Information System and Smart City 2025, 5(1), 2334.
https://doi.org/10.59400/issc2334

Review

Navigating the future of smart cities: Addressing IoT challenges through blockchain solutions

Yasaman Ghaderi[1], Mohammad Reza Ghaderi[2,*]

[1] Department of Urban Planning, Tarbiat Modares University, Tehran 14115-111, Iran
[2] Department of Electrical Engineering, Islamic Azad University, South Tehran Branch, Tehran 1584743311, Iran
*** Corresponding author:** Mohammad Reza Ghaderi, st_mr_ghaderi@azad.ac.ir

CITATION

Ghaderi Y, Ghaderi MR. Navigating the future of smart cities: Addressing IoT challenges through blockchain solutions. Information System and Smart City. 2025; 5(1): 2334. https://doi.org/10.59400/issc2334

ARTICLE INFO

Received: 20 December 2024
Accepted: 14 March 2025
Available online: 27 March 2025

Abstract: As urbanization accelerates, smart cities are increasingly turning to innovative technologies to enhance city management, governance, and citizen engagement. This paper explores the application of blockchain technology in smart cities, particularly its interaction with the Internet of Things (IoT). Despite significant strides in utilizing blockchain for specific applications, existing frameworks often focus on narrow sectors, such as energy management or data security, lacking a holistic integration across municipal functions. This research identifies a critical gap in existing literature: the need for a comprehensive blockchain framework that connects multiple urban sectors, facilitates secure data exchange, and empowers citizens through decentralized systems. The proposed framework underscores the potential of blockchain to create a transparent, efficient, and citizen-friendly urban environment by implementing decentralized identity management, smart contracts for public services, and innovative citizen engagement platforms. By addressing this gap, the study contributes to the discourse on smart city development by providing an adaptable model that can be tailored to the unique needs of diverse urban environments.

Keywords: smart city; blockchain; internet of things (IoT); information technology (IT)

1. Introduction

Rapid population growth has been observed in the world. According to the United [1], about 55% of the world's population has lived in the urban areas and this ratio is estimated to reach to 68% by 2050. Increasing demand for urbanization and growing population bring numerous social, economic, environmental, and technical problems that could jeopardize urban sustainability. Hence, to optimize the use of existing assets of cities, the adoption of smart concepts has been considered by the governments [2]. The smart cities are designed and set up based on many characteristics such as sustainability, urbanization, intelligence, and quality of life (QoL). Smart cities are considered new utopia cities in the modern world [3]. Researchers suggest smart cities as a great solution to urbanization challenges such as transportation, health, pollution, resource scarcity, and waste management. The smart cities have many applications in modern societies. Some of the smart city applications are as follows: Smart buildings [4] , smart energy, smart health [5], smart education, smart government [6], and smart security [7]. A number of developed smart cities in the world are introduced in **Table 1** [8].

Table 1. Characteristics of developed smart cities [8]: Summary of key features and technological initiatives in various developed smart cities.

City	Smart application
Amsterdam/Netherlands	Security/transportation
Barcelona/Spain	Transportation
Barcelona/Spain	Network management
Fujisawa/Japan	Carbon footprints
Groening/Netherlands	Transportation
Manchester, Turin/UK, Italy	Climate
Norfolk/England	Data sharing
Padova/Italy	Lighting/pollution
PlanIT Valley/Portugal	Sensors employment
Santa Cruz/California	Criminal data analysis
Santander/Spain	Smart Production Solution (SPS)
Songdo/South Korea	Buildings
Stockholm/Sweden	Fiber Optic Network (FON)
Uppsala/Sweden	Transportation /pollution
Vienna/Austria	Securing climatic conditions

1.1. IoT-based smart cities

Smart cities composed of components include smart infrastructure, smart transportation, smart citizens, smart health, smart energy, smart technologies, and smart government. In addition, the smart city characteristics can be described by three main factors include attributes, themes, and infrastructures [9,10]. IoT infrastructure, among the smart city infrastructures plays an important role in the smart cities. IoT is the core technology of smart cities. In other words, IoT is the specialized pillar of smart cities. The IoT includes various components such as hardware, software, and sensor networks. The IoT is a network composed of connected objects such as sensors, actuators, buildings, structures, vehicles, energy systems, computers, and smartphones. Communication technology is required to read data from sensors and send control commands to actuators. IoT technologies used to aggregate data in the smart cities include: Radio Frequency Identification (RFID), Near Field Communication (NFC), Low-rate Wireless Personal Area Network (LWPAN), Wireless Sensor Network (WSN), and 4G/Long Term Evolution (4G/LTE) (see **Figure 1**) [11].

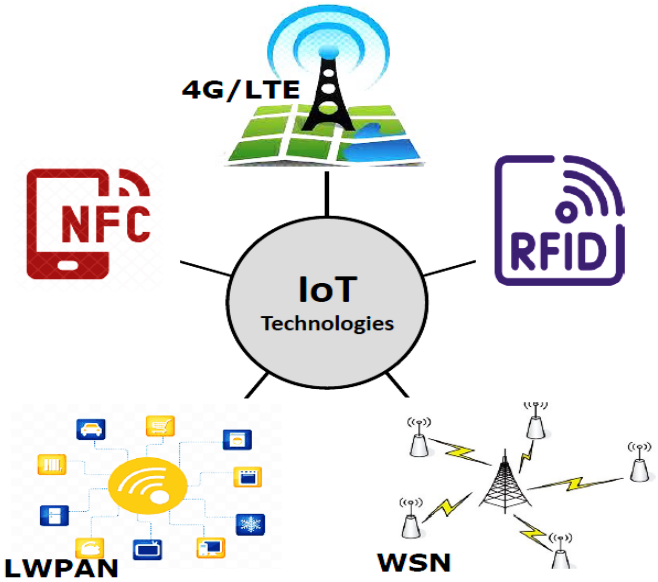

Figure 1. Overview of IoT technologies in smart cities: Illustration of various IoT technologies utilized in enhancing smart city infrastructure and services.

In the RFID technology, tags and readers are used to read data. RFID is used in various IoT applications such as tracking and positioning objects for medical services, car parking, and resource management. In RFID, tags act as sensors. Tags contain manual information and also receive environmental data. NFC is widely used in smartphones for short-distance two-way communication enabling us to share data between various devices. NFC on smartphones can be used as an embedded wallet in some applications of smart cities. In this case, NFC allows us to use smartphones as a bankcard. LWPAN is a wide-range radio technology with a range of 10–15 km. The lower layer protocols of LWPAN include the physical level and the intermediate access level. The upper layer protocols include the ZigBee (Zigbee is a standard for low-power, low-cost wireless mesh networks) and Internet Protocol version 6 (IPv6) over low-power, wireless personal area networks (6LoWPAN) communication protocols. WSN is used in applications such as healthcare and ecosystems. In addition, WSNs can be combined with RFIDs to achieve multiple purposes such as receiving location-identified information. A WSN consists of wireless sensor nodes that communicate with each other in a specific area and read environmental data such as temperature, pressure, vibration, and air pollution. A node in a WSN includes a microcontroller unit, a memory unit, a communication unit, an analog-to-digital converter (ADC) unit, and a power supply unit. The sensors receive analog information from their environments and convert it to digital data using ADC. The data read by the sensors after processing based on application needs are sent to communication infrastructures such as the Internet. 4G and LTE are telecommunications standards in smartphones and data terminals used in wireless networks. These technologies are available worldwide, even in underdeveloped countries. These technologies are designed for applications that require telecommunications, such as wide area networks (WANs). In addition, 4G/5G technologies are used as communication infrastructure to receive information from the sensors to send commands to the actuators for specific purposes.

1.2. Smart city challenges

Although the smart city makes life easier, it faces various challenges. **Figure 2** listed the main challenges in smart cities.

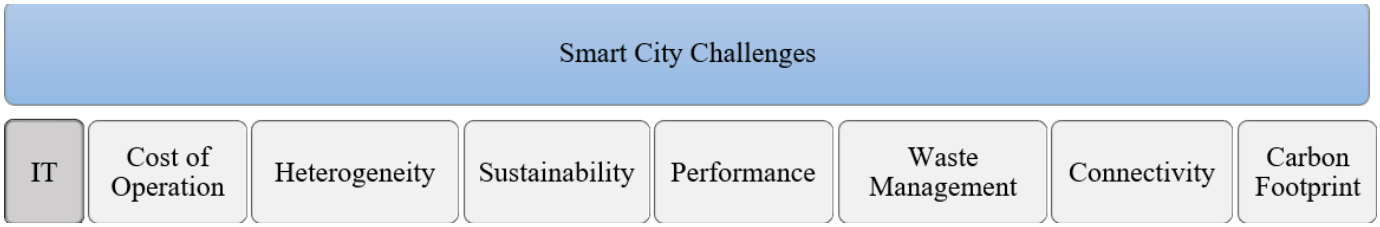

Figure 2. Challenges faced by smart cities: Overview of various challenges that smart cities encounter, including issues related to infrastructure, privacy, security, and governance.

