Array 14 (2022) 100139

Contents lists available at ScienceDirect

Array

journal homepage: www.sciencedirect.com/journal/array

Blockchain in healthcare and IoT: A systematic literature review

Endale Mitiku Adere

PO Box 25395/1000, Addis Ababa, Ethiopia

ARTICLE INFO

Key terms:
Integrating blockchain and IoT
Data management in blockchain
Blockchain and healthcare
Blockchain and IoT
Blockchain and smart city & drug supply chain management

ABSTRACT

Blockchain technology is a highly regarded technology that possesses a plethora of exciting features. This paper analyzes trends and highlights the potential benefits of blockchain deployment in IoT and healthcare. According to the literature, blockchain technology is mostly utilized for data management operations in healthcare and IoT, specifically to improve data security, which includes data integrity, access control, and privacy preservation. In both areas, six distinct types of data security preservation strategies are applied. Additionally, publications highlight how blockchain and IoT, including health IoT, can be used in an integrative way. Three integration mechanisms were seen to accomplish this goal. These solutions range from fully integrating blockchain into data exchanges between IoT devices to using it solely for metadata storage. The most frequently covered area of IoT is a smart city, where blockchain is utilized to improve real-time data sharing, and electricity trading, and so on. Additionally, it is learned that, despite the numerous benefits of blockchain in healthcare, authors typically use it for drug supply chain management and data management purposes in order to avoid counterfeiting and empower patients with regard to their data, respectively.

1. Introduction

Blockchain technology is a widely lauded technological advancement that is projected to fundamentally revolutionize human activities and relationships [1,2]. As a result, academics, developers, and practitioners have developed an increased level of interest. Thus, numerous platforms, systems, and prototypes are designed. Among the most notable platforms are Bitcoin, Ethereum, and Hyperledger, all of which have influenced various issues of blockchain usage.

With the emergence of Bitcoin, blockchain technology became the cryptocurrency's foundation. Following that, Ethereum reintroduced smart contracts, reshaping the way blockchain is used, resulting in the emergence of varied smart contract-based applications such as crowdfunding and smart property. Subsequently, it expanded to be used in a wide variety of application domains, including industry, healthcare, and supply chain, which is referred to as blockchain 3.0 [3].

This progress is the result of advances in computer and economics principles, most notably peer-to-peer networks, asymmetric cryptography, consensus protocols, decentralized storage, decentralized computing & smart contracts, and incentive systems [4].

This review article discusses the use of blockchain in a single application domain, namely healthcare, as well as other areas where blockchain and IoT are employed simultaneously. This is done with a particular emphasis on smart city and drug supply chain, which are the two most notable applications of blockchain in the IoT and healthcare, respectively.

The application of blockchain technology in an IoT environment is made possible by integrating the two technologies. Accordingly, this review examines numerous ways for integrating blockchain with IoT that can be used in a range of application domains. The integration approaches vary in terms of the role of blockchain in the overall system, the extent to which blockchain is involved in data exchanges between IoT devices, and the degree to which systems place an emphasis on blockchain for service provision. The integration mechanisms discussed in this review are classified broadly based on existing literature observations.

Security is one of the benefits that blockchain can provide to healthcare and the Internet of Things. This benefit covers a variety of topics, including the protection of data, systems, and networks. Data security is a crucial component of data management. Data management is presented in this review as the acquisition, processing, dissemination, retrieval, security, and storage of data. For a variety of reasons, it is necessary to strengthen all data management activities in both healthcare and IoT settings. For example, in healthcare, the absence of unique patient identity, the unavailability of messaging that enables syntactic and semantic interoperability between systems, and the lack of data encoding standards can all be noted as impediments [5]. The existence of a high number of devices that generate heterogeneous data and

E-mail address: eaderea@yahoo.com.

https://doi.org/10.1016/j.array.2022.100139
Received 6 October 2021; Received in revised form 21 January 2022; Accepted 4 March 2022
Available online 12 March 2022

operate in both online and offline modes complicates data management tasks in an IoT context. As a result, a more effective data management method has been required. Several authors have advocated blockchain-based systems as a solution. The usage of blockchain in healthcare and the Internet of Things is discussed in this review.

Both smart city and drug supply chain management face challenges on multiple levels. These problems range from technical concerns, such as the explosion of big data, to economic issues, such as financial loss as a result of product counterfeiting. The following figure (Fig. 1) illustrates the issues and solutions that existed prior to the advent of blockchain.

Recently, blockchain has been used alone or in combination with existing solutions in both smart city and the drug supply chain to address some of the issues. The usage of blockchain for these purposes is motivated by its qualitative characteristics, which include the reliability, robustness, and fault-tolerant capabilities of the systems that can be developed on top of it [6–8]. However, designing blockchain-based systems in both the healthcare and IoT domains presents several challenges. The primary ones that the literatures describe the most include securing the confidentiality, increasing throughput and scalability, limited storage capacity, and a lack of regulatory guidance.

Despite the challenges, various systems and prototypes are being developed in both healthcare and IoT. Along with demonstrating the benefits that blockchain brings to these two domains, this review discusses how it is being used for a variety of applications. As so, the review is organized as follows. Following this introduction, background information on blockchain technology, the Internet of Things, and Health Information Technology (HIT) is provided. Following that, the methodology followed to prepare this review is described. Subsequently the review's result is presented, which includes a full summary of the review's findings. After that, succeeding sections include the review's discussion, open issues, conclusion, and limitations.

1.1. Prior reviews

Despite the fact that blockchain is a relatively new study topic, various literature reviews have been undertaken on the subject in general and on certain application areas in particular. Additionally, there are researches that focus on specific issues within a particular application domain. The reviews that were chosen after meeting the screening criteria outlined in the methodology section are listed below (Table 1).

Hence the reviews are longlisted, it may be necessary to conduct a review of the reviews as a tertiary review to assess the areas addressed and the limitations of the research conducted thus far, identical to what is done by Kitchenham B. et al. [20]. Despite the abundance of reviews, there are still issues that have not been addressed by the prior reviews. It is noted that prior reviews.

a. Shy away from showing the deficiencies of researches that have been creating what [21] call "construct identity fallacy", which can impact knowledge development since they are piling knowledge than building it, as described by Ref. [22].
b. Don't demonstrate the pattern being trending in developing artifacts in specific application areas,
c. Don't enquire about the relative performances of prototypes or systems developed within or across application areas,
d. Somehow they don't indicate how to extend solutions from one application area to the other, which [23] calls "exaptation" and [24] labels it "knowledge brokering" in which analogical reasoning is employed to deploy knowledge from where it is known to where it is unknown.

Additionally, as illustrated in Table 1, there is no review that thoroughly addresses the integration of blockchain and IoT. Furthermore, data management activities are not exhaustively covered. When considering data security in isolation, the authors in Refs. [11,12] addressed it to a degree. However [11], does not go into detail about blockchain-based IoT security solutions. According to the authors, this is because there is a dearth of publications devoted to the actual usage of blockchain, and so the majority of works focus on illustrating the benefits associated with its use. On the other hand [12], discusses security in terms of the purpose for which blockchain is being used and the methods used to address security concerns. While the publication covers a variety

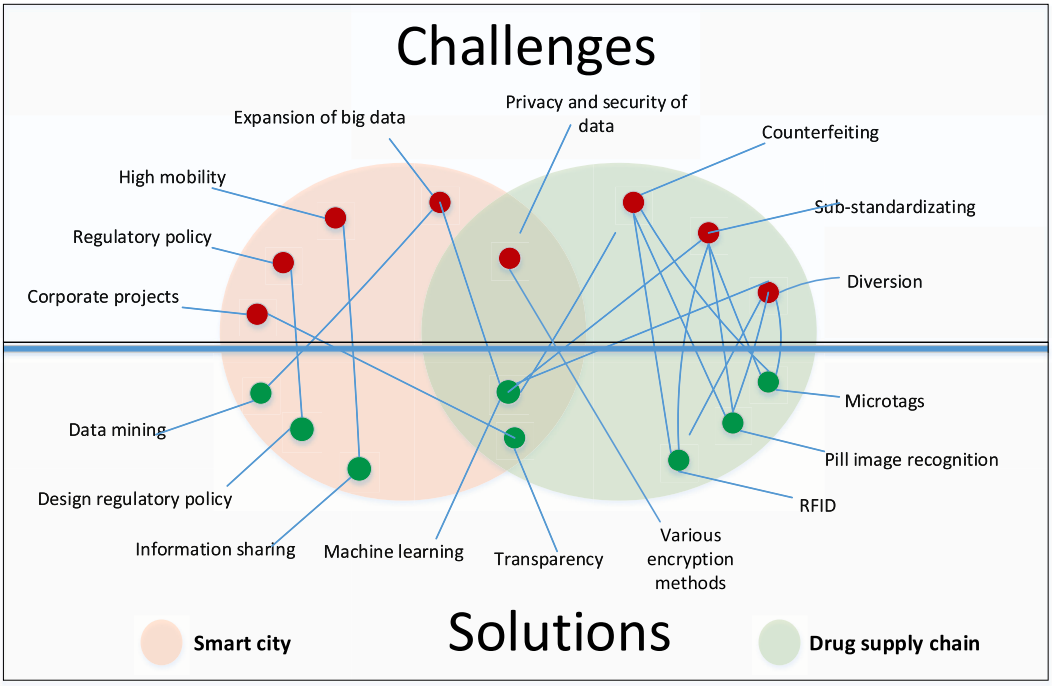

Fig. 1. Some challenges and solutions in smart city and drug supply chain.

Table 1
List of selected prior reviews [9–19].

Author	Issues addressed	Data management	Security	Integration
[9]	Several blockchain projects and startups are mapped based on the activities that they are involved in; furthermore; the potential challenges they have to cope with are also shown.	■	■	■
[10]	Factors that affect integrity, anonymity, and adaptability of blockchain technology usage in some use cases of combined application of blockchain and IoT are explained	■	■	■
[11]	In the IoT environment, security requirements, possible attacks, and solutions by emphasizing the usage of blockchain are presented.	■	■	■
[12]	The major mechanisms employed for maintaining IoT security through the use of blockchain are shown	■	■	■
[13]	Analysis of research on blockchain usage in healthcare, in which the potential areas of applications and possible challenges are highlighted	■	■	■
[14]	The mechanism by which blockchain can be employed for IoT and how blockchain can impact cloud-based IoT usage is presented.	■	■	■
[15]	Demonstrates the focus of blockchain-related research and explains challenges and future directions from a technical point of view.	■	■	■
[16]	Comparison of blockchain platforms that can be employed for biomedicine is made	■	■	■
[17]	Challenges and open issues related to blockchain usage in Electronic Health Record is presented	■	■	■
[18]	The trend in the number of publications on blockchain and the authors' productivity-related issues are shown	Not applicable		
[19]	Classification of blockchain usages and their limitations are shown	■	■	■

Not addressed in the review — Fully addressed in the review

of subjects, it falls short of adequately covering data integrity. As a result, the existence of such gaps motivates this review. Besides, doing this review is necessary to resolve several of the aforementioned shortcomings and to:

1. Describe the trends that have been developing in the development of instantiations.
2. Elaborate how blockchain is being employed for data management, particularly for maintaining data security, access control, and privacy preservation of systems and users.
3. Portray the methods followed to integrate blockchain and IoT for their unified usage.
4. Serve as a foundation for future research that is going to be conducted on the issues covered in the selected application areas

1.2. Contributions

Along with accomplishing the aforementioned objectives, this review contributes to the current literature by filling in certain visible gaps. These include a shortage of comprehensive reviews of the literature on access control and data integrity in blockchain-based systems, as well as a dearth of comprehensive reviews on the integration of blockchain and IoT. Additionally, it contributes to a better knowledge of other issues, such as the privacy-preserving techniques used in blockchain-based systems. The following can be mentioned as significant contributions.

1. The main focus of blockchain research is data management. This review discusses the major data management activities, as well as the techniques employed to improve them.
2. Data security is a critical aspect of data management. In this regard, it is noted that the majority of literatures concentrate on three subjects. These include data integrity, access control, and privacy preservation. This review presents a taxonomy of the methods used in these three areas.
3. During the course of this review, it was discovered that smart city and drug supply chain management are the most highlighted areas in the IoT and healthcare domains, respectively. As a result, the two issues are treated as special issues in this review.
4. Throughout this review, it was discovered that several aspects influence the design of blockchain-based systems. As a result, these factors are specified.

2. Background

This section of the review provides background information on blockchain, IoT, and health information technology (HIT). This includes a discussion of the core components of blockchain, the characteristics of IoT, and HIT.

2.1. Blockchain

There is no widely acknowledged definition of blockchain technology. The once forwarded by various authors thus far imply different topics. For some, such as [11,25,26], blockchain is a distributed digital

ledger. Others, including [27–29], regard it as a data structure and there are also authors for example [30,31] that consider it as a transaction management technology.

The differences arise due to the perspectives from which the authors consider blockchain and the continuous evolution of the technology, which makes it a moving target. As previously presented, blockchain technology has evolved from blockchain 1.0 to blockchain 3.0. The development is made on various aspects particularly those given as the foundations of blockchain in Refs. [32–34] where four distinct concepts are referred to as "fundamentals" in each publication. While concepts are varied, peer-to-peer networks, distributed ledger, consensus mechanism, smart contract, and application area or use can all be considered as critical.

2.1.1. Peer to peer (P2P) network

Essentially, blockchain is a peer-to-peer network. P2P networks have a variety of topologies, communication patterns between nodes, and types of nodes that participate. Predominantly, there are three main categories of network topologies, which are centralized, decentralized structured, and decentralized unstructured [35].

In centralized peer-to-peer networks, a central directory server keeps track of network resources and their addresses. However, in a decentralized structured topology, there is no central directory server, but rather a structure in which selected nodes maintain a Distributed Hash Table (DHT) containing information on the placement of resources is utilized. On the other hand, with a decentralized unstructured topology, there is no central directory server and no file placement guideline dictating the location of data. Rather than that, there is a flexible rule allowing nodes to enter and quit the network freely, and nodes can join the network anonymously. In P2P networks, there are instances where several nodes participate. In these instances, strategies such as clustering are used to make the network manageable. Clustering techniques that are often used include partition-based, density-based, hierarchical-based, and grid-based clustering [36].

The topologies have an effect on the way nodes communicate. After receiving information about the location of data from the directory server, nodes in a centralized P2P network can initiate direct interactions. DHT is maintained at nodes using key and value formats in a decentralized structured topology. The keys are used to denote information about the value, or data. Nodes gain access to data by utilizing the information stored within. In decentralized unstructured networks, communication is accomplished using flooding, gossiping, and random walks, among other techniques. Nodes in this configuration deliver their messages to other nodes at random.

P2P networks can also be characterized as homogeneous or heterogeneous based on the peer types involved. A homogeneous network is defined by nodes that have similar storage, computation, communication, sensing, and energy capabilities. In heterogeneous networks, there is variation in one of the above issues between nodes [37].

As indicated previously, peers can join a decentralized unstructured P2P network freely. In contrast, peers in a centralized P2P network are required to obtain permission. This property of peer-to-peer is inherited by blockchain. Additionally, the governance model is being used to classify blockchains. As a result, blockchain systems can be broadly classified into two classes based on the presence of permission and network governance followed. As per the presence of permission, there are two types, which are permissioned and permissionless. According to governance, there are also two kinds, which are public and private. Comparisons between the two is made in Ref. [38] and the adapted version is depicted in the following table (Table 2).

2.1.2. Distributed ledger

A distributed ledger is made up of blocks that are formed by a group of transactions. To better understand block and transaction, the content of each is presented in the following table (Table 3).

