Blockchain as a Middleware for Iot Sensing and Authentication Within Smart Cities: A Systematic Literature Review

Nada Alasbali
University of Malaya Faculty of Computer Science and Information Technology
Saaidal Razali Azzuhri (saaidal@um.edu.my)
University of Malaya Faculty of Computer Science and Information Technology
Rosli Salleh
University of Malaya Faculty of Computer Science and Information Technology
Miss Laiha Mat Kiah
University of Malaya Faculty of Computer Science and Information Technology

Research

Keywords: Blockchain, Computer networks experiential solutions, Internet of Things, IoT, Smart cities, Systematic literature review

Posted Date: December 4th, 2020

DOI: https://doi.org/10.21203/rs.3.rs-118074/v1

Abstract

Previous research in Smart City technologies has been narrow and system-specific in both their orientation and focus. Specificity creates the homogeneity of systems architecture that, while beneficial from an experimental position, is entirely incompatible with the broader needs of a system standard. The current review seeks to examine existing research and their outcomes and summarize research milestones in the intersection of three domains of blockchain technologies, IoT capabilities, and smart city solutions. Based on the inclusion criteria, eighteen studies extracted from 6 academic journals contained some form of experimental or model-oriented solution and offered a distinct advantage over other proprietary research in this field. The SLR has divided the central concepts and structural solutions illuminated in the blockchain-IoT-related, smart city research conducted in the past four years into its core components: a structural solution of issues of security and authentication in the IoT, a tangible application of smart contract technologies for decentralized smart negotiation and a means of permissions-based performative oversight and administration. Heterogeneity and proprietary technologies will revise IoT's scope and capabilities and capabilities. However, this intermediary role of the Blockchain has been proven in many experimental and exploratory works and offers a significant advantage over prior structural limitations.

I. Introduction

Blockchain technology has gained popularity in recent years and made a lasting impact on the world. For instance, it has provided a suitable haven for the production of dark web marketplaces, affected the currency markets, and gained commercial importance[1]. Moreover, it also influences the rise in cyber-attacks with financial motivation, including denying services against retailers, online organizations, and ransomware[2]. Indeed, the integration and usage of blockchain way exceed its core objective and, therefore, this technology has become the backbone of the first decentralized cryptocurrency of the world[3]. Blockchain technology typically comprises a network of computer nodes, which is meant to maintain a decentralized database of shared records that originally contain Bitcoin cryptocurrency[4]. The innovative features of blockchain technology make it an interesting concept to be applied in many business domains, including the pharmaceutical industry, smart contracts, logistics, banking, and Internet of Things (IoT)-driven smart cities[5].

Recently, academicians have advocated blockchain cities' concept to be implemented to transform the urban environment to meet urbanization challenges[6]. In this context, Blockchain might be considered as a General-Purpose Technology mandatory to organizational and human capital and whose acquaintance was refined by the urban ecosystems of the suppliers of the technology, local authorities, citizens, and political choice[7]. Blockchain technology is also critical in developing a sustainable global economy that ensures improvement in the quality of life (QoL) of individuals and consequently brings about fundamental global changes[8].

The decentralized, shared database administered by Blockchain offers immutability and transparency of transaction details. This technology is implemented in transactions of well-known cryptocurrencies, such as Bitcoin to consider issues of trust. This facet is essential when conducting arbitrary business logic using different alternative blockchain platforms, such as Hyperledger Fabric and Ethereum[9]. Various goals were set-up by cities and states that include several different approaches to maintain and enhance the blockchain wave.

Prior studies about Smart City technologies were limited and system-specific in their orientation and focus. The conjoint dimensions of smart city, however, were heterogeneous in their framing and systematized applicability. In essence, by resolving the individual problems of situational Smart City, these individual studies have provided another layer to the epistemological and ontological foundations necessary to formulate a more unified structural blueprint.

This review paper observes each experiment in blockchain technologies, IoT capabilities, and smart city solutions as a form of useful contribution to a much larger software project. The development of a unified framework for smart city applications standardizes the middle layer data management solution around the Blockchain's high-security and high-credibility foundations. It is essential to conduct a systematic literature review (SLR) to assess the state of progress to date and predict the best-fit solutions that will ultimately form the fabric of uniformity in a blockchain-supported smart city solution in the future. This review aims to examine current studies and their outcomes and summarize the essence of research done in the domains of blockchain technologies, IoT capabilities, and smart city solutions.

There is a lack of a precise, concrete, and comprehensive systematic review of the existing blockchain-facilitated state-of-the-art applications, motivating the researcher to conduct this research. The five research questions presented in the next section are constructed to address the specific limitation. This research aims to enlighten the readers on the blockchain components and offers a snapshot of the existing blockchain-enabled structural solutions in different sectors. This research has emphasized the increasing interest from the academic community based on a systematic review approach and identified three fundamental research streams: (1) smart city applications, (2) integrated solution of Blockchain and IoT with smart cities, and (3) limitations and solutions of blockchain technologies. It is essential to understand that the current review is not exhaustive by any means since Blockchain is a progressively developing technology and changes at a swift pace.

The remainder of this paper is organized as follows: Section II defines the aim and research questions of this SLR. Section III describes the methodology. The research questions and evidences are presented in Section IV followed by the discussions on results in Section V. Finally, Section VI concludes the paper and then recommendations for future work.

Ii. Aim And Research Questions

There is an urgent call for a cohesive solution that can link IoT nodes across the urban fabric for supporting technological interoperability as the commercial tasks limit the scalability of smart city technologies for individual corporations[7]. This study seeks to critically evaluate the current phase of development and innovation concerning Blockchain within IoT-based smart city solutions. This study also proposes a unified standard to integrate the Blockchain into IoT-based smart city applications. For a quick reference, the research questions (RQ) are summarized as:

RQ1. How much progress has been made in securing and protecting IoT-based integration into the smart city solution?

RQ2. What role could Blockchain play in serving as a unified, central database and transaction ledger for IoT-based triggers?

RQ3. What are the advantages (and limitations) of blockchain integration within smart city applications?

RQ4. Which components of the smart city solution can be standardized, and which elements will remain proprietary?

RQ5. Which structural limitations or challenges will prevent blockchain integration, and how could these problems be resolved?

These questions were answered through a systematic analysis and synthesis of primary sources.

Iii. Methodology

This study uses a SLR methodology[10, 11], which closely fits the topic of this paper: the clear steps involved in an SLR are specifically designed to reduce bias, increase transparency and facilitate replication of the review[11]. The precise nature of this paper's research questions means that the SLR methodology is a better fit than other review methodologies because the focus lies on finding, extracting, and systematizing evidences[12]. The underlying philosophy and approach are pragmatism regarding the use of Blockchain technology for IoT in Smart Cities context[13]. In the SLR methodology, the work starts by identifying the need for the review, specifying research questions, and developing the review protocol[11].

Review Method

Key concerns of the SLR method are the reduction of bias and the increase of transparency of a review[11]. The review protocol includes the search strategy, selection criteria, selection procedures, data extraction strategy and data synthesis strategy. The review protocol is reported in this section.

Review Protocol

This paper has conducted an initial systematic mapping review on the broader topic of Blockchain within IoT in Smart Cities[11]. This procedure forms an inductive, semantic approach whereby the three domains are chosen based on general knowledge of their current profile of interest. In addition, research into these three topics may offer new and improved methods for delivering more effective technological solutions in a variety of fields, including smart cities, Information Technology Infrastructures, and many others[14-16]. For this initial mapping review, a pilot search of the Science Direct database was conducted, the authors found minimal experimental or model-specific studies. Furthermore, when keywords such as Blockchain and Smart City were searched, the output from these search terms was not necessarily indicative of a direct relationship, and in many cases, it was found that Blockchain was a secondary or tertiary consideration. Finally, many studies' experimental nature was narrow, which resulted in purposive and selective interpretations that were irrelevant in the broader context of IoT-based smart city solutions. For all those reasons, a primary search strategy was developed to overlook the irrelevant or inconsistent studies and focus more explicitly upon the search terms and focus of the current study. Over the last 4 years (via manual search), this paper has identified 277 potentially relevant papers from science direct database only. This large number is primarily due to a significant increase in the number of IoT-research related papers published since then in dedicated venues. Examining those 277 papers, this SLR considered that experiments in merging Blockchain and IoT-driven smart cities (narrow focus) related to the broader use of “Blockchain for IoT” (wider domain). Blockchain for IoT includes smart cities contexts, but also includes other contexts for more effective solutions and due to the expansion of IoT industry into every aspect. Moreover, Blockchain for IoT attracts high current interest[2-4]. SLR further requires specifying the particular rationales behind research questions as asked. These rationales are presented in next section.

Research Questions and Rationales

This review aims to address the most essential and vital but confronting questions regarding the integration of the Blockchain throughout IoT-driven smart cities. The rationales and the research questions are summarized in Table 1 as an immediate reference.

Table 1: Research Questions and their Rationales

Research Question (R.Q.)	Rationale
RQ1. How much progress has been made in securing and protecting IoT-based integration into the smart city solution?	To assess the technical feasibility of blockchain-supported IoT integration in smart city applications.
RQ2. What role could Blockchain play in serving as a unified, central database and transaction ledger for IoT-based triggers?	To critically assess the central goals and technologies related to smart city applications and digital solutions.
RQ3. What are the advantages (and limitations) of blockchain integration within smart city applications?	To analyse the technological opportunities and limitations of IoT-related capabilities concerning the current standard of practice.
RQ4. Which components of the smart city solution can be standardized, and which elements will remain proprietary?	To assess the viability of blockchain-supported IoT solutions while considering an intermediary authentication ledger's applicability to support smart city scalability.
RQ5. Which structural limitations or challenges will prevent blockchain integration, and how could these problems be resolved?	To assess the factors restricting or limiting blockchain integration and to analyse the extant solutions and alternative models.

Search Strategy

The primary search strategy is relied on an automated online search using a specific search query in a set of academic databases. This SLR has targeted search of multiple academic and industrial databases consisting of peer-reviewed experiments and structural models related to blockchain-based solutions for IoT-Smart City applications. During the identification and selection process, the following strategic controls were used to streamline, focus, and legitimize the results[17]:

- **Key Terms:** Blockchain, IoT, and Smart City.
- **Search Databases** (Table 2)**:** ScienceDirect, Taylor & Francis, IEEE Xplore, Wiley, Sage, Web of Science (WoS).

