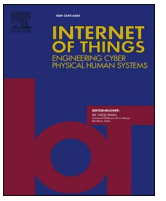
Internet of Things 23 (2023) 100860

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.sciencedirect.com/journal/internet-of-things



Review article

Blockchain and Internet of Things in smart cities and drug supply management: Open issues, opportunities, and future directions

Hassaan Malik [a], Tayyaba Anees [b], Muhammad Faheem [c,*], Muhammad Umar Chaudhry [d], Aatka Ali [e], Muhammad Nabeel Asghar [f]

[a] Department of Computer Science, School of Systems and Technology, University of Management and Technology, Lahore 54000, Pakistan
[b] Department of Software Engineering, School of Systems and Technology, University of Management and Technology, Lahore 54000, Pakistan
[c] School of Technology and Innovations, University of Vaasa, Vaasa 65200, Finland
[d] Department of Computer Engineering, Bahauddin Zakariya University, Multan 60000, Pakistan
[e] Department of Computer Science, Air University Islamabad, Multan Campus, Multan 60000, Pakistan
[f] Department of Computer Science, Bahauddin Zakariya University, Multan 60000, Pakistan

ARTICLE INFO

Keywords:
IoT
Blockchain
BCT, Drug supply
Smart cities
Health management
Data management

ABSTRACT

Blockchain-based drug supply management (DSM) requires powerful security and privacy procedures for high-level authentication, interoperability, and medical record sharing. Researchers have shown a surprising interest in Internet of Things (IoT)-based smart cities in recent years. By providing a variety of intelligent applications, such as intelligent transportation, industry 4.0, and smart financing, smart cities (SC) can improve the quality of life for their residents. Blockchain technology (BCT) can allow SC to offer a higher standard of security by keeping track of transactions in an immutable, secure, decentralized, and transparent distributed ledger. The goal of this study is to systematically explore the current state of research surrounding cutting-edge technologies, particularly the deployment of BCT and the IoT in DSM and SC. In this study, the defined keywords "blockchain", "IoT", drug supply management", "healthcare", and "smart cities" as well as their variations were used to conduct a systematic search of all relevant research articles that were collected from several databases such as Science Direct, JStor, Taylor & Francis, Sage, Emerald insight, IEEE, INFORMS, MDPI, ACM, Web of Science, and Google Scholar. The final collection of papers on the use of BCT and IoT in DSM and SC is organized into three categories. The first category contains articles about the development and design of DSM and SC applications that incorporate BCT and IoT, such as new architecture, system designs, frameworks, models, and algorithms. Studies that investigated the use of BCT and IoT in the DSM and SC make up the second category of research. The third category is comprised of review articles regarding the incorporation of BCT and IoT into DSM and SC-based applications. Furthermore, this paper identifies various motives for using BCT and IoT in DSM and SC, as well as open problems and makes recommendations. The current study contributes to the existing body of knowledge by offering a complete review of potential alternatives and finding areas where further research is needed. As a consequence of this, researchers are presented with intriguing potential to further create decentralized DSM and SC apps as a result of a comprehensive discussion of the relevance of BCT and its implementation.

* Corresponding author: School of Technology and Innovations, University of Vaasa, Vaasa 65200, Finland.
E-mail address: muhammad.faheem@uwasa.fi (M. Faheem).

https://doi.org/10.1016/j.iot.2023.100860

Available online 26 June 2023
2542-6605/© 2023 The Author(s). Published by Elsevier B.V. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

The technology known as blockchain is receiving widespread acclaim, and it is anticipated that this development in technology will fundamentally transform human activities and relationships [1,2]. Academics, software developers, and industry professionals have all demonstrated a discernible rise in their levels of interest, and a lot of prototypes, platforms, and systems are conceived. Bitcoin, Ethereum, and Hyperledger are three of the most notable platforms, and each of these platforms has affected several issues that are associated with BCT. After the introduction of the first cryptocurrency, Bitcoin, the usage of BCT as the primary underlying asset for cryptocurrencies quickly became widespread. Crowd funding and smart property are only two examples of the many use cases made possible by the resurgence of smart contracts on Ethereum, which has completely transformed the way blockchain is applied. Staking, a mechanism for dividing up blockchain resources among users, was also restored in the Ethereum network. The most recent iteration of this distributed ledger technology is known as Blockchain 3.0 [3]. As a direct consequence of this, it came to be utilized extensively throughout a diverse range of sectors, healthcare settings, and logistical networks. This about-face is due to recent progress in computer science and economics, respectively. P2P networks, asymmetric cryptography, consensus protocols, distributed ledger technology (DLT), decentralized transaction currency (DTC), smart contracts, and incentive structures have all contributed to its growth in various ways [4].

This article presents an overview of the usage of BCT in a single application domain, namely healthcare, in addition to other application domains where BCT and IoT are used simultaneously. This is done with a specific emphasis on SC and the DSM, which are the two most noteworthy applications of blockchain in the IoT and healthcare, respectively. The combination of these two technologies paves the way for the use of BCT within an IoT setting. In light of this, this article takes a look at a variety of approaches to integrating BCT with the IoT, all of which are applicable across a variety of application fields. The various approaches to integration differ in the part that blockchain plays in the larger system as a whole, the degree to which blockchain is involved in data exchanges between IoT devices, and the degree to which systems prioritize blockchain when it comes to the delivery of services. The taxonomy of the integration processes that will be explored in this article is founded on data from previously published studies.

Security is one of the advantages that BCT may provide to the DSM, SC, and IoT. This advantage covers a wide range of problems, including the safeguarding of data, systems, and networks, among others. To effectively manage data, it is necessary to keep private information in a storage environment that is always kept securely. The term "data management" will be used throughout this study, and each instance of it will refer to the process of gathering, processing, disseminating, retrieving, storing, and protecting information. It is essential to enhance all procedures involved in data management; this is true not only in the field of medicine but also in the IoT. This is because of a myriad of different contributing elements. For instance, the healthcare industry does not yet have a standardized data encoding format, a single patient identity, or a message protocol that permits syntactic and semantic interoperability among various systems [5]. IoT data management tasks are made more difficult because of the enormous number of devices that generate heterogeneous data and operate in both online and offline modes simultaneously. This presents a significant barrier to communication. It is already difficult to fulfill data management responsibilities in an IoT environment, but the presence of a huge number of various data-generating devices that are operating in both online and offline modes makes the situation even more difficult. The problem is the high level of complexity of the data that is produced by these devices. Because of this, it was necessary to look for a strategy for the administration of data that was not only more effective but also more efficient than the ones that had been tried previously. One of the potential courses of action that have been suggested by several writers [2–11] is to use BCT to construct solutions to the problem.

This investigation will primarily concentrate on the various applications of BCT and IoT in the areas of SC and DSM. Both SC and DSM face challenges on multiple levels. These problems range from technical difficulties, such as the explosion of big data, to economic obstacles, such as monetary loss as a result of product counterfeiting. Before BCT, there were several problems, as shown in the accompanying illustration, and a variety of potential solutions, any one of which could have been put into practice (see Fig. 1). Fig. 1 presents several challenges for DSM such as drug tracking, digitization, compliance, and regulation. In addition, the SC faces several obstacles such as handling a large number of data, high mobility, and regulatory policy. Recently, blockchain has been utilized either on its own or in conjunction with other solutions that are already in place to address some of the problems that have been plaguing SC and the DSM. This can be done either on its own or in combination with other solutions. The aim of doing this was to find solutions to some of the issues that have been troubling these regions. The utilization of BCT for these purposes is driven by the fact that it possesses several desirable qualitative characteristics [6–8]. These features account for the systems that can be constructed on top of it, as well as their reliability, robustness, and fault tolerance. When it comes to the creation of blockchain-based systems for the healthcare industry or the IoT industry, several challenges need to be addressed and overcome [9–12]. There is a lack of regulatory requirements, boosting throughput and scalability [13], restricting storage capacity [14], and securing secrecy [15] are the primary ones that are described the most in the published research [15–17,18,19].

1.1. Prior reviews

Even though blockchain research is just getting started, a considerable corpus of written material has been created on the subject and the different applications of BCT. Several studies have centered their attention on problems that are unique to a certain application domain. After going through the evaluation process, Table 1 presents the reviews that made the cut and were included in the final round. After selecting reviews for the long list, researchers may want to perform a tertiary evaluation of those reviews to learn more about the covered themes and the limits of the prior study. This would be analogous to what Kitchenham et al. [19] accomplished. There are still certain worries that have not been satisfied by the reviews that came before it, although a huge number of reviews have

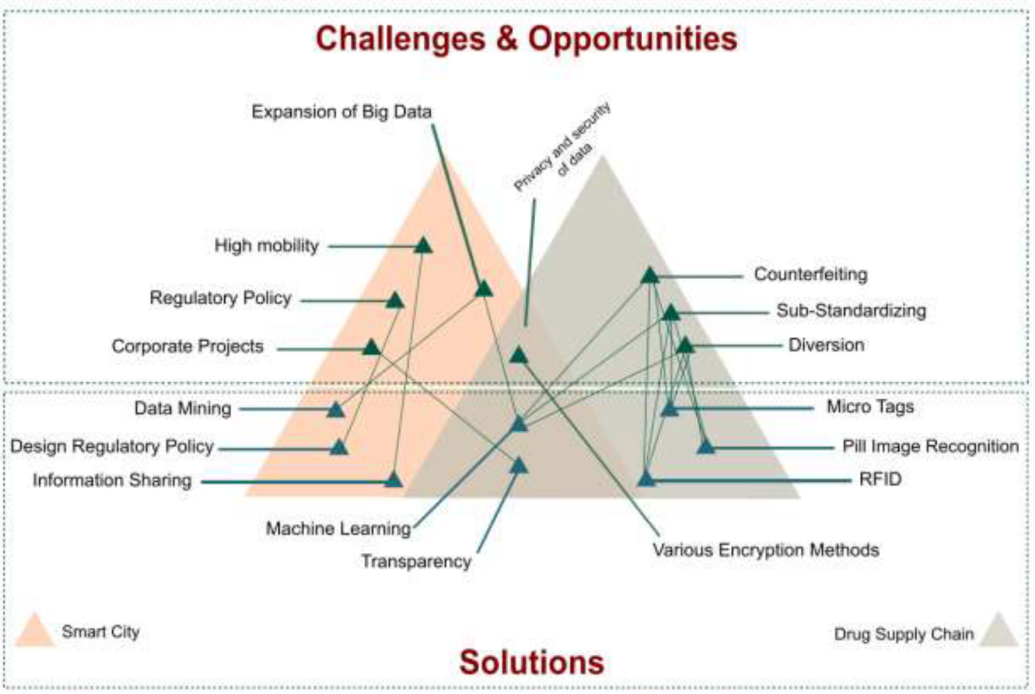


Fig. 1. Both the smart city and the supply chain for illegal drugs present both challenges and opportunities. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Table. 1
Summarize some relevant prior studies using BCT and IoT.

Ref	Issues addressed	Data management	Security	Integration
[9]	Use P2P energy trading to address the problem of energy applications.	✓	✓	✓
[10]	The IoT can be made more decentralized and private by the use of peer-to-peer and BCT.	✓	×	✓
[11]	IoT, security requirements, possible flaws, and remedies are outlined, with an emphasis on the utilization of BCT.	✓	✓	×
[12]	The data that is exchanged between users and applications can be protected and guaranteed to be unaltered if it is stored in and transported using a blockchain.	✓	✓	×
[13]	An analysis of the study done on the use of blockchain technology in the healthcare industry highlights the potential areas of application as well as the possible challenges.	✓	✓	×
[14]	The application of BCT can be used for IoT. In addition, an examination of how BCT can influence cloud-based IoT usage is provided.	✓	✓	✓
[15]	Shows the primary emphasis of current research into blockchain-related topics and explains the technological challenges and possible future directions of BCT.	✓	✓	×
[15]	Analyzed and compared blockchain solutions with potential medical applications.	✓	✓	✓
[16]	Blockchain has the potential to revolutionize the way electronic health records of patients are exchanged and preserved.	✓	×	✓
[18]	Challenges to address the integration of the IoT with blockchain.	✓	×	✓

been published. These issues are broken down in more detail below:

a) It is inappropriate to bring up the research issues that result in the construct identity fallacy, as described in the study [20]. Because of this flaw, the researchers who are impacted tend to concentrate more on data collecting than theory creation, as demonstrated by [21]. As a result, the progression of knowledge can be slowed down.
b) Avoid demonstrating the typical pattern that is used while producing artifacts in certain application domains.
c) Do not inquire how the many different prototypes or systems that have been built inside or across the many application areas compare to one another in terms of their functional capabilities.

d) The studies [22,23] make no recommendations about how to transfer knowledge from one domain to another, which is what is meant by "exaptation" [24] and "knowledge brokering" [25]. Exaptation and knowledge brokering are two ways of moving knowledge from a location in which it is known to a site in which it is unknown. Both methods include the use of analogical reasoning to accomplish this task.

In addition, as shown in Table 1, no evaluation examines the integration of BCT with the IoT comprehensively. In addition, the operations associated with data management are not completely covered. When looking at the issue of data security by itself, the authors of the study [11,12] addressed it to some extent. On the other hand, [11] does not devote a great deal of space to discussing blockchain-based security solutions for the IoT. However, [12] addresses the topic of security about the applications of BCT and the methods that are being implemented to address concerns regarding the safety of the technology, noting that this is because there are not many publications that are dedicated to the actual usage of blockchain [10]. Although it touches on a wide range of topics, the article does not cover data integrity in sufficient depth. A study [13] use of blockchain for the healthcare sector reveals that the majority of publications that were analyzed do not include technical specifics regarding the aspects of blockchain that were employed and that the bulk of research does not present prototype implementations or implementation details. Even when there is a prototype implementation, it is common practice to disclose no information on the components of the blockchain. The study [14] reveals that scalability-related difficulties associated with Blockchain, such as throughput and latency, have been left unstudied because the majority of research [15–18] has concentrated on exposing and improving the limitations of BCT in terms of privacy and security. As a direct consequence of this, the presence of such voids is the impetus behind this review. In addition, it is vital to carry out this review to fix a number of the shortcomings described before, as well as to:

1) Outline the trends that have been forming as instantiations have evolved.
2) The current application of BCT for data management gives rise to problems regarding security, access control, and the privacy of both users and the system; these concerns need to be addressed.
3) Explain the steps that were taken to integrate the BCT and the IoT so that they can be utilized together.
4) Provide a framework for upcoming research to be done on the themes covered in the chosen application.

1.2. Contributions

The most recent findings from research on utilizing BCT and IoT in DSM and SC applications were investigated and reviewed in this study. The objective of the study is to determine the issues, challenges, and recommendations of integrated BCT and IoT with DSM and SC to enhance this technology's effectiveness. Additionally, this review also provides a contribution to the current body of research by filling in several clear knowledge gaps. A few insufficiently detailed evaluations of the integration of BCT with the IoT are just one example. There is also a lack of reviews of published research on access control and data integrity in BCT. In addition, assessments are scarce concerning the combination of BCT and IoT. In addition to this, it helps increase our comprehension of other areas, such as the procedures that are employed in blockchain-based systems to protect the users' privacy. Listed below are the significant contributions of the current study:

1 The primary emphasis of blockchain research is being placed on the administration of data. This analysis has the main emphasis on the primary activities that are associated with data management as well as the strategies that are utilized to enhance those activities.
2 The proper storage and protection of sensitive information is an essential component of efficient data management. The majority of the previous studies focused on three concerns. These are the integrity of the data, control of access, and secrecy of personally identifiable information. This analysis provides a framework for categorizing the many methods that are used in these three different fields.
3 During this investigation, SC and DSM were found to be the most prominent topics in the IoT and healthcare domains, respectively. Thus, these two domains are treated as special issues in this review study.
4 Throughout our review, it became abundantly evident that the architecture of blockchain-based systems is influenced by a wide variety of distinct aspects. As a direct and immediate result of this, considerations and criteria have been outlined.

2. Background

BCT, the IoT, SC, DSM, and health information technology (HIT) are all discussed in this section of the study. All the key concepts of BCT, as well as the traits of IoT and HIT, are outlined here.

2.1. Blockchain

The phrase BCT does not have a universally accepted definition that is understood by most people. It would appear from the various arguments that have been presented up to this point by a variety of authors that there are many distinct subject areas. Examples of these individuals are [11,24,25]. Others, such as [26–28], perceive it as a data structure, while other authors, such as [29,30], consider it to be a technology for the management of transactions. There are still some individuals who maintain the view that it is a data structure. The authors come at the topic of BCT from a variety of perspectives, which leads to a variety of interpretations being offered

regarding the technology. Additionally, because BCT is always being improved, it is difficult to correctly forecast what its status will be in the future. As was said before, the BCT has advanced from BC 1.0v to BC 3.0v. This represents a significant step forward. The advancement is made on a range of facets, particularly those that are described as the foundations of BC [31–33]. Each publication refers to four distinct concepts as "fundamentals," and the development is made on all of these aspects. Peer-to-peer networks (P2P), distributed ledgers (DL), consensus mechanisms (CM), smart contracts (SC), and application domains or uses are some of the most essential ideas that need to be investigated.

2.1.1. Networking based on peer-to-peer (P2P) exchange

BCT may be boiled down to its most essential component, which is a peer-to-peer (P2P), decentralized network. This allows for the technology to be more easily understood. There is a wide variety of communication styles and node types that can be used inside P2P networks, and various topologies can be implemented in practice. P2P networks are also able to take on a variety of purposes. In addition, there are many other configurations that P2P networks might take. Centralized, decentralized structured (DS), and decentralized unstructured networks (DUN) are the three primary categories of topologies for computer networks. [34]. The most typical configuration for a computer network is known as a centralized topology. In P2P networks that are centralized, it is the job of a central directory server to keep a record of the available network resources, along with the addresses that are connected to those resources. In contrast, a Distributed Hash Table (DHT) is maintained by a subset of nodes in a decentralized hierarchical topology. This table, as opposed to a central directory server, contains information on the positioning of resources. The resource locations are stored in this DHT for easy access. In contrast, a decentralized unstructured architecture has no central directory server and no strict constraint on where files should be stored. The reason for this is that no directory is concentrated in any one area. In its place is an adaptable rule that enables nodes to freely join or leave the network at their discretion. Additionally, if they so choose, nodes can join the network in an anonymous capacity if that is what they desire.

There are a few different situations that have the potential to occur in P2P networks, and each of these scenarios has the potential to require participation from numerous nodes. In situations like this, management tactics like clustering are utilized to build a network that is simpler to exercise control over. This makes the network more manageable overall. Common methods of clustering include grid-based, hierarchical-based, partition-based, and density-based clustering [35]. Clustering on a grid is another approach that can be taken. The topologies affect how the nodes connect and the way that information is passed between them. When the nodes in a centralized P2P network have received data placement information from the directory server, they can start interacting with one another and other nodes in the network. The distributed hash table (DHT), also known as a key-value store, is kept up to date at individual nodes in a decentralized hierarchical architecture. The information concerning the value, which is often referred to as the data, can be indicated by employing the keys. By utilizing the information that is stored within them, nodes can gain access to the data that is stored elsewhere.

In decentralized and unstructured networks, communication can be performed through a multitude of mechanisms. Flooding, chatting, and random walks are just a few examples of the various strategies that can be utilized. When it comes to deciding which other nodes will get their messages, the nodes in this configuration employ a method of selection that is completely random. It is also possible to categorize a P2P network as either homogenous or heterogeneous based on the different sorts of peers that are members of the network. The individual nodes that make up a homogeneous network all have capacities that are approximately the same in storage, processing, communication, sensing, and energy. This is what distinguishes a homogenous network from other types of networks. There is a difference in at least one of the issues discussed above across the many nodes that make up heterogeneous networks [36]. There are no limits placed on your ability to communicate with any other individuals. On the other hand, in a centralized P2P system, peers must first be invited to join the network.

The properties of the P2P network, which the BCT is based on, are inextricably woven into the fundamental fabric of the system. This makes it impossible to remove these qualities from the system. A significant number of BC are currently being organized into several categories based on the governance systems that they implement. As a direct result of this fact, BC systems may be broken down into two primary categories according to the presence or absence of permission and the method that is utilized for the governance of the BC network. There are two distinct groups of things: those that require permission and those that do not; the major distinction between the two groups is whether permission is required. In addition, there are two separate varieties of governance, which are referred to as public and private, in that order. These are the two primary groups to consider. In the given article [37], comparisons are drawn between the two, and Table 2 illustrates the altered version.

Table. 2
Comparison of the different methods of governance and permission that are utilized by blockchains [37].

