Arabian Journal for Science and Engineering (2024) 49:3163–3191
https://doi.org/10.1007/s13369-023-07896-5

RESEARCH ARTICLE-COMPUTER ENGINEERING AND COMPUTER SCIENCE

State-of-the-Art Research in Blockchain of Things for HealthCare

Jameel Almalki[1]

Received: 25 July 2022 / Accepted: 15 February 2023 / Published online: 26 May 2023

Abstract
Existing blockchain approaches exhibit a diverse set of dimensions, and on the other hand, IoT-based health care applications manifest a wide variety of requirements. The state-of-the-art analysis of blockchain concerning existing IoT-based approaches for the healthcare domain has been investigated to a limited extend. The purpose of this survey paper is to analyze current state-of-the-art blockchain work in several IoT disciplines, with a focus on the health sector. This study also attempts to demonstrate the prospective use of blockchain in healthcare, as well as the obstacles and future paths of blockchain development. Furthermore, the fundamentals of blockchain have been thoroughly explained to appeal to a diverse audience. On the contrary, we analyzed state-of-the-art studies from several IoT disciplines for eHealth, and also the study deficit but also the obstacles when considering blockchain to IoT, which are highlighted and explored in the paper with suggested alternatives.

Keywords Blockchain · Internet of things · Blockchain of things · Edge computing · HealthCare · Software engineering

1 Introduction

The expansion of mobile devices like smartphones, laptops, sensors, and wearable has fueled extraordinary improvements in IoT in recent years. More than 500 million IoT devices are expected to be connected together by 2030. This tremendous expansion of IoT is expected to result in a flood of new applications and services across various industries like gaming, security surveillance and entertainment. IoT systems usually demand considerable computational capacity to manage data supplied by sensor devices with low latency. This is useful to provide time-sensitive services like transportation and intelligent healthcare. Cloud computing can assist IoT devices with calculating chores, but latency is still an issue. In order to move compute and storage closer to the network's edge, edge computing paradigm is introduced recently. The computational burden is imposed on edge devices in edge computing. However, moving large-scale computing and storage services to the edge introduces security risks, according to Microsoft's Safelight, a cloud computing platform.

Blockchain has been hailed as a viable answer for ensuring security and privacy for edge computing networks, along with enabling future generations of edge computing technologies. Blockchain in coordination with edge computing establishes a new paradigm for edge-IoT networks, which reshapes and changes them to allow new industrial and customer applications and services. However, the difficulty of blockchain, which requires significant computational power, poses a barrier in combining blockchain alongside IoT, which has limited resource and space abilities [1].

1.1 Related Work and Survey Contributions

Various recent studies in IoT, blockchain, and related topics have been examined from technological perspectives. To produce review articles on this research subject, several attempts have been performed. In the survey papers [2–4], an assessment of recent initiatives to integrate blockchain technology into various IoT scenarios and applications was presented. IoT and blockchain technology integration was also covered by the authors of [5]. The examination of block chain potential related to the IoT applications was done, which includes the manufacturing of smart cars, aerial vehicles and 5 G networks. The assessment in [6] focused on an examination of the technical facets of blockchain, including basic principles, networking, and consensus techniques. The authors of [7] talked about the opportunities, problems, and research

✉ Jameel Almalki
jamalki@uqu.edu.sa

[1] Department of Computer Science, College of Computer in Al-Leith, Umm Al-Qura University, Makkah, Saudi Arabia

issues relative to the amalgamation of blockchain and cloud computing. The article [8] surveys the security services in blockchain technology to deliver security services. It also discuss technical qualities to address related problems in IoT and cloud computing. A recent assessment [9] covered an overview of the combined model of blockchain and its association with edge computing, which is a form of extended cloud computing. Table 1 lists the major themes and its literature reviews pertaining to BCoT and this study.

Unlike the review works mentioned in Table 1, the purpose of this essay is to evaluate and analyze current state-of-the-art blockchain projects in several IoT disciplines, with a focus on the health sector. The primary objective of this study is to give readers a complete understanding of the blockchain and IoT integration using information gathered from relevant websites, technical studies, academic articles, and newspapers.

This study also attempts to demonstrate the prospective use of blockchain in healthcare, as well as the obstacles and future paths of blockchain development. In various aspects, this study varies from other research studies. The present study publications [17–20] highlighted prevailing blockchain research on a restricted amount of attributes, while we broke down the examined research into multiple parts. Furthermore, the fundamentals of blockchain have been thoroughly explained to appeal to a diverse audience. On the contrary, we analyzed state-of-the-art studies from several IoT disciplines for eHealth, and also the study deficit but also the obstacles when considering blockchain to IoT, which are highlighted and explored in the paper with suggested alternatives. We adopt a systematic approach to review existing literature. Our primary search engine was Google and search engine of each scientific database. Figure 1a shows a word cloud of commonly found keywords in our collected articles from reputed publishers such as Springer, ACM, IEEE, Science Direct, MDPI, and Research Gate. We refer approximately 400 articles to conduct this survey, largely from last 5-6 years. Figure 1b presents an overview of articles from various scientific sources. The top two sources are Springer and IEEE, while the other technology sources such as blogs and white papers contribute significantly to this survey (Fig. 2).

Although the combination of blockchain with IoT opens up a flood of new business opportunities, there are still a few roadblocks to overcome before the full promise of Blockchain of Things can be achieved. We highlight potential research challenges and unresolved problems in the field based on the thorough assessment of BCoT for healthcare. We also contemplate the state-of-the-art approaches to address these challenges and gaps. To broaden the scope of BCoT in upcoming system and applications, some potential future research trajectories are also investigated.

2 Background Concepts on Blockchain, IoT, and Healthcare

This section describes mainly the background required to understand the context before state-of-the-art in block chain for healthcare. We first present a solid background about blockchain in Sect. 2.1. Section 2.2 further builds a topic and explains potential benefits of blockchain in healthcare. Finally, we build a foundation on Blockchain of Things term in Sect. 2.3.

2.1 Blockchain

A blockchain is a shared and distributed record system that's also governed by various users in a P2P (peer-to-peer) network [21, 22]. Without a central authority or consolidated data storage administration, this method works [23]. Data is dispersed over multiple servers, and data reliability is preserved through reproduction and encoding [24, 25]. Blockchain was first published as an idea on October 31, 2008, according to a white paper created by Satoshi Nakamoto [26]. He devised the concept of bitcoin transactions on a medium that allowed digital transfers to be delivered personally from one peer to the other without the need for a banking agency. His major goal was to make a trust-free [27] program that utilizes peer-to-peer shared ledger innovation to overcome the double-spending challenge by computing the sequential order of activities [28]. The name "blockchain" alludes to a series of blocks, each of which contains a set of data about its history, current, and prospective [29, 30]. Whenever a new block is appended to the chain, each block performs a crucial function in linking with the prior block and the subsequent block [31]. Each block collects, verifies, and disseminates payments to other blocks [32]. This indicates that removing and amending a block in the chain could modify every following block [33, 34].

Blockchain network is a fragmented information scheme [35, 36] that stores details about every transaction history and runs on predetermined guidelines that specify how operations are performed and validated, but also how the whole system and its participants work [37]. Furthermore, because data is maintained on each server running in all of its various channels, such a system is sometimes described as a distributed registry [38, 39].

Any transaction unit in blockchain is merged into blocks of activities linked in the chain by hashing the preceding block's information [40]. As a result of this virtue of irreversible, blockchain networks essential safety characteristic is reinforced [41]. Data in a block is restricted toward modification as it progresses all along the chain (the older it is) [42]. If an intruder attempts to modify any of the variables, the local register will become invalid promptly since, based

Table 1 Major themes and contributions of the literature reviews pertaining to BCoT

Paper	Main contributions
Ferrag et al. [2]	This paper describes the blockchain concepts, specific security objectives, performance, constraints, computing complexity, and communication overhead. There is a side-by-side comparison for all the approaches for security and privacy in blockchain technologies. The authors address potential probable research directions in blockchain technologies for IoT and highlight open research issues based on the results of the current survey
Ali et al. [3]	In order to address these obstacles and successfully employ blockchain to provide a decentralized, safe medium for the IoT, they then develop a narrative on the difficulties presented by the current centralized IoT models
Fernández-Caramés and Fraga-Lamas [4]	Existing difficulties and potential improvements for BIoT applications development and deployment are described in depth. Certain recommendations are mentioned to enhance BIoT researchers and developers on some of the challenges that will need to be resolved before implementing the next generation of BIoT applications
Dai et al. [5]	The authors' main focus is on outlining the convergence of blockchain and IoT and outlining the BCoT architectural proposal. They also go into further detail regarding the challenges of implementing blockchain in IoT applications for the fifth generation and beyond, as well as BCoT's industrial uses
Mingli et al. [6]	The authors conduct a thorough analysis of the consensus mechanisms, the network, and the applications of blockchain technology before classifying it into four levels. Based on the sectors, different blockchain applications are categorized, notably in the Internet of Things (IoT)
Uriarte and DeNicola [8]	The authors take into account current standards for the creation of interoperable, decentralized cloud services that might compete with established providers and avoid vendor lock-in for blockchain systems. They think the study helps the development of cloud systems by examining the current standards and recommending new standardization opportunities, as well as by pointing out incompatibilities between projects and potential solutions for research issues in the area
Yang et al. [9]	The authors explore concepts pending to integrated blockchain and edge computing system and identify the research difficulties. They list various critical elements of the integration of blockchain and edge computing, including drivers, frameworks, enabling features, and difficulties. Finally, a few more expansive viewpoints are investigated
Qureshi et al. [10]	There is a taxonomy of application areas that can be combined with BC and IoT given. In order to fully realize the potential of BC technology for IoT, open research questions and difficulties must be identified and discussed in this article
Amanat et al. [11]	The authors proposed a blockchain-based architecture that secures EHR sharing among various electronic healthcare systems by authenticating user identities using a Proof-of-Stake (POS) cryptography consensus mechanism and Secure Hash Algorithm (SHA256)
Javed et al. [12]	The authors offer a thorough analysis of the current application frameworks for future smart cities. They also talk about the different technological difficulties that smart cities of the future will face. In order to create smart cities that set the standard for smart living, they finally determine the future dimensions of smart cities
Alam et al. [13]	This study mentions some case studies on blockchain technology. It also defines various needs and requirement for the implementations. The study also finds out various implementation needs in the fields of finance, economy, health, energy and many more. To serve as a guide for future deployments, it also addresses the difficulties in successfully integrating blockchain technology into the aforementioned sectors

Table 1 continued

Paper	Main contributions
Shahzad et al. [14]	For the best use of organizational resources, the authors have suggested a Blockchain-based Green Big Data Visualization (BGbV) solution using Hyperledger Sawtooth
Ali et al. [15]	The authors provide an overview of blockchain in terms of IoT reliability. They suggest a revolutionary architecture for trustworthiness in IoT-based smart cities based on blockchain
Qadri et al. [16]	In-depth analysis of how internet of nanotechnologies is changing healthcare IoT systems is provided in this article, along with a forecast of how these new technologies will be used to enhance quality of service (QoS) in future

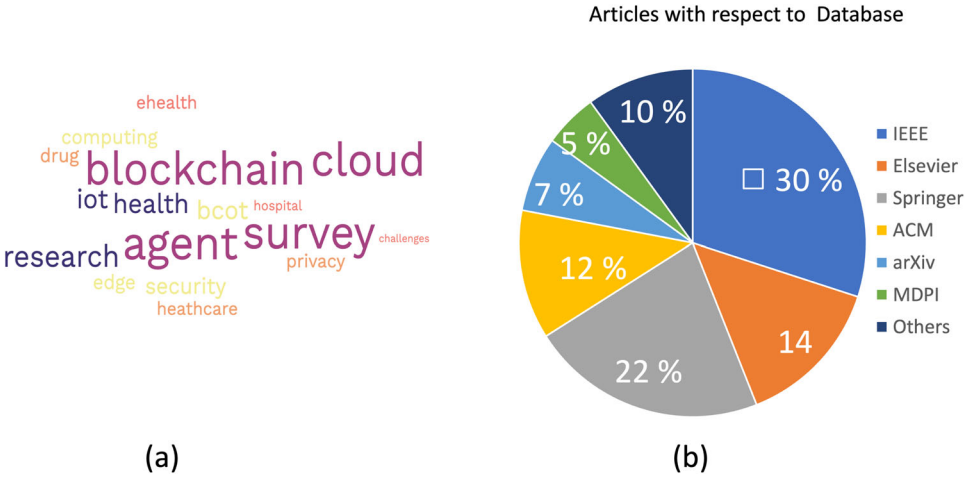

Fig. 1 **a** A word cloud of commonly found keywords in our collected articles for our survey, **b** An overview of percentage of articles from various scientific sources for our survey

on the hash function method, the hash numbers within the next block's directives will be radically distinct [43, 44].

Figure 3 provides an overview of operations in blockchain for Bitcoin. It illustrates a set of operations, when participant A transfers digital coins to another participants B.

2.2 Benefits of Blockchain in Healthcare

Researchers find a strong domain for studying architectures using blockchain in healthcare [45, 46]. This technology helps to create a reliable storage for all health data and to track real-time data at a granular level [47]. The researchers working in healthcare industry may need a large datasets to understand complex disease, advance discovery of drugs, and design a personalized treatment [48]. Blockchain provides a shared ecosystem of a wide variety of exchanging datasets [49, 50]. It allows to include patients of different backgrounds such as socio-economic and ethnic. [51] suggested the enabling of blockchain in integration with the IoT device for Medical healthcare. The authors termed it as IoMT blockchain. Moreover, the shared ecosystem (such as blockchain) makes it easier for healthcare professionals to collect data from participants (e.g., under-severed by medical community), which are in interest for the general public [52–55].

The use of blockchain technologies in healthcare industry will motivate the development of new smart app that would encourage the development of personalized treatments [57, 58]. The validity of information for both the patient and the healthcare unit will remain the same without any changes or obligations. This will result in a brighter option for the treatment [59, 60].

2.3 Blockchain and IoT

IoT connects people, things, and items to give chances for data collection by incorporating powerful computers, monitors, and actuators, all of which broadcast data to the central host, usually a cloud server. IoT data collected from sources is analyzed to generate concepts and techniques that may be used to impact corporate operations and lead to existing offerings. However, the IoT ecosystem's safety and anonymity are major problems that have stymied its widespread adoption. DDoS, Ransomware, and other unwanted assaults frequently target IoT systems. DDoS is a form of threat in which a subject, such as the main database, is assaulted with a large number of concurrent information queries from numerous

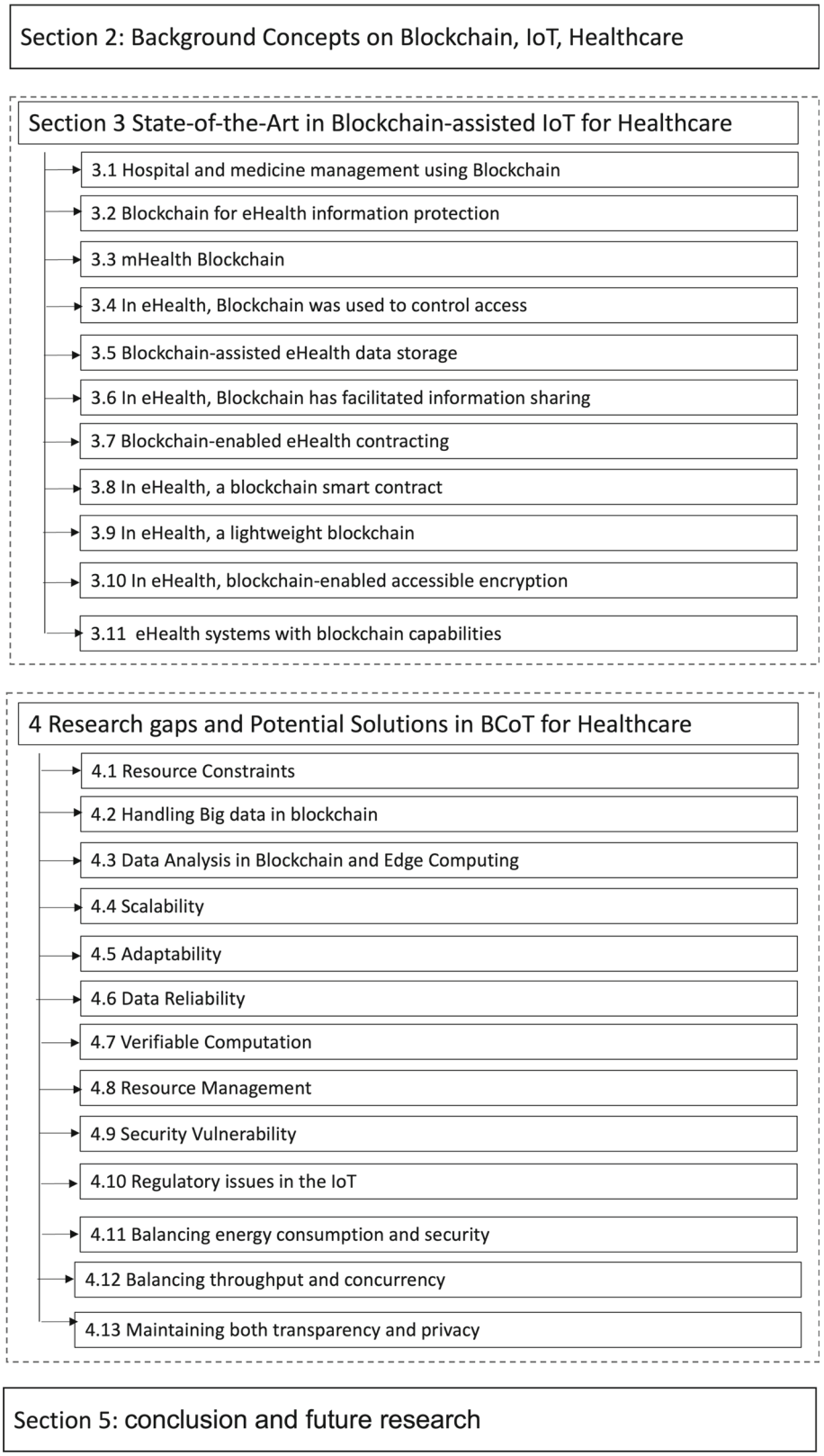

Fig. 2 The organization of this paper, illustrating contributions of this article

