[Array 14 (2022) 100139](https://doi.org/10.1016/j.array.2022.100139)

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | Contents lists available at ScienceDirect |  |
| Array |
| journal homepage: [www.sciencedirect.com/journal/array](https://www.sciencedirect.com/journal/array) |

Blockchain in healthcare and IoT: A systematic literature review Endale Mitiku Adere   
*PO Box 25395/1000, Addis Ababa, Ethiopia*

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

**1. Introduction**

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

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

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

This review article discusses the use of blockchain in a single appli-cation domain, namely healthcare, as well as other areas where block-chain and IoT are employed simultaneously. This is done with a particular emphasis on smart city and drug supply chain, which are the

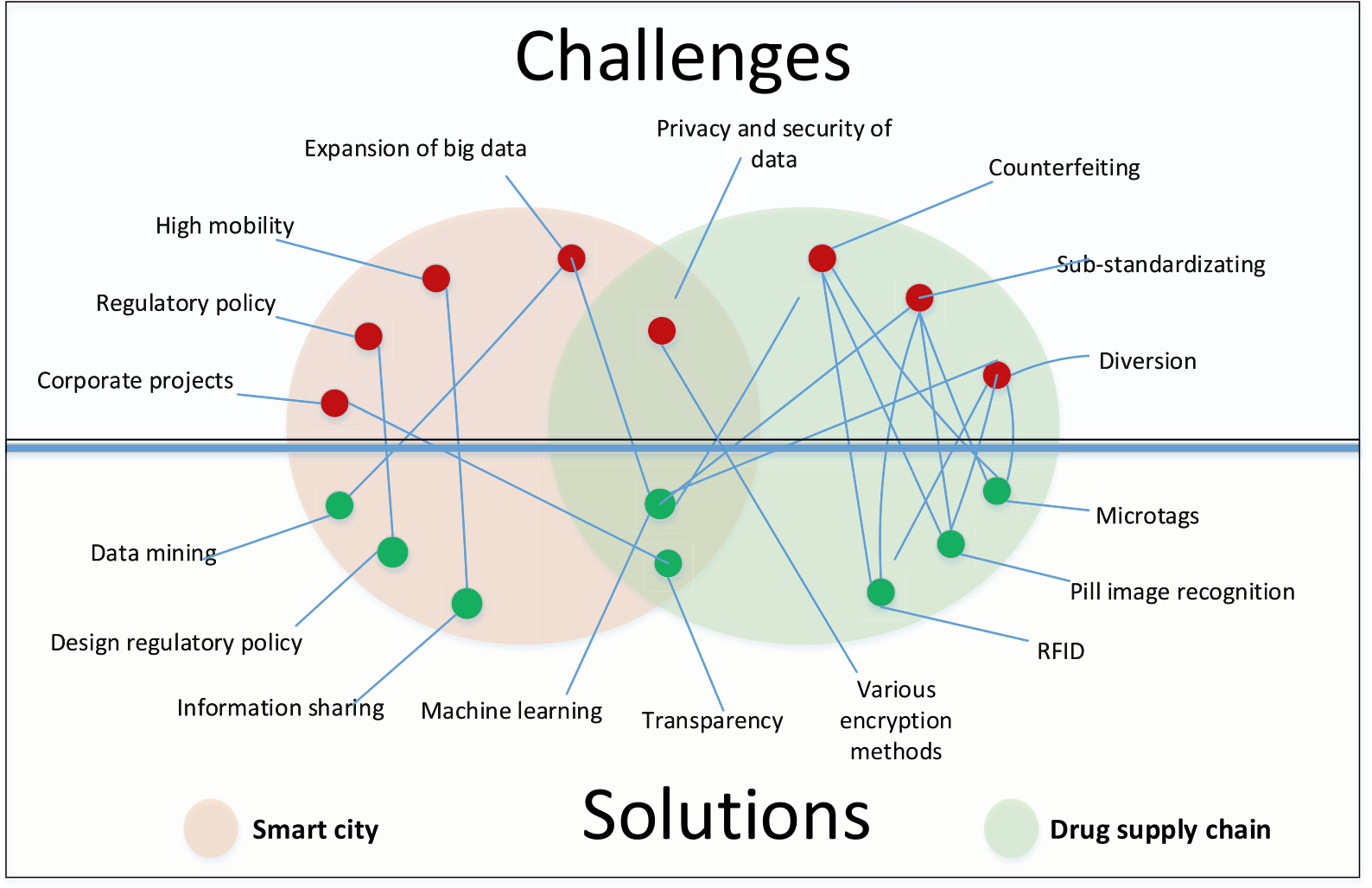
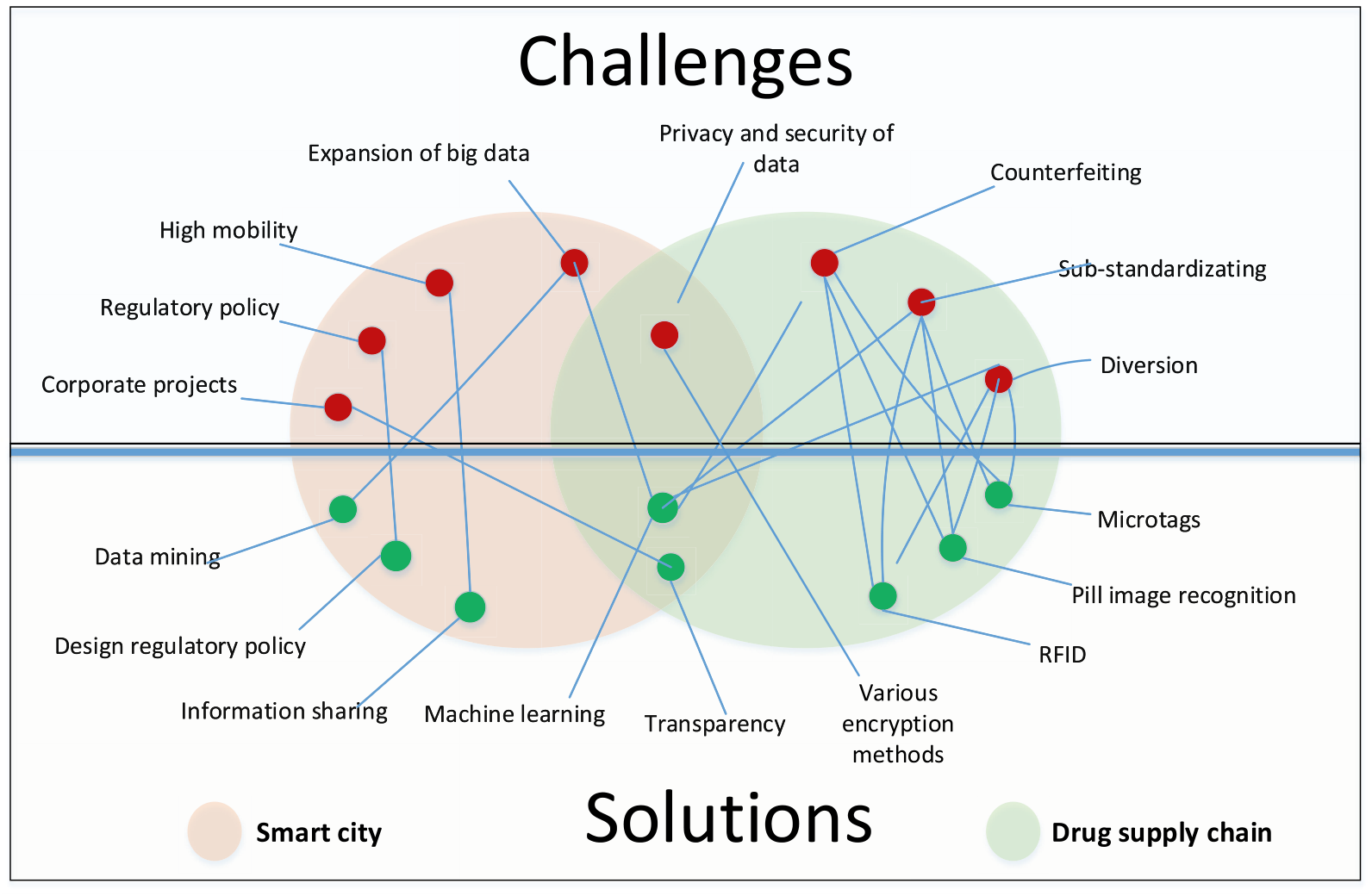
*E-mail address:* [eaderea@yahoo.com](mailto:eaderea@yahoo.com).

two most notable applications of blockchain in the IoT and healthcare, respectively.

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

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

<https://doi.org/10.1016/j.array.2022.100139>   
[Received 6 October 2021; Received in revised](https://doi.org/10.1016/j.array.2022.100139) form 21 January 2022; Accepted 4 March 2022   
Available online 12 March 2022   
[2590-0056](http://creativecommons.org/licenses/by-nc-nd/4.0/)/© 2022 The Author. Published by Elsevier Inc. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).