Access	Consent required	Consent not required
Public	• There are restrictions on either the transaction or the data that may be accessed. • • There is a limit on the total number of consensus-achieving nodes.	• Validation, access, and transactions are unrestricted.
Private	• No restrictions are placed on validation, transactions, or access. • The proprietor decides who is allowed to take part in the consensus process.	• Only authorized users can make transactions. • No participation restrictions are placed on the consensus procedure.

2.1.2. Ledger distributed

Blocks, each of which is composed of a collection of transactions and is structured to make use of those transactions, are used to form a distributed ledger. A distributed ledger is produced using these blocks. Table 3 presents a breakdown of the components that make up a transaction as well as a block to assist you in gaining a better understanding of both ideas. Transactions and their resulting outputs share the same Merkle root hash value, as was shown previously.

The block header of the blockchain stores the value of the hash function that was generated for the prior block. As a direct consequence of this, the immutability of transactions and the security of blocks are both safeguarded. To design a block, you will need to demonstrate that you can solve a mathematical problem. The level of difficulty necessary to finish the challenge is described in the information that is included in the header of each block. Mining is the procedure that leads to the formation of a block and is also known as "block generation." Cryptography is used to accomplish this goal by computing a number that is lower than the difficulty level that was given. The extraction procedure consumes a large amount of time in addition to the computing power that is available. Because of this, the member who can effectively resolve the issue will be rewarded for their efforts, but only after they have provided the required paperwork. This will be carried out as soon as the obstacle has been successfully overcome appropriately. Following the successful mining of a predetermined quantity of coins, the participant will be eligible to receive compensation. However, it is vital to keep in mind that the elements contained within a block can alter depending on the platform that you are playing on. For instance, in Ethereum, the hash of the block that was created by the parent is added to the hash of the block that was created by the parent's sibling. In addition to the hash of the block that was produced by the parent, this also needs to be done. While the Patricia-Merkle tree is used to build the transaction tree in Ethereum and Parity, the Bucket-Merkle tree is the one employed by Hyperledger [32]. This is because the Patricia-Merkle tree is more efficient than the Bucket-Merkle tree in terms of space use. These activities are being taken to improve the efficiency of the process of searching for transactions and bringing them up to date.

2.1.3. Agreement mechanisms

Nodes in a blockchain must reach an agreement on the legitimacy of a block before it can be added to the chain, a process known as "consensus". Computational techniques (like POW) and communicative strategies like Practical Byzantine Fault Tolerance (PBFT) are the two primary categories of consensus-building methods [31,32]. Things like a working proof of work example can be found in the first group. Proving your stake (PoS), reaching a consensus (Threshold Relay), and burning your bridges (Proof of Burn) are all examples of consensus techniques that fall somewhere along this spectrum. These three are only some of the options available. One could consider this spectrum to be located somewhere in the middle. These two extremes exist on completely different ends of the spectrum. In addition to utilizing their well-known versions, the research that was analyzed also made use of their updated variants [39,40].

2.1.4. Smart contract

When carrying out a transaction, a pre-existing protocol can be automatically triggered as part of the process. The use of such contracts in corporate transactions is gaining popularity. A "smart contract" can also be compared to a pre-existing protocol in some contexts. No infrastructure for blockchain does not allow for the creation of smart contracts. Despite this, the languages that may be used to produce smart contracts and the environments in which they can be executed might vary greatly from one blockchain system to the next. Currently, the most popular options for creating smart contracts are Solidity (Sol), Golang (GO), Serpent (SP), Java, Python (PY), and LLL. These programming languages are what are utilized while developing smart contracts. The Docker Image, the Haskell execution environment, the Ethereum Virtual Machine (EVM), and the Java Virtual Machine (JVM) are just a handful of the many possibilities available for use as execution environments [31,32].

2.1.5. Blockchain's potential uses and its applications

The expansion of BCT's potential deployment contexts and uses is a crucial indicator of the technology's development, as was mentioned earlier. The reason for this is that the BCT may be utilized in a decentralized manner to record and verify transactions. The fundamental challenges that are linked with BCT will be impacted in different ways depending on the kind of application that will use

Table. 3
Information revealed within a block as well as a transaction source [38].

Type	Name	Symbol	Description
	Version	VER	VER number of the block.
Block	Hash	H	The value of the block's H.
Header	Parent Hash	pH	The pH value from the block before this one.
	Difficulty	D	The level of D for the proof-of-work aim.
	Timestamp	TS	The duration of the block's creation time
	Merkle Root	MR	The fundamental building block of the MR of transactions.
	Nonce	N	A random N counter that can be used as proof of work (POW).
	Hash	H	A random H counter is to be used for the POW.
Transaction Ledger	Block Number	BN	The transaction is contained within the BN.
	Order	O	The O of transactions within the block.
	Timestamp	TS	The TS at which the transaction was initially created.
	Sender	S	SID
	Receiver	R	RID
	Signature	SIG	Sig, also known as the H Value of the Transaction

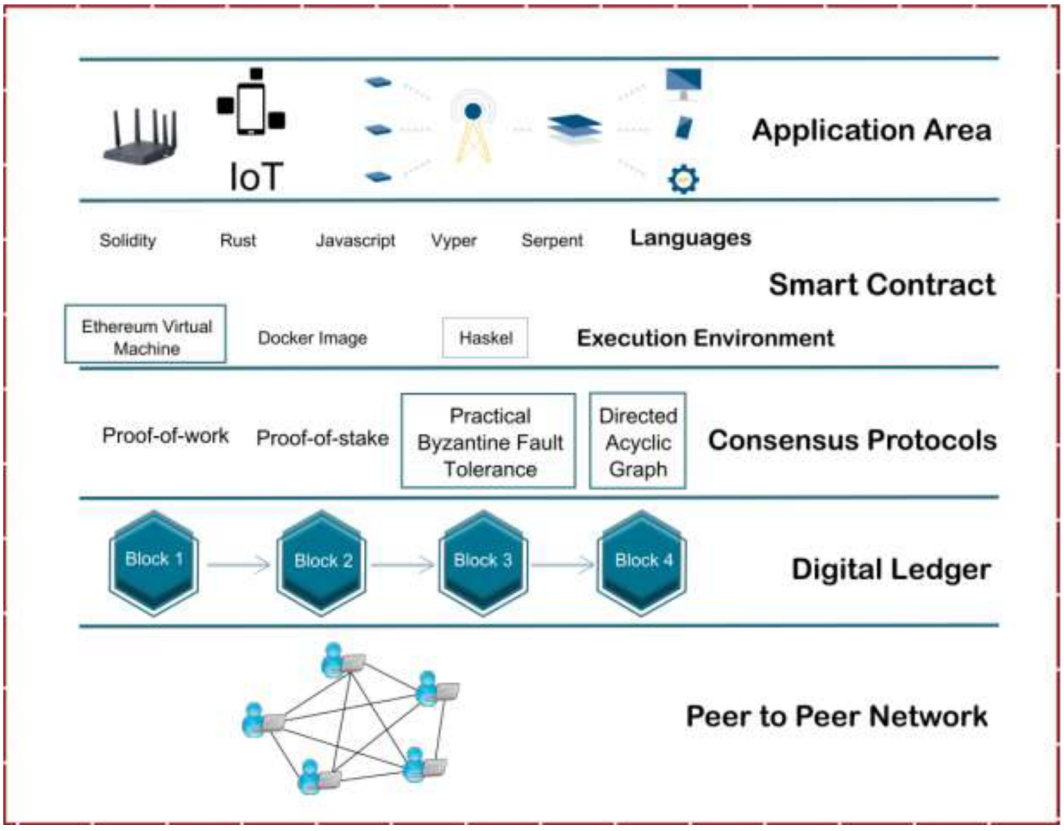


Fig. 2. The core building components that comprise a blockchain. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

and the goals that will be achieved as a result of doing so. In this context, some types of enterprises, such as those dealing with healthcare, financial systems, and digital rights management, are needed to make use of either a private blockchain or a centralized P2P network. Either of these two choices must be implemented. These two varieties of distributed ledger technology are referred to by their respective names, which are permissions private blockchains and centralized P2P networks. In this case, peers are the ones who are accountable for preserving any meta-data or links to their content. In this circumstance, the only ledger that is preserved is the one that is stored on the primary server.

According to the study [41], it is also advised that a decentralized structured topology be used in the banking business. Within this topology, a DHT may be utilized to keep references to data that may be accessed via blockchain. DHT is utilized to improve data availability, and the data can either be stored in a centralized repository such as a cloud or on randomly selected nodes [42].

The decentralized unstructured topology technique is the one that is utilized most frequently when it comes to the construction of blockchain-based architectural designs for Bitcoin and specific IoT settings that incorporate a large number of nodes. Clustering techniques are also utilized in blockchain systems, and the ones that are used are analogous to the ones that were demonstrated in earlier cases [43].

The utilization of BCT does not in any way affect the practicability of the communication strategies. Because of this, Bitcoin can be understood as an illustration of a P2P network that is decentralized and unstructured, and in which participants are informed of transactions through informal means of communication. In other words, Bitcoin is a network that is not governed by any central authority, and which is both dispersed and unstructured [44]. The primary components of blockchain are illustrated in Fig. 2.

2.2. IoT

The IoT is a subset of the Future Internet that envisions how "things" with individual identifiers, attributes, and digital personas would be able to easily connect using sophisticated user interfaces [45]. For an IoT to function, numerous pieces of software, middleware, and hardware must be used.

The creation of an IoT infrastructure calls for the use of a significant number of software, middleware, and hardware components [46]. In addition to this, they have the propensity to be widely dispersed, and examples of them can be found in open habitats located in a wide variety of different geographical regions. In addition to this, the technology that makes it possible to do so was only recently developed [47]. Because of this, they are susceptible to being assaulted, and the preventative measures that they take to keep

themselves safe need to consider for them to be successful. Moreover, it may be possible for the various devices to connect more readily using ad hoc IP protocols [48] including Near Field Communication (NFC), Blue-tooth, IEEE 802.15.4, Wi-Fi, ZigBee, and 6LoWPAN [49]. Additionally, ad hoc communication could take place through the utilization of the Internet, mobile communication networks, satellite networks, or wireless networks [50]. These kinds of communications carry with them the risk of exposing information systems to dangers including data manipulation and intrusion, both of which are common types of cyberattacks. In addition, these kinds of communications also carry the risk of exposing information systems to dangers including ransomware. These forms of communication also entail the risk of exposing information systems to threats such as ransomware, which can be a particularly damaging form of malware.

The lack of a standard layering methodology for IoT also results in architectural differences between products [51]. The application layer, the network layer, and the perception layer are said to be the three components that makeup IoT devices, as stated in several different written works that have been published. The application layer is the first one to appear, then the network layer, and finally the perception layer after that. According to the cited source [52], some applications that can be uncovered in the application layer include healthcare, smart cities, and smart energy. Components such as routers, switches, gateways, and firewalls, among other devices, can be found at the network layer of an operating system. The network layer is the name given to the one that comes after the physical layer. In addition to the sensors that are already a part of it, the perception layer is made up of several kinds of embedded systems. These can include a physical layer, a business layer, a service management layer, or a middleware layer [46]. Adjustments to the layering may be required based on criteria such as the release version of the IoT device, the standard to which service providers adhere, the capabilities and complexity of the device, and so on. The following provides examples of some of these contributing factors: As a result of this incompatibility, devices that are connected to the IoT are vulnerable to attack and are unable to communicate securely with one another.

Additionally, in contrast to traditional devices, which frequently use the same collection of operating systems, the IoT does not have a dominant operating system that is deployed by a large number of devices [53]. This contrasts with traditional devices, which frequently make use of the same collection of operating systems. When compared to traditional devices, which often make use of the same operating systems across the board, this is in stark contrast. In addition, there is a deficiency in the number of specialized data formats. Because of this, it is difficult to develop interoperability between them [46]. This is a direct result of the situation. The utilization of middleware as a strategy to facilitate the integration of IoT devices is one of the strategies that has been put into action [47]. It has been decided to proceed with the implementation of this plan despite the inherent security problems that it presents. Although several earlier attempts have already been made to address these issues, one solution that has recently been proposed is to make use of the technology of blockchains as a possible way to overcome some of the challenges that have been discussed [48].

The environment is transformed into an Internet of Medical Things (IoMT) as a result of the incorporation of medical capabilities into IoT devices. The implementation of IoMT devices is becoming increasingly common as technology continues to progress. In addition, the COVID-19 situation makes it difficult for patients and medical professionals to meet face-to-face. IoMT has entered a new age as a result of the pandemic, which has led to the provision of treatment to patients [46]. The IoMT is building a network that connects individuals and various types of medical devices, including wireless medical devices and implanted medical devices. It exchanges health data with medical facilities such as doctors, hospitals, medical specialists, and so on by utilizing various forms of wireless communication, such as Bluetooth, WiFi, 3 G, 4 G, 5 G, and ZigBee, amongst others [47]. The development of microelectronics has allowed for the creation of intelligent medical devices that can monitor and report on a variety of physiological variables, including blood pressure, heartbeat, oxygen level, and many others. In addition, IoMT has emerged as the most significant change among the developments in the medical field. This is because it allows for the continuous monitoring and treatment of not only elderly patients but also patients of all ages who are ill. IoMT can provide prompt treatment if it is required. Those affected by COVID-19 in particular continue to suffer even after they have fully recovered. The IoMT treatment protocol has gained widespread acceptance among medical practices in a variety of countries throughout the world.

2.3. HIT

Numerous investigations of HIT have been conducted over the past few decades. Many different kinds of systems have been developed and put into use [53]. “Computerized Provider Order Entry” (CPOE), “clinical decision support (CDS)”, “electronic result reporting (ERR)”, “Electronic prescribing (EP)”, “remote monitoring”, and HIMS are a few examples of the types of technologies that fall under the umbrella of “electronic medical record (EMR)” [54–56]. In addition to these, there are further ones, such as picture archiving and communication systems (PACS) and electronic Medication Administration Records (eMAR) [57]. Recently, long-range, and short-range communication technologies have been implemented to link together embedded medical devices, sensors, and IoT-enabled wearable devices that make up the HIoT, a subset of HIT. In the same way that they are utilized in any other IoT situation, sensors are utilized in the HIoT; however, these sensors can either be worn or implanted. According to the information presented in [58], there is a total of five distinct categories that can be utilized to categorize wearable sensors. The sensors that fall within these categories include those that measure pulse, respiration rate, body temperature, blood pressure, and pulse oximetry, respectively. There are several different forms that wearable sensors can take, the most popular of which is the pulse sensor.

HIT refers to crucial systems that are implemented to assist organizations and all stakeholders operating within the healthcare arena in the elimination of disconnected information and the modernization of health processes through the integration of various health functions and departments operating within the healthcare arena [59]. The ability to acquire effective healthcare services is impacted by a variety of factors, including political, economic, socio-technical, and technological actors [7]. Over time, the HIT has undergone tremendous change in the middle of a number of these factors. HIT has made it possible to consolidate all of the many

informational processes and health-related workflows that take place inside the healthcare industry. HIT is frequently contextualized as a system that improves the quality of healthcare services by supporting management and operation processes to afford crucial information and a unified process, technology, and people [7,8]. The study [10] provided a concise summary of HIT by describing it as a system that manages data to share knowledge and insights within the healthcare setting. This conceptual strategy was adopted by [13] to describe HIT as any system inside the healthcare industry that processes data and gives information and knowledge. Mayer et al. [16] emphasized the significance of HIS in the same context, stressing its emergence to address the requirement to store, analyze, and extract information from the system data to optimize operations, improve services offered, and give decision-making support. According to work [26], the current deployment of HIT is allegedly characterized by fragmentation, update instability, and a lack of standardization, all of which limits its capacity to assist with healthcare. In a congruent manner, several authors [28–31] have cited a lack of understanding of the potential of HIT, an underuse of HIT, an inadequate communication network, as well as concerns over security and confidentiality [19].

HIT's goal is to improve hospitals' operational and financial performance by cutting down on medical errors, raising the quality of care provided to patients, increasing the efficiency with which doctors work, and so raising the value of the hospitals they serve [55, 57]. As explained in [59], the IoT has several applications in the healthcare sector, including illness triage, patient monitoring, staff monitoring, modeling, and outbreak containment. Further, it aids clinicians by giving them access to real-time health status and predictive data, and it helps policymakers make informed decisions in the event of a pandemic [59]. It has been a long time since fragmentation in utilization was noticed, and government attempts to increase the exchange of health information between providers have been passed, but the findings of the research reported in [57] suggest, in general, that the application of HIT as a component of group therapy is beneficial [60].

Even more so, there have been numerous initiatives to improve communication among healthcare professionals. Furthermore, there have been various initiatives to enhance the sharing of health information between providers for the benefit of patients. Additionally, there have been initiatives to increase the sharing of patient health data amongst healthcare providers. Efforts have also been undertaken to better disseminate patient health information between professionals. It has been difficult, given the conditions, to make it clear what information ought to be saved in a particular system. For example, in the study [61], it is stated that most physicians regard electronic health records (EHR) to be an internal system. This belief is supported by the fact that EHR has been widely adopted. This holds for most medical facilities, including hospitals, as well as those businesses whose primary focus is on delivering medical care to patients. Personal health records (PHR) pull data from several different systems, and one of those systems is the EHR. As a result, the EHR contains data that the PHR can use to its advantage [5,29]. When viewed from a different angle, the PHR gathers information from several different systems, one of which is the EHR. In addition to this, it has been demonstrated that the utilization of one system can affect that of another system. For instance, electronic medical records and computerized provider order entry can be implemented more readily with the assistance of PACS and eMAR [57].

Integration is necessary since the system has many different types of redundant information and also has dependencies on other parts of the system. Consequently, the system contains a lot of information that is redundant. However, even though system integration is an absolute necessity, it is not particularly often practiced [5,61]. In addition, despite the best efforts of everyone involved, technological and non-technical hurdles continue to express themselves on a range of different levels. This is the case although there have been efforts made to overcome these barriers. System-level problems with workflow design and integration, a discrepancy in the rate of HIT advancement, and the complexity of security and privacy issues in both separate and connected systems all work against the possibility of integration [62]. These problems prevent the systems from being integrated. When these obstacles are considered simultaneously, integration becomes challenging. Obstacles that limit the integration of data between systems include the lack of individual patient identification, the absence of messaging that enables syntactic and semantic compatibility between systems, and the lack of data encoding standards [5]. Additionally, clinicians' inability to accurately identify individual patients is a hurdle that makes it difficult to integrate data from diverse systems.

Even though it happens very infrequently, consideration is typically provided during the integration process to the numerous stakeholders of the healthcare industry. Primary stakeholders include but are not limited to, patients, healthcare providers, and other organizations that collect or distribute health data. Secondary stakeholders are those who have a less direct role in HIT. Health authorities, clinical researchers, and technology providers are all instances of secondary stakeholders [5]. Those directly involved in the HIT are considered primary stakeholders. People who are directly involved in the HIT are considered primary stakeholders. Because there are many different stakeholders, each of whom has its own unique set of information requirements as well as information interests that are always shifting, HIT needs to bear these concerns in mind. For example, throughout history, patients' roles have evolved from merely being recipients of healthcare information to actively participating in the operation of HIT systems [61]. This is because HIT systems have become more complex. This change has taken place as a direct result of the increased incorporation of HIT into the treatment delivery process. This shift is due to the recently observed increased complexity of HIT systems, which resulted in the modification.

According to the study [63], patient participation in HIT is associated with the promotion of favorable health outcomes. These outcomes include a reduction in hospital and emergency room visits, a decreased risk of readmission, and a shorter length of stay. The length of time that the patient is required to stay in the hospital is yet another unfavorable outcome for the patient's health which may be affected by these circumstances. Another patient health outcome that has been demonstrated to be altered is the length of time a patient is required to remain in the hospital. Because of this, it is important to engage in dialog that takes into consideration the several interests that are involved. Therefore, blockchain is being considered a tool for the construction of patient-centric systems in several different ways, such as the administration of digital access rules, the rise in data availability, the increase in data liquidity, and the assignment of unique patient identifiers [64]. These are just some of the ways that blockchain is being considered for this purpose.

After this condensed introduction, this study proceeds to elaborate in further depth on each of these characteristics, in addition to several others that share similar qualities.

2.4. Smart cities

The idea of a "smart city" has garnered interest from all around the world, including that of governments, businesses, educational institutions, and research facilities. Various individuals and organizations have made efforts, from their unique vantage points, to comprehend and explain the concept of the smart city. In the early 1990s, the phrase "smart city" was used for the first time, and ever since then, scholars have emphasized the roles that technology, innovation, and globalization play in the urbanization process [16]. Since 2008, when IBM first introduced its Smarter Planet initiative [17], there has been a significant uptick in interest regarding smart cities. Since that time, the idea of smart cities has gone through a process of continuous expansion and development. A smart city is instrumented, linked, and intelligent, as defined by Ducas et al. [24]. Hammi et al. [25] offered another definition, which included the following six "smart" characteristics: economics, government, environment, people, mobility, and living. The United States of America (USA) was an early pioneer in the field of "smart city" initiatives that incorporate numerous "smarter planet" ideas [28]. The i-Japan Strategy 2015 was implemented in Japan to foster the development of a citizen-centric, secure, and dynamic digital society. To create a smarter city in the future, Singapore has unveiled its Intelligent Nation 2015 plan and begun numerous construction projects [27].