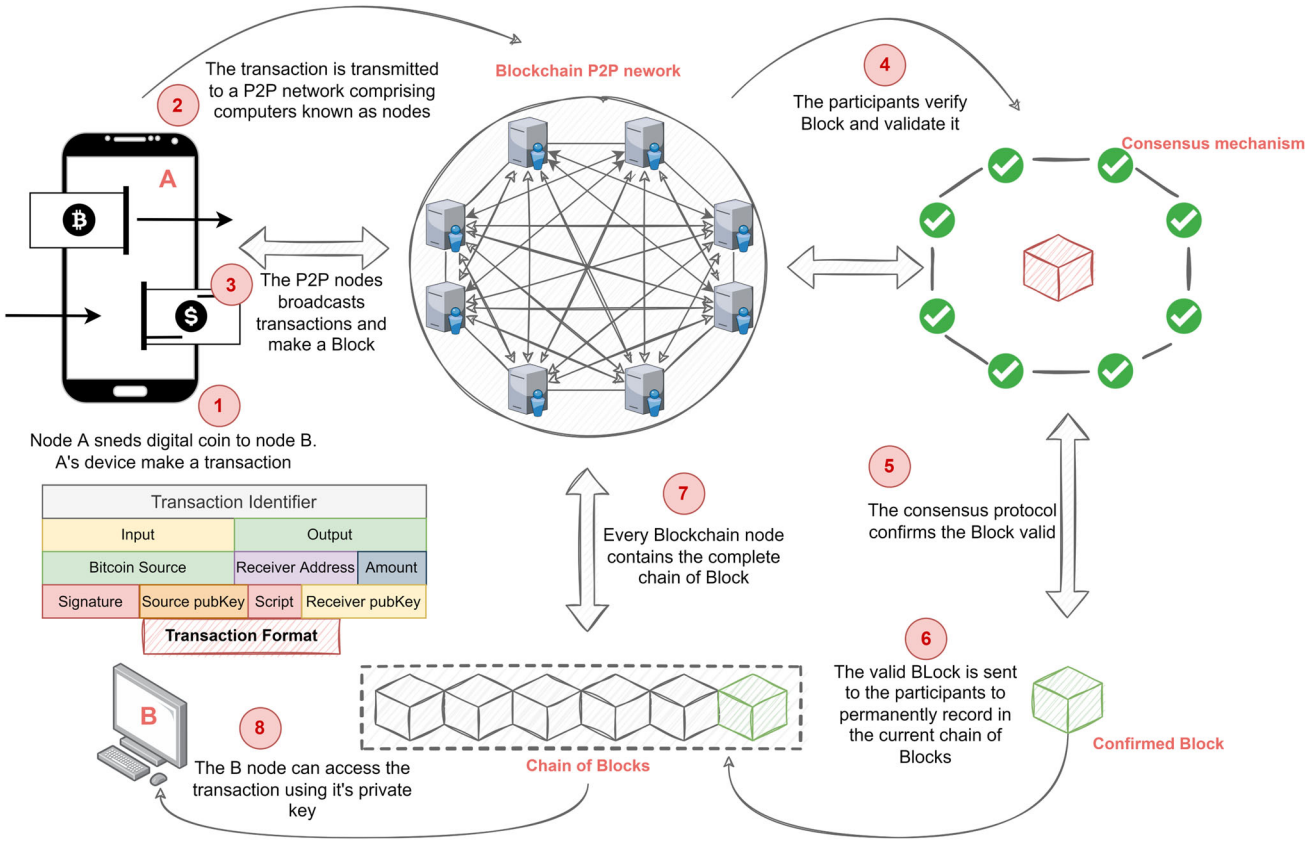

Fig. 3 An overview of operations in blockchain for Bitcoin (image credit to the work [56])

hacked system networks, culminating in a loss of access for affected users on the network. Furthermore, as the volume of gadgets accessing an IoT network grows, current centralized platforms may have bottlenecks when identifying, authorizing, and linking new hubs to the network.

With the answers to such IoT issues, blockchain, also referred to as DTL, has surfaced as a game-changing innovation that has the capacity to solve several of the IoT protection, anonymity, and scalability issues. Blockchain's shared record is tamper-proof, so there's no need to verify the other participants. Smart communities, smart architecture, smart grids, smart mobility, smart homes, and smart medical centers are just a few examples of IoT implementations. The introduction of block chain into the IoT realm results in the formation of a distinctive block chain sector, which can be called as BCIoT. The enormous amount of data which will be produced by the IoT devices under the BCIoT model will have uniform access across the world. The information which is available and redeemed in the pastimes can also be accessed by various parties under the smart contract. The authenticity will be ensured by the telecommunication carriers and third parties which are responsible to hold the data from the block chain-based network. Since the beginning, security and privacy are the largest concern into any block chain network, which might lead to loss of faith and adaptability for the users [61].

- If an IoT system requires a distributed P2P ecosystem, blockchain may address confidentiality and safety concerns.
- If an IoT system needs the preservation of a payment transaction for its offered functions without the involvement of other entities, blockchain can be a potential safe option [62].
- If IoT applications require the preservation of records and verification of consecutive activity, blockchain could be a viable option.

Nonetheless, when creating a system for IoT gadgets in connection with a blockchain registry, there are a few significant challenges that are needed to solve.

- One of the most difficult aspects of merging IoT and blockchain is figuring out how to data generated by multiple IoT sensors on blockchain. Additionally, when performing payments, blockchain may experience slower efficiency or higher delay.

– Maintaining security and activity anonymity is yet another consideration in the blockchain: in an open blockchain, payment record secrecy cannot be guaranteed. By examining activity histories, intruders can learn about the identity of people or gadgets.

3 State-of-the-Art in Blockchain-Assisted IoT for Healthcare

State-of-the-art studies relevant to eHealth systems are examined in this section. eHealth makes healthcare facilities and other clinical advantages available quickly to people who need them. The implementation of blockchain concept in eHealth can adequately solve crucial concerns of *confidentiality and protection*, as well as *improve overall efficiency* to encourage patient treatment and the progressive transition of current medical systems intodistributed eHealth [22, 63–65]. Researchers want to use IoT, fog, cloud, and blockchain to create an eHealth framework for safely providing information, data management, and network management.

Due to recent technological advancements in IoT, the connectivity has allowed the access of patient information, safe medication monitoring, hospital resources, and intelligent devices (e.g., smart phones, medical devices) which have promoted with blockchain-driven healthcare. For example, the physician frequently needs a reference of a patient's previous illness records, which can be compiled while the patient sees several doctors at various hospitals and clinics. Clients do not have recourse to the EMRs of healthcare practitioners in most contemporary eHealth scenarios. Yet, if a patient has insight into his health records, he can minimize the repetition of documents and medically unnecessary testing. Blockchain can significantly affect health service effectiveness and prices by giving patients full ownership over their prior health files, comprising records, financial information, lab results, x-rays and sign checks. Health data collected in distant patient surveillance contexts is quickly increasing and other health data, posing several issues, such as data sharing and data availability outside of healthcare facilities. Patients can use blockchain to improve the permission and trust of their medical records. In the following, we have articulated the state-of-the-art research in the area of IoT eHealthcare with blockchain assistance (Tables 2 and 3).

3.1 Hospital and Medicine Management Using Blockchain

Jamil et al. [66] created a blockchain-driven tracking software for health centers. People wearing sensor modules send important signs to approved blocks on blockchain systems in the hospital. The technology is improved and built on a cloud with front-end development using JavaScript frameworks. REST APIs, which IoT devices or a web user either triggers, offer product-centered solutions on blockchain. A contract enabled regulated entry to a ledger that ensures patient data is kept private and compatible with metadata, and the suggested channel housed blockchain ledger operations. The entry management strategy is also developed to enable network users and consumers to view allowed data and activities, ensuring that only approved professionals have accessibility to and alter IoT. The hubs on blockchain deployed couch storage to store the important sign deals. The system's efficiency is evaluated using the Hyperledger [74] test software, which comprised transaction read latency & throughput. Celesti et al. [75] have presented an eHealth solution that used an Ethereum blockchain to link the clouds of a federal institution to create a tele-medical facility. And though the writers explained the suggested system's medical process, no exhaustive study was performed to establish the platform's viability.

In many nations, a lack of proper state law and rules leads to tests and procurement of drugs from doctors' favored medical centers [67]. In addition, healthcare workers constantly manage patients' medical information, and diagnostic examinations are under their direction and monitoring, with patients being refused entry to those records. As a result, patients need to operate a similar exam two times when they change to a different medical practitioner. Rather et al. [67] presented a blockchain-driven hybrid model for handling multimedia created by IoT services to address these challenges presented in the conventional health service. The project's blockchain network comprises two sorts of hubs: certifying hubs and mining hubs, as well as executing servers. The preset executing block ensures that the miners data is not changed and modified. To assess the hypothesized scheme's safety, NS2 was used to replicate it.

The opportunity for blockchain to protect medicine supply networks is enormous. By making the actual drug logistics accessible to all partners at any point in the system, blockchain can effectively prevent fake products. Haq et al. [76] leverage blockchain to avoid fraudulent medicines in a drug delivery system. From medication creation to delivery, every activity performed on this platform was documented in a permissioned blockchain that approved officials can only access. As an outcome, the program guarantees openness and simplifies drug trading integrity. By combining blockchain, cloud, and IoT, Nguyen et al. [68] developed an abstract, diagnostic evaluation, and management system. They linked the information management software with a data sharing portal using a distributed mobile blockchain connection. A sensible access-based authentication method guarantees data confidentiality and authenticity on the admission security level. However, blockchain's durability and transmission costs were not studied.

Table 2 Summary of related work in eHealth using blockchain

Paper	Main contributions	Limitations
Jamil et al. [66]	The development of a cloud front-end interface for blockchain access. Healthcare providers can define access policies to patient vital signs using smart contracts	Concerns about security and privacy when sending vital signs to blockchain have not been emphasized
Rathee et al. [67]	Mining nodes and executing nodes are the two categories of blockchain nodes. The blocks are verified by the executing nodes	On NS2, the setup settings and deployment processes for blockchain were not detailed
Nguyen et al. [68]	To integrate EHRs and share data among medical professionals and patients, cloud blockchain technology was introduced	The handling of continuous health data on the blockchain has not been discussed
Liang et al. [69]	Data about patients was verified, preserved, and shared with various stakeholders via blockchain	IoT device privacy and security were not taken into consideration, and a real prototype was not created
Nguyen et al. [70]	On the cloud blockchain platform, smart contracts based on EHRs' reliable control mechanism and data exchange protocol were created	Analysis of the proposed system's security and privacy was overlooked
Nguyen et al. [71]	A portable blockchain was created for conducting clinical evaluations	The blockchain's difficulties with scalability and communication costs have not been researched
Ni et al. [72]	To maintain blockchain mining economically viable, the authors created an ideal decision-making procedure	There hasn't been any simulation to evaluate its performance
Ichikawa et al. [73]	To collect wearable sensor data and store it in a private Hyperledger blockchain, the authors created a smartphone app	In terms of throughput and energy usage, performance has not been examined. Unresolved are the security concerns with sensors and mobile apps

Table 3 Summary of related work in security and access control

Paper	Main contributions	Limitations
Tanwar et al. [79]	The blockchain contained access rules for healthcare organizations. They created algorithms for access control	Unresolved security issues included hostile attacks and authentication
Xia et al. [80]	On the Ethereum blockchain, ABE (Attribute-Based Encryption) was implemented using smart contracts	Blockchain delay is still being dealt with
Liu et al.[81]	EHRs were kept in the cloud and their index was kept on the blockchain	Performance evaluation is lacking
Xia et al. [82]	To track users' data access behavior, a smart contract-based access control architecture was created	No in-depth performance study has been done
Dwivedi et al. [83]	For running blockchain, the writers built an overlay network	To assess performance, no simulation of the system was conducted
Shen et al. [84]	Blockchain and a standard P2P network are two distinct networks that were created. Additionally, a session was developed for packaging and removing health data during sharing	There are no descriptions of blockchain settings and configuration
Fan et al. [85]	The authors introduced healthcare data exchange on a blockchain. The provincial hospital engages in block-making and gathers information from community centers	blockchain arrangements are not discussed
Hang et al. [86]	The proposed plan uses blockchain to coordinate EMRs across many institutions. Smart contracts were created to store data, logs, and control data access	The method's viability was shown by its implementation
Zhang et al. [87]	A theoretical framework for exchanging health data was presented, in which the data's hash value was kept on a blockchain	The framework has yet to be created in its actual prototype form

Investigators are very interested in using blockchain to offer safe and dependable storage space for the healthcare industry. But, only a few nations (e.g., Estonia, Peru) have implemented blockchain health systems in actuality. Recently, blockchain-driven medical procurement control system was launched in Peru [77]. blockchain was integrated with the Amazon Cloud to govern the healthcare logistic system, maintaining a safe interaction between sales staff, producers, and customers. Agreements are being created to store medical sensor information to avoid unauthorized changes and adjustments. The suggested technique does have a flaw in that it does not handle privacy protection. The efficacy of blockchain concept in delivering health solutions via IoT and Cloud of Things was noted by Kang et al. [78]. Unfortunately, no performance evaluations for the suggested protocol have been completed.

3.2 Blockchain for eHealth Information Protection

Maintaining anonymity in an eHealth system allows for more effective communication between the doctor and the patient, which is essential for good care, independence, and the prevention of financial harm, shame, and prejudice [88].

Blockchain-driven IoT eHealth was created by experts [89–92] to secure patient and healthcare worker confidentiality. Ref. [89] study is a secrecy health data interchange solution that combines an IoT network with storage on cloud. To protect health records, EMRs are kept safe on the cloud level utilizing clever deal software, while the categorization of the documents is preserved in blockchain. As a result, EMRs cannot be modified or altered irresponsibly. Unfortunately, the system has yet to be applied in a real-world setting.

Ref. [90] used blockchain to create a privacy-preserving cloud health information system. The cloud blockchain record stores bright contract-regulated encrypted medical files. Encrypting content before entering it into blockchain efficiently addresses user privacy concerns, improving the openness and safety of storage on cloud systems. The work's shortcoming is that there were no evaluations among standards and smart contract-based methods.

A robust cloud-assisted blockchain EHR infrastructure was developed in Ref. [91] with four units: a key generation center, healthcare providers, cloud users, and data clients like insurance companies. Blockchain stores patient records with a time-stamped, which improves the legitimacy and transparency of health information. The study's flaw is that no agreement for data storage management has been created. All parties on blockchain P2P system have access to blockchain record. Before publishing a block onto the decentralized blockchain record, users validate its composition. The transparency of blockchain poses a severe threat to patient confidentiality in the eHealth sector. The work [92] redesigned blockchain peer-to-peer system to accommodate Attribute-Based Encryption methods (ABE). Depending on their functions in blockchain network, the experts classed blockchain sites as cluster heads, feature authority, and miners. blockchain network's cluster head is linked to IoT devices to obtain data. The cluster head is in charge of performing algorithmically focused processes such as data acquisition and encryption/decryption. At the same time, Attribute Authorities (AA) can give the competencies needed to decipher statistics to doctors, nurses, and other health professionals standing as miners. The chosen miners can decode the blocks utilizing AA's characteristics for confirming and certifying blocks.