*E.M. Adere*  *Array 14 (2022) 100139*

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

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

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

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

*1.1. Prior reviews*

Despite the fact that blockchain is a relatively new study topic, various literature reviews have been undertaken on the subject in

general and on certain application areas in particular. Additionally, there are researches that focus on specific issues within a particular application domain. The reviews that were chosen after meeting the screening criteria outlined in the methodology section are listed below (Table 1).

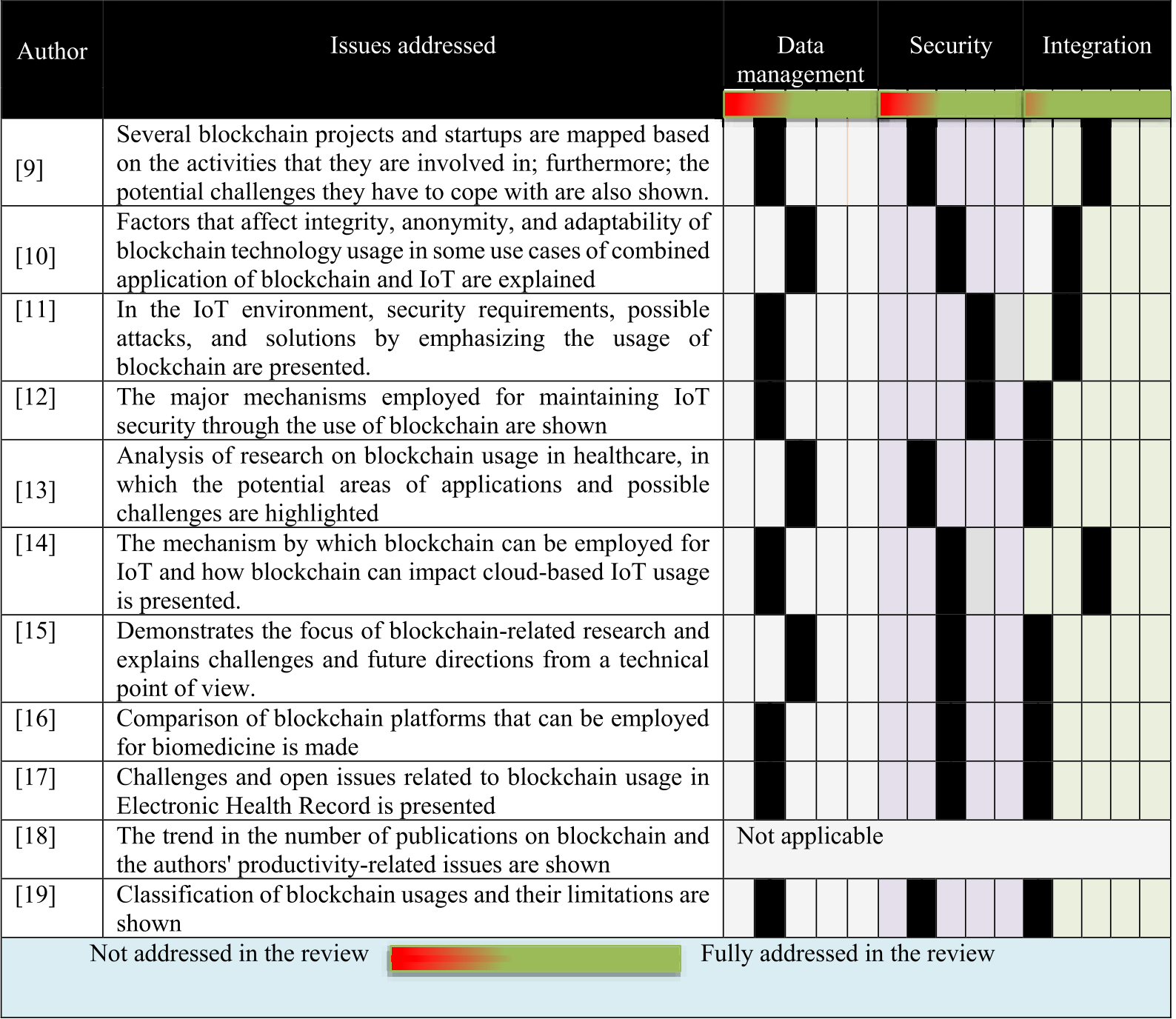
Hence the reviews are longlisted, it may be necessary to conduct a review of the reviews as a tertiary review to assess the areas addressed and the limitations of the research conducted thus far, identical to what is done by Kitchenham B. et al. [20]. Despite the abundance of reviews, there are still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

a. Shy away from showing the deficiencies of researches that have been creating what [21] call “construct identity fallacy”, which can impact knowledge development since they are piling knowledge than building it, as described by Ref. [22].

b. Don’t demonstrate the pattern being trending in developing artifacts in specific application areas,   
c. Don’t enquire about the relative performances of prototypes or sys- tems developed within or across application areas,   
d. Somehow they don’t indicate how to extend solutions from one application area to the other, which [23] calls “exaptation” and [24] labels it “knowledge brokering” in which analogical reasoning is employed to deploy knowledge from where it is known to where it is unknown.

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

**Fig. 1.** Some challenges and solutions in smart city and drug supply chain.   
2



*E.M. Adere*  *Array 14 (2022) 100139*

**Table 1**

List of selected prior reviews [9–19].

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

1. Describe the trends that have been developing in the development of instantiations.

2. Elaborate how blockchain is being employed for data management, particularly for maintaining data security, access control, and pri-vacy preservation of systems and users.

3. Portray the methods followed to integrate blockchain and IoT for their unified usage.

4. Serve as a foundation for future research that is going to be con- ducted on the issues covered in the selected application areas

*1.2. Contributions*

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

3

*E.M. Adere*  *Array 14 (2022) 100139*

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

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

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

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

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

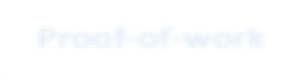
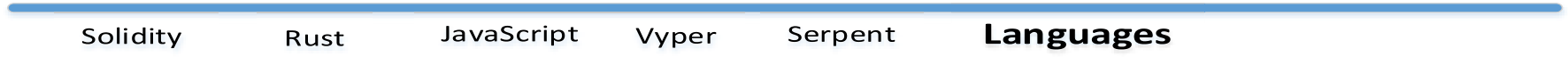
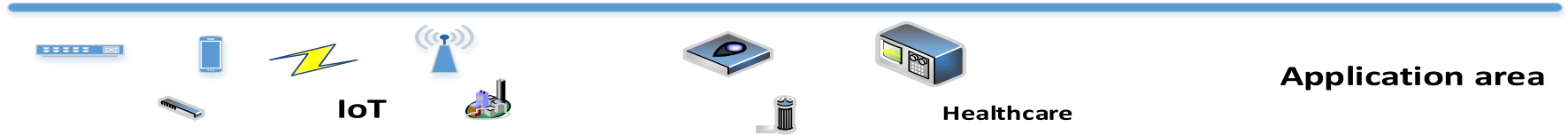
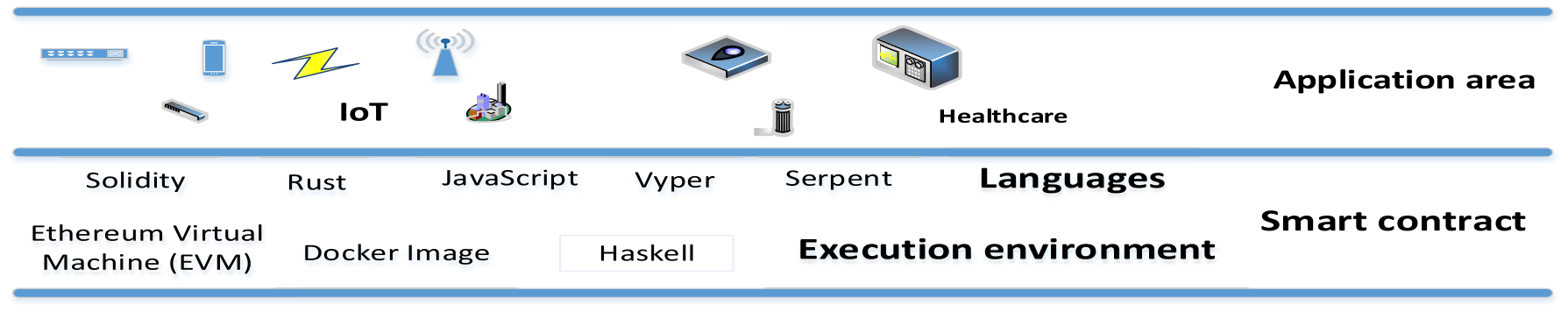
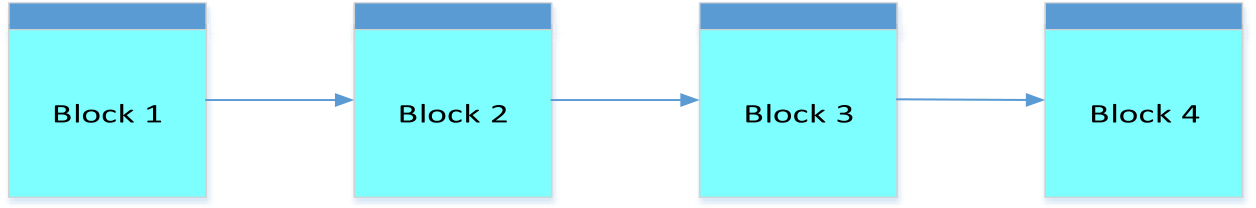
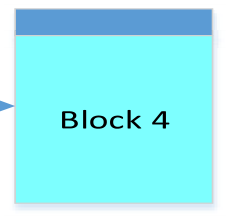
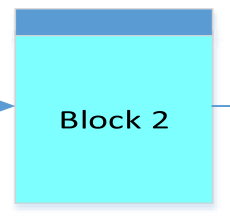
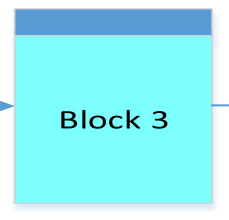
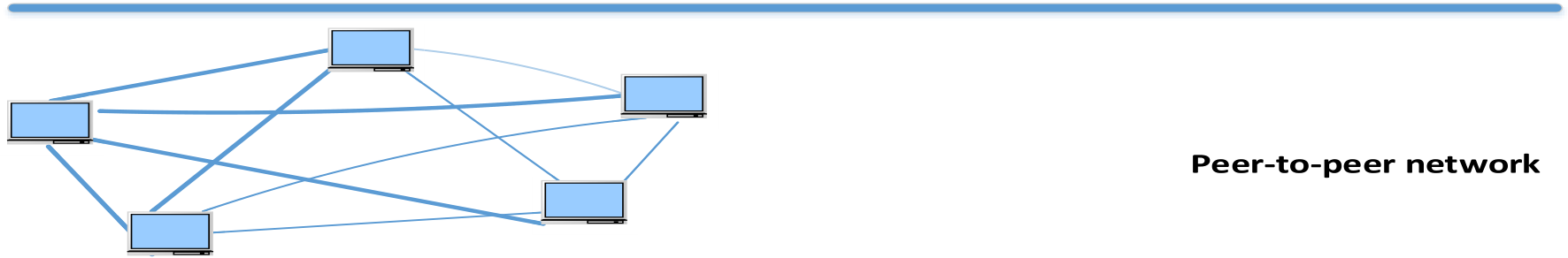
P2P networks can also be characterized as homogeneous or hetero-geneous based on the peer types involved. A homogeneous network is defined by nodes that have similar storage, computation, communica-tion, sensing, and energy capabilities. In heterogeneous networks, there is variation in one of the above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