As illustrated above, the Merkle root hash value of transactions and the prior block's hash value are contained in the block header. This ensures the immutability and security of transactions and blocks. The creation of a block is contingent upon the solving of a mathematical puzzle, the difficulty level of which is specified in the block's header. Mining is the process of creating a block. This is accomplished cryptographically by computing a value less than the specified difficulty level. The mining process consumes time and processing power therefore, the participant who solves the puzzle is compensated for the work, after submitting the evidence.

It is worth noting, however, that the content of a block differs between platforms. In Ethereum, for example, in addition to the parent's block hash, the hash of the parent's sibling is included. Additionally, the transactions tree in Ethereum and Parity is formed using the Patricia-Merkle tree, but in Hyperledger, the Bucket-Merkle tree is used [33]. These are done to improve the efficiency of transaction search and updating.

Table 2
Comparison between blockchain governance and permission Source [38].

	Permissioned	Permission-less
Public	• No restriction on data access or transaction • Consensus is limited to some selected nodes	• No restriction on access, transaction, or validation
Private	• Restriction on data access, writing, and validation is prevalent • Participation in consensus is determined by the owner	• There is a restriction on access and who can transact • No restriction on participation in the consensus mechanism

Table 3
The content of a block and a transaction Source [39].

Block header	
Name	Description
Version	Block version number
Hash	The block's hash value
Parent hash	The previous block's hash value
Difficulty	The proof-of-work target difficulty
Timestamp	Creation time of the block
Merkle root	The root of Merkle Tree of transactions
Nonce	A random counter for proof-of-work
Block body: Transactions	
Transaction 1, Transaction 2 … Transaction n	

Transaction header	
Hash	The transaction's hash value
Block number	Block containing the transaction
Order	The transaction's number in the block
Timestamp	Creation time of the transaction
Sender	Sender's ID
Receiver	Receiver's ID
Signature	Sig{The transaction's hash value}
Payload	
data 1, data 2..data n	

2.1.3. Consensus mechanisms

Consensus is used in blockchain to ensure that nodes agree on the validity of a block. Consensus methods range from those that are entirely computational in nature, such as proof of work, to those that are communication-based, such as Practical Byzantine Fault Tolerance (PBFT) [32,33]. There are various consensus mechanisms in between the two, including Proof of Stake (PoS), Threshold Relay, and Proof of Burn. Along with the popular ones, the reviewed literature makes use of their enhanced variants. In connection with this, there are other high-quality reviews, such as [40,41] that can be referred to for clarification.

2.1.4. Smart contract

A smart contract can be thought of as an automatically invoked procedure that is initiated when a transaction is executed. All blockchain systems support smart contracts; however, they differ in terms of the language in which smart contracts can be written and the environment in which they are executed. Solidity, Golang, Serpent, Java, Python, and LLL are the most often used smart contract languages. There are numerous execution environments available, including the Ethereum Virtual Machine (EVM), Java Virtual Machine (JVM), Docker Image, and Haskell execution environment [32,33].

2.1.5. Application area and use of blockchain

As previously presented, the advancement of blockchain is primarily demonstrated by the growth of its application area and the purpose for which it is used. The application domain and purpose of blockchain utilization have an effect on the aforementioned fundamental blockchain issues.

In this context, certain sectors such as healthcare, financial systems, and digital rights management necessitate the use of a centralized peer-to-peer network or a permissioned private blockchain. A single ledger is used at a central server in this scenario, with peers maintaining metadata or pointers to their data. Decentralized structured topology is also recommended to be employed in banking by Ref. [42], in which a DHT can be employed to maintain references to the data that can be accessible through blockchain. The data can be stored in a centralized store such as a cloud or in randomly selected nodes and DHT is utilized to enhance data availability [43].

Decentralized unstructured topology is the most frequent way for developing blockchain-based architectural designs in cryptocurrency and some IoT contexts that involve several nodes. Clustering techniques similar to those mentioned above are also used in blockchain systems [44]. The communication methods outlined above are equally applicable in instances when blockchain technology is used. In this light, Bitcoin can be viewed as an illustration of a decentralized unstructured P2P network in which transactions are broadcasted to participants through gossiping. Similarly, gossip is utilized in Hyperledger Fabric to distribute metadata when a new peer joins the network and to construct and maintain a local view of other peers [45]. The following figure (Fig. 2) depicts the fundamental components of blockchain.

2.2. Internet of Things (IoT)

The Internet of Things is a subset of the Future Internet, in which "things" with identities, physical characteristics, and virtual personalities integrate seamlessly through intelligent interfaces [46]. In IoT, numerous software, middleware, and hardware devices are involved.

It is a well-known fact that IoT devices have fundamental constraints such as limited memory space, poor processing power, and limited battery life [47]. Additionally, they are typically scattered and may be located in an open setting in a variety of geographical locations. Furthermore, they are relatively new technology [48]. As a result, they are vulnerable to attacks, and their security methods must account for these. Moreover, communication between devices may be based on ad hoc IP protocols [49] such as Near Field Communication (NFC), Bluetooth, IEEE 802.15.4, Wi-Fi, ZigBee, and 6LoWPAN [50]. Also, ad hoc communication can occur over the internet, a mobile communication network, a satellite network, or a wireless network [51]. There is a possibility that such communications will expose information systems to threats such as intrusion and data tampering.

Additionally, due to the lack of a widely acknowledged layering scheme for IoT, there are architectural variances across them [52]. According to a number of publications, IoT devices consist of three layers: application layer, network layer, and perception layer [52]. Smart energy, healthcare, and smart city are all examples of the application layer in Ref. [53]. The network layer, on the other hand, includes devices such as routers, switches, gateways, and firewalls. Embedded systems and sensors are included in the perception layer. Despite this widespread layering, some add a business layer, a service management layer or middleware layer, and a physical layer to the above once [47]. The variation in layering is attributable to a variety of reasons, including the IoT device's release version, the standard that vendors adhere to, the device's functionality and complexity, and so on. This mismatch exposes

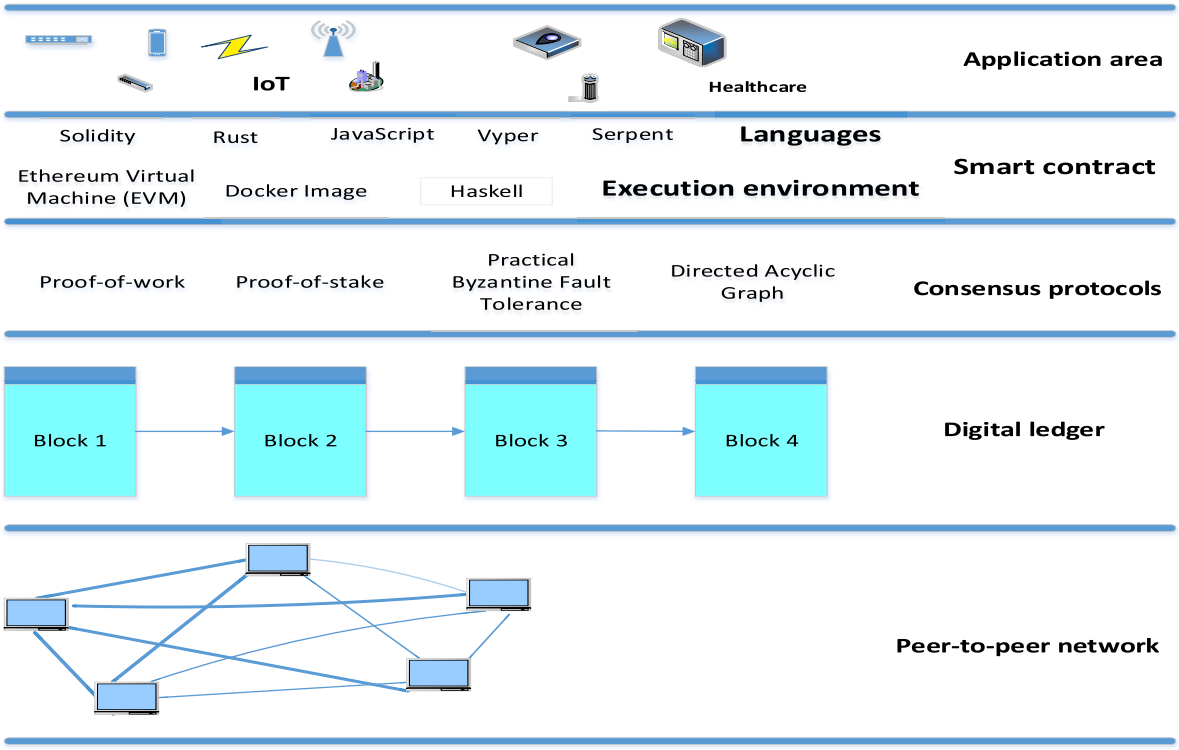

Fig. 2. The fundamental components of a blockchain.

IoT devices to attack and prevents them from communicating securely.

Furthermore, unlike traditional devices, which share some operating systems, there are no dominant operating systems utilized by a large number of devices in IoT [54]. Moreover, there is a lack of specific data formats. As a result, establishing interoperability between them is challenging [47]. One option that has been used is the use of middleware to facilitate the integration of IoT devices [48], although this has inherent security problems. Although numerous other efforts have been made, blockchain technology has recently been suggested as a possible way to address some of the aforementioned challenges.

2.3. Health information technology (HIT)

For decades, health information technology (HIT) has been the focus of various studies. Throughout, a variety of systems have been designed and implemented. Several of these include the Electronic Health Record (EHR), Computerized Provider Order Entry (CPOE), Electronic Medical Record (EMR), clinical decision support, electronic result reporting, electronic prescribing, Personal Health Record (PHR), mobile computing, telemedicine (remote monitoring), electronic health communication, data exchange networks, knowledge retrieval systems, and Health Management Information Systems (HMIS) [55–57]. Additionally, there are others, like electronic Medication Administration Records (eMAR) and Picture Archiving and Communication Systems (PACS) [58].

Recently, health IoT (HIoT), which is the subset of HIT, in which embedded medical devices, sensors, and IoT-enabled wearable devices are connected through long and short-range communication technologies are being synchronously utilized. In HIoT, identical to any IoT environment, sensors are employed but they take two forms, which are wearable and implantable. The wearable sensors are categorized in Ref. [59] into five groups that are pulse sensors, respiratory rate sensors, body temperature sensors, blood pressure sensors, and pulse oximetry sensors.

The overall goal of HIT is to achieve benefits such as reduced medical errors, improved patient outcomes, enhanced patient care, increased physician productivity, increased hospital value, and improved operational and financial performance of hospitals [56,58]. When health IoT is considered in isolation, it enables triage, patient monitoring, personnel monitoring, disease spread modeling and containment, assisting practitioners by providing real-time health status and predictive information, and providing information for policy decisions in pandemic scenarios, as explained in Ref. [60].

In general [58], demonstrates that HIT is effective when used in aggregate. However, it has been a long time since fragmentation in utilization has been noted, and governmental initiatives to improve health information interchange between providers have been passed [61]. In this context, it has been challenging to delineate clearly what information should be retained in a particular system. For instance Ref. [62], notes that many providers view EHR as an internal system. From another perspective, PHR consumes data from a variety of systems, including EHR, and hence EHR has data that is useful to PHR [5,63]. Additionally, it is discovered that one system can induce the use of another. For instance, eMAR and PACS facilitate the use of EMR and CPOE [58].

The existence of various types of duplicate information and dependency necessitates integration. Despite this necessity, system integration is uncommon [5,62]. Moreover, despite efforts, technological as well as non-technical challenges manifest on multiple levels. At the system level, incorrect workflow design and integration, combined with a mismatch in the rate of progress of HIT and the complexity of security and privacy issues in both distinct and integrated systems, preclude integration [64]. Data integration between systems is hampered by the absence of unique patient identification, a lack of messaging that permits syntactic and semantic compatibility between systems and the absence of data encoding standards [5].

Despite its rarity, in the integration effort consideration is usually given to the different stakeholders of healthcare who can be categorized as primary such as providers, purveyors (custodian or keepers of health data), and patients; furthermore, secondary stakeholders who have an indirect role in the HIT such as insurers, health authorities, clinical researchers and technology vendors [5]. These stakeholders have different interests and evolving information demands so HIT should address these issues. For instance, through time, the role of patients has transformed from being healthcare information receivers to becoming active participants of HIT systems [62]. It is also documented in Ref. [65] that patients' participation in HIT has an impact on improving patients' health outcomes such as frequency of hospital and emergency visits, readmission risk, and length of stay. Therefore, deliberation that takes into account the various interests is mandatory. Thus, blockchain is viewed as a tool for developing patient-centric systems in a variety of ways, including managing digital access rules, increasing data availability, increasing data liquidity, and assigning unique patient identities [66], all of which are addressed in greater detail below.

3. Methodology

Numerous authors, including [3,67], have emphasized the pervasive nature of blockchain, and as a result, several publications address the diverse prospective application domains. This increases the number of publications; as a result, the author must choose from a vast body of literature in order to undertake an in-depth review. To this purpose, the application domains, the technique for conducting the literature search, and the screening procedure for the gathered articles are as follows.

3.1. Search strategy and application area selection

At the outset, a literature search strategy was designed by customizing recommendations presented in Refs. [68–70]. Consequently, initially, in December 2018 literature search on various databases described below was conducted by using the key term "blockchain", which yielded a large number of documents. A first evaluation that encompasses the publications' application area, language, impact factor, etc. Were employed to conduct screening on the gathered documents. Afterward, through reading their titles and abstracts, the remaining publications were sorted as per their application areas such as cryptocurrency, IoT, healthcare, smart contract, supply chain management, banking and finance, industry, and other areas. Next, analytical reading was made to decide on which application areas further review is needed. In this regard, although the majority of the publications deal with cryptocurrency, the scope of this review is on those that are commonly categorized under blockchain 3.0. From this class of publications, the most prominent usages are on healthcare and employing blockchain along with IoT. After sorting the documents and selecting the application areas from blockchain 3.0, the second search was started. This was conducted a year later, in December 2019 with search phrases, which are: "blockchain in IoT" and "blockchain in healthcare". This was done together with forward and backward searches as necessary. The reason for conducting the second search with a year gap is to understand the shift in conceptualization and the trend in usage of blockchain in the application areas.

Between the two searches, analytical reading was conducted to have a better grasp of the subject and to establish criteria for document inclusion or removal [69]. Other supporting literature from the application fields was obtained and provided to substantiate the review based on the knowledge gained via the analytical reading. When a gap was discovered between prior information and publications dealing with blockchain, further publications were consumed to round out the evaluation and establish a connection between prior knowledge and the emerging trend in blockchain usage.

3.2. Inclusion criteria

The inclusion criteria for the primary publications were as follows. Publications that belong to the application areas and are published on a journal with an impact factor greater than 1.0, as per the source database of the publication and books or chapters of books are qualified for further processing. However, conference papers are considered cautiously as noted in Ref. [68], but those that are organized by trustworthy professional associations such as AIS, ACM, IEEE, ICIS, INFORM, etc. as suggested by Ref. [71] were qualified for the next processing. However, they were also assessed against the Google h-5 index, in which those that obtained 10 or more in the index were included.

Setting such quality requirements has an effect on a number of issues, including the involuntary exclusion of valuable publications from sources with lower rankings. Apart from the impact factor 1.0 criterion indicated in Ref. [70] as an example of exclusion, there is no cutoff level that specifies a journal's quality, which changes on a periodic basis. Furthermore, the h-5 index is used infrequently. As a result of these concerns, certain high-quality papers may be removed, although this has no effect on the review's replicability.