Smart city development relies heavily on information and communication technologies (ICT). Research into top-level architecture plays an important role in improving studies of resource configuration and driving technological development in all areas of a smart city. Without going into great detail on the technology, Guo et al. [34] presented a smart city architecture that takes into account the need to integrate government, citizens, communities, economies, and basic infrastructure from the vantage points of policy, organization, and technology [31]. According to Zhou et al. [37], data processing technologies should be regarded as basic for all applications related to smart cities [32].

Recently, a growing number of scholars have attempted to design smart city architectures from the perspective of data. The study [33–35] that has been done on smart city architecture has resulted in a methodical understanding of the technologies that are required to build a smart city. The term "smart city" has been given several meanings by various stakeholders, which has led to the architectures described in published works [64–69] having a wide range of variations. The majority of architectural designs illustrate that a smart city is driven and facilitated by cross-disciplinary technology [70], particularly data processing technologies. Smart cities have led to the widespread implementation of a wide range of cutting-edge information technologies, including mobile computing, cloud computing, big data, data vitalization, the IoT, and data cloud computing [71–74]. In each of them, data-centric enabling technologies play a significant role in the implementation of smart city initiatives.

At both the national and international levels, upcoming researchers and Smart Actionists are well familiar with Smart City due to its widespread fame. The creation of a smart city necessitates the use of a wide variety of different kinds of technological advances. The majority of the world's population now resides in urban areas, the majority of which are either metropolises or urban zones [75]. At present, the rapid growth of cities and other urban areas has a direct impact on the number of services offered to citizens by the city's administration as well as the level of quality those services have. The concept of smart cities can now be utilized to assist in the provision of an optimal solution. ICT has been utilized by a variety of smart city efforts, some of which have been led by the government while others have been led by private businesses. The goal of these initiatives is to find a new solution that is both optimized and effective for dealing with the expanding problems that are plaguing cities and metropolitan regions [2,3]. The development of a smart city necessitates facing issues in the areas of healthcare, education, power, transportation, waste management, unemployment, and cybersecurity [4].

The concept of a "Smart City" revolves around the implementation of user-friendly ICT by large corporations in the context of urban areas. Since that time, its significance has grown to encompass the future of cities and the progression of their structures. When seen from a futuristic perspective, intelligent cities give cutting-edge, resource-friendly, and high-quality living options. They also connect the infrastructure that already exists while fostering social and technological innovation.

A city is considered to be smart when it possesses several characteristics, such as sustainability, urbanization, intelligence, and Quality of Life (QoL). The concept of sustainability has emerged as the preeminent paradigm in the field of urban planning, and the rise of smart cities is a direct result of the widespread attention paid to the concept of sustainability. Recent research [54] suggested expanding the concept of sustainability to include additional dimensions, including social concerns, economics, infrastructure and governance, energy and climate change, pollution and waste, and health. Since modern cities use more natural resources than ever before, it's crucial to examine the repercussions of depleting nonrenewable energy sources. The need of protecting smart cities' energy sources and environmental heritages was emphasized in the study [53]. Sustainability refers to a city's continued viability as an economically, socially, and environmentally viable community. Smartness is the drive to raise the bar for the city's social, economic, and environmental standards. Financial and emotional security are indicators of rising quality of life for city dwellers. The process by which a rural area is transformed into an urban one, including the requisite infrastructure, economic, technical, and governmental changes.

2.5. Drug supply management

Blockchain's novel distributed ledger technology has brought revolutionary change to the healthcare sector. The blockchain for the medical industry maintains and keeps the complete supply chain up to current, storing information about drugs, pharmacies, pharmacists, medical prescriptions, physicians, patients, nurses, and the dosages of medications. The drug delivery data lakes function as

their unique repository, which is also sometimes referred to as a distributed blockchain. The data lake is an invaluable resource for undertaking important projects including the analysis, visualization, and reporting of medical data. A hospital, as well as other healthcare-related businesses that require medical data for day-to-day transactions, would profit from having access to this information. In addition, with the patient's consent, doctors can access their data, and the patient can send their data to any doctor in the network. To protect the confidentiality and security of patients' information, these permissions can be established by specifying an access control policy in the smart contract.

The drug supply chain is an industry-specific production distribution chain with numerous constituent links. In the drug supply chain, having the capacity to trace medications at any time and from any of the stakeholders involved is critical. In recent years, an increase in the level of complexity in the manufacturing and distribution channels of the drug supply chain has been seen. For instance, an increase in the number of online pharmacies contributes to an increase in the level of complexity within the logistics system, as well as an increase in the severity of the risk posed by counterfeit items [76]. Within a drug supply chain, increased medicine traceability and transparency are also possible applications for BCT. The system remembers the complete transfer history of a pharmaceutical batch as well as its registration and uploads all of the relevant information onto the network of the platform. To continue exchanging this batch, the sender and the recipient must both provide their permission, and the transaction involving the exchange will be permanently kept on the network. Because of this, there is no longer any chance that a third party will commit fraud [77]. The authors of [78] examine the adoption of traceability procedures in the pharmaceutical business, specifically drug traceability, using BCT.

Using a blockchain platform architecture consisting of five layers, the authors of [79] construct a drug traceability system that is enabled by BCT. They make use of smart contracts and applications connected to the IoT to manage drug identities and make on-chain and off-chain methods more accessible. Through the utilization of real-world data provided by the collaborating firms, Hyperledger Fabric was utilized to test the platform's viability and effectiveness [79]. In [80,81], the authors describe a system for the management of the distribution of restricted pharmaceuticals that is based on a private Ethereum blockchain. All transactions that take place on the distributed ledger are recorded by smart contracts, which ensures transparency, accountability, security, and the provenance of the data. To store content-like images on a huge scale, the authors make use of an off-chain storage system that is built on IPFS.

Another crucial function of the drug supply chain is the monitoring of the distribution of fake pharmaceuticals. The authors of the article [82] explain how BCT can be applied to combat counterfeiting and secure the traceability of drugs. The authors of [83] suggest a blockchain-enabled system that they call Medledger. Their proposed system enhances the supervision of the drug supply chain ecosystem's involved parties as well as their interaction with one another. Furthermore, their system saves and records all activities, events, and transactions on a blockchain that is linked to peer-to-peer decentralized file systems such as IPFS, Swarm, and others [83]. Within the framework of the traceability of logistics, the authors of [84] propose a decentralized architecture to improve the data quality associated with IoT. They apply their methods to a hypothetical situation that involves disposable medical diagnostic kits and several pieces of medical equipment.

Some researchers have built vaccine tracing systems enabled by blockchain technology, in addition to systems for tracking medications and medical devices. The authors of the article [85] offer a software solution for the accumulation and integration of information in vaccine supply for both the supply-side traceability and the demand-side information. The suggested system solves the issue of vaccination traceability from regional centers to the final consumer by utilizing cold storage networks in conjunction with facilities for vaccine handling and administration. The authors of the study [86] construct a system that they refer to as a "vaccine blockchain". This system integrates the technologies of machine learning with blockchain. The proposed system makes it easier to track vaccinations and fulfill the functions of intelligent contracts, all while preventing the expiration of vaccines and the fabrication of records. In addition, models of machine learning can assist vaccination practitioners and receivers in making better-informed judgments on vaccination practices and vaccines [86].

3. Methodology

There have been several authors, such as [3,64], who have underlined how prevalent BCT is, and consequently, there have been several publications that cover the various possible application fields. This results in an increased number of publications; hence, to conduct an in-depth evaluation, the author must select relevant works from among a wide body of existing literature. The following provides specifics of the target application areas, approach for literature search, and article review process to accomplish this purpose.

3.1. Search technique, as well as the selection of application areas

At the outset, a method for searching the published literature was developed by adapting the advice given in studies [65–67]. As a result, a literature search on a variety of databases using the key term "blockchain", "IoT", drug supply management", "healthcare"," and "smart cities were performed in August 2022, and it resulted in the retrieval of a significant number of articles. To screen the collected studies, a preliminary review was performed that takes into account the publications' application area, language, impact factor, etc. Some of the domains that the remaining articles were assigned to include Bitcoin, the IoT, Healthcare, smart contracts, supply chain management (SCM), banking, Industry, etc. To arrive at this conclusion, it was essential to look at the abstracts and titles of the relevant papers. After going through the process of collecting and analyzing the data, it was finally decided which applications need additional scrutiny. The scope of this investigation is restricted to the kinds of items that are commonly categorized as "blockchain 3.0." Although most publications do not specifically cover cryptocurrencies, that topic will serve as the primary focus of this evaluation. The majority of works in this category center on how BCT can be applied to the healthcare industry and the IoT.

The second search was initiated following the organization of the papers and the selection of the blockchain 3.0 application

domains. In December of the following year, we repeated the investigation, but this time we narrowed our focus to the terms "blockchain in IoT" and "blockchain in healthcare." Additionally, we carried out searches that simultaneously looked forward and backward in time. The second search will shed light on how our thinking about BCT has progressed over the previous year as well as how its application has grown to encompass a variety of different fields. In the time that passed between the two searches, we performed some background reading to get a more in-depth grasp of the subject matter and to develop the criteria by which we would determine which publications would be regarded as relevant or irrelevant [66].

The results from the analytical reading were used to inform the search for application-specific literature that was used to support the review and the presentation of that literature. After it was found that there was a gap between the previously known information and the publications that dealt with blockchain, additional publications were read to fill in the gaps in the evaluation and establish a connection between the previously known information and the emerging pattern of blockchain application.

3.2. Inclusion criteria

The following is a list of the inclusion criteria that were used for the primary publications. Books, book chapters, and papers published in journals with an impact factor of more than 1.0 are suitable for further processing, as assessed by the database used to identify publications [67]. According to the study [68], the second processing stage is open to the submission of papers that have been presented at conferences that have been prepared by well-renowned research associations such as Springer, ACM, IEEE, ICIS, INFORM, etc. The procedure of evaluating conference papers, on the other hand, requires that one approach it with the utmost prudence, as stated in [65].

In a manner analogous to this, the papers that are presented at conferences are subjected to a stringent review procedure, which is detailed in [68]. We also analyzed them using the Google H-5 index, and in the end, we only counted those who obtained a score of 10 for inclusion in our total. This is because we wanted to ensure that the results were as accurate as possible. The establishment of such stringent quality standards has repercussions for a variety of problems, one of which is the involuntary removal of valuable publications from sites that have received lower rankings. No cutoff threshold establishes a journal's quality, which shifts regularly. The only exception to this is the criterion of an impact factor of 1.0, which is given in [67] as an example of exclusion. In addition to this, the H-5 index is employed rather seldom. Because of these worries, some high-quality publications may be excluded from the review; nonetheless, this will not affect the review's capacity to be replicated [68].

Despite this, a critical analysis was performed on any articles that satisfied the requirements outlined above. Analyzing "what is known, how knowledge is obtained, what forms of knowledge are produced, how valuable different types of information are in comprehending and describing a subject of interest, and where the boundaries and weaknesses of current knowledge are" is what is meant by "critical assessment" [69].

Critical evaluation is one type of knowledge evaluation. Understanding the level to which blockchain has been revolutionizing the application areas and being savvy about the way the artifacts are composed of constructs (vocabulary and symbols) [70], models (abstractions and representations), methods (algorithms and practices) [71], and instantiations (implemented and prototype systems) [72] are used are the reasons for conducting a critical analysis of literature. Fig. 3 depicts the processes that were completed to complete the article's preparation.

4. Results

In the body of research that was examined, both recurring problems and problems that were application-specific were discovered. Following an in-depth discussion of the findings of the literature review, a summary of those findings is presented here.

4.1. Evaluation of selected papers

However, due to the infancy of blockchain applications for the IoT, only a handful of initiatives have moved past the proof-of-concept or technological readiness stage (TRS) [51]. With regards to blockchain 3.0, this use case has proven to be the most popular. Articles in this field cover a wider variety of topics, including IoT compatibility with BCT, the administration of IoT data, approaches to strengthen IoT security, and the challenges of smart cities [67–71]. The other industry that stands to benefit significantly from the implementation of BCT is the medical field. Most applications for BCT can be found in the healthcare industry. Table 4 that follows provides a list of publications that examine the potential applications of BCT in these two industries. In the field of IoT, two of the most frequently discussed subjects are the creation of systems that may assist in improving the safety of IoT data and the provision of substantial information regarding the advantages of using blockchain for IoT. In addition, several papers show how BCT can be integrated with the IoT. In addition, some studies explain various uses associated with smart cities. These are all broken down into more specific sections.

On the other hand, a few authors highlight the advantages of implementing blockchain technology in healthcare. To this end, blockchain technology may help by allowing the creation of a decentralized and user-managed data provenance system that is trustworthy, secure, immutable, robust against a single point of failure, and incentivized. Furthermore, it may be utilized as a platform for medical payment systems, accelerates insurance claim processing, and keeps medical records securely [6–8]. It can also be used as a database for medical research, clinical trials, and consent management [64,73]. This, in turn, increases the amount of data that is made available and enables the identification of patients. However, as was covered in [74–86], the implementation of BCT in the healthcare industry is not without its share of difficulties. The capacity of blockchain-based [87] systems to maintain their anonymity while also

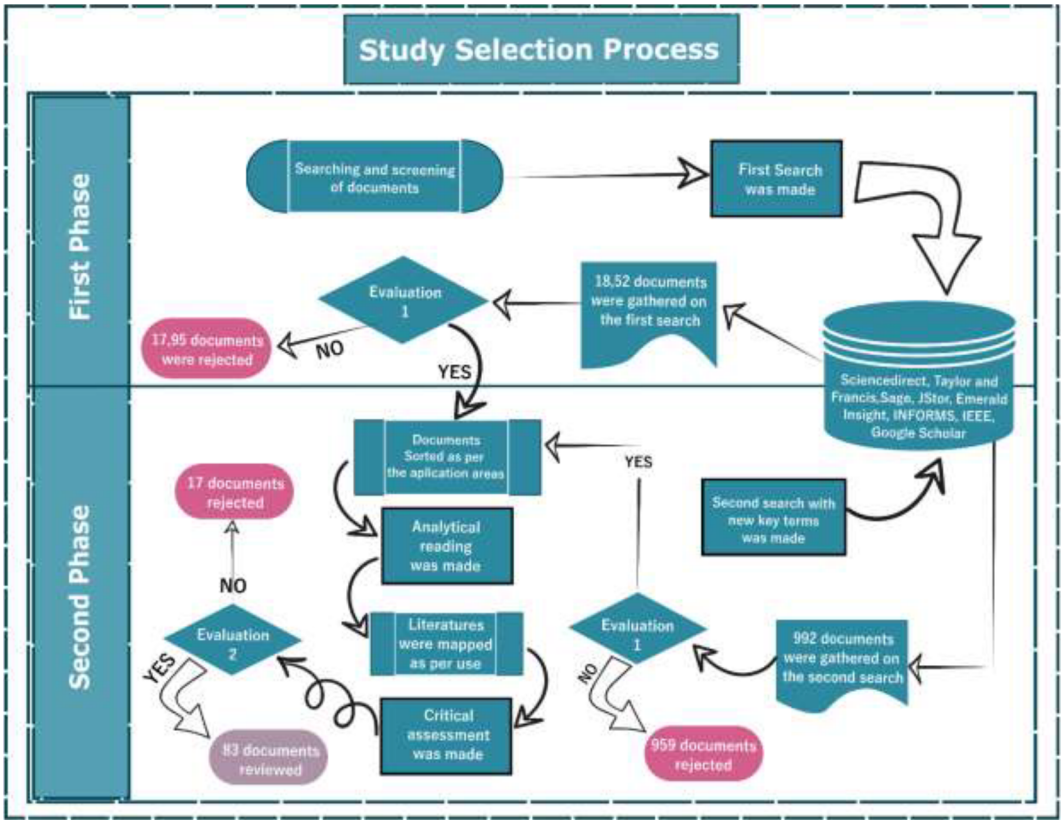


Fig. 3. Steps for conducting this review. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Table. 4
An annotated list of the primary sources.

Usage	The publications concentrate on IoT	Healthcare
Legislative structure	[14,15,55]	[7–9,73,76]
Integrating BCT with IoT	[48,54,58,76–88]	[89–93]
Security	[12,26,47,48,77,79,94,95,29,96,97,29,98–102]	[25,28,93,95,99,105–109]
Information managing	[39,76,89,95,29,96,97,29,112–115,29]	[27,30,66,91,110–115,29,116]
Smart city	[77,119–122]	×
Methods of medication distribution	×	[128–133]
Industry	[88,132]	–

expanding their throughput and scalability is currently a challenge. Keeping considerable volumes of photographic data [88] on a blockchain presents additional challenges due to concerns around data security [89–95,29,96,97,29], the amount of available storage space [98–110], and the associated costs [111–115,29]. Because of this, it can be challenging to keep image data [116] that is big enough to warrant having its blockchain [117].

4.2. Combining BCT with IoT

The authors use blockchain [118–122] in a context that utilizes the IoT [123] so that they can reap the benefits of utilizing both technologies simultaneously [124–126]. However, the decision will be made based on several different factors, including the regulatory climate of the domain of application in which the instantiation will be developed, the requirements for throughput and latency [127], the throughput and latency requirements [128], and the scalability of the players involved in the blockchain. In light of this, two articles have been published that attempt to divide how blockchain and IoT can be integrated into three distinct categories. During data exchange between IoT devices, segment your integration choices according to the volume of data that will be exchanged via blockchain [78]. On the other hand, the article [129] draws parallels between blockchain and cloud computing in terms of service offerings two schools of thought, rather than competing with one another, offer something that the other excels at doing better. As an illustration,

while [78] lays a particular emphasis on the relationship between BCT and IoT devices, [129] expands this connection to encompass the cloud. Data should be tamper-proof during its entire existence [115], in addition to having high credibility, decentralization, and security [38]. It is essential to take measures to safeguard data ownership [42].

Therefore, in the first type of integration, blockchain is not involved in the actual exchange of data between IoT devices; rather, it works as a way of storing some of the data or the metadata of the real data, which is a form of usage that is often referred to as off-chain usage. This is because BCT is not utilized during the actual data transfer between IoT gadgets [78]. Blockchain is not involved in the actual exchange of data between IoT devices because, in this first type of integration, blockchain is not involved in the actual exchange of data between IoT devices. In the first form of integration, blockchain is not included in the process of exchanging data between the IoT devices themselves. This is because BCT is not currently incorporated into the process of information sharing that takes place between IoT devices. Either the data itself or the metadata describing the data can be recorded using blockchain in this scenario. This configuration is referred to as Cloud over Blockchain (CoB), and it is employed by the integration technique that was just described. This is because it enables a continuous connection to the cloud without regard blockchain as the primary service outlet. Because the second architecture offers extensive support for the integration of BCT, all of the data that is generated by the interactions of IoT devices is transferred using blockchain. This is because BCT is decentralized and cannot be altered. Blockchains are decentralized computer networks, and this design makes use of them to carry out the process of service delivery.

The cloud computing model, on the other hand, makes use of networks of computers that are centralized in one location. On the other side, BCT relies on cloud services to get analytical and virtualization capabilities. This architecture is referred to as Blockchain over Cloud (BoC) architecture in the cited material that was previously mentioned. Using the blockchain and various IoT devices, a significant amount of data is sent in the final configuration. Because of this, it is now feasible to make use of the benefits offered by both types of technology at the same time. This technology, which is also known as Mixed Blockchain-Cloud (MBC), is explored in [129], which studies it from the point of view of the superiority of cloud computing in comparison to BCT (see Table 5).

Table. 5
Integration of BCT and IoT that were used in a variety of publications for SC and DSM.