3.2.1 Interoperability

Interoperability between current databases, institutions, and national borders is very important for healthcare industry. This could improve the information quality and patients' life. Au et al. [93] developed a cloud-assisted system for securely sharing medical data. The personal information of patients' can be stored on a cloud server. As a result, doctors can share patient data for further research purposes without releasing personal information.

Patients-driven interoperability, in which users employ assisted APIs to access personal medical data, was the focus of William et al. [94]. The authors looked at how blockchain may be used to protect patient health data interactions, share it with others, identify data seekers, and aggregate disparate data. According to the authors, more research should focus on blockchain patient-assisted interoperability's current limits. They utilize blockchain's scalability difficulty in managing clinical data transaction volume as an example of these difficulties. Finally, Gaby et al. [95]presented the Ancile to address interoperability, which is an Ethereum-based system that employs contracts to regulate data access and privacy. freshly developed encryption techniques were used for privacy, along with the Ethereum-based smart contracts. The framework proposed by the authors, is in early ages in the community and require further more investigation, as well as development. The authors proposes the Ancile as an early stage framework in the Ethereum community, and it needs further investigation and development.

Azaria et al. [96] presented a blockchain-based system that can manage EMRs record. The proposed techniques ensure immutable records, easy access, accountability, authentication and the secrecy of sensitive medical data. It can also be adapted to existing data storage providers' systems, assuring compatibility. However, interoperability involves a significant degree of data sharing and transmission. Information could be copied, spread, or modified due to this. Roehrs et al. [97] proposed a framework that combines disparate data from various sources. OmniPHR is a scalable and elastic sys-

tem that combines blockchain concepts to handle massive datasets.

3.3 mHealth Blockchain

Utilizing mobile-assisted encrypted text messaging, patient applications, and tele-health, healthcare professionals have boosted their patients' involvement and commitment to medical procedures. However, private communications among various hospital units including patients are still the most common usage of portable devices in IoT healthcare in the current environment. Nonetheless, blockchain-related efforts [69, 70, 72, 73] have used smartphone apps to correctly record health information from a patient's sensing devices and provide timely health services.

Liang et al. [69] developed cloud computing environment powered by blockchain, that sends data from sensing devices to cloud processors through a smartphone. The researchers wanted to create a patient-centered system that would allow medical providers and insurance firms to exchange health information. Customers, mobile sensors, health professionals, insurance firms, the cloud environment, and blockchain platform were among the six types of participants in the program. Hyperledger Fabrics, a permission business blockchain, was used to verify and maintain the patient's data while distributing it to other parties. Three goals were achieved by deploying blockchain in the cloud:

- To guarantee that data input is accurate.
- To respond to demands for data entry from other entities.
- User authentication access control should be implemented.

The cloud service is set up to link to the P2P dispersed blockchain channel's members via a Hyperledger Fabric user, ensuring that the cloud user's demands remain anonymous. However, they did disregard safety concerns like vicious assaults on IoT devices.

Similarly, Nguyen et al. [70] proposed a system that would link several EHR systems and allow healthcare practitioners and clients to access health information. blockchain was integrated into a cloud server, where intelligent contracts facilitate data entry operations. In cloud, a decentralized storage makes an effective data sharing than centralized distributed systems that has privacy and low latency. Ni et al. [72] figured out HealthChain. The system which is proposed by the author contains three important parts that were performing the operations as data collection, verification and storage.

The study contemplated various members to maintain less mining cost. They also devised an efficient decision-making approach for maximizing the economic benefits of mining operations. The researchers, however, did not specify which modeling techniques or computer languages were employed to undertake the efficiency investigation.

Ichikawa et al. [73] proposed a mHealth system which used blockchain to protect data from manipulation. They created a mobile app that uses the JSON standard to record data from sensing devices and save it in a Hyperledger Fabrics personal blockchain. In addition, the writers looked at how well health data was integrated into fault circuits. Privacy vulnerabilities between sensors and the mobile app, on the other hand, have not been resolved.

3.4 In eHealth, Blockchain was Used to Control Access

A safety compromise might hinder a patient's privacy, illness, or even life by manipulating patient information, eHealth system safety is critical [98]. Authorization is one of the essential security elements since it guarantees that only authorized users with the appropriate permissions have entry to health services. The privileges of any individual, entity, or institution to obtain health records inside the domain are referred to as access control. Healthcare organizations must, of course, establish fine-grained access control [99]. For example, only prior enrolled providers must have admittance to a real-time Electrocardiograph (EKG) tracking system. Various ways [79, 100–102] have been suggested to handle verification and access control challenges in blockchain eHealth network.

Tanwar et al. [79] suggested distributed ledger to handle health record access rules based on these challenges. In their patient healthcare paradigm, the author conducted many methods that determined entry rules for care providers. They used Hyperledger Fabric & Caliper, Docker, Wireshark recording tool, and Composer to evaluate the system's efficiency regarding bandwidth and delay.

To further secure the security and availability of data, Wang et al. [100] developed a data sharing platform which can provide fine-grained network access. Wang et al. [100] created a distributed cloud infrastructure including an Inter Planetary File System (IPFS) for distributed data, and an Ethereum. A wise contract-based access control managing method has been proposed in this study to execute search terms in the distributed storage, which improves the platform's QoS and security. However, one of the study's flaws is that data protection and the latency caused by access control approaches were not considered. Wang and colleagues [103] desired a blockchain cloud architecture to hold medical data utilizing health data activity login mechanism with blockchain. Blockchain's P2P network detects any changes to the cloud files. In reality, this model reduces the expenditures of third-party digital storage management. The paper, however, does not provide a blockchain sample.

In Ref. [101], Islam et al. built a system to aid Health Prescriptions so that clients obtain doctor suggestions. After

proper validation, the platform issues a Security Access Token (SAT) to IoT systems, that determines the rights of medical devices and assets for the user. When requesting operations from the network, IoT devices have included encoded SAT. Furthermore, it incorporates an access control based on OpenID method to protect illegal access to health gadgets. The design, however, is notional, and no effectiveness study was conducted.

Ramani et al. [102] proposed a blockchain-driven method for data availability for the healthcare. With a patient's authorization, the technology enables doctors to update and extract health data. To assess safety, a unique blockchain was proposed. However, the authors did not use emulator or create a prototype to test the suggested technology's effectiveness.

GDPR [104] defined privacy policies across Europe to safeguard users' rights and secrecy over their health records. As per the rules, a provider must include capabilities for the user's permission and removal of that permission in their platform. Furthermore, the provider must publish a statement on how the user data is managed and utilized on the user's demand. Moreover, the service provider should deliver all of the data to the consumer in a computer-readable manner. Ref. [105] proposed a new eHealth architecture that combined blockchain innovation and the cloud to transmit health data with authenticated persons effectively and openly while adhering to data standards such as GDPR. To assure the QoS of the shared information, the writers used an AI model to evaluate the reliability of health data. However, the article's main flaw is that no effectiveness evaluation was carried out.

3.5 Blockchain-Assisted eHealth Data Storage

In a standard cloud IoT-enabled care system, health records are often handled and kept in cloud, under the management of several Cloud-Service Providers (CSPs). CSP should be open but wary of the potential of necessary patient data being leaked. While adopting cloud network security, EHRs are also vulnerable to numerous data storage assaults. Blockchain has the potential to make existing systems of storing patient records safer and more efficient. Data integrity may be preserved while also assuring that it is tamper-proof using blockchain. On-chain keeping is one technique to save data on a blockchain. However, putting a block on blockchain comes at a considerable cost [110]. Therefore, on-chain storage isn't seen to be economically or practically possible. On blockchain system, though, additional data storage process known as off-chain can be used. The hash code of data that is comparatively brief, is saved in the ledger, while the information is held in standard archives in an off-chain fashion. The on-chain technique has a cheap storage price since the hash value is relatively brief [111]. The majority of the studies described in Tables 4 and 5 have taken an off-chain database strategy to address the memory cost issue on blockchain system. Zheng et al. [105] proposed a methodology for exchanging individual health data in real-time utilizing blockchain-driven distributed storage on cloud. Health records are typically securely stored off-chain in traditional storage on cloud to alleviate the space strain in blockchain system, with only hash values injected into blockchain. But, a basic sample has yet to be created.

The usage of blockchain in healthcare has become fashionable, particularly when it comes to securing medical data sharing and management. The technique is taken by Zyskind et al. [26] uses blockchain which enables service providers and user to share information and data with maintaining security. In this solution, there are two types of transactions. Transactions are used to save and retrieve data, to begin with (Tdata). Second, transactions to access are used to control access. MedRec [96] is a decentralized Electronic Medical Record (EMR) management system based on blockchain. It includes a functioning prototype based on three different Ethereum smart contract types. Patient data is accessed after successful authentication from various medical facilities utilizing MedRec. Yue et al. [112] suggested a blockchain-based

Table 4 Summary of related work in different architectures for BCoT in healthcare

Paper	Main contributions	Limitations
Chen et al. [106]	Blockchain technology was used to create a searchable healthcare system. The lookup index is present in the blockchain	It wasn't shown how searchable encryption based on blockchain outperformed the traditional
Islam et al. [107]	The authors created a framework for recognizing human activities that uses fog-cloud computing powered by blockchain	The authors did not explain how blockchain was used in the suggested architecture, and no performance evaluation of the cloud platform, fog, or blockchain was done
Akkaoui et al. [108]	Edge nodes certify the transactions in a hybrid edge blockchain-based healthcare system, and a second global blockchain keeps metadata	Block processing delay may grow with additional global blockchain use
Calvaresi et al. [109]	Reputation management for the Agents was handled by combining MAS and blockchain technology (BCT)	The article omitted discussing the blockchain's performance

Table 5 Summary of related work in blockchain of things for resource-constrained devices

Paper	Main contributions	Limitations
Park et al. [119]	To offer incentives to data owners, a crowd-sourcing platform built on the blockchain was created	The proposed scheme's performance has not been tested
Daraghmi et al. [124]	The authors created a timed smart contract-based architecture for managing permissions for access to medical records. To do away with the necessity for digital currency, an incentive-based mining procedure was suggested	The continuous patient monitoring data were not intended for use in the model
Kazmi et al. [125]	The licensing of medical personnel and equipment for remote patient monitoring is managed and controlled by smart control	When obtaining data from wearable sensors, security and privacy concerns were disregarded
Malamas et al. [128]	Blockchain technology was suggested as a way to store digital evidence and logs in a medical forensic framework	The proposal's prototype was not put into practice
Mytis-Gkometh et al. [129]	The suggested solution uses blockchain technology to secure biomedical database searches	Different cybersecurity attacks relating to blockchain were not covered
Ismail et al. [130]	Only the cluster head keeps the blockchain ledger in a lightweight blockchain that has been developed	The approach is unable to guarantee that the data cannot be altered
Jinhong Yang et al. [131]	Proof of Familiarity, a novel context-aware consensus procedure, was introduced to acquire knowledge from medical experts and patients who have recovered in order to make medical decisions	High-level performance study was conducted; however, the proposal's prototype has not yet been put into action

healthcare data gateway. Its purpose is to provide patients control over their information while also protecting their privacy. On the other hand, the authors do not go into enough depth regarding how to prevent a service from unfolding content of data when computing raw data. [113] employed an agreement system and identity-assisted authentication to verify user membership. However, only those who have been invited and authenticated are able to exchange sensitive health information safely. Patients and clinicians can access cloud archives and share data with Medshare [82], a blockchain-driven solution described by the same authors. Provenance, control, and auditing of data are all guaranteed.

3.6 In eHealth, Blockchain has Facilitated Information Sharing

Given the delicate aspect of patient records, protecting patient confidentiality while transferring EHRs is a crucial concern. Because of its scalability and tampering resilience, blockchain has emerged as a viable answer to this problem [81]. Xia et al. proposed a medical data exchange paradigm dubbed Medshare in Ref. [82], which used blockchain to exchange data between unknown CSPs. The authors developed an entry tracking model that enables smart contracts to monitor data users' access behavior and identify security breaches. blockchain-driven CSPs could allow inspection and confirm the origin of healthcare experts without jeopardizing privacy protection. Cloud-assisted data acquisition issues should be acknowledged and resolved. The study in Ref. [80] provided a standard encryption solution for ensuring adequate access control and user identification when transporting information in the cloud layer to resolve this concern.

Doctors are often trained to provide medication and treatment to patients to treat a given ailment. Many disorders, meanwhile, necessitate cross-border health expertise from a variety of medical providers around the world. For more accurate medical care, specific assessment, and cure, blockchain system can ease the interchange of health providers' skills. Wang et al. [100] proposed a modified healthcare system that combines expertise from three areas: synthetic intelligence, computer tests, and concurrent execution to increase the accuracy of medical care and cure. First, a "descriptive cognition" artificial healthcare system (AHS) was created to replicate and represent patients' and doctors' fixed and fluid properties. Second, computer studies were performed to combine several illness situations to examine the relevance of alternative therapy courses in AHS. "Intelligence anticipatory" is the name of the stage. Finally, the final routine was picked from a roster of experts' recommendations and implemented simultaneously in AHS and the existing healthcare system to give "prescriptive knowledge". To enable EHRs to be traded, reviewed, and verified, the platform used a consortium blockchain that included users, health experts & institutions in healthcare and blockchain-powered intelligent contracts.

Health data storage on blockchain is a transparent and fair platform that can help to improve health services. Indeed,

integrating cloud, IoT, and blockchain can significantly allow innovative health solutions to develop [114]. Dwivedi et al. devised a distributed blockchain data protection mechanism in Ref. [83]. Five elements make up the equipment: an overlaid network, cloud servers, care providers, intelligent contracts, and clients. The work used a P2P network to connect blockchain to storage on cloud. Each storage on cloud maintains health information in the shape of blocks, and the hash bits of these blocks are saved in blockchain, making it easier to trace any modifications in the cloud data. A dual encryption system is also offered to protect info from possible threats. The study's flaw is that no accurate tests of the proposed safety method have been produced.

Nguyen et al. [70] proposed a blockchain-driven EHR sharing design with standard interplanetary file system storage (IPFS). In addition, smart contracts were created to construct a reliable access control system to improve the safety of EHRs throughout their transfer. In particular, a data transfer method for client entry to the EHRs network was created. Amazon Web Services offered cloud for the mobility trials, which were done on a mobile Android application. The assessment's findings show that the proposed method can be used in various e-health settings.

Medchain, a system for exchanging medical records, was suggested by Shen et al. [84]. The writers used two decentralized systems: a blockchain peer-to-peer channel and a traditional peer-to-peer channel. blockchain network keeps irreversible data summaries and info, activity, and operation fingerprints, whereas the conventional P2P network retains mutable data and meeting details. In the data exchange process, a procedure for bundling and removing changeable data is included, which can decrease storage overhead. Fan et al. [85] proposed a blockchain-driven clinical sharing feature in which local clinics acquire medical abstracts from regional hospitals and other healthcare centers' electronic medical records. After analysis, the local hospitals bundle health information into blocks and send them to the agreement hubs. Inciting inquiries, checking, and confirming blocks is the duty of hospitals serving as both commands and endorsers. A hospital can choose to keep its patient data on its ledger or send it to blockchain.

3.7 Blockchain-Enabled eHealth Contracting

The outsourcing medical services to CSPs have grown important in reducing the computing burden [115] locally in recent years. An act of relocating a company's inner activities or products and decision-making to providers through contractual agreements is known as outsourcing [116]. Outsourcing work to a cloud computing service, on the other hand, presents many additional issues. For example, the cloud provider may be interested in a recipient's sensitive information and violate the client's confidentiality. In addition, the customer must sign contracts with a provider to ensure that privacy is protected [117]. Blockchain has been examined as a possible solution to resource exporting concerns such as safety, anonymity, money, and agreement [118–120].

Cao et al. [118, 119] introduced a cloud-assisted eHealth system that uses blockchain to safeguard medical users' EHR exports. A blockchain system called Ethereum was used to handle user activities without the demand for a third party. Health records were inserted into tamper-proof Ethereum to protect the validity of EHRs. A smart contract for service management, on the other hand, has not been examined. Park et al. [119] proposed using cloud-assisted crowd-sourcing to create the CORUS medical correction and assessment system. Crowd-sourcing is a method of gathering works, information, or viewpoints/opinions from many individuals using the web, social networks, and mobile apps. Crowd-sourcing enthusiasts work as paid contractors, whereas others volunteer to accomplish jobs [121].