Despite this, on publications that pass the above criteria, a critical assessment was made. Critical assessment is elaborated in [69, p. 265] as a way that helps to broaden the "analysis of what is known, how knowledge is acquired, what types of knowledge is produced, how useful different types of knowledge are in understanding in explaining a problem of interest and where the boundaries and weaknesses of existing knowledge are". The reason for making a critical analysis of literature is to get an understanding of the knowledge that has been gained from using blockchain for the application areas, to comprehend the level at which blockchain has been revolutionizing the application areas and to savvy the way the artifacts which are composed of constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices) and instantiations (implemented and prototype systems) [72] are being developed. The critical assessment enables the author to conduct a second evaluation that helps to screen out publications that have fewer relevancies and are deprived of depth in their presentation. Some publications excluded in this regard include [73–75]. The steps followed in preparing the article is shown in Fig. 3.

4. Result

The publications reviewed cover some common themes and other application-specific issues. This section summarizes the findings from the literature review.

4.1. The reviewed publications

Due to the fact that blockchain applications in IoT are still in their infancy, few initiatives have gone beyond the proof-of-concept or

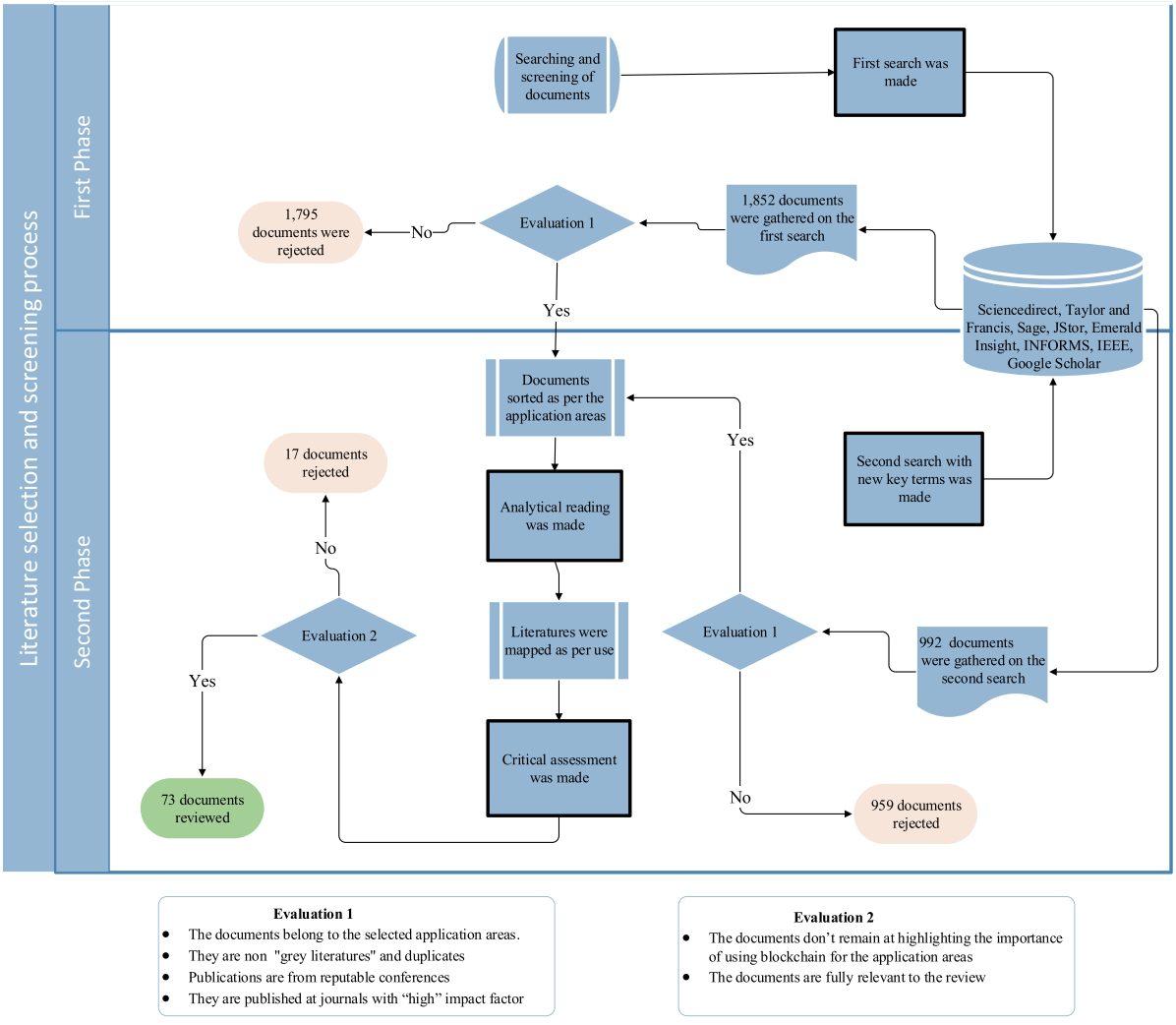

Fig. 3. Steps followed in the review process.

technology readiness stage (TRL) [52]. However, of all the application domains that are typically classified as blockchain 3.0, this is the most prevalent use. Articles in this domain address a broader range of subjects, including how blockchain can be integrated with IoT, how IoT data is managed, IoT security, and smart city-related challenges.

The other area in which blockchain technology has the potential to make a big change is healthcare. Blockchain technology is mostly utilized in healthcare to manage data. The following table presents a list of publications that discuss the applicability of blockchain technology in these two sectors (Table 4).

In IoT, the most commonly covered topics include providing substantial information about the benefits of blockchain for IoT and designing systems that can help in enhancing the security of IoT data. Additionally, various publications demonstrate the integration of blockchain with IoT. Furthermore, some papers explain smart city-related usages. All these are presented in greater detail.

On the other hand, some authors discuss the potential benefits of using blockchain in healthcare. To this aim, potential benefits of blockchain technology include the ability to develop a reliable, secure, immutable, robust against a single point of failure, and incentive-based decentralized and user-managed data provenance system. Additionally, it improves drug supply chain, acts as a database for medical research, clinical trials, and consent management, and can be used as a platform for medical payment systems, streamlines insurance claim processing, and securely shares and stores medical records [6–8]. Moreover, it enhances data availability and enables patient identity assignment by promoting data immutability through immediate access to clinical information [66].

However, the use of blockchain in healthcare is not without challenges, as discussed in Refs. [6,7,77]. Maintaining confidentiality is a problem, as is increasing the throughput and scalability of blockchain-based systems. Moreover, security concerns and limited storage space make it difficult to store image data that is large enough to be maintained on a blockchain, and cost-effectiveness is another issue.

4.2. Integrating blockchain with IoT

While the authors apply blockchain in an IoT setting, they do it in a way that they believe will enable them to take advantage of the benefits associated with the concurrent use of both technologies. However, their decision is determined by the application area in which they aim to develop the instantiation, the required latency and throughput, the application area's regulatory environment, and the manageability of the blockchain's participants, among other factors.

With this in mind, two articles seek to classify the integration methods of blockchain and IoT into three distinct categories. On the one hand [81], classify integration solutions according to the amount of data that flows through blockchain during data exchange between IoT devices. On the other hand [135], compares blockchain with cloud for service provision. The two approaches are not mutually exclusive; rather, they complement one another. For example, whereas [81] emphasizes the relationship between blockchain and IoT devices [135], broadens the association from IoT devices to the cloud.

To this effect, in the first way of integration, while the normal communications between IoT devices are intact i.e. in the data exchange between IoT devices, blockchain plays no role rather it serves as a medium of storage for some of the data or the metadata of the actual data; and this is usually termed as off-chain usage [81]. Prolonging this relationship to the cloud, in this integration method, blockchain isn't considered as the main service outlet rather it assists the cloud and this is termed as Cloud over Blockchain (CoB) as per [135]. The second architecture allows a significant involvement of blockchain; hence all data created through the interactions between IoT devices pass through it. In comparison to the cloud, in this architecture, blockchain serves as the central channel of service provision but obtains analytical and virtualization services from the cloud, which is termed as Blockchain over Cloud (BoC) in Ref. [135]. In the last setting, a fair share of data interchanges happens on both the blockchain and the IoT devices, which enables the simultaneous and direct utilization of the qualities of both technologies. From the perspective of cloud against blockchain dominance viewpoint, this method is referred to as Mixed Blockchain-Cloud (MBC) in Ref. [135].

While generalization is difficult, it is noticed in the literatures that systems that integrate blockchain and IoT come under one or more of the approaches discussed above (Table 5).

Table 4
List of primary literature.

Usage	Publications focus on	
	IoT	Healthcare
General explanation/ framework	[76]	[6–8,74,77]
Integrating blockchain with IoT	[47,52,53,78–90]	[91–95]
Security	[11,26,47,48,79,80, 96–108]	[27,30,91,92,103, 109–115]
Data management	[39,78,91,97–101, 116–120]	[27,30,66,92,109–115, 121]
Smart city	[83,122–129]	
Drug supply chain		[130–133]
Industry	[90,134]	

4.3. Blockchain and IT security

The IoT is the topic of security-related literature, with a particular emphasis on data security. However, blockchain technology may be used to address a variety of additional security concerns. This section discusses the benefits of utilizing blockchain to accomplish this goal. However, the following section on data management discusses data security.

In [11] the security challenges associated with IoT and the manner in which blockchain technology can assist overcome them is discussed. Similarly [12], conducted a review of the literature on the application of blockchain for security purposes, with an emphasis on IoT security. Numerous other researches, including [46,47,102,106], emphasize the potential security benefits of blockchain technology in the IoT security arena. As a result, the following benefits accrue in this regard:

- The immutability of transactions maintained on the blockchain can enable the registration, tracing, and management of the Identity of Things (IDoT) throughout their life.
- The use of cryptography and distributed ledger technology endows IoT devices with fault tolerance;
- The use of smart contracts facilitates user authorization, maintains software integrity, enhances software synchronization, and privacy;
- The presence of lightweight blockchain-based security protocols can simplify the process of establishing secure communication between IoT devices.
- The distributed nature of blockchain can avoid a single point of failure.
- The extra address space that blockchain has over IPv6 makes it suitable for evading collusion in providing Global Unique Identity (GUI) for IoT devices;

Although such benefits exist, the majority of articles focus on data security, which is a subset of data management that is discussed in the following section.

4.4. Data management

Data management can be considered as the process of acquiring, processing, securing, disseminating, retrieving, and storing data in an

Table 5
Integration methods employed in various publications.

Publication	Employed method	Integration method employed		
		IoT-IoT (CoB)	IoT-blockchain (BoC)	Hybrid
[126]	Intelligent vehicles communicate with each other and the data is stored in local dynamic blockchain (LDB) and main blockchain (MB)		✓	
[80]	A cluster-based overlay network is placed between the cloud and the smart home. An overlay cluster head maintains blockchain on a ledger opened for each node for keeping a record of transactions sent to request or share data.			✓
[94]	The hash value of data collected from wearables and providers is stored at the blockchain. Furthermore, the access history of providers and insurance companies are recorded	✓		
[125]	Place edge network between the IoT devices and the core network (the blockchain). The edge nodes pre-process data and transfer it to the core network.			✓
[90]	The blockchain receives data collected by sensors and forwards it to the IoT platform. Participants that include suppliers, logistic providers, shipping agencies, and warehouses query from the blockchain		✓	
[86]	Edge computing receives data from IoT devices then processes and analyzes them before sending them to the blockchain.			✓
[30]	The querying history of data is stored on the blockchain	✓		
[112]	While the cloud is employed to store encrypted PHR the blockchain is used to maintain the metadata and access log. In the system, the gateway server has a critical role.			✓
[109]	The blockchain is employed to store some data and the pointers of image data whose size is large to be maintained therein. As a solution, they create a data lake for larger files			✓
[91]	The hash value of data is maintained on the blockchain and the corresponding actual data is kept in an encrypted data block in the cloud.	✓		
[99]	All transactions pass through blockchain, which is connected to Mobius server that uploads data to the blockchain by operating between IoT devices and the application		✓	
[110]	The blockchain is employed for registering the list of images and the patient to whom they belong, the list of entities for whom the patient grants access rights, and the source node from where they can access the image.	✓		
[88]	In the three-tier architecture, the blockchain is placed at the cloud where cloud service providers register rendered services and share with peers. Furthermore, at the fog node level, the blockchain is employed for the provision of enhanced service. In both cases, some data pass through the blockchain.			✓
[87]	The blockchain is part of the cloud service employed to ascertain the secure and proper validation of transactions.			✓

orderly fashion. These data management operations are influenced by a variety of factors, including the requirements of an application area, the architecture chosen for the system, and the intended purpose for which the system is supposed to be used. Several blockchain-based data management solutions have been proposed in the literature. Due to the differences in the characteristics of healthcare and IoT-based applications, the usage of blockchain for data management activities varies. Those designed for IoT take into mind the qualitative characteristics mentioned above, such as the numerousness of sensors and the ad hoc nature of IoT networks. On the other hand, those that are healthcare-focused take into account the requirements of healthcare systems, such as latency susceptibility and high-security sensitivity of healthcare data.

Numerous factors contribute to the use of blockchain technology for data management. To begin with, with IoT, which includes HIoT, devices primarily collect data via sensors. Nowadays, the number of sensors is expanding exponentially, heralding the arrival of an era of global sensor networks requiring a sophisticated data management system [136]. Second, these devices generate heterogeneous data streams in real-time, resulting in the emergence of big data 3.0 [137]. However, standard data management approaches are not highly scalable enough to handle enormous volumes of data [138], necessitating the development of a more robust data management system. Thirdly, traditional data management systems based on client/server interactions, which are currently employed in healthcare and IoT, are susceptible to a single point of failure. Even worse, the current distributed network architecture, protocol, and techniques are unsuitable for addressing new difficulties and developing service requirements [79]. Fourth, data kept on numerous servers are frequently unencrypted, posing a security concern [39], whereas blockchain-based systems employ data storage mechanisms that apply a variety of encryption techniques. Fifth, in IoT-enabled systems, data management operations are performed both online and offline, which traditional data management methods struggle to manage [139]. As a result, there has been a search for a data management mechanism that enables the transmission of small data packets, does not require a big channel bandwidth with delay tolerance capability, and consumes lowenergy [140].

As a result, while blockchain does not meet all of the requirements, it is viewed as a tool for addressing these types of challenges. Apart from resolving these issues, the need to use blockchain for data management arises due to a number of its characteristics, including its ability to

secure data ownership [43], improve data assurance and resilience [119], endow data with high credibility, decentralization, and security [39], and tamper-proof data throughout its lifecycle [120].

4.4.1. Data acquisition

Data acquisition is one of the data management operations that blockchain technology has the potential to improve by securely assigning a unique identifier to things, entities, and users throughout the authentication process. This property of blockchain enables data to be acquired from the right source.

Acquiring data from the right source is accomplished by the enhancement of message authentication, transaction authentication, entity authentication, and key authentication through the distributed consensus processes. Various authentication designs and methodologies are used in the reviewed articles. To name a few, in an IoT context, for example, in Ref. [96], special devices called Manager Servers (MS) assign IDs to other devices using the devices' private key. Secure virtual zones (bubbles with group ID) are employed in Ref. [26] to enable secure communication between nodes. In healthcare, for example [103], patients are identified through a Virtual Identity built using blockchain's pseudonymous naming capabilities. On the other hand [114], authenticate users with an Interactive Voice Response System (IVRS). However, the most widely used form of establishing identity is through the use of a public and private key pair, with the public key serving as the digital identity, as described in Ref. [111].