Table 2: Search Databases

Organization	Database	URL
Clarivate	Web of Science	https://webofknowledge.com/
Elsevier	Science Direct	http://www.sciencedirect.com/
IEEE	Xplore	http://ieeexplore.ieee.org/Xplore/
Sage Group	Sage	https://journals.sagepub.com/
Taylor & Francis Group	Taylor & Francis	https://www.tandfonline.com/
Wiley	Wiley Online Library	https://onlinelibrary.wiley.com/

Quality assessment standards emphasized complete, experimental solutions that met all of the inclusion criteria and offered peer-reviewed or conference-based models with a high level of academic credibility. For this reason, some databases or journals were excluded due to their lack of mainstream credibility and academic value. An initial development of the inclusion/exclusion criteria created a baseline for defining the search terms and focus of the database search function. The SLR search strategy involved the following stages of investigation, interpretation, and analysis:

Stage 1: Conduct keyword search of specific academic databases in order to identify possible range of sources meeting conditions of inclusion criteria.

Stage 2: Eliminate or exclude studies failing to meet all criteria and identify studies which qualify for further screening.

Stage 3: Screen and eliminate duplicate or incomplete studies failing to add instrumental value to the blockchain, IoT, and smart city discussion.

Stage 4: Identify the central findings and core theoretical insights developed by each of the included studies.

Stage 5: Compare and interpret the cohort of outcomes in order to draw conclusions to the core research questions and synthesize the models into a single, unified proposition.

Study Selection Criteria

This paper has defined a set of inclusion and exclusion criteria presented in Table 3 for papers to be included in the SLR based on its purpose[11, 17]. It worth noted that the extraction period for inclusion criteria was set in 2016 because of the beginning of the appropriate integration of Blockchain and smart city applications[2, 18].

Table 3: Inclusion-Exclusion Criteria

Inclusion	Exclusion
· Studies published from January 1, 2016, till Aug 2019	· Studies published before 2016
· Experimental research with targeted model	· Non-experimental research or failure to include model or design
· Include blockchain and smart city solutions	· Only Blockchain or only smart city
· IoT-oriented or indicative	· No consideration for IoT
· Peer-reviewed journal or legitimate academic conference	· Non-peer reviewed or small-scale study (e.g., blog post, non-academic conference)
· Realistic or practical application	· Unrealistic, non-translational application or model

Search Process

The search query used for this SLR combines keywords that were directly derived from the aim and five research questions presented in Table 1. To develop the search query, the SLR has followed this process:

Stage 1: Utilize multiple search terms and the operators "AND" and "OR" to combine Blockchain, IoT, and Smart City and their synonyms into a single search function.

Stage 2: Eliminate any review or editorial studies and focus on smart city-specific research considering the broader, experimental implications of an innovative, blockchain-based solution.

Stage 3: Identify the primary and secondary studies relevant to this model and determine whether to include or exclude for some reasons (e.g., lack of experimental relevance).

Stage 4: Remove any redundant study that has been included in other databases. For example, WoS is an aggregation database and not a journal or article-specific database. Therefore, some articles like Sharma and Park[19], Hammi et al.[20], Rahman et al.[21], and Fayad et al.[22] were replicated from other databases. As a result, they were included in the SLR but counted only once.

Data Extraction

This research process acknowledges that the experimental procedures, technologies, and applications for each study were different from the other research; however, several overlapping elements were critical to

reflect the meaning and significance of blockchain technologies in IoT-based smart city solutions. The data items included in this SLR were based on the following extracted elements: Title, Journal, Volume (No), Year of publication, Pages, Overview, and Findings (Appendix A).

Data Synthesis

The review utilized sources that met the inclusion and exclusion criteria. The analysis revolved around the emerging themes based on research questions. The research questions were independently carried out by the reviewers[23].

Screening Process

A systematic approach was applied to the comparative and critical analysis of multiple studies that reflected the indicative characteristics of experimental solutions related to blockchain technologies for IoT in smart cities solutions. However, this study rejected many of these approaches to follow the central dimensions of the inclusion criteria[17].

Any inconsistency was resolved through mutual consensus regarding the quality of reviewed articles. Several studies were excluded because of their lack of focus on the technical elements of blockchain technology and blockchain architecture.

Table 4 further refines these controls into the PICO(s) model proposed by Cochrane[24] as a systematic solution for comparing evidence-based studies in the health care field. By refocusing this model on the problem essential to this investigative process, a solution which meets three different criteria, it was possible to narrow the search process down further and restrict the outputs of the SLR to a narrower, more manageable selection of appropriate studies. Most notably, studies without a practical or model-specific consideration that could be translated into a general, broad-spectrum application for a unified smart city solution were now excluded during this search process.

Table 4: PICO(S) Framework for Study Selection

PICO(S)	Inclusion Criteria	Exclusion Criteria
Problem	Blockchain AND IoT AND Smart City	Individual emphasis on keywords or focus outside of the immediate context
Intervention	Experimental, Model-Oriented, Inclusive	Non-Experimental, Outlaying, Exploratory, Conceptual
Comparator	Underlying Purpose Related to Smart City Applications	Underlying Purpose Related to Other Applications
Outcomes	Proposed Model or Contributory Solution	Revised Concept, Future Research Recommendations
Study Design	Experimental, Architectural, Non-Proprietary	Proprietary, Empirical, Application-Limited

Therefore, the summary output of this systematic exercise was indicative of multiple academic, peer-reviewed, and conference studies that were experimental and reflected meaningful contributions and innovations to a middleware layer of blockchain integration within the broader complexity of an IoT-navigated smart city environment. Table 5 presents the search queries that were used to determine the scope of the research.

According to the search strategy, the search on the selected six databases was conducted from May to July 2019. Variations of the keywords were used to complete the comprehensive search; however, those articles were ultimately selected, including the full set of keywords (IoT and Blockchain and Smart City). Other searches were just treated as a part of the process (e.g., a learning exercise) to assess the scope and depth of the available literature during the selection procedures and ensure that the distillation of relevance is consistent with the inclusion criteria. In the Taylor and Francis database, even though it contained more than 3,000 articles related to the IoT and Smart city applications, none of the articles were associated with blockchain technologies' experimental nature. Instead, these articles adopted a theoretical or summary approach reflected throughout many of these databases.

Prisma Flow Diagram

The summary output model presented in Figure 1 highlights the effects of the systematic distillation process which resulted in the parsing of many thousands of studies down to a much smaller, directly-relevant sample. Figure 1 provides a visual representation of the PRISMA (2019) flow diagram employed to increase the overall transparency of this SLR reporting process. It further highlights the critical assessment and rejection process based upon the increasingly specific search functions performed during the individual database reviews. At each stage in the PRISMA model, studies were either included

or excluded on the basis of the screening criteria which included the inclusion/exclusion criteria, a determination of completeness or topical relevance (e.g. needed to include blockchain), and a quality assessment of the journal or source of publication. In many cases, studies were excluded because they failed to link blockchain models to smart city solutions. In other cases, smart city solutions focused on IoT nodes but failed to consider the blockchain. All three of these top-level keywords, blockchain, IoT, and smart city were critical to ensuring that this study met the central research objectives and answered all of the questions developed for this research process. As evident from this model:

- This review has identified 26 studies which were based on blockchain technologies, IoT capabilities, and smart city solution conducted in the period from 2016 to 2019. This list can be used by other studies to expand the work in this particular field (Appendix A).
- This review has selected 18 primary studies that fulfill the criteria mentioned in Table III for quality evaluation, were published in academic journals, contained some form of experimental or model-oriented solution, and most importantly, offer a distinct advantage over other proprietary research in this field: transferability and adaptability.
- The final primary studies can offer appropriate benchmarks for comparative analysis against the current review paper.
- This review paper has also conducted an in-depth review of the selected experimental studies to elaborate on the ideas, considerations, and research in blockchain technologies, IoT capabilities, and smart city solutions.
- This study has presented an SLR concerning applications in which Blockchain can be implemented with the collaboration of IoT capabilities and smart city solutions.
- Appendix A presents a structured summary and systematic evaluation of the central perspectives and findings relative to each of these included studies.

Threat to Validity

Although the studies identified over the course of this SLR are indicative of the leading research in this field of blockchain innovation and IoT applications, their reliability and practical functionality remains under-tested. Validity in the context of the IoT is about immutability and any potential repudiation, conditions that cannot be tested without an ecosystem in which to experiment, evaluate, and confirm the practical value of the originating solution. The review of these experimental models is derived from an assumption of reliability and validity that is conditioned both by the credibility of the source documents (e.g. journals, conference papers) and the reputation and identity of the authors in question (e.g. professors, students, researchers). These findings, therefore, assume construct validity on the basis of the comparable similarities between these approaches and the overlapping characteristics of the methods and models in question. Future testing and analysis will be needed to determine whether this proposition

is reliable or sustainable over the full scope of implementation, testing, and usage. In this case, the comparable overlap between the individual studies has been used to establish the validity of the results from the SLR and to confirm that there is an interwoven theoretical and conceptual position that has evolved out of multi-directional study, model development, and experimentation in this field.

Moreover, there are numerous threats that may emerge when carrying-out a systematic review. For instance, not all studies or sources identified are relevant based on information. In this regard, different search criteria were identified and researched for different databases for eliminating this threat. Different criteria and logical operators were applied for increasing coverage. All relevant documents were found through different keywords combinations. Majority of the research attained after the exclusion criteria were published in 2016-2019 even though the subject was completely new. In this regard, it is assumed that the missing article review on the subject was too minimal for influencing the findings of this study.

A threat in this context is associated to unpublished works or related works that are not currently present in the selected scientific database. The excluded publications do not influence the internal validity since the selected databases were well-articulated and researched. It might be claimed that a margin of error might be present due to initial sampling even though the articles were covered based on the selection criteria. Thereby, the margin of error is used for calculating the internal validity in systematic literature review studies. External validity refers to the level the outcomes of the study can be generalized for other circumstances, times, and individuals. The data obtained, in systematic review, as an outcome of research questions are assumed for reflecting general outcomes with respect to existing blockchain patterns and research.