Among the challenges of the smart cities, perhaps the challenge related to IT is the most important. Due to the wide use of IoT in smart cities, the IT-based challenges such as data security, are the most crucial challenges of smart cities. In traditional smart cities, the data collected by IoT infrastructure is stored in the centralized server systems. Central systems are exposed to various challenges including the disclosure of important information due to data hacking, the single point of failure (SPoF), and data loss [12]. In addition, in conventional centralized systems intrusion and data manipulation are possible. Therefore, centralization challenges necessitate a paradigm shift to decentralized data storage and management [13].

1.3. Blockchain-based solutions

The advent of blockchain technology has been primarily aimed at securing digital documents. However, it is tied to the issue of Bitcoin. Bitcoin in the role of an electronic cryptocurrency was introduced as a peer-to-peer (p2p) payment system on the blockchain platform [14]. A blockchain is an immutable distributed ledger system without central control, according to the National Institute of Standards and Technology (NIST) definition [15]. Each node in the blockchain network keeps a copy of the distributed ledger (or database). Blockchain technology uses a p2p network for sharing distributed database. Due to blockchain attributes, it is a perfect solution to overcome the IT challenges in the smart cities. Smart cities design incorporate blockchain technology into urban infrastructure such as health care, cryptocurrency, supply chain, banking, web services, cellular network, reputation, and electricity [16]. Blockchain technology provides a faster, more secure, and better experience for generated data in smart cities. It can be used as an excellent tool to eliminate corruption and inefficiency in the management and execution of smart city operations. Therefore, compared to traditional online services that have normal security, blockchain becomes a preferred option.

In this paper, a comprehensive review of Smart City IoT-Based challenges and Blockchain-based solutions is presented. The rest of the paper is organized as follows: In Section 2, we describe blockchain technology. In Section 3, smart city IoT-based challenges and blockchain-based solutions are discussed and in Section 4, a blockchain-based framework for smart cities is presented. In Section 5, literature

review and related works are presented and finally, in the last Section, we summarize and conclude the article.

In recent years, the rapid growth of urban populations has prompted cities to explore advanced technological solutions to address complex challenges such as traffic congestion, resource distribution, and governance. Smart city initiatives leverage technologies like the Internet of Things (IoT) and blockchain to enhance service delivery, promote efficiency, and facilitate citizen participation. As blockchain technology gains traction, its potential to revolutionize city management and operations is increasingly recognized.

However, a critical review of the existing literature reveals a research gap in holistic frameworks that integrate blockchain with IoT in the context of smart cities. Most existing models primarily focus on specific applications (such as energy distribution, supply chain management, or security protocols) often neglecting the interplay between different urban sectors and the broader implications for governance and public engagement.

This paper proposes a comprehensive blockchain framework tailored for smart cities, aiming to bridge this identified gap. The key contributions of the research include:

1) Holistic Integration: By synthesizing various urban applications, the framework facilitates interoperability between sectors, enhancing overall urban management.
2) Citizen Empowerment: The framework introduces decentralized identity management and engagement platforms, promoting transparency and encouraging citizen participation in governance processes.
3) Adaptability and Scalability: Unlike traditional models, this framework offers flexibility, allowing cities to customize solutions based on their unique challenges and objectives.

By articulating these contributions, this research reinforces the potential of blockchain technology to transform urban governance, emphasizing its role in fostering innovation and public trust within smart cities.

2. Blockchain technology

2.1. Blockchain forming technologies

Blockchain is a system includes four essential technologies include; 1) Distributed ledger, 2) consensus mechanism, 3) encryption algorithm, and 4) smart contract [17]. Blockchain forming technologies and their benefits for the IoT-based applications in smart cities are briefly listed in **Table 2** [18].

Table 2. Blockchain technologies and their benefits for IoT applications: Summary of various blockchain-forming technologies and the advantages they offer for enhancing IoT applications.

Blockchain technologies	Benefits for IoT-based applications
1. Distributed Ledger	Enabling large transactions Support IoT devices A solution for data aggregation
2. Consensus Mechanism	Information management and integration Support IoT applications Enabling agreement between the two parties to the transaction no need to a third party (central authorities)
3. Cryptography Algorithm	Ability to control the central power Ensure transaction integrity Change the direction of finance and business
4. Smart Contracts	Create more independence for IoT devices Ability to remove regulatory overhead Ability to create a high level of cooperation and authority

2.1.1. Distributed ledger

Blockchain is a distributed ledger. A blockchain network includes a set of "blocks" interconnected by a chain. In the blockchain network, blocks contain encrypted transactions (data) [19,20]. Blockchain can provide an efficient platform for data security and decentralized storage, using attributes such as distributed ledger (database), decentralized consensus mechanism [21], smart contracts [22,23], and security [24]. In blockchain, all transactions are stored in a p2p-distributed network without the possibility of manipulation. **Figure 3** shows the block structure in a blockchain. Blockchain attributes are essential features that enhance network reliability. In the following, we will explain how these attributes can help the smart cities to overcome the IT challenges. To better understand the concept of blockchain, we describe the structure of blocks which are the essential elements in a blockchain. Each block contains data (transactions) that should be distributed on the network so that the information is equally available to all nodes (i.e., distributed ledger). In addition, each block includes some information known as a block header. Block header includes the previous block header hash, the block creation date (timestamp), the nonce, and the current block hash data. A "hash" is a code generated by a function, known as the "hash function". As an example, the "SHA256" is a hash function that generates 256-bit hashes. To simplify the display of these codes and shorten the hash length, they are displayed in hexadecimal with a size of 64 characters. The Merkel Tree (MT) is used to store data securely, efficiently, and without tampering. MT allows large-sized data to be securely authenticated. The root that is produced is called the Merkel root (MR). **Figure 3** shows how the MT root is formed. Each transaction is hashed, and then the transactions are hashed in pairs to finally form the MT root. Any change in the data blocks is reflected in Merkel's root. MT is one of the hash-based cryptographies used in blockchain technology. Utilizing the hierarchical nature of MT, only one branch of a block is sufficient to authenticate the relevant transactions [25]. The nonce is an incremental counter that is added to block header information during the generating, creating, and adding of a new block to the blockchain so that the new block can hash the entire block information to obtain the desired hash value for the

current block. The nodes based on a "consensus" protocol must verify each transaction in the blockchain [21]. Blocks and transactions created in the blockchain are immutable. This has a significant security advantage for this technology that can overcome the data security challenge in the smart cities.

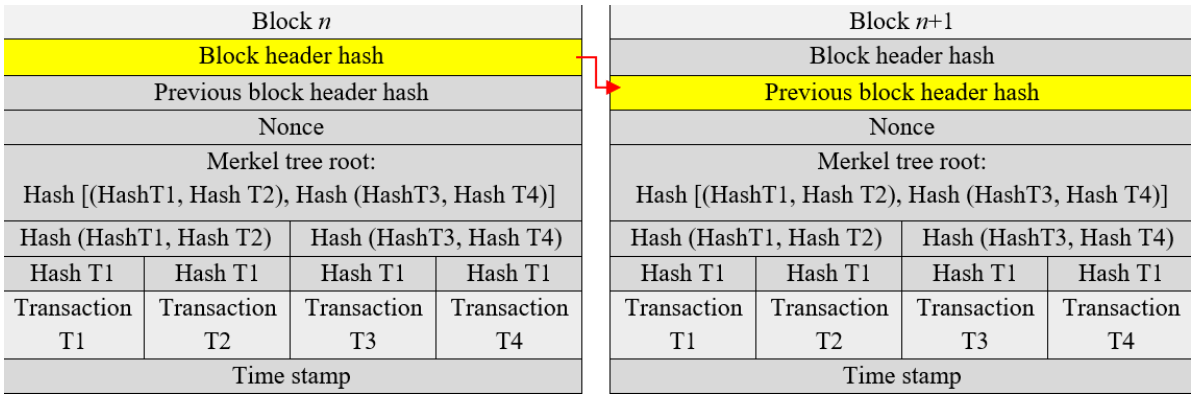

Figure 3. Illustration depicting the components and organization of a block within a blockchain network.

As shown in **Figure 4**, the workflow in the blockchain for joining a block to the blockchain can be summarized in four steps, including 1) creating a block, 2) broadcasting a block, 3) validating a block, and 4) adding a block to the blockchain [26].

