Fig. 1, the paper selection process proceeded in the following steps:

- **Step 1**: Initial collection involved gathering papers based on their titles and keywords, accumulating 300 papers.
- **Step 2**: Subsequent refinement comprised removing duplicates and focusing on the abstract and conclusion sections. After this step, 150 papers remained.
- **Step 3**: In the final step, a thorough examination of the entire content of each paper was undertaken, and any unsuitable ones were excluded. This meticulous process led to the ultimate selection of 110 papers specifically associated with healthcare, IoT, and Blockchain, all included in this survey.

1.2 Contributions and comparisons to other survey articles

In this survey, we assessed the adoption of Blockchain in an IoT-based eHealth system Besides, we will emphasize the importance of blockchain in such a system and describe how the scientific community views the future of blockchain–IoT healthcare integration. To achieve our goals, we reviewed modern research and studies focusing on the most common challenges surrounding the use of Blockchain and IoT in eHealth applications. Table 1 summarizes the key findings and contributions of previous comprehensive surveys that have examined the integration of IoT and blockchain in eHealth systems. In our research evaluation, we highlighted the breakdown of the studies into various components and noted several key observations. Figure 2 shows the paper's contributions.

The survey's primary contributions include:

- A detailed examination of the value of eHealth systems, offering insights into their importance and potential impact in the healthcare domain (Sect. 2).
- An enhanced understanding of IoT, including a brief overview and exploration of its challenges, aiding readers in grasping complexities in IoT implementation in healthcare (Sect. 3).
- An investigation into IoT rules (Sect. 4), providing guidance for comprehending regulatory frameworks governing IoT, especially in healthcare applications, optimizing IoT utilization in the sector.
- A comprehensive overview of Blockchain technology and its applications (Sect. 5), offering valuable insights into the role of blockchain in enhancing healthcare systems.
- Discussion of recent research efforts in integrating IoT with Blockchain in healthcare (Sect. 6), providing a snapshot of the current state, advancements, and challenges in this evolving field.
- Exploring contributions and limitations of recent research in IoT-based healthcare integrated with blockchain (Sect. 7).

The ultimate purpose of the survey is to familiarize researchers with the relevance of IoT in the eHealth industry and the challenges that arise from it. The survey enables readers to make informed judgments about incorporating blockchains into their IoT-focused healthcare practices by studying future trends and offering solutions.

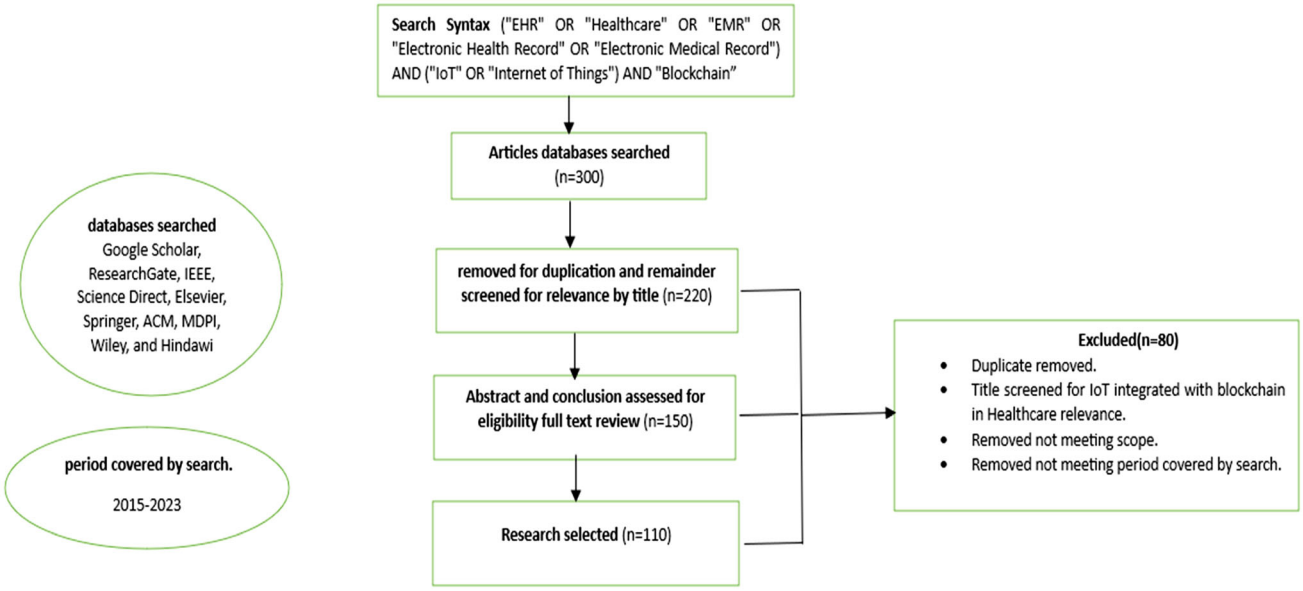


Fig. 1 PRISMA Chart for paper selection process

Table 1 Recent survey comparisons

References	Years	Blockchain	IoT	Healthcare application	Security	Privacy	Data management	Scalability
[7]	2019	X	✔	X	✔	X	X	X
[8]	2020	✔	✔	X	✔	✔	X	X
[9]	2020	✔	X	✔	✔	✔	X	X
[10]	2019	✔	✔	X	✔	✔	✔	X
[11]	2020	✔	X	✔	✔	X	X	X
[12]	2022	✔	✔	X	✔	✔	X	X
Our survey	2023	✔	✔	✔	✔	✔	✔	✔

1.3 Paper organization

The structure of the paper is as follows: the value of the eHealth system is discussed in Sect. 2. Section 3 provides a brief on the IoT and the difficulties it faces. In Sect. 4, IoT rules are investigated to assist in better comprehending the many healthcare applications that employ IoT. Section 5 presents the blockchain overview and its applications. Section 6 discusses recent research in IoT integrated with Blockchain in healthcare. Section 7 shows the contributions and limitations in recent research in IoT based on healthcare integrated with blockchain. Section 8 concludes the paper and future directions.

2 eHealth

eHealth is extremely important for public health and medical treatment. It is estimated that advancements in health and medical care can increase life expectancy by several years. They may even greatly enhance the quality of life and functional abilities [13].

eHealth is the treatment, amelioration, and diagnosis of injuries and mental disabilities in people and the improvement of their health. eHealth is provided by doctors, pharmacists, dentists, nurses, optometrists, psychologists, midwives, audiologists, and others.

eHealth [14] (Electronic Health) refers to how information technology may improve patient health and the healthcare system. Experts expect that this area of healthcare will continue to expand since technology has helped minimize wait times and some of the responsibilities placed on medical personnel. During the COVID-19 epidemic, eHealth has been immensely popular since it has

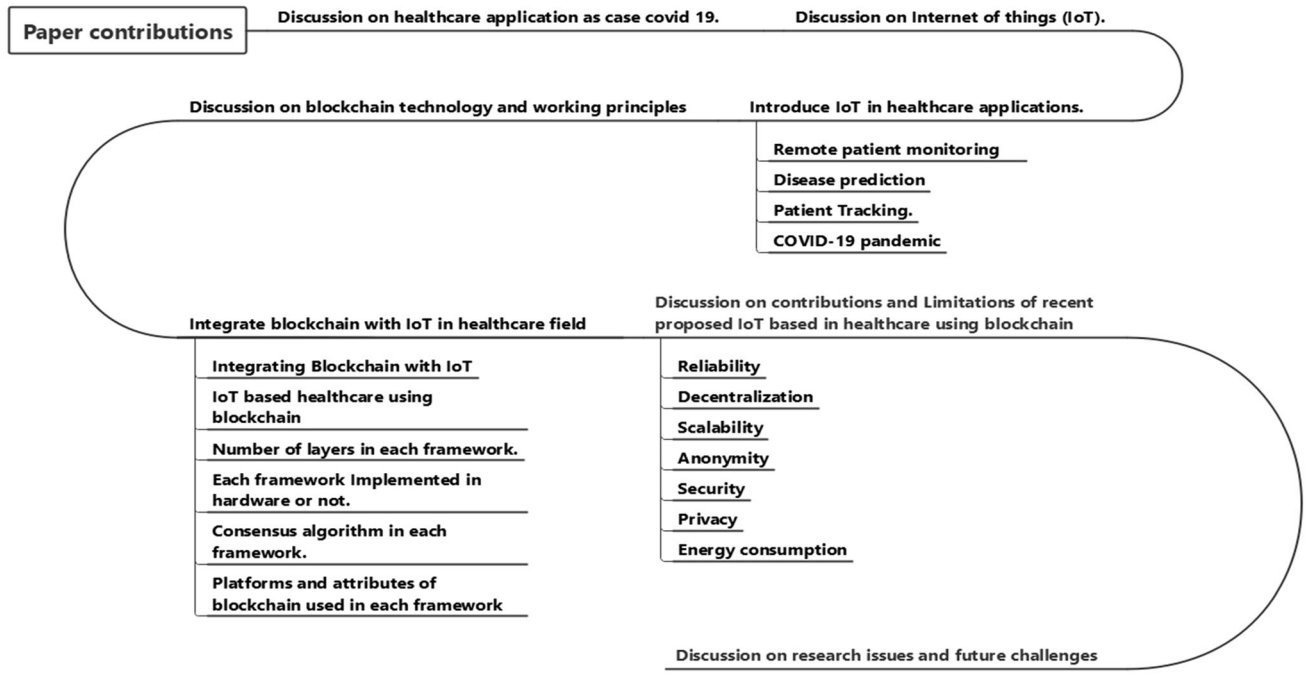


Fig. 2 Paper contributions

allowed healthcare providers to provide front-line medical treatments to patients despite the closure of local surgical facilities and hospital departments.

A study conducted by [15], which surveyed 398 healthcare professionals, found that telemedicine usage is expected to remain at a high-level post-pandemic, with over 20% of patient appointments being handled through telemedicine. This represents a significant increase from the pre-pandemic usage of 2% and possibly as high as 61% during the pandemic. Figure 3 depicts the percentage of patient appointments in the United States that were done via telemedicine before, during, and after COVID-19. The integration of IoT technology is revolutionizing conventional healthcare systems, particularly through the monitoring of patient behavior. Within healthcare systems, data collected by IoT sensors plays a pivotal role [4].

Various forms of data, like Personal Health Records (PHR), enable individuals to take charge of their health information despite facing security concerns during data transfer. Electronic Medical Records (EMR) concentrate on medical histories within a specific practice, encountering challenges in interoperability. Electronic Health Records (EHR) offer a comprehensive overview across healthcare providers, sharing similar interoperability concerns. Common issues encompass difficulties in data exchange, security vulnerabilities, and the potential for Unauthorized access. In the IoT healthcare landscape, a combination of these records is employed, presenting security challenges during data transfer that necessitate robust measures for maintaining data integrity and interoperability [16]. This transformative impact extends to patient care, where IoT solutions may mitigate the need for

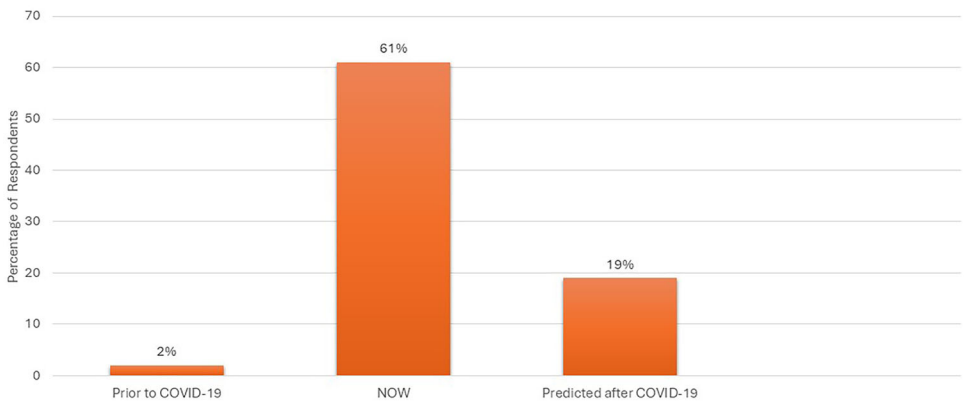


Fig. 3 April 2020, patient appointments, and telemedicine before, during, and after COVID-19 [15]

emergency department visits or hospital stays, proving particularly advantageous for individuals with mobility challenges, even enhancing convenience in utilizing public transportation [17].

3 Internet of Things (IoTs)

IoT is attracting significant attention from researchers and academics due to its ability to introduce new services and solutions across various applications [19, 20]. IoT seamlessly connects various "things" (devices) to create an IoT network infrastructure where communication, processing, and sensing activities are carried out without human intervention [21]. According to ("IoT devices installed base worldwide 2015–2025 | Statista," n.d.), by 2025, the total number of IoT-connected things (devices) in use will reach 75 billion devices.

Figure 4 demonstrates the rapid expansion of IoT-connected devices. The IoT industry is projected to experience significant revenue growth, increasing from $892 billion in a device in 2018 to approximately $4 trillion in devices by 2025. The IoT applications including Healthcare, Smart Cities, Environments, Grids, Retail, Farming, and many more [22]. Figure 5 shows the IoT's history, current, and future architecture. The gadgets will not only be connected to the epidemic [15].

SIoT is the concept of social IoT that is becoming more prevalent. It allows various social networking users to connect to devices via SIoT, enabling them to share the IoT devices in public over the internet. Therefore, SIoT creates new ways for people to communicate and interact with each other and with connected devices [23].

IoT will bring innovation to many aspects of our modern society, both at home and in the workplace. Among them, the healthcare industry is a strong challenger. Real-time patient monitoring can be made possible with IoT, which is particularly important for individuals with chronic diseases. This allows instant and continuous monitoring of the patient's state, providing healthcare providers valuable information to help manage and treat their condition [25].

From 2016 to 2025, in [24], Fig. 6 depicts the expected size of the IoT in the eHealth industry. In 2016, eHealth-related IoT sales reached about 24 billion dollars, with estimates indicating that by 2025, the previous number would rise to more than 135 billion dollars. It demonstrates the value of IoT in the eHealth industry. Implementing IoT in healthcare has several benefits, including:

- Data collection errors reduction.
- Patient care Improvement.
- Enhancing the management of hospital resources.

By automating data collection and analysis, IoT can help improve the accuracy and speed of healthcare delivery while enabling more efficient resource use.