4.4.2. Data processing

Since smart contracts became a critical component of blockchain usage, the majority of blockchain-based systems now rely on them to process data autonomously. However, it is noted that the number of smart contracts used in systems varies. For example [27], employs six smart contracts [97], utilizes four smart contracts [101], plans to consume as many smart contracts as the amount of "sidechains" that will be constructed [95], uses three smart contracts, and [104] utilizes one smart contract for each resource owner. All of these articles defend their use; nevertheless, to the author's knowledge, no publication compares the performance of such types of employment.

On the other hand, authors create various architectural mechanisms for data processing, such as assigning nodes that have a better capability as processing nodes [78], besides in Refs. [86–88], fog and edge computing along with blockchain are employed to offload data processing. Differently [26], creatively partition the IoT network, and others for instance Refs. [96,126], establish hierarchies of blockchains. These architectural solutions have an effect on system latency, as the presence of hierarchy and partition might impede consensus on a global truth.

4.4.3. Data security

While data security involves a variety of issues, it is noticed that blockchain-based systems are primarily concerned with resolving three topics: data integrity, access control, and privacy preservation. Essentially, security concerns are not distinct from one another; rather, they are inextricably linked. Despite, publications have concentrated on those subjects, which are discussed in detail below.

4.4.3.1. Data integrity. The term "data integrity" refers to the process of ensuring the accuracy and consistency of data throughout its lifecycle [116]. Prior publications, such as [141,142] expound on the fact that data integrity strategies are concerned with avoiding, identifying, and correcting data integrity issues. Methods such as journaling and building encrypted file systems are aimed at avoiding data integrity issues. Additionally, check-summing, mirroring, Cyclic Redundancy Check (CRC), and parity are used to detect data integrity risks. On the other side, correcting data integrity concerns are addressed using methods such as majority vote and RAID parity.

Numerous strategies are applied in the publications reviewed, as summarized in the following table (Table 6).

4.4.3.2. Access control. Access control, or the management of the rights provided to a resource, is a critical component of security. It has been considered from a variety of angles in the literatures. For example [143], uses the Objective, Model, Architecture, and Mechanism (OMAM) reference model to categorize access control mechanisms used in IoT. To this purpose, models such as Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Usage Control (UCON), and Capability-Based Access Control (CapBAC) are discussed. On the other hand, architectures include Extensible Access Control Markup Language (XACML), Open Authorization (OAuth), and User Managed Access (UMA). These models and architectures are used to accomplish objectives such as ISO/EIC 27002/27,005 standards, among others, through the use of mechanisms such as Access Control Lists. On the other hand, as the review and classification offered in Ref. [144] demonstrate, the access control approaches discussed above and others have multiple variants. Additionally, there are access control models that combine access control and privacy protection, such as those described in Refs. [145,146].

The literatures that employ blockchain technology make use of a variety of access control approaches and structures, including those listed in the following table (Table 7).

4.4.3.3. Privacy preservation. The other issue that the literatures address is the preservation of privacy. According to Ref. [147], privacy preservation techniques can be categorized into two broad categories: data privacy and context privacy. While data privacy concerns difficulties such as maintaining privacy throughout data aggregation and

Table 6
Techniques employed for maintaining data integrity.

Publications	The technique used to maintain data integrity	Application area	
		IoT	Healthcare
[92]	Equivalence checking of Magnetic Resonance Image (MRI) through radiomic features (shape features)		MRI related imaging systems such as MRI scanner
[114]	Zero-knowledge proof		Clinical trial data management
[101]	The Interplanetary File System (IPFS) Content Identification (CID)	Generic	
[91]	Lightweight ring signature, Addition Rotation and XOR (ARX ciphers), and public encryption schemes are used		Healthcare IoT
[27]	Data is encrypted and then hashed before being stored on and off-chain		Electronic Health Record (EHR)
[116]	Encrypting the hash value of a block	Generic	
[125]	Digital signature and hashing the data with Argon2 based hashing scheme to store the data at the blockchain	Smart city	
[94]	Data are arranged in a Merkle tree format by using Chainpoint open standard so that any modification is identifiable.		Health IoT
[30]	Data is hashed with Keccak 256 and the hash is included in a smart contract.		Biomedical database
[93]	A smart contract is employed to generate automatic notifications of health events to the users so that any tampering is detected		Health IoT

Table 7
Access control method utilized.

Publications	Access Control method employed	Application area	
		IoT	Healthcare
[104,117]	Employ smart contract as a policy enforcement tool that grants authorization through token	Generic	
[112]	Fine-grained and flexible proxy re-encryption is used. Furthermore, a gateway server that stores access-list acts as a semi-trusted entity		Personal Health Record (PHR)
[101]	A validator node is assigned in each sidechain that monitors incoming access requests and controls access at the sidechain level. Globally, a consortium made up of validators is responsible for controlling access to outsiders. Furthermore, they employ Interplanetary File System (IPFS) that helps in decentralizing access control.	Generic	
[97]	They employ a decoder to translate various access control models and mechanisms into Access Control List (ACL), Capabilities and Attributes, which the authors believe could lead to compatibility between various models	Generic	
[109]	Access control is expected to be realized through a multi-signature method for which the capability of NEM blockchain platform enables securing access control and data sharing.		Diabetes-related healthcare data
[78]	For controlling access, lightweight nodes called management nodes that are connected to blockchain on an ad hoc basis which don't store blockchain information are utilized	Generic	
[94]	Employ Hyperledger Certificate Authority (CA) for getting enrollment and transaction certificates for participating nodes		Mobile healthcare applications
[91]	Lightweight ring signature Addition Rotation XOR (ARX ciphers) and public encryption schemes are used		Health IoT

Table 8
Methods used for privacy preservation.

Publications	Privacy preservation method employed	Application area	
		IoT	Healthcare
[101]	Maintaining the logging history of each node and dividing the network into smaller "sidechains"	Generic	
[112]	A gateway server that acts as a semi-trusted entity by playing roles such as authenticating users, re-encrypting data before sending it to requesters, and storing logging information on the blockchain is utilized. The gateway doesn't have the opportunity to learn about the data.		Personal Health Record (PHR)
[98]	Privacy of transaction data is maintained through Attribute Based Encryption	Generic	
[91]	Lightweight ring signature Addition Rotation XOR (ARX ciphers) and public encryption schemes are used		Health IoT
[39]	Threshold Secure Multiparty Computing (TSMPC) protocol	Generic	
[27]	Distributed proxy re-encryption with blinding		Electronic Health Record (EHR)
[99]	A smart contract is created with zero proof of knowledge function	Smart meter	
[103]	Pseudonym Based Encryption with Different Authorities (PBE-DA)		Electronic Health Record (EHR)
[80]	Hierarchical architecture with centralized Immutable Ledger (IL) at the local IoT network level and a decentralized public blockchain at higher-end devices	Smart home	

querying methods, context privacy deals with location and temporal privacy.

In situations when blockchain is used as part of a system [148], conducted a literature survey and classified privacy-preserving techniques into four categories. These are (a) smart contract or key management derivation through the use of secure multiparty computation (SMPC), and (b) identity anonymization, which focuses on securing the identities of users participating in a transaction through the use of mixing, ring signatures, and zero proof of knowledge. (c) Transaction data anonymization, which focuses on ensuring the privacy of transaction contents through mixing, differential privacy, zero-knowledge proofs, and homomorphic hiding; and (d) on-chain data protection, which focuses on securing data stored on the blockchain using encryption techniques such as asymmetric encryption and attribute-based encryption.

While this is the case, the following table summarizes the privacy preservation techniques used by the publications (Table 8).

4.4.4. Dissemination

Dissemination of data can take a variety of forms. Fundamentally, there are two main groups of data dissemination methods depending on who initiates the data transmission, i.e. whether a client requests or a server supplies the data. The first is push-based, while the second is pull-based. While push-based dissemination involves a server pushing data to clients, pull-based dissemination involves a client requesting data from a server. In terms of timing, both techniques of data dissemination allow for scheduled or random data transfer. Additionally, data delivery might be one-to-many or point-to-point.

The data delivery mechanism used in pull-based aperiodic data dissemination with point-to-point communication is characterized by request and response. However, if the communication is one-to-many, the mechanism used to convey the request and response data is snooping. In contrast, polling is used to deliver data in a pull-based periodic point-to-point communication, whereas snooping is used to deliver data in a one-to-many communication. On the other hand, when data is delivered randomly in a push-based one-to-many communication, it is referred to as publish and subscribe; when data is delivered periodically, it is referred to as broadcast. Triggers are used to refer to aperiodic point-to-point data transmission [149].

On the other hand, in Wireless Sensor Networks (WSN), data routing strategies can be classified as flat, hierarchical, or location-based according to their network topology. If the operation of their protocol is used to classify them, they fall into five categories: negotiation-based, multipath-based, query-based, Quality of Service (QoS)-based, and coherent-based [150].

Combinations of the aforementioned mechanisms, structures, and actions are noted in several of the reviewed literatures. For example, in Ref. [95], the data dissemination mechanism is publish and subscribe, in which a blockchain publisher provides information to an IoT-enabled blockchain, from which nodes can acquire data by subscribing. In Ref. [98] a hybrid of pull- and push-based data transmission techniques with a hierarchical framework is employed. The cluster head takes data from sensors and then distributes it to peers.

Leaving the details for the subsequent section, the usage of blockchain in IoT comprises smart city, with smart transport being one of the

information dissemination-based systems. In this regard, publications such as [119,122] use trigger to disseminate data. These publications, on the other hand, propose distinct network structures. In Ref. [126], propagation occurs either from a single vehicle to a large number of vehicles or from a single vehicle to another vehicle or to infrastructure, with the goal of establishing two-tier blockchains (Local Dynamic Blockchain and Main Blockchain). In Ref. [129], messaging between vehicles occurs in a one-to-many or point-to-point fashion.

4.4.5. Retrieval

In blockchain-based systems; data is stored in an encrypted form. As a result, data retrieval approaches such as Searchable Symmetric Encryption (SSE), which was first presented as a Boolean search scheme by Song et al. [151], are helpful. Several authors have enhanced SSE, most notably Swaminathan et al. [152], who developed ranked ordered search for encrypted documents. These two approaches can serve as a starting point for developing appropriate data retrieval solutions. On the other hand, when image data is encrypted, Lu et al. [153] first proposed algorithm for image retrieval over an encrypted image. Since its inception, the mechanism has evolved to incorporate additional characteristics such as privacy preservation. Ferreira et al. [154] proposed the approach for privacy-preserving encrypted picture retrieval, and it is currently considered an emerging field.

Despite these, data retrieval is not a primary objective of many of the reviewed papers. The only publication that focuses on it is [30], in which blockchain is situated as a contract service between biomedical databases and data consumers. The blockchain data acts as permanent proof of data retrieval activity, which is tracked in part by comparing the hash value of a query to the hash value of a result.

In the remaining research, it is found that some researchers treat data retrieval from blockchain as a transaction, while others do not due to performance concerns. To name a few, whereas [29,38] consider it in the former manner [78], does not account for it as a transaction except for critical access control systems.

Additionally, there are distinctions in the literatures about the provision of a right to retrieve and learn about data between blockchain participants. In this regard [39], mentions that the results of a query are decrypted by a designated entity called a leader [112], explains that a gateway server performs re-encryption and the requester decrypts it, and [113] states that a user decrypts data on their own but retrieves it through an intermediary called a Private Accessible Unit (PAU). In contrast, a query in Ref. [94] can be made by a variety of entities, including a provider, a user, and a healthcare insurance company.

4.4.6. Data storage

According to some authors, blockchain is a distributed database. Despite their similarities, distributed databases and blockchains are not identical. To name a few, in blockchain, replicated copies of data are stored at nodes to circumvent the need for a central trust point; yet, distributed databases are maintained to optimize database efficiency by splitting information retrieval and processing. Additionally, the data stored in the nodes of a distributed database is not homogeneous. The other distinction is that, in contrast to distributed databases, blockchain technology incorporates an automatically executable program known as a smart contract [42].

There are numerous data storage strategies in an IoT environment, including (1) external storage, in which nodes send data to a base station or gateway without processing it, and (2) local storage, in which each node stores data. (3) data-centric storage, which involves nodes that are chosen to store data depending on a preset criterion (4) fully distributed data storage, which allocates storage responsibility in a fair manner to all participating nodes [155,156].

From the standpoint of data storage, disparities in blockchain utilization are found. These are due to a variety of variables, including legal concerns about privacy, latency requirements, and the size of the file to be stored. In this context, healthcare is subject to a variety of legal challenges, making it particularly sensitive to privacy concerns. Additionally, the size of the data has an effect on its storage. As a result, huge files, the majority of which are the result of radiology, are treated differently than laboratory tests and other research data.

The usage of blockchain in radiology focuses on leveraging it as a storage for some data, pointers, and metadata associated with imaging tests that are typically low in volume but high in cost [157], such as CT scans, X-rays, magnetic resonance imaging (MRI), and electrocardiogram (ECG) files. To cite a few publications [109], created a data lake to store large files off-chain [27], maintained the hash value of patients' data pointers [110], uses blockchain to register only the list of images, the patients' names, the names of individuals who have access to the images, and the parties who have accessed the files throughout the files' existence [111], proposes storing metadata on the blockchain, and [115] stores the address of a patient's data pointer.

In terms of regulations, several of the literatures discuss certain statutes. For example [111], focuses on a standard called Fast Healthcare Interoperability Resources (FHIR), which is primarily concerned with the exchange of medical data in transit and storage. As required by the standard, the system saves data pointers on the blockchain. Another paper, namely [118], examines the European Union's General Data Protection Regulation (GDPR), which imposes constraints on the length of data storage, among other things. In accordance with this, one of the objections leveled towards blockchain-based systems is that their immutability precludes them from being regulated, however, the authors address this concern through the use of ontology. Ontology has the potential to resolve semantic heterogeneity associated with the use of various IoT devices. This is accomplished, for example, by raising awareness of security threats. However, they use it for intelligence policy analysis in their system, which includes consent management for data acquisition, update, and disposal.

4.5. Blockchain and smart city

The smart city concept is a subset of the smart planet agenda, with a spatial demarcation for its execution [158] that is conceptualized in two distinct ways. The first defines smart city or smartness as the level at which places are connected through IoT, implying that technocracy plays a role in cities management. On the other hand, the second one stresses the establishment and spread of a knowledge-based economy, in which information and communication technologies play a crucial role in the development of the envisioned economic model [159]. Both conceptualizations emphasize the importance of technology in the form of IoT.

Smart city applications include smart buildings, smart education, smart healthcare, and social care, smart energy, smart grid (smart metering of natural gas, water, and electrical energy), smart utilities (smart water distribution and waste management), smart parking, and smart & integrated transportation [160]. The implementation of a smart city presents various challenges, including the influx of big data, which demands real-time management and analyses of massive volumes of complicated data. Additionally, system-level challenges include ensuring the privacy and security of collected data, achieving low latency and high mobility, structural scalability, network bandwidth constraints, single-point of failure, infrastructure security, operational security, and compliance with environmental and governmental regulatory policies [125,128,159,161–163]. The involvement of companies in the realization of smart city projects exacerbates the challenges. These kinds of "corporate smart city" schemes are criticized by Ref. [164] due to data privacy concerns, the hidden motives of companies, and the lack of community participation.