I. Research Questions and Evidences

Research Question 1: *How much progress has been made so far in securing and protecting IoT-based integration into smart city solutions?*

The original novelty of IoT-related smart city solutions has gradually evaporated from the academic compendium and has replaced uncertainty and optimistic innovation with a more pragmatic, utilitarian, and integrative focus. Ideology in this field of study was related to IoT-based innovations and indicative of a complex tension between uncertainty and innovative potential. This was attributed to the lack of structural vision and the competing spectrum of heterogeneous technologies and smart city applications[25-27]. In fact, Almirall et al.[28] and Chen et al.[29] have connected network security threats with the heterogeneity of IoT-related technologies and innovations in a scholarly manner. Nevertheless, the SLR has illuminated an alternative structural shift in the field of IoT research. Therefore, it has replaced the underlying questions of why, what, how, and where. Progress in this field has shifted away from the technical functionality of blockchain-based IoT integration in the smart city, and instead, towards understanding the means of unifying the intermediary standard of authentication and data management. Researchers are now pursuing understanding of how IoT nodes can be deployed, secured, and activated without requiring the proprietary limitations of existing applications and service provisions; instead,

linking the capabilities of the IoT through a broader, unified proposition of blockchain-supported connections (e.g. smart contracts).

Innovation, by definition, in the modern fabric of the IoT architecture, is now defined by the integrative potential of the individual nodes within a broader digital footprint[22]. Khan and Salah[30] once predicted an iterative security solution capable of leveraging ontological integration and threat identification to shape the security function. Studies established that the modern IoT agenda was predicated based on holistic, structure-integrated, non-repudiated, and ubiquitous cyber-security standards[31-33]. More importantly, the IoT was no longer object-specific; instead, it was a mesh-based solution that incorporates multiple decentralized nodes into a performance-broadened, function-diversified solution that emphasizes service execution over data encapsulation[32].

Blockchain, whether private, public, consortium or hybrid, is a peer-to-peer distributed ledger technology that records agreements, transactions, sales, and contracts. It also confirms transactions for creating a verified as well as unchangeable information ledger. The attributes of open, interconnected, transparent, and peer-to-peer sharing and storage are appropriate in the Blockchain to the interconnection, peer-to-peer, openness, and shared attributes of the energy internet.

Blockchain can develop significant smart grids and networks, changing how everything is developed from the vote and established credit to receive energy. In certain ways, it could be an essential constituent of what is required for circumventing outdated systems and providing lasting solutions to cities.

Six central themes have been identified within this SLR regarding IoT-related innovation and the contribution of research evolution to a revised frame of reference related to IoT adaptation for smart city solutions presented as a visual representation in Figure 2. The brief explanation of each iterative dimension of the IoT solution is as follows:

- **Adaptive:** For the IoT to meet the varying needs of urban residents, individual nodes and their underlying software technologies must be sufficiently adaptive to create a mesh network of valuable, specific, and interdependent information resources[34,35].
- **Integrative:** Any IoT solution is sufficiently valuable as a standalone service (e.g., smart locks on the house); however, integrative IoT solutions provide users and companies incentives to link and connect multiple devices to a central database or information management solution[24].
- **Intelligent:** By interpreting and purposefully triggering actions related to predetermined guidelines and authorizations, each node in the IoT becomes a critical service agent within the smart city solution[36]. Although adaptation and integration provide the basis for a connected overlapping network, it is the intellectual functioning of the IoT that ultimately meets the requirements of smarter, high-functioning services[21,31,37].
- **Secure:** Given the critical nature of the information being collected regarding user behaviors, locations, and identities, the IoT must be sufficiently secured through confidence-enhancing

technologies to motivate user participation[38,39]. Integration further exposes systemic vulnerabilities; therefore, some intermediary or standardized security protocol is required to protect users against internal and external threats[32].

- **User-Defined:** User-definitions serve as conditions for shaping IoT services and shaping IoT services and protecting individuals against the loss of control over such critical, personal resources[35].
- **Service-Oriented:** The IoT is service-oriented, and as a result, the data collection process is only secondary to the end outcome of the user-device relationship: the service[36]. By designing IoT-based solutions that meet specific needs or expectations, companies are reshaping the nature of human-technology interaction, and as a result, they are precipitating and accelerating the evolution of information-supported, autonomous service provision[32].

There is an immediate need for a framework capable of fulfilling lightweight security requirements and performing information management functions[40]. Critical factors related to dependability, authentication, security, and decentralization are important antecedents to the future of smart city technologies[40,41]. Through a review of experimental studies, it has been made evident that the unified concept of a 'canopy framework' described by Paul et al.[42] is an essential layer of innovation that will provide the next generation of system designs with a more efficient and unified solution. Central conditions of this standard include a lightweight, low-power, and low-computing standard of technology that transfers the responsibility for information management to either a central blockchain node or to outlying administrative nodes that limit the need for IoT-based information processing[42].

This standard validates the model presented in Figure confirming the expectation of heterogeneity and adaptively and emphasizing a direct relationship between a predictable and standardized middle-layer technology (Blockchain) and outlying IoT-based proprietary nodes. In this way, the Blockchain as a service (BaaS) standard eliminates the companies' need to develop their database management solutions. It will ideally allow smart city technologies to be added and removed from the network solution according to the need rather than technological dependency[35,37]. Accordingly, API solutions will remain proprietary and can be developed to support the independent module and objectives of a company. Similarly, the revised homogeneity of the Blockchain's middle layer solution is an important innovation that will realize the broader objectives of a secure, scalable, and interdependent smart city standard[18,43].

Research Question 2: *What role could Blockchain play in serving as a unified, central database and transaction ledger for IoT-based triggers?*

Throughout this SLR, the evidence captured has illuminated a form of transformative shift, whereby uncertainty regarding blockchain technologies exemplified by prior theoretical research has struggled to address the practical and the theoretical inconsistencies[36,44,45]. Whether it is conceptual or theoretical, the Blockchain serves as a placeholder or viable solution that needs additional testing and exploration in

various exemplary contexts and system specifications[36]. When implemented practically, Blockchain becomes a modality or method of goal actualization; it transforms the underlying limitations of extant IoT technologies into a form of catalyst for innovation and model adoption[17]. The SLR has illuminated a gateway opportunity in blockchain technologies that can address many of the underlying limitations and deficiencies reflected in the innovative effects of IoT development and deployment in a technologically heterogeneous marketplace. The following five dimensions represent the blockchain solution's indicative characteristics and their roles in servicing and shaping integrative technologies of the IoT-based smart city.

- **Security and Authentication:** This characteristic of the blockchain-based ledger solution secures and connects with the hash-based, encryption-supported, proof-of-work standard of authentication and data protection[18]. IoT nodes are vulnerable to inner attacks or external tampering due to their low-security profiles and lightweight characteristics. By maintaining records of service-related transactions on the decentralized ledger, individual users, and support agents acquire the ability to provide or restrict access to the resources, databases, and actions necessary to make the IoT a high-functioning, service-centered solution[46,47]. IoT nodes self-authenticate autonomously without requiring a central authority and system changes can be detected relative to blockchain-level permissions and records. The base of security is to ensure the validity of identity of a device that access to the network in the IoT. Authentication is a mechanism by which a network refers whether the user has access to specific resources. The authentication can be classified into three classifications: (1) possession, (2) ownership, and (3) knowledge. Public key cryptography is used for preventing illegal devices in order to access the IoT for authenticating IoT entities. The major difference is that a peer-to-peer authentication methodology is introduced regardless of third-party based on blockchain. Security protection ensures the reliability of the IoT devices. It still has the risk of being attacked by malicious users because of the system or software even if a device has passed the authentication of other nodes. The network entity is modified by the intruder for leaving a backdoor in the device for preparing corresponding infiltration and modifying the fundamental configuration file in the device. Critical data have been regularly verified for discovering potential intrusions instantly.
- **Encryption and Access Keys:** Through the hash-based encryption capabilities of the Blockchain that employ a standard like Ethereum, companies can anonymize and protect user information and identities[35,47]. Yet in spite of this protocol, the pseudo-anonymous character of these alt-coin solutions may potentially expose the blockchain to linking attacks along downstream nodes[35]. Encryption also can be used to secure cloud-based storage solutions and to reduce the likelihood that any usable data could be scraped or accessed by individuals with malicious intent[37]. Access keys (public and private) afford the owner the right to initiate a transaction or access a resource, and are secured by complex cryptographic signatures that make reverse-engineering and replication a nearly impossible exercise[48]. Shared secret key technique is used for delivering secret key in the header request for accessing the endpoints. REST protocol is used for providing a standard

approach to access the endpoints. Basic HTTP Authentication is used to secure all REST endpoints or by using a shared secret key.

- **Structure and Network Integration:** The middleware status of the Blockchain was a critical antecedent to the universal integration of this data management solution across all IoT-based networks[38]. Even in scenarios where companies choose to maintain a private blockchain, Blockchain's unified centralization ultimately indicates its adaptability across several network configurations and service-based solutions[47]. The blockchain is characterized by a range of public, private, and hybrid solutions that can be customized according to the unique protocol and computing needs of the intermediary network (e.g. public entity, private enterprise, consortium)[32].
- **Decentralization and Transactional Management:** One of the smart city vision's primary goals is to automate and decentralize service solutions and letting smart city vision's primary goals are to automate and decentralize service solutions and let artificial intelligence and algorithmic controls respond to user behavior in productive ways[43]. By decentralizing these responsibilities, government agencies have reduced the weight of resources and information technology agents invested in system monitoring and task execution processes[32]. Similarly, companies participate in a peer-to-peer solution by integrating additional modules and technological mechanisms to expand the scope of smart information and services[49,50].
- **Smart Contracts and Activity Triggers:** The antecedent to a secure and efficient blockchain solution for smart city applications is the smart contract[36]. This contract is defined by its predetermined authorizations and triggered by both the user and service providers[30]. The reciprocity of this input-output-based system ensures the protection of users during the information transfer process[51].