Despite IoT-based eHealth benefits, some obstacles need to be overcome. One of these obstacles is the management of information. As information plays a critical role in the decision-making process for patient care, the massive data volume generated by IoT devices may be overwhelming. By 2025, based on the IDC (International Data Corporation), 41.6 billion IoT devices will be in use, generating 79.4 Zettabytes of data, which must be collected, stored, and analyzed securely and efficiently to be useful in healthcare ("The Growth in Connected IoT Devices is Expected to Generate 79.4 ZB of Data in 2025, According to a New IDC Forecast | TelecomTV," n.d.). This massive unstructured data must be handled in a real-time way. Processing, data collection, and interpretation need a huge amount of computing, network, and storage resources. The monitoring data must be synced and evaluated on time so the treating physician can make suitable and informed decisions.

IoT security challenges revolve around ensuring data confidentiality, integrity, and availability (CIA) [26]. Confidentiality concerns involve protecting sensitive information from unauthorized access ensuring that only authorized parties can access and interpret the data

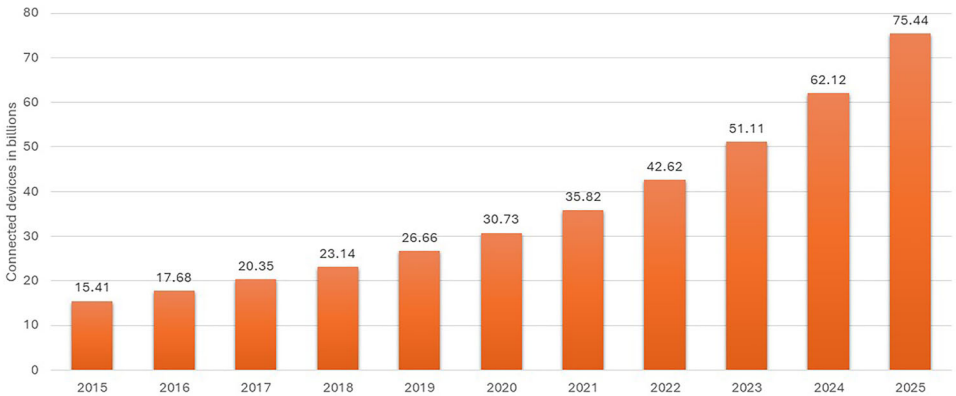


Fig. 4 IoT-connected devices in use worldwide from 2015 to 2025 [18]

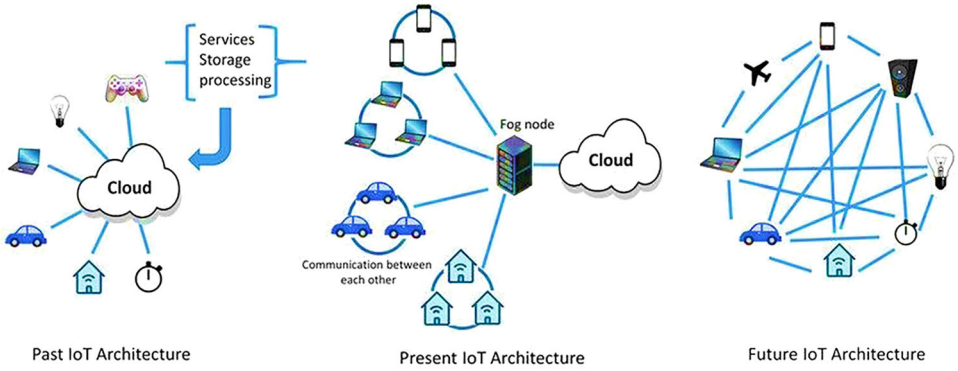


Fig. 5 Different architecture of IoT [23]

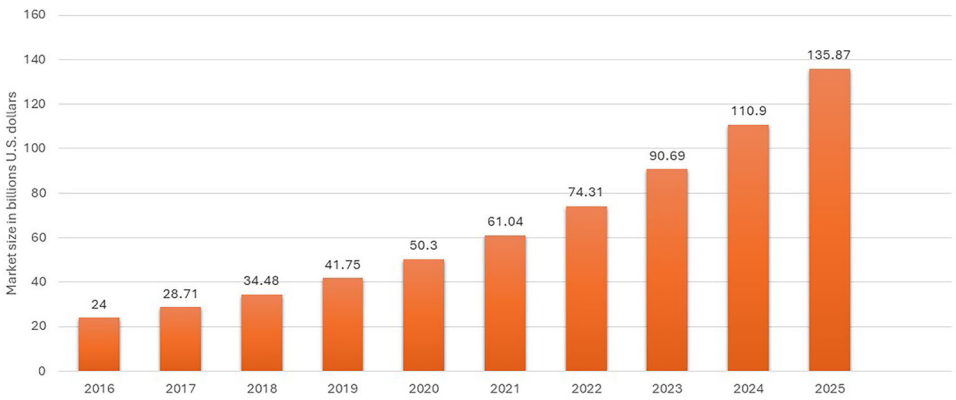


Fig. 6 IoT in the healthcare industry [24]

generated by IoT devices. Integrity focuses on maintaining the accuracy and reliability of the data, preventing any unauthorized tampering or alterations. Availability is crucial for IoT devices' continuous and reliable operation, requiring measures to prevent disruptions or denial of service attacks. IoT systems' diverse and interconnected nature intensifies these challenges, necessitating robust security measures to mitigate potential risks and vulnerabilities in this rapidly expanding and interconnected landscape. Additionally, the diversity of IoT devices and systems presents challenges for interoperability, especially as IoT is increasingly being used in large-scale projects such as smart cities where many kinds of devices and systems need to communicate seamlessly. There is no widely agreed-upon standard to follow [27]. The lack of standardization among IoT devices can make implementing successful IoT systems in healthcare challenging. One of the possible solutions to this problem is to use Blockchain. It can help to solve interoperability issues by creating a secure, decentralized network that can share data across different devices and systems. Additionally, blockchain can help to improve security by supporting a secure and tamper-proof way to save and transfer sensitive patient data. Therefore, blockchain technology is still relatively new, and its potential in IoT healthcare applications is still being explored [6].

4 Healthcare IoT applications

The Internet of Things enables sensor integration into physical components that collect health data such as heart rate, vital signs, blood pressure, and body temperature. These components will be connected to the internet through a different gateway and deliver real-time eHealth information to various authorities (analysis laboratories, rays, ambulances, hospitals, etc.(. Recent research has suggested that this information can be analyzed and interpreted using ML (Machine Learning) algorithms, which can then be used to diagnose and treat illnesses and provide proactive forecasts in some situations. This can lead to more accurate and efficient healthcare, enabling healthcare providers to make better-informed decisions about patient care. Currently, several healthcare applications [2] use IoT medical devices, as shown in Fig. 7 and Table 2.

4.1 Remotely monitoring patients

The patient's remote monitoring refers to the use of technology to collect and transmit patient data for analysis and review by healthcare providers, allowing for remote monitoring of patients. Entity management healthcare system prototype proposed to utilize eHealth sensors to gather patient's data and exchange it with the entity. The system

includes various sensors such as ECG to monitor the heart's muscle activity, BTS, accelerometers, and environmental sensors [28]. Another eHealth system employed ECG equipment to observe heart rhythm and use the k-nearest neighbor method to diagnose cardiac arrhythmias [29]. A third proposed eHealth system is an IoT-based real-time system using MQTT (Message Queuing Telemetry Transport) for remotely monitoring patients' systems, which aims to ensure the integrity of real-time ECG data [30].

4.2 The prediction of diseases

In [31] the proposed healthcare system is a mobile application using cloud and IoT networks to observe and anticipate critical illnesses. It uses the UCI Repository dataset and medical sensors to develop a systematic approach for identifying and forecasting diabetes and related medical data. A novel classification technique called the Fuzzy Rule-based Neural Classifier is presented to determine the illness and its severity. Furthermore, Al-Makhadmeh et al. proposed an eHealth system that combines the Internet of Things and neural networks to know heart properties from previous studies and forecast most heart illnesses. The authors used the University of California Irvine (UCI) dataset and MATLAB tool to calculate the system's efficiency, and the suggested method had a 99.03% accuracy with an 8.5-s time complexity [32].

In [33], the Authors proposed an eHealth system to discover chronic kidney illness. Their approach resulted in categorization with a prediction accuracy of 97.75%. They also plan to use feature selection and clustering approaches to enhance the model performance.

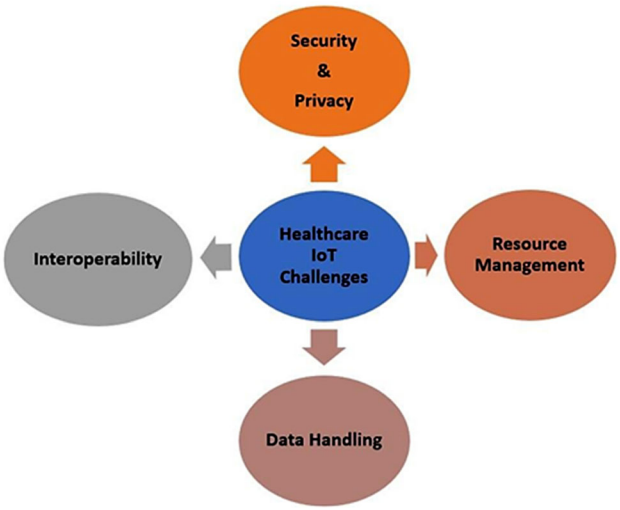


Fig. 7 Healthcare IoT applications

4.3 Tracking of patients

In [34], Alzimio is a mobile application designed to help individuals with dementia, autism, and Alzheimer's disease by utilizing geofencing and activity-based notifications. The app has been shown to effectively detect activities with an accuracy rate of over 95% and minimal delay using various threshold-based algorithms, such as "max-in-window," which results in fewer than 30 s.

Moreover, an IoT-based eHealth system for soldiers was proposed, using a heart rate and other sensors for tracking and monitoring [35].

4.4 Coronavirus (COVID-19)

In [36] a system for detecting and monitoring COVID-19 was developed, utilizing wearable sensors and mobile applications to gather current symptom information. Machine learning techniques were applied to analyze a dataset of 14,251 COVID-19 cases to identify potential virus cases.

In [37] an IoT architecture was proposed to detect the infected person. Smart sensors and IoT are being used to measure and record body signs. Individuals' temperatures aid in identifying those who are affected. In addition, it assists in maintaining social distance. Healthcare systems incorporating IoT technology can improve decision-making by utilizing cloud computing and data analysis.

Authors [38] demonstrated an IoT-based method for preventing COVID-19 in the workplace. Instead of using a manual biometric system, they recommended using face recognition. They also recommended using non-contact infrared sensors to monitor people's body temperatures and alert authorities when they exceeded a certain level.

Authors [39] proposed a method for early detection of COVID-19 illness using IoT and AI technology to reduce direct communication with infected patients. The system utilizes various advanced eHealth sensors, such as a pulse sensor, heat monitoring, and others. These technologies can work independently without human intervention.

In their work [40] authors proposed an architecture that combines SDN and NFV technologies, proposing an IoT-SDN model with multiple controllers to manage automated industrial systems during the COVID-19 pandemic. Emphasizing the heightened dependence on the internet and cloud-based activities in the current global scenario, the system aims to provide substantial automation while ensuring security and privacy in networking. It enhances the efficiency and reliability of Industry 4.0 applications, thereby effective pandemic management. The model supports intelligent and smart industry practices, encourages social distancing, and aligns with Industry 4.0 principles.

Table 2 Different healthcare applications that used IoT

Papers	Types	Years	Sensors	Contribution	Implemented in hardware/ simulated	Future work
[28]	Remote monitoring of patients	2016	ECG BTS (Body Temperature Sensor)	A prototype has been developed that utilizes an eHealth sensor to gather patient data and transmit it, allowing for the simultaneous monitoring of multiple patients	Implemented	Add new health sensors Appropriate Communication bandwidth
[29]	Remote monitoring of patients	2020	ECG sensor	ECG equipment to observe the heart rhythm Fog technology is utilized to decrease delays in data transmission by keeping patient information on local devices rather than sending it to the cloud	Implemented	the use of wearable devices Utilizing a variety of additional data mining techniques
[30]	Remote monitoring of patients	2020	ECG sensor	This system reduces the need for patients to travel, particularly those living in rural or suburban areas, thus decreasing travel time and costs	Implemented	Adding more eHealth sensors Improving performance by decreasing jitter delay and removing noise signal
[31]	Disease Prediction	2018	Medical dataset	Developed a mobile healthcare app utilizing cloud technology and the IoT to track, detect, and diagnose critical health issues	Simulated	Using various security mechanisms to improve medical data security on cloud databases
[32]	Disease Prediction	2019	Wearable watch	Enhancing the detection rate of heart conditions by utilizing a vast amount of data. Decreasing the complexity of analyzing heart disease and ensuring a low rate of incorrect classification when predicting heart data	Simulated	Enhancing the diagnosing procedure for medical diseases with IoT Utilizing effective feature selection approaches and optimal methodologies
[33]	Disease Prediction	2020	CKD dataset	Data is collected utilizing IoT devices That is linked to the individual To increase the data quality, do pre-process operations The LR model was used by combining the LR and Adam Optimization models On the tested CKD dataset, the classification model had a prediction accuracy of 97.75%	Not specified	Different feature selection and clustering approaches must be used to enhance the model
[34]	Patient Tracking	2016	Android phone	A mobile application that employs geofencing and alarms triggered by specific activities to assist individuals with dementia, autism, and Alzheimer's	Simulated	A bigger range of users/patients should be evaluated Need to implement on different platforms
[35]	Patient Tracking	2017	Pulse rate Oxygen Analyzer Sensor Temperature	An IoT-based system for monitoring and tracking the health of soldiers could include wearables or sensors that gather vital signs data and send it to a central command center for real-time monitoring. Location tracking would enable quick response in case of lost or injured soldiers and prevent soldiers from going missing in action. The system could also facilitate communication among soldiers during emergencies	Implemented	Added several sensors to provide more tracking services

Table 2 (continued)

Papers	Types	Years	Sensors	Contribution	Implemented in hardware/ simulated	Future work
[36]	COVID-19 Pandemic	2020	COVID-19 cases dataset	Proposed frameworks reduce the effect of infectious illnesses and death rates This approach would also allow for improved follow-up on patients who have recovered	Not specified	Need to evaluate the real system
[37]	COVID-19 Pandemic	2020	ITS (Infrared Thermometer Sensor) Smart watch Optical and IP Camera	Using smart sensors to detect and record body temperatures can help identify individuals who may be sick and need medical attention. This technology can also assist in maintaining social distancing by monitoring and alerting individuals if they come into proximity with others	Proposed framework	Need to evaluate the real system
[38]	COVID-19 Pandemic	2020	Camera Non-contact infrared sensor	The work that is suggested to ensure the health and safety of its employees or members	Implemented	We must set up portable system devices to verify an individual is health
[39]	COVID-19 Pandemic	2021	Pulse sensor Thermal monitoring Blood sensors	To eliminate direct interaction with patients, assist clinicians in detecting the Coronavirus remotely	Implemented	Test cases will be required for accurate evaluation

The significance of IoT has been growing recently, especially with the advent of COVID-19. As such, the value of IoT will be further examined as follows:

- IoT ensures that all data is considered when making better patient decisions. Fully interactive technology and networked health options reinforce and improve treatment efficacy.
- Advanced IoT technology enhances emergency care and makes it more efficient.
- Advanced medical technology encourages individuals to take their drugs as prescribed. On-time delivery and other vital health IoT have been shown to increase patient care comfort.
- IoT enables doctors to consult with experts from all around the world on complex issues.
- Doctors can use a variety of sophisticated sensors and technology to assist them in their work. With ease, check the patient's health and internal sentiments [28–30, 32, 38, 39].