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

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

As illustrated above, the Merkle root hash value of transactions and

4



*E.M. Adere*  *Array 14 (2022) 100139*

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

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

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

Decentralized unstructured topology is the most frequent way for developing blockchain-based architectural designs in cryptocurrency and some IoT contexts that involve several nodes. Clustering techniques similar to those mentioned above are also used in blockchain systems [44]. The communication methods outlined above are equally appli-cable in instances when blockchain technology is used. In this light, Bitcoin can be viewed as an illustration of a decentralized unstructured P2P network in which transactions are broadcasted to participants through gossiping. Similarly, gossip is utilized in Hyperledger Fabric to

distribute metadata when a new peer joins the network and to construct and maintain a local view of other peers [45]. The following figure (Fig. 2) depicts the fundamental components of blockchain.

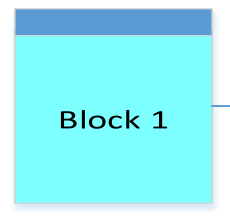
*2.2. Internet of Things (IoT)*

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

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

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





**Fig. 2.** The fundamental components of a blockchain.

5

*E.M. Adere*  *Array 14 (2022) 100139*

IoT devices to attack and prevents them from communicating securely.

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

*2.3. Health information technology (HIT)*

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

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

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

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

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

6

*E.M. Adere*  *Array 14 (2022) 100139*

*3.2. Inclusion criteria*

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

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

Despite this, on publications that pass the above criteria, a critical assessment was made. Critical assessment is elaborated in [69, p. 265] as a way that helps to broaden the “analysis of what is known, how knowledge is acquired, what types of knowledge is produced, how useful different types of knowledge are in understanding in explaining a

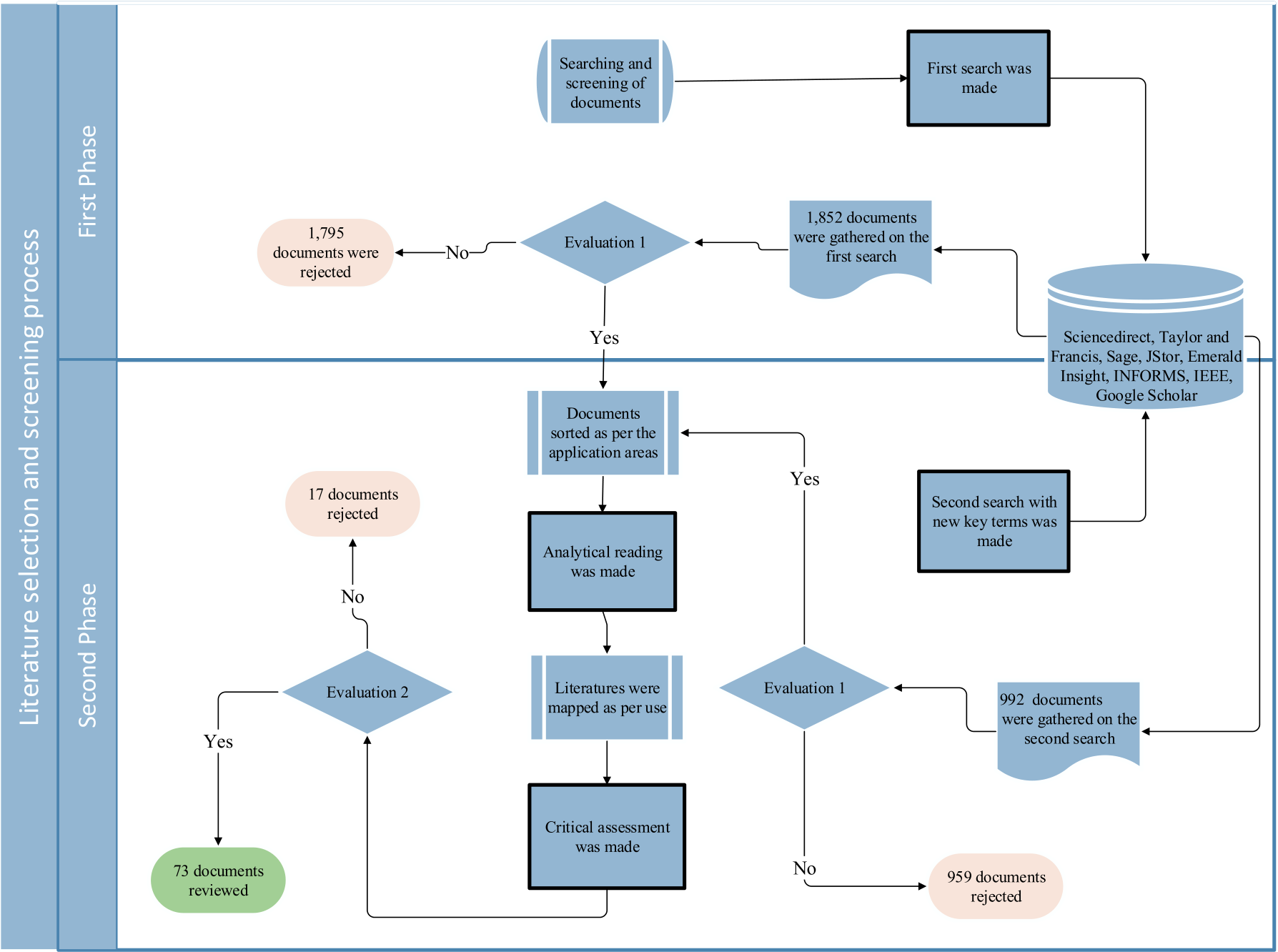
problem of interest and where the boundaries and weaknesses of exist-ing knowledge are”. The reason for making a critical analysis of litera-ture is to get an understanding of the knowledge that has been gained from using blockchain for the application areas, to comprehend the level at which blockchain has been revolutionizing the application areas and to savvy the way the artifacts which are composed of constructs (vo-cabulary and symbols), models (abstractions and representations), methods (algorithms and practices) and instantiations (implemented and prototype systems) [72] are being developed. The critical assess-ment enables the author to conduct a second evaluation that helps to screen out publications that have fewer relevancies and are deprived of depth in their presentation. Some publications excluded in this regard include [73–75]. The steps followed in preparing the article is shown in Fig. 3.