Crowd-sourcing on a typical system has various flaws, including a sole source of error, the operator's hidden misconduct, and a disagreement between task applicants and employees [120]. The distributed account in blockchain enhances the credibility of verified records and the efficacy of the suggested crowd-sourcing system [119]. Blockchain, a groundbreaking distributed concept, can be adjusted to eliminate the shortcomings of conventional crowd-sourcing schemes and usher in technological advances such as devolution and openness [120, 122]. Furthermore, Park et al. [119] used blockchain to entice many users by giving funds for delivering accurate data. However, the efficiency study of the cloud blockchain has not been explored, which is a flaw in the paper.

3.8 In eHealth, a Blockchain Smart Contract

Due to their programmed aspect, smart contracts have become one of the most looked at innovations since the advent of blockchain [123]. A smart contract consists of rules and agreements expressed in computer code. When a contract-related event occurs, the intelligent contract recorded in the shared database is executed directly on blockchain without needing a third party [123].

Daragh et al. [124] created a smart medical contract with a timer design to manage record entry and permissions. By implementing appropriate user rules, the agreements proposed in this study control activities and track computations on EMRs. Authors presented an incentive-driven mining mechanism to reduce the need for virtual money. In this mining method, the server with the lowest rating creates the next block, while high rated nodes approves newer nodes in the blockchain system. This maintains provider stability and the system's long-term viability. The testing was performed on Ethereum, an open-source network that includes

the implementation of smart contracts making use of solidarity programming syntax. But, cybersecurity was not handled, and there was no way to obtain continual health records on blockchain.

Kazmi et al. [125] created a blockchain-driven remote monitoring platform that used smart contracts to register patients as well as healthcare providers and grant permits for wearable sensors. In addition, the software can provide a genuine notice, encouraging consumers and healthcare professionals to participate in patient surveillance. The suggested program's intelligent contracts were created using the Ethereum network. They used Remix, an open-source web engine, to develop, analyze, and publish their smart contracts. Unfortunately, safety and confidentiality concerns were overlooked while obtaining data from sensors.

Hang et al. [126] presented a blockchain-driven infrastructure to safeguard EMR administration across hospital divisions. Smart contracts were used to store patient records, record files, and limit entry to healthcare data among various health organizations in the EMR administration network. They put the framework through an experiment conducted on many hospitals to show that the system is feasible in effectiveness and potency. Hyperledger was used to create smart contracts. The tests and concepts were detailed in great depth. The paper in Ref. [127] identified the use of blockchain and IoT driven e-Healthcare systems.

Malamas et al. [128] developed a forensics-enabled architecture for medical equipment using blockchain. The technology uses smart contracts on blockchain to provide good authorization. The intelligent agreement establishes rules and ensures that records are kept safe and secure. In addition, the Proof-of-Stake (PoS) consensus protocol certifies blockchain activities. Patients, doctors, healthcare providers, and investigators typically make a wide array of inquiries to a biological database utilizing appropriate API at any one time. Therefore, it is essential in a typical log record process to ensure tamper-proof content and client inquiries. According to Mytis et al. [129], blockchain confirms a validity and non-repudiation of data recovery from a traditional biological registry. The scheme consists of three parts:

- A front-end functionality that third parties can use to make requests.
- A connection for conversing with the biomedical functionality.
- A smart contract among applications and the database connection logs all users inquiries in blockchain.

The Ethereum blockchain implemented smart contract to ensure authorization modules written in Solidity. MongoDB was used to store Biomedical data.

3.9 In eHealth, a Lightweight Blockchain

Due to mathematical concepts like required cryptographic methods, PoW and the Merkle Hash Tree [132], most critically, IoT is frequently underperforming. Experts have offered a range of ways to improve present blockchain [127, 130, 133].

Ismail et al. [130] presented a gentle blockchain-driven healthcare design. The authors separated blockchain network regionally and assigned distinct functions to blockchain hubs. The Leader Blockchain Manager (HBCM), often known as the cluster head, is in charge of operations and block creation. The HBC avoids forking by keeping a replica of ledgers for its users. The personalized blockchain can speed up computing and interaction, but it cannot ensure that the record is tamper-proof. Regarding convenience and computation complexity, the suggested approach was tested on NS3 and contrasted with the Bitcoin blockchain. Srivastava et al. [134] used lightweight cryptographic techniques like the ARX encryption method to reduce energy usage of blockchain-driven healthcare. Furthermore, the Ring Signatures were employed to improve the singer's secrecy and personal qualities.

Ray et al. [135] also announced the creation of IoBHealth. This new IoT-driven eHealthcare blockchain architecture is more resilient, safe, accessible, and efficient for collecting and sharing EHR data in healthcare. Attia et al. [136] designed a system that is IoT-driven blockchain-assisted to follow patients via intelligent devices. The writers built an User Interface that allows users can view data ledger in simple representations and displays using Hyperledger Fabric as a blockchain. Furthermore, rather than employing device IDs, the platform used the Naming Data Networking method, which facilitates data portability between discrete groups.

After a miner accomplishes the PoW for a block in a chain-organized blockchain, the block is transmitted all across the system, creating a scalability issue and a high network overhead. Srivastava et al., by adding the GHOSTDAG mechanism, a transactional verification system, [137] developed a sustainable blockchain for remote monitoring. Instead of a single massive chain of blocks, the GOSTDAGE method treats each operation as a cluster.

The issues of combining blockchain with sensing devices were addressed by Dwivedi et al. [133]. blockchain network, storage on cloud, medical providers, intelligent contracts, and clients outfitted with devices for the clinical purposes are all part of the network. The algorithm, which regulates the block chain network comprises of a centralized server, which acts on top in the hierarchy. This server is responsible to handle all the blocks that are committed across the various peer nodes in the P2P network. The clustered server is responsible for the inspection as well as execution of the blocks.

Yang et al. [131] presented a new consensus protocol to support eHealth blockchain applications. Proof of Familiar-

ity (PoF) is a suggested decentralized system that comprises a cooperative medical decision-making process for providing healthcare to a person. The technology allows a healed patient to help a new patient with comparable conditions and illnesses, a medical judgment from various doctors, and health company marketing strategies during this procedure. To make an excellent shared medical choice, all parties, both healthcare practitioners and formerly treated patients, contribute comments. This judgment and the hash of the patient records are saved on-chain, while the health information is held off-chain in a database server. The paper's flaw is that the model has yet to be tested to see if the suggested consensus process is feasible.

3.10 In eHealth, Blockchain-Enabled Accessible Encryption.

The initial method of storing health data has altered due to the fast expansion of cloud computing [106]. In principle, health data is critical and must be safeguarded from illegal access. Therefore, before being uploaded to cloud services, health data is usually protected. The data encryption determines the effectiveness of obtaining these data on the cloud [138]. SE (Searchable Encryption), a potential cipher technology, ensures data protection while preserving data discoverability [106]. However, most current systems, especially Searchable Public-key Encryption (SPE), are subject to dynamic leakage-exploiting threats or are incapable of fulfilling the performance demands of real applications [106]. Authors have explored combining blockchain with a regular cloud retention system to provide a robust and reliable keyword search in the healthcare sector.

Chen et al. offer improved searchable encryption in Ref. [106]. Blockchain is being used to create a healthcare system. The search indicator is saved on blockchain, while the cloud service records the information. To obtain the data, customers must first request approval and an encryption key from the holder. In contrast to prior research in Ref. [139], the platform used a complicated Boolean expression to retrieve the index-building EHRs. It permitted queries that allowed various care workers to seek authorization to view and engage with the health records. In addition, Ethereum blockchain-based smart contract was built to track remuneration, comprising transaction cost, between the people participating in a multi-user situation.

Wang et al. [140] devised a blockchain-driven cloud-aided consortium structure for managing and retrieving electronic health data. blockchain maintains encoded phrases to make it easier to find health data that has been transmitted to the cloud. They designed the framework of blocks and operations to store information safely and created basic cryptosystems. When users have consented to the data owner, the cloud database supports re-encryption and transmits the re-encrypted cipher text to the selected data applicant. A blockchain-assisted accessible EHR storage solution was also proposed in the paper [141]. To guarantee fine-grained user access to EHRs, the cloud provider saves health data by utilizing attribute-based cryptography. blockchain contains EHR data phrases used to create indexes that allow data users to locate data material on storage on cloud. Blockchain was advocated by Noh et al. [142] for logging records of health files controlled by cloud providers. A proxy re-encryption mechanism was added to the original study for privately transferring patient data.

Yuksel et al. [143] looked into E-Health Services' privacy, security, and integrity (EHS). They described and classified the existing encryption methods in use in this industry based on access control, searching, and emergency response strategies. Khan et al. [144] investigated GPIT, a patient identification system that anonymizes patient information while preserving the data connected with it. An identity key, which encrypts the patient's name, gender, and mobile phone number, is used to gain access to medical records. The GPIT system was put to the test in Bangladesh's healthcare sector. Suzuki and Muai [145] proposed a blockchain-driven log system that is based on strict audit for confirming the request response system for the client and the server.

3.11 eHealth Systems with Blockchain Capabilities

Fog computing offers numerous advantages and is ideal for applications requiring quick reaction times, low latency, and authentic operations, particularly in healthcare [107, 146]. On the other hand, fog computing raises questions about multiple systems, safety, anonymity, reliability, and strategic planning [147]. Blockchain has been implemented in fog-enabled systems to address these challenges. In video stream analysis, Islam et al. [107] upload the input to a fog server located near the video camera rather than the cloud. The writers created a framework for recognizing human activities that used blockchain-driven fog–cloud computing. Before entering information into a multi-class Support Vector Machine (SVM) decoder using an error correction, they selected the main characteristics from the video feed. The paper's advantage is that it examines the reliability of the movement detection method utilizing various databases. Nevertheless, the writers did not explain how blockchain was used in the proposed methodology, and no performance evaluation of blockchain, fog, or cloud services was done.

A mixed edge blockchain-driven eHealth structure is utilized by Akkaoui et al. [108]. Four layers make up the structure: end users, border pool, worldwide blockchain, off-chain memory. The concept is similar to that proposed in Ref. [146] to run mining processes on edge to improve performance and transactional processing delay. The edge comprises many devices that verify the legitimacy of opera-

tions and categorize them as normal or not relevant. Ethereum stores blocks containing EMR metadata and body area sensor data while [146] runs a mining system on the edge network and stores blocks consisting of metadata on edge [108]. It used a second blockchain to speed up the production of blocks. In addition, the writers [108] have created many smart contracts to provide role-based patient data sharing.

Neto et al. [148] proposed blockchain as a study topic for applications that change DNA sequence data. A blockchain-driven architecture for generic e-health applications has been presented as a solution. They also developed a proof of concept using DNA sequence data to investigate the blockchain applicability in e-health applications and a research map. Finally, Neto et al. [149] described the use of blockchain in an e-health, which included a performance analysis of transaction validation times using the distributed database BigchainDB.

Chendeb et al. [150] built and adapted a multi-layer IoT/blockchain-driven architecture for medical applications. Doctors, healthcare providers, insurance firms, and pharmacies are just a few of the people who deal with this information. The design concepts are essential to correctly manage the raw data streams provided by a distributed blockchain using cloud architecture. The suggested architecture has high availability, resilience, real-time data transmission and low latency.

4 Research Gaps and Potential Solutions

Although the combination of blockchain with IoT opens up a flood of new business opportunities, there are still a few roadblocks to overcome before the full promise of Blockchain of Things (BCoT) can be achieved. We identify several main problems in integrating blockchain into IoT in this article, describe the current state-of-the-art and offer solutions.

4.1 Resource Constraints

The bulk of devices is resource-constrained. Computational capabilities, storage, battery, and network connectivity are all constrained in sensors and RFID tags, for example. Passive RFID tags, for example, have no batteries and rely on RFID readers or the ambient environment for energy [151]. On the other hand, General Blockchain necessitates significant computer power, bandwidth, and speed. For example, most blockchain systems use Proof of Work (PoW) as their primary consensus mechanism. However, PoW mining requires a substantial amount of computing power. In addition, Bitcoin's PoW, for example, has been discovered to require a significant amount of energy [152]. As a result, low-power IoT devices may not use energy-intensive consensus methods.

Most IoT devices have limited computing power and precise hardware specification. As a result, IoT devices cannot perform blockchain mining tasks because they are insufficiently capable or time-consuming. Aside from that, blockchain requires data encryption regularly. Since different IoT devices have diverse computational capabilities, encryption performance and time may differ. Furthermore, additional procedures such as consistency algorithms and frequent testing necessitate a large amount of CPU power, which is incompatible with the low battery capacity of IoT devices.

In addition, because of the vast bulk of blockchain data, widespread adoption of blockchains in the IoT is not possible. As time goes on, the ledger will grow. On the other hand, most devices have limited physical storage. Low-power IoT typically have 10 to 100 KB of memory for data and memory storage. However, storing the entire chain on a blockchain necessitates a significant storage space. Bitcoin, for example, necessitates more than 200 GB of memory, but Ethereum necessitates over 1.5T. The storage of a copy of blockchain for IoT components is not conceivable. Blockchain will be too large for each IoT device to keep.

Large volumes of data captured in near real-time exacerbate the dilemma. Furthermore, blockchains are architected for a situation with a constant network connectivity, which may not be achievable in IoT, which commonly suffers from poor network connectivity and an unpredictable network due to device failure (e.g., battery depletion). Data is constantly sent from IoT devices and the IoT system requires real-time response [153]. Due to its extensive cryptography protection system and validation procedures, blockchain systems are restricted and they lacks the ability of real-time. A big quantity of data is required for the fast coordination of fresh blocks between blockchain servers in a chain-structured database, which can boost blockchain performance [154, 155]. Furthermore, IoT devices are anticipated to be linked to high computational, memory, and network capabilities to exchange IoT data with prospective partners. As a result, the challenge is to improve overall efficiency of blockchain to fulfill the demand for real-time requirements in IoT systems.

Furthermore, to reach to an agreement on how to keep blockchain correct and generate new blocks, the consensus process in blockchain requires constant information sharing between nodes. This approach needs bandwidth and a minimum network latency. The bandwidth requirements for IoT devices, on the other hand, are always strict.

Using edge computing and cloud computing technologies in conjunction with Blockchain of Things could enable IoT devices to overcome resource constraints. For instance, cloud or some edge servers may act as a primary node, storing all data and participating in most operations like initiating and validating transactions (i.e., mining). In contrast, devices can act as lightweight nodes to store only a portion of data (e.g.,

hash value of blockchain data) and performing less computationally intensive tasks (e.g., initiating transactions) [156]. The orchestration of edge and cloud becomes a crucial challenge in resource allocation in BCoT [157].

4.2 Handling Big Data in Blockchain

Every user in blockchain network contains an access to the personal minor ledger. A new block is appended and broadcasted across the entire P2P network. All the hierarchical servers updates the local records based on the local record. This type of distributed system can help to get performance, remove bottlenecks, and reduce the demand for third-party credibility [158], IoT systems can be a threat to the memory capacity of a member in the P2P network. For instance, if 1000 users trade a single MB image every day in blockchain system, the analysis in Ref. [158] estimated that a blockchain server would require around 730 GB of file storage annually. As a result, when it comes to blockchain and IoT data, one of the challenges is to respond to the growing digital storage demands.

Crypto-currencies have been the most successful implementation of Blockchain, to complete transactions with minor charges for third party support. On the other hand, eHealth differ from crypto-currencies in terms of storage needs [159]. Health data is continuously streamed in a patient monitoring system, and transactions are created more often. Blockchain topology makes storing all health data on blockchain challenging for patients. In Ref. [160], the Patient Agent was given the ability to determine quick repositories for each data block based on its characteristics and privacy needs to overcome these challenges. The distributed ledger stores data blocks that require blockchain-driven secure storage. For instance, billing records, healthcare professional notes, and drug summaries can all be analyzed and kept in ledger.

A plethora of archives for records have emerged in the healthcare recently. Examples are government-managed EHRs, healthcare provider-managed EMRs, patient-managed Personal Health Records (PHRs), and current blockchain-driven systems handled mainly through technology. Repositories differ in security and quality. Depending on circumstances, the sensitivity and value of the health data contained in archives differ greatly from patient to patient. It isn't easy to know which digital record store is optimal for preserving entire datasets. Wearable device health data is collected on a continuous basis. Because of the usage of technology, the issues are magnified. This effort was aided by the writers [160]. They allowed the Patient-Centric Agent to be utilized in machine learning-based applications and a storage model for data including suggestions.