To address these and other challenges, blockchain is considered to make a substantial contribution, as seen by the growth of publications addressing its usage. As a result, authors such as [123,125] suggest frameworks for utilizing blockchain technology in smart city applications. In Ref. [123], blockchain serves two purposes. On the one hand, it

is used at the prosumer level to connect smart devices to a smart meter. Additionally, the smart meter is linked to the micro-grid, smart appliances, and sensors. The micro-grid acts as a data hub and a tool for energy exchange in the design. On the other side, each community and smart grid are connected through a blockchain at the household level. According to the authors, this type of usage enables a community to self-manage its energy consumption. The architecture described in Ref. [125] places edge computing between a blockchain, which serves as the core network, and an IoT device network. The obvious goal of processing data at the edge network and then transmitting it to the blockchain through edge computing is to alleviate the blockchain's workload.

In [128] a smart home architecture that layers blockchain on top of a smart home network but beneath the cloud computing network is presented. All transactions in the smart home are routed over the blockchain and are handled by a block manager who is in charge of the generation, verification, and storage of transactions into blocks.

The authors of [124,126] focus on the application of blockchain technology to smart transportation. In Ref. [124] an overview of how blockchain can be used in conjunction with smart transportation by describing seven tiers of intelligent transportation systems that utilize blockchain technology is provided. According to the article, the most successful application of blockchain in intelligent transportation systems is the real-time sharing of information. A similar issue is addressed in Ref. [126], which employs a point or token system that begins with the purchase of a car and subsequently accrues points based on traffic-related performance. They refer to their point-based system as Intelligent Vehicle Trust Point (IVTP), in which reward points are used as a prize, similar to how Bitcoin pays miners, but this time based on traffic-related performance. They propose a two-tiered blockchain system comprised of a local and a central layer. While the local blockchain is branched and stores data for a limited length of time, the main blockchain tracks IVTP transactions in the same way as Bitcoin does.

Smart grids have also garnered attention from authors, including [83,127]. In Ref. [127], a survey of blockchain application cases is presented. As such, in conjunction with the smart grid, blockchain may be utilized primarily as an infrastructure for peer-to-peer energy trading and as a deterrent to data tampering in the power-producing and distribution industries. Consistent with this [83], a layered structure based on blockchain that they believe can enable energy policy enforcement, energy trading, and security enhancement is proposed. To accomplish these goals, the blockchain is deployed through a virtual private network, with each node implemented by software.

4.6. Blockchain and drug supply chain

One of the difficulties in managing the pharmaceutical supply chain is avoiding fraudulent activities such as counterfeiting, sub standardization, and diversion (stealing and selling medicine) [130]. Counterfeiting, for example, has three forms: (a) modification, (b) using the correct product's information to create a forged one, and (c) removing the correct product's information and reusing it to a fake one [165].

Numerous solutions are being used to overcome these challenges, including smartphone verification systems and pill image recognition tools. Additionally, RFID technology is being utilized, including microtags attached to individual pill units and data integration with other sources of data. Moreover, technology such as machine learning and online verification was employed. However, blockchain technology, which is comprised entirely of distributed ledgers and is coupled with IoT, is also being investigated as a possible remedy [130]. In comparison to all of these processes [130,131], credit blockchain with resolving the aforementioned issues by making the drug supply chain trustworthy, transparent, traceable, verifiable, and resistant to the intrusion of counterfeit medicines. Nonetheless, there are a number of disadvantages to blockchain implementation, including the lack of regulatory guidelines and the necessity to preserve pharmaceutical users' privacy [132].

Several blockchain-based systems, on the other hand, are being proposed. In this regard [131], create a system that includes codes printed on tablets that can be read by stakeholders' cellphones. Due to the fact that the code is stored on the blockchain and the movement of the medicine is tracked, each entity scans and signs the code as the drug passes through the supply chain, preventing counterfeiting. Similarly [133], develops a method for ensuring the transparency of drug-related transaction data across the supply chain. Their system is comprised of four entities: alliance members who grant licenses to miners (government and manufacturers), full nodes (wholesalers and hospitals), and normal nodes (pharmacies and consumers). According to their design description, a public key is utilized to generate a Quick Response (QR) code that acts as a unique identifier (ID) for medications. When medicine is manufactured, information about it is stored on the blockchain as the hash value of its name, location, and timestamp of the manufacturing date and time. Unspent Transaction Outputs (UTXOs) and private keys, respectively, can be used to detect fraudulent transactions such as sales by unlawful distributors and unauthorized persons.

5. Discussion

The purpose of this review is to discuss how blockchain is utilized for data management and delves into the application areas of IoT and healthcare. Additionally, it assesses the integration strategies utilized to integrate blockchain with IoT. As a result, selected works from a list of publications are reviewed to demonstrate the approaches used to integrate blockchain and IoT. Moreover, data management activities which are data acquiring, processing, security, dissemination, retrieval, and storage strategies used in blockchain-based systems are demonstrated. Furthermore, the use of blockchain in smart cities and the drug supply chain is discussed.

5.1. On integrating blockchain and IoT

Clearly, blockchain, like IoT, is pervasive [3,67], and its adoption can benefit a wide variety of applications. Healthcare is one sector where HIoT has the potential to make an impact. However, while the integrative use of both technologies is beneficial, the qualitative aspects of both technologies have an effect on the integration efforts. These include the existence of a large number of sensors, the low memory capacity of blockchain and IoT, the low processing capacity and battery life of IoT, and the low latency of various blockchain-based consensus processes. Blockchain is being used in IoT not only for its qualitative benefits but also to resolve some of the shortcomings that IoT currently possesses.

According to the publications cited previously, there are three methods for integrating blockchain with IoT. The methods used are influenced by the sensitivity of the data, the legal requirements, the amount of the data, and the system's latency and throughput requirements.

The degree of interaction between IoT devices and the degree to which blockchain is integrated into systems, as well as the level of emphasis placed on the blockchain, serve as the basis for categorizing integration mechanisms. According to these, blockchain plays a minor part in the first method, dubbed IoT-IoT or CoB. The second technique, known as IoT-blockchain or BoC, utilizes blockchain heavily for data storage, while the hybrid model incorporates an edge, fog, or overlay network into the grand system. It should be noted that these strategies do not cover all possible applications; thus, some circumstances require a combination of them. Nonetheless, some typical works are shown in a tabular fashion above, taking into account the primary classification criteria.

In contrast to other domains, the presentation demonstrates that the dominating architecture in HIoT is the first type in which blockchain is utilized as a store for the metadata associated with actual files. This is mostly owing to the existence of radiology-related data, as previously noted. One advantage of utilizing this type of integration in healthcare is

that it resolves the bandwidth issue associated with storing a file on the blockchain. Additionally, it enables blockchain-based systems to comply with some regulatory obligations for the secure storage and sharing of data. The intricacies of one regulation in terms of blockchain application are discussed in Ref. [111]. On the other hand, the hybrid integration leverages the benefits of both blockchain and IoT, making it ideal for situations requiring a high level of latency. Additionally, it is suitable for systems with a high number of sensors.

5.2. On data management in IoT and healthcare

Data management is described in this review as the key duties performed throughout the data life cycle, including data acquiring, processing, security, dissemination, retrieval, and storage. According to the literatures, blockchain technology helps all of these data management processes, most notably data security.

In terms of data security, blockchain is most frequently used to ensure data integrity, access control, and privacy preservation. These will have a number of benefits across a range of application domains, including those that incorporate both blockchain and IoT. As mentioned before, an IoT network is comprised of numerous and heterogeneous devices that generate large amounts of data; also, their network functions in both online and offline modes. As a result, systems developed for data management tasks must take these considerations into account. Additionally, the adoption of blockchain for data management purposes is motivated by a desire to compensate for the deficiencies of IoT in the aforementioned data management functions.

In healthcare, blockchain-based data management is designed to provide patients authority over their data. Their empowerment enables individuals to control who has access to their data and to track who has accessed it. Additionally, blockchain technology improves the integrity, availability, access control, and preservation of privacy.

Acquiring data from the appropriate source is crucial to data management success. In this regard, the authors demonstrate that, in addition to the widely used technique of identifying objects and persons through their public key and pseudonym names, alternative means of authentication, such as voice recognition, have been used in blockchain-based systems. Additionally, it is noticed that architecturally assigning entities, such as management servers, are utilized for assigning unique IDs to objects and users.

In terms of data processing, smart contracts and the design of data-processing-friendly architecture have been employed. In this regard, it has been revealed that it is difficult to justify the number and purpose of smart contract usage, which explains why, as previously said, the number of smart contracts utilized in systems is inconsistent.

The reviewed literature indicates that the most frequently used strategy for assuring data integrity is to encrypt data prior to hashing it, or vice versa. Moreover, third-party systems such as IPFS, Argon2, and Chainpoint are used to produce unique identifiers, form a digital signature, and generate data structures. These techniques and applications are unrelated to the area of the application.

There is no single dominating strategy for access control and privacy preservation that has been widely adopted by a significant number of authors. However, due to their certificate authority and multi-signature provisioning capabilities, established blockchain platforms such as Hyperledger and NEM are being used for access control. In some works, on the other hand, access control is believed to be managed structurally, for example, by allocating access control tasks to selected participant nodes. On the other hand, there is a publication that demonstrates how to utilize a decoder to ensure compatibility between multiple access control models.

Meanwhile, many encryption techniques such as proxy re-encryption with blinding, attribute-based re-encryption, and pseudonym-based encryption with multiple authorities are considered to maintain privacy preservation. Certain encryption techniques are also employed to ensure the integrity, access control, and privacy of a single system. In this regard [91], for example, combines ring signatures, addition rotation, and XOR with public encryption to accomplish all three goals.

To protect privacy, some authors employ architectural strategies such as segmenting the network into “sidechains,” while another publication establishes a hierarchy of blockchains at the local and global levels. This kind of clustering minimizes the danger of identification and transaction exposure beyond the cluster bounds. Additional techniques are applied to bolster the architectural solutions. Generally, no discernible pattern has evolved in this direction. The figure below, Fig. 4, illustrates the taxonomy of data security methods in general.

The other data management activities are dissemination and retrieval. This review’s application domains include smart transportation, which is one of the dissemination-based applications. The common mechanism in this area is a method called trigger but publications differ in the architecture they follow. On top of disseminating data from a vehicle to a vehicle, some authors include the dissemination of data from infrastructure to vehicles as well. In other publications, hybrids of pull and push data dissemination methods are being employed. In all these dissemination methods blockchain plays a differing role depending on the integration method followed. Regarding data retrieval, the majority of the publications don’t explicitly specify the data retrieval methods that should be employed on data stored on and off-chain. However, many applicable ways of data retrieval methods are compatible with blockchain.

Regarding data storage, which is heavily influenced by the method of integration chosen, legal requirements, data size, throughput, and latency demanded from a system, the application area a system is intended to be employed, and the number of participants of a blockchain system. Therefore, the three integration methods discussed above have a direct bearing on the placement and type of data maintained in the system. It is observed that literatures solve these issues by following appropriate integration methods, and by creatively designing architectures that take those concerns into consideration.

6. Open issues

An examination of the literature reveals some unresolved issues that require attention. Additionally, it is clear from the explanations provided in the publications and the analysis conducted on them that in the two application areas, a set of factors dictate the integration methods and data management activities. These include the legal requirements imposed on an application area, the intended use of a system, the number of IoT devices involved, the architecture chosen, the application area itself, the sensitivity of data, and the required throughput and latency. The inre-relationships between the usage areas and their determinant factors is presented in Fig. 5.

The examined researches develop instantiations within the confines of those influencing criteria. Despite the fact that these publications had several remarkable solutions, there are some concerns they did not address and there are inconsistencies between them about specific themes, such as the following.

To begin, the numerous instantiations mentioned here strive to establish the prototype’s superiority over other comparable solutions that they believe are related to resolving the problem at hand. However, when doing this review, the author observed inconsistencies between them, such that what one publication considers a strength is shown as a flaw in another publication. As a result, a review is necessary that focuses on comparing the performance of these different types of instantiations.

Second, data processing is listed as a data management operation in the preceding sections. In blockchain-based systems, more autonomous processing capacity is provided by smart contracts. However, it has been discovered that the number of smart contracts employed in such systems varies. As such use may have an effect on system performance, research examining the number of smart contracts that are suitable for use on systems can serve as a foundation for future work.

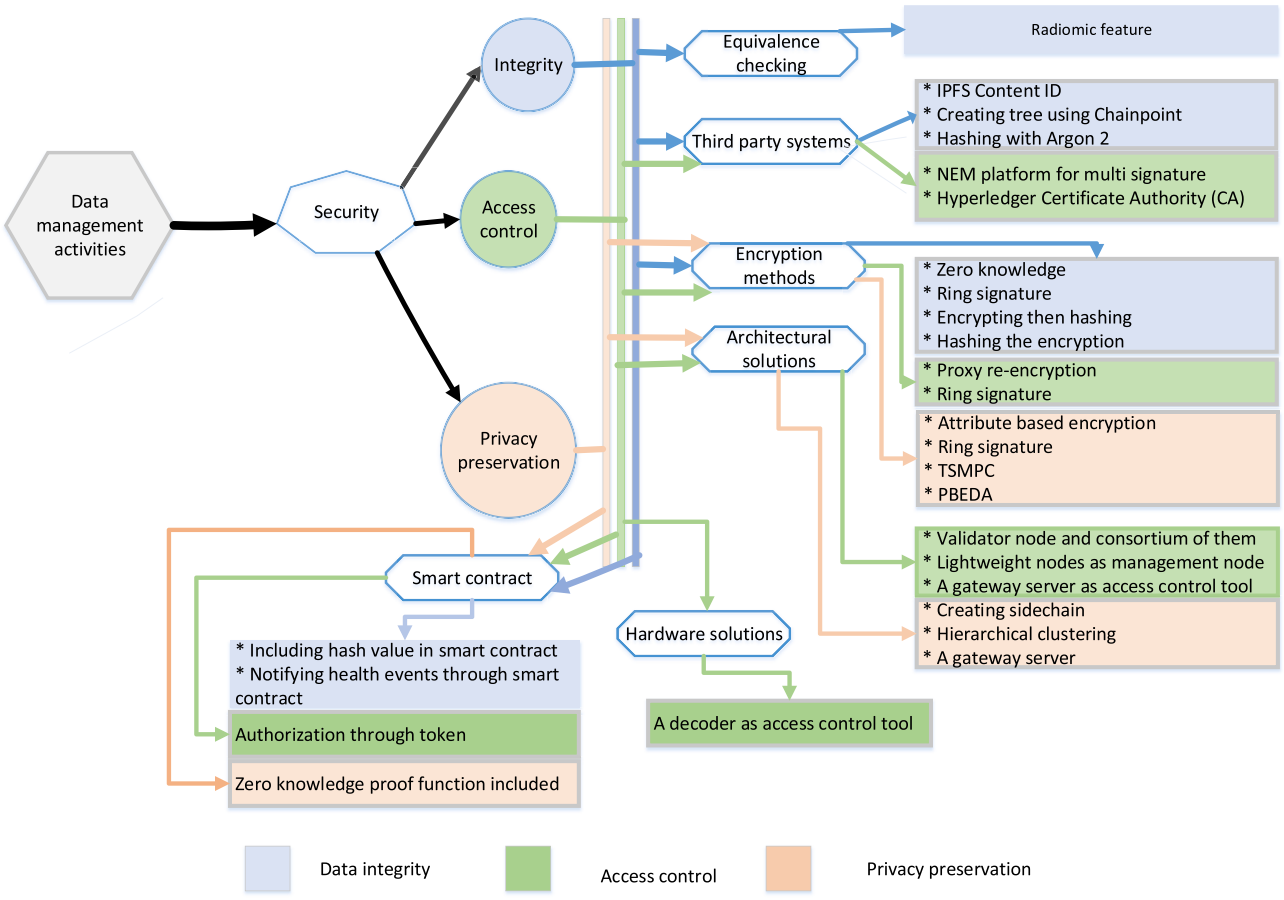

Fig. 4. Classification of the major data security methods employed in blockchain systems.