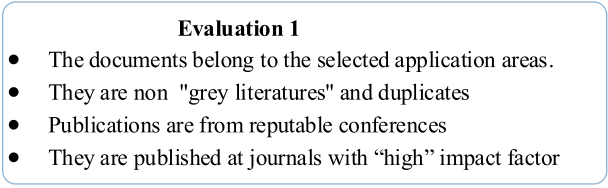
**4. Result**

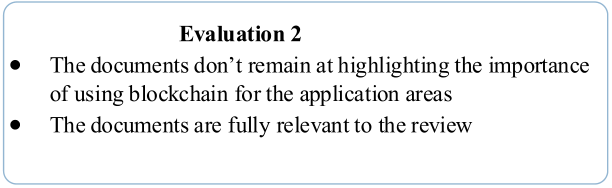
The publications reviewed cover some common themes and other application-specific issues. This section summarizes the findings from the literature review.

*4.1. The reviewed publications*

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







**Fig. 3.** Steps followed in the review process.   
7

*E.M. Adere*  *Array 14 (2022) 100139*

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

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

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

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

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

*4.2. Integrating blockchain with IoT*

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

With this in mind, two articles seek to classify the integration methods of blockchain and IoT into three distinct categories. On the one hand [81], classify integration solutions according to the amount of data that flows through blockchain during data exchange between IoT de-vices. On the other hand [135], compares blockchain with cloud for service provision. The two approaches are not mutually exclusive;

**Table 4**   
List of primary literature.

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

8

*E.M. Adere*  *Array 14 (2022) 100139*

**Table 5**   
Integration methods employed in various publications.

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

9

*E.M. Adere*  *Array 14 (2022) 100139*

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

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

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

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

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

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

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

10

*E.M. Adere*  *Array 14 (2022) 100139*

**Table 7**   
Access control method utilized.

**Table 8**   
Methods used for privacy preservation.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Publications | Access Control method employed | Application area | | Publications | Privacy preservation method | Application area | |
|  |  | IoT | Healthcare |  | employed | IoT | Healthcare |

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

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

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

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

*4.4.4. Dissemination*   
 Dissemination of data can take a variety of forms. Fundamentally, there are two main groups of data dissemination methods depending on who initiates the data transmission, i.e. whether a client requests or a server supplies the data. The first is push-based, while the second is pull- based. While push-based dissemination involves a server pushing data to

11

*E.M. Adere*  *Array 14 (2022) 100139*

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

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

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

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

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

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

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

From the standpoint of data storage, disparities in blockchain utili-zation are found. These are due to a variety of variables, including legal concerns about privacy, latency requirements, and the size of the file to be stored. In this context, healthcare is subject to a variety of legal