As a result, you can make decisions fast, even while using real-time data. The model is divided into two parts: an upper part deals with input processing and algorithms to create dataset for training, and the lower half deals with ML models. The upper component of the model receives input from a variety of data blocks with various features. Several procedures are used to decide the repository for each data block, including correlation coefficient analysis, distance measures, heuristics rules and user preferences.

4.3 Data Analysis in Blockchain and Edge Computing

Large volumes of data are being created in near real-time. IoT data is vast in volume, varied in nature, and valuable in business. Big Data Analytics (BDA) may extract hidden information from IoT data and make intelligent decisions. On the other hand, traditional BDA methodologies are challenging to implement in blockchain of Things because of two factors: (1) Traditional BDA systems cannot be used with devices due to resource constraints. In addition, complex BDA methods cannot be built directly on IoT due to their limited computational capabilities.

Furthermore, keeping it locally on IoT devices is impractical due to the vast amount of blockchain data. Although cloud can help with challenges for data upload including privacy breach and latency [161]; the execution of algorithms for the data analysis on any block chain network as anonymous peer node will be difficult. Blockchain can address privacy by encrypting and digitally signing data records. Performing data analytics, on the other hand, frequently necessitates data decryption. Despite this, the decryption process often takes time, resulting in inefficient data analytics [162]. Without the decryption parameter, it is very tough to identify any means of data analysis on the data present in the block chain.

Edge computing can complement cloud computing by bringing computation from the cloud to the edge, which is closer to the customers. In addition, edge computing can increase reaction time, privacy protection, and context awareness compared to cloud computing. As a result, outsourcing BDA functions to edge servers can address the problem of cloud computing privacy leakage and long latency [163]. For the data analytics over the blockchain applications, there have been some significant advancements:

1. Complicated community detection over network [164] to identify many addresses for the same user.
2. Feature extraction of Bitcoin data transaction patterns to identify relationships [165].
3. Analysis of Ethereum user accounts & codes to detect fraud.

4.4 Scalability

Blockchains are also not extensively used in large-scale IoT due to their scalability. Transactions per second can be a unit

for measuring the scalability. A plot between transactions per second vs. a number of IoT devices and workloads was made [127, 166]. Unfortunately, many blockchain systems have difficulty with throughput. As an example, Bitcoin process seven transactions per second, according to the authors in [167]. On the other hand, VISA can manage 2,000+ transactions/second, while PayPal can handle nearly 170 [168, 169]. Therefore, due to its lack of scalability, the Bitcoin may not be suited for IoT according to reference [170]. In conclusion, existing Blockchain may not be sufficient for high-volume transaction applications such as IoT.

Two approaches to improving blockchain scalability in IoT are possible: 1) developing scalable consensus algorithms and 2) creating private or consortium blockchain for devices. First, to boost transaction throughput, we can employ the consensus-localization technique. Meanwhile, new blockchain structures such as Directed Acyclic Graph [171] may be built that permits non-conflicting blocks to be linked with the primary chain, reducing the bifurcation resolution cost. Alternatively, one may combine PoW with Practical Byzantine Fault Tolerance (PBFT) [172] to boost PoW performance, similar to the Sharing Protocol described in [173], in which a puzzle was handled completely in POW, and then consensus is established in numerous small groups.

The transactions which are taking place into the private block chain can complete faster in comparison to the public block chain transactions due to the full controlled access to limited users. Private blockchain make forming an agreement simple. Furthermore, completely regulated blockchain meets the need for an organization to have complete control over several critical sectors [127, 133]. Despite some efforts (such as Hyperledger,[1] GemOS,[2] and Multichain[3]), more mature consortium blockchain platforms serving specific sectors are envisaged.

4.5 Adaptability

There is a significant rise in the devices and applications used by these devices. As a result, one of the challenges for the integrated blockchain and edge is to deal with increasing number of user as well as the tasks of varying complexities, as well as the ability to adapt in the environment that allows various applications or IoT devices to connect to or leave blockchain network freely.

Tt is very difficult to acquire and achieve a high scalability in a block chain network, which is fully decentralized and highly secure. As per Vitalik Buterin, it is really impossible to achieve such high level of scalability. In contrast to the fact, IoT devices are more easily accessible and data can be fetched from these devices with ease, as compared to a secure decentralized block chain network. As a general fact, the IoT devices connect to the network on and off at various intervals of time. For example, PBFT [172] consensus method is well suited to IoT systems. In contrast, the PBFT approach can only be used in a fixed-size network with members who cannot easily change. For managing a number of devices, that isn't scalable.

4.6 Data Reliability

IoT-based edge computing architectures are currently complex, with poor communication security and largely upstream communication pathways. As a result, data integrity and reliability are compromised. These challenges include data loss, malicious data insertion, network overload as well as computing power overload at the central node. For example, devices in homes have access to personal information about our lives and daily routines. This data must be shared with other devices and services to be valuable to us. However, this suggests that the homeowners are at a high risk of being targeted by hackers. In addition, companies and governments that invest in IoT are more vulnerable to data thefts from offshore thieves, competitors, or adversaries. Allowing blockchain to control data access on IoT devices would add an extra layer of security that any malicious agent would have to get around. In addition, it would be safeguarded by some of the most potent encryption standards available.

Traditional data protection measures, such as using a trusted central institution, rely on a centralized approach. Conventional systems are inappropriate for edge computing because the trusted central entity may have single point for failure possibilities. The security of the entire edge computing system is affected if the centralized system's integrity-preserving system is compromised. A blockchain, a decentralized ledger that tracks transactions, is a viable solution. In blockchain, transactions are recorded as blocks, which form a linked list data structure. A hash value is assigned to each newly created block, which joins the previous and current blocks in an irreversible chain. This process is broadcast to all miners, and when the majority of miners return to the agreement, the freshly created block is successfully added. Because all users can confirm the transaction's legality, it's practically impossible to attack unless the attacker has control of majority of the clients, which is a feature of blockchain's decentralized nature. As a result, in edge computing, blockchain is essential for assuring data integrity.

[1] Hyperledger project. https://www.hyperledger.org/.

[2] GemOS: blockchain operating system, https://enterprise.gem.co/.

[3] MultiChain: Open platform for building blockchains, https://www.multichain.com/.

4.7 Incentive Mechanism in Blockchain for IoT

A well-designed incentive structure is a good stimulant for blockchain systems. For example, a miner who completes the computationally tricky task first will be rewarded with a certain amount of Bitcoins. Meanwhile, an Ethereum transaction can be charged a fee (i.e., gas) to compensate miners for contract execution. As a result, when designing incentive mechanisms for blockchain, there are two issues to consider: (1) a fee for proving (or mining) a block and (2) a price for completing a transaction (or a contract).

Designing an organized system for Blockchain of Things that meets the needs of a wide range of applications, on the other hand, is challenging. Digital currency platforms, for example, are in which miners are interested in a digital currency's price. The BTC reward for a produced block, for example, will be half every 210,000 blocks [158]. As a result, miners can be discouraged from contributing to the puzzle's solution due to the lower payout, leading them to seek out alternative blockchain platforms. Therefore, it's critical to understand how to build a reliable digital currency rewarding and publishing mechanism to ensure blockchain systems' integrity.

On the other side, users in consortium blockchain are driven by their integrity and reputation. As a result, in addition to digital currency, reputation credits (similar to the credit score in bank) can be considered as beneficial in personal repudiation systems [174], shareable economic [175], provenance of data [176], and the medical drug supply chain [177]. For example, RepChain [178] is a recent study that creates an incentive structure based on each node's reputation.

4.8 Verifiable Computation

Edge computing administration is a constraint for edge computing, due to dispersed edge devices, their fragmented ownership, and population.

While the decentralized edge computing platform eliminates the need for a centralized administrative center, the issue is establishing decentralized mutual trust among participants. Verifiable computing, for example, permits computation to be offloaded to specific untrustworthy clients while the results remain correct. One of the difficulties with edge computing networks is maintaining verifiability in uploading computational activities to edge computation devices. The computation is outsourced to one or more servers using the computation function or the public key, and the result is provided along with proof to confirm the computation. By incorporating Blockchain, edge computing can be scaled to vast numbers of computations available in devices and third-party services. At the same time, smart contracts in blockchain should ensure efficient computation scheduling and correctness due to the incentive and autonomy of smart contracts.

4.9 Resource Management

Blockchain does not depend on a centralized server to maintain transaction data unlike other systems making use of centralized ledgers. Instead, users of blockchain network record and distribute data blocks. High transaction throughput as well as efficiency can be achieved by blockchain. It also ensures data privacy and integrity.

Deploying blockchain application in the edge devices has various challenges. First, it is because of mining process, which necessitates a large amount of computer processing power and energy from mobile devices to solve the Proof-of-Work (PoW) problem. The edge computing paradigm was created to address the issue, allowing miners to offload their mining work to a service provider making use of an edge computing device. However, efficiently allocating the limited edge computing resources to miners remains a problem.

4.10 Security Vulnerability

Although deploying blockchain at devices can improve security by providing encryption and digital signatures, due to the flaws in edge devices and blockchain systems, security remains a serious concern for BCoT.

On the one hand, edge devices are becoming more popular in industrial settings because of their ease of use and scalability. However, on the other hand, IoT is prone to security weaknesses such as passive eavesdropping [179] and replaying attacks [180] because of open wireless channel. Furthermore, due to resource constraints, traditional heavyweighted encryption algorithms may not be viable for IoT devices [181]. Furthermore, managing keys (which are essential to encryption schemes) in a distributed context is difficult.

Meanwhile, blockchain such as smart contract programming faults [182], have their own security problems. Malevolent users can intercept blockchain communications utilizing the Border Gateway Protocol (BGP) routing mechanism, as proven in [183], resulting in prolonged block broadcasting delays. [184] also shows how a DAO attack exploited smart contract vulnerabilities to steal $50 million in Ethereum.

Security issues in blockchain can be solved by either strengthening IoT system security or addressing loopholes in blockchain. For instance, a collaborative jamming [185] was developed to improve security while requiring no additional hardware for IoT nodes. The work [186] uses key generations in a Long Range (LoRa) IoT network based on the unpredictability of wireless channels. There have also been notable developments in the area of blockchain defect correction. SABRE, for example, is a secure network for blockchain that can protect them against routing assaults,

according to a recent paper by [187]. Furthermore, Corda and Stellar sacrifice smart contract expressiveness for smart contract verifiability [127].

4.11 Regulatory Issues in the IoT

Blockchain's precision and security draw a wide range of applications in economics as well as law. For example, recently, a ransom attack was observed on the private network of New York Times, which was grabbed by the attention of U.S. Congress. A possible solution for such a cyberattack is to deploy a decentralized block chain network. The organization is currently looking on, and effective solution with the help of block chain. Since there are no regulations in the blockchain application management, various underground trading sites like now-defunct Silk [188] resulted in various scandals.

While some blockchain technical aspects like independence, security, and digitization are potential safety options for a variety of IoT applications, these characteristics when coupled provide a series of significant regulatory complexities [172]. For instance, data is continuously recorded in the Distributed Transaction Ledger (DTL) on peer-to-peer system and cannot be erased or updated, according to the immutability function. Furthermore, information cannot be vetted for secrecy before being published on blockchain given the lack of management. Activities taken as a response of running code on a DTL, such as smart agreements, may be illegal. Owing to the obscurity of the DTL, it is difficult to discern the individuals involved in illicit activities exchanges. While blockchain's automated function has numerous benefits, the players responsible for certain behaviors like coding faults and obfuscation remain unclear. Existing IoT legislations are becoming obsolete, particularly with the introduction of emerging competitive technologies like blockchain, and must be updated in order to complete the DTL [158].

Filippi et al. [189] describe blockchain to be a transforming technology from "Code is a law" to "Law is Code". Because of the decentralized nature of blockchain, traditional legislation cannot regulate it. Smart contract, which converts legislation into code can make laws. A smart device can be leveraged to turn directly into a product. Blockchain's agreement Within the knowledge-driven economy, Pokrovskaia et al. [190] stressed the importance of having tax, financial, and societal regulating mechanisms. They stressed the importance of a well-defined regulatory framework for blockchain and fog computing. Effective governance and monitoring are essential for the long-term viability and adaptation of Blockchain. To appropriately control any cyberspace applications, Lessig [191] outlined three methods: law, economic means, and social norms. Combining these three methods allows blockchain-driven IoT applications to be governed appropriately. During the present scenario, there are no rules and regulations that will regulate the block chain applications inside a public or private network. Various IoT driven applications which are collecting data from sensors based devices will be responsible to define certain social norms. The rules will be applied to all the block chain applications so as to control and manage the data flowing through the information channel across these applications. One of the most important feature is to activate the smart contracts in the block chain network. A blockchain smart contract can be used to turn law into a product. Within the knowledge-driven economy, Pokrovskaia et al. [190] stressed the importance of having control mechanisms for tax, finance, and society. They emphasized the importance of a well-designed regulatory framework for blockchain and edge. Effective governance and monitoring are required for Blockchain to be sustainable and adaptable. Lessig [192] outlined four methods for adequately controlling any cyberspace applications: social norms, laws, and economic means. By combining these four methods, blockchain-driven IoT applications may be successfully governed. No legislations are available to handle and manage the blockchain applications. IoT application-oriented smart agents can define the norms for the blockchain applications to cope with tracking and controlling blockchain. It shows how an architecture of IoT and blockchain might specify regulating norms that are now absent in crypto-currencies such as Bitcoin, which has a solid security architecture, but other regulatory mechanisms have yet to be implemented.

Heimdall, a distributed smart contract-based framework described by Batista et al. [193], allows users to regulate access to sensitive data acquired by IoT devices while adhering to GDPR and the General Data Protection Law. User must be able to activate or deprive from any type of access without the intervention of a third party; personal data may or may not be accessible depending on the norms and protocol of the system; and audit the data from being modified to deleted. To do so, create a smart contract which can manage access control, write a protocol that explains the various operations and the activities that go along with them, define access rules, create a distributed system to check access rules.

4.12 To Balance Between Energy Consumption and Security

The enormous computing capacity requires to execute blockchain, which has hindered the development of digital services on top of blockchain platforms, for instance, energy consumption of Bitcoin in a contrast with Ireland's residential electricity usage that the IoT devices cannot acquire [194]. According to Zhou et al. [154], the Bitcoin system consumes far more power than numerous countries. Furthermore, IoT data handling is being challenged by experts in blockchain.

The experts claim that core mechanisms can be optimized to improve the number of verified blocks per second [195]. PoW agreement method for blockchain elimination can be used, for example, cut energy usage and improve results [196]. PoW, on the other hand, protects the blocks from hostile Sybil threats and renders them tamper-proof. The aim is to fine-tune blockchain operations such that safety and reliability must be balanced [197].

Mining blocks on P2P blockchain requires more resources than resource-constrained devices can provide. A blockchain agent (described in Refs. [146, 198]) may handle blockchain actions on behalf of devices when running on cloud and edge. The blockchain agent in Ref. [198] maintains various blockchain for IoT data and performs a consensus process.

Uddin et al. [198] aided in overcoming the difficulties of developing EHR blockchain to enable remote patient monitoring. An agent can be created in this proposal to connect blockchain. It is a software agent with AI models, which runs on a user's device. However, creating a software agent on a smartphone is problematic because these devices may be linked to various sensors. For example, suppose the agent-containing device can be stolen or hacked. In that case, the activities of several IoT devices connected to the Gateway may be disrupted, exposing them to various harmful assaults [199]. As a result, the software agent must run on device or cloud to support distributed environments [200].

The blockchain agent (described in Ref. [198]) has the following functions.

- On the patient's end, provide security and privacy.
- Determine how much data needs to be stored and how secure it needs to be. Some streams, for example, will require storage on blockchain, while others can be archived with less security.
- Manage blockchain service providers. For example inserting in a blockchain by selecting a service provider and picking a miner based on latency, trust, energy consumption, and availability.

Uddin et al. [198] built a system for the monitoring of a patient in a hospital (as shown in Fig. 4), which uses an agent to connect blockchain to IoT devices. The framework's agent is responsible to handle a specific piece of the blockchain, which includes the access control, mining as well as the selection of a minor. The handling of real-time of data is done with the help of several block chain connecting together for managing the privacy. To enhance the protection of the data across this agent oriented architecture, a lightweight communication protocol is used. The application which runs on a patience personal device ensures that the aging process runs on it. The intermediate device between a smart phone and the network of the agent block chain connects the sensor which are located at the body of the patient. The connectivity between the block chain peer nodes with the sensors is managed by the intermediate device. In this work, Java was used in the blockchain to analyze the performance of critical algorithms. The NetBeans IDE analyzed the performance of blockchain over network.