Components such as being distributed, secure, shared, smart, and encrypted offer the mechanism for being democratized, automatic, private, and transparent in the computing of blockchain-based sharing services. The computing block-based sharing services support the automation of business services and transactions. IoT devices can take part in trust-free transactions, and contracts can be acquired in computing codes for automatically performing the obligations that users have committed to in accord when enabled by blockchain technology.

It should be noted that a smart contract has now been integrated into the Blockchain. It is also noted that code functions are integrated within a smart contract and can connect with other contracts, store data, send ether to others, and make decisions. A blockchain is integrated into Watson IoT that facilitates information from devices such as device-reported data, barcode scanned events, and radiofrequency identification (RFID) to validate smart contracts or to be shared with device-reported data[52]. Software agents can be adjusted for dynamically managing each distributed independent organization, which connects physical nodes in a network to devices throughout a series of contextualized smart contracts. Sharing business will be automated by computing blockchain-based sharing services and the highly efficient IoT supported by the internet and a series of contracts, smart transactions, and agents[53].

Research Question 3: *What are the advantages (and limitations) of Blockchain's integration within smart city applications?*

One of the major revelations of this SLR was that any limitation to blockchain integration was due to a delayed response to the gradual and niche-based research development in this field of study. Researchers have envisioned a new pragmatic future for blockchain integration; the transition from an enigmatic and misunderstood status to this progressive frame of reference has been checked thoroughly for any uncertainty[16,18,47]. Specifically, this SLR has revealed multiple layers of uncertainty related to the following critical advantages of blockchain integration:

- **Immutability:** Once the data has arrived at the Blockchain, it remains immutable, as the hash serves as a mechanism to validate the unaltered data[32,35]. As an advantage, immutability ensures accuracy in the smart contract exchange and reduces user vulnerability to unauthorized or inconsistent manipulations of the agreement[35].
    - **Limitation:** If the data enters the corrupt Blockchain, it will remain corrupt when recorded within the same blockchain ledger[35]. This vulnerability creates challenges for IoT developers, and device-level security is required to restrict the possibility of misleading or inaccurate transactions.
- **Decentralization:** More than 5 billion IoT devices are connected to the internet, and it is predicted that more than 29 billion IoT devices will be connected by 2022; therefore, a decentralized and autonomous database is needed to process large amounts of data without threatening the privacy of the individual users[31].
    - **Limitation:** The lack of centrality in the administration of smart agreements and contracts could lead to conflicts between proprietary designs and organizational solutions when organizations fail to embrace a blockchain-based proof of work standard[17].
- **Non-Repudiation:** Contractual conflicts and legitimacy are restricted in blockchain-supported smart networks because of the hash-based, smart contract-controlled processing, and storage of data within each block[30]. By optimizing the number of blocks within a given system and restricting outlying variants through mining-based hash-maps, Blockchain offers a non-reputed solution that is confirmative and transaction-validated[31].
    - **Limitation:** Corruption of the Blockchain via unauthorized or false contracts could create mistrust and network vulnerability[17]. Structural solutions that restrict tampering potential, such as edge-aware and smart semantic contracts, could potentially eliminate the majority of these threats in a blockchain-integrated network[49].
- **Network Framework and Integration:** For smart cities to realize their optimal, integrated structure; there is a critical need for an intermediary layer capable of objectively and autonomously negotiating smart contracts and providing agents and users with appropriate access[17]. The Blockchain's decentralized character is valuable for a multi-layered system fulfilling a critical gap in IoT-based

smart city design that would potentially have been filled by some form of limited proprietary technology[49].

- **Limitation:** Organizational buy-in and user support is a critical antecedent to the investment in this process, and as a result, it acts as a limitation that could potentially restrict such engagement in short to medium term[34].

The smart city experiences several challenges. Some of the most substantial challenges are associated with an elevated amount of data transfer that ensures security. This study encourages developing the capabilities to use novel blockchain technologies that can overcome challenges by taking benefit of the opportunities and advantages of Blockchain and other associated technologies. Blockchain technology offers massive possibilities for shaping the improved smart communities in the forthcoming events that are more efficient and offer a better quality of life. The technology should be enabled for changing the existing situation, which should be replaced via innovation for delivering on its promise. This study further demonstrates how blockchain-based sharing services can assist in creating smart cities and discusses the foundations and concepts of Blockchain and the application of blockchain technology. Clear examples of the practicality of this technique are indicated in different economies in different sectors. It indicates the comprehensive, continuous, and successful experiments, offering a clear perception of the benefits and advantages. The technique also highlights the challenges that could be encountered in the integration of such technologies in other contexts.

Research Question 4: *Which components of the smart city solution can be standardized, and which components will remain proprietary?*

For a smart city design that meets the diversified requirements of complex urban environments, any unified solution must consider the scalability and adaptability of the distributed yet interconnected nodes[33,36]. As a result, blockchain technologies' middleware solution presents a potential for standardization, whereby data processing, cloud-based storage technologies, and security authentication are connected to smart contracts and transaction signatures[39]. In each of the studies reviewed within the SLR, it became evident that the blockchain solution's conceptual underpinnings remained constant, while the outer level nodes were adaptive according to their user and administrative guidelines. There are several central dimensions of the standardized blockchain solution that need to be incorporated into any smart city solution. Figure 3 visualizes four central traits of a unified and standardized blockchain solution to facilitate lifecycle usability and maximize the blockchain solution's efficiency and intra-transactional value. These core components are further defined as follows:

- Scalability and Centrality: The blockchain solution must be sufficiently scalable and maintained centrally in order to allow for network connections across broadly defined public channels. This means that additional IoT nodes can be added or subtracted freely and without damaging the continuity and reliability of the network.

- Trust and Security: There is a unified expectation that any connections to the network will be sufficiently trustworthy and that they will afford the security to restrict access to user data or identity (e.g. anonymity, encryption, protections). This means protecting against both insider and outside attacks, creating stop-gap solutions that restrict unauthorised access, and affording users the ability to set, modify, and remove permissions.
- Authentication and Authorisation: Established as the formal basis of the API contract between the user and the service provider, the authentication protocol should create a consistent basis for authorising actions on both ends of the smart contract.
- Transaction-Oriented Ledger: Based upon immutable record keeping, consistent transactional processing, and predefined agreements, the blockchain operates as a central ledger or clearinghouse for the IoT providing the basis for fulfilment and execution of the contractual agreements.

Where the blockchain, the proof of work concept, and the data storage protocol will need to be standardised in order to address the scalar complexity of the smart city architecture, the need for proprietary and heterogeneous software and hardware solutions must also be considered. The varying contractual terms required for smart energy meters and self-driving automobiles are different, and for this reason, contractual dimensions cannot be established by the service provider[39,51]. Besides, the type of information collected by the IoT node should be considered, and while the terms of the smart contract will define the access to this data, consumers will also need to be able to maintain control over how and when their data is accessed and used[31,52].

Finally, proprietary APIs and data interpretation software will be needed to make sense of the broadening scope of big data that will ultimately be captured via these diversified smart nodes. Decentralized data collection will have opportunities for both public and private enterprises; therefore, as consumers recognize the potential advantages of data sharing and access granting, this smart mesh network's net benefit will become contingent upon the proprietary leverage of fog-based information resources[32]. The SLR has demonstrated how purpose-built experimental models are designed to connect individual technologies (e.g., one IoT node) with specific transactions or behaviors (e.g., smart electricity monitoring). Simultaneously, the broader complexity of a more dynamic solution that considers the integrative potential of a centralized data management solution (e.g., a public database) must be considered within the context of both public and private enterprises.

Research Question 5: *Which structural limitations or challenges will prevent blockchain integration, and how could these problems be resolved?*

One of the major limitations observed within this SLR was the uncertainty and misunderstanding that has made blockchain adoption so inconsistent over the past decade. While academic vision and innovation provide the primary antecedents, more productive structural solutions such as experimentation are entirely inadequate when considering smart city applications' breadth. Independent studies conducted by

Ouida et al.[47] and Rahman et al.[18] have established a framework of progress and proof of work design capable of facilitating change and transforming the structural expectations regarding blockchain integration; however, additional real-world demonstrations are needed to highlight the scalability and connectivity of such solutions. Further, the commercialization of any Blockchain integrated solution will require both consumers and corporations to trust in an enigmatic technology that has generally been associated with crypto-currencies and controversy. With security threats publicized and the risks of unchecked and potentially vulnerable technologies are debated at public forums, the blockchain solution's legitimacy and consistent fidelity have yet to be proven.

Another problem with the aspirational development of a unified blockchain solution is collaborative innovation or a centralized, publicly-supported framework. Independent innovations such as the multiple adaptations of the Ethereum protocol create conduits to structural progress, but they also raise questions about the viability of a singular, centralized standard[19,35,48]. For Blockchain to become an effective middleware solution; there must be a regulatory body or overarching standard established for smart city service management. Proprietary IoT nodes are invaluable and must be supported to ensure that the smart city reality is achievable; however, these decentralized nodes represent just one layer of a mesh solution that places outlying edge-level nodes into a purpose-built technological fog[34,35]. Therefore, to overcome the myriad structural, security, and data management limitations that affect the practical advantages of the IoT-based smart city solution, a unified blockchain framework is needed to establish, control and legitimize the underlying smart contracts.

Big data management might be eased through the secure and verifiable blockchain structure[54]. On the contrary, data analytics via blockchain structure, implying too much overhead. All transactions will not be essential, and therefore, efficient or intermediate auxiliary structures might be integrated to increase the overall efficiency. Thereby, solutions must be implemented on an ad-hoc basis. Nonetheless, there already remain blockchain-based structural solutions for big data storage[55].

II. Overall Discussion

Many issues have yet to be addressed while blockchain applications are being broadly deployed, which would make them durable, scalable, and efficient[56]. The components they provide are not unique if evaluated individually, and most of the platforms are well-represented for years. However, combining these components make them competent for several applications to justify the intense interest of several sectors[57].

Their applications are anticipated to penetrate additional domains or industries compared to the ones covered in this survey as blockchains' become more mature [58]. However, this is far from the truth; while many applications propose blockchains as a solution and an alternative to databases, there are many other solutions where conventional databases must be utilized instead[59]. The individual attributes are identified that are mainly needed per each application domain. This enables selecting the appropriate

Blockchain and the subsequent platforms for tailoring the Blockchain to the actual requirements of the application[60].