12

*E.M. Adere*  *Array 14 (2022) 100139*

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

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

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

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

*4.6. Blockchain and drug supply chain*

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

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

Several blockchain-based systems, on the other hand, are being

13

*E.M. Adere*  *Array 14 (2022) 100139*

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

*5.2. On data management in IoT and healthcare*

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

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

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

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

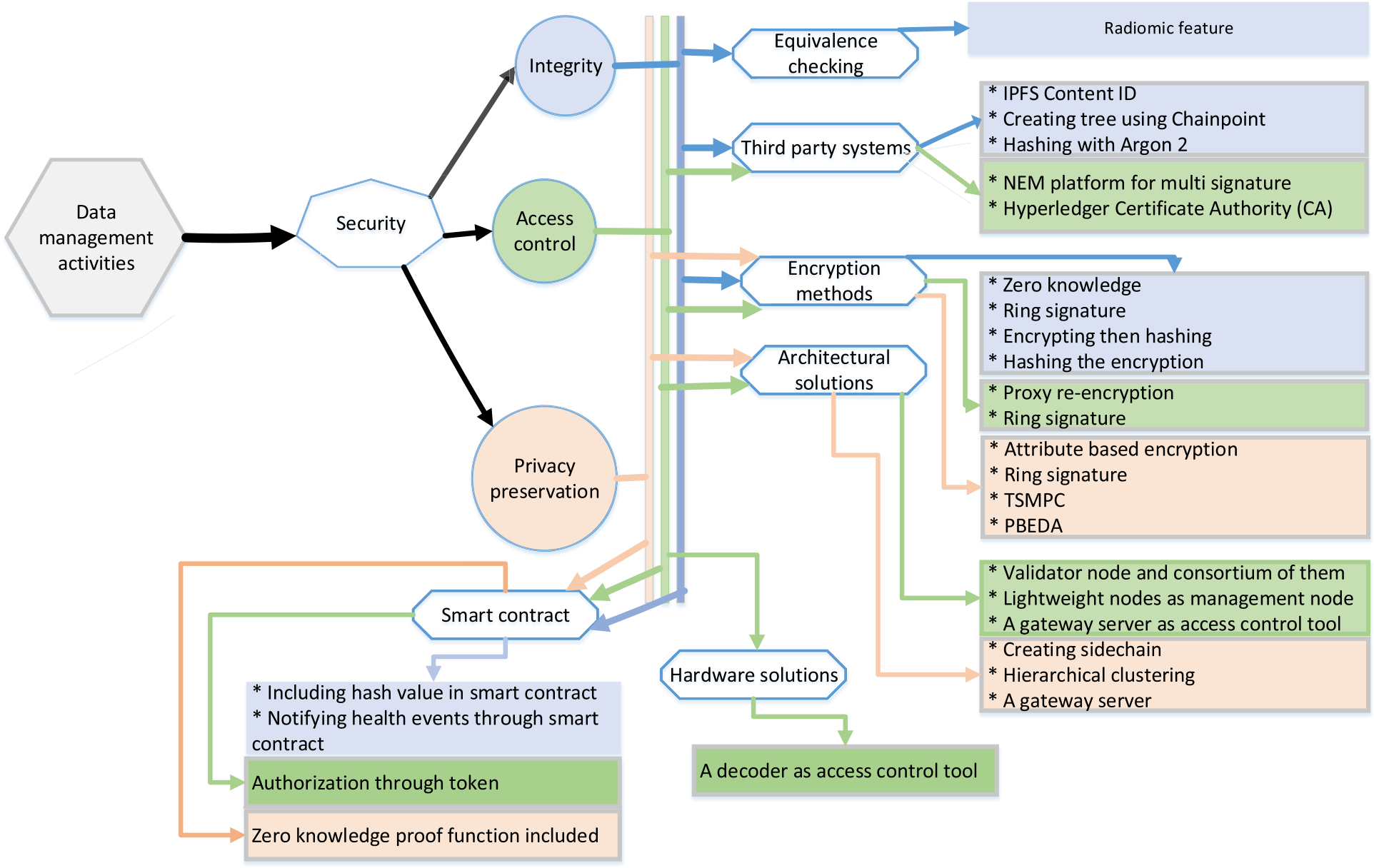
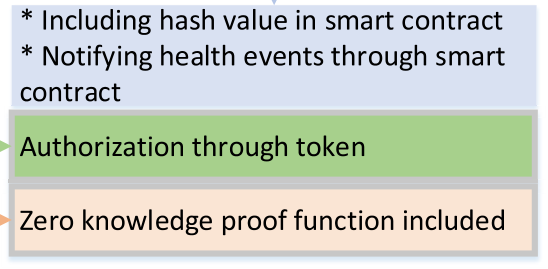
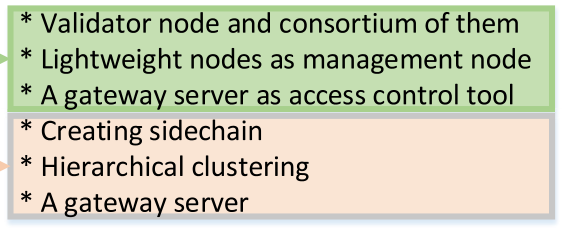
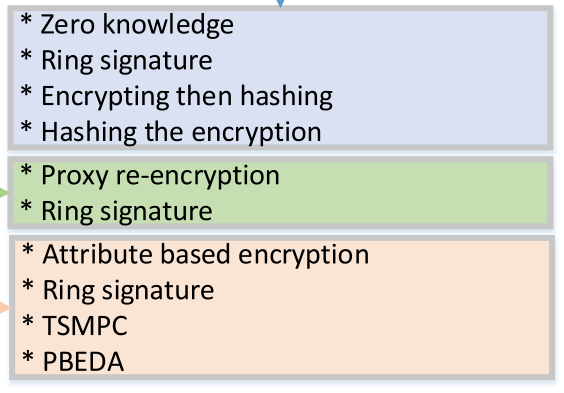
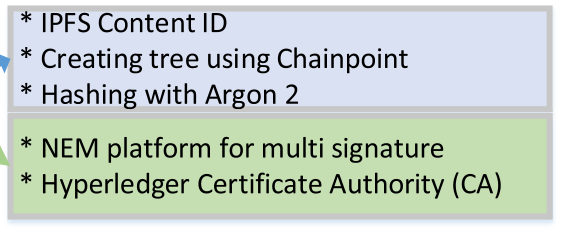
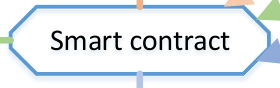
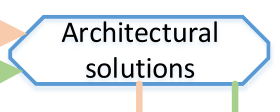
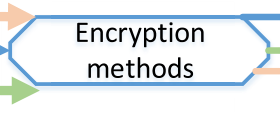
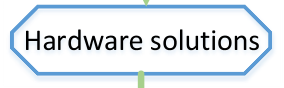
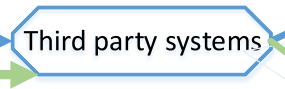
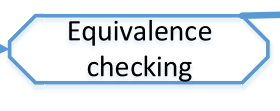
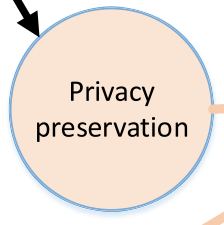
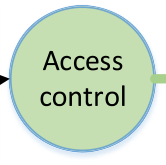
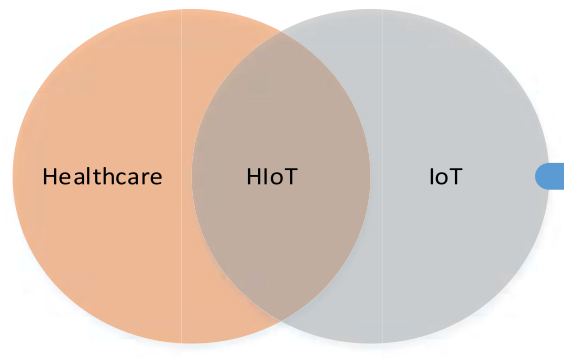
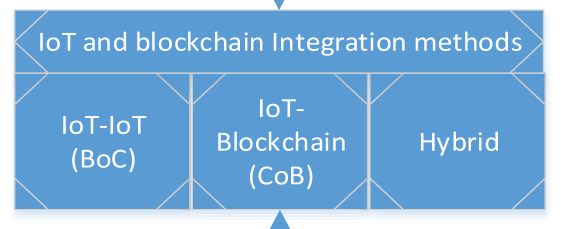
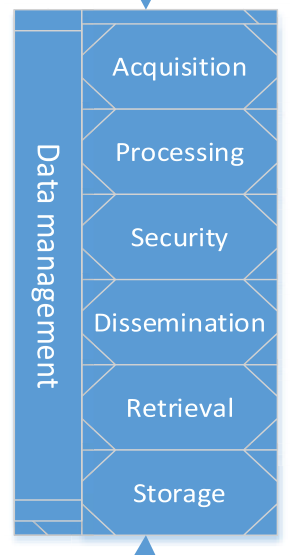
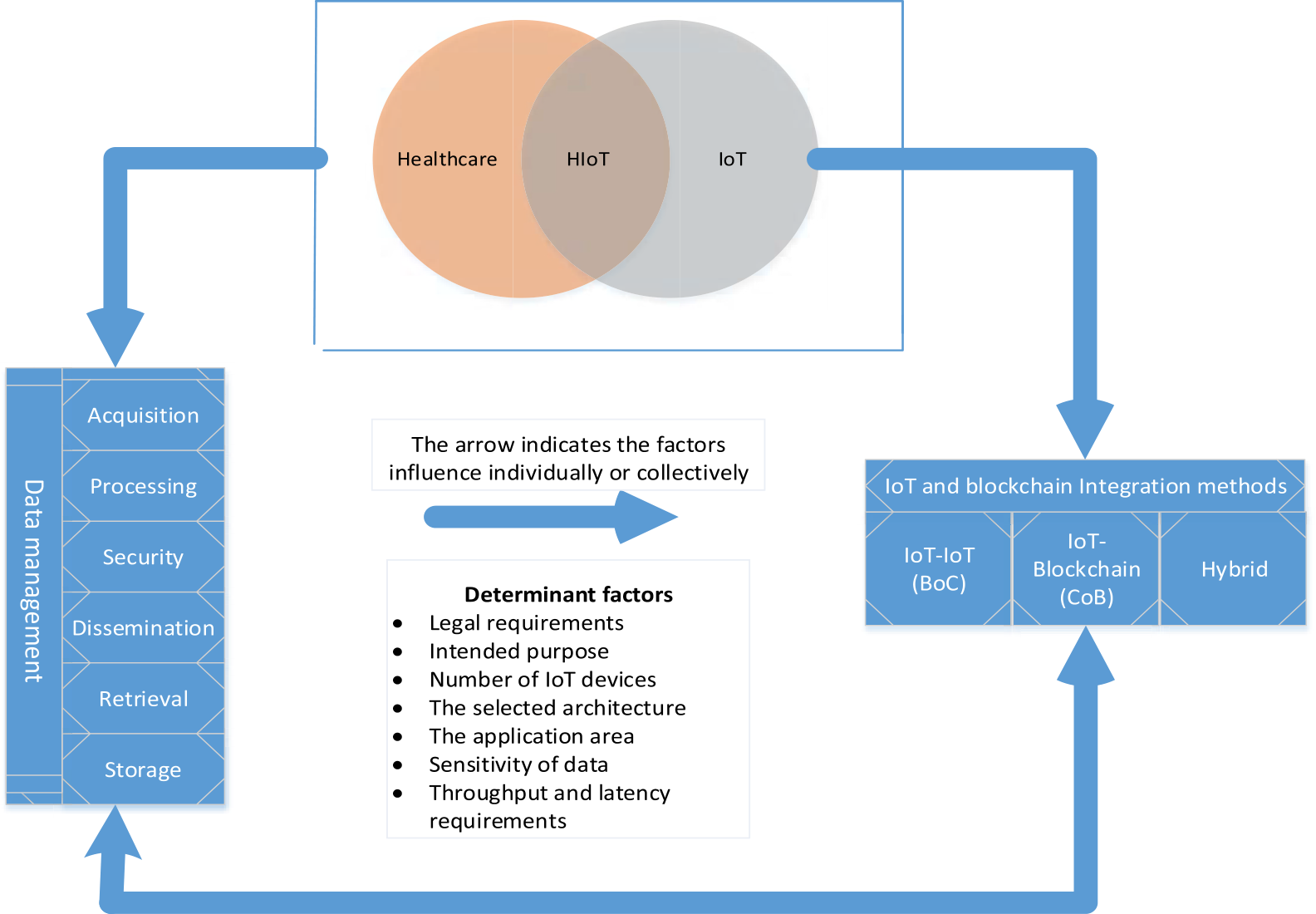
In terms of data processing, smart contracts and the design of data- processing-friendly architecture have been employed. In this regard, it has been revealed that it is difficult to justify the number and purpose of smart contract usage, which explains why, as previously said, the number of smart contracts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

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

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

Meanwhile, many encryption techniques such as proxy re-encryption with blinding, attribute-based re-encryption, and pseudonym-based encryption with multiple authorities are considered to maintain pri-vacy preservation. Certain encryption techniques are also employed to ensure the integrity, access control, and privacy of a single system. In

14



|  |  |  |  |
| --- | --- | --- | --- |
| *E.M. Adere* |  |  | *Array 14 (2022) 100139* |

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

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

15

*E.M. Adere*  *Array 14 (2022) 100139*

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

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

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

**7. Conclusion**

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

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

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

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

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

16

*E.M. Adere*  *Array 14 (2022) 100139*

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

[6] [Roman-Belmonte JM](https://doi.org/10.25300/MISQ/2016/40.3.02), De la Corte-Rodriguez H, Rodriguez-Merchan EC. How blockchain technology can change medicine. Postgrad Med 2018;130(4):420–7. <https://doi.org/10.1080/00325481.2018.1472996>.

[7] [Angraal S, Krumholz HM, Schulz WL. Blockchain t](https://doi.org/10.1080/00325481.2018.1472996)echnology: applications in health care. Circ Cardiovasc Qual Outc 2017;10(9). [https://doi.org/10.1161/](https://doi.org/10.1161/CIRCOUTCOMES.117.003800) [CIRCOUTCOMES.117.003800](https://doi.org/10.1161/CIRCOUTCOMES.117.003800).

[8] [T.-T. Kuo, H.-E. Kim, and L. O](https://doi.org/10.1161/CIRCOUTCOMES.117.003800)hno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications,” J Am Med Inf Assoc, vol. 24, no. 6, pp. 1211–1220, Nov. 2017, doi: 10.1093/jamia/ocx068.

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

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

<https://doi.org/10.1109/AICCSA.2016.7945805>.