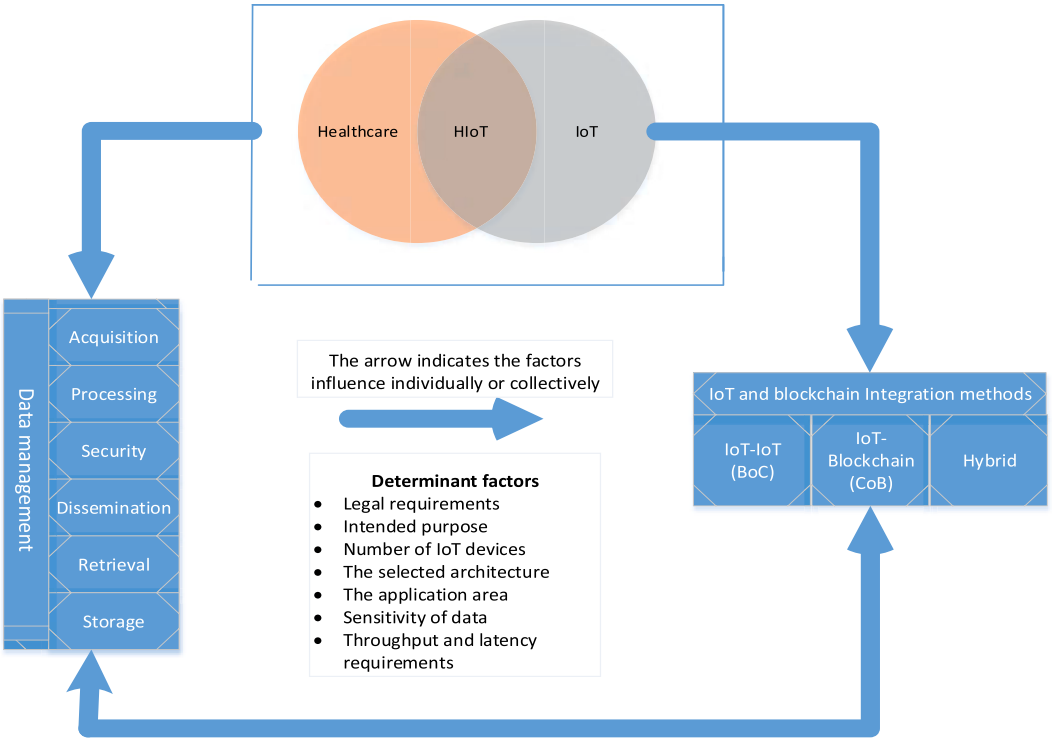

Fig. 5. The inter-relationships between the usage areas and their determinant factors.

Third, the bulk of articles does not define how data should be retrieved. Due to the intricacy of data retrieval in blockchain-based systems, retrieval may occur on- or off-chain. Additionally, image files are encrypted and stored on-chain in healthcare. Data retrieval from encrypted files, including the usage of searchable encrypted image files, may be essential in such instances. However, research in this field is stagnant. As a result, this field requires additional research.

Fourth, is the disintegrative use of HIT, which is caused, among other things, by the lack of a trustworthy technique for assigning unique IDs. In this sense, one of the characteristics of blockchain is that it can help solve such a problem; yet, it is uncommon to come across literature that uses blockchain to integrate disparate healthcare systems. Thus, integrative HIT utilization has a beneficial effect on the domain; these issues can be viewed as a solution to a long-standing problem.

Fifth, there are further challenges, such as how blockchain can be used to monitor patients, triage, providers' operational and financial performance, and disease spread surveillance, that has received scant attention in publications but require additional investigation.

7. Conclusion

This review examines how the selected publications leverage blockchain technology to streamline data management activities and how they integrate blockchain with IoT. Furthermore, in addition to examining the presence of trends in developing instantiations, the article demonstrates the benefits of adopting blockchain in subsets of the two domains, namely smart cities and drug supply chains. The preceding observations allow us to deduce the following.

Blockchain technology has the potential to significantly improve a variety of application areas within a smart city. This includes enabling self-management of energy consumption and trade in conjunction with smart utilities. Additionally, it facilitates real-time information exchange and improves traffic-related performance in the context of smart transportation applications through a reward system that is demonstrated with designed instantiations. Similarly, blockchain technology can assist in combating counterfeiting, sub-standardization and diversion through increasing transparency throughout the drug supply chain.

The primary application of blockchain is for data management. The premise that blockchain can manage heterogeneous big data prevent a single point of failure, and function with encrypted data both online and offline is driving the adoption of blockchain for data management. To determine whether these objectives have been met, several publications focusing on data management activities such as data acquisition, processing, security, distribution, retrieval, and storage have been assessed.

As a result, it is learned that the primary focus of the literatures is data security, which includes three components: data integrity, access control, and privacy preservation. Through the use of blockchain technology, a variety of ways are being used to enhance these areas. The strategies employed for those topics are classified into the following six categories: Equivalence verification, the usage of third-party systems, encryption techniques, architectural methods, a hardware solution, and smart contracts. From them, the most frequently used strategies include the use of various encryption technologies, third-party solutions, architectural designs, and smart contracts.

Other data management tasks, such as data acquisition, benefit from the authentication enhancement capabilities of blockchain-based systems. Various authentication methods have been reported to be applied, ranging from biological mechanisms to public-key encryption schemes. This means that independent of the application domain, a variety of decentralized autonomous authentication procedures for blockchain-based systems can be developed. Similarly, one of the benefits of blockchain for data processing is the revival of smart contracts, which were available before the widespread use of blockchain but were not widely used as a data processing tool. However, blockchain-based systems leverage it for a range of activities, including autonomous data processing.

Dissemination and retrieval of data are the least targeted tasks in data management. Nonetheless, numerous authors present the dissemination mechanisms employed in their instantiations in an unambiguous manner. It is learned that the majority of dissemination mechanisms are based on publish and subscribe, hierarchical structures, and trigger-based one-to-many and many-to-many procedures. However, despite the fact that blockchain adoption has an effect on data retrieval processes, the literatures do not discuss or address data retrieval methods to be used in blockchain-based systems.

Alternatively, it is recognized that a large number of variables have a significant impact on data storage. To circumvent these obstacles, designers employ solutions such as creating a data lake, preserving only file locations, and registering a list of files. To address legal problems, developers customize their systems to conform to the applicable legal standards.

By and large, data management tasks and integration approaches are inextricably linked. In this regard, the three approaches to integrating blockchain and IoT are diverse in terms of the complexity introduced to data management. This is because metadata management is required in addition to data management. However, when (a) file size increases, (b) regulation is strict, (c) the number of participants is large, (d) data sensitivity is subtle, and (e) throughput and latency requirements are high, designers opt for IoT-IoT (BoC) and hybrid integration approaches. This is a prevalent trend in both healthcare and the Internet of Things.

8. Limitations

As with any research, this review is not without limits. To begin, it is subject to publication bias due to the scarcity of literatures reporting negative outcomes associated with the use of blockchain, with the exception of some, such as [121], which rejects the use of blockchain for assigning unique IDs to patients, and [32], which casts doubt on the usability of blockchain for large-scale purposes due to the disadvantages associated with data processing activities. Similarly, while many advocates for the use of blockchain to boost security [166], discusses the security issues associated with blockchain-based systems designed utilizing Proof of Work (PoW) and Proof of Stake (PoS) consensus techniques. Despite this, publications suggest prototypes and solutions and advocate for blockchain's benefits. As a result, the review is influenced by a lack of negative reporting and exaggerated claims about positive research outcomes in the form of instantiations with an uncertain future.

Second, independent of the reputation of the journals in which they are published or the conferences at which they are presented, this review assigns equal weight to all literature that meets the screening requirements. However, the majority of blockchain-related noble publications are presented as white papers, which are disqualified. This has an effect on the unintentional exclusion of valuable publications.

Declaration of competing interest

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

References

[1] Aste T, Tasca P, Di Matteo T. Blockchain technologies: the foreseeable impact on society and industry. Computer 2017;50(9):18–28. https://doi.org/10.1109/MC.2017.3571064.

[2] P. De Filippi, M. Mannan, and W. Reijers, "Blockchain as a confidence machine: the problem of trust & challenges of governance," Technol Soc, vol. 62, p. 101284, Aug. 2020, doi: 10.1016/j.techsoc.2020.101284.

[3] Swan M. Blockchain: blueprint for a new economy. first ed. Beijing: Sebastopol, CA: O'Reilly; 2015.

[4] Eberhardt J, Tai S. On or off the blockchain? Insights on off-chaining computation and data. In: De Paoli F, Schulte S, Broch Johnsen E, editors. Service-Oriented and Cloud Computing, vol. 10465. Cham: Springer International Publishing; 2017. p. 3–15. https://doi.org/10.1007/978-3-319-67262-5_1.

[5] Kohli R. Electronic health records: how can IS researchers contribute to transforming healthcare? MIS Q 2016;40(3):553–73. https://doi.org/10.25300/MISQ/2016/40.3.02. Mar.

[6] Roman-Belmonte JM, De la Corte-Rodriguez H, Rodriguez-Merchan EC. How blockchain technology can change medicine. Postgrad Med 2018;130(4):420–7. https://doi.org/10.1080/00325481.2018.1472996.

[7] Angraal S, Krumholz HM, Schulz WL. Blockchain technology: applications in health care. Circ Cardiovasc Qual Outc 2017;10(9). https://doi.org/10.1161/CIRCOUTCOMES.117.003800.

[8] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," J Am Med Inf Assoc, vol. 24, no. 6, pp. 1211–1220, Nov. 2017, doi: 10.1093/jamia/ocx068.

[9] M. Andoni et al., "Blockchain technology in the energy sector: a systematic review of challenges and opportunities," Renew Sustain Energy Rev, vol. 100, pp. 143–174, Feb. 2019, doi: 10.1016/j.rser.2018.10.014.

[10] Conoscenti M, Vetro A, De Martin JC. Blockchain for the Internet of Things: a systematic literature review. In: *Proceedings of the 13th International Conference of Computer Systems and Applications (AICCSA)*, Agadir, Morocco; 2016. p. 1–6. https://doi.org/10.1109/AICCSA.2016.7945805.

[11] Khan MA, Salah K. IoT security: review, blockchain solutions, and open challenges. Future Generat Comput Syst 2018;82:395–411. https://doi.org/10.1016/j.future.2017.11.022.

[12] Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo K-KR. A systematic literature review of blockchain cyber security. Digit Commun Netw 2019. https://doi.org/10.1016/j.dcan.2019.01.005. S2352864818301536.

[13] Hölbl M, Kompara M, Kamišalić A, Nemec Zlatolas L. A systematic review of the use of blockchain in healthcare. Symmetry 2018;10(10):470. https://doi.org/10.3390/sym10100470.

[14] Fernandez-Carames TM, Fraga-Lamas P. A review on the use of blockchain for the internet of things. IEEE Access 2018;6:32979–3001. https://doi.org/10.1109/ACCESS.2018.2842685.

[15] Yli-Huumo J, Ko D, Choi S, Park S, Smolander K. Where is current research on blockchain technology?—a systematic review. PLoS One 2016;11(10):e0163477. https://doi.org/10.1371/journal.pone.0163477.

[16] Kuo T-T, Zavaleta Rojas H, Ohno-Machado L. Comparison of blockchain platforms: a systematic review and healthcare examples. J Am Med Inf Assoc 2019;26(5):462–78. https://doi.org/10.1093/jamia/ocy185.

[17] Mayer AH, da Costa CA, Righi R da R. Electronic health records in a Blockchain: a systematic review. Health Inf J 2019. https://doi.org/10.1177/1460458219866350. 146045821986635.

[18] S. Miau and J.-M. Yang, "Bibliometrics-based evaluation of the Blockchain research trend: 2008 – march 2017," Technol Anal Strat Manag, vol. 30, no. 9, pp. 1029–1045, Sep. 2018, doi: 10.1080/09537325.2018.1434138.

[19] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: current status, classification and open issues," Telematics Inf, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.

[20] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering – a systematic literature review," Inf Software Technol, vol. 51, no. 1, pp. 7–15, Jan. 2009, doi: 10.1016/j.infsof.2008.09.009.

[21] Larsen KR, Bong CH. A tool for addressing construct identity in literature reviews and meta-analyses. MIS Q 2016;40(3):529–51. https://doi.org/10.25300/MISQ/2016/40.3.01. Mar.

[22] Tate M, Furtmueller E, Evermann J, Bandara W. Introduction to the special issue: the literature review in information systems. Commun Assoc Inf Syst 2015;37. https://doi.org/10.17705/1CAIS.03705.

[23] Gregor S, Hevner AR. Positioning and presenting design science research for maximum impact. MIS Q 2013;37(2):337–55. https://doi.org/10.25300/MISQ/2013/37.2.01.

[24] Hargadon AB. Brokering knowledge: linking learning and innovation. Res Organ Behav 2002;24:41–85. https://doi.org/10.1016/S0191-3085(02)24003-4. Jan.

[25] Ducas E, Wilner A. The security and financial implications of blockchain technologies: regulating emerging technologies in Canada. Int J Can J Glob Pol Anal 2017;72(4):538–62. https://doi.org/10.1177/0020702017741909.

[26] Hammi MT, Hammi B, Bellot P, Serhrouchni A. Bubbles of Trust: a decentralized blockchain-based authentication system for IoT. Comput Secur 2018;78:126–42. https://doi.org/10.1016/j.cose.2018.06.004.

[27] Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain Cities Soc 2018;39:283–97. https://doi.org/10.1016/j.scs.2018.02.014.

[28] Danzi P, Kalor AE, Stefanovic C, Popovski P. Analysis of the communication traffic for blockchain synchronization of IoT devices. In: 2018 IEEE International Conference on Communications (ICC); 2018. p. 1–7. https://doi.org/10.1109/ICC.2018.8422485. Kansas City, MO, May.

[29] Qiu T, Zhang R, Gao Y. Ripple vs. SWIFT: transforming cross border remittance using blockchain technology. Procedia Comput Sci 2019;147:428–34. https://doi.org/10.1016/j.procs.2019.01.260.

[30] Kleinaki A-S, Mytis-Gkometh P, Drosatos G, Efraimidis PS, Kaldoudi E. A blockchain-based notarization service for biomedical knowledge retrieval. Comput Struct Biotechnol J 2018;16:288–97. https://doi.org/10.1016/j.csbj.2018.08.002.

[31] S. Kamble, A. Gunasekaran, and H. Arha, "Understanding the Blockchain technology adoption in supply chains-Indian context," Int J Prod Res, vol. 57, no. 7, pp. 2009–2033, Apr. 2019, doi: 10.1080/00207543.2018.1518610.

[32] Dinh TTA, Liu R, Zhang M, Chen G, Ooi BC, Wang J. Untangling blockchain: a data processing view of blockchain systems. IEEE Trans Knowl Data Eng 2018;30(7):1366–85. https://doi.org/10.1109/TKDE.2017.2781227.

[33] Dinh TTA, Wang J, Chen G, Liu R, Ooi BC, Tan K-L. BLOCKBENCH: a framework for analyzing private blockchains. In: Proceedings of the 2017 ACM International Conference on Management of Data; 2017. p. 1085–100. https://doi.org/10.1145/3035918.3064033. Chicago Illinois USA.