It has been noted that the smart city is becoming much smarter because of the existing expansion of digital technologies. Smart cities comprise different kinds of electronic equipment integrated by some applications, including sensors in a transportation system and cameras in a monitoring system. Also, the use of individual mobile equipment can be explored. Therefore, different terms such as participants, motivations, security policies, and objects' characteristics should be considered by taking a heterogeneous environment. Smart cities' essential elements include smart energy, smart buildings, smart technology, smart healthcare, smart infrastructure, smart mobility, smart citizens, smart governance, and education.

Interoperable Imperative

A critical antecedent to identify an adaptive, information-rich, and fluid smart city ecosystem is represented through networked interdependencies. The intersection between dynamic and static resources will enable a process of data-rich, behavior-aware and smart transactions that will essentially change the scope of technology-improved decision-making in unified urban spaces using iterative enhancements[61-63].

The competitive precedent for siloed technological development has caused structural fissures as algorithms, networks and proprietary modules, and network-spanning information exchange of smart nodes in the smart city ecosystem despite all benefits[64,65]. A unified proposition for interconnected and integrated solutions is indicated via recent decentralized wireless networks such as Helium and IOTA proposed that allow positioning data ledgers as intermediary clearing houses for transaction-aware smart networks[65,66]. The existing solution suggests a non-proprietary, standardized, and unified protocol for inter-connecting IoT-based smart city solutions with a blockchain middle layer for protecting both user and commercial preferences in a distributed and circulated smart city ecosystem.

Blockchain and the IOT

The IoT is accomplishing a widespread technological perspective of multi-nodal and integrated communication across distributed networks via multi-function, low-power, and lightweight devices[68]. The scale of IoT-based solutions is rapidly expanding from smart home solutions to critical city features. The potential to mine and interpret these data resources is restricted because of the paucity of interoperability across proprietary systems with several devices attaining usage, environmental and behavioural information[32].

Each hardware unit of the IoT is restricted in both communication and computing power when classified as restricted nodes that constrain its competency to effectively secure and monitor unauthorized

activities and security breaches[57]. It becomes essential for systematically mitigating the code size by modifying the connection network's infrastructure via a distributed solution with both light and full nodes, whereas blockchain solutions can address the authentication stress of the IoT[57].

This network topology depends upon what has been realized by[69] as a distributed consortium network and outlying side-chain networks connecting IoT devices to intermediary notary nodes on the blockchain-based on an edge-computing protocol. A parallel consensus and transaction-verified authentication have been facilitated from the central conceptual foundation for the Helium network or Tangle proposed by[67], which ensures paucity of conflict between the existing and any previous transactions[69]. Blockchain technologies were proposed as a decentralized solution that is dynamically susceptible to double-spending, security breaches, and exploitation for online transactional systems[31,37,39]. The authenticity and non-repudiation of the blockchain exchange are immutable as it forms a foundation of distributed accountability and trust that resolves the essential conflicts surrounding agreement-based legitimacy through hash-based registration of outgoing and incoming transactions[39]. Therefore, this trustworthiness addresses most of the security and susceptibility-based issues, which undermine lightweight IoT nodes' resiliency.

Existing IoT solutions work on proprietary networks with limited interoperability, which result in single-stream transaction outcomes such as user-device-service provider. Cross-service communication between devices is needed for integrated smart IoT applications for facilitating authorized trigger-command-response outputs and enhances the comparative smart value system[70]. For instance, an in-vehicle module can use geographic information system (GIS) data for triggering home automation throughout the final phases of the drive, which could open the garage, illuminate the home and maintain a preferred temperature based on user-prescribed settings. Integrated commands should be communicated and responded based on several APIs developed for each IoT-based node, which an unrealistic process is considering a lack of multi-modal communication across individual devices and proprietary challenges[71].

The wireless mesh network is one of the pragmatic developments developed through current long-range and high-frequency wireless technologies[67,72]. Autonomous IoT solutions are developed to negotiate with thousands of clients and obtain data appropriate to service support and provision by implementing a large-scale advanced metering and monitoring system[73]. An open-source and centralized blockchain-enabled solution is developed by involving the proprietary-network architecture for data transaction procedures while restricting data access and unauthorized transactions for extending this model[64,74]. This middleware layer will reduce the requirement for high-bandwidth and complex network connections using cloud-limited access and blockchain authentication. Instead, IoT nodes to use any authorized network to communicate when fundamental tolerances or circumstances are fulfilled.

Trust, Security, and Smart City Applications

Data exchange's scope and specificity are considerable across smart city nodes, and security and authorized access are fundamental issues for service providers[75]. The extent of corruptible intermediaries related to networked interfaces is limited, and trust-based exchanges are ensured by applying cohesive standard IoT devices for a centralized and Blockchain negotiated database[76]. The proprietary APIs and user interfaces are retained by navigating transactions to edge computing and centralized blockchain requirements, while centralized transaction navigation is transmitted to cloud-based intermediary services throughout the blockchain solution[77,78].

The benefits of transmitting data and computing management restrict corporate entities from small-scale experimental models of this interface and offer users the competence to navigate and limit access to their device-shared data[79]. Smart city interfaces offer an opportunity to navigate and interpret the noise and impairments featured through human behaviour for city officials. These solutions entail establishing real-time models, and predictive metrics merged with multiple layers of inputs for presenting a pragmatic aspect of supply and demand postulations[18]. Therefore, the effectiveness of future responses relies upon the connection between real-time updates and informational awareness, which increases the significance of a standardized and unified middle layer competent to connect several proprietary devices across the urban ecosystem. The adaptability of infinite loop architecture regulates data management and security abilities while encompassing the edge-to-edge elasticity of technology innovators, service providers, and developers[11,80]. In smart city solutions, there are multiple paradigms of the application of this model:

- Smart Energy Meters: Supply and demand data are transmitted by user-defined interfaces customized for both energy consumers and city managers via demand profiles and IoT tracking nodes to monitor route energy and enhance the overall efficiency of non-activity periods[39,51].
- Smart Trash Management: Real-time data can be reported by smart waste bins prepared with IoT sensors for waste management administrators to trigger consistent and on-demand pickups[81,82].
- Smart Route and Environment Monitoring: The ability to track carbon emissions, urban flow and population density over extended periods are monitored through real-time analytics for proposing solutions for flow-routing, pedestrian awareness, and capacity-building[83,84].

The Solution: Standard-Setting and Blockchain Integration

It becomes vital that any coordinating solution is competent enough to address the particular restrictions about security and scalability due to the confined computing power in each node, the susceptibility of always-on or on-demand network connections, and the scale of the IoT[85]. The fundamental aspect of blockchain-based IoT is to use the decentralized agreement mechanism for guaranteeing information security before transactions are executed with possibly corruptible external nodes[86]. Transactions are predictive of IoT processing solutions where user events trigger downstream responses once identities are confirmed based on the contractual agreement[87].

The blockchain middleware solution offers a high-efficiency and high-integrity solution to realize the overall intersected objectives of smart city solutions via mining-verified decentralized ledger, encryption, and security keys. Therefore, this study proposes the integrated solution based on five fundamental conditions that will achieve the overall objectives of interoperability, smart city deployment, and decentralization once the IoT is integrated with the blockchain middle-layer. These conditions are listed as under:

- Scalability and IoT Information Exchange: The maximum potential for expanding information processing abilities comparative to demand or supply network scale while integrating nodes on-demand[80,88].
- Unified IoT Networking and Interdependency: Cooperative consensus, exchange-based architecture, user-defined controls, standardized protocol, and trans-organizational network solution[89].
- Digital Authentication: Restriction and authorization are ensured by digitally signed transactions based on pre-existing permissions and contracts[76,77].
- Autonomous Exchange and Transaction Processing: Permissions-based intuitive decision-making, independent transaction processing and restricted human navigation and network interaction[79,90].
- Security and Threat Mitigation: Continuity-ensuring and access-restricted controls based on adaptive, independent, and encryption-protected interventions[91,92].

The Model

A Blockchain solution is proposed in Figure 4, based on a current standard of exchange, even though it is dependent on the transactional modality, which has yet to be examined and investigated in practice. This model features an infinite-loop foundation for IoT consortium-based integration. Two external notary nodes are introduced by the model present beyond the mechanism of transactional control in the Blockchain, which includes user-defined preferences, software support, terms and consensus of the service solution, and privacy controls offered by the legit companies. The IoT nodes are brought online, and the privacy preferences are developed, and the terms of quality of service and sharing are ensured once they have physically transferred ownership from corporation to consumer.

At the IoT node, transactions are triggered in the side-chain network, which activates the Blockchain's smart contract. This will allow the network to approve and record responses as per the company's software solution at the notary node. There is a transmission of blockchain-encrypted information between companies according to the terms of the agreement. Return response to another IoT node will be triggered through responses following the information sent from Company A to Company B, which will result in the pre-approved action. In this regard, each IoT remains in its decentralized autonomy, but it is also competent for responding immediately and efficiently to the trigger or signal sent from the service provider.

Vi. Conclusion

Critically, this SLR has emphasized and reviewed the fundamental concepts and structural solutions represented in the previous years of blockchain-based smart city research concerning its support for IoT innovations. The findings have included three central outcomes: A structural solution for security and authentication in the IoT, a tangible application of smart contract technologies for decentralised smart negotiation, and a means of permissions-based performative oversight and administration.

- Structural Solution: A middleware clearing house for IoT transactions capable of receiving and sending requests and approvals according to predetermined contracts between the user (IoT node holder), the service provider (software owner/API creator), and the responsible organization (developer or service provider).
- Smart Contract Technologies: The ability to accept, interpret, and respond to contractual triggers that allow for activation of IoT nodes based upon security-authenticated initiation either independently or autonomously by the user or associated agents (e.g. smart speaker, smart module, in-home node).
- Permission-Based Oversight: A central agreement reflecting the commitments of both parties to a single contract based upon the expectation of service (e.g. in and out triggers).