[11] [Khan MA, Salah K. IoT security: review, blockch](https://doi.org/10.1109/AICCSA.2016.7945805)ain solutions, and open challenges. Future Generat Comput Syst 2018;82:395–411. [https://doi.org/](https://doi.org/10.1016/j.future.2017.11.022) [10.1016/j.future.2017.11.022](https://doi.org/10.1016/j.future.2017.11.022).

[12] [Taylor PJ, Dargahi T, Dehgha](https://doi.org/10.1016/j.future.2017.11.022)ntanha A, Parizi RM, Choo K-KR. A systematic literature review of blockchain cyber security. Digit Commun Netw 2019. [https://](https://doi.org/10.1016/j.dcan.2019.01.005) [doi.org/10.1016/j.dcan.2019.01.005](https://doi.org/10.1016/j.dcan.2019.01.005). S2352864818301536.

[13] [H](https://doi.org/10.1016/j.dcan.2019.01.005)¨[olbl M, Kompara M, Kami](https://doi.org/10.1016/j.dcan.2019.01.005)ˇ[sali](https://doi.org/10.1016/j.dcan.2019.01.005)´[c A, N](https://doi.org/10.1016/j.dcan.2019.01.005)emec Zlatolas L. A systematic review of the use of blockchain in healthcare. Symmetry 2018;10(10):470. [https://doi.org/](https://doi.org/10.3390/sym10100470) [10.3390/sym10100470](https://doi.org/10.3390/sym10100470).

[14] [Fernandez-Carames TM](https://doi.org/10.3390/sym10100470), Fraga-Lamas P. A review on the use of blockchain for the internet of things. IEEE Access 2018;6:32979–3001. [https://doi.org/10.1109/](https://doi.org/10.1109/ACCESS.2018.2842685) [ACCESS.2018.2842685](https://doi.org/10.1109/ACCESS.2018.2842685).

[15] [Yli-Huumo J, Ko D, Ch](https://doi.org/10.1109/ACCESS.2018.2842685)oi S, Park S, Smolander K. Where is current research on blockchain technology?—a systematic review. PLoS One 2016;11(10):e0163477. <https://doi.org/10.1371/journal.pone.0163477>.

[16] [Kuo T-T, Zavaleta Rojas H, Ohno-Machado L. C](https://doi.org/10.1371/journal.pone.0163477)omparison of blockchain platforms: a systematic review and healthcare examples. J Am Med Inf Assoc 2019;26(5):462–78. <https://doi.org/10.1093/jamia/ocy185>.

[17] Mayer AH, da Costa [CA, Righi R da R. Electronic health reco](https://doi.org/10.1093/jamia/ocy185)rds in a Blockchain: a systematic review. Health Inf J 2019. [https://doi.org/10.1177/](https://doi.org/10.1177/1460458219866350)   
[1460458219866350](https://doi.org/10.1177/1460458219866350). 1460458219866[35.](https://doi.org/10.1177/1460458219866350)

[18] [S. Miau and J.-M. Y](https://doi.org/10.1177/1460458219866350)ang, “Bibliometrics-based evaluation of the Blockchain research trend: 2008 – march 2017,” Technol Anal Strat Manag, vol. 30, no. 9, pp. 1029–1045, Sep. 2018, doi: 10.1080/09537325.2018.1434138.

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

[20] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S.

Linkman, “Systematic literature reviews in software engineering – a systematic literature review,” Inf Software Technol, vol. 51, no. 1, pp. 7–15, Jan. 2009, doi: 10.1016/j.infsof.2008.09.009.

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

[22] [Tate M, Furtm](https://doi.org/10.25300/MISQ/2016/40.3.01)ueller E, Evermann J, Bandara W. Introduction to the special issue: the literature review in information systems. Commun Assoc Inf Syst 2015;37. <https://doi.org/10.17705/1CAIS.03705>.

[23] [Gregor S, Hevner AR. Positioning and p](https://doi.org/10.17705/1CAIS.03705)resenting design science research for maximum impact. MIS Q 2013;37(2):337–55. [https://doi.org/10.25300/MISQ/](https://doi.org/10.25300/MISQ/2013/37.2.01) [2013/37.2.01](https://doi.org/10.25300/MISQ/2013/37.2.01).

[24] [Hargadon AB.](https://doi.org/10.25300/MISQ/2013/37.2.01) Brokering knowledge: linking learning and innovation. Res Organ Behav 2002;24:41–85. <https://doi.org/10.1016/S0191-3085(02)24003-4>. Jan.

[25] Ducas E, Wilner A. The [security and financial implications of blockchai](https://doi.org/10.1016/S0191-3085(02)24003-4)n technologies: regulating emerging technologies in Canada. Int J Can J Glob Pol Anal 2017;72(4):538–62. <https://doi.org/10.1177/0020702017741909>.

[26] Hammi MT, Hammi B, Be[llot P, Serhrouchni A. Bubbles of Trust: a dece](https://doi.org/10.1177/0020702017741909)ntralized blockchain-based authentication system for IoT. Comput Secur 2018;78:126–42. <https://doi.org/10.1016/j.cose.2018.06.004>.

[27] [Dagher GG, Mohler J, Milojkovic M, Marell](https://doi.org/10.1016/j.cose.2018.06.004)a PB. Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain Cities Soc 2018;39:283–97. [https://doi.org/](https://doi.org/10.1016/j.scs.2018.02.014) [10.1016/j.scs.2018.02.014](https://doi.org/10.1016/j.scs.2018.02.014).

[28] [Danzi P, Kalor AE, Stefano](https://doi.org/10.1016/j.scs.2018.02.014)vic C, Popovski P. Analysis of the communication traffic for blockchain synchronization of IoT devices. In: 2018 IEEE International Conference on Communications (ICC); 2018. p. 1–7. [https://doi.org/10.1109/](https://doi.org/10.1109/ICC.2018.8422485) [ICC.2018.8422485](https://doi.org/10.1109/ICC.2018.8422485). Kansas City, MO, May.

[29] [Qiu T, Zhang R, G](https://doi.org/10.1109/ICC.2018.8422485)ao Y. Ripple vs. SWIFT: transforming cross border remittance using blockchain technology. Procedia Comput Sci 2019;147:428–34. [https://](https://doi.org/10.1016/j.procs.2019.01.260) [doi.org/10.1016/j.procs.2019.01.260](https://doi.org/10.1016/j.procs.2019.01.260).

[30] [Kleinaki A-S, Mytis-Gkometh P, Dros](https://doi.org/10.1016/j.procs.2019.01.260)atos G, Efraimidis PS, Kaldoudi E.

A blockchain-based notarization service for biomedical knowledge retrieval.

Comput Struct Biotechnol J 2018;16:288–97. [https://doi.org/10.1016/j.](https://doi.org/10.1016/j.csbj.2018.08.002)

[csbj.2018.08.002](https://doi.org/10.1016/j.csbj.2018.08.002).

[31] [S. Kamble, A. Gu](https://doi.org/10.1016/j.csbj.2018.08.002)nasekaran, and H. Arha, “Understanding the Blockchain technology adoption in supply chains-Indian context,” Int J Prod Res, vol. 57, no. 7, pp. 2009–2033, Apr. 2019, doi: 10.1080/00207543.2018.1518610.

17

*E.M. Adere*  *Array 14 (2022) 100139*

Kenya: an identity work perspective. MIS Q 2019;43(4):1177–200. [https://doi.](https://doi.org/10.25300/MISQ/2019/14187) [org/10.25300/MISQ/2019/14187](https://doi.org/10.25300/MISQ/2019/14187).

[58] [Karahanna E, Adela C, Liu QB, Se](https://doi.org/10.25300/MISQ/2019/14187)rrano C. Capitalizing on health information technology to enable advantage in U.S. Hospitals. MIS Q 2019;43(1):113–40.

<https://doi.org/10.25300/MISQ/2019/12743>.

[59] [Baker SB, Xiang W, Atkinson I. Internet of th](https://doi.org/10.25300/MISQ/2019/12743)ings for smart healthcare: technologies, challenges, and opportunities. IEEE Access 2017;5:26521–44.

<https://doi.org/10.1109/ACCESS.2017.2775180>.

[60] [Gubbi J, Buyya R, Marusic S, Palaniswami M. In](https://doi.org/10.1109/ACCESS.2017.2775180)ternet of Things (IoT): a vision, architectural elements, and future directions. Future Generat Comput Syst 2013; 29(7):1645–60. <https://doi.org/10.1016/j.future.2013.01.010>.

[61] Vest JR, Gamm [LD. Health information exchange: persistent c](https://doi.org/10.1016/j.future.2013.01.010)hallenges and new strategies: table. J Am Med Inf Assoc 2010;17(3):288–94. [https://doi.org/](https://doi.org/10.1136/jamia.2010.003673) [10.1136/jamia.2010.003673](https://doi.org/10.1136/jamia.2010.003673).