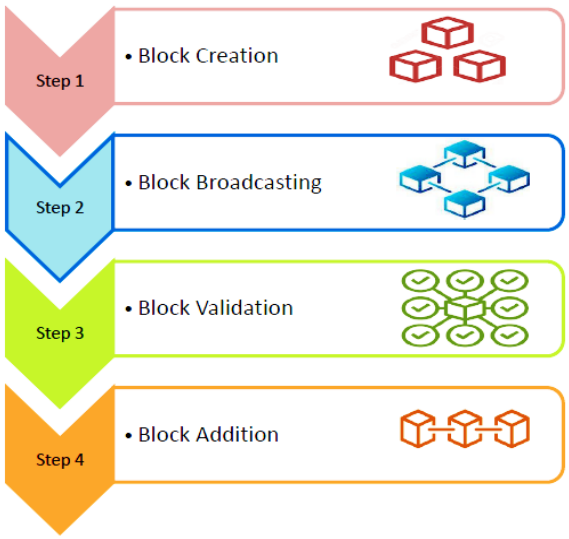

Figure 4. Workflow in a typical blockchain: Diagram illustrating the process flow and interactions within a standard blockchain system.

2.1.2. Consensus mechanism

The consensus mechanism is used to validate blocks. Different consensus algorithms have been presented for various types of blockchains [22,27] . Proof of work (PoW), proof of stack (PoS), proof of authority (PoA), and practical Byzantine fault tolerance (PBFT) are some of the well-known consensus algorithms. Various consensus algorithms have different attributes. PoW has a mechanism in which the verification of the blocks is performed by the "miners". Miners solve complex cryptographic algorithms to validate and add new blocks to the blockchain. Large blockchain networks use the PoW algorithm to validate blocks. The Bitcoin

blockchain uses the PoW algorithm. The authentication time of each block in the Bitcoin blockchain network is about 10 min [28]. In PoS [29], validation of the blocks is performed based on the percentage of "stocks". In PoS, transactions are not authenticated by the "mining". The validation process in PoS is less complex than PoW. Ethereum as a cryptocurrency blockchain, uses PoS as a consensus algorithm [30]. In PoA, private software is run on the network to confirm and add a new block to the blockchain. In PBFT [31], if some nodes send invalid data to other nodes, the level of trust in the network is decreased and there is no mechanism to correct it. In this consensus algorithm, the goal is to reach an agreement to eliminate the errors caused by sending invalid data through the network.

2.1.3. Encryption algorithm

Blockchain uses a method of cryptography called asymmetric cryptography. Each blockchain user has two keys: A public key, and a private key. In a blockchain network, the public key is used to present a unique address and the private key is used to sign transactions. A user signs a transaction with a private key and broadcasts it to the network. While the nodes in the network receive the signed transaction, they validate it and announce it to the network. All of the network nodes were involved in the transaction validation until they reached a collective agreement on the transaction validation [32]. In each block, transactions have their own transaction identifications (TIDs). It means each TID is an encrypted hash of the information kept in the block. TIDs are hashed in pairs and creating a hash tree as shown in **Figure 3** [33].

2.1.4. Smart contract

The smart contract is defined as a computer program that controls the transfer of currency or assets in a blockchain network. It is the same as a regular contract between two or more parties under certain conditions. The main difference between a traditional contract and a smart contract is that the smart contract unlike the traditional contract is more secure and infallible. In other words, the smart contract states the terms of the contract and executes them alone. The smart contract is a completely unbiased, smart, and completely accurate contract and there is no possibility of human error in it.

3. Smart city IoT-based challenges and blockchain-based solutions

Blockchain is the same as an operating system for a smart city [34]. An important advantage of the blockchain is that a group of organizations is able to agree on a particular activity. In this case there is no need for a third party. The agreement can be recorded, secured, and shared with all of the blockchain users. Blockchain integrates P2P networking and cryptographic techniques to support a shared distributed ledger among a group of users or entities (such as organizations, companies, standalone vehicles, smart devices, etc.). Therefore, all users involved in this agreement agree to its content. All transactions in the network are secure and cannot be changed after joining these transactions (data blocks) to the blockchain. In addition, based on the blockchain attributes, traceable audit trails, measurable components, and access to accurate information about transactions recorded in the chain can be provided. Therefore, it enables accurate validation, tracking, and measurements. Various IoT,

fog, and cloud systems belonging to various organizations in a smart city can use blockchain futures to build an acceptable level of trust between them and maintain the accurate records of transactions. Smart city projects have become very popular, and many cities such as Barcelona, Madrid, Amsterdam, and Manchester have active planning smart city strategies [35]. Smart cities deal with a number of IoT-based challenges. Blockchain is a suitable option to overcome the IoT-based challenges in the smart cities. The smart cities IoT-based challenges and blockchain-based solutions are summarized in **Figure 5**. In this section, first discuss smart cities IoT-based challenges and then present the blockchain-based solutions as shown in **Figure 5**.

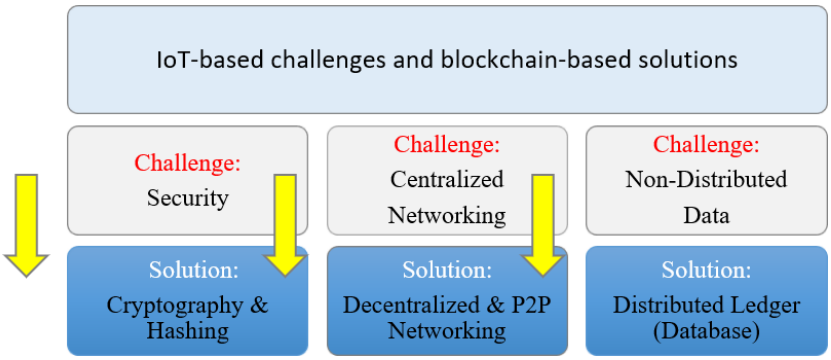

Figure 5. IoT challenges in smart cities and blockchain solutions: Comparison of IoT-based challenges in smart cities and corresponding blockchain-based solutions.

3.1. Smart city IoT-based challenges

3.1.1. Security

To improve urban management and public services, data mining needs to be performed from big data aggregated by the smart city IoT devices. Therefore, data integrity and reliability are of great importance because unauthorized alteration of data can lead to catastrophic results.

3.1.2. Centralized networking

The complexity of applications and the number of IoT devices in smart cities are increasing exponentially. Therefore, IoT networks as the leading information technology produce a large amount of data. In the conventional centralized systems, data set is aggregated on central servers. This increases the risk of loss of data due to the SPoF problem. In addition, nodes, devices, or objects in IoT-based data aggregation networks in the smart city require a degree of flexibility to connect to or go offline at any time according to their needs.

3.1.3. Non-distributed data

Citizens have a serious request for transparency, democracy, and participation in urban affairs. Governments must therefore pass on specific information to citizens such as the decision-making process, environmental data, and government data. Sharing citizens' data, organizational data, and IoT data can improve urban management and decision-making. Conventional systems store data centrally due to their centralized nature. In addition to the risks of data loss, this will not provide the transparency required to review and track data. Conventional non-distributed systems, therefore, cannot pursue transparency, democracy and public participation.

3.2. Blockchain-based solutions

3.2.1. Cryptography and hashing

Data security in the blockchain is supplied using encryption and hashing. In this case, data will be unchangeable and secure. All transactions are secured by digital signatures. Transactions (data) blocks are securely interconnected via a one-way encryption hash function. The input of a hash function is information of any length while the output is a fixed-length string. In the hash function, any minor change in the input represents a severe change in the output hash value. Therefore, the manipulation of the data in each block represents a change in all subsequent blocks of the blockchain. Therefore, data immutability through encryption and hashing is an essential feature in blockchain that can meet the challenge of data security in information technology in smart cities.

3.2.2. Decentralized and p2p networking

Using centralized systems for data aggregation is one of the issues related to the IoT challenge in smart cities. In centralized systems, transactions are validated through a central process. Centrally trusted intermediaries by the central server reduce the performance of the system and incur additional costs. In the blockchain network, there is no need for a centralized system to control network activities.