Blockchain, as a middleware solution, is a form of intermediary supplement to a peer-based transaction dynamics and information exchange system that has remained functional as a competent security platform. Proprietary and heterogeneity technologies will expand to modify the abilities and scope of the IoT but this intermediary blockchain role has been accepted in many exploratory and experimental attempts for providing a substantial (immutability) benefit over previous structural restrictions and limitations. Therefore, the independent transaction nature will be system-defined by reducing human intervention risk from the information exchange platform to support the IoT, thereby restricting the potential for malicious or opportunistic security threats, and precipitating a more trustworthy and adaptable solution for smart city integration.

Limitations

There is a need to appreciate the contributions of this SLR, particularly after taking into account its limitations. The current SLR has confined its scope of the review to articles focusing on prior structural limitations in the comprehensively specified sectors, particularly embracing a large volume of literature on the Blockchain. It is also acknowledged that the search was done till Aug 2019 and the manual screening process of filtering thousands of articles down to a selected range introduces subjectivity. In this regard, high-quality articles could have been excluded. Finally, SLR requires ample time to collect large volumes of data and pursue an empirical analysis to address the research question adequately. This SLR has selected the sufficiently explicit and authentic series of articles for supporting the results.

Future Work

The preference to merge the data management standard precipitates the decentralization of smart city-data. The interoperability of the distributed nodes consisting of IoT will be truncated regardless of standardized and middleware proprietary technologies, firewalled databases, and restrictive algorithms. Blockchain is viewed in the proposed solution as the intermediary node at both the receiving and sending ends of this chain in an infinite loop consisting of infinite external nodes. The integrated potential for smart city applications is navigated by continuing the omnidirectional mechanism of secured and authenticated information beyond proprietary technologies' network restrictions. Future research will investigate this theoretical postulation by comparing integrated associations across objective-built APIs and service management firms for predicting the mutual efficiency of a standardized protocol for network alliance. There are several implications of this work that can be further investigated. In the first place, it will be interesting to organize more blockchain use cases that are executed in the industry for the application-oriented use case review. This will allow comparing the executed use cases and identifying the benefit provided by the research and industry through a strict association. In IoT networks, security has been asserted as a stressing need for the industry and has received the optimum enhancement and adoption preference.

However, there is a lack of evidence regarding the factors associated with decisions and feasibility for adopting this technology and existing IoT security threats or risks in an apparent context, which allow to imagine and then create future vectors in this particular domain. At the macro-sector level, the existing association of the application level can review the sustainable frameworks in the second place. The research related to IoT security using blockchain technologies usually commented on power consumption and network latency for maintaining the distributed network. For this review paper, it was impossible to estimate such data due to differentiability in solutions adopted by each researchers' cohort. Future research can explore the more micro-level interactions between the specific urban sustainability, blockchain use cases, and smart city framework indicators.

List Of Abbreviations

BaaS Blockchain as a Service

GIS Geographic Information System

IoT Internet of Things

PICO Problem, Intervention, Comparator, Outcome

PRISMA Preferred Reporting Items for Systematic Reviews and Meta-Analyses

QoL Quality of life

RFID Radio Frequency Identification

RQ Research Question

SLR	Systematic Literature Review
WoS	Web of Science

Declarations

Availability of data and materials

The datasets used and analysed during the current study are available at Appendix A and from the corresponding author on reasonable request.

Competing Interest

This research holds no conflict of interest

Funding

This research is partially funded by FRGS (grant no. FP071-2019A).

Author Contributions

All authors participated.

Acknowledgement

The author is very thankful to all the associated personnel in any reference that contributed to/for this research.

Authors' information

NADA ALASBALI is a Ph.D. candidate at Faculty of Computer Science and Information Technology (FSCIT), University of Malaya (UM). Her research interests include Internet of Things, smart cities and blockchain integration.

ROSLI BIN SALLEH received the B.S. degree in computer science from the University of Malaya, Malaysia, in 1994, and the M.Sc. and Ph.D. degrees from the University of Salford, U.K., in 1997 and 2001, respectively. Since 2001, he has been a Lecturer with the Department of Computer System and

Technology, Faculty of Computer Science and Information Technology, University of Malaya. He was appointed as a Senior Lecturer in 2007 and an Associate Professor in 2013. His research interests include SDN, mobile IPv6 handover and security, botnet, and wireless sensor networks.

SAAIDAL RAZALLI BIN AZZUHRI received the Ph.D. degree from the University of Queensland, Australia, in wireless network system, specializing in wireless ad-hoc routing protocol. His current research focuses on microfiber laser, wireless network protocols, blockchain, and autonomous unmanned aerial vehicle (UAV).

MISS LAIHA MAT KIAH joined the Faculty of Computer Science and Information Technology, University of Malaya, Malaysia as a tutor in 1997. She was appointed as a lecturer in 2001. She received her BSc. (Hons) in Computer Science from the University of Malaya in 1997, a MSc from Royal Holloway, University of London, UK in 1998 and a Ph.D. also from Royal Holloway, University of London in 2007. She is a full Professor at the Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya. Since 2008, she has been actively doing research particularly in the Security area of Computing and Networking. Amongst of her research grants were a High-Impact Research Grant by the Ministry of Higher Education, Malaysia in 2012 for duration of 4 years, working on secure framework for Electronic Medical Records, and a eScience grant by the Ministry of Science, Technology and Innovation in 2013 for the duration of 3 years, working on Secure Group Communication for Critical National Information Infrastructure (CNII). Her current research interests include Cyber Security, IoT and Cryptography.

References

1. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," Digital Communications and Networks, Feb. 2019.
2. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Nov. 2016.
3. K. Lo, Y. Liu, S. Y. Chia, X. Xu, Q. Lu, L. Zhu, and H. Ning, "Analysis of Blockchain Solutions for IoT: A Systematic Literature Review," IEEE Access, vol. 7, pp. 58822–58835, 2019.
4. Shen and F. Pena-Mora, "Blockchain for Cities—A Systematic Literature Review," IEEE Access, vol. 6, pp. 76787–76819, 2018.
5. W. S. Ruhlandt, "The governance of smart cities: A systematic literature review," Cities, vol. 81, pp. 1–23, Nov. 2018.
6. Leka, B. Selimi, and L. Lamani, "Systematic Literature Review of Blockchain Applications: Smart Contracts," 2019 International Conference on Information Technologies (InfoTech), Sep. 2019.
7. R. Andrian, N. B. Kurniawan, and Suhardi, "Blockchain Technology and Implementation: A Systematic Literature Review," 2018 International Conference on Information Technology Systems and Innovation (ICITSI), Oct. 2018. Doi: doi.org/10.1109/icitsi.2018.8695939

8. Daneva and B. Lazarov, "Requirements for smart cities: Results from a systematic review of literature," 2018 12th International Conference on Research Challenges in Information Science (RCIS), May 2018. Doi: doi.org/10.1109/rcis.2018.8406655
9. Chauhan, N. Agarwal, and A. K. Kar, "Addressing big data challenges in smart cities: a systematic literature review," info, vol. 18, no. 4, pp. 73–90, Jun. 2016. Doi: doi.org/10.1108/info-03-2016-0012
10. Khalid S Khan, Regina Kunz, Jos Kleijnen, and Gerd Antes. 2003. Five steps to conducting a systematic review. Journal of the Royal Society of Medicine 96, 3 (2003), 118–121.
11. Barbara A Kitchenham. 2007. Guidelines for performing systematic literature reviews in software engineering. In Technical report, Ver. 2.3 EBSE Technical Report. EBSE.
12. Sebastian K Boell and Dubravka Cecez-Kecmanovic. 2015. On being systematic in literature reviews in IS. Journal of Information Technology 30, 2 (2015), 161–173.
13. Michael Bacon. 2012. Pragmatism: an introduction. Polity Press, Malden, MA.
14. Almirall, J. Wareham, C. Ratti, P. Conesa, F. Bria, A. Gaviria, and A. Edmondson, "Smart Cities at the Crossroads," California Management Review, vol. 59, no. 1, pp. 141–152, Nov. 2016. Doi: doi.org/10.1177/0008125616683949
15. Lazaroiu and M. Roscia, "Smart district through IoT and Blockchain," 2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA), Nov. 2017. Doi: doi.org/10.1109/icrera.2017.8191102
16. Lv, B. Hu, and H. Lv, "Infrastructure Monitoring and Operation for Smart Cities Based on IoT System," IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 1957–1962, Mar. 2020. Doi: https://doi.org/10.1109/tii.2019.2913535
17. Kitchenham, "Procedure for Performing Systematic Reviews," Keele University Technical Report. 2004.
18. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," Telematics and Informatics, vol. 36, pp. 55–81, 2019.
19. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," Future Generation Computer Systems, vol. 86, pp. 650–655, Sep. 2018. Doi: doi.org/10.1016/j.future.2018.04.060
20. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," Computers & Security, vol. 78, pp. 126–142, Sep. 2018. Doi: doi.org/10.1109/wcnc.2018.8376948
21. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City," IEEE Access, vol. 7, pp. 18611–18621, 2019. Doi: doi.org/10.1109/access.2019.2896065
22. Fayad, B. Hammi, and R. Khatoun, "An adaptive authentication and authorization scheme for IoT's gateways: a blockchain based approach," 2018 Third International Conference on Security of Smart

Cities, Industrial Control System and Communications (SSIC), Oct. 2018. Doi: doi.org/10.1109/ssic.2018.8556668