Publication	Description of methods used in IoT & BCT	Combination of IoT & BCT		SC	DSM
		IoT – IoT	IoT + BCT		
[120]	Intelligent cars can communicate with one another, and the data from these exchanges are kept in both the main blockchain and the local dynamic blockchain (LDB).	✓	×	×	✓
[77]	A cluster-based overlay network was developed to improve communication between the cloud and the smart home. This network was designed to fulfill the goal. The leaders of overlay clusters are the ones who are tasked with the maintenance of a public ledger that is always up to date with the most recent transaction records from all nodes and contains all previous records. This ledger keeps track of requests for data and the responses that are sent to those requests.	×	✓	✓	×
[91]	The information that is gathered from wearables and vendors will have their hash values recorded and kept in the blockchain. In addition to this, records of previous visits made by both providers and insurers are also kept for future reference.	✓	×	×	✓
[119]	After connecting the main network, move on to connecting the edge network to the IoT devices (the blockchain). Before passing along the information they have received to the primary network, edge nodes will perform some initial processing on the data that has been sent to them.	✓	×	✓	×
[87]	An intermediary edge network needs to be set up to connect the core network to the devices that make up the IoT. Before passing along the information they have received to the primary network, edge nodes will perform some initial processing on the data that has been sent to them.	✓	×	✓	×
[83]	Edge computing is used to collect information from IoT devices, then process and evaluate that information before transferring it to a blockchain.	✓	×	✓	×
[29]	On the blockchain is recorded every query that has ever been made against the data.	×	✓	✓	×
[107]	While the cloud is used to store PHRs that have been encrypted, BCT is utilized to manage metadata and keep track of who has accessed what. The gateway server performs an essential function within the system.	✓	×	✓	×
[104]	On the blockchain, we keep some data together with references to much larger picture data. These picture data references can be rather large. They came up with the idea of the data lake to facilitate the management of enormous databases.	×	✓	×	✓
[88]	As the original data is stored in an encrypted cloud-based data block, the hash value is recorded on the blockchain. BCT is distributed across multiple computers. Each component is stored on a different server, often in a different physical location.	✓	×	✓	×
[29]	Modifications to the blockchain are handled by the Mobius server, which uses information gleaned from communications between IoT devices and the app.	×	✓	✓	×
[105]	The identity of the patient who owns a set of photographs, the entities to which the patient gives access, and the node from which the image was obtained are all recorded on the blockchain. The blockchain also contains a record of the access permissions for each patient.	×	✓	×	✓
[85]	The cloud is where the blockchain resides in the three-tier paradigm, making it the key hub where cloud providers can record the services they have given and communicate data with one another. This makes the cloud the most important component. In addition, BCT is utilized in the delivery of improved services at the fog node level. Within the confines of the blockchain, there will invariably be some data movement.	✓	×	✓	×
[84]	The cloud service that is used to verify the legitimacy of financial transactions safely and dependably includes a component known as the blockchain.	✓	×	✓	×

4.3. Blockchain and information technology security

In the context of the IoT, research has largely centered on information security and more especially data protection. Regardless, the BCT is adaptable enough to deal with many other types of security issues. What follows is some discussion of why using BCT for this purpose is beneficial. However, in the part that follows on the administration of data, we discuss data security. The article [11] discusses the different ways in which BCT can assist in overcoming the security concerns that are linked to the IoT. [12] conducted a literature review on the implementation of BCT to strengthen security, with a particular emphasis given to the protection of IoT. The potential benefits of BCT in terms of security have been the subject of debate in several other studies [45,46,29,101]. These studies are related to the IoT. As a direct consequence of this, the following advantages are generated in this context:

- It is feasible to maintain track of and manage the identities of objects for the course of their useful lives due to the immutability of the transactions that are kept in a blockchain. This makes it possible for items to have many uses.
- Fault tolerance in IoT devices can be accomplished by utilizing technologies such as encryption and distributed ledgers to realize this goal.
- The usage of smart contracts makes it easier to authorize users, protects the integrity of software, improves synchronization between software, and increases privacy.
- Establishing encrypted communication between IoT devices can be made much easier if there are lightweight security protocols available that are based on BCT.
- Due to the decentralized and distributed nature of blockchain, it is possible to eliminate single points of failure.
- Because it has a larger address space than IPv6, BCT is an excellent choice for preventing collusion when providing a graphical user interface (GUI) to IoT devices. In contrast, IPv6 only supports approximately 4 billion unique addresses.

Although these benefits exist, a significantly higher amount of emphasis has been paid to the topic of data security in the relevant literature. Information assurance is a subfield of data administration, which we shall talk about in the next paragraphs.

4.4. Data management (DM)

DM is taken to gather, process, secure, disseminate, store, and retrieve data. The DM strategy taken may be affected by the requirements of an application domain, the architecture chosen for the system, and the intended outcome of its implementation. A plethora of BCT-based data management strategies have been offered by the academic community. There are substantial distinctions between the IoT and healthcare that might make the adoption of BCT for data management appear very different in each setting. Those developed specifically for the IoT account for the vast number of sensors and the ad hoc character of the networks that comprise it. Healthcare experts know several considerations must be made while developing new systems, including minimal latency and stringent privacy. The implementation of BCT for the management of data is influenced by a great number of factors. To begin, the IoT, which includes HIoT, relies mostly on sensors to collect data from various connected devices. The exponential rise in sensor installations over the past few years heralds a new era of worldwide sensor networks. This, in turn, calls for the creation of a cutting-edge data management system [130]. In addition, these gadgets produce a great deal of real-time data streams, which has led to the emergence of big data 3.0 [131].

On the other hand, standard data management systems do not have the scalability required to deal with enormous amounts of data [132]. As a consequence of this, it is necessary to create a data management system that is more trustworthy. Thirdly, the current data management systems that are used in healthcare and the IoT are dependent on interactions between clients and servers, which makes them susceptible to the existence of a single point of failure. This is a problem because it is difficult to reliably transfer data between clients and servers. Worse, the current design, protocol, and tactics of dispersed networks are not suitable to satisfy the growing service requirements and new issues that are being experienced [76]. The fact that the data is stored on many servers, some of which do not encrypt the data, is the fourth reason why there is potentially a security issue.

The data storage mechanisms of blockchain-based systems, on the other hand, make use of a broad variety of encryption methods to protect the data they store. The ability of systems enabled by the IoT to carry out data management responsibilities both online and offline presents a challenge for more conventional methods [133]. This is the sixth benefit that comes with having systems that are enabled for the IoT. The result of this is those traditional methods of managing data are facing a huge challenge as a result of their situation. Therefore, scientists have been trying to find a data management system that can tolerate delays, makes efficient use of available channel bandwidth, permits the transfer of manageable data packet sizes, and consumes as little power as possible [134]. Consequently, blockchain is considered a resource for addressing such challenges, although it does not meet all the requirements. Besides these benefits, there are more compelling arguments in favor of using BCT for data management. These reasons include the fact that BCT can: The articles that were examined make use of a wide variety of approaches, which are presented in Table 6.

4.5. Data acquisition

The use of BCT could simplify the process of data collecting, which is an element of data management. The capacity of the technology to securely provide a unique identification to things, entities, and humans at each stage of the authentication process suggests that this goal may be easier to achieve than previously thought [135]. With blockchain's distributed ledger, we may reliably collect data from the source of our choosing. Developments in distributed consensus approaches have allowed for improvements in

Table. 6
Various methods that are used to ensure the integrity of the data.

Ref	Data integrity methods	Domain area IoT	Health sector
[89]	Checking the equivalence of Magnetic Resonance Images (MRI) using radiometric characteristics (shape features)	×	Systems for imaging with MRI.
[29]	Lack of information necessitates proof	×	Data management for clinical trials
[97]	The Content Identification Protocol (CIP) for the Interplanetary File System (IPFS).	Nonspecific	-
[88]	Public encryption algorithms, lightweight ring signatures, addition rotation, exclusive OR ciphers, and so on are utilized for security.	×	Connected Health Devices
[26]	Before being stored on or off-chain, data undergoes encryption and hashing procedure.	×	Electronic Health Records (EHR)
[111]	Concealing a block's hash value in encrypted form.	Nonspecific	×
[119]	Digitally signing and hashing data with the Argon2 hashing algorithm for blockchain storage	The Intelligent Metropolitan Area	×
[100]	The Merkle tree format and the Chain point open standard makes it possible to track down the origin of every data modification. Therefore, you can have peace of mind knowing that your information is safe.	×	HIoT
[33]	Keccak 256 is used to hash data, and that hash is stored in a smart contract.	×	Medical records repository
[95]	By using a smart contract to produce automatic notifications of health occurrences for the users, any attempts to tamper with the system are immediately revealed.	×	HIoT

authenticating messages, transactions, entities, and keys, allowing for more reliable information acquisition from the correct sources [136]. When looking at the reviewed literature, we found a wide variety of authentication methods. Manager Servers (MS) are specialized machines that, in the context of the IoT, make use of the private keys stored on other devices to uniquely identify such devices. As detailed in [25], secure virtual zones, often referred to as bubbles with the group ID, are utilized to permit secure communication between nodes. In the healthcare industry, for instance [98], patients are given a Virtual Identity that is constructed using the qualities of blockchain that allow for pseudonymous naming. You could also [109] utilize an interactive voice response system to verify user identity (IVRS). It is common practice to utilize public and private key pairs to verify an individual's digital identity, as explained in [106].

4.6. Data processing

Since smart contracts are crucial to the operation of blockchains, they are typically used by these systems for all processing operations. Examples include [26], which uses six smart contracts, [94], which uses four, [97], which proposes to use as many as the number of "sidechains" that will be established, [92], which uses three, and [99], which uses one smart contract for each resource owner. Instead, the authors develop several architectural methods for data processing, such as user nodes with more resources specifically for processing [75]. Cloud computing, business process outsourcing, and fog computing are all examples of offloading shown in the cited works [83–85]. Create a hierarchy on the blockchain [93,120]. Latency is affected by these architectural choices because it may be harder to get agreement on a single, universal truth when layers of hierarchy and partitions are present.

4.7. Data security

It has been noted that the primary concerns of blockchain-based systems are maintaining data integrity, regulating user access, and safeguarding user privacy. This is although data security encompasses a range of different problems [137]. Security concerns are not separate from one another; rather, they are intertwined and interdependent on one another [138]. Several studies [111,135,136, 139–154] have focused their attention on certain topics of data security such as data integrity, access control, protection of individual confidentiality, etc., which are discussed below.

4.7.1. Data integrity

The term "data integrity" refers to the process of verifying and updating data for accuracy and consistency [111]. Previous publications, such as [135,136], elaborate on the idea that assuring the data integrity of a system entails preventing, locating, and repairing any potential errors with the system's data. Data integrity difficulties can be avoided with the help of journaling and encrypted file systems [137–139]. Check-summing, mirroring (CSM) [139], the Cyclic Redundancy Check (CRC) [140], and parity are only some of the methods that can be used to detect potential risks to data integrity [141]. Majority voting and RAID parity are two methods that can be used to fix data integrity problems.

4.7.2. Access control

One of the cornerstones of every security system is the ability to regulate who has access to what. It's been studied by scholars from several fields over the years [142–144]. The Object, Model, Architecture, and Mechanism (OMAM) reference model is used in one classification of IoT access control systems [137]. The paradigms of Role-Based Access Control (RBAC) [145], Attribute-Based Access Control (ABAC), Usage-Based Control (UCON) [146], and Capability-Based Access Control (CBAC) [147] are addressed (CapBAC). On the contrary, designs incorporate mechanisms like Open Authorization (OAuth), Extensible Access Control Markup Language (XACML), and User Managed Access (UMA). Models and architectures like this are used to implement practices like Access Control Lists (ACL), which help organizations conform to regulations like ISO/EIC 27,002/27,005 [148]. It is clear, however, from the evaluation and classification provided in [138], that there are many variants of the various access control techniques, including ones that have been studied in the past. Access control can also be implemented in other ways, some of which are discussed in the cited works. [139,140], which combines security measures for protecting sensitive data with access control. Table 7 details a few of the many ACL methods and structures used by BCT-using works.

4.7.3. Protection of individual confidentiality

The literature also deals with the related topic of privacy protection. Data privacy and context privacy are the two main types of privacy preservation approaches, as described in [141]. Contextual privacy addresses issues of space and time, as opposed to data privacy's focus on challenges such as maintaining privacy during data aggregation and querying methods [149]. We surveyed the literature and divided privacy-preserving methods used in conjunction with BCT into four distinct classes [142]. These are 1) secure multiparty computation (SMPC) [150] is used to derive a smart contract or key management system; 2) Identity anonymization employs mixing, ring signatures, and zero-knowledge proofs to conceal the identity of transaction participants [151]; 3) Anonymizing transaction data, or transaction data mixing, differential privacy, zero-knowledge proofs, and homomorphic concealment, is a method for protecting the privacy of transaction contents [152]; and 4) cryptography methods like asymmetric encryption and attribute-based encryption are used to safeguard data while it is being stored on the blockchain, a method known as "on-chain data protection" [153]. Table 8 presents the overview of the publications' respective privacy protection policies.

4.7.4. Dissemination

The distribution of data can take many different shapes. There are two essentially different categories of data dissemination methods, and each one is determined by who starts the transmission of the data; specifically, whether a client requests the data or a server gives it to the client. The first one is driven by push-based dissemination, whereas the second one is driven by pull-based dissemination. In push-based dissemination, clients receive data from servers at the request of the servers, whereas in pull-based dissemination, clients receive data from servers at their initiative. Both methods of data distribution allow for the transfer of information either according to a predetermined timetable or at random, depending on the circumstances. In addition, there are two different modes of data transmission: point-to-point and one-to-many. The data delivery mechanism in pull-based aperiodic data dissemination with point-to-point communication is characterized by request and response. If, on the other hand, the communication is one-to-many, the technology utilized to convey the request and response data is considered to be eavesdropping.

Surveillance is used to supply data via one-to-many communication, whereas polling is used to deliver data via periodic pull-based point-to-point communication. On the other hand, the term publish and subscribe is used to describe the process in which data is delivered at random in a push-based one-to-many connection; the term broadcast describes the process in which data is delivered frequently; and the term triggers is used to describe the process in which data is transmitted aperiodically from one point to another [143]. When it comes to Wireless Sensor Networks (WSN), the data routing algorithms that are utilized can be categorized as either flat, hierarchical, or location- based on the structure of the networks themselves. If how their protocol is used to carry out its functions is used to classify them, then they can be broken down into the following five categories: negotiation-based, multipath-based, query-based, Quality of Service (QoS)-based, and coherent-based [144].

The usage of BCT in the IoT involves smart cities, with information-based smart transport systems being one of them. Consequently, publications such as [114,116] utilize triggers to disseminate data. According to the findings of the study [120], propagation can take place from a single vehicle to a large number of vehicles, or from a single vehicle to another vehicle or infrastructure, all to construct two-tier blockchains (a Local Dynamic Blockchain and a Main Blockchain). According to a study [123], communication between vehicles might take place in a one-to-many or point-to-point form.

4.7.5. Retrieval

When using a BCT-based system, it is best to practice encrypting data at rest. Song et al. [145] first presented Searchable Symmetric Encryption (SSE) [158] as a Boolean search methodology, and it has since been shown to be a useful method of information retrieval. Several authors have contributed to the development of SSE, but Swaminathan et al. [146], who introduced ranked ordered searches for encrypted documents, deserve special recognition for their contributions. Insights from these two methods could pave the way to improved data retrieval systems in the future. However, when image data is encrypted, Lu et al. [147] initially developed a method for retrieving images via encrypted images [153–159]. As the image data was being encrypted, this happened. This system has evolved to incorporate features like enhanced privacy protection [159]. A method for retrieving encrypted images that preserves user privacy was developed by Ferreira et al. [148], and this area of study is active at present. Although these factors should be considered, the reviewed literature does not concentrate heavily on data retrieval.

The other work [29] to address this issue is, which positions blockchain as a contract service between biological databases and data

Table. 7
Various access control methods are used in IoT & health domain.

Ref	Access control	Domain area	
		IoT	Health sector
[99,112]	Make use of smart contracts as a mechanism for the enforcement of policies, which grants authorization via tokens.	Generic	×
[107]	Modularity and fine-grained control are utilized for proxy re-encryption. Moreover, an access-list-storing gateway server acts as a sort-of trustworthy third party.	×	Personal Health Records (PHR)
[97]	Each sidechain has a dedicated validator node that monitors and enforces access requests and other sidechain-specific rules. A worldwide group of validators is in charge of regulating who can join the network from the outside. In addition, they use IPFS, which helps spread control over which files can be accessed by whom over the network.	Generic	×
[94]	A decoder is used to convert between ACL, Capabilities, and Attributes, the three primary representations of the many various access control models and methods. The authors believe this could pave the way for model interoperability.	Generic	×
[104]	The usage of a multi-signature approach is expected to achieve access control, and the capabilities of the NEM blockchain platform make this possible, allowing for safe data transfer and protection of access controls.	×	Information about diabetes healthcare
[75]	Ad hoc management nodes are small, lightweight nodes that do not permanently store any blockchain data. When needed, they connect to the blockchain and serve as a means of access control.	Generic	×
[91]	To get enrollment and transaction certificates of nodes and Hyperledger CA.	×	Programs for healthcare-related mobile devices

Table. 8
Various privacy preservation methods are used in IoT & health areas.

Ref	Privacy preservation approaches	Domain area IoT	Health sector
[97]	The network is divided into smaller "sidechains," and a log of all activity is kept at each node.	Nonspecific	×
[107]	Semi-trusted entities are used to perform tasks like user authentication, data re-encryption before delivery to requesters, and record maintenance on the blockchain.	×	PHR
[95]	Confidential consumer transaction data is encrypted using Attribute-Based Security.	Nonspecific	-
[88]	Using public encryption methods in conjunction with a lightweight ring signature.	×	HIoT
[38]	TSMPC (Threshold Secure Multiparty Computing) protocol is used.	Generic	×
[26]	Blinding technology for redistributed proxy re-encryption.	×	EHR
[29]	The building of a smart contract includes the use of a zero-knowledge proof function.	Smart meter	×
[98]	Encryption based on Pseudonyms Utilizing Multiple Authorities (PBE-DA)	×	EHR
[77]	In this architecture, lower-level devices interact with a centralized Immutable Ledger (IL), while higher-level devices interact with a public blockchain that is accessible to everyone.	Smart home	×

consumers. Data on a blockchain provides unarguable evidence of data retrieval activity by comparing the hash values of a query with the hash values of a return. The integrity of the blockchain will be ensured by this comparison. The following research demonstrates that there is a split in the academic community over whether or not data extraction from a blockchain constitutes a transaction. A few sources (e.g., [28,37,75]) take the latter tack, while [75] does not count it as a transaction unless it involves a critically important access control system. In addition, the literature is unclear on who should have access to what data in a blockchain and how that should be done. A user decrypts data on their own but retrieves it from a Private Accessible Unit (PAU), as described in [38,107], and [108]. The results of a query must be decrypted by a leader, as stated in [38]. According to [107], re-encryption occurs at the gateway server, while decryption occurs at the requesting node. According to [108], decryption is performed locally by the user. However, a healthcare provider, a patient, or a healthcare insurance provider are all considered appropriate referrals for a query [91].

4.7.6. Data storage

The blockchain has been described as a decentralized database by several publications. Blockchains and distributed databases sometimes get confused with one another, yet they are very different technologies. When employing a blockchain, a central authority is unnecessary because several copies of the data are kept at various nodes [160]. The purpose of distributed database administration is to increase database throughput by decentralizing data access and processing. Furthermore, in a distributed database, data saved in multiple nodes are not identical [146]. BCT stands apart from other distributed databases because it includes a smart contract, a self-executing piece of code [41]. External storage, in which nodes transmit data directly to a base station or gateway without intervening processing, and local storage, in which nodes store data on their own, are the two most common ways of data storage in an IoT scenario. Finally, we have data-centric storage, in which nodes are selected to store data based on a set of criteria [149,150].

There are inconsistencies when considering blockchain from the standpoint of information storage. These emerge for a variety of reasons, such as the legal requirement to safeguard individuals' privacy, the imperative of providing rapid responses to requests, and the sheer volume of data that must be maintained [161]. This condition leaves the healthcare business vulnerable to several legal challenges, heightening its sensitivity to patients' privacy concerns [162]. In addition, data storage costs are proportional to data volume. Since radiology generates most of these extremely large files, they are processed otherwise than conventional research data such as laboratory results. CT scans, x-rays, MRIs, and ECGs are just some examples of the types of imaging data that can be kept in a blockchain efficiently and cost-effectively.

Some examples of published works are [104], which proposes storing metadata on the blockchain, [26], which created a data lake for storing large files off-chain, and [105], which used the blockchain to register only the list of images [106], the names of patients, the names of individuals with access to the images, and the parties that have access to the files throughout their entire existence [110]. This finding was recorded [104]. The many laws and their ramifications have been the subject of numerous written works. In [106], for instance, the Fast Healthcare Interoperability Resources (FHIR) standard is highlighted for its significance in the field of medical data storage and transfer.

The standard used by the system necessitates the storage of data pointers on the blockchain [163]. Additional research is being conducted on the European Union's General Data Protection Regulation (GDPR) [113]. The length of time that data can be kept is restricted by this rule. One criticism leveled with BCT-based systems is that they are inherently uncontrollable. However, ontology is used by the authors to solve this problem. One way to accomplish this is by educating the public about security threats. They use it in a system to evaluate intelligence policies, which necessitates managing users' permissions for collecting, utilizing, and erasing information.