In the utilization of sensors in healthcare settings has led to a substantial increase in data generation. These sensors, integrated into various medical devices and wearable technologies, continuously collect and monitor patient information, including vital signs, activity levels, and other health-related metrics. The continuous and real-time data streams produced by these sensors result in large volumes of data, commonly called big data. While big data offers numerous advantages in healthcare, such as predictive analytics and early detection of health issues, handling and processing such vast amounts of data can be resource-intensive and complex. As an alternative approach, researchers and healthcare practitioners also leverage datasets that may not fall into the big data category but are still valuable for analysis [31, 33, 36]. These datasets may be more manageable in size and easier to work with, providing meaningful insights without the same level of computational demands as big data analysis.

As shown in Fig. 8, several problems exist in eHealth based IoT, including:

- Keeping data secure and private is the most challenging task since the daily data acquired is so huge [41].
- Overusing medical devices might generate network congestion and poor data transfer speeds.

Obtaining IoT devices remains a huge challenge [6]. Blockchain technology presents a solution to these issues, and we will explore the different types of blockchains and their features in the next section. Additionally, we will

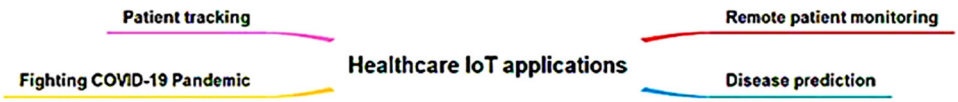


Fig. 8 Challenges of IoT in healthcare

discuss the advantages of using blockchain in healthcare and the consensus methods that are employed in healthcare.

5 Blockchain technology

The term "Blockchain" was first coined by [42] to describe the technology behind the digital currency Bitcoin. Blockchain technology is a distributed and peer-to-peer network in which all transaction records are distributed across all nodes.

Three types of blockchains have been identified: public, private, and consortium, which are used to connect different organizations and promote cooperation among the parties involved. Like private blockchains, consortium blockchains do not have transaction costs, and publishing new blocks is not computationally expensive. However, it doesn't provide complete decentralization and censorship resistance; it still provides auditability and reduces the transaction processing time [43].

The following are blockchain technology's key features:

(1) *Decentralization* centralized networks incur expenses and have performance limitations. In contrast, blockchain-based infrastructures allow for transactions between two nodes without a central organization needing to keep track of data or authorize transactions.
(2) *Immutability* the blockchain is censorship-resistant and difficult to tamper with because all peers agree upon all new updates through decentralized consensus algorithms.
(3) *Transparency* unlike centralized systems, where the central server has complete control over everything, blockchain technology provides a high degree of transparency because all peers have entry to all transaction information that has ever occurred in their network [44].
(4) *Security* using the public key system and the consensus mechanism makes the blockchain resistant to various attacks. Additionally, blockchain eliminates a single point of failure, making it more secure than centralized systems [45].
(5) *Anonymity* blockchain technology allows for anonymity by protecting users' privacy using anonymous identities on the shared distributed ledger [46].
(6) *Cost* blockchain technology can significantly lower costs associated with setup and maintaining centralized systems by utilizing the processing power of communication devices. Unlike centralized systems which require extensive hardware and software, blockchain's distributed nature obviates the need for a centralized server [47].

The features of using blockchain in medical eHealth such as:

1. Patients may submit records to anybody without worrying about data corruption or manipulation since the blockchain is immutable and traceable.
2. A medical record created and uploaded to the blockchain will work similarly to be safe.
3. Patients can have some say in how their medical information is used and shared by the research institutions. Any entity needing medical information about a patient may use the blockchain to obtain the required authorization.
4. A reward mechanism can also motivate the patient's positive behavior. For example, they can earn tokens for following a care plan or being healthy. They can also be compensated with tokens for providing data for clinical trials and research.
5. Because of the type of product they handle, pharmaceutical firms must have a highly secure supply chain. Pharmaceuticals are often stolen from the supply chain and sold illegally to various customers. Furthermore, counterfeit pharmaceuticals alone cost these businesses roughly $200 billion every year. A transparent blockchain will assist these firms in enabling close tracking of medications back to their place of origin,

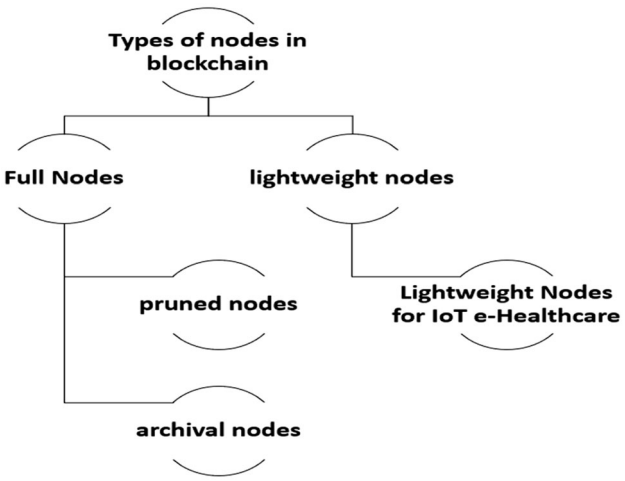


Fig. 9 Types of nodes in the blockchain

therefore reducing the incidence of counterfeit medication. As shown in Fig. 9, Full and lightweight nodes are different types of nodes that may be used for blockchain-based operations. The blockchain network's nodes oversee mining, data storage, block generation, block validation, cryptocurrency purchasing and distribution, and information distribution among peers.

Research on consensus algorithms has been a prevalent topic for the past 30 years, even before the creation of blockchain technology. Reference [48] give a summary of some of the early work in distributed systems consensus. Consensus algorithms play a vital role in the functioning of blockchain technology. They are designed to securely update and maintain replicated shared states across all peers in the network. By using consensus methods, the blockchain can ensure that all copies of the shared state agree and synchronize at any given moment, a key aspect of the blockchain's state machine replication system. According to [49] and [50], deterministic consensus cannot tolerate errors in completely asynchronous communication models. Therefore, partial synchrony assumptions and maximum latency limits for propagating transactions are necessary [51]. In previous work on consensus procedures, the building elements that went into establishing "Decentralized" consensus algorithms utilized in blockchain networks included cryptography and partial synchronous, as well as predecessor designs and suggestions of digital currency [52, 53].

There are many forms of decentralized blockchain consensus algorithms currently in use, as well as their applicability for IoT networks, particularly in the supply of healthcare services as follows [54]:

1. *Proof of Work* (*PoW*): PoW requires high network bandwidth, making it unsuitable for IoT applications. However, it is widely used in various platforms, so it is likely to be incorporated into healthcare services.
2. *Proof of Stake* (*PoS*): In this algorithm, the next block is mined by selecting a node through a lottery or random selection process. It is considered the most democratic system available. This mechanism may be a viable solution for eHealth application submissions due to its democratic nature.
3. *Delegated Proof of Stake* (*DPoS*): is democratically representative. It speeds up transactions but comes at a higher price in terms of centralization. There is a procedure for identifying rogue delegates and voting them out. As a result, it has great potential for use in eHealthcare settings.
4. *Leased Proof of Stake* (*LPoS*) LPoS enables low-balance nodes to participate in a lease contract. This algorithm has the potential to foster a high-quality eHealth service.
5. *Proof of Significance* (*PoI*) it is a step forward from PoS. It considers the balance of nodes as well as the reputation of nodes. It's a more efficient network. It is suggested to be used for eHealth care services since doctors' reputations may be used to help people make decisions.
6. *Practical Byzantine Fault Tolerance* (*PBFT*) this algorithm is more efficient and superior to PoW and PoS, making it suitable for private blockchain use. It also has a low tolerance for malicious nodes. The aim is to apply this protocol to influence the use of eHealth services.
7. *Byzantine Fault Tolerance Delegated* (*dBFT*) is a step forward from PBFT. Nodes are chosen from different nodes as a result, it appears that eHealthcare services are gaining popularity.
8. *Proof of Capacity* (*PoC*) this is a step forward from Proof of Work (PoW). It will most likely need to store a large amount of data to mine the next. Other nodes block it. It is incompatible with the Internet of Things. We also advise against using it for health-related purposes services.
9. *Proof of Activity* (*PoA*) this approach combines PoW and PoS to validate transactions. The process starts with PoW, and then a group of validators performs PoS to place the transaction in the Miner's header. However, due to its high latency, PoA is not suitable for Internet of Things (IoT) applications and, therefore, is not an appropriate choice for eHealth.
10. *Proof of Burn* (*PoB*) this is the process of transferring bitcoin to an address that cannot be recovered. Burned coins give a miner a higher priority in terms of mining. Because it is dependent on the presence of a monetary framework, it is ideal for cryptocurrency implementation but terrible for IoT. It is unsuitable for eHealth-related applications due to its random burning technique.
11. *Proof of Elapsed Time* (*PoET*) Intel proposed a low-energy alternative to Proof of Work (PoW). It uses a random wait time to select the winning miner and is considered IoT-friendly due to the use of trusted execution environments such as Intel's Software Guard Extension (SGX). However, it is highly specialized for SGX-based environments and may not be suitable for eHealth.
12. *The Stellar Consensus Protocol* (*SCP*) is an advancement from the Practical Byzantine Fault Tolerance (PBFT) algorithm. It comprises two parts: the nomination protocol and the ballot protocol. It is well-suited for low-latency microfinance services.

Therefore, SCP may be a suitable option for a decentralized application (dAPP) developer to use when creating a healthcare service.

The comprehensive evaluation of consensus algorithms in the realm of blockchain technology involves an in-depth analysis based on a multitude of critical parameters. These essential factors, encompassing blockchain type, transaction rate, scalability, adversary tolerance model, experimental setup, latency, throughput, bandwidth, communication model, communication complexity, and attack finality, collectively serve as crucial metrics for a nuanced comparison. This extensive set of parameters forms the foundation for assessing various consensus algorithms, providing insights into their strengths and weaknesses within the dynamic landscape of blockchain technology.

In the comparative study of recently proposed algorithms [55, 56], such as Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Leased Proof of Stake (LPoS), Proof of Significance (PoI), Practical Byzantine Fault Tolerance (PBFT), Byzantine Fault Tolerance Delegated (dBFT), Proof of Capacity (PoC), Proof of Activity (PoA), Proof of Burn (PoB), Proof of Elapsed Time (PoET), and the Stellar Consensus Protocol (SCP), distinctive attributes emerge, significantly influencing their suitability for diverse blockchain applications. For example, PoW, commonly associated with public blockchains, showcases medium to high transaction rates but exhibits moderate scalability. Despite resilience to Sybil attacks, PoW is susceptible to 51% attacks, requiring substantial computational power and resulting in moderate latency and throughput with elevated bandwidth requirements. Conversely, PoS, applicable to both public and private blockchains, offers higher scalability with lower computational demands, albeit vulnerable to Long-Range attacks. DPoS introduces governance layers, reducing latency and enhancing throughput, while LPoS maintains similar characteristics with a slightly lower throughput. The adaptability of PoI is highlighted, offering transaction rates and scalability in the medium range, with performance contingent on the chosen significance metric. PBFT and dBFT, tailored for private blockchains, exhibit high transaction rates, moderate scalability, and resilience to a limited number of malicious nodes. Each consensus algorithm introduces unique trade-offs, underscoring the importance of considering specific application requirements and network conditions during their selection.

6 IoT-based healthcare using blockchain

In this section, we evaluated the integration of Blockchain into an IoT-based eHealth system. Additionally, we will highlight the significance of blockchain within this system and explain the scientific community's perspective on the future integration of blockchain and IoT in healthcare. To achieve our goals, we conducted a thorough review of recent research and studies. Initially, we discussed the importance of blockchain in IoT applications, presenting related work in this domain. Following that, we delved into the impact of this integration in healthcare applications and presented key research findings in this evolving field.

6.1 Integrating blockchain with IoT

IoT systems encounter various challenges, including interoperability issues, resource constraints, and security vulnerabilities. Blockchain emerges as a powerful solution by introducing a decentralized and tamper-evident ledger that significantly enhances the confidentiality, integrity, and availability (CIA) of data within IoT networks. The distributed and consensus-driven nature of blockchain ensures the integrity of IoT data, making tampering highly resistant and fostering trust in the information generated by connected devices. Its cryptographic techniques improve confidentiality by encrypting data during transmission and storage, restricting access to authorized entities. Moreover, the decentralized structure of blockchain strengthens availability, ensuring continuous operation despite potential node failures or attacks. These features fortify the security of IoT systems and establish a robust foundation for transparent, trustworthy, and resilient data management across interconnected devices. A comparative analysis of the features and capabilities of both IoT and blockchain technologies provides valuable insights into their synergies and distinctions, Table 3 presents a comparison of these features and capabilities [8].

Furthermore, integrating blockchain technology into IoT systems can improve their scalability and stability. The distributed nature of blockchain allows for distributed data saving and processing, which can support many devices and transactions [57]. In comparison to existing IoT solutions, blockchain provides the following possible benefits as shown in Table 4 [58].