23. , Bittner, and I. Spence, Manging Iterative Software Development Projects. Boston, MA: Pearson Education. 2007.
24. 'PICO Ontology.' Cochrane, 2019. Available At: https://linkeddata.cochrane.org/pico-ontology.
25. , Wu, T.J., Lu, F.Y., Ling, J., Sun, and H.Y. Du, "Research on the architecture of the internet of things," *IEEE*, 2010, 1-5.
26. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," 2012 10th International Conference on Frontiers of Information Technology, Dec. 2012. Doi: doi.org/10.1109/fit.2012.53
27. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," International Journal of Computer Applications, vol. 111, no. 7, pp. 1–6, Feb. 2015. Doi: doi.org/10.5120/19547-1280
28. Almirall, J. Wareham, C. Ratti, P. Conesa, F. Bria, A. Gaviria, and A. Edmondson, "Smart Cities at the Crossroads," California Management Review, vol. 59, no. 1, pp. 141–152, Nov. 2016. Doi: doi.org/10.1177/0008125616683949
29. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, and Y. Jin, "Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice," Journal of Hardware and Systems Security, vol. 2, no. 2, pp. 97–110, May 2018. Doi: doi.org/10.1007/s41635-017-0029-7
30. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, May 2018. Doi: doi.org/10.1016/j.future.2017.11.022
31. He, Y. Xu, Z. Liu, J. He, Y. Sun, and R. Zhang, "A privacy-preserving Internet of Things device management scheme based on blockchain," International Journal of Distributed Sensor Networks, vol. 14, no. 11, p. 1-12, 155014771880875, Nov. 2018. Doi: doi.org/10.1177/1550147718808750
32. Casado-Vara, P. Chamoso, F. De la Prieta, J. Prieto, and J. M. Corchado, "Non-linear adaptive closed-loop control system for improved efficiency in IoT-blockchain management," Information Fusion, vol. 49, pp. 227–239, Sep. 2019. Doi: doi.org/10.1016/j.inffus.2018.12.007
33. Dorri, S. S. Kanhere, and R. Jurdak, "MOF-BC: A memory optimized and flexible blockchain for large scale networks," Future Generation Computer Systems, vol. 92, pp. 357–373, Mar. 2019. Doi: doi.org/10.1016/j.future.2018.10.002
34. Bruneo, S. Chillari, S. Distefano, M. Giacobbe, A. Longo Minnolo, F. Longo, G. Merlino, D. Mulfari, A. Panarello, G. Patane, A. Puliafito, C. Puliafito, M. Scarpa, N. Tapas, and G. Visalli, "Building a Smart City Service Platform in Messina with the #SmartME Project," 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), May 2018. Doi: doi.org/10.1109/waina.2018.00109
35. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," Future Generation Computer Systems, vol. 88, pp. 173–190, Nov.

2018. Doi: doi.org/10.1016/j.future.2018.05.046

36. Lazaroiu and M. Roscia, "Smart district through IoT and Blockchain," 2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA), Nov. 2017. Doi: doi.org/10.1109/icrera.2017.8191102
37. Qiao, S. Zhu, Q. Wang, and J. Qin, "Optimization of dynamic data traceability mechanism in Internet of Things based on consortium blockchain," International Journal of Distributed Sensor Networks, vol. 14, no. 12, p. 155014771881907, Dec. 2018.
38. W. Kravitz, "Transaction Immutability and Reputation Traceability: Blockchain as a Platform for Access Controlled IoT and Human Interactivity," 2017 15th Annual Conference on Privacy, Security and Trust (PST), Aug. 2017. Doi: doi.org/10.1109/pst.2017.00012
39. Hong, B. Hu, and Z. Sun, "Toward secure and accountable data transmission in Narrow Band Internet of Things based on blockchain," International Journal of Distributed Sensor Networks, vol. 15, no. 4, p. 155014771984272, Apr. 2019. Doi: doi.org/10.1177/1550147719842725
40. F. Zorzo, H. C. Nunes, R. C. Lunardi, R. A. Michelin, and S. S. Kanhere, "Dependable IoT Using Blockchain-Based Technology," 2018 Eighth Latin-American Symposium on Dependable Computing (LADC), Oct. 2018. Doi: doi.org/10.1109/ladc.2018.00010
41. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Dec. 2016. Doi: doi.org/10.1109/hpcc-smartcity-dss.2016.0198
42. Paul, P. Baidya, S. Sau, K. Maity, S. Maity, and S. B. Mandal, "IoT Based Secure Smart City Architecture Using Blockchain," 2018 2nd International Conference on Data Science and Business Analytics (ICDSBA), Sep. 2018. Doi: doi.org/10.1109/icdsba.2018.00045
43. Tedeschi, G. Piro, J. A. S. Murillo, N. Ignjatov, M. Pilc, K. Lebloch, and G. Boggia, "Blockchain as a service: Securing bartering functionalities in the H2020 symbIoTe framework," Internet Technology Letters, vol. 2, no. 1, p. e72, Sep. 2018.
44. Kshetri, "Can Blockchain Strengthen the Internet of Things?," I.T. Professional, vol. 19, no. 4, pp. 68–72, 2017.
45. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," Procedia Computer Science, vol. 132, pp. 1815–1823, 2018.
46. Gallo, S. Pongnumkul, and U. Quoc Nguyen, "BlockSee: Blockchain for IoT Video Surveillance in Smart Cities," 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe), Jun. 2018.
47. Ouida, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: a new Blockchain-based access control framework for the Internet of Things," Security and Communication Networks, vol. 9, no. 18, pp. 5943–5964, Dec. 2016.
48. J. A. Pinno, A. R. A. Grégio, and L. C. E. De Bona, "ControlChain: A new stage on the IoT access control authorization," Concurrency and Computation: Practice and Experience, p. e5238, Mar. 2019.

49. Yang, Z. Lu, and J. Wu, "Smart-toy-edge-computing-oriented data exchange based on blockchain," Journal of Systems Architecture, vol. 87, pp. 36–48, Jun. 2018.
50. Li, S. Bahramirad, A. Paaso, M. Yan, and M. Shahidehpour, "Blockchain for decentralized transactive energy management system in networked microgrids," The Electricity Journal, vol. 32, no. 4, pp. 58–72, May 2019.
51. Li, W. Yang, P. He, C. Chen, and X. Wang, "Design and management of a distributed hybrid energy system through smart contract and blockchain," Applied Energy, vol. 248, pp. 390–405, Aug. 2019.
52. O'Connor C. What Blockchain means for the Internet of Things. Internet of Things Blog., https://www.IBM.com/blogs/internet-of-things/watson-iot-blockchain. 2016.
53. Morrison, "Blockchain and smart contract automation: How smart contracts automate digital business", Defense University of PLA, Beijing. 2016 Mar;100091.
54. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," IEEE EUROCON 2017 -17th International Conference on Smart Technologies, Jul. 2017. Doi: https://doi.org/10.1109/eurocon.2017.8011213
55. Jamali, A. Abdul Rahman, P. Boguslawski, P. Kumar, and C. M. Gold, "An automated 3D modeling of topological indoor navigation network," GeoJournal, vol. 82, no. 1, pp. 157–170, Sep. 2015. Doi: https://doi.org/10.1007/s10708-015-9675-x
56. Pahl, N. El Ioini, S. Helmer, and B. Lee, "A semantic pattern for trusted orchestration in IoT edge clouds," Internet Technology Letters, vol. 2, no. 3, p. e95, Apr. 2019.
57. Reilly, M. Maloney, M. Siegel, and G. Falco, "An IoT Integrity-First Communication Protocol via an Ethereum Blockchain Light Client," 2019 IEEE/ACM 1st International Workshop on Software Engineering Research & Practices for the Internet of Things (SERP4IoT), May 2019.
58. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. Guizani, "Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges," IEEE Network, vol. 34, no. 1, pp. 8–14, Jan. 2020. Doi: https://doi.org/10.1109/mnet.001.1900178
59. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT," Sensors, vol. 19, no. 2, p. 326, Jan. 2019. Doi: https://doi.org/10.3390/s19020326
60. Dekhane, K. Mhalgi, K. Vishwanath, S. Singh, and N. Giri, "GreenCoin: Empowering smart cities using Blockchain 2.0," 2019 International Conference on Nascent Technologies in Engineering (ICNTE), Jan. 2019. Doi: https://doi.org/10.1109/icnte44896.2019.8946014
61. Barlow, Smart Cities, Smarter Citizens. Sebastpol, CA: O'Reilly Media, 2017.
62. Stone, J. Knaper, G. Evans, E. Aravopoulou, Information management in the smart city. The Bottom Line, 2018;31(¾):214-249.
63. G. H. AL Zamil, S. Samarah, M. Rawashdeh, A. Karime, and M. S. Hossain, "Multimedia-oriented action recognition in Smart City-based IoT using multilayer perceptron," Multimedia Tools and Applications, vol. 78, no. 21, pp. 30315–30329, 2019. Doi: https://doi.org/10.1007/s11042-018-6919-z

64. Ibba, A. Pinna, M. Seu, and F. E. Pani, "CitySense," Proceedings of the XP2017 Scientific Workshops on – XP 17, 2017. Doi: https://doi.org/10.1145/3120459.3120472
65. Haleem, A. Allen, A. Thompson, M. Nijadam, R. Garg, Helium: A Decentralized Wireless Network. Helium, 2018. http://whitepaper.helium.com/.
66. Popov, The Tangle. Iota, 2018. https://www.iota.org/research/academic-papers.
67. K. Zheng, L. H. Zhu, M. Shen, F. Gao, C. Zhang, Y. D. Li, J. Yang, Scalable and Privacy-Preserving Data Sharing Based on Blockchain. Journal of Computer Science and Technology, 2018;33(3): 557-567.
68. Paul and R. Jeyaraj, "Internet of Things: A primer," Human Behavior and Emerging Technologies, vol. 1, no. 1, pp. 37–47, Jan. 2019. Doi: https://doi.org/10.1002/hbe2.133
69. Jiang, C. Wang, Y. Wang, and L. Gao, "A Cross-Chain Solution to Integrating Multiple Blockchains for IoT Data Management," Sensors, vol. 19, no. 9, p. 2042, May 2019. Doi: https://doi.org/10.3390/s19092042
70. Wissner, "The Smart Grid – A saucerful of secrets?," Applied Energy, vol. 88, no. 7, pp. 2509–2518, Jul. 2011. Doi: https://doi.org/10.1016/j.apenergy.2011.01.042
71. Bertoldo, M. Poumadère, and L. C. Rodrigues Jr., "When meters start to talk: The public's encounter with smart meters in France," Energy Research & Social Science, vol. 9, pp. 146–156, Sep. 2015. Doi: https://doi.org/10.1016/j.erss.2015.08.014
72. Cilfone, L. Davoli, L. Belli, and G. Ferrari, "Wireless Mesh Networking: An IoT-Oriented Perspective Survey on Relevant Technologies," Future Internet, vol. 11, no. 4, p. 99, Apr. 2019. Doi: https://doi.org/10.3390/fi11040099
73. Malandra and B. Sansò, "Performance Evaluation of Large-scale RF-Mesh Networks in a Smart City Context," Mobile Networks and Applications, vol. 23, no. 4, pp. 912–920, Nov. 2017. Doi: https://doi.org/10.1007/s11036-017-0958-y
74. Sun, J. Yan, and K. Z. K. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities," Financial Innovation, vol. 2, no. 1, Dec. 2016. Doi: https://doi.org/10.1186/s40854-016-0040-y
75. H. Chen, K. R. Lo, "Application of Internet of Things." International Journal of Geo-Information, 2018;7:1-6.
76. Kundu, "Blockchain and Trust in a Smart City," Environment and Urbanization ASIA, vol. 10, no. 1, pp. 31–43, Mar. 2019. Doi: https://doi.org/10.1177/0975425319832392
77. Juskalian, "Inside the Jordan Refugee Camp That Runs on Blockchain." MIT Technology Review, 2018, https://www.technologyreview.com/s/610806/inside-the-jordan-refugee-camp-that-runs-on-blockchain/.
78. Wokye, "Blockchain is Helping Build a New Kind of Energy Grid." MIT Technology Review, 2017, https://www.technologyreview.com/s/604227/blockchain-is-helping-to-build-a-new-kind-of-energy-grid/.