[62] [Payton F, Pare G, Le Rouge C](https://doi.org/10.1136/jamia.2010.003673), Reddy M. Health care IT: process, people, patients and interdisciplinary considerations. J Assoc Inf Syst Online 2011;12(2):I–XIII. <https://doi.org/10.17705/1jais.00259>. Feb.

[63] [R. G. Fichman, R. Kohli, and R. Krishn](https://doi.org/10.17705/1jais.00259)an, Eds., “**Editorial overview** —the role of information systems in healthcare: current research and future trends,” Inf Syst Res, vol. 22, no. 3, pp. 419–428, Sep. 2011, doi: 10.1287/isre.1110.0382.

[64] Kwon J, Johnson ME. Meaningful healthcare security Does meaningful attestation improve information security performance. MIS Q 2018;42(4):1043–67. [https://](https://doi.org/10.25300/MISQ/2018/13580) [doi.org/10.25300/MISQ/2018/13580](https://doi.org/10.25300/MISQ/2018/13580).

[65] [Bao C, Bardhan IR, Singh H, Meyer B](https://doi.org/10.25300/MISQ/2018/13580)A, Kirksey K. Patient-provider engagement and its impact on health outcomes: a longitudinal study of patient portal use. MIS Q 2020;44(2):699–723. <https://doi.org/10.25300/MISQ/2020/14180>.

[66] Gordon WJ, Catalini C. [Blockchain technology for healthcare: facilita](https://doi.org/10.25300/MISQ/2020/14180)ting the transition to patient-driven interoperability. Comput Struct Biotechnol J 2018;16: 224–30. <https://doi.org/10.1016/j.csbj.2018.06.003>.

[67] Efanov D[, Roschin P. The all-pervasiveness of the bl](https://doi.org/10.1016/j.csbj.2018.06.003)ockchain technology. Procedia Comput Sci 2018;123:116–21. [https://doi.org/10.1016/j.](https://doi.org/10.1016/j.procs.2018.01.019)

[procs.2018.01.019](https://doi.org/10.1016/j.procs.2018.01.019).

[68] [Webster J, Watson](https://doi.org/10.1016/j.procs.2018.01.019) [RT. Analyzing the past to prepare for the future: writing a](http://refhub.elsevier.com/S2590-0056(22)00010-8/sref68) [literature review. MIS Q 2002;26(2):xiii–xxii.](http://refhub.elsevier.com/S2590-0056(22)00010-8/sref68)

[69] [Boell SK, Cecez-Kecmanovic D. A hermeneuti](http://refhub.elsevier.com/S2590-0056(22)00010-8/sref68)c approach for conducting literature reviews and literature searches. Commun Assoc Inf Syst 2014;34. [https://doi.org/](https://doi.org/10.17705/1CAIS.03412) [10.17705/1CAIS.03412](https://doi.org/10.17705/1CAIS.03412).

[70] [Bandara W, Furtmuelle](https://doi.org/10.17705/1CAIS.03412)r E, Gorbacheva E, Miskon S, Beekhuyzen J. Achieving rigor in literature reviews: insights from qualitative data analysis and tool- support. Commun Assoc Inf Syst 2015;37. [https://doi.org/10.17705/](https://doi.org/10.17705/1CAIS.03708)   
[1CAIS.03708](https://doi.org/10.17705/1CAIS.03708).

[71] [Levy Y, Ellis](https://doi.org/10.17705/1CAIS.03708) TJ. A systems approach to conduct an effective literature review in support of information systems research. Info Sci Int J Emerg Transdiscipl 2006;9: 181–212. <https://doi.org/10.28945/479>.

[72] Hevner A[R, March ST, Park J, Ram S. D](https://doi.org/10.28945/479)esign science in information systems research. MIS Q 2004;28(1):75–105. Mar. [http://misq.org/design-science-in-in](http://misq.org/design-science-in-information-systems-research.html?SID=shpier0675mhpes3hkfagcqee1)

[73] [Hoy MB. An introduction to the blockchain and its implications for l](http://misq.org/design-science-in-information-systems-research.html?SID=shpier0675mhpes3hkfagcqee1)ibraries and [formation-systems-research.html?SID=shpier0675mhpes3hkfagcqee1](http://misq.org/design-science-in-information-systems-research.html?SID=shpier0675mhpes3hkfagcqee1).

medicine. Med Ref Serv Q 2017;36(3):273–9. [https://doi.org/10.1080/](https://doi.org/10.1080/02763869.2017.1332261) [02763869.2017.1332261](https://doi.org/10.1080/02763869.2017.1332261).

[74] [Zhang P, Walker MA, Wh](https://doi.org/10.1080/02763869.2017.1332261)ite J, Schmidt DC, Lenz G. Metrics for assessing blockchain-based healthcare decentralized apps. In: 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom).

Dalian; 2017. p. 1–4. <https://doi.org/10.1109/HealthCom.2017.8210842>.

[75] Engelhardt MA. Hitch[ing healthcare to the chain: an introduction to bloc](https://doi.org/10.1109/HealthCom.2017.8210842)kchain technology in the healthcare sector. Technol Innov Manag Rev 2017;7(10):22–34. <https://doi.org/10.22215/timreview/1111>.

[76] [Pahl C, El Ioini N, Helmer S. A decision fr](https://doi.org/10.22215/timreview/1111)amework for blockchain platforms for IoT and edge computing. In: Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security. Madeira, Portugal: Funchal; 2018.

p. 105–13. <https://doi.org/10.5220/0006688601050113>.

[77] Esposito C, [De Santis A, Tortora G, Chang H, Choo K-KR](https://doi.org/10.5220/0006688601050113). Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput 2018;5 (1):31–7. <https://doi.org/10.1109/MCC.2018.011791712>. Jan.

[78] Novo O. B[lockchain meets IoT: an architecture for scalable](https://doi.org/10.1109/MCC.2018.011791712) access management in IoT. IEEE Internet Things J 2018;5(2):1184–95. [https://doi.org/10.1109/](https://doi.org/10.1109/JIOT.2018.2812239) [JIOT.2018.2812239](https://doi.org/10.1109/JIOT.2018.2812239). Apr.

[79] [Sharma PK, Singh S,](https://doi.org/10.1109/JIOT.2018.2812239) Jeong Y-S, Park JH. DistBlockNet: a distributed blockchains- based secure SDN architecture for IoT networks. IEEE Commun Mag 2017;55(9): 78–85. <https://doi.org/10.1109/MCOM.2017.1700041>.

[80] Dorri A[, Kanhere SS, Jurdak R. Towards an optimized](https://doi.org/10.1109/MCOM.2017.1700041) BlockChain for IoT. In: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation - IoTDI ’17; 2017. p. 173–8. [https://doi.org/10.1145/](https://doi.org/10.1145/3054977.3055003) [3054977.3055003](https://doi.org/10.1145/3054977.3055003). Pittsburgh, PA, USA.

[81] [A. Reyna, C. Martí](https://doi.org/10.1145/3054977.3055003)n, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT. Challenges and opportunities,” Future Generat Comput Syst, vol. 88, pp. 173–190, Nov. 2018, doi: 10.1016/j.future.2018.05.046.

[82] Teslya N, Ryabchikov I. Blockchain-based platform architecture for industrial IoT. In: 2017 *21st* Conference of Open Innovations Association (FRUCT); 2017.

p. 321–9. <https://doi.org/10.23919/FRUCT.2017.8250199>. Helsinki, Nov.

[83] Lombardi [F, Aniello L, De Angelis S, Margheri A, Sassone](https://doi.org/10.23919/FRUCT.2017.8250199) V. A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids. London, UK.

In: Living in the Internet of Things: Cybersecurity of the IoT - 2018; 2018. p. 42. <https://doi.org/10.1049/cp.2018.0042>.

18

*E.M. Adere*  *Array 14 (2022) 100139*

Management, Cryptocurrencies and Blockchain Technology, vol. 11025. Cham: Springer International Publishing; 2018. p. 329–44. [https://doi.org/10.1007/](https://doi.org/10.1007/978-3-030-00305-0_23) [978-3-030-00305-0\_23](https://doi.org/10.1007/978-3-030-00305-0_23).

[109] [S. L. Cichosz, M. N. St](https://doi.org/10.1007/978-3-030-00305-0_23)ausholm, T. Kronborg, P. Vestergaard, and O. Hejlesen, “How to use blockchain for diabetes health care data and access management: an operational concept,” J Diabetes Sci Technol, vol. 13, no. 2, pp. 248–253, Mar. 2019, doi: 10.1177/1932296818790281.

[110] Patel V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Inf J 2018. [https://doi.org/10.1177/](https://doi.org/10.1177/1460458218769699) [1460458218769699](https://doi.org/10.1177/1460458218769699). 146045821876969.