[34] Croman K, et al. On scaling decentralized blockchains: (A position paper). In: Clark J, Meiklejohn S, Ryan PYA, Wallach D, Brenner M, Rohloff K, editors. Financial Cryptography and Data Security, vol. 9604. Berlin, Heidelberg: Springer Berlin Heidelberg; 2016. p. 106–25. https://doi.org/10.1007/978-3-662-53357-4_8.

[35] Lv Q, Cao P, Cohen E, Li K, Shenker S. Search and replication in unstructured peer-to-peer networks. In: Proceedings of the 16th international conference *on* Supercomputing - ICS '02; 2002. p. 84. https://doi.org/10.1145/514191.514206. New York, New York, USA.

[36] Min E, Guo X, Liu Q, Zhang G, Cui J, Long J. A survey of clustering with deep learning: from the perspective of network architecture. IEEE Access 2018;6:39501–14. https://doi.org/10.1109/ACCESS.2018.2855437.

[37] Das SK, Ammari HM. Routing and data dissemination. In: Zheng J, Jamalipour A, editors. Wireless Sensor Networks. Hoboken, NJ, USA: John Wiley & Sons, Inc.; 2009. p. 67–143. https://doi.org/10.1002/9780470443521.ch4.

[38] Ølnes S, Ubacht J, Janssen M. Blockchain in government: benefits and implications of distributed ledger technology for information sharing. Govern Inf Q 2017;34(3):355–64. https://doi.org/10.1016/j.giq.2017.09.007.

[39] Zhou L, Wang L, Sun Y, Lv P. BeeKeeper: a blockchain-based IoT system with secure storage and homomorphic computation. IEEE Access 2018;6:43472–88. https://doi.org/10.1109/ACCESS.2018.2847632.

[40] Cachin C, Vukolić M. Blockchain Consensus Protocols in the Wild. ArXiv170701873 Cs; 2017. Dec. 26, 2021. [Online]. Available: http://arxiv.org/abs/1707.01873.

[41] Xiao Y, Zhang N, Lou W, Hou YT. A survey of distributed consensus protocols for blockchain networks. IEEE Commun Surv Tutor 2020;22(2):1432–65. https://doi.org/10.1109/COMST.2020.2969706.

[42] Peters GW, Panayi E. Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money. In: Tasca P, Aste T, Pelizzon L, Perony N, editors. Banking Beyond Banks and Money. Cham: Springer International Publishing; 2016. p. 239–78. https://doi.org/10.1007/978-3-319-42448-4_13.

[43] Zyskind G, Nathan O. A. "Sandy" Pentland, "decentralizing privacy: using blockchain to protect personal data. In: 2015 IEEE Security and Privacy Workshops; 2015. p. 180–4. https://doi.org/10.1109/SPW.2015.27. San Jose, CA.

[44] Huang B, Liu Z, Chen J, Liu A, Liu Q, He Q. Behavior pattern clustering in blockchain networks. Multimed Tool Appl 2017;76(19):20099–110. https://doi.org/10.1007/s11042-017-4396-4.

[45] Berendea N, Mercier H, Onica E, Riviere E. Fair and efficient gossip in hyperledger fabric. In: 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS); 2020. p. 190–200. https://doi.org/10.1109/ICDCS47774.2020.00027. Singapore, Singapore, Nov.

[46] European Commission - Information Society and Media DG. Internet of things: strategic research roadmap. Sep. 15. 2009. May 07, 2019. [Online]. Available: http://europa.eu/information_society.

[47] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: the challenges, and a way forward," J Netw Comput Appl, vol. 125, pp. 251–279, Jan. 2019, doi: 10.1016/j.jnca.2018.10.019.

[48] Minoli D, Occhiogrosso B. Blockchain mechanisms for IoT security. Internet Things 2018;1–2:1–13. https://doi.org/10.1016/j.iot.2018.05.002.

[49] Jose DV, Vijyalakshmi A. An overview of security in internet of things. Procedia Comput Sci 2018;143:744–8. https://doi.org/10.1016/j.procs.2018.10.439.

[50] Sadique KM, Rahmani R, Johannesson P. Towards security on internet of things: applications and challenges in technology. Procedia Comput Sci 2018;141:199–206. https://doi.org/10.1016/j.procs.2018.10.168.

[51] Suo H, Wan J, Zou C, Liu J. Security in the internet of things: a review. In: 2012 International Conference on Computer Science and Electronics Engineering; 2012. p. 648–51. https://doi.org/10.1109/ICCSEE.2012.373. Hangzhou, Zhejiang, China, Mar.

[52] Pustišek M, Kos A. Approaches to front-end IoT application development for the Ethereum blockchain. Procedia Comput Sci 2018;129:410–9. https://doi.org/10.1016/j.procs.2018.03.017.

[53] Atlam HF, Alenezi A, Alassafi MO, Wills GB. Blockchain with internet of things: benefits, challenges, and future directions. Int J Intell Syst Appl 2018;10(6):40–8. https://doi.org/10.5815/ijisa.2018.06.05.

[54] Hahm O, Baccelli E, Petersen H, Tsiftes N. Operating systems for low-end devices in the internet of things: a survey. IEEE Internet Things J 2016;3(5):720–34. https://doi.org/10.1109/JIOT.2015.2505901.

[55] Chaudhry B, et al. Systematic review: impact of health information technology on quality, efficiency, and costs of medical care. Ann Intern Med 2006;144(10):742. https://doi.org/10.7326/0003-4819-144-10-200605160-00125.

[56] M. B. Buntin, M. F. Burke, M. C. Hoaglin, and D. Blumenthal, "The benefits of health information technology: a review of the recent literature shows predominantly positive results," Health Aff (Millwood), vol. 30, no. 3, pp. 464–471, Mar. 2011, doi: 10.1377/hlthaff.2011.0178.

[57] Bernardi R, Sarker S, Sahay S. The role of affordances in the dis-institutionalization of a dysfunctional health management information system in

Kenya: an identity work perspective. MIS Q 2019;43(4):1177–200. https://doi.org/10.25300/MISQ/2019/14187.
[58] Karahanna E, Adela C, Liu QB, Serrano C. Capitalizing on health information technology to enable advantage in U.S. Hospitals. MIS Q 2019;43(1):113–40. https://doi.org/10.25300/MISQ/2019/12743.
[59] Baker SB, Xiang W, Atkinson I. Internet of things for smart healthcare: technologies, challenges, and opportunities. IEEE Access 2017;5:26521–44. https://doi.org/10.1109/ACCESS.2017.2775180.
[60] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): a vision, architectural elements, and future directions. Future Generat Comput Syst 2013; 29(7):1645–60. https://doi.org/10.1016/j.future.2013.01.010.
[61] Vest JR, Gamm LD. Health information exchange: persistent challenges and new strategies: table. J Am Med Inf Assoc 2010;17(3):288–94. https://doi.org/10.1136/jamia.2010.003673.
[62] Payton F, Pare G, Le Rouge C, Reddy M. Health care IT: process, people, patients and interdisciplinary considerations. J Assoc Inf Syst Online 2011;12(2):I–XIII. https://doi.org/10.17705/1jais.00259. Feb.
[63] R. G. Fichman, R. Kohli, and R. Krishnan, Eds., "**Editorial overview** —the role of information systems in healthcare: current research and future trends," Inf Syst Res, vol. 22, no. 3, pp. 419–428, Sep. 2011, doi: 10.1287/isre.1110.0382.
[64] Kwon J, Johnson ME. Meaningful healthcare security Does meaningful attestation improve information security performance. MIS Q 2018;42(4):1043–67. https://doi.org/10.25300/MISQ/2018/13580.
[65] Bao C, Bardhan IR, Singh H, Meyer BA, Kirksey K. Patient-provider engagement and its impact on health outcomes: a longitudinal study of patient portal use. MIS Q 2020;44(2):699–723. https://doi.org/10.25300/MISQ/2020/14180.
[66] Gordon WJ, Catalini C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Comput Struct Biotechnol J 2018;16: 224–30. https://doi.org/10.1016/j.csbj.2018.06.003.
[67] Efanov D, Roschin P. The all-pervasiveness of the blockchain technology. Procedia Comput Sci 2018;123:116–21. https://doi.org/10.1016/j.procs.2018.01.019.
[68] Webster J, Watson RT. Analyzing the past to prepare for the future: writing a literature review. MIS Q 2002;26(2):xiii–xxii.
[69] Boell SK, Cecez-Kecmanovic D. A hermeneutic approach for conducting literature reviews and literature searches. Commun Assoc Inf Syst 2014;34. https://doi.org/10.17705/1CAIS.03412.
[70] Bandara W, Furtmueller E, Gorbacheva E, Miskon S, Beekhuyzen J. Achieving rigor in literature reviews: insights from qualitative data analysis and tool-support. Commun Assoc Inf Syst 2015;37. https://doi.org/10.17705/1CAIS.03708.
[71] Levy Y, Ellis TJ. A systems approach to conduct an effective literature review in support of information systems research. Info Sci Int J Emerg Transdiscipl 2006;9: 181–212. https://doi.org/10.28945/479.
[72] Hevner AR, March ST, Park J, Ram S. Design science in information systems research. MIS Q 2004;28(1):75–105. Mar. http://misq.org/design-science-in-information-systems-research.html?SID=shpier0675mhpes3hkfagcqee1.
[73] Hoy MB. An introduction to the blockchain and its implications for libraries and medicine. Med Ref Serv Q 2017;36(3):273–9. https://doi.org/10.1080/02763869.2017.1332261.
[74] Zhang P, Walker MA, White J, Schmidt DC, Lenz G. Metrics for assessing blockchain-based healthcare decentralized apps. In: 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom). Dalian; 2017. p. 1–4. https://doi.org/10.1109/HealthCom.2017.8210842.
[75] Engelhardt MA. Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector. Technol Innov Manag Rev 2017;7(10):22–34. https://doi.org/10.22215/timreview/1111.
[76] Pahl C, El Ioini N, Helmer S. A decision framework for blockchain platforms for IoT and edge computing. In: Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security. Madeira, Portugal: Funchal; 2018. p. 105–13. https://doi.org/10.5220/0006688601050113.
[77] Esposito C, De Santis A, Tortora G, Chang H, Choo K-KR. Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput 2018;5 (1):31–7. https://doi.org/10.1109/MCC.2018.011791712. Jan.
[78] Novo O. Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J 2018;5(2):1184–95. https://doi.org/10.1109/JIOT.2018.2812239. Apr.
[79] Sharma PK, Singh S, Jeong Y-S, Park JH. DistBlockNet: a distributed blockchains-based secure SDN architecture for IoT networks. IEEE Commun Mag 2017;55(9): 78–85. https://doi.org/10.1109/MCOM.2017.1700041.
[80] Dorri A, Kanhere SS, Jurdak R. Towards an optimized BlockChain for IoT. In: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation - IoTDI '17; 2017. p. 173–8. https://doi.org/10.1145/3054977.3055003. Pittsburgh, PA, USA.
[81] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," Future Generat Comput Syst, vol. 88, pp. 173–190, Nov. 2018, doi: 10.1016/j.future.2018.05.046.
[82] Teslya N, Ryabchikov I. Blockchain-based platform architecture for industrial IoT. In: 2017 *21st* Conference of Open Innovations Association (FRUCT); 2017. p. 321–9. https://doi.org/10.23919/FRUCT.2017.8250199. Helsinki, Nov.
[83] Lombardi F, Aniello L, De Angelis S, Margheri A, Sassone V. A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids. London, UK. In: Living in the Internet of Things: Cybersecurity of the IoT - 2018; 2018. p. 42. https://doi.org/10.1049/cp.2018.0042.
[84] Rožman N, Vrabič R, Corn M, Požrl T, Diaci J. Distributed logistics platform based on Blockchain and IoT. Procedia CIRP 2019;81:826–31. https://doi.org/10.1016/j.procir.2019.03.207.
[85] Chakraborty RB, Pandey M, Rautaray SS. Managing computation load on a blockchain – based multi – layered internet – of – things network. Procedia Comput Sci 2018;132:469–76. https://doi.org/10.1016/j.procs.2018.05.146.
[86] Han Y, Park B, Jeong J. A novel architecture of air pollution measurement platform using 5G and blockchain for industrial IoT applications. Procedia Comput Sci 2019;155:728–33. https://doi.org/10.1016/j.procs.2019.08.105.
[87] Stanciu A. Blockchain based distributed control system for edge computing. In: 2017 *21st* International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania; 2017. p. 667–71. https://doi.org/10.1109/CSCS.2017.102.
[88] Sharma PK, Chen M-Y, Park JH. A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access 2018;6:115–24. https://doi.org/10.1109/ACCESS.2017.2757955.
[89] Vishal N, Kumaresan M, Abhishek N, Prasenjit B. A Fully Observable Supply Chain Management System Using Block Chain and IOT," presented at the 3rd International Conference for Convergence in Technology. I2CT); 2018. https://doi.org/10.1109/I2CT.2018.8529725.
[90] Miller D. Blockchain and the internet of things in the industrial sector. IT Prof 2018;20(3):15–8. https://doi.org/10.1109/MITP.2018.032501742.
[91] Dwivedi A, Srivastava G, Dhar S, Singh R. A decentralized privacy-preserving healthcare blockchain for IoT. Sensors 2019;19(2):326. https://doi.org/10.3390/s19020326.
[92] Brunese L, Mercaldo F, Reginelli A, Santone A. A blockchain based proposal for protecting healthcare systems through formal methods. Procedia Comput Sci 2019;159:1787–94. https://doi.org/10.1016/j.procs.2019.09.350.
[93] Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J Med Syst 2018;42(7):130. https://doi.org/10.1007/s10916-018-0982-x.
[94] 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). Montreal: QC; 2017. p. 1–5. https://doi.org/10.1109/PIMRC.2017.8292361.
[95] Rifi N, Agoulmine N, Chendeb Taher N, Rachkidi E. Blockchain technology: is it a good candidate for securing IoT sensitive medical data? Wireless Commun Mobile Comput 2018;2018:1–11. https://doi.org/10.1155/2018/9763937.
[96] Qu C, Tao M, Zhang J, Hong X, Yuan R. Blockchain based credibility verification method for IoT entities. Secur Commun Network 2018;2018:1–11. https://doi.org/10.1155/2018/7817614.
[97] Pinno OJA, Gregio ARA, De Bona LCE. ControlChain: blockchain as a central enabler for access control authorizations in the IoT. In: GLOBECOM 2017 - 2017 IEEE Global Communications Conference; 2017. p. 1–6. https://doi.org/10.1109/GLOCOM.2017.8254521. Singapore, Dec.
[98] Rahulamathavan Y, Phan RC-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); 2017. p. 1–6. https://doi.org/10.1109/ANTS.2017.8384164. Bhubaneswar, Dec.
[99] Hyeok L, Ki-Hyung K. Implementation of IoT system using block chain with authentication and data protection. Apr. 19, 2019. [Online]. Available: https://ieeexplore.ieee.org/servlet/opac?punumber=8337483; 2018.
[100] Pouraghily A, Islam MN, Kundu S, Wolf T. Poster abstract: privacy in blockchain-enabled IoT devices. In: 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI); 2018. p. 292–3. https://doi.org/10.1109/IoTDI.2018.00045. Orlando, FL.
[101] Ali MS, Dolui K, Antonelli F. IoT data privacy via blockchains and IPFS. In: Proceedings of the Seventh International Conference on the Internet of Things - IoT '17. Austria: Linz; 2017. p. 1–7. https://doi.org/10.1145/3131542.3131563.
[102] Banerjee M, Lee J, Choo K-KR. A blockchain future for internet of things security: a position paper. Digit Commun Netw 2018;4(3):149–60. https://doi.org/10.1016/j.dcan.2017.10.006.
[103] Badr S, Gomaa I, Abd-Elrahman E. Multi-tier blockchain framework for IoT-EHRs systems. Procedia Comput Sci 2018;141:159–66. https://doi.org/10.1016/j.procs.2018.10.162.
[104] Ouaddah A, Elkalam AA, Ouahman AA. Harnessing the power of blockchain technology to solve IoT security & privacy issues. In: Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing - ICC '17; 2017. p. 1–10. https://doi.org/10.1145/3018896.3018901. Cambridge, United Kingdom.
[105] Tselios C, Politis I, Kotsopoulos S. Enhancing SDN security for IoT-related deployments through blockchain. In: 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks. Berlin, Nov: NFV-SDN); 2017. p. 303–8. https://doi.org/10.1109/NFV-SDN.2017.8169860.
[106] Y. Qian et al., "Towards decentralized IoT security enhancement: a blockchain approach," Comput Electr Eng, vol. 72, pp. 266–273, Nov. 2018, doi: 10.1016/j.compeleceng.2018.08.021.
[107] Pal O, Alam B, Thakur V, Singh S. Key management for blockchain technology. ICT Express; 2019. https://doi.org/10.1016/j.icte.2019.08.002. S2405959519301894.
[108] Ulbricht M-R, Pallas F. YaPPL - a lightweight privacy preference language for legally sufficient and automated consent provision in IoT scenarios. In: Garcia-Alfaro J, Herrera-Joancomartí J, Livraga G, Rios R, editors. Data Privacy