6.1.1 The blockchain of things architecture

In [58], an architecture was proposed to integrate IoT with Blockchain. This architecture has two advantages:

- it provides an abstraction from IoT's lower levels,

Table 3 Comparison between IoT and Blockchain

Parameters	IoT	Blockchain
Privacy	X	✔
Security	X	✔
Latency	X	✔
Scalability	X	✔
Resources	Restricted	Consumed
Scalability	✔	X
System Structure	Centralized	Decentralized

- it offers consumers services based on blockchain technology.

There are five sublayers in the blockchain, as shown in Table 5. The overlay network is a part of the network sublayer in IoT systems. It comprises digital or tangible links connecting the nodes in the communication networks that form the foundation, which can be cabled or Wi-Fi. The overlay network creates a logical topology on the physical connection's infrastructure, allowing the nodes to communicate and exchange data. It serves as the communication backbone of the IoT structure, enabling the devices to link and interact. The architecture of IoT-based connection is depicted in Table 6, along with comparisons of related protocols.

In the consensus sublayer, there are many different consensus algorithms. Still, we need to choose a consensus algorithm more suitable for IoT in [59] proposed that PoS, DPoS, and LPoS are partially compliant with IoT, but PoET is more supported and compliant with IoT.

6.1.2 Related work of IoT with Blockchain

Many studies have touted blockchain technology as the answer to addressing confidentiality and safety concerns in the IoT structure [60]. The article introduces the security problems that arise in IoT systems, specifically focusing on the layers of IoT systems. The authors also survey recent solutions to these security problems and propose that blockchain technology could be a practical way to address these challenges. Reference [61] reviewed IoT and industrial IoT (IIoT) concerns and classified them according to their susceptibility. Then, to address some of the security challenges, he proposed blockchain technology. They also discussed some of the issues that blockchain presents concerning IoT.

Similarly, Reference [62] the authors evaluated various security measures for IoT and identified a lack of datasets as a concern among academics and practitioners. They proposed utilizing blockchain to establish a safe environment for exchanging IoT datasets while acknowledging some difficulties associated with implementing this technology. Furthermore, Reference [63] the authors created a blockchain-based IoT framework that aims to provide a confidential and safe system while minimizing the technical burden of blockchain [64]. Also examine the ability of blockchain technology to analyze the IoT system's security

Table 4 Solutions for IoT problems using Blockchain

IoT problem	Solution using Blockchain
Poor interoperability	IoT data is being transformed and stored in blockchains
	P2P overlay network, which enables ubiquitous internet access, blockchains are built
Security	Blockchain uses cryptography techniques and digital signatures such as the Elliptic curve
	Using some blockchain technologies to improve security in IoT, such as a smart contract
Traceability and reliability	Blockchain is traceable
Resource Constraints	Using lightweight nodes that can verify a transaction's trustworthiness without downloading or storing the entire blockchain
Failure point	Blockchain enables individuals and entities to communicate and transact in a distributed way without needing a centralized authority to manage the flow of information and transactions
Scalability	The blockchain can be leveraged to create a scalable solution that can manage a large number of IoT devices due to its ability to share and validate data across a network of participants
Flexibility	The technology of Blockchain, using various open-source solutions, allows for a flexible setting in which a variety of IoT devices can operate by providing a distributed platform that provides secure and transparent communication between them
Costs	The decentralized design of blockchain technology ensures that data transfer and exchange are more secure, as it reduces the risk of a failure point. This also eliminates costly investments in servers with advanced software and hardware capabilities

Table 5 Blockchain layers used in IoT

Blockchain layers	Description
Data sub-layer	Blockchain uses asymmetric cryptographic algorithms and hash functions to get data from lower-level IoT (Internet of Things) devices, such as those in the perception layer, and secure that data by encrypting it and adding a digital signature, providing an additional layer of security and integrity to the data transferred
Network sub-layer	Responsible for communicating between nodes (wired or wireless communication)
Consensus sub-layer	In this layer, implement consensus algorithms as explained in the blockchain section
Incentive sub-layer	In this blockchain layer, participants who contribute to the distributed consensus mechanism, such as through mining, should be rewarded for their efforts in maintaining and validating the network
Service sub-layer	Industries such as manufacturing, logistics, supply chains, food and agriculture, and utilities, among others, could benefit from implementing blockchain-based services, as they support a safe, transparent, and tamper-proof way of managing transactions and data

Table 6 Network communication protocols

Protocol Standards	Bandwidth	Range	Cost
Wi-Fi	100+ Mbps	25–50 m	Low
Cellular	5G: 50 Mbps, 4G: 15 Mbps, 3G: 4 Mbps	1–5 km	Medium
Bluetooth	25 Mbps	50–100 m	Very low
LPWAN (NB-IoT)	200 kbps	1 m to 10 km	Medium
Satellite	50 Mbps	Anywhere	Very high

needs and how combining the IoT with blockchain might solve these problems [7]. The authors gave an overview of the security issues and risks in IoT applications and discussed various solutions that are being developed to enhance trust in these systems. Four specific solutions, FC (fog computing), EC (edge computing), blockchain, and ML (machine learning), were presented as ways to improve security in IoT. The overall subject of IoT security was also examined.

Furthermore, Reference [65] reviewed IoT security challenges before suggesting the blockchain as a potential solution to these problems. They also talked about how IoT and blockchain may work together. Furthermore, Reference [66] the authors presented a smart contract as a solution to address confidentiality and security issues in IoT systems and enable safe interactions between IoT devices. By utilizing blockchain technology, their approach enables decentralization of access control, authentication, and payments. Furthermore, in their work [67] the authors introduced an optimized and comprehensive framework for resource management within a Blockchain-enabled software-defined Internet of Things (IoTs) ecosystem. The framework incorporates a novel cluster-head selection algorithm and a distributed flow-rule verification technique, ensuring network consistency and security. The proposed Blockchain-enabled SDN-IoT architecture exhibits improved average throughput, energy utilization, and overall end-to-end delay compared to a traditional Blockchain approaches. Blockchain approaches. In [68], the author presented a distributed model for smart cities incorporating Blockchain, Software-Defined Networking (SDN), and Network Function Virtualization (NFV). A key contribution is an energy-optimized cluster head selection algorithm designed for efficient procedures. The SDN controller oversees IoT device activities, and Blockchain is employed for detecting and mitigating cyber-attacks in IoT networks. Experimental results demonstrate the superiority of the proposed architecture over existing ones, such as Core and DistArch-SCNet. The presented model exhibits improved throughput, response time, gas consumption, and communication overhead, leading to notable enhancements in overall system performance [69].

The study provided an overview of using blockchain technology to address safety and confidentiality concerns on the Internet of Things and presented the advantages and potential drawbacks of integrating blockchain-based IoT. Similarly, Reference [70] gave a study to establish the specifications for developing an IoT identity management system. They then advocated combining blockchain with the IoT to create a more efficient identity management system to deliver more confidence and effectiveness. Furthermore, Reference [71] presented a blockchain-based

integrated IoT infrastructure to protect the integrity of sensing data. Their platform allowed end-users and devices to monitor and control each other in real-time. The results showed that their technology might be a suitable fit for IoT devices with limited resources. Furthermore, Reference [72] the framework proposed using Ethereum for less-power IoT devices to address power consumption issues during communication, transaction verification, and security. Blockchain was suggested to enhance access control efficiency and effectiveness [73]. For example, I presented an access management system based on the blockchain to address confidentiality and security issues in IoT systems. As a decentralized access manager, they used blockchain to make access decisions [75].

The author also proposed using blockchain to create a decentralized control paradigm for Internet of Things systems. They believed this could increase the efficiency of handling access management in IoT solutions. Furthermore, Zhang et al. (2019) the author proposed an access control mechanism based on a smart contract system that utilizes several ACCs (access control contracts).

The cost-effective use of blockchain technology has been proposed to enhance the security and confidentiality of healthcare data [77]. One way to utilize blockchain is to improve the confidentiality of health information by implementing a pseudonym-based encryption system, known as PBE-DA, for electronic health records. Additionally, blockchain can serve as a bridge between medical systems and the Internet of Things health devices. In addition Mishra and Tyagi (2019) suggested a solution to use blockchain technology to produce an intrusion detection system for IoT that can detect unauthorized entry and analyze connection activity. They applied their suggestion to protect patient data in the healthcare industry. Table 7 also includes current studies on blockchain and IoT integration (Fig. 10).

The study presents the statistical data of the reviewed publications by relevant fields and the role of blockchain in various IoT solutions, with many of the articles focusing on utilizing blockchain in eHealth (Uddin et al. 2021). As recent researchers are interested in healthcare, the next section reviews the state of the arts related to IoT-based healthcare by blockchain.

6.2 IoT-based healthcare using blockchain

The sensitivity of healthcare information requires strict privacy measures. The execution of blockchain in eHealth can address these concerns, enhance service efficiency, and facilitate the shift towards decentralized eHealth systems.

Here is an example of how blockchain can benefit IoT-based healthcare systems. It can be represented in Fig. 11. IoT devices collect patient data, such as vital signs, medication adherence, and other health-related information. This information is then transferred to a blockchain network, which is decentralized and secure. The information is saved on the blockchain, which provides an immutable ledger of all transactions.

Smart contracts and rules can be used to define how the data is used and shared. For example, a smart contract could be used to ensure that only authorized healthcare providers have access to the patient's information. Rules can be set up to govern how the data is used, such as who can access it and for what purposes. Healthcare providers can access the data on the blockchain network if they are authorized to do so. This can help improve patient care, as providers can access real-time data about their patients' health status.

Overall, blockchain technology can be very helpful for IoT-based healthcare systems, as it provides:

(1) *Secure Data Sharing* blockchain technology provides a secure and decentralized way to store and share data. Patient data is encrypted and stored on a distributed ledger, which authorized healthcare providers can access. This ensures that patient data is secure and cannot be tampered with or accessed by unauthorized parties.
(2) *Improved Interoperability* blockchain technology can help to improve interoperability between different healthcare systems. Data stored on a blockchain can be accessed by different healthcare providers, regardless of the system they are using. This can help to ensure that patient data is available to providers when and where they need it.
(3) *Enhanced Data Privacy* blockchain technology can help to protect patient data privacy. Data stored on a blockchain is encrypted and can only be accessed by authorized parties. Patients can control who has access to their data and can revoke access at any time.

The following literature highlights the objectives of blockchain-based IoT in healthcare. Literature work can be categorized into different domains, each contributing unique perspectives and solutions to enhance healthcare through technological innovation.

6.2.1 Digital healthcare systems

Author [79] proposed a novel protocol, "Blockchain-enabled IoMT Authenticated Key Exchange" (B-IAKE), this work establishes a distributed environment within the Internet of Medical Things (IoMT). By leveraging Hyperledger Fabric and smart contracts, it eliminates the need for a central trusted entity, ensuring secure access to IoMT-generated data.

Table 7 Current studies on blockchain and IoT integration

Papers	Survey	Framework	Security	Privacy	Healthcare papers
[7]	✔	X	✔	X	X
[60]	✔	X	✔	X	X
[61]	✔	X	✔	X	X
[62]	✔	X	✔	X	X
[74]	X	✔	✔	X	X
[64]	✔	X	✔	X	X
[65]	✔	X	✔	X	X
[66]	X	X	✔	✔	X
[69]	✔	X	✔	X	X
[70]	✔	X	✔	✔	X
[71]	X	✔	X	X	X
[72]	X	✔	✔	✔	X
[73]	X	✔	✔	✔	X
[75]	X	✔	✔	X	X
[76]	X	✔	✔	X	X
[77]	X	✔	X	✔	✔
[78]	X	X	✔	X	✔

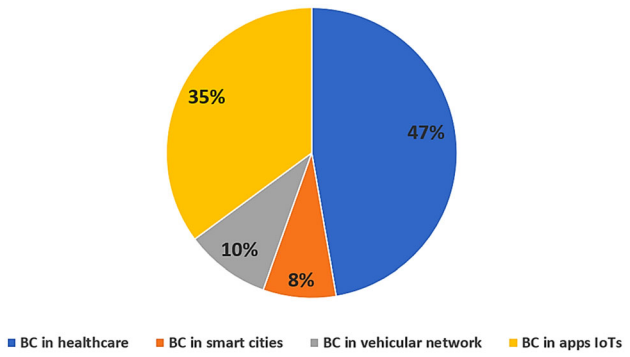


Fig. 10 Using BCs in various IoT applications

6.2.2 Fighting COVID-19

In [3] integrating cognitive computing, IoT, and Blockchain, authors proposed a comprehensive healthcare solution to manage the effects of the COVID-19 epidemic. The architecture spans network, IoT/Blockchain/AI layers, employing smart contracts for effective coordination. In [80] addressing challenges associated with the COVID-19 pandemic, this research delves into the design of IoT and Blockchain systems. The proposed architecture, although not explicitly detailed, contributes solutions proven to be effective in various scenarios. In [81] authors presented a blockchain-enabled Internet of Medical Things (IoMT) system, this study focuses on confidentiality issues. The architectural layers include a device, EC, blockchain network, and data analytics, with an emphasis on combating challenges related to COVID-19. In [82] authors Introduced a telemedical laboratory service, this work employs Cloud Computing, Blockchain, and IoT layers. Clinical tests conducted on patients using IoT medical equipment are communicated instantly, showcasing a distributed approach to healthcare. Authors [83] proposed a zero-knowledge blockchain architecture for Bahrain's IoT smart cities, this study addresses the secure sharing of health information. The architecture involves user layers, data query layers, data structure layers, and existing database infrastructure layers.

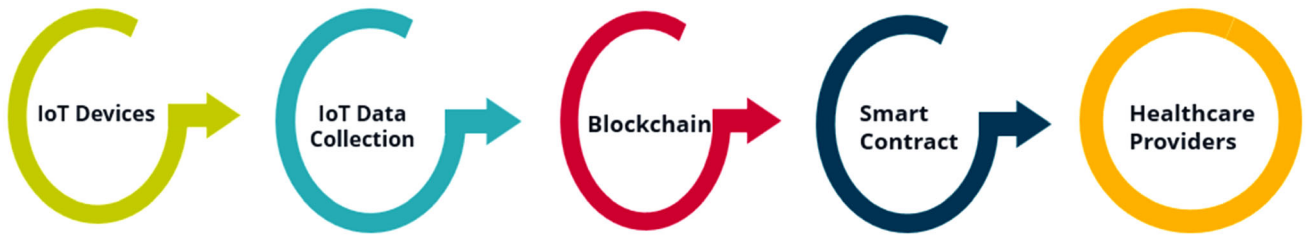


Fig. 11 Diagram of blockchain for IoT-based healthcare

6.2.3 Patient monitoring

In [84] authors utilized Hyperledger, this work employed blockchain for secure data storage in patient monitoring. The proposed architecture involves IoT sensing and gateway layers, ensuring tamper-proof storage of medical sensor data. Authors [85] focused on a mobile crowdsourcing system for diabetes research, this study integrates local users, remote users, and mHealth fog services. Continuous Glucose Monitoring (CGM) devices connected to the IoT form the basis of patient monitoring [86]. Proposing a patient monitoring architecture with sensor networks, blockchain cloud networks, and user interfaces, this work emphasizes federated learning and smart contracts for secure and private healthcare.