4.8. Use of blockchain in smart cities

A smart city provides a multitude of benefits, some of which include improved accessibility to government services, facilitation of civic engagement, active infrastructure, optimal resource utilization, more sustainable livelihoods, improved quality of life, and the provision of educational and environmental services. The authors of [10] assert that the primary objective of a smart city is to raise the living standards of its residents through the implementation of cutting-edge technology like blockchain to maintain suitable environmental conditions. It was proved that a platform built on top of the Hyperledger Fabric permissioned Blockchain system is both practicable and efficient due to the notion of profile management that was created by the authors of [11]. The design concept presented a relevant analysis and exhibited Blockchain's capacity to handle data using a blockchain network that offers complete data protection. Any infraction is logged permanently, and related parties can easily obtain access to this information.

The smart city notion, which is a subset of the broader smart planet initiative, can be conceptualized in two ways concerning its actual, concrete boundaries [153,154]. Building a smart city is difficult because of the deluge of big data, which requires the real-time management and analysis of huge amounts of complex data. Moreover, there are challenges of structural scalability, network bandwidth limitations, single points of failure, infrastructure security, operational security, and environmental and government regulatory policy compliance to address [119,122,153,155–157]. The challenge of resolving these challenges is exacerbated when private enterprises are involved in the development of smart city projects. Concerns about data privacy, muddled economic motivations, and a lack of community involvement are only some of the issues raised by [158] against these "corporate smart city" initiatives. Research into BCT's potential as a solution to these and other problems is ongoing now. have a significant effect, as evidenced by the growth in the volume of literature addressing its use. In response, authors like [117,119] show how researchers have presented frameworks for incorporating BCT into smart city applications.

As stated in the cited article [117], BCT serves dual purposes. Specifically, it links prosumer-level electronics to a smart meter. Additional intelligent gadgets and sensors, such as the smart meter, are built into the microgrid as well. In this configuration, the microgrid serves as both a data hub and a means of energy distribution. On the other side, every house is connected to the blockchain so that data may be shared between the neighborhood and the smart grid. The authors claim that installing systems of this type would give neighborhoods more say over their energy budgets. In [119], edge computing is located between the blockchain (the core network) and the IoT devices. The purpose of edge computing is to reduce the workload on the blockchain by processing data at the network's edge before sending it there.

For the network architecture of a smart home, as depicted in [122], blockchain sits above the smart home network but below the cloud computing network. This layout emphasizes the importance of a smart home network. A block manager oversees the creation, verification, and sequential ordering of the blocks that include the transactions related to smart homes. The authors of [118,120] focus on the role of BCT in the larger field of ICT as it relates to transportation. In [118], the author summarizes the use of BCT in intelligent transportation systems (ITS) by detailing the seven phases in which BCT is used. By doing so, we seek to demonstrate the mutual benefits of these two technological advancements. Findings from this study point to real-time data distribution as BCT's most fruitful use in intelligent transportation systems.

The system proposed by the authors of the study [120] involves the purchase of a car as the initial step, with further accomplishments in the realm of vehicular traffic leading to the accumulation of points or tokens. Their grading scale is called Intelligent Vehicle Trust Points (IVTP) [164]. The system employs reward points as compensation, much like Bitcoin does for its miners, except the award is conditional on a performance parameter connected to traffic. They propose constructing a blockchain system with a user-facing decentralized layer and an underlying central, more secure layer. Local blockchains are forked and can only keep data for a finite amount of time, while IVTP transactions are recorded on the main blockchain in the same way that Bitcoin ones are [165]. Many authors, including those in [80,121], have discussed extensively smart grids. Regarding [121], a comprehensive analysis of the various uses for BCT is provided. To prevent data tampering in the power generation and distribution sectors and to facilitate peer-to-peer energy trading, BCT may be used in combination with the smart grid.

The implementation of smart cities is greatly aided by the use of ICT. The successful delivery of public services to citizens and the improvement of city management can both be aided by the systematic collection and examination of data. The applications of big data technology to smart cities have been researched and analyzed by Al Nuaimi et al. [166], who also conducted a study of the prospects, difficulties, and benefits. To facilitate a quick, efficient, and accurate traffic management system in smart cities, Djahel et al. [167] have provided a comprehensive survey of the technologies (such as machine learning) used in various stages of today's systems, from data collection to service delivery. The study [168] focuses on storing data in the cloud as their primary topic. It has been suggested that a blockchain-based system like BlockDS may be used to store data safely and guarantee its integrity. Three separate parts make up the system: the data proprietor, the data consumer, and the blockchain nodes. Documents about the individual are provided by the owner of the data. A list of keywords is included in each document. A person who subscribes to their documents is considered to be a data consumer. A component that performs keyword searches is utilized by the data consumer to retrieve only the required documents. In a federated cloud, the blockchain nodes are represented by individual cloud service providers. In the method that is now being considered, encrypted documents are kept in a cloud data storage system that is not part of the blockchain, whereas encrypted keyword identifiers are kept on the blockchain.

Batty et al. [169] have provided a detailed analysis of smart cities, which includes research aims, research problems, scenarios, and project areas. The study [170] has provided a detailed review of the topic of smart cities, beginning with a description and moving on to application domains, architectural designs, essential enabling technologies, and research problems. The study [171] analyzes the problems and potential solutions that arise regarding information security in smart cities. Research conducted by [172] on an urban IoT system looked into the enabling technologies, protocols, and architecture. In the article [173], they analyze the benefits and

drawbacks of six different IoT-enabled trash management models, with a particular emphasis on waste management in smart cities.

4.9. Blockchain and the supply chain for pharmaceuticals

Counterfeiting, sub-standardization, and diversion are just some of the fraudulent behaviors that can be difficult to manage while managing the supply chain for pharmaceutical commodities (taking medicine and selling it on the black market) [124]. There are a few distinct ways that a product can be counterfeited: (a) with minor changes made to the original, (b) by copying the information from the original product to make a forgery, and (c) by completely wiping the information from the original and using it to produce a fake [159]. To get past these issues, people have turned to various methods, such as pill-recognition software and smartphone verification systems. Individual pills are being outfitted with radio frequency identification (RFID) micro tags, and information from a wide range of sources is being aggregated [166]. We also used several technologies, including online verification and machine learning, as extra precautions. BCT [124], on the other hand, is based on distributed ledgers and is IoT-friendly, therefore it is also being investigated.

Blockchain is seen as the most trustworthy, open, traceable, verifiable, and resistant to the introduction of counterfeit drugs among all these processes [124,125]. The necessity to protect the privacy of pharmaceutical customers [126] and the absence of regulatory guidelines are two of the biggest obstacles to BCT deployment. However, there are alternative system ideas that are based on BCT. Therefore [125], organize a system that makes use of barcodes printed on tablets and readable by the users' mobile devices. To ensure the integrity of the drug supply chain, every person or entity that handles the medicine must scan the code and verify its authenticity. The distributed ledger (blockchain) [167] records the code, allowing for the traceability of the dispensed drug.

Similarly, [127] sets up a process to guarantee the openness of all data about the worldwide distribution and sale of pharmaceuticals. Their network consists of four core elements: alliance members (the government and manufacturers) [168], full nodes (wholesalers and hospitals), and regular nodes. It is the responsibility of Alliance members to grant mining licenses (pharmacies and consumers) [169]. The plan calls for using a public key to generate a QR code that can serve as the drug's unique ID. The pharmaceutical bottle features a QR code for easy access to relevant information. A medication's hash value, location, and timestamp with the date and time of manufacturing are all recorded on the blockchain. Unspent Transaction Outputs (UTXOs) and private keys can be used to detect fraudulent transactions such as sales to unauthorized individuals or distribution by unlicensed parties [170–174].

The characteristics of blockchains have presented a variety of benefits to a wide range of industrial domains, and they have the potential to become an effective tool in DSM applications. MeDShare is a system that was proposed in the study [171] for authenticating data, performing data audits, and providing data protection during the exchange of medical data in an environment that is not trustworthy across multiple entities, such as research and medical institutions. MeDShare was built on BCT, and it makes use of smart contracts, to effectively identify data behavior, as well as to detect cyberattacks on the entities' offending activity. A new data preservation system (DPS) was presented in the study [172], and it would make use of BCT as a dependable storage solution. This would ensure that the data that are kept are both primary and verifiable, while also safeguarding user privacy. This system utilizes the integrated blockchain and DPS to support frameworks and permanently maintain critical data, while also providing the capability to verify the authenticity of data if there is a suspicion that it has been manipulated. A study [91] describes the development of a framework for cross-domain picture sharing. Within this framework, a blockchain is used as a distributed storage to construct a ledger of radiological examinations and patient authorization. The creation of this framework gets rid of the need for third parties to protect medical data, satisfies the requirements for an interoperable health system, and expands its application to domains other than medical imaging.

Serial numbers are allocated to pharmaceutical products, and other security elements are added to each product so that they can be validated by customers and distinguished from fakes. The transparent and chain code-based transactions enabled by BCT also contribute to an increased level of security. Trust and transparency are essential components of the pharmaceutical sector. This is because, in the absence of trust, the business of counterfeiting pharmaceuticals grows, putting the general population in danger from the consumption of low-quality or inferior medications. According to a study [166], the utilization of blockchain technology in quality control and the identification of counterfeit pharmaceuticals increases overall safety and the prevention of unnecessary deaths. Regarding the percentage of fake medications in circulation, Jraisat et al. [162] investigated the vulnerabilities of traditional drug supply chains and found that these chains are vulnerable because it is difficult to track them, which provides possibilities for counterfeiters to put fraudulent items into the market. A management and recommendation system for the drug supply chain that is based on BCT and machine learning (ML) has been presented. Both an ML-based drug recommendation system and a blockchain-based DSM system are connected to the system using REST APIs. The evaluation of blockchain applications for the pharmaceutical business was discussed by Alshahrani & Alshahrani [173]. They revealed that healthcare professionals' attitudes, a lack of cooperation, and economic disparity were the primary barriers to blockchain adoption in the pharmaceutical industry in Saudi Arabia. System resilience, data safety, enhanced supply chain management, decentralization, interoperability, and government regulations and legislation were also mentioned as variables that could assist blockchain applications.

The authors of [174] examined the architectures of using blockchain for drug traceability as well as the issues that come along with adopting this technology. They discussed problems with product traceability in the pharmaceutical supply chain and highlighted potential solutions for making efficient use of BCT in tracking and tracing to prevent the sale of fake pharmaceuticals. The authors did not cover BCT or the concerns and challenges linked to other domains of the technology's uses in the pharmaceutical sector.

In the study that Alladi et al. [29] conducted, the authors offered a method for the management of medication supply chains that are based on a blockchain technology that is deployed in Hyperledger Fabric. This method depends on smart contracts to ensure supply chain safety and security. In the study [139], the authors proposed a decentralized application that would support immutable tracing by utilizing blockchain and serialization technologies. The research [153] made a recommendation for a way to stop the sale of fake

medicines from getting into the supply chain for pharmaceuticals. Proof of ownership was established through the use of blockchains. This is significant because, before a drug is administered to a patient, ownership of the medication passes from the producer to the distributor to the pharmacist. The authors detailed the difficulty posed by the ability to readily clone RFID tags, emphasized the capacity of blockchain technology to overcome this difficulty, and added additional features to the chain. To ensure that only parties who could be completely relied upon joined the network, a blockchain with permissions was developed.

In addition, the study [163] proposed a framework that is built on a simulated blockchain and provides support for the biopharmaceutical supply chain. Proof of authority and smart contracts form the foundation of the proposed framework, which has also been subjected to a preliminary empirical investigation to evaluate it. The double-spending problem for medicines (sometimes known as "spending" the same drug twice), which is analogous to the double-spending problem for digital currency, inspired the development of the Gcoin blockchain [151]. After a drug has been registered on the blockchain, which verifies its validity through the use of a drug-specific QR code scanning technology, Gcoin ensures that it cannot be replaced with a fake version of the drug. At the precise instant that each medicine is manufactured, a QR code is generated [157]. PharmaCrypt is a blockchain-based technology that was produced in a study [158] to prevent the counterfeiting of pharmaceuticals. This tool was developed based on feedback from interviews with pharmaceutical industry specialists and blockchain industry experts, which helped to establish the software requirements. Putting a wireless sensor into the packaging of medicine as part of a solution for the IoT enables real-time location tracking to its final destination [159]. A comparable IoT option involves affixing a chip-enabled label to the packaging of the medication. Another tracking idea involves establishing a distinct identifier for each drug, with the expectation that all relevant parties will utilize the identity to access information regarding the drug's handling and history [160].

5. Discussion

The IoT and healthcare will be two of the key areas of focus as we investigate the potential applications of BCT in the realm of data management [171]. The methods used to integrate BCT and IoT are also broken down and examined in detail for more transparency. Because of this, it's important to look at some previously published papers to see how other researchers have approached bringing BCT into the IoT [29,116–124]. The many steps taken throughout the process will be revealed. Data collecting, processing, and storage are also covered, as they are integral parts of blockchain-based systems and thus deserve their section. Processes like encrypting [172], dispersing [173], retrieving, and storing [174] data fall under this category. To keep blockchain-based systems running, all these methods are implemented. The pharmaceutical industry's supply chain and smart city applications for BCT are also covered in this article.

The DSM can benefit from SC in a variety of different ways [175]. To improve different aspects of urban life, including transportation, logistics, and healthcare [176–178], SC implements cutting-edge technologies and data-driven systems. Integrating smart city infrastructure and solutions into the DSM can result in the realization of several beneficial outcomes. Here are some possible advantages:

- **Enhanced visibility and tracking**

Complete supply chain visibility for DSM can be provided by SC technologies such as sensors connected to the IoT, radio frequency identification (RFID) tags, and real-time monitoring systems [179]. This makes it possible for stakeholders to monitor the flow of pharmaceuticals from producers to distributors to pharmacies and, finally, to patients [180]. Increased monitoring helps prevent the production of counterfeit medications, cuts down on theft, and protects the integrity of supply chains [178].

- **Efficient inventory management**

SC technology can automate the processes involved in inventory management in healthcare organizations and pharmacies [181]. Connected systems can, for example, monitor stock levels in real time, automatically commence reordering when inventory reaches a particular threshold, and optimize storage and distribution to avoid waste and stockouts [182]. Connected systems also can automate reordering when inventory reaches a certain threshold.

- **Predictive analytics and demand forecasting**

Predictive analytics can be used to assist in anticipating drug demand patterns [183]. This is accomplished by examining data that has been acquired from a range of sources within an SC, such as EHR, prescription data, and demographic information [184]. This makes it possible for production planning and distribution to be more precise, which in turn reduces the likelihood of stock-outs or surpluses.

- **Improved delivery and logistics**

The infrastructure of an SC has the potential to make it easier to administer medication in a way that is both effective and kind to the environment [185]. For example, algorithms that are intelligently routed can optimize delivery routes, which in turn reduces congestion and lowers the amount of gasoline used [176–178]. It may be possible to complete the final leg of delivery using a drone or an autonomous vehicle, particularly in locations that are difficult to reach or in the event of an emergency.

- **Real-time monitoring of temperature and storage conditions**

To preserve the effectiveness of some medicines, such as vaccines and biologics, they have to be kept at a particular temperature and in a particular environment while they are being stored. Through the use of smart city technologies, it is possible to provide continuous monitoring of temperature, humidity, and other environmental conditions to guarantee the correct storage of drugs at every stage of the supply chain [171–173]. In the case that there is a deviation from the norm, notifications can be created, allowing for prompt action to be taken.

5.1. Incorporation of BCT and the IoT

Like the IoT, BCT is ubiquitous [3,64]. Further, BCT deployment can be advantageous to many kinds of applications. Although it is beneficial to apply both technologies together in an integrative manner, the amount of work required to do so varies depending on the qualities of both [44–50]. For example, IoT devices have limited processing power and battery life, and using different blockchain-based consensus mechanisms can cause delays [52]. Additionally, there is restricted web access for IoT gadgets [53]. There is a huge number of sensors, but only so much storage space for blockchain and the IoT. The studies discussed thus far have come to three main findings about how BCT and IoT might be combined to achieve various ends [68]. The latency and throughput requirements, data sensitivity, and legal limits all play a role in solution selection. The degree to which BCT is incorporated into pre-existing infrastructure and the extent to which value is transferred to the blockchain are two factors that help define how integration techniques are characterized [74]. We also assess how successfully IoT-connected devices communicate with one another and how well BCT is integrated into existing systems. Some have argued that the first option, known as IoT-IoT, does not fully take advantage of the accessible BCT.

BoC (blockchain of the IoT) [86] is the second method, and it heavily depends on BCT for data storage. The hybrid strategy, on the other hand, involves combining the functionality of an edge [87], fog [88], or overlay network with that of a traditional backbone network [96,97]. The studies [29,98–100] show that, in contrast to other fields, HIoT's dominant design is the first type to use blockchain to store metadata related to actual files [139]. The availability of data connected to medical imaging is primarily responsible for this phenomenon. Using this form of connection in healthcare has the advantage of resolving the bandwidth issue that is linked with the storage of a file on the blockchain, which is one of the advantages of using this type of integration. Additionally, it enables systems based on blockchain to comply with certain regulatory requirements for the safe storage and exchange of data, which is a significant advantage. In [104–106], the complexities of one legislation are examined regarding the applications of BCT. It's a big plus since blockchain-based systems can now adhere to strict regulatory standards for the integrity of the data they store and transmit [72]. This benefit enables systems to meet the requirements of relevant regulatory criteria concerning the secure archiving and dissemination of information. In the cited article [106], the author explores the ramifications of breaking even one of the many rules governing BCT deployment. Hybrid integration, on the other hand, takes advantage of both BCT and IoT simultaneously. This makes it a viable choice where instantaneous response time is crucial. Further, it is a technique that works well in complicated systems with many sensors [28–36].

5.2. Managing data on the IoT and in healthcare

In this research, "data management" [78] refers to the overall set of actions that must be accomplished throughout the data life cycle. Collecting, analyzing, and storing data, as well as sharing, retrieving, and protecting it, are all required to successfully carry out the duties associated with this position [79]. Research [107] suggests that the BCT is helpful for all these tasks related to data management but notably valuable for ensuring data security [80]. Most often, BCT is used to protect information by making sure it can't be tampered with, restricting who can see it, and keeping personal information private. These will benefit a wide range of application enterprises, including those that make use of BCT and the IoT, in several useful ways [81]. As was previously noted, an IoT-based network is composed of numerous devices, all of which produce their own unique data set. One advantage of using a network built for the IoT is that its functionality is not dependent on being connected to the internet. Therefore, it is crucial for the systems created to handle the duties of data management [82] to think about these difficulties while conceptualizing their designs.

The necessity of offsetting the shortcomings of IoT in these data management tasks is a driving force behind the adoption of BCT [83]. This need is being driven by the enhanced record-keeping possibilities made possible by BCT's decentralized nature. Medical professionals are currently looking into blockchain-based data management technologies to see whether they can give patients more say over their health data. Doing so is part of a bigger initiative to give people more say over who sees their health records [66]. An individual's control over who can access their data and how often has grown as a direct effect of a rise in the agency. BCT improves data security in several ways, including the ability to regulate who has access to the data, how private the data is, and how readily it can be accessed [68]. BCT helps to safeguard the data's integrity, ensuring that it is not altered, in addition to improving its dependability, accessibility, control over who has access to it, and privacy for its users. The authors show that blockchain-based systems have already implemented alternatives to traditional user verification, such as speech recognition [70]. User authentication in blockchain-based systems is often implemented through the use of public keys and pseudonym identification [71].

Multiple entities in a BCT-enabled setting can be given unique identifiers using this method. Unique identifiers are typically assigned by architecturally identifying entities, such as management servers. To make data processing easier, smart contracts have been formed, and an architecture that is conducive to data processing has been designed [88]. No one should be too surprised to learn that it could be challenging to secure many smart contracts working together toward a common goal. This allows for a more

straightforward justification for the observed range in the overall number of smart contracts implemented across systems. The study's [108–110] authors found that encrypting data before hashing it, or vice versa, is an effective technique for ensuring data authenticity. A common practice for safeguarding private information. In addition, with the help of third-party systems like IPFS, Argon2, and Chain Point, data structures, digital signatures, and unique identities can be built. Despite much research, the problem of access control and the protection of personal privacy has not been reduced to a single, optimal solution [84]. However, user authentication is now being handled via blockchain systems. Hyperledger and NEM are two instances of such systems. This is possible because these systems include a built-in certificate authority and can generate multiple signatures [166].

Other researchers [111–114] adopt a more structural strategy, such as assigning specific network nodes responsibility for access control. On the other hand, there is a publication [163] that explains how to make use of a decoder so that multiple access control models can be compatible with one another.