4.13 Balancing Throughput and Concurrency

Because a blockchain depends on a decentralized ledger, the participants must spread blocks over the network to include and synchronize them by executing a validation method. The bandwidth of devices is restricted [5]. However, some of devices at the edge have been found to have enough bandwidth, due to the technology advancements. The bandwidth necessary to run a blockchain, on the other hand, may reach the upper limits of edge servers. To address this issue, an agent [198] don't commit the transactions directly; instead, it organizes a set of transactions into blocks. As a result, many transactions do not move over decentralized network in real time. As a result, incorporating blockchain agent [198] into the eHealth architecture can help to reduce bandwidth requirements. In addition, reduction of the bandwidth consumption can be achieved by the blockchain agent.

In Ref. [198], the agent operates on the patient's hardware and facilitates collaboration among blockchain network and IoT sensors [200]. Due to this, the patient data is usually at stake of the cyberattacks (e.g., denial of service). Ref. [146] suggested a solution to this challenge. Ref. [146] decentralized the blockchain agent by replicating it at the smartphone level. This is achieved with the placement of the Body Area Sensor Networks, at the processing fog layer and the far processing takes place at the cloud layer. The fuzzy inference method was used to create a lightweight modified PoS consensus system for blockchain to process patient records quickly. At fog and cloud, the consensus mechanism to process data was incorporated.

They are replicating the blockchain Agent in Refs. [146] at three levels allows patients' responsibilities to be outsourced to edge and cloud nodes while maintaining privacy. The method of decentralization for the patient agent data in eHealth design ensures software longevity. It also preserves the secure storage of medical data without third-party trusted authorities. The near processing layer consists of edge devices, which is the next level of the sensing layer. The suitable component, which comprises numerous cloud service providers, enables blockchain to handle and store large amounts of data. The iFogSim was used to model a decentralized eHealth framework. Java was used to implement a consensus mechanism and an algorithm that preserves privacy in task migration. To measure the energy usage and block generation, the performance of essential algorithms was examined. Scyther [183, 198] was used to test the security systems' strength and resilience against significant

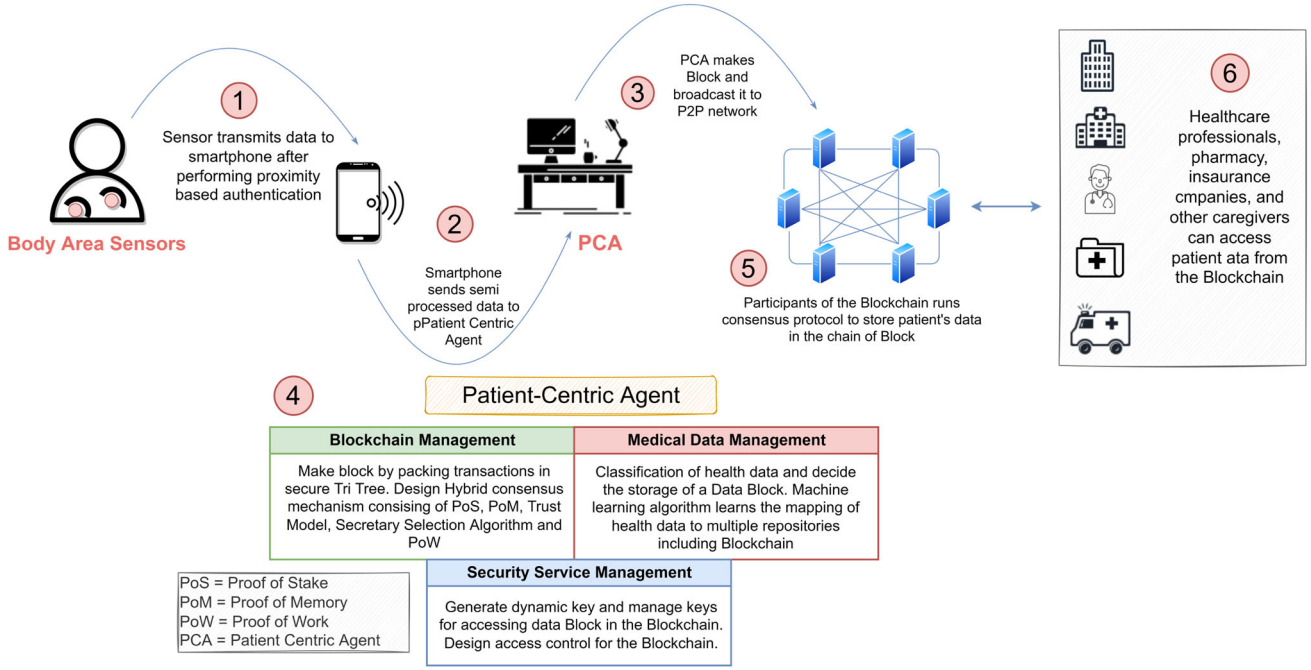

Fig. 4 Basic operations in blockchain of things for Healthcare (image credit to the work [56])

cyberattacks. Finally, the proposed frameworks were compared to other existing methods in terms of several metrics to illustrate the practicality of the methodology in eHealth monitoring.

4.14 Maintaining Both Transparency and Privacy

Critical industries like banking requires the transaction openness. Blockchain is a suitable solution to achieve this. However, while fetching data from the IoT platforms, like eHealth that are enabled with blockchain, there are chances for the customer privacy compromise [158]. Since the blockchain data is decentralized in nature and is replicated in various nodes, information processing may lead to data leak or breach. Homomorphic encryption technology in association with blockchain architecture can be a probable solution to preserve user data [201]. Homomorphic encryption technique handles user data without decryption, while addressing data privacy concerns. In a decentralized approach, the combination of homomorphic encryption with blockchain-driven eHealth can address a privacy challenge [201]. Therefore, a scheme using homomorphic encryption is need to be developed.

COVID-19's current worldwide health issue necessitates tracking patients without a centralized entity, tamper-proof data exchange, and ensuring privacy while collecting COVID-19 data. To address COVID-19 issues, blockchain can be highly beneficial. The use of federated AI and learning in blockchain [192, 202, 203] can enable data collection and share user information while addressing privacy concerns.

5 Conclusion and Future Research

The combination of blockchain with IoT establishes a new paradigm for edge-IoT networks, which reshapes and changes them to allow new emerging applications in various fields such as healthcare. Several obstacles to implementing blockchain technology in the IoT area are noted in this review article, and it discusses how these obstacles are being overcome. Examining existing blockchain and Internet of Things (IoT) articles in relation to several aspects reveals both their strengths and weaknesses. Because BCoT has received so much interest from academia and business, other technologies will probably have an impact on its evolution. Future services and applications may have access to a variety of opportunities due to the confluence of BCoT and these technologies. In order to empower both worlds, we will provide future research directions for integrating BCoT in such technologies and share insights on these technologies in this area.

5.1 BCoT and machine Learning

Future BCoT's key goal is to offer ubiquity in IoT services while enhancing system performance and security to keep up with the rising demands of user traffic and new services in future networks, such as 5 G and beyond. It is impera-

tive to develop solutions for crucial BCoT network problems such resource scheduling, system management, and networking optimization if we are to meet these objectives. The majority of present-day solutions, however, are built on centralized designs or conventional optimization techniques, which presents some significant difficulties [167]. The data explosion which is expected to occur with the immense amount of data streaming through the IOT devices to the blockchain network may render the conventional method of data analytics and processing ineffective. It is also expected that the data streams at a very faster rate, which might provide latency issues due to the high rate of dynamics. Machine learning has been a highly effective approach to addressing these issues and helping future BCoT. The use of machine learning is very pronounced and accepted across a wide range of applications globally. Whether it is computer vision, recognition of speech, diagnosis of medical images, etc., the use of machine learning empowers the application by enabling artificial intelligence in machines to take effective decisions. Supervise and non-supervisory learning parameters are really responsible for providing intelligence to the machines, for taking their own decisions. Data training model to learn from these inputs, and deliver profound results is indeed one of the key features, which is responsible to provide enhanced network performances in machine learning technology. It is also expected that the use of machine learning will be able to revolutionize the present BCoT services.

5.2 In 5 G Networks and Beyond: BCoT

The unfathomable level of innovation offered by the next mobile network generations (5 G and beyond), along with some key benefits like high data rates, low network latency, energy savings, lower operating costs, higher system throughput, and widespread device connectivity, has completely changed industry and society. However, use of computing paradigms like 5 G, SDN, cloud computing and D2D communications can be very susceptible to security and privacy concerns of an individual user [120]. For instance, there are still significant security concerns with SDN, including forged or simulated traffic, control plane, and controller vulnerabilities, and a lack of trust-based protocols between the applications [121]. Additionally, it's still unclear how to ensure between the service provider and the user to reduce the danger of data leakage during resource sharing between NFV clients and servers [122]. In such situations, the blockchain can offer workable security solutions. For instance, SDN implementation for the decentralized authorization using the smart contracts make use of blockchain to establish decentralized authentication methods [123]. Blockchain can also increase trust between network elements, such as SDN controllers and network users, by utilizing shared ledgers, allowing for dependable interactions and safe data exchange. Blockchain technology in NFV can protect system integrity from data risks, such as malicious VM alterations and data attacks, and secure the delivery of network functions [132]. The network slicing idea, which enables different tenants to share the same physical gear, is another component of 5 G that is necessary to support upcoming IoT applications. Inter-slice security vulnerabilities still exist with the network slicing procedure, though. For example, by taking advantage of information stored on the block corresponding to a target sliced user or domain [130].

Blockchain network is also expected to provide end-to-end networks slices, which creates dependable resources for the supplier. There will be a full control with the help of such a mechanism. [134]. Slice requests are submitted to the blockchain network using smart contracts for authentication. This allows resource providers to trade resources on contracts that include sub-slice components, and it also allows for the immutable recording and storage of sub-slice deployment information on the blockchain. Blockchain is able to foster confidence among all the D2D users and guarantee open and trustworthy data exchange between various users in 5 G networks [136]. Resourceful devices as laptops, servers or smartphones can be used for engaging mining of data at the blockchain servers. However, the lightweight devices involved in the D2D transactions are only for the use of services. These devices are only communicating for services and do not contribute to the mining of blockchain data [131].

References

1. Özyılmaz, K.R.; Yurdakul, A: Work-in-progress: integrating low-power IOT devices to a blockchain-based infrastructure. In: 2017 International Conference on Embedded Software (EMSOFT), pp. 1–2. IEEE (2017)
2. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H.: Blockchain technologies for the internet of things: research issues and challenges. IEEE Internet Things J. **6**(2), 2188–2204 (2019)
3. 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)
4. 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)
5. Dai, H.-N.; Zheng, Z.; Zhang, Y.: Blockchain for internet of things: a survey. IEEE Internet Things J. **6**(5), 8076–8094 (2019)
6. Mingli, W.; Wang, K.; Cai, X.; Guo, S.; Guo, M.; Rong, C.: A comprehensive survey of blockchain: From theory to IoT applications and beyond. IEEE Internet Things J. **6**(5), 8114–8154 (2019)
7. Park, J.H.; Park, J.H.: Blockchain security in cloud computing: use cases, challenges, and solutions. Symmetry **9**(8), 164 (2017)
8. Uriarte, R.B.; DeNicola, R.: Blockchain-based decentralized cloud/fog solutions: challenges, opportunities, and standards. IEEE Commun. Stand. Mag. **2**(3), 22–28 (2018)
9. Yang, R.; Richard Yu, F.; SI, P.; Yang, Z.; Zhang, Y.: Integrated blockchain and edge computing systems: a survey, some research

issues and challenges. IEEE Commun. Surv. Tutor. **21**(2), 1508–1532 (2019)
10. Qureshi, J.N.; Farooq, M.S.; Abid, A.; Umer, T.; Bashir, A.K.; Zikria, Y.B.: Blockchain applications for the internet of things: systematic review and challenges. Microprocess. Microsyst. **94**, 104632 (2022)
11. Amanat, A.; Rizwan, M.; Maple, C.; Zikria, Y.B.; Almadhor, A.S.; Kim, S.W: Blockchain and cloud computing-based secure electronic healthcare records storage and sharing. *Front. Public Health*, pp. 2309 (2022)
12. Javed, A.R.; Shahzad, F.; ur Rehman, S.; Zikria, Y.B.; Razzak, I.; Jalil, Z.; Guandong, X.: Future smart cities: requirements, emerging technologies, applications, challenges, and future aspects. Cities **129**, 103794 (2022)
13. Alam, S.; Shuaib, M.; Khan, W.Z.; Garg, S.; Kaddoum, G.; Shamim Hossain, M.; Zikria, Y.B.: Blockchain-based initiatives: current state and challenges. Comput. Netw. **198**, 108395 (2021)
14. Shahzad, I.; Maqbool, A.; Rana, T.; Mirza, A.; Khan, W.Z.; Kim, S.W.; Zikria, Y.B.; Din, S.: Blockchain-based green big data visualization: BGbV. Complex Intell. Syst. **8**(5), 3707–3718 (2022)
15. Ali, R.; Qadri, Y.A.; Zikria, Y.B.; Al-Turjman, F.; Kim, B.-S.; Kim, S.W.: A blockchain model for trustworthiness in the internet of things (IoT)-based smart-cities. Trends in cloud-based IoT, pp. 1–19 (2020)
16. Qadri, Y.A.; Nauman, A.; Zikria, Y.B.; Vasilakos, A.V.; Kim, S.W.: The future of healthcare internet of things: a survey of emerging technologies. IEEE Commun. Surv. Tutor. **22**(2), 1121–1167 (2020)
17. Sengupta, J.; Ruj, S.; Bit, S.D.: A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J. Netw. Comput. Appl. **149**, 102481 (2020)
18. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N.: A survey on privacy protection in blockchain system. J. Netw. Comput. Appl. **126**, 45–58 (2019)
19. Zhu, Q.; Loke, S.W.; Trujillo-Rasua, R.; Jiang, F.; Xiang, Y.: Applications of distributed ledger technologies to the internet of things: a survey. ACM Comput. Surv. (CSUR) **52**(6), 1–34 (2019)
20. Chen, W.; Xu, Z.; Shi, S.; Zhao, Y.; Zhao, J.: A survey of blockchain applications in different domains. In: Proceedings of the 2018 International Conference on Blockchain Technology and Application, pp. 17–21 (2018)
21. Rabah, K.: Challenges and opportunities for blockchain powered healthcare systems: a review. Mara. Res. J. Med. Health Sci. **1**(1), 45–52 (2017)
22. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L.: A systematic review of the use of blockchain in healthcare. Symmetry **10**(10), 470 (2018)
23. McGhin, T.; Raymond Choo, K.-K.; Zhechao Liu, C.; He, D.: Blockchain in healthcare applications: research challenges and opportunities. J. Netw. Comput. Appl. **135**, 62–75 (2019)
24. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.-K.R.: Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. **5**(1), 31–37 (2018)
25. Engelhardt, M.A: Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector. *Technol. Innov. Manag. Rev.*, 7(10) (2017)
26. Zyskind, G.; Nathan, O.; et al.: Decentralizing privacy: using blockchain to protect personal data. In: 2015 IEEE Security and Privacy Workshops, pp. 180–184. IEEE (2015)
27. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. *Decent. Bus. Rev.*, p. 21260 (2008)
28. Curran, B.: What are the trustless environments and how cryptocurrencies create them. Blockonomi. com, 9 (2018)
29. Khatoon, A.; Verma, P.; Southernwood, J.; Massey, B.; Corcoran, P.: Blockchain in energy efficiency: potential applications and benefits. Energies **12**(17), 3317 (2019)
30. Ismail, L.; Materwala, H.: A review of blockchain architecture and consensus protocols: use cases, challenges, and solutions. Symmetry **11**(10), 1198 (2019)
31. Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K.: Where is current research on blockchain technology? A systematic review. PLoS ONE **11**(10), e0163477 (2016)
32. Parker, J.F.: Blockchain technology simplified: the complete guide to blockchain management, mining, trading and investing cryptocurrency. CreateSpace Independent Publishing Platform (2018)
33. Beck, R.; Avital, M.; Rossi, M.; Thatcher, J.B.: Blockchain technology in business and information systems research (2017)
34. Hofmann, E.; Strewe, U.M.; Bosia, N.: Supply Chain Finance and Blockchain Technology: The Case of Reverse Securitisation. Springer, Berlin (2017)
35. Meng, W.; Tischhauser, E.W.; Wang, Q.; Wang, Yu.; Han, J.: When intrusion detection meets blockchain technology: a review. Ieee Access **6**, 10179–10188 (2018)
36. Gipp, B.; Kosti, J.; Breitinger, C.: Securing video integrity using decentralized trusted timestamping on the bitcoin blockchain. In: Mediterranean Conference on Information Systems (MCIS). Association For Information Systems (2016)
37. Benchoufi, M.; Ravaud, P.: Blockchain technology for improving clinical research quality. Trials **18**(1), 1–5 (2017)
38. Angraal, S.; Krumholz, H.M.; Schulz, W.L.: Blockchain technology: applications in health care. Circ. Cardiovasc. Qual. Outcomes **10**(9), e003800 (2017)
39. Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B.: Blockchain technology innovations. In: 2017 IEEE Technology & Engineering Management Conference (TEMSCON), pp. 137–141. IEEE (2017)
40. Ahmed, O.: Block chain technology: Concept of digital economics (2017)
41. Khan, D.; Jung, L.T.; Hashmani, M.A.; Waqas, A.: A critical review of blockchain consensus model. In: 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), pp. 1–6. IEEE (2020)
42. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L.: Blockchain technology and its relationships to sustainable supply chain management. Int. J. Prod. Res. **57**(7), 2117–2135 (2019)
43. Jaikaran, C.: Blockchain: background and policy issues. Congressional Research Service, Washington, DC (2018)
44. Glaser, F.: Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis. (2017)
45. Carson, B.; Romanelli, G.; Walsh, P.; Zhumaev, A.: Blockchain beyond the hype: What is the strategic business value. McKinsey & Company, 1 (2018)
46. Kuo, T.-T.; Kim, H.-E.; Ohno-Machado, L.: Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inform. Assoc. **24**(6), 1211–1220 (2017)
47. Randall, D.; Goel, P.; Abujamra, R.; et al.: Blockchain applications and use cases in health information technology. J. Health Med. Inform. **8**(3), 1–17 (2017)
48. Kshetri, N.: Blockchain and electronic healthcare records [cybertrust]. Computer **51**(12), 59–63 (2018)
49. Bennett, Brennan: Blockchain hie overview: a framework for healthcare interoperability. Telehealth and Medicine Today, 2(3) (2017)
50. Radanović, I.; Likić, R.: Opportunities for use of blockchain technology in medicine. Appl. Health Econ. Health Policy **16**(5), 583–590 (2018)
51. Almalki, J.; Al Shehri, W.; Mehmood, R.; Alsaif, K.; Alshahrani, S.M.; Jannah, N.; Khan, N.A.: Enabling blockchain with IoMT devices for healthcare. Information **13**(10), 448 (2022)