6.2.4 Drug transportation

In [87] the context of pharmaceutical supply chain management, this study implements a blockchain system. The architecture involves sensor and blockchain layers, demonstrating efficiency in transaction latency and energy consumption.

6.2.5 IoT applications in healthcare

Authors [88] Introduced a multiagent system architecture utilizing private, distributed blockchain, this work focuses on lightweight and secure solutions for Internet of Things (IoTs) systems in healthcare.

In Table 8 provides an overview of various healthcare applications utilizing blockchain technology. Notably, the applications cover diverse aspects of healthcare, ranging from patient monitoring to fighting COVID-19. The proposed architectures, consensus algorithms, and platforms employed differ across studies. In the digital healthcare system proposed in [79], a novel protocol named "Blockchain-enabled IoMT Authenticated Key Exchange" (B-IAKE) is introduced, leveraging Hyperledger Fabric. Similarly, in [3], a solution integrating cognitive computing, IoT, and blockchain is proposed for managing the impact of COVID-19. The patient monitoring system in [84] utilizes Hyperledger, emphasizing secure data storage through blockchain. The study [87] focuses on drug transportation, implementing a hardware-based blockchain system with AES-128 encryption and SHA-256. moreover, the IoT applications in healthcare proposed in [88] introduce a multiagent system architecture with a lightweight consensus algorithm and Diffie–Hellman key exchange. Frameworks proposed in [80–82] address fighting COVID-19, each introducing distinct architectures and platforms (e.g., Ethereum, Hyperledger). Furthermore, Reference [83] proposes a zero-knowledge blockchain for IoT smart cities in Bahrain, ensuring secure health information sharing. Patient monitoring solutions presented in [85, 86, 89] highlight various aspects, such as federated learning, private smart healthcare architecture, and proof of concept with enhanced homomorphic encryption. Each study brings its unique approach to leveraging blockchain in healthcare, contributing to the evolving landscape of IoT-based healthcare applications.

In Table 9 compares the limitations of the discussed frameworks. While some frameworks exhibit strengths in decentralization, scalability, and security, others may fall short in certain aspects, such as energy consumption, reliability, and anonymity. The variations in these attributes emphasize the trade-offs inherent in designing blockchain-based healthcare systems.

In Table 10 summarizes the contributions of various healthcare applications utilizing IoT. Each study addresses specific challenges in healthcare, ranging from secure key exchange [79] and COVID-19 management [3, 81] to drug transportation [87] and patient monitoring [85, 86, 89]. These contributions collectively advance the understanding and implementation of blockchain and IoT in healthcare, providing valuable insights into diverse applications and potential improvements for future developments.

7 Open research issues and future challenges

Blockchain technology is still in its early stages, but it has the potential to be powerful. As a result, despite its many benefits, it is confronting several development obstacles, as well as in terms of IoT adoption in healthcare. Overcoming these challenges can be categorized into eight main categories, as demonstrated in Fig. 12. To summarize these challenges and provide potential solutions, we have included Table 11, which outlines each challenge and suggests an algorithm to address it.

7.1 Limited resources

IoT devices frequently have limited resources, such as limited computational power, storage, battery life, and network connectivity. In contrast, blockchain's centralized consensus processes often require significant computational resources and energy. For instance, the PoW mechanism utilized in Bitcoin has been shown to consume a large amount of energy [57]. Because of this, low-power IoT devices may be unable to handle consensus processes requiring a significant amount of energy. Additionally, the large amount of information in blockchains makes implementing them fully on IoT devices infeasible. As of September 2018, the Bitcoin blockchain has grown to

Table 8 Comparison between frameworks in IoT-based healthcare using blockchain

References	Years	Application type	Layers	Hardware implementation	Consensus algorithm	Attributes	Platforms
[79]	2023	Digital healthcare system	Not specified	Proposed architecture	Not specified	Smart contract	Hyperledger
[3]	2022	Fighting COVID-19	Network Layer IoT/ Blockchain/ Ai Layer Applications Layer	Proposed architecture	Not specified	Smart contract	Proposed by author
[84]	2022	Patient Monitoring	IoT sensing Layer IoT gateway Layer	Hyperledger	Permissioned consensus algorithm	Smart contract	Hyperledger caliper
[90]	2019	Patient Trackability	Not specified	NS2	Not specified	SHA-256	Proposed by author
[87]	2021	Drug transportation	Sensor Layer Blockchain Layer	Implemented in hardware	PoAh [58]	AES-128 Encryption algorithm SHA-256	Proposed by author
[88]	2021	IoT Applications (healthcare)	Local Blockchain Manager Fog Blockchain Manager Cloud Blockchain Manager	Proposed architecture	Lightweight consensus algorithm	Diffie–Hellman Key exchange algorithm asymmetric algorithm	Private blockchain
[80]	2020	Fighting COVID-19	Not specified	Proposed architecture	Not specified	Not specified	Proposed by author
[81]	2020	Fighting COVID-19	Device Layer EC (edge computing) Layer Blockchain network Layer Data analytics Layer	Proposed architecture	Not specified	Asymmetric encryption/ decryption smart contracts	Proposed by author
[82]	2020	Fighting COVID-19	Cloud computing Layer Blockchain Layer IoT Layer	Ethereum	POW	Smart contract	Ethereum

Table 8 (continued)

References	Years	Application type	Layers	Hardware implementation	Consensus algorithm	Attributes	Platforms
[83]	2021	Fighting COVID-19	User Layer Data query Layer Data structure Layer Existing database infrastructure Layer	Ethereum	POW	Smart-contract SHA256	Ethereum
[85]	2019	Patient Monitoring	Local users Remote users mHealth fog service	Ethereum OrbitDB, Android, ARMbian	POW	Smart contract GlucoCoin	Ethereum
[86]	2022	Patient Monitoring	Sensor network blockchain cloud network User interfaces (monitories)	Proposed architecture	Not specified	Federated learning. smart contracts	Proposed by author
[89]	2022	Digital healthcare system	Not specified	Hyperledger Fabric PyCharm	proof of concept	Enhanced homomorphic encryption (EHE), smart contracts	Hyperledger Fabric

Table 9 Comparison between limitations in different research

References	Reliability	Decentralization	Scalability	Anonymity	Security	Privacy	Energy consumption
[79]	X	✔	✔	X	✔	X	X
[3]	✔	✔	✔	✔	✔	✔	X
[84]	X	✔	X	X	✔	✔	X
[90]	X	✔	X	X	✔	X	X
[87]	X	✔	X	X	X	X	✔
[88]	X	✔	X	X	✔	✔	X
[80]	X	X	✔	X	✔	X	X
[81]	X	✔	X	X	✔	✔	X
[82]	X	✔	X	✔	✔	X	X
[83]	X	X	✔	X	✔	X	X
[85]	✔	✔	✔	X	X	X	X
[86]	✔	✔	✔	X	✔	✔	X
[89]	✔	X	✔	✔	X	X	X

almost 185 GB, making storing the entire blockchain on each IoT device impractical.

7.1.1 Suggested solution

Utilizing mobile edge computing (MEC) and cloud computing technologies can help IoT devices overcome their resource limitations. IoT devices can function as lightweight nodes, storing only a portion of the blockchain data (such as the hash value), carrying out less computationally demanding tasks (e.g., initiating transactions), and utilizing Mobile Edge Computing and cloud for more computationally heavy tasks [91]. Fog/Edge-based design reduces latency while allowing for more computational complexity with limited resources [91]. This way, applications that require high processing power and quick

Table 10 Different healthcare applications that used IoT

References	Contribution
[79]	Proposed a novel protocol known as "Blockchain-enabled IoMT Authenticated Key Exchange" (B-IAKE), designed to establish a distributed environment using Hyperledger Fabric within the Internet of Medical Things (IoMT). This protocol effectively removes the requirement for a central trusted entity and guarantees secure access to data produced by IoMT devices
[3]	A healthcare solution that combines cognitive computing and IoT with Blockchain has been proposed. The proposal is effective in managing the effects of the COVID-19 outbreak in the examples given
[84]	For safe data storage, the suggested concept employs blockchain technology. The proposed solution for secure data storage utilizes blockchain technology. Medical sensor data is stored in a blockchain format on a medical server, making it tamper-proof and preserving patient privacy. This enhances the confidentiality of the eHealth services
[90]	The proposed framework outlines the use of blockchain in eHealth to improve and strengthen the security, transparency, and accessibility of electronic records and to track the movement of medical documents and pharmaceuticals from provider to patient using IoT devices. It emphasizes the need for blockchain to collect and record data on intermediary activity, patient records, and the shipping process between providers and patients
[87]	In the context of this research, a blockchain system was developed to manage the supply chain of pharmaceuticals. The system's efficiency was evaluated by analyzing various parameters, such as the time it takes for a response to be received (latency), the amount of energy used by the system (energy consumption), and the additional data added to a packet for control functions (packet overhead). The study's findings indicated that the proposed blockchain system demonstrated a significant decrease in transaction latency, indicating a viable and efficient solution. Furthermore, the use of a simpler consensus mechanism allowed for the validation of blocks to be performed efficiently on devices with limited computational capabilities and low power consumption. Specifically, the validation process took 30 ms and consumed 45 mJ of energy
[88]	The primary contribution of this research. is the introduction of a new multiagent system architecture that utilizes a private, distributed blockchain. This design offers a lightweight solution and security for Internet of Things (IoTs) systems
[80]	The design of IoT and Blockchain is described in this proposal, as well as its problems and possible uses. The two case studies are thoroughly reviewed, and solutions are offered and worked on to implement them. The solutions to the challenges have been proven to be safe in a variety of scenarios
[81]	The study presented a blockchain-enabled Internet of Medical Things (IoMTs) system to address confidentiality problems. The research also examined the potential benefits that the blockchain-enabled IoMT could bring to address challenges related to COVID-19 from five different perspectives
[82]	A telemedical laboratory service is being introduced in which clinical tests are conducted on patients by technicians directly at the hospital using Internet of Things (IoTs) medical equipment, and the results are instantly communicated to doctors from distributed hospitals for validation and/or review through the hospital Cloud
[83]	The study proposed a zero-knowledge blockchain architecture for Bahrain's IoT smart cities, which can be used to support a secure method for sharing health information in smart cities
[85]	The study explains how the application and assessment of a mobile crowdsourcing system for diabetes research and care uses a Continuous Glucose Monitoring (CGM) device connected to the Internet of Things (IoTs). The system is designed to gather blood glucose data quickly, easily, and affordably from a large population, providing a transparent and reliable source of data for diabetes research and care
[86]	A secure and private smart healthcare architecture that utilizes Federated Learning and blockchain technology to protect patient data on IoT cloud platforms. This system allows for scalable machine learning applications in healthcare using Federated Learning

response times can be handled. In contrast, most IoT devices use minimal bandwidth. As the number of connected devices grows and blockchain technology demands, significant bandwidth usage may be required. Various suggestions have been put forth to tackle these obstacles, such as utilizing permissioned blockchains for IoT devices [92, 93]. Another option is to employ Blockchain networks that are based on a low-energy consensus method like PoET PBET. Another alternative algorithm is outlined in [94]. IOTA is a solution that is designed for use in IoT systems. It is built on the directed acyclic graph (DAG) called "tangle" [95].

7.2 Security

The IoT system is made up of billions of diverse IoT devices that are often manufactured with minimal focus on security measures. IoT devices with weak security measures are vulnerable to various security risks. Combining IoT with blockchain technology can enhance Confidentiality, Integrity, and Privacy by utilizing blockchain's encryption, immutability, tamper-proofing, and digital signature capabilities. However, security is still a significant concern in deploying a high-performing IoT system that incorporates blockchain. Furthermore, the IoT system cannot use advanced, complicated encryption techniques

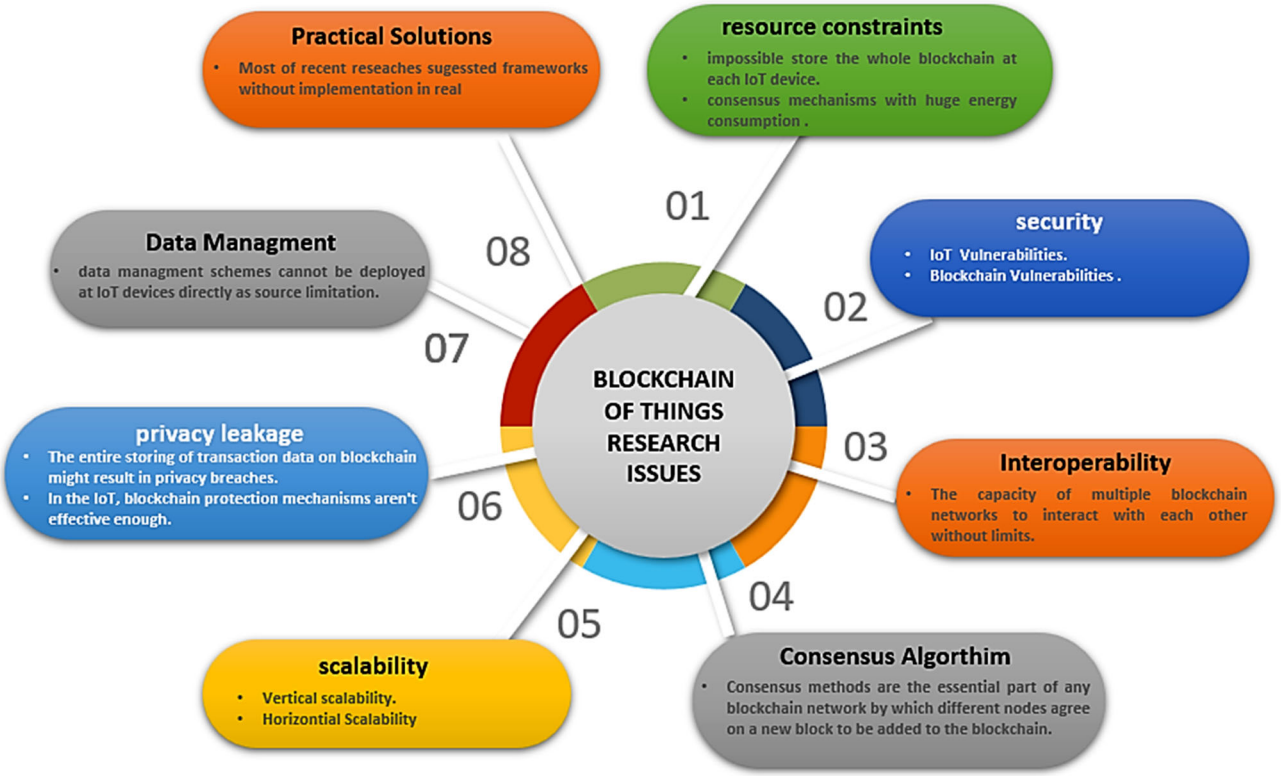


Fig. 12 Research issues in blockchain of things

Table 11 Research issues and suggested algorithm

Research issues	Suggested algorithm
Limited resources	• Fog/edge computing [91]
	• IOTA [95]
Security	• SABRE [98]
	• Corda and Stellar [99]
Privacy	• Private Blockchain [75, 102, 103]
	• Homomorphic encryption and proxy re-encryption [106–108]
Scalability	• Scalable consensus algorithms [58]
	• Off-chain, on-chain [109, 110]
Interoperability	• GS1-based data standards [111–113]
Data Management	• Off-chain solutions [116]
Consensus Algorithm	• Proof of elapsed time and Stellar consensus [59]
	• Tangle [94]

due to resource limitations. Meanwhile Reference [96], Blockchain technology has some vulnerabilities in security measures, such as attacks on smart contract software and attacks on decentralized autonomous organizations (DAOs).