It is generally agreed that certain kinds of encryption, such as proxy re-encryption with blinding, attribute-based re-encryption, and pseudonym-based encryption with various authorities, are successful at shielding the privacy of their users [165]. Proxy re-encryption with blinding, attribute-based re-encryption, and pseudonym-based encryption with various authorities are examples of encoding methods that are believed to provide enough privacy protection. Certain encryption methods can be used to safeguard the privacy of computer systems [169–173], in addition to preserving the system's integrity and allowing administrators to exert control over who has access to the system [88]. While some authors [115,29,116–118] recommend splitting the network into several "sidechains" to protect user privacy, others advocate for a local and global blockchain hierarchy [174]. In Fig. 4, we see a taxonomy that classifies various means of data security.

Retrieval and distribution processes are two additional aspects of data management that must be thought out [118]. While the trigger mechanism may be common knowledge in the business, the precise architecture used by distinct publications may vary significantly [184–189]. Several authors explore the information exchange that occurs when infrastructure transmits data to gateways in addition to the exchange that occurs between individual gateways [125–130]. The term hybrid describes an increasing trend among media, especially magazines, to publish information using both pull and push methods of content distribution [190]. The part that BCT plays in each of these many routes of information distribution varies depending on the sort of integration chosen. Most works do not explain how to best retrieve information stored both on and off-chain. This is an issue since information needs to be retrieved from both storage areas [131–135].

BCT is compatible with a large variety of existing data retrieval methods. A blockchain system's throughput—its ability to store data—may be high, medium, or low, depending on the circumstances [139,191–194,20]. Important factors that determine this include the chosen method of integration, applicable laws, data size, throughput, and latency requirements of the system, the intended domain of use, and the number of users [140,141]. Moreover, the integration approaches have a direct bearing on the data types that can be stored in the system [142]. It has been found that an effective way to solve these concerns is to follow accepted integration procedures and creatively construct designs that account for the challenges that are stated in the relevant literature [87–92].

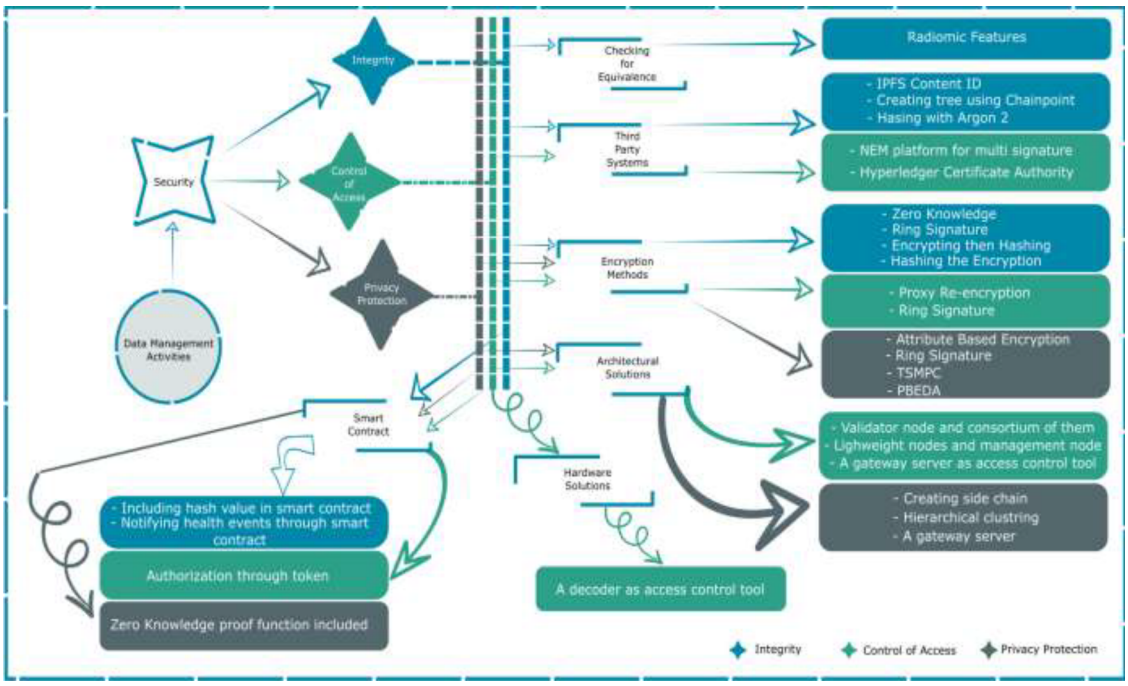


Fig. 4. Taxonomy of data protection strategies utilized by blockchain systems. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

5.3. Open issues

We can pinpoint research gaps by reviewing the existing literature to see what has been done and what hasn't. In addition, it is clear from the explanations offered in the publications and the analysis that was performed on them that a set of factors such as storage, privacy, blockchain size, etc. influence the integration methods and data management activities that occur in the SC and DSM applications [117–123]. The number of connected devices, the type of data being transmitted, the urgency of that data, the network's throughput and latency needs, and any applicable regulations are all important considerations when developing an IoT network [125–135]. Fig. 5 depicts the connections between different types of usage and the underlying motivations for those types of usage.

Nonetheless, while writing this evaluation, the author noticed a few inconsistencies. One such difference is the fact that what few studies see as a strength [54,63,66,69], another study can see as a weakness [23,78,29], and so on. Therefore, it's important to investigate the similarities and differences between the features provided by the various kinds of instantiations [123,29]. When smart contracts are implemented in blockchain-based systems, data processing inside those systems becomes decentralized and self-sufficient [126,196]. Researchers have found that the actual number of smart contracts used by such systems may vary widely between different instances of the same system. This occurs because there is no interdependence between the many system iterations [185]. Additional study is required on the topic because there is a possibility that implementing such a solution could alter the way the system operates [197–200].

Exploring how many existing smart contracts are compatible with systems can lay the groundwork for future work, thus doing so is vital [143]. Most articles do not provide detailed instructions on how to collect the data [145]. Depending on the setup, objects can be recovered either from within the chain or outside of it. Some medical images are also archived on a distributed ledger system. The photos and the accompanying information are both encrypted [48,34]. Data extraction from encrypted files may be necessary in such cases, which could call for the deployment of searchable encrypted image files [190]. The lack of a reliable method for the assignment of unique identifiers contributes to the disjointed nature of the HIT application, the fourth obstacle [201]. One of blockchain's merits is that it can be used to tackle problems like these, although it's unusual to find examples in the literature of how blockchain is used to integrate multiple healthcare systems [137]. This is due to the blockchain's initial intent of serving a decentralized network [202]. Therefore, implementing integrative HIT benefits the industry, and the aforementioned challenges may be viewed as the answer to a problem that has been for a very long time [163–168]. There are additional problems, such as how blockchain can be used to monitor patients [172], triage, providers' operational [173] and financial performance, and disease transmission surveillance [203], that have received limited attention in publications [155–159] but deserve additional exploration.

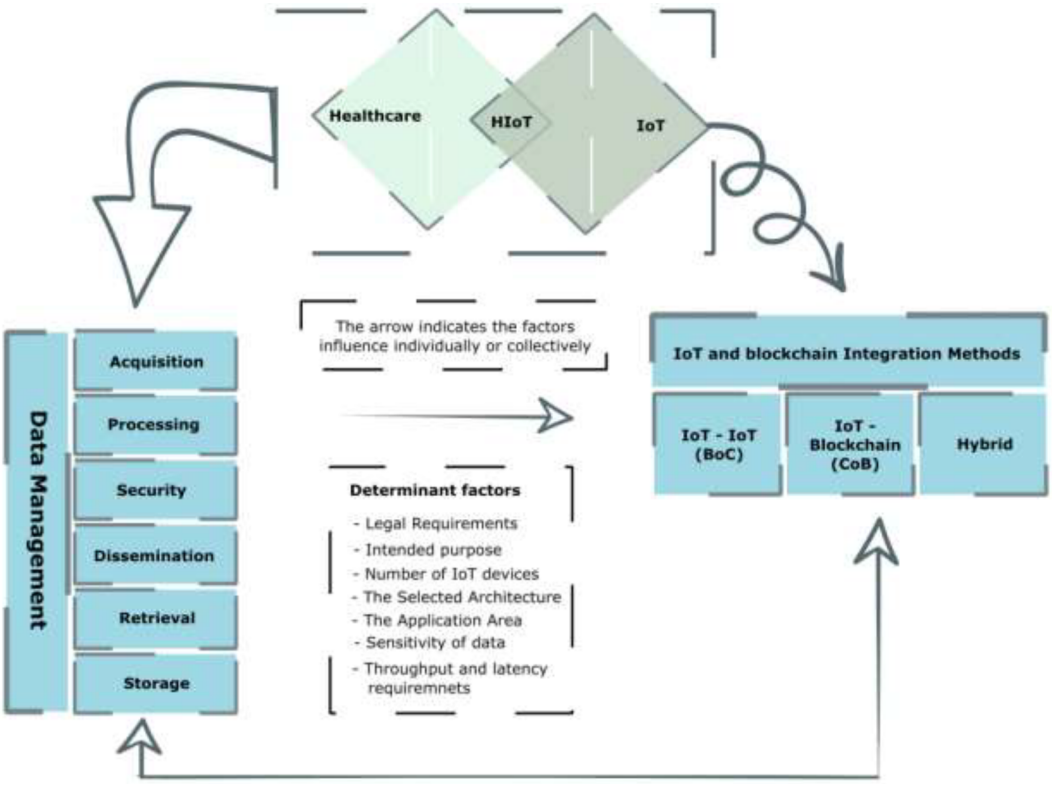


Fig. 5. The links that are present between the many different application domains as well as the elements that contribute to the establishment of these domains. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

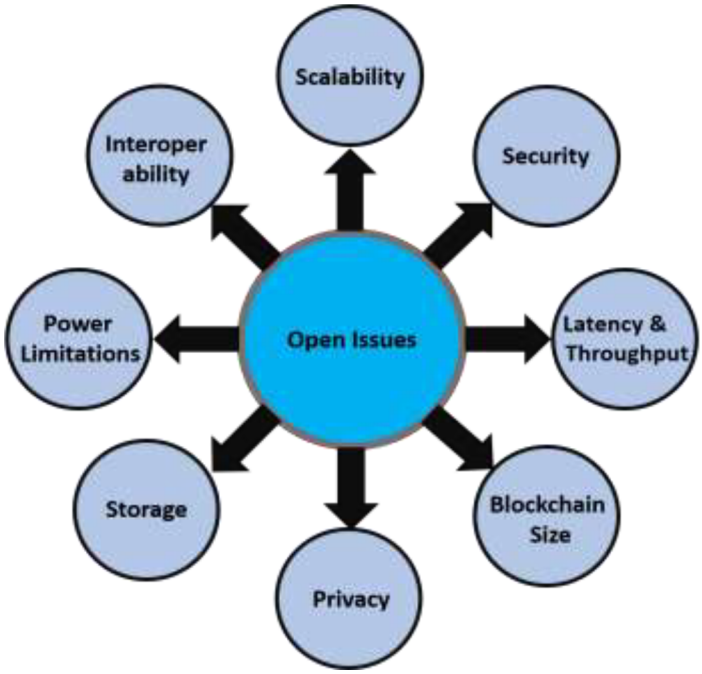


Fig. 6. Open Issues Categories in Using BCT and IoT in SC and DSM. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

When implemented appropriately, BCT offers a reliable answer to a variety of problems that are inherent to SC and DSM applications, including those about data privacy and integrity, as well as sharing, interoperability, accessibility, and the capacity to do real-time data updates [204]. However, there are some boundaries and constraints imposed by the BCT. Even though BCT has many advantages, its development and implementation in SC and DSM applications have presented substantial research challenges that call for additional investigation. The challenges that are presented by blockchain technology are broken down and analyzed in this section. Fig. 6 illustrates the category of these challenges.

5.3.1. Scalability

A significant problem in terms of scalability and growing overhead or computational resources in IoMT devices is presented by the blockchain system as a result of the increased number of system members [192]. Due to the complexity of this problem, it may become necessary to allocate additional processing resources to the entire blockchain infrastructure [205]. Because the processing capabilities of smart devices and sensors are lower than those of a regular computer, the difficulty of this problem grows as the number of smart devices and sensors increases [206–208]. The IoT devices that are part of the BCT require a substantial amount of computational power and include a high bandwidth overhead. IoT devices do not possess the necessary amount of computational capacity to make use of the capabilities offered by BCT. As a result, these devices may run at suboptimal or potentially excessive speeds and are unable to simultaneously execute both their original software and blockchain software [209].

5.3.2. Security

The architecture and implementation of BCT with IoT each have several particular security flaws. The classical consensus mechanism, which is used to confirm and verify transactions, is often the source of flaws that might compromise the security of a blockchain [195]. These security weaknesses include but are not limited to, Distributed Denial of Service (DDoS) [86], Transaction Malleability [87], Difficulty Raising, Block Discarding [101], Eclipse, Selfish Mining, Sybil, 51%, Block Withholding, and Double Spending Attacks. In a distributed blockchain system using IoT, the algorithms that make up the consensus mechanism will not be able to mitigate these security risks [97]. The theoretical possibility of addressing the risks is rendered unattainable by the exorbitant expense of the resources that are required to do so. The design of consensus procedures is irrelevant to addressing these security vulnerabilities because of their nature [126–130].

To put it another way, the perfect approach would consist of a routine that included preventative measures against attacks of this nature. Due to security flaws, malicious software has the potential to implement decentralized applications that are based on BCT [134]. These malicious attacks take use of security holes in the way a smart contract was implemented to support a variety of criminal activities, including the theft of identities and the exfiltration of data [135]. The fact that the blockchain network is open to the public means that the flow of transactions can be tracked to discover real-world identities or other supplementary information; this poses a potential threat to users' privacy and security (also known as pseudo-anonymity) [145–148].

5.3.3. Latency and throughput

Integration of blockchains into DSM and SC applications that demand real-time response to events and data collecting may be difficult because most blockchain technologies will require time for consensus to be obtained and transactions to be completed [156]. About the latency of transactions, the processing of transactions on a blockchain takes some time. For instance, the blockchain that underpins BitCoin [62] requires a ten-minute waiting period before it can validate any transaction that occurs within the network [53]. It is advisable to wait around one hour for each transaction to be confirmed, even though adding five or six blocks to the chain is necessary before confirmation may occur [28]. On the other hand, the majority of traditional database systems can confirm a transaction in just a few seconds [85]. Regarding throughput restrictions, RPM [101–103] and EHR [84] in IoT are blockchain-based; in these systems, massive volumes of transactions per second are often required, which poses a potential issue for blockchains [172–176]. For example, the original blockchain that underpins Bitcoin can support up to seven transactions every single second. Throughput is a crucial parameter for choosing the blockchain that is most suited for IoT deployment. This is because many different transactions can be optimized (for example, by increasing the size of the blocks) [85].

5.3.4. Blockchain size

When each device, such as an IoT-RPM [101] and an EHR [84], performs transactions, blockchains are continually developing and demand the utilization of more powerful miners [139]. The restricted resources of traditional IoMT devices make it impossible for them to manage even the smallest blockchains [194]. Therefore, research needs to be done on compression methods in the blockchain that make use of different ways, such as mini-blockchains [102,103].

5.3.5. Privacy

The present secure communication architectures of EHR do not respect the privacy of users or patients [13]. One example of this is the exchanging system releasing all data without the authorization of the proprietors, and another example is noise in the data requester summary [72]. For the requester to be able to provide individualized services, however, accurate patient data will be required. This is because existing EHR applications may be built on a blockchain [51]. The creation of a framework that uses cryptographic mechanisms to ensure data privacy and integrity on a blockchain-based electronic health record is necessary to fulfill the need of protecting the confidentiality of patient data [61]. Because of this feature, it is quite challenging to identify a particular patient based on their current account number. Any framework that is even remotely comparable must address the deficiencies that exist in the security of the patient's private information [27–30]. To begin, patients need to share their data in a way that is accessible to users, as the utilization of blockchain-based frameworks within EHR necessitates a sizeable quantity of processing power in addition to a sizeable amount of time to finish each task. Adding a new node to the blockchain network, which is required for new patients, needs many processes to verify the honesty of the patient [74,95].

5.3.6. Storage

When it comes to recording transactions throughout an entire network, a blockchain needs a significant amount of storage space, which might be problematic for nodes that have restricted data transmission capabilities [5–10]. The immutability, unforgeability, and verifiability of EHR data that are saved and shared can be guaranteed by BCT [149]; nevertheless, the storage requirements of large-scale distributed EHR data can be prohibitively expensive [153].

5.3.7. Power limitations

The data from IoMT devices that are acquired by blockchain are frequently subject to computational constraints, which prevent the adoption of cryptographic techniques [181]. In several SC and DSM-related applications, cryptosystems in resource-constrained devices that manage sensor and actuator protection have exceedingly constrained computational resources [161]. In other words, they are up against modern methods of public-key cryptography that are completely safe [118]. It is difficult to choose suitable cryptography because the majority of blockchains utilize public-key cryptosystems based on elliptic-curve cryptography (ECC) [190]. These cryptosystems have problems with efficiency and security and make it more difficult to use them [88]. Blockchain cryptosystems should be aware of the threat posed by post-quantum computing and should search for energy-efficient quantum-safe algorithms [155].

5.3.8. Interoperability

Applications in both SC and healthcare suffer from a lack of interoperability since there are no mechanisms for the gathering, exchange, or analysis of information [15–25]. Existing EHR systems are managed through the use of centralized local databases and an inactive architecture, in contrast to the decentralized nature of BCT on the cloud [33]. Therefore, advancing healthcare systems in this direction and using blockchain technology would initially require a successful EHR system that can allow collaboration and interoperability among medical and scientific communities [42–44]. To successfully migrate electronic health record data to blockchain technology, some technical difficulties need to be resolved first. Because the existing healthcare ledger (database) is not distributed [58–61].

6. Conclusion

In this research, we analyze how BCT is applied to the IoT and how BCT is used to improve data management processes in the selected publications. The fundamental contribution of this study is an extensive review and classification of relevant research

publications on the blockchain with IoT and their integration with a variety of SC and DSM applications, which reveals different trends in the relevant body of literature. BCT's expanding popularity as a data management solution is due in large part to its ability to handle a wide variety of big data types, to make use of encrypted data in both online and offline situations, and to not rely on a single point of failure. On top of that, it can decrypt encrypted data even when not connected to the internet. Many articles have looked at many aspects of data management to determine if these objectives have been met, including data collection, processing, and security, as well as data distribution, retrieval, and storage.

Several other BCT-based solutions are also being deployed to boost the standard of these areas. In BCT-based computer systems, improved authentication features, such as data gathering, can increase output. One example of this is the use of public keys in encryption protocols. Other responsibilities of data administration, such as data acquisition, are made easier with the assistance of the improved authentication capabilities provided by systems based on BCT. It has been reported that a variety of authentication methods, including biological mechanisms to public-key encryption algorithms, have been used. In a similar vein, one of the benefits of BCT for the processing of data is the resurgence of smart contracts. Smart contracts were around before the broad use of BCT, but they were not widely employed as a data processing tool at the time. Blockchain-based systems, on the other hand, make use of it for a variety of functions, such as data processing without human intervention. The least targeted jobs in data management are the ones dealing with dissemination and retrieval. Despite this, a large number of authors provide the distribution techniques that were employed in their implementations in a way that is understandable and succinct. On the other hand, we have identified several factors that have a significant impact on the storage of data. The designers adopt strategies such as constructing a data lake, retaining only file locations, and registering a catalog of files to get over these constraints. To avoid potential legal problems, programmers will often modify their systems so that they conform to any applicable legal requirements. The future application of BCT combined with IoT devices has huge potential to have a significant influence not only on the healthcare industry, and smart cities but also on other industries such as agriculture, automotive, etc.

7. Limitations

There are limitations to this review that you should be aware of, as there are with any research. BCT is susceptible to publication bias since there is a dearth of research that examines the negative repercussions of utilizing BCT. There are a few notable outliers, such as [29], which casts doubt on BCT's ability to provide unique identifiers to patients, and [31], which raises doubts about BCT's scalability due to the inherent challenges in data processing. The results of both experiments contradict the assumption that BCT might be utilized to provide individuals with new, separate identities. Even though many people support the use of BCT to increase security, [160] investigates the potential threats to blockchain-based systems built on the PoW and PoS consensus procedures. Nonetheless, several articles extol the benefits of BCT and provide a variety of instances of how to get around the limitations. This assessment is faulty due to the absence of positive data and the use of unverified historical analogies to predict future technological developments [104–107]. The combination of these two causes an overly optimistic outlook on the future [106]. Second, we'll be using the same criteria to evaluate everything, so only the finest content will make it past our initial curation [109–114].