3.2.3. Distributed ledger (database)

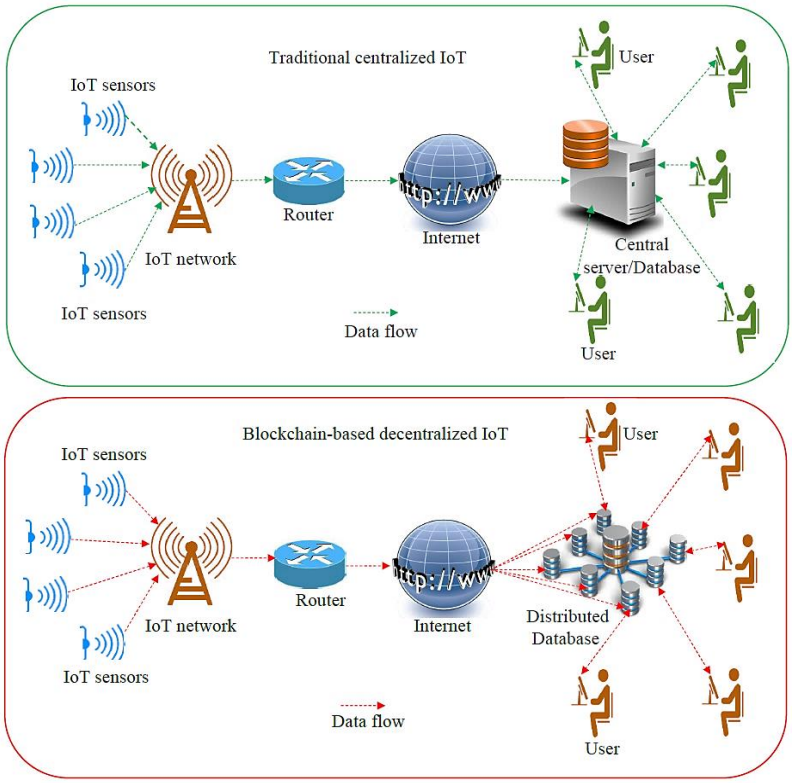

Figure 6. Comparison of centralized and decentralized IoT systems; Visual representation of the differences between centralized and decentralized architectures in IoT systems.

Before attaching a block to the blockchain, all network nodes try to validate the block by implementing consensus algorithms to reach a collective agreement. All nodes in the blockchain contribute to the decision-making process and democratize it. Each node in the blockchain network is assigned an alias address that hides the identity of the nodes. This is especially true for applications that require the identity of users to be private. Because there is no SPoF in the blockchain network due to its distributed and p2p structure, network security has increased. In addition, due to the availability of distributed records of transactions (ledger or database) to all of the nodes, transparency is kept in the blockchain system. **Figure 6** shows a comparison between a centralized system with a central database, and a blockchain-based system with a decentralized structure and distributed ledger (database) from a data flow point of view.

4. Blockchain-based framework for smart cities

Figure 7 shows a general view of a blockchain-based smart city. Various data are collected from different IoT devices and sent to the IoT servers in a blockchain network. In this case, the IoT servers act as nodes in a blockchain network. The data aggregated on the IoT servers in a distributed blockchain-based network ensures the security of data. The architecture is designed with flexibility to adapt to any application in the smart city.

Although blockchain can be widely used in the smart city services, the essential issue in this regard is the compatibility of these applications with the model provided for various services in the smart city. Therefore, having simple design architecture can be suitable for most fields of applications and services of smart cities with minimal changes. This leads us to develop a modular architecture based on blockchain technology. Modular architecture has the advantage of achieving any services from smart cities. It can be achieved by making changes in some modules and leaving the rest of the architecture intact. Therefore, it is necessary to define a specific framework for blockchain-based smart city services. In blockchain-based modular framework design, each specific application module can deal with specific application functions such as application-related dashboards, application-related data processes, implementation of algorithms, and processing of relevant user actions. The blockchain-based framework with a modular architecture is shown in **Figure 8**. The framework consists of four layers: 1) data aggregation and networking, 2) consensus, 3) data storage, and 4) application layer.

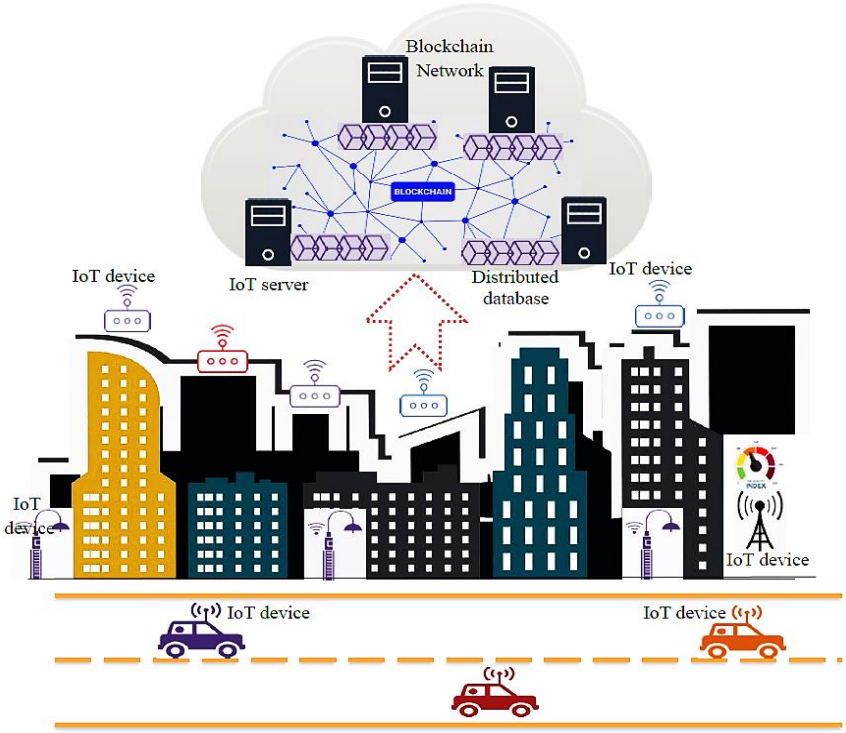

Figure 7. A blockchain-based smart city: Illustration of a smart city framework powered by blockchain technology, showcasing its interconnected systems and applications.

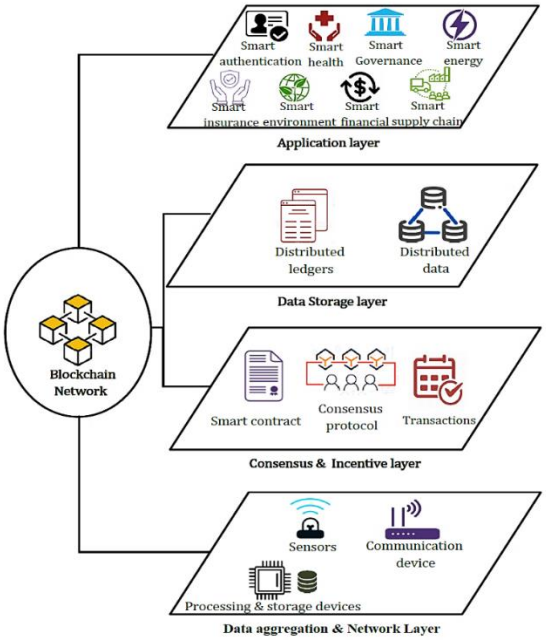

Figure 8. Typical blockchain-based framework for smart cities; schematic representation of a blockchain framework designed to support various smart city applications and services.

4.1. Data aggregation and network layer

The information read by the sensor or other data-receiving equipment that receives the required data from different environments and locations is aggregated and

processed in this layer. It should be noted that this framework could execute and process thousands of data transactions securely in local area networks (LANs) and wide area networks (WANs). Therefore, to use the full processing capability of this framework, powerful IT infrastructures such as high-speed servers and clients and gigabit speed are needed. This framework can be easily deployed on the IT infrastructure in any smart city.

4.2. Consensus and incentive layer

The consensus and incentive layer is responsible for managing the application data. In this layer, rules are set so that data changes can be made in accordance with agreed rules and regulations, known as consensus. This layer parses the traded data of the user, encrypts the data and packages it, and organizes the data to generate the transaction block. In general, this layer coordinates user actions between the application layer and the blockchain network.

4.3. Data storage layer

This layer is a key element for securing network data. In this layer, encrypted transactions are stored securely. Users can view transactions. Data based on cryptographic and hash features in the Chinese block is safe from tampering and their compatibility with the original data is guaranteed. Because the data is stored as a distributed general ledger, it needs to be synchronized at regular intervals while updating the block record.

4.4. Application layer

This layer separates the various activities based on the required services and is responsible for the infrastructure implementation technologies for connecting each layer. This layer can be adjusted to meet the service level needs of most application services provided by smart cities. The services of this platform can be hosted locally with an internal server or any cloud platform, and the user can connect to the service through a client-specific application or through a secure web browser via hypertext transfer protocol secure (HTTPS). This layer ensures that only authenticated users are allowed to access the application. User authentication can be done through various methods such as biometric fingerprint sensors, retina scans, and one-time passwords so that the user can connect to the application through the web.