7.2.1 Suggested solutions

Addressed by either improving the security of IoT systems or closing loopholes in the blockchain. For instance, a cooperative jamming strategy [97] several methods were studied to enhance security issues with the Internet of Things without requiring additional hardware for current Internet of Things nodes. In particular, Reference [98] SABRE (Secure and Authenticated Blockchain Routing Engine) has recently been proposed as a protected relaying system for blockchains that can safeguard blockchains from BGP routing vulnerabilities. To protect against DAO vulnerabilities, platforms such as Corda and Stellar have traded the flexibility of smart contracts for their

verifiability [99]. An issue of security in the healthcare sector is implementing blockchain technology in tracking patients, specifically with permission and consortium blockchain systems [100]. In [101] a solution based on a public blockchain that addresses issues of SPOF (single point of failure), MitM attacks, DoS, and data sniffing vulnerabilities for Remote Hardware Management.

7.3 Privacy

Because the healthcare industry requires a high level of privacy, using public Blockchains to store and distribute sensitive data is inappropriate. Every transaction on a public Blockchain is visible to everybody. Having an anonymous identity does not guarantee the safety of sensitive information.

7.3.1 Suggested solution

Private and permissioned Blockchains, in general, are not affected by the privacy issue. As a result, the private Blockchain is the best option for a healthcare application [75, 102, 103]. Gathering personal data, including health details, location, and images, can compromise an individual's privacy. To safeguard against privacy breaches, privacy-preserving scientific computations (PPSC) can be used [104] should be used. Another strategy for developing IoT application trust has been developed [105]. To protect user privacy on a blockchain network, research in both blockchain and IoT has looked into Methods like homomorphic encryption and proxy re-encryption. These methods depend on the Chinese remainder theorem (CRT) and have been studied by researchers like [106–108]. Federated learning-based Blockchain provides private data processing. Federated learning enables participants of the Blockchain to learn an ML algorithm without exchanging their information. The Blockchain can then secure the trained algorithm via a smart contract, ensuring its integrity and confidentiality.

7.4 Scalability

Scalability is a complex issue encompassing various factors, such as max delivery ratio, delay, start-up time, and cost per verified transaction. It also refers to a consensus mechanism's ability to be more scalable by supporting many nodes. The primary focus is often on throughput and latency. Throughput measures the number of successful TPS, while latency refers to the period needed to validate and execute a transaction. These properties are decided by the consensus algorithm employed in the Blockchain network.

7.4.1 Suggested Solution

References [109, 110] a review proposed categorizing available scaling solutions into three tiers: Layer-0 for solutions that improve data transmission standards, Layer-1 for on-chain solutions such as connections, consensus, and data structure, and Layer-2 for off-chain solutions such as off-chain channels, cross-chain protocols, and side-chain approaches. Additionally, the survey also suggested the use of private or consortium blockchains for IoT and the creation of more scalable consensus algorithms [58].

7.5 Interoperability

Refers to the capability of various Blockchains to interact seamlessly with one another. This is a main challenge in the field of healthcare, as many Blockchain-based systems in eHealth use a wide range of Blockchain networks and platforms.

7.5.1 Suggested solutions

The growing adoption of Blockchain technology across multiple industries has highlighted the need for a solution allowing different Blockchains to interact and communicate. Blockchain interoperability is a key solution to this problem, and various methods, such as cross-blockchain frameworks, smart contract interaction, and token transfers, have been proposed to achieve this. Additionally, existing standards, such as the GS1-based data standards, are also being used by companies like IBM and Microsoft to facilitate interoperability between different blockchain networks [111–113].

7.6 Data management

One primary difficulty when utilizing blockchain technology is its limited storage capacity. Unlike the Internet of Things, known for producing large amounts of data, blockchain was not designed to handle and store significant volumes of information. This limitation in storage capacity can pose significant challenges to developing blockchain in IoT applications. The whole Bitcoin blockchain is roughly 150 terabytes in size, as is the complete Ethereum blockchain. The blockchain is around 400 terabytes in size. It's necessary to save all the blockchain blocks. In the absence of IoT, devices, like all prior blocks, cannot authenticate transactions generated by other devices. Besides, to create new transactions, past data is necessary [114]. Due to its restricted storage space, the large amount of information produced by IoT sensors, measured in zettabytes, makes it impossible to store on the blockchain. In blockchain networks, it is required that multiple, or even all, nodes have a

copy of the data, which put a strain on the constrained resources of IoT devices. This presents a significant obstacle for the combined blockchain and the Internet of Things, as the devices cannot handle and store such massive volumes of information.

7.6.1 Suggested Solutions

Reference [115, 116] to handle the issue of limited storage capacity in blockchain, many researchers have proposed the use of off-chain solutions to handle the vast amount of information sent by IoT. One approach is to combine blockchain storage with traditional cloud storage. Another option is to send IoT data among different sources, such as cloud services, which can provide various storage options, including repositories, local computers, and utilizing a blockchain that is on-chain based on the characteristics of the data and the specific scenario. This method enables the efficient and effective storage of large amounts of information generated by IoT sensors while minimizing the usage of the constrained resources of IoT sensors.

7.7 Consensus algorithm

Consensus is used in blockchain to develop a way for all blockchain nodes to agree. Because of the resource constraints in IoT, selecting a consensus algorithm is critical to resolving resource constraints and security issues in IoT and blockchain.

7.7.1 Suggested solution

Reference [59] suggested Proof of elapsed time and Stellar consensus protocols (SCP) as a good solution for IoT based on healthcare applications with high scalability and low computation overhead, and [94] Tangle is a lightweight, endlessly scalable framework that's ideal for IoT networks.

7.8 Practical solutions

When preparing this survey, we found that most works suggested frameworks without showing practical solutions, such as [3, 84, 88, 117–120].

7.8.1 Suggested solutions

Using blockchain to integrate with existing healthcare systems and IoT that require extensive adjustments to current systems (such as a significant duration, meticulous planning, financial support, and specialized human expertise) and additional expenses. In explaining research gaps, we introduce suggested solutions that guide the researchers in implementing and evaluating blockchain integrated with IoT based on healthcare.

8 Discussion

In this survey, the discussion explores and categorizes key challenges encountered in integrating blockchain technology with Internet of Things (IoTs) applications in healthcare. The first challenge, limited resources on IoT devices, necessitates innovative solutions such as leveraging Mobile Edge Computing (MEC) and cloud computing technologies to overcome computational and storage limitations. Addressing security concerns is paramount, given the diverse and often insecure nature of IoT devices, and proposed strategies include cooperative jamming and systems like SABRE to fortify blockchain against vulnerabilities. Privacy concerns, particularly pertinent in the healthcare sector, are addressed by recommending private and permissioned blockchains, complemented by privacy-preserving scientific computations and federated learning. Scalability, a complex issue affecting throughput and latency, can be mitigated using tiered scaling solutions and private or consortium blockchains. Interoperability challenges in healthcare arising from diverse blockchain networks find potential resolutions in cross-blockchain frameworks and standardization efforts. The limited storage capacity of blockchain versus the massive data generated by IoT devices underscores the need for off-chain solutions involving the combination of blockchain with traditional cloud storage or distributed data management. Selecting appropriate consensus algorithms, like Proof of Elapsed Time and Stellar Consensus Protocols, is crucial for overcoming resource constraints and ensuring scalability in healthcare focused IoT applications. Lastly, the gap between theoretical frameworks and practical implementation is highlighted, urging the research community to develop and evaluate tangible solutions for the seamless integration of blockchain and IoT in healthcare systems. Overall, addressing these challenges is imperative for unlocking the full potential of blockchain technology in revolutionizing healthcare through the Internet of Things.

9 Conclusion

This study examines the challenges and opportunities of combining IoT and blockchain technology in the rapidly expanding eHealth industry. The adoption of eHealth, which enables remote care using various technologies has improved the management of chronic illnesses and positively impacted various healthcare domains including EHRs, Remote patient monitoring, forecasting illnesses,

tracking medication, and controlling infectious diseases. However, using IoT devices also introduces new security and privacy concerns. The decentralized and dispersed characteristics of blockchain technology and the cryptography employed in its processes, are seen as a potential solution to these challenges. The study aims to provide a detailed overview of the current state of IoT-based healthcare systems utilizing blockchain technology Additionally, it seeks to outline the primary drivers for improving, developing, updating, and implementing new blockchain algorithms to facilitate the creation of a more efficient, safe, and successful eHealth system based on IoT. Furthermore, the study explores current research on IoT-based healthcare integration using blockchain, identifying areas for future research and highlighting challenges in the field.

Author contributions All authors contributed to the study's conception and design. Aya Hatem performed material preparation, data collection, and analysis, Aya Hatem wrote the first draft of the manuscript, and all authors commented on previous versions. All authors read and approved the final manuscript.

Funding Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB). No funding was received to assist with the preparation of this manuscript. The authors have no relevant financial or non-financial interests to disclose.

Data availability Datasets generated during and /or analyzed during the current study are available from the first author upon reasonable request.

Consent to publish Not applicable.

Declarations

Conflict of interest The Author declares that there is no conflict of interest.

Ethical approval Not applicable.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Policy Advice: Healthcare Statistics for 2021. Policy Advice. https://www.healthcareradius.in/features/management/28852-global-healthcare-spending-expected-to-reach-over-10-trillion-by-2024-on-account-of-covid-19. Accessed 6 Jan 2024
2. Omnia Health Insights: The Importance of Accessible and Sustainable Healthcare. Omnia Health Insights. https://insights.omnia-health.com/management/importance-accessible-and-sustainable-healthcare. Accessed 6 Jan 2024
3. Azbeg, K., Ouchetto, O., Andaloussi, S.J., Fetjah, L.: A taxonomic review of the use of IoT and blockchain in healthcare applications. IRBM **43**(5), 511–519 (2022). https://doi.org/10.1016/J.IRBM.2021.05.003
4. Vahdati, M., Gholizadeh HamlAbadi, K., Saghiri, A.M.: IoT-based healthcare monitoring using blockchain. Stud. Big Data **83**, 141–170 (2021). https://doi.org/10.1007/978-981-15-9547-9_6
5. Ajerla, D., Mahfuz, S., Zulkernine, F.: A real-time patient monitoring framework for fall detection. Wirel. Commun. Mob. Comput. (2019). https://doi.org/10.1155/2019/9507938
6. Gupta, S., Malhotra, V., Singh, S.N.: Securing IoT-driven remote healthcare data through blockchain. Lect. Notes Netw. Syst. **94**, 47–56 (2020). https://doi.org/10.1007/978-981-15-0694-9_6
7. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., Sikdar, B.: A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access **7**, 82721–82743 (2019). https://doi.org/10.1109/ACCESS.2019.2924045
8. Atlam, H.F., Azad, M.A., Alzahrani, A.G., Wills, G.: A review of blockchain in Internet of Things and AI. Big Data Cogn. Comput. **4**(4), 28 (2020). https://doi.org/10.3390/BDCC4040028
9. Chukwu, E., Garg, L.: A systematic review of blockchain in healthcare: frameworks, prototypes, and implementations. IEEE Access **8**, 21196–21214 (2020). https://doi.org/10.1109/ACCESS.2020.2969881
10. Ali, M.S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., Rehmani, M.H.: Applications of blockchains in the Internet of Things: a comprehensive survey. IEEE Commun. Surv. Tutor. **21**(2), 1676–1717 (2019). https://doi.org/10.1109/COMST.2018.2886932
11. Tandon, A., Dhir, A., Islam, N., Mäntymäki, M.: Blockchain in healthcare: a systematic literature review, synthesizing framework and future research agenda. Comput. Ind. **122**, 103290 (2020). https://doi.org/10.1016/J.COMPIND.2020.103290
12. Abdelmaboud, A., et al.: Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges and future research directions. Electronics **11**(4), 630 (2022). https://doi.org/10.3390/ELECTRONICS11040630
13. Rosén, M., Haglund, B.: Chapter 10. The importance of health and medical care for public health. Scand. J. Public Health **Suppl 58**, 219–230 (2001). https://doi.org/10.1177/14034948010290032701
14. Glasser, M., Karen, P.: E-health | health care |. In: E-health. Britannica (2013). https://www.britannica.com/science/e-health. Accessed 6 Jan 2024
15. Statista: COVID-19 Telemedicine Appointments U.S. COVID-19 Impact 2020. Statista. https://www.statista.com/statistics/1133920/telemedicine-and-covid-19-impact-us/. Accessed 6 Jan 2024
16. Heart, T., Ben-Assuli, O., Shabtai, I.: A review of PHR, EMR and EHR integration: a more personalized healthcare and public health policy. Health Policy Technol. **6**(1), 20–25 (2017). https://doi.org/10.1016/J.HLPT.2016.08.002