Author contributions

The contributions of all authors are the same.

Data availability

Not applicable.

Code availability

Not applicable.

Consent for publication

We agree to publish.

Ethical approval

This study does not contain ethical issues.

Informed consent

Not applicable.

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.

Data availability

No data was used for the research described in the article.

Acknowledgement

The research work of M. Faheem is supported by the University of Vaasa and Acadamy of Finland.

References

[1] Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain technologies: the foreseeable impact on society and industry.
[2] M. Swan, Blockchain: blueprint for a new economy, O'Reilly Media, Inc., 2015.
[3] J. Eberhardt, S. Tai, On or off the blockchain? Insights on off-chaining computation and data, in: European Conference on Service-Oriented and Cloud Computing, Springer, Cham, 2017, pp. 3–15.
[4] R. Kohli, S.S.L. Tan, Electronic Health Records, Mis. Q. 40 (3) (2016) 553–574.
[5] J.M. Roman-Belmonte, H. De la Corte-Rodriguez, E.C. Rodriguez-Merchan, How blockchain technology can change medicine, Postgrad. Med. 130 (4) (2018) 420–427.
[6] S. Angraal, H.M. Krumholz, W.L. Schulz, Blockchain technology: applications in health care, Circ. Cardiovasc. Qual. Outcomes 10 (9) (2017).
[7] H.H. Khan, M.N. Malik, Z. Konečná, A.G. Chofreh, F.A. Goni, J.J. Klemeš, Blockchain technology for agricultural supply chains during the COVID-19 pandemic: benefits and cleaner solutions, J. Clean. Prod. 347 (2022), 131268.
[8] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, A. Peacock, Blockchain technology in the energy sector: a systematic review of challenges and opportunities, Renew. Sustain. Energy Rev. 100 (2019) 143–174.
[9] M. Conoscenti, A. Vetro, J.C. De Martin, Blockchain for the Internet of Things: a systematic literature review, in: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), IEEE, 2016, pp. 1–6.
[10] M.A. Khan, K. Salah, IoT security: review. Blockchain solutions. and open challenges, Fut. Gener. Comput. Syst. 82 (2018) 395–411.
[11] P.J. Taylor, T. Dargahi, A. Dehghantanha, R.M. Parizi, Choo-K-KR. *A systematic literature review of blockchain cyber security*, Dig. Comm. Netw. 6 (2) (2020) 147–156.
[12] M. Hölbl, M. Kompara, A. Kamišalić, L. Nemec Zlatolas, A systematic review of the use of blockchain in healthcare, Symmetry (Basel) 10 (10) (2018) 470.
[13] M. Tiago, T.M. Fernandez-Carames, P. Frafa-Lamas, A review on the use of blockchain for the Internet of Things, IEEE Access 6 (2018) 32979–33001.
[14] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on blockchain technology? —A systematic review, PLoS One 11 (10) (2016), e0163477.
[15] T.T. Kuo, H. Zavaleta Rojas, L. Ohno-Machado, Comparison of blockchain platforms: a systematic review and healthcare examples, J. Am. Med. Inform. Assoc. 26 (5) (2019) 462–478.
[16] A.H. Mayer, C.A. da Costa, R.D.R. Righi, Electronic health records in a Blockchain: a systematic review, Health Inform. J. 26 (2) (2020) 1273–1288.
[17] S. Miau, J.M. Yang, Bibliometrics-based evaluation of the Blockchain research trend: 2008–March 2017, Technol. Anal. Strateg. Manag. 30 (9) (2018) 1029–1045.
[18] F. Casino, k. Thomas, Dasaklis, and Constantinos Patsakis,"A systematic literature review of blockchain-based applications: current status, classification, and open issues, Telemat. Inform. 36 (2018) 55–81.
[19] S. Badshah, A.A. Khan, B. Khan, Towards process improvement in DevOps: a systematic literature review, in: Proceedings of the evaluation and assessment in software engineering, 2020, pp. 427–433.
[20] K.R. Larsen, C.H. Bong, A tool for addressing construct identity in literature reviews and meta-analyses, Mis. Q. 40 (3) (2016) 529–552.
[21] M. Tate, E. Furtmueller, J. Evermann, W. Bandara, Introduction to the special issue: the literature review in information systems, Commun. Assoc. Inf. Syst. 37 (1) (2015) 5.
[22] S. Gregor, A.R. Hevner, Positioning and presenting design science-types of knowledge in design science research, MIS Q. 37 (2) (2013) 337–355.
[23] A.B. Hargadon, Brokering knowledge: linking learning and innovation, Res. Organ. Behav. 24 (2002) 41–85.
[24] E. Ducas, A. Wilner, The security and financial implications of blockchain technologies: regulating emerging technologies in Canada, Int. J. 72 (4) (2017) 538–562.
[25] M.T. Hammi, B. Hammi, P. Bellot, A. Serhrouchni, Bubbles of Trust: a decentralized blockchain-based authentication system for IoT, Comput. Sec. 78 (2018) 126–142.
[26] G.G. Dagher, J. Mohler, M. Milojkovic, P.B. Marella, Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, Sustain. Cities Soc. 39 (2018) 283–297.
[27] P. Danzi, A.E. Kalor, C. Stefanovic, P. Popovski, Analysis of the communication traffic for blockchain synchronization of IoT devices, in: 2018 IEEE International Conference on Communications (ICC), IEEE, 2018, pp. 1–7.
[28] T. Qiu, R. Zhang, Y. Gao, Ripple vs. SWIFT: transforming cross border remittance using blockchain technology, Proc. Comput. Sci. 147 (2019) 428–434.
[29] N.J. Vickers, Animal communication: when i'm calling you, will you answer too? Curr. Biol. 27 (14) (2017) R713–R715.
[30] S. Kamble, A. Gunasekaran, H. Arha, Understanding the Blockchain technology adoption in supply chains-Indian context, Int. J. Prod. Res. 57 (7) (2019) 2009–2033.
[31] T.T.A. Dinh, R. Liu, M. Zhang, G. Chen, B.C. Ooi, J. Wang, Untangling blockchain: a data processing view of blockchain systems, IEEE Trans. Knowl. Data Eng. 30 (7) (2018) 1366–1385.
[32] K. Croman, C. Decker, I. Eyal, A.E. Gencer, A. Juels, A. Kosba, R. Wattenhofer, On scaling decentralized blockchains, in: International conference on financial cryptography and data security, Berlin, Heidelberg, Springer, 2016, pp. 106–125.
[33] Q. Lv, P. Cao, E. Cohen, K. Li, S. Shenker, Search and replication in unstructured peer-to-peer networks, in: Proceedings of the 16th International Conference On Supercomputing, 2002, pp. 84–95.
[34] X. Guo, E. Zhu, X. Liu, J. Yin, Deep embedded clustering with data augmentation, in: Asian Conference on Machine Learning, PMLR, 2018, pp. 550–565.
[35] Das, S.K., & Ammari, H.M. (2009). Routing and data dissemination. A networking perspective, 67a.
[36] S. Ølnes, J. Ubacht, M. Janssen, Blockchain in government: benefits and implications of distributed ledger technology for information sharing, Gov. Inf. Q. 34 (3) (2017) 355–364.
[37] L. Zhou, L. Wang, Y. Sun, P. Lv, Beekeeper: a blockchain-based iot system with secure storage and homomorphic computation, IEEE Access 6 (2018) 43472–43488.

[38] C. Cachin, Blockchains and consensus protocols: snake oil warning, in: 2017 13th European Dependable Computing Conference (EDCC), IEEE, 2017, pp. 1–2.
[39] G.W. Peters, E. Panayi, Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money. Banking Beyond Banks and Money, Springer, Cham, 2016, pp. 239–278.
[40] G. Zyskind, O. Nathan, Decentralizing privacy: using blockchain to protect personal data. 2015 IEEE Security and Privacy Workshops, IEEE, Chicago, 2015, pp. 180–184.
[41] B. Huang, Z. Liu, J. Chen, A. Liu, Q. Liu, Q. He, Behavior pattern clustering in blockchain networks, Multimed. Tools Appl. 76 (19) (2017) 20099–20110.
[42] N. Berendea, H. Mercier, E. Onica, E. Riviere, Fair and efficient gossip in hyperledger fabric, in: 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2020, pp. 190–200.
[43] A. de Saint-Exupery, Internet of things, strategic research roadmap. Surrey: Internet of Things Initiative, 2009.
[44] I. Makhdoom, M. Abolhasan, H. Abbas, W. Ni, Blockchain's adoption in IoT: the challenges, and a way forward, J. Netw. Comput. Appl. 125 (2019) 251–279.
[45] D. Minoli, B. Occhiogrosso, Blockchain mechanisms for IoT security, IoT 1 (2018) 1–13.
[46] D.V. Jose, A. Vijyalakshmi, An overview of security in Internet of Things, Proc. Comput. Sci. 143 (2018) 744–748.
[47] K.M. Sadique, R. Rahmani, P. Johannesson, Towards security on internet of things: applications and challenges in technology, Proc. Comput. Sci. 141 (2018) 199–206.
[48] H. Suo, J. Wan, C. Zou, J. Liu, Security in the internet of things: a review, in: 2012 International Conference on Computer Science and Electronics Engineering 3, IEEE, 2012, pp. 648–651.
[49] M. Pustišek, A. Kos, Approaches to front-end IoT application development for the ethereum blockchain, Telematic 129 (2018) 410–419.
[50] Muhammad Faheem, et al., Smart grid communication and information technologies in the perspective of Industry 4.0: opportunities and challenges, Comput. Sci. Rev. 30 (2018) 1–30.
[51] O. Hahm, E. Baccelli, H. Petersen, N. Tsiftes, Operating systems for low-end devices in the internet of things: a survey, IEEE IoT J. 3 (5) (2015) 720–734.
[52] G. Paré, C. Sicotte, M. Chekli, M. Jaana, C.D. Blois, M. Bouchard, A pre-post evaluation of a telehomecare program in oncology and palliative care, Telemed. e-Health, 15 (2) (2009) 154–159.
[53] M.B. Buntin, M.F. Burke, M.C. Hoaglin, D. Blumenthal, The benefits of health information technology: a review of the recent literature shows predominantly positive results, Health Aff. 30 (3) (2011) 464–471.
[54] R. Bernardi, S. Sarker, S. Sahay, The role of affordances in the deinstitutionalization of a dysfunctional health management information system in Kenya: an identity work perspective, MIS Q. 43 (4) (2019) 1177–1200.
[55] S.B. Baker, W.E.I. Xiang, S. Member, I.A.N. Atkinson, Internet of Things for smart Healthcare.pdf, IEEE Access 5 (2017) 26521–26544.
[56] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, Fut. Gener. Comput. Syst. 29 (7) (2013) 1645–1660.
[57] J. Dunn, What private organizations should know when building HIEs. Lessons can be learned from public health, Health Manag. Technol. 33 (9) (2012) 12–13.
[58] F.C. Payton, G. Pare, C.M. Le Rouge, M. Reddy, Health care IT: process, people, patients and interdisciplinary considerations, J. Assoc. Inf. Syst. 12 (2) (2011) 4.
[59] R.G. Finchman, R. Kohli, R. Krishnan, Editorial overview—The role of IS in healthcare, Inf. Syst. Res. 22 (3) (2011) 419–428.
[60] J. Kwon, M.E. Johnson, Meaningful healthcare security: does meaningful-use attestation improve information security performance? MIS Q. 42 (4) (2018) 1043–1068.
[61] W.J. Gordon, C. Catalini, Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability, Comput. Struct. Biotechnol. J. 16 (2018) 224–230.
[62] S.K. Boell, D. Cecez-Kecmanovic, A hermeneutic approach for conducting literature reviews and literature searches, Commun. Assoc. Inf. Syst. 34 (1) (2014) 12.
[63] D. Efanov, P. Roschin, The all-pervasiveness of the blockchain technology, Telematic 123 (2018) 116–121.
[64] W. Bandara, E. Furtmueller, E. Gorbacheva, S. Miskon, J. Beekhuyzen, Achieving rigor in literature reviews: insights from qualitative data analysis and tool-support, Commun. Assoc. Infor. Syst. 37 (1) (2015) 8.
[65] Y. LEVY, T. ELLIS, A systems approach to conduct an effective literature review in support of information systems research, 2006, Inf. Sci. 9 (2017).
[66] M. Faheem, et al., Software defined communication framework for smart grid to meet energy demands in smart cities, in: 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), IEEE, 2019.
[67] M.B. Hoy, An introduction to the blockchain and its implications for libraries and medicine, Med. Ref. Serv. Q. 36 (3) (2017) 273–279.
[68] P. Zhang, M.A. Walker, J. White, D.C. Schmidt, G. Lenz, Metrics for assessing blockchain-based healthcare decentralized apps, in: 2017 IEEE 19th international conference on e-health networking, applications and services (Healthcom), IEEE, 2017, pp. 1–4.
[69] M.A. Engelhardt, Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector, Technol. Innov. Manage. Rev. 7 (10) (2017).
[70] C. Pahl, N. El Ioini, S. Helmer, A decision framework for blockchain platforms for IoT and edge computing, IoTBDS (2018) 105–113.
[71] C. Esposito, A.D. Santis, G. Tortora, H. Chang, K.R. Choo, Blockchain: a Panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. 5 (1) (2018) 31–37, 2018.
[72] O. Novo, Blockchain meets IoT: an architecture for scalable access management in IoT, IEEE IoT. J. 5 (2) (2018) 1184–1195.
[73] P.K. Sharma, S. Singh, Y Jeong, S. Park JH, DistBlockNet: a distributed blockchains-based secure SDN architecture for IoT networks, IEEE Commun. Mag. 55 (9) (2017) 78–85.
[74] M. Faheem, R.A. Butt, Big datasets of optical-wireless cyber-physical systems for optimizing manufacturing services in the internet of things-enabled industry 4.0, Data Brief 42 (2022), 108026.
[75] A. Reyna, C. Martin, J. Chen, E. Soler, M. Diaz, Onblockchain and its integration with IoT. Challenges and opportunities, Fut. Gener. Comput. Syst. 88 (2018) 173–190.
[76] N. Teslya, I. Ryabchikov, Blockchain-based platform architecture for industrial IoT, in: 2017 21st Conference of Open Innovations Association (FRUCT), IEEE, 2017, pp. 321–329.
[77] Lombardi, F., Aniello, L., De Angelis, S., Margheri, A., & Sassone, V. (2018). A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids.
[78] M. Faheem, G. Fizza, M.W. Ashraf, R.A. Butt, M.A. Ngadi, V.C. Gungor, Big Data acquired by Internet of Things-enabled industrial multichannel wireless sensors networks for active monitoring and control in the smart grid Industry 4.0, Data Brief 35 (2021), 106854.
[79] R.B. Chakraborty, M. Pandey, S.S. Rautaray, Managing computation load on a blockchain–based multi–layered Internet–of–Things network, Telematic 132 (2018) 469–476.
[80] H. Yohan, P. Byungjun, J. Jongpil, A novel architecture of air pollution measurement platform using 5 G and blockchain for industrial IoT application, Procedia Comput. Sci 155 (2019) 728–733.
[81] A. Stanciu, Blockchain based distributed control system for edge computing, in: 2017 21st International Conference On Control Systems And Computer Science (CSCS), IEEE, 2017, pp. 667–671.
[82] P.K. Sharma, M.Y. Chen, J.H. Park, A software defined fog node based distributed blockchain cloud architecture for IoT, IEEE Access 6 (2017) 115–124.
[83] N. Prajapati, D. Mehta, S.K. Rajendra, K. Abhishek, Driving-point impedance and particle swarm optimization based circuit synthesis of power transformer winding, in: 2018 3rd International Conference for Convergence in Technology (I2CT), IEEE, 2018, pp. 1–5.
[84] D. Miller, Blockchain and the Internet of Things in the industrial sector, IT Prof. 20 (3) (2018) 15–18.
[85] A.D. Dwivedi, G. Srivastava, S. Dhar, R. Singh, A decentralized privacy-preserving healthcare blockchain for IoT, Sensors 19 (2) (2019) 326.

[86] M. Faheem, R.A. Butt, B. Raza, H. Alquhayz, M.Z. Abbas, M.A. Ngadi, V.C. Gungor, A multiobjective, lion mating optimization inspired routing protocol for wireless body area sensor network based healthcare applications, Sensors 19 (23) (2019) 5072.
[87] K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, J. Med. Syst. 42 (2018) 130.
[88] X. Liang, J. Zhao, S. Shetty, J. Liu, D. Li, Integrating blockchain for data sharing and collaboration in mobile healthcare applications, in: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE, 2017, pp. 1–5.
[89] N. Rifi, N. Agoulmine, N. Chendeb Taher, E. Rachkidi, Blockchain technology: is it a good candidate for securing iot sensitive medical data? Wirel. Commun. Mobile Comput. 2018 (2018).
[90] E.F. Jesus, V.R. Chicarino, C.V. De Albuquerque, A.A.D.A. Rocha, A survey of how to use blockchain to secure internet of things and the stalker attack, Sec. Commun. Netw. (2018), 2018.
[91] Y. Rahulamathavan, R.C.W. Phan, M. Rajarajan, S. Misra, A. Kondoz, Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption, in: 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), IEEE, 2017, pp. 1–6.
[92] C.H. Lee, K.H. Kim, Implementation of IoT system using block chain with authentication and data protection, in: 2018 International Conference on Information Networking (ICOIN), IEEE, 2018, pp. 936–940.
[93] A. Pouraghily, M.N. Islam, S. Kundu, T. Wolf, Privacy in blockchain-enabled iot devices, in: 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), IEEE, 2018, pp. 292–293.
[94] H. Zareen, S. Awan, M.B. E Sajid, S.M. Baig, M. Faisal, N Javaid, Blockchain and IPFS based service model for the internet of things, in: Conference on Complex, Intelligent, and Software Intensive Systems, Cham, Springer, 2021, pp. 259–270.
[95] M. Banerjee, J. Lee, K.K.R. Choo, A blockchain future to Internet of Things security: a position paper, Dig. Commun. Netw. (2017). URL, http://www.sciencedirect.com/science/article/piiS.
[96] A. Ouaddah, A. Abou El Kalam, A.A Ouahman, Harnessing the power of blockchain technology to solve IoT security & privacy issues, in: ICC, 2017, p. 7. -1.
[97] C. Tselios, I. Politis, S. Kotsopoulos, Enhancing SDN security for IoT-related deployments through blockchain, in: 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), IEEE, 2017, pp. 303–308.
[98] O. Pal, B. Alam, V. Thakur, S. Singh, Key Management For Blockchain Technology, 7, ICT Express, 2021, pp. 76–80.
[99] M.R. Ulbricht, F. Pallas, Yappl-A lightweight privacy preference language for legally sufficient and automated consent provision in iot scenarios. Data Privacy Management, Cryptocurrencies and Blockchain Technology, Springer, Cham, 2018, pp. 329–344.
[100] S.L. Cichosz, M.N. Stausholm, T. Kronborg, P. Vestergaard, O. Hejlesen, How to use blockchain for diabetes health care data and access management: an operational concept, J. Diab. Sci. Technol. 13 (2) (2019) 248–253.
[101] V. Patel, A framework for secure and decentralized sharing of medical imaging data via blockchain consensus, Health Inform. J. 25 (4) (2019) 1398–1411.
[102] P. Zhang, J. White, D.C. Schmidt, G.R. Lenz, FHIR Chain: applying blockchain to securely and scalably share, Comput. Struct. Biotechnol. J. 16 (2018) 267–278.
[103] T.T. Thwin, S. Vasupongayya, Blockchain-based access control model to preserve privacy for personal health record systems, Sec. Commun. Netw. 2019 (2019).
[104] A. Al Omar, M.S. Rahman, A. Basu, S Kiyomoto, Medibchain: a blockchain based privacy preserving platform for healthcare data, in: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Cham, Springer, 2017, pp. 534–543.
[105] D.R. Wong, S. Bhattacharya, A.J. Butte, Prototype of running clinical trials in an untrustworthy environment using blockchain, Nat. Commun. 10 (1) (2019) 1–8.
[106] J. Zhang, N. Xue, X. Huang, A secure system for pervasive social network-based healthcare, IEEE Access 4 (2016) 9239–9250.
[107] B. Liu, X.L. Yu, S. Chen, X. Xu, L. Zhu, Blockchain based data integrity service framework for IoT data, in: 2017 IEEE International Conference on Web Services (ICWS), IEEE, 2017, pp. 468–475.
[108] A. Ouaddah, A.A. Elkalam, A.A. Ouahman, Towards a novel privacy-preserving access control model based on blockchain technology in IoT. Europe and MENA Cooperation Advances in Information and Communication Technologies, Springer, Cham, 2017, pp. 523–533.
[109] K. Rantos, G. Drosatos, K. Demertzis, C. Ilioudis, A. Papanikolaou, Blockchain-based Consents Management For Personal Data Processing in the IoT Ecosystem, ICETE, 2018, p. 298.
[110] X. Liang, J. Zhao, S. Shetty, D. Li, Towards data assurance and resilience in IoT using blockchain, in: MILCOM 2017 2017 IEEE Military Communications Conference (MILCOM), 2017, pp. 261–266.
[111] J. Lin, Z. Shen, A. Zhang, Y. Chai, Blockchain and IoT based food traceability for smart agriculture, in: Proceedings of the 3rd International Conference on Crowd Science and Engineering, 2018, pp. 1–6.
[112] E.C. Cheng, Y. Le, J. Zhou, Y. Lu, Healthcare services across China–on implementing an extensible universally unique patient identifier system, Int. J. Healthc. Manag. 11 (3) (2018) 210–216.
[113] J. Sun, J. Yan, K.Z.J.F.I.Z.K. Zhang, Blockchain-based sharing services: what blockchain technology can contribute to smart cities, Financ. Innov. 2 (1) (2016) 26.
[114] C. Lazaroiu, M. Roscia, Smart district through IoT and blockchain, in: 2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA), IEEE, 2017, pp. 454–461.
[115] Y. Yuan, F.Y. Wang, Towards blockchain-based intelligent transportation systems, in: 2016 IEEE 19th International Conference On Intelligent Transportation Systems (ITSC), IEEE, 2016, pp. 2663–2668.
[116] T. Alladi, V. Chamola, J.J. Rodrigues, S.A. Kozlov, Blockchain in smart grids: a review on different use cases, Sensors 19 (22) (2019) 4862.
[117] S Singh, R. In-Ho, M. Weizhi, K. Maninder, C. Gi Hwan, 2019. SH-BlockCC: a secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology, Int. J. Distrib. Sens. Netw 15 (4) (2019), 1550147719844159.
[118] S. Singh, I.H. Ra, W. Meng, M. Kaur, G.H. Cho, SH-BlockCC: a secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology, Int. J. Distrib. Sens. Netw. 15 (4) (2019), 1550147719844159.
[119] T.K. Mackey, G. Nayyar, A review of existing and emerging digital technologies to combat the global trade in fake medicines, Expert Opin. Drug Saf. 16 (5) (2017) 587–602.
[120] S. Vruddhula, Application of on-dose identification and blockchain to prevent drug counterfeiting, Pathog Glob. Health 112 (4) (2018) 161.
[121] E.A. Breeden, C. Davidson, T.K. Mackey, Leveraging blockchain technology to enhance supply chain management in Healthcare: an exploration of challenges and opportunities in the health supply chain, Blockchain Health (2018).
[122] J.H. Tseng, Y.C. Liao, B. Chong, S.W. Liao, Governance on the drug supply chain via gcoin blockchain, Int. J. Environ. Res. Public Health 15 (6) (2018) 1055.
[123] J.J. Sikorski, J. Haughton, M. Kraft, Blockchain technology in the chemical industry: machine-to-machine electricity market, Appl. Energy 195 (2017) 234–246.
[124] K. Gai, K.K.R. Choo, L. Zhu, Blockchain-enabled reengineering of cloud datacenters, IEEE Cloud Comput. 5 (6) (2018) 21–25.
[125] J. Niu, L. Shu, Z. Zhou, Y. Zhang, Mobile sensing and data management for sensor networks, Int. J. Distrib. Sens. Netw. 9 (9) (2013), 898169.
[126] I. Lee, Big data: dimensions, evolution, impacts, and challenges, Bus. Horiz. 60 (3) (2017) 293–303.
[127] M. Abu-Elkheir, M. Hayajneh, N.A. Ali, Data management for the internet of things: design primitives and solution, Sensors 13 (11) (2013) 15582–15612.
[128] A. Ijaz, L. Zhang, M. Grau, A. Mohamed, S. Vural, A.U. Quddus, R. Tafazolli, Enabling massive IoT in 5 G and beyond systems: PHY radio frame design considerations, IEEE Access 4 (2016) 3322–3339.
[129] G. Sivathanu, C.P. Wright, E. Zadok, Ensuring data integrity in storage: techniques and applications, in: Proceedings of the 2005 ACM Workshop on Storage Security and Survivability, 2005, pp. 26–36.
[130] A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC press, 2018.