52. Skiba, D.J.; et al.: The potential of blockchain in education and health care. Nurs. Educ. Perspect. **38**(4), 220–221 (2017)
53. Heston, T.: A case study in blockchain healthcare innovation. (2017)
54. Boulos, Kamel; Maged, N.; Wilson, James T.; Clauson, Kevin A.: Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. Int. J. Health Geogr. **17**(1), 1–10 (2018)
55. Ølnes, S.; Ubacht, J.; Janssen, M.: Blockchain in government: benefits and implications of distributed ledger technology for information sharing. Gov. Inform. Quart. **34**(3), 355–364 (2017)
56. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V.: A survey on the adoption of blockchain in IoT: challenges and solutions. Blockchain: Res. Appl. **2**(2), 100006 (2021)
57. Kuo, T.T.; Ohno-Machado, L.: Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. *arXiv preprint* arXiv:1802.01746 (2018)
58. Greenberger, M.: Block what? the unrealized potential of blockchain in healthcare. Nurs. Manage. **50**(5), 9–12 (2019)
59. Stawicki, S.P.; Firstenberg, M.S.; Papadimos, T.J.; et al.: What's new in academic medicine? Blockchain technology in health-care: Bigger, better, fairer, faster, and leaner. Int. J. Acad. Med. **4**(1), 1 (2018)
60. Rejeb, A.; Bell, L.: Potentials of blockchain for healthcare: Case of Tunisia. Available at SSRN 3475246 (2019)
61. Kamran, M.; Khan, H.U.; Nisar, W.; Farooq, M.; Rehman, S.-U.: Blockchain and internet of things: a bibliometric study. Comput. Electr. Eng. **81**, 106525 (2020)
62. Salah, K.; Habib Ur Rehman, M.; Nizamuddin, N.: Blockchain for ai: review and open research challenges. IEEE Access **7**, 10127–10149 (2019)
63. Seyednima Khezr, Md.; Moniruzzaman, A.Y.; Benlamri, R.: Blockchain technology in healthcare: a comprehensive review and directions for future research. Appl. Sci. **9**(9), 1736 (2019)
64. Pham, H.T.; Pathirana, P.N.: Measurement and assessment of hand functionality via a cloud-based implementation. In: International Conference on Smart Homes and Health Telematics, pp. 289–294. Springer (2015)
65. Li, S.; Pathirana, P.N.: Cloud-based non-invasive telerehabilitation exercise monitoring. In: 2014 IEEE Conference on Biomedical Engineering and Sciences (IECBES), pp. 385–390. IEEE (2014)
66. Jamil, F.; Ahmad, S.; Iqbal, N.; Kim, D.-H.: Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. Sensors **20**(8), 2195 (2020)
67. 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), 9711–9733 (2020)
68. Nguyen, D.C.; Nguyen, K.D.; Pathirana, P. N.: A mobile cloud based iomt framework for automated health assessment and management. In: 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 6517–6520. IEEE (2019)
69. Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D.: Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1–5. IEEE (2017)
70. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A.: Blockchain for secure ehrs sharing of mobile cloud based e-health systems. IEEE Access **7**, 66792–66806 (2019)
71. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A.: Privacy-preserved task offloading in mobile blockchain with deep reinforcement learning. IEEE Trans. Netw. Serv. Manage. **17**(4), 2536–2549 (2020)
72. Ni, W.; Huang, X.; Zhang, J.; Yu, R.: Healchain: A decentralized data management system for mobile healthcare using consortium blockchain. In: 2019 Chinese Control Conference (CCC), pp. 6333–6338. IEEE (2019)
73. Ichikawa, D.; Kashiyama, M.; Ueno, T.; et al.: Tamper-resistant mobile health using blockchain technology. JMIR Mhealth Uhealth **5**(7), e7938 (2017)
74. Ampel, B.; Patton, M.; Chen, H.: Performance modeling of hyperledger sawtooth blockchain. In: 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 59–61. IEEE (2019)
75. Celesti, A.; Ruggeri, A.; Fazio, M.; Galletta, A.; Villari, M.; Romano, A.: Blockchain-based healthcare workflow for telemedical laboratory in federated hospital IoT clouds. Sensors **20**(9), 2590 (2020)
76. Haq, I.; Esuka, O.M.: Blockchain technology in pharmaceutical industry to prevent counterfeit drugs. Int. J. Comput. Appl. **180**(25), 8–12 (2018)
77. Celiz, R.C.; De La Cruz, YE; Sanchez, D.M.: Cloud model for purchase management in health sector of peru based on IoT and blockchain. In: 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 328–334. IEEE (2018)
78. Kang, M.; Park, E.; Cho, B.H.; Lee, K.-S.: Recent patient health monitoring platforms incorporating internet of things-enabled smart devices. Int. Neurourol. J. **22**(Suppl 2), S76 (2018)
79. Tanwar, S.; Parekh, K.; Evans, R.: Blockchain-based electronic healthcare record system for healthcare 4.0 applications. J. Inform. Secur. Appl. **50**, 102407 (2020)
80. Xia, Q.; Sifah, E.B.; Smahi, A.; Amofa, S.; Zhang, X.: BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information **8**(2), 44 (2017)
81. Liu, X.; Wang, Z.; Jin, C.; Li, F.; Li, G.: A blockchain-based medical data sharing and protection scheme. IEEE Access **7**, 118943–118953 (2019)
82. Xia, Q.I.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Xiaojiang, D.; Guizani, M.: Medshare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access **5**, 14757–14767 (2017)
83. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R.: A decentralized privacy-preserving healthcare blockchain for IoT. Sensors **19**(2), 326 (2019)
84. Shen, B.; Guo, J.; Yang, Y.: Medchain: Efficient healthcare data sharing via blockchain. Appl. Sci. **9**(6), 1207 (2019)
85. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y.: Medblock: Efficient and secure medical data sharing via blockchain. J. Med. Syst. **42**(8), 1–11 (2018)
86. Hang, L.; Ullah, I.; Kim, D.-H.: A secure fish farm platform based on blockchain for agriculture data integrity. Comput. Electron. Agric. **170**, 105251 (2020)
87. Zhang, Y.; Deng, R.H.; Liu, X.; Zheng, D.: Blockchain based efficient and robust fair payment for outsourcing services in cloud computing. Inf. Sci. **462**, 262–277 (2018)
88. Nass, S.J.; Levit, L.A.; Gostin, L.O.; et al.: The value and importance of health information privacy. In: Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. National Academies Press (US) (2009)
89. Liu, J.; Li, X.; Ye, L.; Zhang, H.; Du, X.; Guizani, M.: BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. In: 2018 IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE (2018)
90. Kaur, H.; Afshar Alam, M.; Jameel, R.; Mourya, A.K.; Chang, V.: A proposed solution and future direction for blockchain-based

heterogeneous medicare data in cloud environment. J. Med. Syst. **42**(8), 1–11 (2018)
91. Al Omar, A.; Bhuiyan, M.Z.A.; Basu, A.; Kiyomoto, S.; Rahman, M.S.: Privacy-friendly platform for healthcare data in cloud based on blockchain environment. Futur. Gener. Comput. Syst. **95**, 511–521 (2019)
92. Rahulamathavan, Y.; Phan, R.C.W.; Rajarajan, M.; Misra, S.; Kondoz, A.: Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In: 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1–6. IEEE (2017)
93. Au, M.H.; Yuen, T.; Liu, J.; Susilo, W.; Huang, X.; Xiang, Y.; Jiang, Z.: A general framework for secure sharing of personal health records in cloud system. J. Comput. Syst. Sci. **90**, 46–62 (2017)
94. Gordon, W.J.; Catalini, C.: Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. Comput. Struct. Biotechnol. J. **16**, 224–230 (2018)
95. Dagher, G.; Mohler, J.; Milojkovic, M.; Marella, P.: Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain. Cities Soc. **39**, 02 (2018)
96. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A.: Medrec: Using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30 (2016)
97. Roehrs, A.; da Costa, C.A.; da Rosa Righi, R.: Omniphr: A distributed architecture model to integrate personal health records. J. Biomed. Inform. **71**, 70–81 (2017)
98. Kahani, N.; Elgazzar, K.; Cordy, J.R.: Authentication and access control in e-health systems in the cloud. In: 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), pp. 13–23. IEEE (2016)
99. Lu, S.; Hong, Y.; Liu, Q.; Wang, L.; Dssouli, R.: Access control in e-health portal systems. In: 2007 Innovations in Information Technologies (IIT), pp. 88–92. IEEE (2007)
100. Wang, S.; Zhang, Y.; Zhang, Y.: A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. Ieee Access **6**, 38437–38450 (2018)
101. Islam, S.M.R.; Hossain, M.; Hasan, R.; Duong, T.Q.: A conceptual framework for an IoT based health assistant and its authorization model. In: 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), pp. 616–621. IEEE (2018)
102. Ramani, V.; Kumar, T.; Bracken, A.; Liyanage, M.; Ylianttila, M.: Secure and efficient data accessibility in blockchain based healthcare systems. In: 2018 IEEE Global Communications Conference (GLOBECOM), pp. 206–212. IEEE (2018)
103. Wang, H.; Song, Y.: Secure cloud-based ehr system using attribute-based cryptosystem and blockchain. J. Med. Syst. **42**(8), 1–9 (2018)
104. Marelli, L.; Lievevrouw, E.; Van Hoyweghen, I.: Fit for purpose? The GDPR and the governance of European digital health. Policy Stud. **41**(5), 447–467 (2020)
105. Zheng, X.; Mukkamala, R.R.; Vatrapu, R.; Ordieres-Mere, J.: Blockchain-based personal health data sharing system using cloud storage. In: 2018 IEEE 20th International Conference on e-health Networking, Applications and Services (Healthcom), pp. 1–6. IEEE (2018)
106. Chen, L.; Lee, W.-K.; Chang, C.-C.; Choo, K.-K.R.; Zhang, N.: Blockchain based searchable encryption for electronic health record sharing. Futur. Gener. Comput. Syst. **95**, 420–429 (2019)
107. Islam, N.; Faheem, Y.; Din, I.U.; Talha, M.; Guizani, M.; Khalil, M.: A blockchain-based fog computing framework for activity recognition as an application to e-healthcare services. Futur. Gener. Comput. Syst. **100**, 569–578 (2019)
108. Akkaoui, R.; Hei, X.; Cheng, W.: Edgemedichain: A hybrid edge blockchain-based framework for health data exchange. IEEE Access **8**, 113467–113486 (2020)
109. Calvaresi, D.; Dubovitskaya, A.; Calbimonte, J.P.; Taveter, K.; Schumacher, M.: Multi-agent systems and blockchain: Results from a systematic literature review. In: International Conference on Practical Applications of Agents and Multi-agent Systems. pp. 110–126. Springer (2018)
110. Hepp, T.; Sharinghousen, M.; Ehret, P.; Schoenhals, A.; Gipp, B.: On-chain vs. off-chain storage for supply-and blockchain integration. it-Inform. Technol. **60**(5–6), 283–291 (2018)
111. Xu, X.; Weber, I.; Staples, M.; Zhu, L.; Bosch, J.; Bass, L.; Pautasso, C.; Rimba, P.: A taxonomy of blockchain-based systems for architecture design. In: 2017 IEEE International Conference on Software Architecture (ICSA), pp. 243–252. IEEE (2017)
112. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W.: Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. J. Med. Syst. **40**(10), 1–8 (2016)
113. Libing, W.; Zhang, Y.; Xie, Y.; Alelaiwi, A.; Shen, J.: An efficient and secure identity-based authentication and key agreement protocol with user anonymity for mobile devices. Wireless Pers. Commun. **94**, 3371–3387 (2017)
114. Du, Y.; Liu, J.; Guan, Z.; Feng, H.: A medical information service platform based on distributed cloud and blockchain. In: 2018 IEEE International Conference on Smart Cloud (SmartCloud), pp. 34–39. IEEE (2018)
115. Kavosi, Z.; Rahimi, H.; Khanian, S.; Farhadi, P.; Kharazmi, E.: Factors influencing decision making for healthcare services outsourcing: A review and delphi study. Med. J. Islam Repub. Iran **32**, 56 (2018)
116. Skipworth, H.; Delbufalo, E.; Mena, C.: Logistics and procurement outsourcing in the healthcare sector: a comparative analysis. Eur. Manag. J. **38**(3), 518–532 (2020)
117. Zhang, H.; Jia, Yu.; Chengliang Tian, P.; Zhao, G.X.; Lin, J.: Cloud storage for electronic health records based on secret sharing with verifiable reconstruction outsourcing. IEEE Access **6**, 40713–40722 (2018)
118. Cao, S.; Zhang, G.; Liu, P.; Zhang, X.; Neri, F.: Cloud-assisted secure ehealth systems for tamper-proofing ehr via blockchain. Inf. Sci. **485**, 427–440 (2019)
119. Park, J.; Park, S.; Kim, K.; Lee, D.: Corus: Blockchain-based trustworthy evaluation system for efficacy of healthcare remedies. In: 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), pp. 181–184. IEEE (2018)
120. Zhu, S.; Cai, Z.; Huafu, H.; Li, Y.; Li, W.: ZKCROWD: a hybrid blockchain-based crowdsourcing platform. IEEE Trans. Industr. Inf. **16**(6), 4196–4205 (2019)
121. Xiaolong, X.; Liu, Q.; Zhang, X.; Zhang, J.; Qi, L.; Dou, W.: A blockchain-powered crowdsourcing method with privacy preservation in mobile environment. IEEE Trans. Comput. Soc. Syst. **6**(6), 1407–1419 (2019)
122. Li, M.; Weng, J.; Yang, A.; Wei, L.; Zhang, Y.; Hou, L.; Liu, J.-N.; Xiang, Y.; Deng, R.H.: Crowdbc: A blockchain-based decentralized framework for crowdsourcing. IEEE Trans. Parallel Distrib. Syst. **30**(6), 1251–1266 (2018)
123. Macrinici, D.; Cartofeanu, C.; Gao, S.: Smart contract applications within blockchain technology: a systematic mapping study. Telematics Inform. **35**(8), 2337–2354 (2018)
124. Daraghmi, E.-Y.; Daraghmi, Y.-A.; Yuan, S.-M.: Medchain: A design of blockchain-based system for medical records access and permissions management. IEEE Access **7**, 164595–164613 (2019)
125. Kazmi, H.S.Z.; Nazeer, F.; Mubarak, S.; Hameed, S.; Basharat, A.; Javaid, N.: Trusted remote patient monitoring using blockchain-