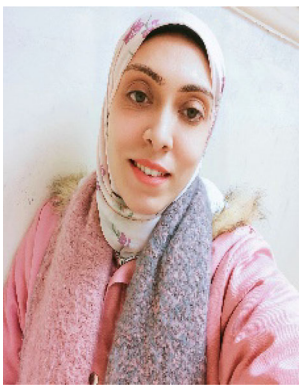
17. Akkaş, M.A., Sokullu, R., Ertürk Çetin, H.: Healthcare and patient monitoring using IoT. Internet Things **11**, 100173 (2020). https://doi.org/10.1016/J.IOT.2020.100173
18. Statista: IoT Devices Installed Base Worldwide 2015–2025. Statista. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. Accessed 6 Jan 2024
19. Nguyen, D.C., Pathirana, P.N., Ding, M.: A Seneviratne, Integration of blockchain and cloud of things: architecture, applications and challenges. IEEE Commun. Surv. Tutor. **22**(4), 2521–2548 (2020)
20. Ellouze, F., Fersi, G., Jmaiel, M.: Blockchain for Internet of Medical Things: a technical review. In: Lecture Notes in Computer Science (including Subseries Lecture Notes Artificial Intelligence, Lecture Notes in Bioinformatics), 2020, vol. 12157, pp. 259–267 (2020). https://doi.org/10.1007/978-3-030-51517-1_22/TABLES/1
21. Panda, S.S., Satapathy, U., Mohanta, B.K., Jena, D., Gountia, D.: A blockchain based decentralized authentication framework for resource constrained IOT devices. In: 2019 10th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2019, July 2019 (2019). https://doi.org/10.1109/ICCCNT45670.2019.8944637
22. Fernández-Caramés, T.M., Fraga-Lamas, P.: A review on the use of blockchain for the Internet of Things. IEEE Access **6**, 32979–33001 (2018). https://doi.org/10.1109/ACCESS.2018.2842685
23. Frustaci, M., Pace, P., Aloi, G., Fortino, G.: Evaluating critical security issues of the IoT world: present and future challenges. IEEE Internet Things J. **5**(4), 2483–2495 (2018). https://doi.org/10.1109/JIOT.2017.2767291
24. Statista: IoT in Healthcare Market Size Worldwide 2016–2025 Forecast. Statista. https://www.statista.com/statistics/997959/worldwide-internet-of-things-in-healthcare-market-size/. Accessed 10 Jan 1BC
25. Aktaş, F., Çeken, C., Erdemli, Y.E.: Transmission of physiological signals with quality of service support by using wireless body area networks. In: 2015 Medical Technologies National Conference TIPTEKNO 2015, January 2016 (2016). https://doi.org/10.1109/TIPTEKNO.2015.7374581
26. Xu, T., Wendt, J.B., Potkonjak, M.: Security of IoT systems: design challenges and opportunities. In: 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, 2014 (2014)
27. Song, Z., Cárdenas, A.A., Masuoka, R.: Semantic middleware for the Internet of Things. In: 2010 Internet of Things, IoT 2010, 2010 (2010). https://doi.org/10.1109/IOT.2010.5678448
28. Ghosh, A.M., Halder, D., Hossain, S.K.A.: Remote health monitoring system through IoT. In: 2016 5th International Conference on Informatics, Electronics and Vision, November 2016, pp. 921–926 (2016). https://doi.org/10.1109/ICIEV.2016.7760135
29. Moghadas, E., Rezazadeh, J., Farahbakhsh, R.: An IoT patient monitoring based on fog computing and data mining: cardiac arrhythmia use case. Internet Things (Neth.) (2020). https://doi.org/10.1016/J.IOT.2020.100251
30. Yew, H.T., Ng, M.F., Ping, S.Z., Chung, S.K., Chekima, A., Dargham, J.A.: IoT based real-time remote patient monitoring system. In: 2020 16th IEEE International Colloquium on Signal Processing and Its Applications, February 2020, pp. 176–179 (2020). https://doi.org/10.1109/CSPA48992.2020.9068699
31. Kumar, P.M., Lokesh, S., Varatharajan, R., Chandra Babu, G., Parthasarathy, P.: Cloud and IoT based disease prediction and diagnosis system for healthcare using Fuzzy neural classifier. Future Gener. Comput. Syst. **86**, 527–534 (2018). https://doi.org/10.1016/J.FUTURE.2018.04.036
32. Al-Makhadmeh, Z., Tolba, A.: Utilizing IoT wearable medical device for heart disease prediction using higher order Boltzmann model: a classification approach. Measurement **147**, 106815 (2019). https://doi.org/10.1016/J.MEASUREMENT.2019.07.043
33. Arulanthu, P., Perumal, E.: An intelligent IoT with cloud centric medical decision support system for chronic kidney disease prediction. Int. J. Imaging Syst. Technol. **30**(3), 815–827 (2020). https://doi.org/10.1002/IMA.22424
34. Helmy, J., Helmy, A.: The Alzimio App for dementia, autism and Alzheimer's: using novel activity recognition algorithms and geofencing. In: 2016 IEEE International Conference on Smart Computing, June 2016 (2016). https://doi.org/10.1109/SMARTCOMP.2016.7501720
35. Patil, N., Iyer, B.: Health monitoring and tracking system for soldiers using Internet of Things (IoT). In: 2017 International Conference on Computing, Communication and Automation, January 2017, pp. 1347–1352 (2017). https://doi.org/10.1109/CCAA.2017.8230007
36. Otoom, M., Otoum, N., Alzubaidi, M.A., Etoom, Y., Banihani, R.: An IoT-based framework for early identification and monitoring of COVID-19 cases. Biomed. Signal Process. Control **62**, 102149 (2020). https://doi.org/10.1016/J.BSPC.2020.102149
37. Kumar, K., Kumar, N., Shah, R.: Role of IoT to avoid spreading of COVID-19. Int. J. Intell. Netw. **1**, 32 (2020). https://doi.org/10.1016/J.IJIN.2020.05.002
38. Baskaran, K., Baskaran, P., Rajaram, V., Kumaratharan, N.: IoT based COVID preventive system for work environment. In: Proceedings of the 4th International Conference of IoT in Social, Mobile, Analytics and Cloud, ISMAC 2020, October 2020, pp. 65–71 (2020). https://doi.org/10.1109/I-SMAC49090.2020.9243471
39. Elagan, S.K., Abdelwahab, S.F., Zanaty, E.A., Alkinani, M.H., Alotaibi, H., Zanaty, M.E.A.: Remote diagnostic and detection of coronavirus disease (COVID-19) system based on intelligent healthcare and Internet of Things. Results Phys. (2021). https://doi.org/10.1016/J.RINP.2021.103910
40. Rahman, A., et al.: SDN–IoT empowered intelligent framework for Industry 4.0 applications during COVID-19 pandemic. Clust. Comput. **25**(4), 2351–2368 (2022). https://doi.org/10.1007/S10586-021-03367-4/TABLES/5
41. Makina, H., Ben Letaifa, A., Rachedi, A.: Survey on security and privacy in Internet of Things-based eHealth applications: challenges, architectures, and future directions. Secur. Priv. (2023). https://doi.org/10.1002/SPY2.346
42. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. Decentralized Business Review (2008). http://www.bitcoin.org/
43. Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H.: Blockchain challenges and opportunities: A survey. Int. J. Web Grid Serv. **14**(4), 352–375 (2018). https://doi.org/10.1504/IJWGS.2018.095647
44. Wu, H., Li, Z., King, B., Ben Miled, Z., Wassick, J., Tazelaar, J.: A distributed ledger for supply chain physical distribution visibility. Information **8**(4), 137 (2017). https://doi.org/10.3390/INFO8040137
45. Atlam, H.F., Azad, M.A., Alassafi, M.O., Alshdadi, A.A., Alenezi, A.: Risk-based access control model: a systematic literature review. Future Internet **12**(6), 103 (2020). https://doi.org/10.3390/FI12060103
46. Heilman, E., Baldimtsi, F., Goldberg, S.: Blindly signed contracts: anonymous on-blockchain and off-blockchain bitcoin transactions. In: Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence, Lecture Notes in Bioinformatics), LNCS, 2016, vol. 9604, pp. 43–60 (2016). https://doi.org/10.1007/978-3-662-53357-4_4

47. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things. IEEE Access **4**, 2292–2303 (2016). https://doi.org/10.1109/ACCESS.2016.2566339
48. Turek, J., Shasha, D.: The many faces of consensus in distributed systems. Computer (Long Beach Calif.) **25**(6), 8–17 (1992). https://doi.org/10.1109/2.153253
49. Fischer, M.J., Lynch, N.A., Paterson, M.S.: Impossibility of distributed consensus with one faulty process. J. ACM **32**(2), 374–382 (1985). https://doi.org/10.1145/3149.214121
50. Dolev, D., Dworkt, C., Stockmeyer, L.: On the minimal synchronism needed for distributed consensus. J. ACM **34**(1), 77–97 (1983)
51. Malkhi, D., Reiter, M.: Byzantine quorum systems. Distrib. Comput. **11**, 203–213 (1998)
52. Holotescu, V., Vasiu, R.: Challenges and emerging solutions for public blockchains. BRAIN Broad Res. Artif. Intell. Neurosci. **11**(1), 58–83 (2020). https://doi.org/10.18662/BRAIN/11.1/15
53. Taskinsoy, J.: Bitcoin could be the first cryptocurrency to reach a market capitalization of one trillion dollars. SSRN Electron. J. (2020). https://doi.org/10.2139/SSRN.3693765
54. Salimitari, M., Chatterjee, M.: A Survey on Consensus Protocols in Blockchain for IoT Networks (2018). https://doi.org/10.48550/arxiv.1809.05613
55. Chaudhry, N., Yousaf, M.M.: Consensus algorithms in blockchain: comparative analysis, challenges and opportunities. In: ICOSST 2018—2018 International Conference on Open Source Systems and Technologies, Proceedings, July 2018, pp. 54–63 (2018). https://doi.org/10.1109/ICOSST.2018.8632190
56. Almalki, J.: State-of-the-art research in blockchain of things for healthcare. Arab. J. Sci. Eng. **1–29**, 2023 (2023). https://doi.org/10.1007/S13369-023-07896-5
57. Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M.: On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst. **88**, 173–190 (2018). https://doi.org/10.1016/J.FUTURE.2018.05.046
58. Dai, H.N., Zheng, Z., Zhang, Y.: Blockchain for Internet of Things: a survey. IEEE Internet Things J. **6**(5), 8076–8094 (2019). https://doi.org/10.1109/JIOT.2019.2920987
59. Ray, P.P., Dash, D., Salah, K., Kumar, N.: Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases. IEEE Syst. J. **15**(1), 85–94 (2021). https://doi.org/10.1109/JSYST.2020.2963840
60. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: IoT security: review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. **82**(4), 395–411 (2018). https://doi.org/10.1109/COMST.2015.2444095
61. Sengupta, J., Ruj, S., Das Bit, S.: A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J. Netw. Comput. Appl. **149**, 102481 (2019). https://doi.org/10.1016/J.JNCA.2019.102481
62. Banerjee, M., Lee, J., Choo, K.K.R.: A blockchain future for Internet of Things security: a position paper. Digit. Commun. Netw. **4**(3), 149–160 (2018). https://doi.org/10.1016/J.DCAN.2017.10.006
63. (PDF) Blockchain in Internet of Things: Challenges and Solutions. https://www.researchgate.net/publication/306281414_Blockchain_in_Internet_of_Things_Challenges_and_Solutions. Accessed 6 Jan 2024
64. Polyzos, G.C., Fotiou, N.: Blockchain-assisted information distribution for the Internet of Things. In: Proceedings—2017 IEEE International Conference on Information Reuse and Integration, IRI 2017, January 2017, pp. 75–78 (2017). https://doi.org/10.1109/IRI.2017.83
65. Karthikeyyan, P., Velliangiri, S., Joseph, I.T.: Review of Blockchain based IoT application and its security issues. In: 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies, ICICICT 2019, July 2019, pp. 6–11 (2019). https://doi.org/10.1109/ICICICT46008.2019.8993124
66. Fotiou, N., Siris, V.A., Polyzos, G.C.: Interacting with the Internet of Things using smart contracts and blockchain technologies. In: Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence, Lecture Notes in Bioinformatics), LNCS, 2019 vol. 11342, pp. 443–452 (2019). https://doi.org/10.48550/arxiv.1901.07807
67. Rahman, A., et al.: SmartBlock-SDN: an optimized blockchain-SDN framework for resource management in IoT. IEEE Access **9**, 28361–28376 (2021). https://doi.org/10.1109/ACCESS.2021.3058244
68. Islam, M.J., et al.: Blockchain-SDN-based energy-aware and distributed secure architecture for IoT in smart cities. IEEE Internet Things J. **9**(5), 3850–3864 (2022). https://doi.org/10.1109/JIOT.2021.3100797
69. Tandon, A.: An empirical analysis of using blockchain technology with Internet of Things and its application. Int. J. Innov. Technol. Explor. Eng. **8**(9 Special Issue 3), 1470–1475 (2019). https://doi.org/10.35940/IJITEE.I3310.0789S319
70. Zhu, X., Badr, Y.: Identity management systems for the Internet of Things: a survey towards blockchain solutions. Sensors **18**(12), 4215 (2018). https://doi.org/10.3390/S18124215
71. Hang, L., Kim, D.H.: Design and implementation of an integrated IoT blockchain platform for sensing data integrity. Sensors **19**(10), 2228 (2019). https://doi.org/10.3390/S19102228
72. Kadam S.B., John, S.K.: Blockchain integration with low-power Internet of Things devices. In: Handbook of Research on Blockchain Technology, pp. 183–211 (2020). https://doi.org/10.1016/B978-0-12-819816-2.00008-3
73. Dukkipati, C., Zhang, Y., Cheng, L.C.: Decentralized, blockchain based access control framework for the heterogeneous Internet of Things. In: ABAC 2018—Proceedings of the 3rd ACM Workshop on Attribute-Based Access Control. Co-located with CODASPY 2018, January 2018, pp. 61–69 (2018). https://doi.org/10.1145/3180457.3180458
74. Dorri, A., Kanhere, S.S., Jurdak, R.: Blockchain in Internet of Things: Challenges and Solutions (2016)
75. Novo, O.: Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J. **5**(2), 1184–1195 (2018). https://doi.org/10.1109/JIOT.2018.2812239
76. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., Wan, J.: Smart contract-based access control for the Internet of Things. IEEE Internet Things J. **6**(2), 1594–1605 (2019). https://doi.org/10.1109/JIOT.2018.2847705
77. Badr, S., Gomaa, I., Abd-Elrahman, E.: Multi-tier blockchain framework for IoT-EHRs systems. Procedia Comput. Sci. **141**, 159–166 (2018). https://doi.org/10.1016/J.PROCS.2018.10.162
78. Mishra, S., Tyagi, A.K.: Intrusion detection in Internet of Things (IoTs) based applications using blockchain technology. In: Proceedings of the 3rd International Conference (I-SMAC) on IoT Social, Mobile, Analytics and Cloud, I-SMAC 2019, 2019, pp. 123–128 (2019). https://doi.org/10.1109/I-SMAC47947.2019.9032557
79. Tomar, A., Gupta, N., Rani, D., Tripathi, S.: Blockchain-assisted authenticated key agreement scheme for IoT-based healthcare system. Internet Things **23**, 100849 (2023). https://doi.org/10.1016/J.IOT.2023.100849
80. Garg, V., Sukhija, K., Verma, S.: IOT based blockchain solution: COVID-19 and defense. India Int. J. Technol. Res. Sci. (Special Issue) (2020). https://doi.org/10.30780/specialissue-ICACCG2020/006
81. Dai, H.-N., Imran, M., Haider, N.: Blockchain-enabled Internet of Medical Things to combat COVID-19. IEEE Internet Things