[131] A. Ouaddah, H. Mousannif, A. Abou Elkalam, A.A. Ouahman, Access control in the Internet of Things: big challenges and new opportunities, Comput. Netw. 112 (2017) 237–262.
[132] H.A. Maw, H. Xiao, B. Christianson, J.A. Malcolm, A survey of access control models in wireless sensor networks, J. Sens. Actuat. Netw. 3 (2) (2014) 150–180.
[133] R. Zhang, Y. Zhang, K. Ren, Distributed privacy-preserving access control in sensor networks, IEEE Trans. Parallel Distrib. Syst. 23 (8) (2011) 1427–1438.
[134] D. He, J. Bu, S. Zhu, S. Chan, C. Chen, Distributed access control with privacy support in wireless sensor networks, IEEE Trans. Wirel. Commun. 10 (10) (2011) 3472–3481.
[135] N. Li, N. Zhang, S.K. Das, B. Thuraisingham, Privacy preservation in wireless sensor networks: a state-of-the-art survey, Ad Hoc. Netw. 7 (8) (2009) 1501–1514.
[136] B.J.C.J. Hernandez-Ramos, J.L. Moreno, R.T. Skarmeta, A privacy-preserving solutions for blockchain: review and challenges, IEEE Access 7 (2019) 164908–164940.
[137] K. Akkaya, M. Younis, A survey on routing protocols for wireless sensor networks, Ad Hoc. Netw. 3 (3) (2005) 325–349.
[138] U. Sumarmo, Berpikir Dan Disposisi Matematik Serta Pembelajarannya, UPI, Bandung, 2013.
[139] M.J. Franklin, S.B. Zdonik, Dissemination-based information systems, IEEE Data Eng. Bull. 19 (3) (1996) 20–30.
[140] A. Swaminathan, Y. Mao, G.M. Su, H. Gou, A. Varna, S. He, D. Oard, Confidentiality preserving rank-ordered search [C], in: Proceedings of the 2007 ACM Workshop on Storage Security and Survivability, 2007.
[141] W. Lu, A. Swaminathan, A.L. Varna, M. Wu, Enabling search over encrypted multimedia databases. Media Forensics and Security (Vol. 7254, pp. 404–414), SPIE, 2009.
[142] B. Ferreira, J. Rodrigues, J. Leitao, H. Domingos, Privacy-preserving content-based image retrieval in the cloud, in: 2015 IEEE 34th Symposium on Reliable Distributed Systems (SRDS), IEEE, 2015, pp. 11–20.
[143] K. Ahmed, M.A. Gregory, Techniques and challenges of data centric storage scheme in wireless sensor network, J. Sens. Actuat. Netw. 1 (1) (2012) 59–85.
[144] P. Gonizzi, G. Ferrari, V. Gay, J. Leguay, Data dissemination scheme for distributed storage for IoT observation systems at large scale, Inf. Fus. 22 (2015) 16–25.
[145] S. Ayabakan, I. Bardhan, Z. Zheng, K. Kirksey, The impact of health information sharing on duplicate testing, MIS Q. 41 (4) (2017).
[146] S. Kehua, L. Jie, F. Hongbo, Smart city and the applications. electronics, communications and control (ICECC), in: 2011 International Conference on, 2011.
[147] Keane, K., & Nisi, V. (2013). Experience Prototyping, 224–237.
[148] M. Eremia, L. Toma, M. Sanduleac, The smart city concept in the 21st century, Proc. Eng. 181 (2017) 12–19.
[149] R. Petrolo, V. Loscri, N. Mitton, Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms, Trans. Emerg. Telecommun. Technol. 28 (1) (2017) e2931.
[150] J. Gil-Garcia, S. Mellouli, K. Nahon, T. Pardo, H. Scholl, Understanding smart cities: an integrative framework, in: 45th Hawaii International Conference on System Sciences. Proceedings, Maui, 2012.
[151] I. Ghansah, Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks (2009) 47. CECâ€ 500â€ 2012â.
[152] R.G. Hollands, Critical interventions into the corporate smart city. Cambridge journal of regions, Econ. Soc. 8 (1) (2015) 61–77.
[153] N. Alzahrani, N. Bulusu, 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, 2018, pp. 30–35.
[154] T.P. Keenan, Alice in blockchains: surprising security pitfalls in PoW and PoS blockchain systems, in: 2017 15th Annual Conference on Privacy, Security and Trust (PST), IEEE, 2017, pp. 400–4002.
[155] W. Viriyasitavat, T. Anuphaptrirong, D. Hoonsopon, When blockchain meets Internet of Things: characteristics, challenges, and business opportunities, J. Ind. Inf. Integr. 15 (2019) 21–28.
[156] M.R. Raza, A. Varol, W. Hussain, Blockchain-based IoT: an Overview, in: 2021 9th International Symposium on Digital Forensics and Security (ISDFS), IEEE, 2021, pp. 1–6.
[157] B. Mbarek, N. Jabeur, T. Pitner, A.U.H. Yasar, Mbs: multilevel blockchain system for IoT, Pers. Ubiquitous Comput. 25 (1) (2021) 247–254.
[158] M.S. Asif, H. Gill, Blockchain technology and green supply chain management (GSCM)–improving environmental and energy performance in multi-echelon supply chains, in: IOP Conference Series: Earth and Environmental Science 952, IOP Publishing, 2022, 012006.
[159] F. Chehbour, Z. Doukha, S. Moussaoui, M. Guerroumi, Congestion aware data collection with mobile sinks in smart city, in: 2020 International Symposium on Networks, Computers and Communications (ISNCC), IEEE, 2020, pp. 1–7.
[160] L. Alves, E. Ferreira Cruz, S.I. Lopes, P.M. Faria, A.M. Rosado da Cruz, Towards circular economy in the textiles and clothing value chain through blockchain technology and IoT: a review, Waste Manage. Res. 40 (1) (2022) 3–23.
[161] D. Mahmudnia, M. Arashpour, R. Yang, Blockchain in construction management: applications, advantages and limitations, Autom. Constr. 140 (2022), 104379.
[162] L. Jraisat, M. Jreissat, A. Upadhyay, A. Kumar, Blockchain technology: the role of integrated reverse supply chain networks in sustainability. Supply Chain Forum: An International Journal, Taylor & Francis, 2022, pp. 1–14.
[163] J. Jabbar, H. Mehmood, H. Malik, Security of cloud computing: belongings for the generations, Int. J. Eng. Technol. 9 (2) (2020) 454–457.
[164] H. Saeed, H. Malik, U. Bashir, A. Ahmad, S. Riaz, M. Ilyas, M.I.A. Khan, Blockchain technology in healthcare: a systematic review, PLoS One 17 (4) (2022), e0266462.
[165] J. Jabbar, H. Mehmood, U. Hafeez, H. Malik, H. Salahuddin, T.H. Jabbar, Socialize the behavior of iot on human to devices interaction and internet marketing, IJCSNS Int. J. Comput. Sci. Netw. Sec. 20 (5) (2020) 158–164.
[166] E. Al Nuaimi, H. Al Neyadi, N. Mohamed, J Al-Jaroodi, Applications of big data to smart cities, J. Int. Serv. Appl. 6 (1) (2015) 1–15.
[167] S. Djahel, R. Doolan, G.M. Muntean, J. Murphy, A communications-oriented perspective on traffic management systems for smart cities: challenges and innovative approaches, IEEE Commun. Surv. Tutor. 17 (1) (2014) 125–151.
[168] H.G. Do, W.K. Ng, Blockchain-based system for secure data storage with private keyword search, in: 2017 IEEE World Congress on Services (SERVICES), IEEE, 2017, pp. 90–93.
[169] M. Batty, K.W. Axhausen, F. Giannotti, A. Pozdnoukhov, A. Bazzani, M. Wachowicz, Y. Portugali, Smart cities of the future, Eur. Phys. J. 214 (2012) 481–518.
[170] J. Jabbar, H. Mehmood, U. Hafeez, H. Malik, H. Salahuddin, On COVID-19 outburst and smart city/urban system connection: worldwide sharing of data principles with the collaboration of IoT devices and AI to help urban healthiness supervision and monitoring, Int. J. Eng. Technol. 9 (3) (2020) 630–635.
[171] B. Bhushan, A. Khamparia, K.M. Sagayam, S.K. Sharma, M.A. Ahad, N.C. Debnath, Blockchain for smart cities: a review of architectures, integration trends and future research directions, Sustain. Cities Soc. 61 (2020), 102360.
[172] Deepa, N., Pham, Q.V., Nguyen, D.C., Bhattacharya, S., Prabadevi, B., Gadekallu, T.R., & Pathirana, P.N. (2022). A survey on blockchain for big data: approaches, opportunities, and future directions. Fut. Gener. Comput. Syst..
[173] S. Singh, P.K. Sharma, B. Yoon, M. Shojafar, G.H. Cho, I.H. Ra, Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city, Sustain. Cities Soc. 63 (2020), 102364.
[174] L.B. Furstenau, Y.P.R. Rodrigues, M.K. Sott, P. Leivas, M.S. Dohan, J.R. López-Robles, K.K.R. Choo, Internet of things: conceptual network structure, main challenges and future directions, Dig. Commun. Netw. (2022).
[175] X. Chen, C. He, Y. Chen, Z. Xie, Internet of Things (IoT)—Blockchain-enabled pharmaceutical supply chain resilience in the post-pandemic era, Front. Eng. Manag. 10 (1) (2023) 82–95.
[176] E. Manavalan, K. Jayakrishna, A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements, Comput. Ind. Eng. 127 (2019) 925–953.
[177] A. Rejeb, J.G. Keogh, H. Treiblmaier, Leveraging the internet of things and blockchain technology in supply chain management, Fut. Int. 11 (7) (2019) 161.
[178] F. Salazar, M.S. Martínez-García, A. de Castro, C. Chávez-Fuentes, M. Cazorla, J.D.P. Ureña-Aguirre, S. Altamirano, UAVs for business adoptions in smart city environments: inventory management system, Electronics (Basel) 12 (9) (2023) 2090.
[179] H.K. Shee, S.J. Miah, T. De Vass, Impact of smart logistics on smart city sustainable performance: an empirical investigation, Int. J. Logistics Manag. (2021).

[180] R. Sujatha, E.P. Ephzibah, S.S. Dharinya, IoTBDs Applications: smart Transportation, Smart Healthcare, Smart Grid, Smart Inventory System, Smart Cities, Smart Manufacturing, Smart Retail, Smart Agriculture, Etc. The Internet of Things and Big Data Analytics, Auerbach Publications, 2020, pp. 275–300.
[181] J. Schlingensiepen, F. Nemtanu, R. Mehmood, L. McCluskey, Autonomic transport management systems—Enabler for smart cities, personalized medicine, participation and industry grid/industry 4.0, Intell. Transp. Syst.–Probl. Perspect. (2016) 3–35.
[182] F. Sudari, I. Priskilla, M. Febiola, R.K. Sinuraya, Strategies to improve the vaccine distribution and community awareness of taking COVID-19 vaccine in rural areas in Indonesia, Pharmacia 69 (2) (2022) 543–553.
[183] L. Sharma, P.K. Garg, S.K. Khatri, Smart E-healthcare with Internet of Things: current trends, challenges, solutions, and technologies. From Visual Surveillance to Internet of Things, Chapman and Hall/CRC, 2019, pp. 215–234.
[184] L. Ismail, R. Buyya, Artificial intelligence applications and self-learning 6 G networks for smart cities digital ecosystems: taxonomy, challenges, and future directions, Sensors 22 (15) (2022) 5750.
[185] A. Heidari, N.J. Navimipour, M. Unal, Applications of ML/DL in the management of smart cities and societies based on new trends in information technologies: a systematic literature review, Sustain. Cities Soc. (2022), 104089.
[186] W. Alshahrani, R. Alshahrani, Assessment of blockchain technology application in the improvement of pharmaceutical industry, in: 2021 International Conference of Women in Data Science At Taif University (WiDSTaif), IEEE, 2021, pp. 1–5.
[187] U. Khalil, O.A. Malik, S. Hussain, A Blockchain footprint for authentication of IoT-enabled smart devices in smart cities: state-of-the-art advancements, challenges and future research directions, IEEE Access 10 (2022) 76805–76823.
[188] M. Abubakar, Z. Jarocheh, A. Al-Dubai, X. Liu, A Survey on the integration of blockchain and IoT: challenges and opportunities, Big Data Priv. Sec. Smart Cities (2022) 197–221.
[189] H. Kaur, M.A. Alam, R. Jameel, A.K. Mourya, V. Chang, A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment, J. Med. Syst. 42 (2018) 1–11.
[190] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, M. Guizani, BPDS: a blockchain based privacy-preserving data sharing for electronic medical records, in: 2018 IEEE Global Communications Conference (GLOBECOM), IEEE, 2018, pp. 1–6.
[191] Q.I. Xia, E.B. Sifah, K.O. Asamoah, J. Gao, X. Du, M. Guizani, MeDShare: trust-less medical data sharing among cloud service providers via blockchain, IEEE Access 5 (2017) 14757–14767.
[192] S. Rouhani, L. Butterworth, A.D. Simmons, D.G. Humphery, R. Deters, MediChain TM: a secure decentralized medical data asset management system, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018, pp. 1533–1538.
[193] H. Tian, J. He, Y. Ding, Medical data management on blockchain with privacy, J. Med. Syst. 43 (2019) 1–6.
[194] P. Zhang, J. White, D.C. Schmidt, G. Lenz, S.T. Rosenbloom, FHIRChain: applying blockchain to securely and scalably share clinical data, Comput. Struct. Biotechnol. J. 16 (2018) 267–278.
[195] A. Al Omar, M.Z.A. Bhuiyan, A. Basu, S. Kiyomoto, M.S Rahman, Privacy-friendly platform for healthcare data in cloud based on blockchain environment, Fut. Gener. Comput. Syst. 95 (2019) 511–521.
[196] Y. Chen, S. Ding, Z. Xu, H. Zheng, S. Yang, Blockchain-based medical records secure storage and medical service framework, J. Med. Syst. 43 (2019) 1–9.
[197] K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, J. Med. Syst. 42 (2018) 1–7.
[198] Y. Ji, J. Zhang, J. Ma, C. Yang, X. Yao, BMPLS: blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems, J. Med. Syst. 42 (2018) 1–13.
[199] P. Sharma, S. Namasudra, R.G. Crespo, J. Parra-Fuente, M.C. Trivedi, EHDHE: enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain, Inf Sci (Ny) 629 (2023) 703–718.
[200] E.R.D. Villarreal, J. García-Alonso, E. Moguel, J.A.H. Alegría, Blockchain for healthcare management systems: a survey on interoperability and security, IEEE Access 11 (2023) 5629–5652.
[201] G. Al-Sumaidaee, R. Alkhudary, Z. Zilic, A. Swidan, Performance analysis of a private blockchain network built on Hyperledger Fabric for healthcare, Inf. Process. Manag. 60 (2) (2023), 103160.
[202] D. Aloini, E. Benevento, A. Stefanini, P. Zerbino, Transforming healthcare ecosystems through blockchain: opportunities and capabilities for business process innovation, Technovation 119 (2023), 102557.
[203] Z. Wenhua, F. Qamar, T.A.N. Abdali, R. Hassan, S.T.A. Jafri, Q.N. Nguyen, Blockchain technology: security issues, healthcare applications, challenges and future trends, Electronics (Basel) 12 (3) (2023) 546.
[204] E.A. Salimi, M. Rezaei Ghahroudi, Distributed ledger technologies (DLTs): impacts and implications on the education system, Technol. Educ. J. (TEJ) (2023) 391–406.
[205] H. Subramanian, A decentralized marketplace for patient-generated health data: design science approach, J. Med. Internet Res. 25 (2023) e42743.
[206] F. Ullah, F. Al-Turjman, A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities, Neural Comput. Appl. 35 (7) (2023) 5033–5054.
[207] A. Balan, S. Alboaie, K. Kourtit, P. Nijkamp, Blockchain systems for smart cities and regions: an illustration of self-sovereign data governance, Knowl. Manag. Region. Pol. Mak. (2023) 163–190.
[208] O.C. Uchani Gutierrez, G Xu, Blockchain and smart contracts to secure property transactions in smart cities, Appl. Sci. 13 (1) (2023) 66.
[209] B. Rawat, A.S. Bist, D. Apriani, N.I. Permadi, E.A. Nabila, AI based drones for security concerns in smart cities, APTISI Trans. Manage. (ATM) 7 (2) (2023) 125–130.