Management, Cryptocurrencies and Blockchain Technology, vol. 11025. Cham: Springer International Publishing; 2018. p. 329–44. https://doi.org/10.1007/978-3-030-00305-0_23.
[109] S. L. Cichosz, M. N. Stausholm, T. Kronborg, P. Vestergaard, and O. Hejlesen, "How to use blockchain for diabetes health care data and access management: an operational concept," J Diabetes Sci Technol, vol. 13, no. 2, pp. 248–253, Mar. 2019, doi: 10.1177/1932296818790281.
[110] Patel V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Inf J 2018. https://doi.org/10.1177/1460458218769699. 146045821876969.
[111] Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST. FHIRChain: applying blockchain to securely and scalably share clinical data. Comput Struct Biotechnol J 2018;16:267–78. https://doi.org/10.1016/j.csbj.2018.07.004.
[112] Thwin TT, Vasupongayya S. Blockchain-based access control model to preserve privacy for personal health record systems. Secur Commun Network 2019:1–15. https://doi.org/10.1155/2019/8315614.
[113] Al Omar A, Rahman MS, Basu A, Kiyomoto S. MediBchain: a blockchain based privacy preserving platform for healthcare data. In: Wang G, Atiquzzaman M, Yan Z, Choo K-KR, editors. Security, Privacy, and Anonymity in Computation, Communication, and Storage, vol. 10658. Cham: Springer International Publishing; 2017. p. 534–43. https://doi.org/10.1007/978-3-319-72395-2_49.
[114] Wong DR, Bhattacharya S, Butte AJ. Prototype of running clinical trials in an untrustworthy environment using blockchain. Nat Commun Dec. 2019;10(1):917. https://doi.org/10.1038/s41467-019-08874-y.
[115] Zhang J, Xue N, Huang X. A secure system for pervasive social network-based healthcare. IEEE Access 2016;4:9239–50. https://doi.org/10.1109/ACCESS.2016.2645904.
[116] Liu B, Yu XL, Chen S, Xu X, Zhu L. Blockchain based data integrity service framework for IoT data. In: 2017 IEEE International Conference on Web Services. Honolulu, HI, USA, Jun: ICWS); 2017. p. 468–75. https://doi.org/10.1109/ICWS.2017.54.
[117] Ouaddah A, Elkalam AA, Ouahman AA. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In: Rocha Á, Serrhini M, Felgueiras C, editors. Europe and MENA Cooperation Advances in Information and Communication Technologies. vol. 520. Cham: Springer International Publishing; 2017. p. 523–33. https://doi.org/10.1007/978-3-319-46568-5_53.
[118] Rantos K, Drosatos G, Demertzis K, Ilioudis C, Papanikolaou A. Blockchain-based consents management for personal data processing in the IoT ecosystem. In: Proceedings of the 15th International Joint Conference on e-Business and Telecommunications. Porto, Portugal; 2018. p. 738–43. https://doi.org/10.5220/0006911007380743.
[119] Liang X, Zhao J, Shetty S, Li D. Towards data assurance and resilience in IoT using blockchain. In: Milcom 2017 - 2017 IEEE Military Communications Conference. Baltimore, MD: MILCOM); 2017. p. 261–6. https://doi.org/10.1109/MILCOM.2017.8170858.
[120] Lin J, Shen Z, Miao C. Using blockchain technology to build trust in sharing LoRaWAN IoT. In: Proceedings of the 2nd International Conference on Crowd Science and Engineering - ICCSE'17; 2017. p. 38–43. https://doi.org/10.1145/3126973.3126980. Beijing, China.
[121] Cheng EC, Le Y, Zhou J, Lu Y. Healthcare services across China – on implementing an extensible universally unique patient identifier system. Int J Healthc Manag 2018;11(3):210–6. https://doi.org/10.1080/20479700.2017.1398388.
[122] Sun J, Yan J, Zhang KZK. Blockchain-based sharing services: what blockchain technology can contribute to smart cities. Financ Innov 2016;2(1):26. https://doi.org/10.1186/s40854-016-0040-y.
[123] Lazaroiu C, Roscia M. Smart district through IoT and blockchain. In: 2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA); 2017. p. 454–61. https://doi.org/10.1109/ICRERA.2017.8191102. San Diego, CA, Nov.
[124] Yuan Y, Wang F-Y. Towards blockchain-based intelligent transportation systems. In: 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC); 2016. p. 2663–8. https://doi.org/10.1109/ITSC.2016.7795984. Rio de Janeiro, Brazil, Nov.
[125] Sharma PK, Park JH. Blockchain based hybrid network architecture for the smart city. Future Generat Comput Syst 2018;86:650–5. https://doi.org/10.1016/j.future.2018.04.060.
[126] M. Singh and S. Kim, "Branch based blockchain technology in intelligent vehicle," Comput Network, vol. 145, pp. 219–231, Nov. 2018, doi: 10.1016/j.comnet.2018.08.016.
[127] Alladi T, Chamola V, Rodrigues JJPC, Kozlov SA. Blockchain in smart grids: a review on different use cases. Sensors 2019;19(22):4862. https://doi.org/10.3390/s19224862.
[128] Singh S, Ra I-H, Meng W, Kaur M, Cho GH, Sh-BlockCC. A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. Int J Distributed Sens Netw 2019;15(4). https://doi.org/10.1177/1550147719844159. 155014771984415.
[129] Awais Hassan M, Habiba U, Ghani U, Shoaib M. A secure message-passing framework for inter-vehicular communication using blockchain. Int J Distributed Sens Netw 2019;15(2). https://doi.org/10.1177/1550147719829677. 155014771982967.
[130] Mackey TK, Nayyar G. A review of existing and emerging digital technologies to combat the global trade in fake medicines. Expet Opin Drug Saf 2017;16(5):587–602. https://doi.org/10.1080/14740338.2017.1313227.
[131] Vruddhula S. Application of on-dose identification and blockchain to prevent drug counterfeiting. Pathog Glob Health 2018;112(4):161. https://doi.org/10.1080/20477724.2018.1503268.
[132] Clauson KA, Breeden EA, Davidson C, Mackey TK. Leveraging blockchain technology to enhance supply chain management in healthcare. Blockchain Healthc Today Mar 2018. https://doi.org/10.30953/bhty.v1.20.
[133] Tseng J-H, Liao Y-C, Chong B, Liao S. Governance on the drug supply chain via gcoin blockchain. Int J Environ Res Publ Health 2018;15(6):1055. https://doi.org/10.3390/ijerph15061055.
[134] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: machine-to-machine electricity market," Appl Energy, vol. 195, pp. 234–246, Jun. 2017, doi: 10.1016/j.apenergy.2017.03.039.
[135] Gai K, Choo K-KR, Zhu L. Blockchain-enabled reengineering of cloud datacenters. IEEE Cloud Comput 2018;5(6):21–5. https://doi.org/10.1109/MCC.2018.064181116. Nov.
[136] Niu J, Shu L, Zhou Z, Zhang Y. Mobile sensing and data management for sensor networks. Int J Distributed Sens Netw 2013;9(9):898169. https://doi.org/10.1155/2013/898169.
[137] Lee I. Big data: dimensions, evolution, impacts, and challenges. Bus Horiz 2017;60(3):293–303. https://doi.org/10.1016/j.bushor.2017.01.004.
[138] Ma Y, et al. An efficient index for massive IOT data in cloud environment. In: Proceedings of the 21st ACM international conference on Information and knowledge management - CIKM '12. Hawaii, USA: Maui; 2012. p. 2129. https://doi.org/10.1145/2396761.2398587.
[139] M. Abu-Elkheir, M. Hayajneh, and N. Ali, "Data management for the internet of things: design primitives and solution," Sensors, vol. 13, no. 11, pp. 15582–15612, Nov. 2013, doi: 10.3390/s131115582.
[140] Ijaz A, et al. Enabling massive IoT in 5G and beyond systems: PHY radio frame design considerations. IEEE Access 2016;4:3322–39. https://doi.org/10.1109/ACCESS.2016.2584178.
[141] Sivathanu G, Wright CP, Zadok E. Ensuring data integrity in storage: techniques and applications. In: Proceedings of the 2005 ACM workshop on Storage security and survivability - StorageSS '05; 2005. p. 26. https://doi.org/10.1145/1103780.1103784. Fairfax, VA, USA.
[142] Menezes AJ, Van Oorschot PC, Vanstone SA. Handbook of applied cryptography. Boca Raton: CRC Press; 1997.
[143] A. Ouaddah, H. Mousannif, A. Abou Elkalam, and A. Ait Ouahman, "Access control in the Internet of Things: big challenges and new opportunities," Comput Network, vol. 112, pp. 237–262, Jan. 2017, doi: 10.1016/j.comnet.2016.11.007.
[144] Maw H, Xiao H, Christianson B, Malcolm J. A survey of access control models in wireless sensor networks. J Sens Actuator Netw 2014;3(2):150–80. https://doi.org/10.3390/jsan3020150.
[145] Zhang R, Zhang Y, Ren K. DP^{2}AC: distributed privacy-preserving access control in sensor networks. In: *Ieee INFOCOM 2009 - The 28th Conference on Computer Communications*, Rio De Janeiro, Brazil; 2009. p. 1251–9. https://doi.org/10.1109/INFCOM.2009.5062039.
[146] He D, Bu J, Zhu S, Chan S, Chen C. Distributed access control with privacy support in wireless sensor networks. IEEE Trans Wireless Commun 2011;10(10):3472–81. https://doi.org/10.1109/TWC.2011.072511.102283.
[147] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks: a state-of-the-art survey," Ad Hoc Netw., vol. 7, no. 8, pp. 1501–1514, Nov. 2009, doi: 10.1016/j.adhoc.2009.04.009.
[148] Bernal Bernabe J, Canovas JL, Hernandez-Ramos JL, Torres Moreno R, Skarmeta A. Privacy-preserving solutions for blockchain: review and challenges. IEEE Access 2019;7:164908–40. https://doi.org/10.1109/ACCESS.2019.2950872.
[149] Franklin MJ, Zdonik SB. Dissemination-based information systems. IEEE Data Eng. Bull. 1996;19(3):20–30.
[150] Al-Karaki JN, Kamal AE. Routing techniques in wireless sensor networks: a survey. IEEE Wirel Commun 2004;11(6):6–28. https://doi.org/10.1109/MWC.2004.1368893.
[151] Dawn Xiaoding Song, Wagner D, Perrig A. Practical techniques for searches on encrypted data. In: Proceeding 2000 IEEE Symposium on Security and Privacy. Berkeley, CA, USA: S&P 2000; 2000. p. 44–55. https://doi.org/10.1109/SECPRI.2000.848445.
[152] Swaminathan A, et al. Confidentiality-preserving rank-ordered search. In: Proceedings of the 2007 ACM workshop on Storage security and survivability - StorageSS '07; 2007. p. 7. https://doi.org/10.1145/1314313.1314316. Alexandria, Virginia, USA.
[153] Lu W, Swaminathan A, Varna AL, Wu M. Enabling search over encrypted multimedia databases. 2009. p. 725418. https://doi.org/10.1117/12.806980.
[154] Ferreira B, Rodrigues J, Leitao J, Domingos H. Privacy-preserving content-based image retrieval in the cloud. In: 2015 IEEE 34th Symposium on Reliable Distributed Systems (SRDS); 2015. p. 11–20. https://doi.org/10.1109/SRDS.2015.27. Montreal, QC, Canada, Sep.
[155] Ahmed K, Gregory MA. Techniques and challenges of data centric storage scheme in wireless sensor network. J Sens Actuator Netw 2012;1(1):59–85. https://doi.org/10.3390/jsan1010059.
[156] P. Gonizzi, G. Ferrari, V. Gay, and J. Leguay, "Data dissemination scheme for distributed storage for IoT observation systems at large scale," Inf Fusion, vol. 22, pp. 16–25, Mar. 2015, doi: 10.1016/j.inffus.2013.04.003.
[157] Ayabakan S, Bardhan I, Eric Zheng Z, Kirksey K. The impact of health information sharing on duplicate testing. MIS Q 2017;41(4):1083–103. https://doi.org/10.25300/MISQ/2017/41.4.04.

[158] Su K, Li J, Fu H. Smart city and the applications. In: 2011 International Conference on Electronics, Communications and Control (ICECC); 2011. p. 1028–31. https://doi.org/10.1109/ICECC.2011.6066743. Ningbo, China, Sep.
[159] Kitchin R. The real-time city? Big data and smart urbanism. Geojournal 2014;79 (1):1–14. https://doi.org/10.1007/s10708-013-9516-8.
[160] Eremia M, Toma L, Sanduleac M. The smart city concept in the 21st century. Procedia Eng 2017;181:12–9. https://doi.org/10.1016/j.proeng.2017.02.357.
[161] Petrolo R, Loscrì V, Mitton N. Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms: R. Petrolo, V. Loscrì and N. Mitton. Trans Emerg Telecommun Technol 2017;28(1):e2931. https://doi.org/10.1002/ett.2931.
[162] Chourabi H, et al. Understanding smart cities: an integrative framework. In: 2012 45th Hawaii International Conference on System Sciences; 2012. p. 2289–97. https://doi.org/10.1109/HICSS.2012.615. Maui, HI, USA, Jan.
[163] Otuoze AO, Mustafa MW, Larik RM. Smart grids security challenges: classification by sources of threats. J Electr Syst Inf Technol 2018;5(3):468–83. https://doi.org/10.1016/j.jesit.2018.01.001.
[164] R. G. Hollands, "Critical interventions into the corporate smart city," Camb J Reg Econ Soc, vol. 8, no. 1, pp. 61–77, Mar. 2015, doi: 10.1093/cjres/rsu011.
[165] Alzahrani N, Bulusu N. Block-supply chain: a new anti-counterfeiting supply chain using NFC and blockchain. In: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems - CryBlock'18; 2018. p. 30–5. https://doi.org/10.1145/3211933.3211939. Munich, Germany.
[166] Keenan TP. Alice in blockchains: surprising security pitfalls in PoW and PoS blockchain systems. In: 2017 15th Annual Conference on Privacy, Security and Trust (PST), Calgary, AB; 2017. p. 400–4002. https://doi.org/10.1109/PST.2017.00057.