Figure 9 shows the workflow of a typical blockchain-based platform in the IoT network [36]. Both technical infrastructure and user service framework are considered in this platform. In the platform, the distributed ledger and smart contract are provided to applications as services by the blockchain network. The application client has an intuitive interface for submitting transaction proposals to the blockchain network. The user can use this interface for services such as user registration, device registration and task generation services provided by the blockchain network. After registration and before a transaction can be sent on the network, a certificate must be provided to a particular participant that contains the private keys to sign the transaction. A transaction can be defined as a process of reading or writing data from the blockchain ledger. In this platform, the device owner can send a transaction through the IoT server

to register a new device or create a new task. Then the request sent to the server is transferred to the blockchain network. In addition, the IoT server can transfer the task request from the client to the device. In this case, the collected measurement data or status changes are sent from the device in real time. Transactions of a physical device associated with a specific owner can be sent directly to the blockchain network. The measurement data is then added to the blockchain ledger and transactions are sent directly to the blockchain network. With the help of the smart contract, according to the network rules, the platform can generate a notification to warn the device owner if necessary. This platform is an example of typical blockchain-based IoT platforms that can be used for smart city applications. **Table 3** shows a summary of workflow operations on this platform based on the process shown in **Figure 9**.

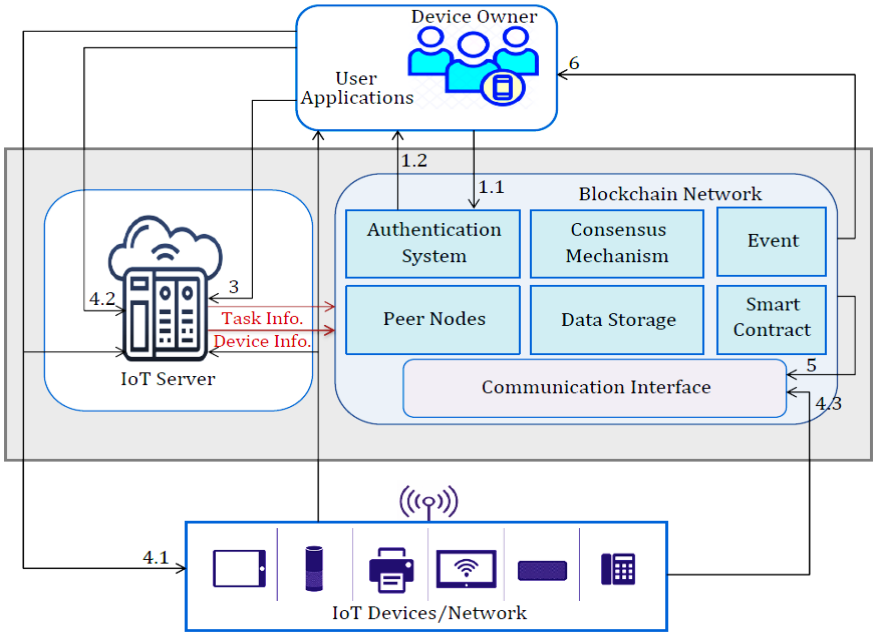

Figure 9. System workflow of a typical IoT-based blockchain: Flowchart illustrating the operational processes and interactions within a typical IoT-based blockchain system.

Table 3. Description of platform workflow shown in **Figure 9**: Detailed explanation of each step and component in the system workflow of the typical IoT-based blockchain depicted in **Figure 9**.

1.1	Enrollment
1.2	Certification
2	Device Registration
3	Generation Task
4.1	Task
4.2	Task Execution Result
4.3	Submit Sensing Data/Device Status
5	Store Sensing Data/Update Device Status
6	Event Notification

5. Review literature

5.1. Research methodology

This investigation employed the PRISMA framework to shape the literature review process, adopting a systematic and clear-cut method to pinpoint and assess pertinent sources. The PRISMA approach was selected due to its organized methodology, which facilitates an in-depth examination of the extensive research surrounding IoT and blockchain. Although alternative methods were contemplated, PRISMA's thoroughness in overseeing the screening and categorization of intricate literature makes it especially appropriate for exploring this field.

5.2. Data retrieval and source identification methodology

The methodology for researching the security of IoT devices through blockchain integration is structured to guarantee a comprehensive and robust analysis. The PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework was utilized as the foundation for our strategy. Recognized as the benchmark for systematic reviews, PRISMA offers a systematic and transparent framework for identifying, assessing, and synthesizing relevant research [37]. The search commenced with a meticulous process across various academic databases, such as Science Direct, Google Scholar, IEEE, and ACM. This extensive search approach enabled us to gather a wide array of scholarly articles focused on IoT security and blockchain integration, while avoiding time limitations to ensure the inclusion of pertinent literature.

5.3. Inclusion and exclusion criteria

The selection of keywords is vital to the search strategy. We thoughtfully curated a list of keywords, including "IoT security," "blockchain integration," "cybersecurity," "smart devices," and "distributed ledger technology." These terms were chosen to encapsulate the primary themes and ideas relevant to our research. Titles that emerged during the search were evaluated against the criteria outlined in the PRISMA checklist. Duplicate entries were eliminated using EndNote 21.1 reference management software. Articles passing the initial screening were further examined based on their titles and abstracts. The study was meticulously structured and executed in accordance with the systematic review and scoping guidelines, following the PCC (population, context, and concept) framework. This framework aids in systematically formulating research questions and identifying relevant components, ensuring a thorough analysis.

In applying the search strategy, the titles and abstracts of the retrieved articles were carefully evaluated against the predefined PRISMA criteria. Duplicate articles were identified and removed to streamline the screening process. During the full-text review, each article was evaluated for relevance, duplication, and accessibility. Only English-language articles that fulfilled the inclusion criteria were selected for further analysis. Journal statistics were reviewed to understand the distribution of relevant literature across various publications, providing valuable context for the findings.

Alongside the systematic review, a detailed analysis of existing literature was conducted to pinpoint relevant studies on IoT security, blockchain integration, and related domains. This dual approach offers a comprehensive evaluation of blockchain technology's role in securing IoT devices. Exclusion criteria were applied to maintain the focus and integrity of the analysis. Articles with duplicate information, irrelevant content, or those not directly associated with IoT security and blockchain integration were excluded from the review. Additionally, sources such as case series, reports, brief communications, and editorials were omitted from the final selection to uphold the scientific rigor of the research. This methodical approach aimed to achieve a clear understanding of how blockchain technology can secure IoT devices. By adhering to established methodologies and guidelines, the objective was to generate precise, trustworthy, and actionable research outcomes. The literature screening followed PRISMA guidelines, ensuring a structured method for source selection and analysis, with criteria including relevance to IoT security and integration, publication dates, and resource constraints in IoT environments. The discussion connects these insights to practical IoT applications, emphasizing the pivotal role of blockchain in enhancing data security and privacy across sectors like healthcare, supply chains, and smart cities.

5.4. Related works

A multitude of studies have explored the applications of blockchain technology within the Internet of Things (IoT) and smart cities. This section provides an overview of some significant contributions to the field.

In their 2018 study, Khan and Salah delved into IoT network protocols and identified critical security issues facing IoT systems. Their work classified these concerns and examined various blockchain-based solutions, highlighting how blockchain can enhance security by providing decentralized and tamper-resistant data management.

Eckhoff and Wagner [38] emphasized the critical role of privacy in the context of smart cities. They discussed the various applications of privacy-enhancing technologies, detailing the challenges that arise and presenting advanced solutions necessary for developing secure smart city infrastructures. Their findings underscore the importance of safeguarding personal data against potential misuse.

In [39], the authors focused on the potential advantages and integration strategies of blockchain technology with IoT systems. They investigated a range of IoT applications, outlining challenges such as scalability and interoperability, and examined several blockchain platforms that could support these integrations. Their work suggests ways to leverage blockchain capabilities to improve the reliability and efficiency of IoT services.

Cui et al. [40] tackled issues of security and privacy specifically within smart cities, assessing these challenges from a cybersecurity perspective. They discussed various protective measures, drawing from technologies such as cryptography, biometrics, and blockchain, to enhance the overall security landscape in urban environments.

Researchers Fernandez-Caramés and Fraga-Lamas [41] introduced a blockchain specifically optimized for IoT applications within smart cities, termed Blockchain-

based IoT (BIoT). This study explored how a dedicated blockchain solution could address the unique requirements of IoT ecosystems while ensuring compatibility with existing smart city infrastructures.

In [30], the authors engaged with several technical challenges related to blockchain, including issues of forking, cryptographic protocols, networking difficulties, layered architecture, consensus mechanisms, and overall security within a blockchain network. Their examination provides a comprehensive understanding of the complexities involved in implementing blockchain technology.

The study by Sookhak et al. [42] discussed the foundational structures supporting smart cities, which they refer to as the four infrastructure pillars: social, economic, institutional, and physical. In their analysis, they addressed privacy and security challenges and proposed solutions, aiming to create a holistic framework for the development of smart urban environments.

Wang et al. [12] conducted a thorough analysis of the smart contracts mechanism present in popular blockchain platforms. They developed a six-tier framework that outlines the lifecycle of smart contracts, discussing challenges, strategic plans, and future development trends that could shape the use of smart contracts in IoT applications. In their follow-up work, Wang et al. [43] investigated the security vulnerabilities associated with smart contracts and proposed related solutions, further solidifying the understanding of risks involved in deploying such technologies.