Mag. **3**(3), 52–57 (2020). https://doi.org/10.1109/IOTM.0001.2000087
82. Celesti, A., Ruggeri, A., Fazio, M., Galletta, A., Villari, M., Romano, A.: Blockchain-based healthcare workflow for tele-medical laboratory in federated hospital IoT clouds. Sensors (Basel) (2020). https://doi.org/10.3390/S20092590
83. Al-Aswad, H., El-Medany, W.M., Balakrishna, C., Ababneh, N., Curran, K.: BZKP: blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation. Arab. J. Basic Appl. Sci. **28**(1), 154–171 (2021). https://doi.org/10.1080/25765299.2020.1870812
84. Singh, A., Prabha, P., Chatterjee, K.: Security of IoT-Based E-Healthcare System: A Blockchain Solution, pp. 227–237 (2022). https://doi.org/10.1007/978-981-16-1220-6_20
85. Fernández-Caramés, T.M., Froiz-Míguez, I., Blanco-Novoa, O., Fraga-Lamas, P.: Enabling the Internet of Mobile Crowdsourcing Health Things: a mobile fog computing, blockchain and IoT based continuous glucose monitoring system for diabetes mellitus research and care. Sensors **19**(15), 3319 (2019). https://doi.org/10.3390/S19153319
86. Singh, S., Rathore, S., Alfarraj, O., Tolba, A., Yoon, B.: A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. Future Gener. Comput. Syst. **129**, 380–388 (2022). https://doi.org/10.1016/J.FUTURE.2021.11.028
87. Maitra, S., Yanambaka, V.P., Puthal, D., Abdelgawad, A., Yelamarthi, K.: Integration of Internet of Things and blockchain toward portability and low-energy consumption. Trans. Emerg. Telecommun. Technol. **32**(6), e4103 (2021). https://doi.org/10.1002/ETT.4103
88. Sun, S., Du, R., Chen, S., Li, W.: Blockchain-based IoT access control system: towards security, lightweight, and cross-domain. IEEE Access **9**, 36868–36878 (2021). https://doi.org/10.1109/ACCESS.2021.3059863
89. Ali, A., et al.: An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. Sensors **22**(2), 572 (2022). https://doi.org/10.3390/S22020572
90. Rathee, G., Sharma, A., Saini, H., Kumar, R., Iqbal, R.: A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. Multimed. Tools Appl. **79**(15–16), 9711–9733 (2020). https://doi.org/10.1007/S11042-019-07835-3/FIGURES/13
91. Dai, Y., Xu, D., Maharjan, S., Zhang, Y.: Joint computation offloading and user association in multi-task mobile edge computing. IEEE Trans. Veh. Technol. **67**(12), 12313–12325 (2018). https://doi.org/10.1109/TVT.2018.2876804
92. Qiu, C., Yao, H., Yu, F.R., Jiang, C., Guo, S.: A service-oriented permissioned blockchain for the Internet of Things. IEEE Trans. Serv. Comput. **13**(2), 203–215 (2020). https://doi.org/10.1109/TSC.2019.2948870
93. Faizullah, S., Khan, M.A., Alzahrani, A., Khan, I.: Permissioned blockchain-based security for SDN in IoT cloud networks. In: 2019 International Conference on Advances in Emerging Computing Technologies, AECT 2019, February 2020 (2020). https://doi.org/10.1109/AECT47998.2020.9194181
94. Salimitari, M., Chatterjee, M., Fallah, Y.P.: A survey on consensus methods in blockchain for resource-constrained IoT networks. Internet Things **11**, 100212 (2020). https://doi.org/10.1016/J.IOT.2020.100212
95. Popov, S.: The Tangle (2018)
96. Wang, X., et al.: Survey on blockchain for Internet of Things. Comput. Commun. **136**, 10–29 (2019). https://doi.org/10.1016/J.COMCOM.2019.01.006
97. Hu, L., et al.: Cooperative jamming for physical layer security enhancement in Internet of Things. IEEE Internet Things J. **5**(1), 219–228 (2018). https://doi.org/10.1109/JIOT.2017.2778185
98. Apostolaki, M., Zurich, E., Marti, G., Müller, J., Vanbever, L.: SABRE: Protecting Bitcoin against Routing Attacks. https://doi.org/10.14722/ndss.2019.23252
99. Tuan, T., et al.: Untangling Blockchain: A Data Processing View of Blockchain Systems (2017). https://doi.org/10.1109/TKDE.2017.2781227
100. Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T.: Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J. Med. Syst. (2018). https://doi.org/10.1007/S10916-018-0982-X
101. Ali, M.S., Vecchio, M., Putra, G.D., Kanhere, S.S., Antonelli, F.: A decentralized peer-to-peer remote health monitoring system. Sensors **20**(6), 1656 (2020). https://doi.org/10.3390/S20061656
102. Lv, P., Wang, L., Zhu, H., Deng, W., Gu, L.: An IoT-oriented privacy-preserving publish/subscribe model over blockchains. IEEE Access **7**, 41309–41314 (2019). https://doi.org/10.1109/ACCESS.2019.2907599
103. Javaid, U., Aman, M.N., Sikdar, B.: BlockPro: blockchain based data provenance and integrity for secure IoT environments. In: BlockSys 2018—Proceedings of the 1st Workshop on Blockchain-Enabled Networked Sensor Systems, Part SenSys 2018, November 2018, pp. 13–18 (2018). https://doi.org/10.1145/3282278.3282281
104. Yan, Z., Zhang, P., Vasilakos, A.V.: A survey on trust management for Internet of Things. J. Netw. Comput. Appl. **42**, 120–134 (2014). https://doi.org/10.1016/J.JNCA.2014.01.014
105. Li, C., Wang, G.: A light-weight commodity integrity detection algorithm based on Chinese remainder theorem. In: Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2012—11th IEEE International Conference on Ubiquitous Computing and Communications, IUCC-2012,2012, pp. 1018–1023 (2012). https://doi.org/10.1109/TRUSTCOM.2012.37
106. Shrestha, R., Kim, S.: Integration of IoT with blockchain and homomorphic encryption: challenging issues and opportunities. Adv. Comput. **115**, 293–331 (2019). https://doi.org/10.1016/BS.ADCOM.2019.06.002
107. Gao, Y., Chen, Y., Lin, H., Rodrigues, J.J.P.C.: Blockchain based secure IoT data sharing framework for SDN-enabled smart communities. In: IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2020, July 2020, pp. 514–519 (2020). https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162725
108. Khan, L.U., Saad, W., Han, Z., Hossain, E., Hong, C.S.: Federated learning for Internet of Things: recent advances, taxonomy, and open challenges. IEEE Commun. Surv. Tutor. **23**(3), 1759–1799 (2020). https://doi.org/10.48550/arxiv.2009.13012
109. Zhou, Q., Huang, H., Zheng, Z., Bian, J.: Solutions to scalability of blockchain: a survey. IEEE Access **8**, 16440–16455 (2020). https://doi.org/10.1109/ACCESS.2020.2967218
110. Nasir, M.H., Arshad, J., Khan, M.M., Fatima, M., Salah, K., Jayaraman, R.: Scalable blockchains—a systematic review. Future Gener. Comput. Syst. **126**, 136–162 (2022). https://doi.org/10.1016/J.FUTURE.2021.07.035
111. Jin, H., Dai, X., Xiao, J.: Towards a novel architecture for enabling interoperability amongst multiple blockchains. In: Proceedings—International Conference on Distributed Computer Systems, July 2018, pp. 1203–1211 (2018). https://doi.org/10.1109/ICDCS.2018.00120

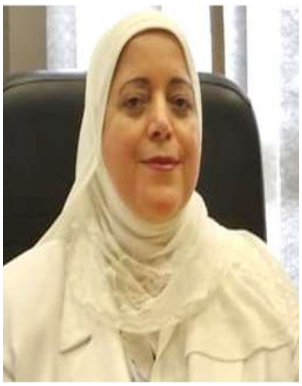
112. Schulte, S., Sigwart, M., Frauenthaler, P., Borkowski, M.: Towards blockchain interoperability. Lect. Notes Bus. Inf. Process. **361**, 3–10 (2019). https://doi.org/10.1007/978-3-030-30429-4_1
113. Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y.: Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput. Appl. **34**(14), 11475–11490 (2022). https://doi.org/10.1007/S00521-020-05519-W/METRICS
114. Alenezi, A., Zulkipli, N.H.N., Atlam, H.F., Walters, R.J., Wills, G.B.: The impact of cloud forensic readiness on security. In: CLOSER 2017—Proceedings of the 7th International Conference on Cloud Computing and Services Science, 2017, pp. 511–517 (2017). https://doi.org/10.5220/0006332705390545
115. Uddin, M.A., Stranieri, A., Gondal, I., Balasubramanian, V.: Rapid health data repository allocation using predictive machine learning. Health Inform. J. **26**(4), 3009–3036 (2020). https://doi.org/10.1177/1460458220957486
116. Ashraf Uddin, M., Stranieri, A., Gondal, I., Balasubramanian, V.: Dynamically recommending repositories for health data: a machine learning model. In: ACM International Conference Proceeding Series, February 2020 (2020). https://doi.org/10.1145/3373017.3373041
117. Banotra, A., Sharma, J.S., Gupta, S., Gupta, S.K., Rashid, M.: Use of Blockchain and Internet of Things for Securing Data in Healthcare Systems, pp. 255–267 (2021). https://doi.org/10.1007/978-981-15-8711-5_13
118. Kazmi, H.S.Z., Nazeer, F., Mubarak, S., Hameed, S., Basharat, A., Javaid, N.: Trusted remote patient monitoring using blockchain-based smart contracts. Lect. Notes Netw. Syst. **97**, 765–776 (2019). https://doi.org/10.1007/978-3-030-33506-9_70
119. Ahmadi, V., Benjelloun, S., El Kik, M., Sharma, T., Chi, H., Zhou, W.: Drug governance: IoT-based blockchain implementation in the pharmaceutical supply chain. In: 2020 6th International Conference on Mobile and Secure Services, MOBISECSERV 2020, February 2020 (2020). https://doi.org/10.1109/MOBISECSERV48690.2020.9042950
120. Lemieux, V.L., et al.: Having our 'Omic' cake and eating it too? Evaluating user response to using blockchain technology for private and secure health data management and sharing. Front. Blockchain **3**, 59 (2021). https://doi.org/10.3389/FBLOC.2020.558705

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Aya H. Allam Received B.Sc. in computer science from Faculty of Computers and Artificial intelligence, Benha University, Egypt in 2013 and received the M.Sc. degree in 2020. She is currently working as teaching assistant at computer science department, Faculty of Computers and Artificial intelligence, Benha University, Egypt. Currently, she is working on his Ph.D. degree. Her research interests are: Blockchain, security, IoT and healthcare.

Ibrahim Gomaa received the B.Sc. degree in Electrical Engineering (Communication section), from Cairo University, Egypt, in 2002, the M.Sc. degree In Electronics Engineering (Computers and Systems Department), from Helwan University and National Telecommunication Institute, Egypt, in 2011. In 2014, he joined Helwan University to complete Ph.D. degree in Computer Science. He spent 13 years as a network security expert at National Telecommunication Institute, Cairo, Egypt (2005–2018). His current research interests include Information Security, network security, Virtualization, Cloud Computing, Big-data science, and Internet of Things. He is currently an Assistant Professor at National Telecommunication Institute (NTI), Cairo, Egypt.



Hala H. Zayed received her B.Sc. in electrical engineering (with honor degree) in 1985, the M.Sc. in 1989 and Ph.D. in 1995 from Benha university in electronics engineering. She is the ex-dean of faculty of Computers and Artificial Intelligence, at Benha university. She is now a professor at faculty of engineering, Egypt University of Informatics, Egypt. She is a member of the committee of experts in the national committee of UNESCO (committee of communications and informatics). Her areas of research are computer vision, biometrics, image forensics, image processing and machine learning.

Mohamed Taha is an Associate Professor at Benha University, Faculty of Computers and Artificial intelligence, Computer Science Department, Egypt. He received his M.Sc. degree and his Ph.D. degree in computer science at Ain Shams University, Egypt, in February 2009 and July 2015. He is the founder and coordinator of "Networking and Mobile Technologies" program, Faculty of Computers and Artificial Intelligence, Benha University. His research interest's concern: Computer Vision (Object Tracking-Video Surveillance Systems), Digital Forensics (Image Forgery Detection – Document Forgery Detection - Fake Currency Detection), Image Processing (OCR), Computer Network (Routing Protocols - Security), Augmented Reality, Cloud Computing, and Data Mining (Association Rules Mining-Knowledge Discovery). Taha has contributed more than 20+ technical papers in international journals and conferences.