[111] [Zhang P, White J, S](https://doi.org/10.1177/1460458218769699)chmidt DC, Lenz G, Rosenbloom ST. FHIRChain: applying blockchain to securely and scalably share clinical data. Comput Struct Biotechnol J 2018;16:267–78. <https://doi.org/10.1016/j.csbj.2018.07.004>.

[112] Thwin TT, Vasupon[gayya S. Blockchain-based access control m](https://doi.org/10.1016/j.csbj.2018.07.004)odel to preserve privacy for personal health record systems. Secur Commun Network 2019:1–15. <https://doi.org/10.1155/2019/8315614>.

[113] [Al Omar A, Rahman MS, Basu A, Kiyom](https://doi.org/10.1155/2019/8315614)oto S. MediBchain: a blockchain based privacy preserving platform for healthcare data. In: Wang G, Atiquzzaman M, Yan Z, Choo K-KR, editors. Security, Privacy, and Anonymity in Computation, Communication, and Storage, vol. 10658. Cham: Springer International Publishing; 2017. p. 534–43. <https://doi.org/10.1007/978-3-319-72395-2_49>.

[114] Wong DR, Bhattacharya S, Bu[tte AJ. Prototype of running clinical trials in an](https://doi.org/10.1007/978-3-319-72395-2_49) untrustworthy environment using blockchain. Nat Commun Dec. 2019;10(1):917. <https://doi.org/10.1038/s41467-019-08874-y>.

[115] [Zhang J, Xue N, Huang X. A secure system fo](https://doi.org/10.1038/s41467-019-08874-y)r pervasive social network-based healthcare. IEEE Access 2016;4:9239–50. [https://doi.org/10.1109/](https://doi.org/10.1109/ACCESS.2016.2645904)   
[ACCESS.2016.2645904](https://doi.org/10.1109/ACCESS.2016.2645904).

[116] [Liu B, Yu XL, Chen S, X](https://doi.org/10.1109/ACCESS.2016.2645904)u X, Zhu L. Blockchain based data integrity service framework for IoT data. In: 2017 IEEE International Conference on Web Services.

Honolulu, HI, USA, Jun: ICWS); 2017. p. 468–75. [https://doi.org/10.1109/](https://doi.org/10.1109/ICWS.2017.54) [ICWS.2017.54](https://doi.org/10.1109/ICWS.2017.54).

[117] [Ouaddah A, E](https://doi.org/10.1109/ICWS.2017.54)lkalam AA, Ouahman AA. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In: Rocha ´A, Serrhini M, Felgueiras C, editors. Europe and MENA Cooperation Advances in Information and Communication Technologies. vol. 520. Cham: Springer International Publishing; 2017. p. 523–33. [https://doi.org/10.1007/978-3-319-](https://doi.org/10.1007/978-3-319-46568-5_53) [46568-5\_53](https://doi.org/10.1007/978-3-319-46568-5_53).

[118] [Rantos K, D](https://doi.org/10.1007/978-3-319-46568-5_53)rosatos G, Demertzis K, Ilioudis C, Papanikolaou A. Blockchain-based consents management for personal data processing in the IoT ecosystem. In: Proceedings of the 15th International Joint Conference on e-Business and Telecommunications. Porto, Portugal; 2018. p. 738–43. [https://doi.org/10.5220/](https://doi.org/10.5220/0006911007380743) [0006911007380743](https://doi.org/10.5220/0006911007380743).

[119] [Liang X, Zhao J, She](https://doi.org/10.5220/0006911007380743)tty S, Li D. Towards data assurance and resilience in IoT using blockchain. In: Milcom 2017 - 2017 IEEE Military Communications Conference.

Baltimore, MD: MILCOM); 2017. p. 261–6. [https://doi.org/10.1109/](https://doi.org/10.1109/MILCOM.2017.8170858) [MILCOM.2017.8170858](https://doi.org/10.1109/MILCOM.2017.8170858).

[120] [Lin J, Shen Z, Miao C. U](https://doi.org/10.1109/MILCOM.2017.8170858)sing blockchain technology to build trust in sharing LoRaWAN IoT. In: Proceedings of the 2nd International Conference on Crowd Science and Engineering - ICCSE’17; 2017. p. 38–43. [https://doi.org/10.1145/](https://doi.org/10.1145/3126973.3126980) [3126973.3126980](https://doi.org/10.1145/3126973.3126980). Beijing, China.

[121] [Cheng EC, Le Y, Zh](https://doi.org/10.1145/3126973.3126980)ou J, Lu Y. Healthcare services across China – on implementing an extensible universally unique patient identifier system. Int J Healthc Manag 2018;11(3):210–6. <https://doi.org/10.1080/20479700.2017.1398388>.

[122] Sun J, Yan J, Zhan[g KZK. Blockchain-based sharing services: what bl](https://doi.org/10.1080/20479700.2017.1398388)ockchain technology can contribute to smart cities. Financ Innov 2016;2(1):26. [https://doi.](https://doi.org/10.1186/s40854-016-0040-y) [org/10.1186/s40854-016-0040-y](https://doi.org/10.1186/s40854-016-0040-y).

[123] [Lazaroiu C, Roscia M. Smart dist](https://doi.org/10.1186/s40854-016-0040-y)rict through IoT and blockchain. In: 2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA); 2017. p. 454–61. <https://doi.org/10.1109/ICRERA.2017.8191102>.

San Diego, CA, Nov.

[124] Yuan Y, Wang F-Y. Towards blockchain-based intelligent transportation systems.

In: 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC); 2016. p. 2663–8. <https://doi.org/10.1109/ITSC.2016.7795984>. Rio de Janeiro, Brazil, Nov.

[125] Sharma PK, Park JH. Blockchain based hybrid network architecture for the smart city. Future Generat Comput Syst 2018;86:650–5. [https://doi.org/10.1016/j.](https://doi.org/10.1016/j.future.2018.04.060)

[future.2018.04.060](https://doi.org/10.1016/j.future.2018.04.060).

[126] [M. Singh and S. Kim](https://doi.org/10.1016/j.future.2018.04.060), “Branch based blockchain technology in intelligent vehicle,” Comput Network, vol. 145, pp. 219–231, Nov. 2018, doi: 10.1016/j.

comnet.2018.08.016.

[127] Alladi T, Chamola V, Rodrigues JJPC, Kozlov SA. Blockchain in smart grids: a review on different use cases. Sensors 2019;19(22):4862. [https://doi.org/](https://doi.org/10.3390/s19224862) [10.3390/s19224862](https://doi.org/10.3390/s19224862).

[128] [Singh S, Ra I-H, Me](https://doi.org/10.3390/s19224862)ng W, Kaur M, Cho GH, Sh-BlockCC. A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. Int J Distributed Sens Netw 2019;15(4). [https://doi.org/](https://doi.org/10.1177/1550147719844159) [10.1177/1550147719844159](https://doi.org/10.1177/1550147719844159). 155014771984415.

[129] [Awais Hassan M, Habiba U, G](https://doi.org/10.1177/1550147719844159)hani U, Shoaib M. A secure message-passing framework for inter-vehicular communication using blockchain. Int J Distributed Sens Netw 2019;15(2). <https://doi.org/10.1177/1550147719829677>.

155014771982967.

[130] Mackey TK, Nayyar G. A review of existing and emerging digital technologies to combat the global trade in fake medicines. Expet Opin Drug Saf 2017;16(5): 587–602. <https://doi.org/10.1080/14740338.2017.1313227>.

19

*E.M. Adere*  *Array 14 (2022) 100139*

[158] Su K, Li J, Fu H. Smart city and the applications. In: 2011 International Conference on Electronics, Communications and Control (ICECC); 2011.

p. 1028–31. <https://doi.org/10.1109/ICECC.2011.6066743>. Ningbo, China, Sep. [159] Kitchin R. T[he real-time city? Big data and smart urbanism](https://doi.org/10.1109/ICECC.2011.6066743). Geojournal 2014;79 (1):1–14. <https://doi.org/10.1007/s10708-013-9516-8>.

[160] Eremia M[, Toma L, Sanduleac M. The smart city conce](https://doi.org/10.1007/s10708-013-9516-8)pt in the 21st century. Procedia Eng 2017;181:12–9. <https://doi.org/10.1016/j.proeng.2017.02.357>.

[161] Petrolo R, Loscrì V, Mitton N. [Towards a smart city based on cloud of things](https://doi.org/10.1016/j.proeng.2017.02.357), a survey on the smart city vision and paradigms: R. Petrolo, V. Loscrì and N. Mitton.

Trans Emerg Telecommun Technol 2017;28(1):e2931. [https://doi.org/10.1002/](https://doi.org/10.1002/ett.2931) [ett.2931](https://doi.org/10.1002/ett.2931).

[162] [Chourab](https://doi.org/10.1002/ett.2931)i H, et al. Understanding smart cities: an integrative framework. In: 2012 45th Hawaii International Conference on System Sciences; 2012. p. 2289–97.

<https://doi.org/10.1109/HICSS.2012.615>. Maui, HI, USA, Jan.

20