Alladi et al. [44] examined various blockchain applications specifically in the context of the Industrial IoT (IIoT). Their research not only highlighted the potential benefits but also addressed the challenges and unresolved issues that remain in the field, creating a pathway for future exploration.

Xie et al. [45] explored the application of blockchain across multiple smart areas within smart cities, discussing associated challenges. Their work sheds light on the diverse potential of blockchain to facilitate innovation in urban services while acknowledging the hurdles to full implementation. In the study conducted by Ali et al. [46], researchers comprehensively analyzed challenges related to privacy, untrustworthy architectures, security concerns, identity management, and data management within decentralized, blockchain-based IoT environments. They offered insights and orientations to address these complex challenges, setting the stage for further advancements in decentralized IoT.

Ferrag et al. [33] studied different blockchain protocols applicable to IoT and presented various threat models specifically designed for blockchain-based IoT systems. Their work contributed invaluable knowledge to understanding how to protect IoT systems integrating blockchain. In [47], the authors provided a detailed exposition of security requirements for both IoT and IIoT systems, arguing that blockchain could play a pivotal role in enhancing security measures within these environments, thus facilitating broader acceptance and implementation.

Chen et al. [48] examined blockchain's role as a trusted technology, analyzing its capacity as a secure platform, access control mechanism, and automated payment facilitator in IoT ecosystems. They emphasized how blockchain can transform IoT applications by providing a secure and reliable environment for data exchange. Dadin et al. [49] investigated the applications of blockchain within various sectors, including e-health, smart cities, smart transportation, and smart industries. They provided

insights into how blockchain can enhance IoT, cloud IoT, and fog IoT infrastructures, illustrating its transformative potential in these domains.

Uzbek et al. [50] focused on the intersection of IoT and blockchain in healthcare, addressing specific challenges and solutions related to blockchain-based IoT deployments within the health sector. They highlighted critical issues, such as the constraints of IoT devices concerning computational and storage capacities compared to the high-resource requirements of blockchain technology.

Saxena et al. [51] offered an in-depth discussion on the security improvements that blockchain can bring to IoT systems. They also addressed the challenges that emerge from integrating these technologies, emphasizing the need for a balanced approach to harnessing the benefits while managing the complexities. In [52], the authors evaluated essential considerations and concepts surrounding blockchain technology. They provided a detailed assessment of potential security threats and the solutions that could mitigate such risks, contributing to a better understanding of the security landscape in blockchain applications.

Additionally, numerous surveys have been conducted relating to the applications of IoT and smart cities, covering areas such as healthcare, transportation, agriculture, smart grids, smart homes, and supply chains. The most relevant surveys to the topic of this paper are summarized in **Table 4**.

Table 4. Summary of surveys and reviews on blockchain applications in IoT-based smart cities: Overview of key findings and insights from various surveys and reviews discussing the role of blockchain technology in enhancing IoT applications within smart cities.

Ref.	Year	Scope	Description
[53]	2017	Smart grid	Review of blockchain- based microgrid systems.
[54]	2018	Smart grid	Review of p2p electricity energy trading markets.
[55]	2018	Smart home	Discussion about blockchain-based IoT integration, analysis of the utility of blockchain-based methods and technologies in IoT system.
[56]	2019	Smart city	Review of security and privacy issues of blockchain in smart cities applications.
[57]	2019	Smart city	Review of blockchain applications in smart cities such as IoT, supply chain, healthcare, business, education, data management, and privacy.
[58]	2019	Smart city	Review of the main blockchain-based applications.
[59]	2019	Smart city	Review of blockchain architecture concepts and its applications in IoT , healthcare, and business.
[60]	2019	Smart city	Review of the blockchain-based applications in smart cities.
[61]	2019	healthcare	Review of the blockchain-based solutions for the healthcare challenges and limitations.
[62]	2019	healthcare	Review of the blockchain-based healthcare applications and categorised them to data management, supply chain management, and internet of medical things (IoMT).
[63]	2019	healthcare	A review about the application of blockchain in healthcare and categorised the study to the problems, solutions, and security.
[64]	2019	healthcare	A classified reviewed to six use cases including electronic record of health-related (EMR) information management, pharmaceutical supply chain, biomedical research, remote patient monitoring, health insurance, and health data analytics.
[65]	2019	Transportation	Review of the lightweight security for blockchain–based vehicular ad hoc network (VANET).
[66]	2019	Supply chain	Review of the blockchain-based applications and discussion about using smart contracts in the supply chain management (SCM).
[67]	2019	Supply chain	Discussion about the complexity of the international trading process, electronic trading, validation, and SCM.
[68]	2019	Supply chain	Discussion about application of blockchain in SCM and its future challenges.

Table 4. (*Continued*).

Ref.	Year	Scope	Description
[69]	2019	Smart grid	Reviews of the blockchain-based application in the energy projects and startups.
[70]	2019	Smart grid	Review of the blockchain-based point-to-point microgrid networks.
[71]	2020	Smart city	Review of the distributed ledgers and blockchain for some special applications of smart cities.
[72]	2020	healthcare	Review of the blockchain-based IoT for healthcare.
[73]	2020	healthcare	Review of the blockchain technology, start-up involved in blockchain-based healthcare solutions and review the potential research directions.
[74]	2020	healthcare	Review of the requirements of healthcare systems, blockchain attributes, applications and constraints.
[75]	2020	healthcare	Review of the requirements of the healthcare systems, review of the blockchain, and research directions.
[76]	2020	Transportation	Review on the blockchain applications in IoV among the three blockchain layers: application, perception, and networking.
[77]	2020	smart agriculture	Review of the IoT-based blockchain for agriculture, opportunities in food safety, supply chain, and discussion about various patterns IoT-based agriculture.
[78]	2020	smart agriculture	Review of the blockchain-based applications in agricultural insurance, smart agriculture, food supply chains, and agricultural e-commerce.
[79]	2020	smart agriculture	Review of the blockchain technology, applications classification, blockchain-based platforms, and compare them, reviews blockchain-based agricultural methods, and investigate their challenges.
[80]	2020	smart agriculture	Review of the security classification, access control, privacy solutions and consensus mechanisms in smart agriculture.
[81]	2020	Supply chain	Review of the blockchain-based solutions according to the type of the blockchain, categorized solutions based on the agriculture sector and products, investigate commercial solutions and discussion on future blockchain challenges.
[82]	2020	Supply chain	Review of supply chain studies and classified them based on the type of their approaches, discusses adoption barriers, challenges and utilities for manufacturers.
[83]	2020	Supply chain	Review of the blockchain-based supply chain studies from 2016 to January 2020 and classified them into theoretical sense making, conceptualizing and testing blockchain applications, digital supply chain management (SCM), the design of blockchain applications, and framing blockchain in supply chains.
[84]	2020	Smart grid	Survey on the blockchain-based application in smart grid.
[85]	2020	Smart grid	Survey of blockchain-based approaches for energy sectors such as decentralized storage and control in a power grid, P2P marketing in smart grid, and electrical vehicle.
[86]	2020	Smart grid	Survey of the blockchain-based cybersecurity architectures and techniques in the smart grid.
[87]	2020	Smart home	Discussion about blockchain-based smart home, investigation of two blockchain-based case studies, smart home energy marketing in smart grids, and smart home data sharing. Investigate main challenges such as security and privacy, data collection and sharing, data analytics, and latency in smart home blockchain-based application.
[88]	2020	Smart home	Review of the blockchain-based IoT solutions in power systems, especially in the distribution level, residential section, smart buildings, smart homes, and energy hubs schemes.
[89]	2020	Smart home	Review of the security and privacy challenges in IoT layers and discussion about blockchain-based IoT framework.
[90]	2021	Transportation	Analyzing the blockchain-based Internet of vehicles (IoV) for security, trust, privacy, architecture, certificate management, data management, and data monetization.
[91]	2021	Transportation	Discussion about blockchain-based intelligent transportation system (ITS) for security, privacy, and trust requirements.
[92]	2022	Smart home	Discussion about blockchain-based Industry 4.0 applications, security and privacy requirements, attacks on blockchain networks, and investigation of the industrial blockchain-based applications .

6. Conclusion

Rapid population growth along with the rapid trend of urbanization has endangered the environmental and economic sustainability of cities. To address these

concerns, the concept of the "smart city" has been proposed. In the smart city, IoT is used in a smart way to create a sustainable urban environment and improve the QoL. However, smart cities face some IoT-based challenges such as SPoF, data security, and lack of transparency. Blockchain technology due to its features such as cryptography and distributed ledger/database, can address IoT-based challenges in smart cities. In this paper, we present a comprehensive review of the blockchain-based solutions for overcoming the IoT-based challenges in the smart cities.

Conflict of interest: The authors declare no conflict of interest.