based smart contracts. In: International Conference on Broadband and Wireless Computing, Communication and Applications, pp. 765–776. Springer (2019)
126. Hang, L.; Choi, E.; Kim, D.-H.: A novel emr integrity management based on a medical blockchain platform in hospital. Electronics **8**(4), 467 (2019)
127. Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J.: Untangling blockchain: a data processing view of blockchain systems. IEEE Trans. Knowl. Data Eng. **30**(7), 1366–1385 (2018)
128. Malamas, V.; Dasaklis, T.; Kotzanikolaou, P.; Burmester, M.; Katsikas, S.: A forensics-by-design management framework for medical devices based on blockchain. In: 2019 IEEE World Congress on Services (SERVICES), vol. 2642, pp. 35–40. IEEE (2019)
129. Mytis-Gkometh, P.; Drosatos, G.; Efraimidis, P.S.; Kaldoudi, E.: Notarization of knowledge retrieval from biomedical repositories using blockchain technology. In: International Conference on Biomedical and Health Informatics, pp. 69–73. Springer (2017)
130. Ismail, L.; Materwala, H.; Zeadally, S.: Lightweight blockchain for healthcare. IEEE Access **7**, 149935–149951 (2019)
131. Jinhong Yang, Md.; Onik, M.H.; Lee, N.-Y.; Ahmed, M.; Kim, C.-S.: Proof-of-familiarity: a privacy-preserved blockchain scheme for collaborative medical decision-making. Appl. Sci. **9**(7), 1370 (2019)
132. Liu, Y.; Wang, K.; Lin, Y.; Wenyao, X.: LightChain: A lightweight blockchain system for industrial internet of things. IEEE Trans. Industr. Inf. **15**(6), 3571–3581 (2019)
133. Esposito, C.; Castiglione, A.; Martini, B.; Choo, K.-K.R.: Cloud manufacturing: security, privacy, and forensic concerns. IEEE Cloud Comput. **3**(4), 16–22 (2016)
134. Srivastava, G.; Crichigno, J.; Dhar, S.: A light and secure healthcare blockchain for IoT medical devices. In: 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), pp. 1–5. IEEE (2019)
135. 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 (2020)
136. Attia, O.; Khoufi, I.; Laouiti, A.; Adjih, C.: An IoT-blockchain architecture based on hyperledger framework for health care monitoring application. In: NTMS 2019-10th IFIP International Conference on New Technologies, Mobility and Security, pp. 1–5. IEEE Computer Society (2019)
137. Srivastava, G.; Dwivedi, A.D.; Singh, R.: Automated remote patient monitoring: Data sharing and privacy using blockchain. *arXiv preprint* arXiv:1811.03417 (2018)
138. Li, H.; Tian, H.; Zhang, F.; He, J.: Blockchain-based searchable symmetric encryption scheme. Comput. Electr. Eng. **73**, 32–45 (2019)
139. Hu, S.; Cai, C.; Wang, Q.; Wang, C.; Luo, X.; Ren, K.: Searching an encrypted cloud meets blockchain: a decentralized, reliable and fair realization. In: IEEE INFOCOM 2018-IEEE Conference on Computer Communications, pp. 792–800. IEEE (2018)
140. Wang, Y.; Zhang, A.; Zhang, P.; Wang, H.: Cloud-assisted ehr sharing with security and privacy preservation via consortium blockchain. IEEE Access **7**, 136704–136719 (2019)
141. Yang, X.; Li, T.; Liu, R.; Wang, M.: Blockchain-based secure and searchable ehr sharing scheme. In: 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), pp. 822–8223. IEEE (2019)
142. Noh, S.-W.; Park, Y.; Sur, C.; Shin, S.-U.; Rhee, K.-H.: Blockchain-based user-centric records management system. Int. J. Control Autom. **10**(11), 133–144 (2017)
143. Yüksel, B.; Küpçü, A.; Özkasap, Ö.: Research issues for privacy and security of electronic health services. Futur. Gener. Comput. Syst. **68**, 1–13 (2017)
144. Khan, S.I.; Hoque, A.S.L.: Privacy and security problems of national health data warehouse: a convenient solution for developing countries. In: 2016 International Conference on Networking Systems and Security (NSysS), pp. 1–6. IEEE (2016)
145. Suzuki, S.; Murai, J.: Blockchain as an audit-able communication channel. pp. 516–522, 07 (2017)
146. Jin, H.; Luo, Y.; Li, P.; Mathew, J.: A review of secure and privacy-preserving medical data sharing. IEEE Access **7**, 61656–61669 (2019)
147. Mutlag, A.A.; Abd Ghani, M.K.; Arunkumar, N.; Mohammed, M.A.; Mohd, O.: Enabling technologies for fog computing in healthcare IoT systems. Futur. Gener. Comput. Syst. **90**, 62–78 (2019)
148. Neto, M.M.; Marinho, C.S.S.; Coutinho, E.F.; Moreira, L.O.; Machado, J.C. de; Souza, José N. de: Research opportunities for e-health applications with DNA sequence data using blockchain technology. In: 2020 IEEE International Conference on Software Architecture Companion (ICSA-C), pp. 95–102 (2020)
149. Moreira Neto, M.; Coutinho, E.F.; Moreira, L.O.; Souza, J.N. de: Toward blockchain technology in iot applications: An analysis for e-health applications. In: IFIP International Internet of Things Conference, pp. 36–50. Springer (2019)
150. Chendeb, N.; Khaled, N.; Agoulmine, N.: Integrating blockchain with IoT for a secure healthcare digital system. In: 8th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE 2020), pp. 1–8 (2020)
151. Xiao, L.; Niyato, D.; Jiang, H.; Kim, D.I.; Xiao, Y.; Han, Z.: Ambient backscatter assisted wireless powered communications. IEEE Wirel. Commun. **25**(2), 170–177 (2018)
152. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M.: On blockchain and its integration with IoT. Challenges and opportunities. Futur. Gener. Comput. Syst. **88**, 173–190 (2018)
153. Sharma, P.K.; Kumar, N.; Park, J.H.: Blockchain technology toward green IoT: Opportunities and challenges. IEEE Network **34**(4), 263–269 (2020)
154. Zhou, Q.; Huang, H.; Zheng, Z.; Bian, J.: Solutions to scalability of blockchain: a survey. Ieee Access **8**, 16440–16455 (2020)
155. Dwivedi, A.D.; Malina, L.; Dzurenda, P.; Srivastava, G.: Optimized blockchain model for internet of things based healthcare applications. In: 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), pp. 135–139. IEEE (2019)
156. Yueyue Dai, D.X.; 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)
157. Tran, T.X.; Hajisami, A.; Pandey, P.; Pompili, D.: Collaborative mobile edge computing in 5g networks: new paradigms, scenarios, and challenges. IEEE Commun. Mag. **55**(4), 54–61 (2017)
158. Saito, K.; Iwamura, M.: How to make a digital currency on a blockchain stable. Futur. Gener. Comput. Syst. **100**, 58–69 (2019)
159. Krishnan, S.; Emilia Balas, V.; Golden, J.; Harold Robinson, Y.; Balaji, S.; Kumar, R.: Handbook of Research on Blockchain Technology. Academic Press, Cambridge (2020)
160. Ashraf Uddin, Md.; Stranieri, A.; Gondal, I.; Balasubramanian, V.: Dynamically recommending repositories for health data: a machine learning model. In: Proceedings of the Australasian Computer Science Week Multiconference, pp. 1–10 (2020)
161. Wang, P.; Gao, R.X.; Fan, Z.: Cloud computing for cloud manufacturing: benefits and limitations. J. Manuf. Sci. Eng. **137**(4), 040901 (2015)
162. Wang, N.; Xiao, X.; Yang, Y.; Hoang, T.D.; Shin, H.; Shin, J.; Yu, G.: Privtrie: Effective frequent term discovery under local differential privacy. In: 2018 IEEE 34th International Conference on Data Engineering (ICDE), pp. 821–832 (2018)

163. Yueyue Dai, D.X.; Maharjan, S.; Chen, Z.; He, Q.; Zhang, Y.: Blockchain and deep reinforcement learning empowered intelligent 5g beyond. IEEE Netw. **33**(3), 10–17 (2019)
164. Remy, C.; Rym, B.; Matthieu, L.: Tracking bitcoin users activity using community detection on a network of weak signals. In: International conference on complex networks and their applications, pp. 166–177. Springer (2017)
165. Tasca, P.; Hayes, A.; Liu, S.: The evolution of the bitcoin economy: extracting and analyzing the network of payment relationships. J. Risk Financ. **19**(2), 94–126 (2018)
166. Dinh, T.T.A.; Wang, J.; Chen, G.; Liu, R.; Ooi, B.C.; Tan, K.L.: Blockbench: A framework for analyzing private blockchains. In: Proceedings of the 2017 ACM International Conference on Management of Data, pp. 1085–1100 (2017)
167. Croman, K.; Decker, C.; Eyal, I.; Gencer, A.E.; Juels, A.; Kosba, A.; Miller, A.; Saxena, P.; Shi, E.; Gün Sirer, E.; et al.: On scaling decentralized blockchains. In: International Conference on Financial Cryptography and Data Security, pp. 106–125. Springer (2016)
168. Vermeulen, J.: Bitcoin and ethereum vs visa and paypal–transactions per second. My Broadband, 22 (2017)
169. Albrecht, S.; Reichert, S.; Schmid, J.; Strüker, J.; Neumann, Dirk; Fridgen, Gilbert: Dynamics of blockchain implementation-a case study from the energy sector. In: Proceedings of the 51st Hawaii International Conference on System Sciences (2018)
170. Conoscenti, M.; Vetro, A.; De Martin, J.C.: Blockchain for the internet of things: a systematic literature review. In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1–6. IEEE (2016)
171. Lewenberg, Y.; Sompolinsky, Y.; Zohar, A.: Inclusive block chain protocols. In: International Conference on Financial Cryptography and Data Security, pp. 528–547. Springer (2015)
172. Castro, M.; Liskov, B.; et al.: Practical byzantine fault tolerance. OsDI **99**, 173–186 (1999)
173. Luu, L.; Narayanan, V.; Zheng, C.; Baweja, K.; Gilbert, S.; Saxena, P.: A secure sharding protocol for open blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 17–30 (2016)
174. Yasin, A.; Liu, L.: An online identity and smart contract management system. In: 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), vol. 2, pp. 192–198. IEEE (2016)
175. Bogner, A.; Chanson, M.; Meeuw, A.: A decentralised sharing app running a smart contract on the ethereum blockchain. In: Proceedings of the 6th International Conference on the Internet of Things, pp. 177–178 (2016)
176. Liang, X.; Shetty, S.; Tosh, D.; Kamhoua, C.; Kwiat, K.; Njilla, L.: Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In: 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), pp. 468–477. IEEE (2017)
177. Glover, D.G.; Hermans, J.: Improving the traceability of the clinical trial supply chain. (2017)
178. Huang, C.; Wang, Z.; Chen, H.; Qiwei, H.; Zhang, Q.; Wang, W.; Guan, X.: Repchain: a reputation-based secure, fast, and high incentive blockchain system via sharding. IEEE Internet Things J. **8**(6), 4291–4304 (2020)
179. Li, X.; Wang, H.; Dai, H.N.; Wang, Y.; Zhao, Q.: An analytical study on eavesdropping attacks in wireless nets of things. *Mobile Inform. Syst.*, vol. 2016 (2016)
180. Lin, J.; Wei, Yu.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W.: A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J. **4**(5), 1125–1142 (2017)
181. Yang, Y.; Longfei, W.; Yin, G.; Li, L.; Zhao, H.: A survey on security and privacy issues in internet-of-things. IEEE Internet Things J. **4**(5), 1250–1258 (2017)
182. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q.: A survey on the security of blockchain systems. Futur. Gener. Comput. Syst. **107**, 841–853 (2020)
183. Apostolaki, M.; Zohar, A.; Vanbever, L.: Hijacking bitcoin: Routing attacks on cryptocurrencies. In: 2017 IEEE symposium on security and privacy (SP), pp. 375–392. IEEE (2017)
184. Adhami, S.; Giudici, G.; Martinazzi, S.: Why do businesses go crypto? An empirical analysis of initial coin offerings. J. Econ. Bus. **100**, 64–75 (2018)
185. Lin, H.; Wen, H.; Bin, W.; Pan, F.; Liao, R.-F.; Song, H.; Tang, J.; Wang, X.: Cooperative jamming for physical layer security enhancement in internet of things. IEEE Internet Things J. **5**(1), 219–228 (2017)
186. Weitao, X.; Jha, S.; Wen, H.: LoRa-key: secure key generation system for loRa-based network. IEEE Internet Things J. **6**(4), 6404–6416 (2018)
187. Apostolaki, M.; Marti, G.; Müller, J.; Vanbever, L.: Sabre: Protecting bitcoin against routing attacks. *arXiv preprint* arXiv:1808.06254 (2018)
188. Yeoh, P.: Regulatory issues in blockchain technology. *J. Financ. Regul. Compliance* (2017)
189. Hassan, S.; De Filippi, P.: The expansion of algorithmic governance: from code is law to law is code. Field Actions Science Reports. *J. Field Actions*, (Special Issue 17):88–90 (2017)
190. Pokrovskaia, N.N.: Tax, financial and social regulatory mechanisms within the knowledge-driven economy. blockchain algorithms and fog computing for the efficient regulation. In: 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM), pp. 709–712. IEEE (2017)
191. Lessig, L.: The law of the horse: what cyber law might teach. Harv. L. Rev. **113**, 501 (1999)
192. Hard, A.; Rao, K.; Mathews, R.; Ramaswamy, S.; Beaufays, F.; Augenstein, S.; Eichner, H.; Kiddon, C.; Ramage, D.: Federated learning for mobile keyboard prediction. *arXiv preprint* arXiv:1811.03604 (2018)
193. Nascimento Gomes, A.; Coutinho, E.F.: An architecture proposal for e-health data collection and storage based on internet of things and blockchain. In: 9th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE 2021), Proc. of the 9th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE 2021), pp. 29–38, Zaragoza, Spain, February 2021. Rafael Tolosana Calasanz, General Chair and Gabriel Gonzalez-Castañé, TPC Co-Chair and Nazim Agoulmine, Steering Committee Chair.
194. O'Dwyer, K.J.; Malone, D.: Bitcoin mining and its energy footprint. (2014)
195. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A.: Blockchain and IoT integration: a systematic survey. Sensors **18**(8), 2575 (2018)
196. Ashraf Uddin, Md.; Stranieri, A.; Gondal, I.; Balasubramanian, V.: An efficient selective miner consensus protocol in blockchain oriented iot smart monitoring. In: 2019 IEEE International Conference on Industrial Technology (ICIT), pp. 1135–1142. IEEE (2019)
197. Huang, J.; Kong, L.; Chen, G.; Min-You, W.; Liu, X.; Zeng, P.: Towards secure industrial IoT: blockchain system with credit-based consensus mechanism. IEEE Trans. Industr. Inf. **15**(6), 3680–3689 (2019)
198. Ashraf Uddin, Md.; Stranieri, A.; Gondal, I.; Balasubramanian, V.: Continuous patient monitoring with a patient centric agent: a block architecture. IEEE Access **6**, 32700–32726 (2018)
199. Tuli, S.; Tuli, S.; Wander, G.; Wander, P.; Gill, S.S.; Dustdar, S.; Sakellariou, R.; Rana, O.: Next generation technologies for smart

healthcare: challenges, vision, model, trends and future directions. Internet Technol. Lett. **3**(2), e145 (2020)
200. Ashraf Uddin, Md.; Stranieri, A.; Gondal, I.; Balasubramanian, V.: A decentralized patient agent controlled blockchain for remote patient monitoring. In: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 1–8. IEEE (2019)
201. Shrestha, R.; Kim, S.: Integration of IoT with blockchain and homomorphic encryption: challenging issues and opportunities. Adv. Comput. **115**, 293–331 (2019)
202. Xie, J.; Richard Yu, F.; Huang, T.; Xie, R.; Liu, J.; Wang, C.; Liu, Y.: A survey of machine learning techniques applied to software defined networking (SDN): research issues and challenges. IEEE Commun. Surv. Tutor. **21**(1), 393–430 (2018)
203. Chamola, V.; Hassija, V.; Gupta, V.; Guizani, M.: A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, ai, blockchain, and 5g in managing its impact. IEEE Access **8**, 90225–90265 (2020)