References

1. United Nations. Department of Economic and Social Affairs 2018. [Online] Available online: https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html (acessed on 10 December 2024).
2. Bibri SE, Krogstie J. Smart sustainable cities of the future: An extensive interdisciplinary literature review. Sustainable Cities and Society. 2017; 31: 183-212. doi: 10.1016/j.scs.2017.02.016
3. Datta A. New urban utopias of postcolonial India. Dialogues in Human Geography. 2015; 5(1): 3-22. doi: 10.1177/2043820614565748
4. Collotta M, Pau G. An Innovative Approach for Forecasting of Energy Requirements to Improve a Smart Home Management System Based on BLE. IEEE Transactions on Green Communications and Networking. 2017; 1(1): 112-120. doi: 10.1109/tgcn.2017.2671407
5. Vora J, Nayyar A, Tanwar S, et al. BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. 2018 IEEE Globecom Workshops (GC Wkshps). Published online December 2018. doi: 10.1109/glocomw.2018.8644088
6. Alotaibi SS. Registration Center Based User Authentication Scheme for Smart E-Governance Applications in Smart Cities. IEEE Access. 2019; 7: 5819-5833. doi: 10.1109/access.2018.2884541
7. Mohammad N. A Multi-Tiered Defense Model for the Security Analysis of Critical Facilities in Smart Cities. IEEE Access. 2019; 7: 152585-152598. doi: 10.1109/access.2019.2947638
8. Nayak J, Vakula K, Dinesh P, et al. Intelligent Computing in IoT-Enabled Smart Cities: A Systematic Review. Green Technology for Smart City and Society. 2021; pp. 1–21.
9. Silva BN, Khan M, Han K. Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. Sustainable Cities and Society. 2018; 38: 697-713. doi: 10.1016/j.scs.2018.01.053
10. Harrison C, Eckman B, Hamilton R, et al. Foundations for Smarter Cities. IBM Journal of Research and Development. 2010; 54(4): 1-16. doi: 10.1147/jrd.2010.2048257
11. Pathak S, Pandey M. Smart cities: Review of characteristics, composition, challenges and technologies. In: Proceedings of the Sixth International Conference on Inventive Computation Technologies; 2021.
12. Wang S, Ouyang L, Yuan Y, et al. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2019; 49(11): 2266-2277. doi: 10.1109/tsmc.2019.2895123
13. Novo O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. IEEE Internet of Things Journal. 2018; 5(2): 1184-1195. doi: 10.1109/jiot.2018.2812239
14. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. SSRN; 2008.
15. Pilkington M. Blockchain technology: principles and applications. Research Handbook on Digital Transformations. Published online September 30, 2016. doi: 10.4337/9781784717766.00019
16. Alnahari MS, Ariaratnam ST. The Application of Blockchain Technology to Smart City Infrastructure. Smart Cities. 2022; 5(3): 979-993. doi: 10.3390/smartcities5030049
17. Sikorski JJ, Haughton J, Kraft M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. Applied Energy. 2017; 195: 234-246. doi: 10.1016/j.apenergy.2017.03.039
18. Abdelmaboud A, Ahmed AIA, Abaker M, et al. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. Electronics. 2022; 11(4): 630. doi: 10.3390/electronics11040630
19. Wattenhofer R. The science of the blockchain, 1 st ed. Inverted Forest Publishing; 2016.

20. Wu J, Tran NK. Application of Blockchain Technology in Sustainable Energy Systems: An Overview. Sustainability. 2018; 10(9): 3067. doi: 10.3390/su10093067
21. Danzi P, Angjelichinoski M, Stefanovic C, et al. Distributed proportional-fairness control in microgrids via blockchain smart contracts. Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm); 2017. doi: 10.1109/smartgridcomm.2017.8340713
22. Mengelkamp E, Gärttner J, Rock K, et al. Designing microgrid energy markets. Applied Energy. 2018; 210: 870-880. doi: 10.1016/j.apenergy.2017.06.054.
23. Yuan Y, Wang FY. Towards blockchain-based intelligent transportation systems. In: 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC). 2016; 2663-2668. doi: 10.1109/itsc.2016.7795984
24. BitInfoCharts. Bitcoin, Ethereum Block Time historical chart. Avilable online: https://bitinfocharts.com/comparison/confirmationtime-btc-eth.html#3m (accessed on 10 November 2024).
25. Majeed U, Khan LU, Yaqoob I, et al. Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. Journal of Network and Computer Applications. 2021; 181: 103007. doi: 10.1016/j.jnca.2021.103007.
26. Banerjee M, Lee J, Choo KKR. A blockchain future for internet of things security: a position paper. Digital Communications and Networks. 2018; 4(3): 149-160. doi: 10.1016/j.dcan.2017.10.006.
27. GitHub. Proof of Stake FAQ. Avilable online: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ (accessed on 10 November 2024).
28. Buterin V. Ethereum scalability research and development subsidy programs. Availbale online: https://blog.ethereum.org/2018/01/02/ethereum-scalability-research-development-subsidy-programs (accessed on 10 November 2024).
29. Castro M, Liskov B. Practical Byzantine Fault Tolerance. In: Proceedings of the Third Symposium on Operating Systems Design and Implementation; 1999.
30. Wu M, Wang K, Cai X, et al. A Comprehensive Survey of Blockchain: From Theory to IoT Applications and Beyond. IEEE Internet of Things Journal. 2019; 6(5): 8114-8154. doi: 10.1109/jiot.2019.2922538
31. Yaga D, Mell P, Roby N, et al. Blockchain Technology Overview. National Institute of Standards and Technology; 2018. doi: 10.6028/nist.ir.8202.
32. Ali A, Rahouti M, Latif S, et al.Blockchain and the future of the internet: A comprehensive review. arXiv preprint; 2019.
33. Ferrag MA, Derdour M, Mukherjee M, et al. Blockchain Technologies for the Internet of Things: Research Issues and Challenges. IEEE Internet of Things Journal. 2019; 6(2): 2188-2204. doi: 10.1109/jiot.2018.2882794
34. Bagloee SA, Heshmati M, Dia H, et al. Blockchain: The operating system of smart cities. Cities. 2021; 112: 103104. doi: 10.1016/j.cities.2021.103104
35. Bhushan B, Khamparia A, Sagayam KM, et al. Blockchain for smart cities: A review of architectures, integration trends and future research directions. Sustainable Cities and Society. 2020; 61: 102360. doi: 10.1016/j.scs.2020.102360
36. Hang L, Kim DH. Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. Sensors. 2019; 19(10): 2228. doi: 10.3390/s19102228
37. aylor PJ, Dargahi T, Dehghantanha A, et al. A systematic literature review of blockchain cyber security. Digital Communications and Networks. 2020; 6(2): 147-156. doi: 10.1016/j.dcan.2019.01.005
38. Wagner I, Eckhoff D. Technical Privacy Metrics. ACM Computing Surveys. 2018; 51(3): 1-38. doi: 10.1145/3168389
39. Reyna A, Martín C, Chen J, et al. On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems. 2018; 88: 173-190. doi: 10.1016/j.future.2018.05.046
40. Cui L, Xie G, Qu Y, et al. Security and Privacy in Smart Cities: Challenges and Opportunities. IEEE Access. 2018; 6: 46134-46145. doi: 10.1109/access.2018.2853985
41. Ferrag MA, Maglaras L, Janicke H. Blockchain and its role in the internet of things. In: Strategic innovative marketing and tourism. Springer, Cham; 2019.
42. Sookhak M, Tang H, He Y, et al. Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges. IEEE Communications Surveys & Tutorials. 2019; 21(2): 1718-1743. doi: 10.1109/comst.2018.2867288
43. Wang T, Zheng Z, Rehmani MH, et al. Privacy Preservation in Big Data From the Communication Perspective—A Survey. IEEE Communications Surveys & Tutorials. 2019; 21(1): 753-778. doi: 10.1109/comst.2018.2865107
44. Alladi T, Chamola V, Parizi RM, et al. Blockchain Applications for Industry 4.0 and Industrial IoT: A Review. IEEE Access. 2019; 7: 176935-176951. doi: 10.1109/access.2019.2956748

45. Xie J, Tang H, Huang T, et al. A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. IEEE Communications Surveys & Tutorials. 2019; 21(3): 2794-2830. doi: 10.1109/comst.2019.2899617
46. Ali MS, Vecchio M, Pincheira M, et al. Applications of Blockchains in the Internet of Things: A Comprehensive Survey. IEEE Communications Surveys & Tutorials. 2019; 21(2): 1676-1717. doi: 10.1109/comst.2018.2886932
47. Wang Q, Zhu X, Ni Y, et al. Blockchain for the IoT and industrial IoT: A review. Internet of Things. 2020; 10: 100081. doi: 10.1016/j.iot.2019.100081
48. Chen F, Xiao Z, Cui L, et al. Blockchain for Internet of things applications: A review and open issues. Journal of Network and Computer Applications. 2020; 172: 102839. doi: 10.1016/j.jnca.2020.102839
49. Uddin MA, Stranieri A, Gondal I, et al. A survey on the adoption of blockchain in IoT: challenges and solutions. Blockchain: Research and Applications. 2021; 2(2): 100006. doi: 10.1016/j.bcra.2021.100006
50. Azbeg K, Ouchetto O, Andaloussi SJ, et al. A Taxonomic Review of the Use of IoT and Blockchain in Healthcare Applications. IRBM. 2022; 43(5): 511-519. doi: 10.1016/j.irbm.2021.05.003
51. Saxena S, Bhushan B, Ahad MA. Blockchain based solutions to secure IoT: Background, integration trends and a way forward. Journal of Network and Computer Applications. 2021; 181: 103050. doi: 10.1016/j.jnca.2021.103050
52. Singh S, Hosen ASMS, Yoon B. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. IEEE Access. 2021; 9: 13938-13959. doi: 10.1109/access.2021.3051602
53. Goranovic A, Meisel M, Fotiadis L, et al. Blockchain applications in microgrids an overview of current projects and concepts. Proceedings of the IECON 2017—43rd Annual Conference of the IEEE Industrial Electronics Society; 2017. doi: 10.1109/iecon.2017.8217069
54. Abdella J, Shuaib K. Peer to Peer Distributed Energy Trading in Smart Grids: A Survey. Energies. 2018; 11(6): 1560. doi: 10.3390/en11061560
55. Panarello A, Tapas N, Merlino G, et al. Blockchain and IoT Integration: A Systematic Survey. Sensors. 2018; 18(8): 2575. doi: 10.3390/s18082575
56. Mohanta BK, Jena D, Panda SS, et al. Blockchain technology: A survey on applications and security privacy Challenges. Internet of Things. 2019; 8: 100107. doi: 10.1016/j.iot.2019.100107
57. Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics. 2019; 36: 55-81. doi: 10.1016/j.tele.2018.11.006
58. Lu Y. The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration. 2019; 15: 80-90. doi: 10.1016/j.jii.2019.04.002
59. Syed TA, Alzahrani A, Jan S, et al. A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations. IEEE Access. 2019; 7: 176838-176869. doi: 10.1109/access.2019.2957660
60. Aggarwal S, Chaudhary R, Aujla GS, et al. Blockchain for smart communities: Applications, challenges and opportunities. Journal of Network and Computer Applications. 2019; 144: 13-48. doi: 10.1016/j.jnca.2019.06.018
61. McGhin T, Choo KKR, Liu CZ, et al. Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications. 2019; 135: 62-75. doi: 10.1016/j.jnca.2019.02.027
62. Khezr S, Moniruzzaman M, Yassine A, et al. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. Applied Sciences. 2019; 9(9): 1736. doi: 10.3390/app9091736
63. Hussien HM, Yasin SM, Udzir SNI, et al. A Systematic Review for Enabling of Develop a Blockchain Technology in Healthcare Application: Taxonomy, Substantially Analysis, Motivations, Challenges, Recommendations and Future Direction. Journal of Medical Systems. 2019; 43(10). doi: 10.1007/s10916-019-1445-8
64. Agbo CC, Mahmoud QH, Eklund JM. Blockchain Technology in Healthcare: A Systematic Review. Healthcare. 2019; 7(2): 56. doi: 10.3390/healthcare7020056
65. Sharma S, Kaushik B. A survey on internet of vehicles: Applications, security issues & solutions. Vehicular Communications. 2019; 20: 100182. doi: 10.1016/j.vehcom.2019.100182
66. Amulya G, Jestin J. Potential of blockchain technology in supply chain management: a literature review. International Journal of Physical Distribution & Logistics Management. 2019; 49(9): 881-900. doi: 10.1108/ijpdlm-11-2018-0371
67. Husam J, Khaled S, Ibrahim K. A Survey on Using Blockchain in Trade Supply Chain Solutions. IEEE Access; 2019.
68. Wang Y, Singgih M, Wang J, et al. Making sense of blockchain technology: How will it transform supply chains? International Journal of Production Economics. 2019; 211: 221-236. doi: 10.1016/j.ijpe.2019.02.002 2019

69. Andoni M, Robu V, Flynn D, et al. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews. 2019; 100: 143-174. doi: 10.1016/j.rser.2018.10.014
70. Ahl A, Yarime M, Tanaka K, et al. Review of blockchain-based distributed energy: Implications for institutional development. Renewable and Sustainable Energy Reviews. 2019; 107: 200-211. doi: 10.1016/j.rser.2019.03.002
71. Maesa F, Mori P. Blockchain 3.0 applications survey. Journal of Parallel and Distributed Computing. 2020; 138: 99-114. doi: 10.1016/j.jpdc.2019.12.019
72. Qadri YA, Nauman A, Zikria YB, et al. The Future of Healthcare Internet of Things: A Survey of Emerging Technologies. IEEE Communications Surveys & Tutorials. 2020; 22(2): 1121-1167. doi: 10.1109/comst.2020.2973314
73. Farouk A, Alahmadi A, Ghose S, et al. Blockchain platform for industrial healthcare: Vision and future opportunities. Computer Communications. 2020; 154: 223-235. doi: 10.1016/j.comcom.2020.02.058
74. Shi S, He D, Li L, et al. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & Security. 2020; 97: 101966. doi: 10.1016/j.cose.2020.101966
75. Chukwu E, Garg L. A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations. IEEE Access. 2020; 8: 21196-21214. doi: 10.1109/access.2020.2969881
76. Peng C, Wu C, Gao L, et al. Blockchain for Vehicular Internet of Things: Recent Advances and Open Issues. Sensors. 2020; 20(18): 5079. doi: 10.3390/s20185079
77. Torky M, Hassanein AE. Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges. Computers and Electronics in Agriculture. 2020; 178: 105476. doi: 10.1016/j.compag.2020.105476
78. Xiong H, Dalhaus T, Wang P, et al. Blockchain Technology for Agriculture: Applications and Rationale. Frontiers in Blockchain. 2020; 3. doi: 10.3389/fbloc.2020.00007
79. Lin W, Huang X, Fang H, et al. Blockchain Technology in Current Agricultural Systems: From Techniques to Applications. IEEE Access. 2020; 8: 143920-143937. doi: 10.1109/access.2020.3014522
80. Amine FM, Shu L, Yang X, et al. Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges. IEEE Access. 2020; 8: 32031-32053. doi: 10.1109/access.2020.2973178
81. Demestichas K. Blockchain in Agriculture Traceability Systems: A Review. Applied Sciences; 2020.
82. Peter G, Katsikouli P, Herskind L, et al. Blockchain Implementations and Use Cases for Supply Chains-A Survey. IEEE Access. 2020; 8: 11856-11871. doi: 10.1109/access.2020.2964880
83. Benjamin M, Heiko G, Evi H. Blockchain Technology in Logistics and Supply Chain Management—A Bibliometric Literature Review From 2016 to January 2020. IEEE Transactions on Engineering Management. 2020; 67(4): 988-1007. doi: 10.1109/tem.2020.2980733
84. Mollah M. B. et al. "Blockchain for future smart grid: A comprehensive survey". In: IEEE Internet of Things Journal (2020).
85. Bao J, et al. A survey of blockchain applications in the energy sector. IEEE Systems Journal. 2020.
86. Zhuang P, Zamir T, Liang H. Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey. IEEE Transactions on Industrial Informatics. 2021; 17(1): 3-19. doi: 10.1109/tii.2020.2998479
87. Moniruzzaman M. Blockchain for smart homes: Review of current trends and research challenges. Computers & Electrical Engineering. 2020; 83.
88. Hosseinian H. Blockchain outlook for deployment of IoT in distribution networks and smart homes. International Journal of Electrical and Computer Engineering.2020. doi: 10.11591/ijece.v10i3.pp2787-2796
89. Alfandi O, Khanji S, Ahmad L, et al. A survey on boosting IoT security and privacy through blockchain. Cluster Computing. 2020; 24(1): 37-55. doi: 10.1007/s10586-020-03137-8
90. Wang C, Cheng X, Li J, et al. A survey: applications of blockchain in the Internet of Vehicles. EURASIP Journal on Wireless Communications and Networking. 2021; 2021(1). doi: 10.1186/s13638-021-01958-8
91. Mikavica B. Kosti'c-Ljubisavljevi'c A. Blockchain-based solutions for security, privacy, and trust management in vehicular networks: a survey. The Journal of Supercomputing. 2021; pp. 1-56.
92. Hameed K, Barika M, Garg S, et al. A taxonomy study on securing Blockchain-based Industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues. Journal of Industrial Information Integration. 2022; 26: 100312. doi: 10.1016/j.jii.2021.100312