79. Copeland, "Blockchain Powers a Personal Data Revolution." DECODE, 2017, https://decodeproject.eu/blog/blockchain-powers-personal-data-revolution.
80. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City," IEEE Access, vol. 7, pp. 18611–18621, 2019. Doi: https://doi.org/10.1109/access.2019.2896065
81. Pahl, N. EL Ioini, and S. Helmer, "A Decision Framework for Blockchain Platforms for IoT and Edge Computing," Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security, 2018. Doi: https://doi.org/10.5220/0006688601050113
82. Shukla and N. Shukla, "Smart Waste Collection System based on IoT (Internet of Things): A Survey," International Journal of Computer Applications, vol. 162, no. 3, pp. 42–44, Mar. 2017. Doi: https://doi.org/10.5120/ijca2017913381
83. Lv, B. Hu, and H. Lv, "Infrastructure Monitoring and Operation for Smart Cities Based on IoT System," IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 1957–1962, Mar. 2020. Doi: https://doi.org/10.1109/tii.2019.2913535
84. Sharmin and S. T. Al-Amin, "A Cloud-based Dynamic Waste Management System for Smart Cities," Proceedings of the 7th Annual Symposium on Computing for Development, Nov. 2016. Doi: https://doi.org/10.1145/3001913.3006629
85. Akhter, S. Khadivizand, H. R. Siddiquei, M. E. E. Alahi, and S. Mukhopadhyay, "IoT Enabled Intelligent Sensor Node for Smart City: Pedestrian Counting and Ambient Monitoring," Sensors, vol. 19, no. 15, p. 3374, Aug. 2019. Doi: https://doi.org/10.3390/s19153374
86. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. Imran, "Securing IoTs in distributed blockchain: Analysis, requirements and open issues," Future Generation Computer Systems, vol. 100, pp. 325–343, Nov. 2019. Doi: https://doi.org/10.1016/j.future.2019.05.023
87. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "IoT information sharing security mechanism based on blockchain technology," Future Generation Computer Systems, vol. 101, pp. 1028–1040, Dec. 2019. Doi: https://doi.org/10.1016/j.future.2019.07.036
88. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," Future Generation Computer Systems, vol. 97, pp. 512–529, Aug. 2019. Doi: https://doi.org/10.1016/j.future.2019.02.060
89. i, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, "Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues," IEEE Access, vol. 6, pp. 1513–1524, 2018. Doi: https://doi.org/10.1109/access.2017.2779263
90. C. Snow, D. D. Håkonsson, and B. Obel, "A Smart City Is a Collaborative Community," California Management Review, vol. 59, no. 1, pp. 92–108, Nov. 2016. Doi: https://doi.org/10.1177/0008125616683954
91. Vermesan, A. Broring, E. Tragos, M. Serrano, D. Bacciu, S. Chessa, "Internet of Robotic Things: Converging Sensing/Actuating, Hyperconnectivity, Artificial Intelligence, and IoT Platforms. In:

Vermesan, O., Bacquet, J. (Eds.) Cognitive Hyperconnected Digital Transformation: Internet of Things Intelligence Evolution. Gistrup: River Publishers, 2017; 97-155.

92. Hadar, S. Siboni, and Y. Elovici, "A Lightweight Vulnerability Mitigation Framework for IoT Devices," Proceedings of the 2017 Workshop on Internet of Things Security and Privacy – IoTS & P '17, 2017. Doi: https://doi.org/10.1145/3139937.3139944

Tables

Table 1: Research Questions and their Rationales

Research Question (R.Q.)	Rationale
RQ1. How much progress has been made in securing and protecting IoT-based integration into the smart city solution?	To assess the technical feasibility of blockchain-supported IoT integration in smart city applications.
RQ2. What role could Blockchain play in serving as a unified, central database and transaction ledger for IoT-based triggers?	To critically assess the central goals and technologies related to smart city applications and digital solutions.
RQ3. What are the advantages (and limitations) of blockchain integration within smart city applications?	To analyse the technological opportunities and limitations of IoT-related capabilities concerning the current standard of practice.
RQ4. Which components of the smart city solution can be standardized, and which elements will remain proprietary?	To assess the viability of blockchain-supported IoT solutions while considering an intermediary authentication ledger's applicability to support smart city scalability.
RQ5. Which structural limitations or challenges will prevent blockchain integration, and how could these problems be resolved?	To assess the factors restricting or limiting blockchain integration and to analyse the extant solutions and alternative models.

Table 2: Search Databases

Organization	Database	URL
Clarivate	Web of Science	https://webofknowledge.com/
Elsevier	Science Direct	http://www.sciencedirect.com/
IEEE	Xplore	http://ieeexplore.ieee.org/Xplore/
Sage Group	Sage	https://journals.sagepub.com/
Taylor & Francis Group	Taylor & Francis	https://www.tandfonline.com/
Wiley	Wiley Online Library	https://onlinelibrary.wiley.com/

Table 3: Inclusion-Exclusion Criteria

Inclusion	Exclusion
· Studies published from January 1, 2016, till Aug 2019	· Studies published before 2016
· Experimental research with targeted model	· Non-experimental research or failure to include model or design
· Include blockchain and smart city solutions	· Only Blockchain or only smart city
· IoT-oriented or indicative	· No consideration for IoT
· Peer-reviewed journal or legitimate academic conference	· Non-peer reviewed or small-scale study (e.g., blog post, non-academic conference)
· Realistic or practical application	· Unrealistic, non-translational application or model

Table 4: PICO(S) Framework for Study Selection

PICO(S)	Inclusion Criteria	Exclusion Criteria
Problem	Blockchain AND IoT AND Smart City	Individual emphasis on keywords or focus outside of the immediate context
Intervention	Experimental, Model-Oriented, Inclusive	Non-Experimental, Outlaying, Exploratory, Conceptual
Comparator	Underlying Purpose Related to Smart City Applications	Underlying Purpose Related to Other Applications
Outcomes	Proposed Model or Contributory Solution	Revised Concept, Future Research Recommendations
Study Design	Experimental, Architectural, Non-Proprietary	Proprietary, Empirical, Application-Limited

Table 5: Summary Output of Article Identification and Selection Process

Database: Science Direct					
Search Date	**Keyword/s**	**Total Articles**	**Journal Publications**	**Relevant Articles**	**Included**
May-Jun, 2019	Blockchain AND (Smart City OR Smart Cities)	372	206	14	8
	Blockchain AND (Internet of Things OR IoT)	724	426		
	(Internet of Things OR IoT) AND (Smart City OR Smart Cities)	4283	2955		
	Blockchain AND (Smart City OR Smart Cities) AND (Internet of Things OR IoT)	277	154		
Database: Taylor and Francis					
Search Date	**Keyword/s**	**Total Articles**	**Journal Publications**	**Relevant Articles**	**Included**
June-July, 2019	Blockchain AND (Smart City OR Smart Cities)	66	66	0	0
	Blockchain AND (Internet of Things OR IoT)	154	150		
	(Internet of Things OR IoT) AND (Smart City OR Smart Cities)	3,128	3,000		
	Blockchain AND (Smart City OR Smart Cities) AND (Internet of Things OR IoT)	34	25		
Database: IEEE Xplore					
Search Date	**Keyword/s**	**Total Articles**	**Journal Publications**	**Relevant Articles**	**Included**
June-July, 2019	Blockchain AND (Smart City OR Smart Cities)	124	10	8	6
	Blockchain AND (Internet of Things OR IoT)	670	94		
	(Internet of Things OR IoT) AND (Smart City OR Smart Cities)	2,362	296		
	Blockchain AND (Smart City OR Smart Cities) AND (Internet of Things OR IoT)	62	3		
Database: Wiley					
Search Date	**Keyword/s**	**Total Articles**	**Journal Publications**	**Relevant Articles**	**Included**
July, 2019	Blockchain AND (Smart City OR Smart Cities)	148	74	4	4

	Blockchain AND (Internet of Things OR IoT)	234	94		
	(Internet of Things OR IoT) AND (Smart City OR Smart Cities)	948	441		
	Blockchain AND (Smart City OR Smart Cities) AND (Internet of Things OR IoT)	85	41		
Database: Sage					
Search Date	**Keyword/s**	**Total Articles**	**Journal Publications**	**Relevant Articles**	**Included**
July, 2019	Blockchain AND (Smart City OR Smart Cities)	38	30	10	4
	Blockchain AND (Internet of Things OR IoT)	41	34		
	(Internet of Things OR IoT) AND (Smart City OR Smart Cities)	276	225		
	Blockchain AND (Smart City OR Smart Cities) AND (Internet of Things OR IoT)	17	13		
Database: Web of Science					
Search Date	**Keyword/s**	**Total Articles**	**Journal Publications**	**Relevant Articles**	**Included**
July-Aug, 2019	Blockchain AND (Smart City OR Smart Cities)	129	46	11	4
	Blockchain AND (Internet of Things OR IoT)	641	278		
	(Internet of Things OR IoT) AND (Smart City OR Smart Cities)	3437	1274		
	Blockchain AND (Smart City OR Smart Cities) AND (Internet of Things OR IoT)	67	27		

Figures

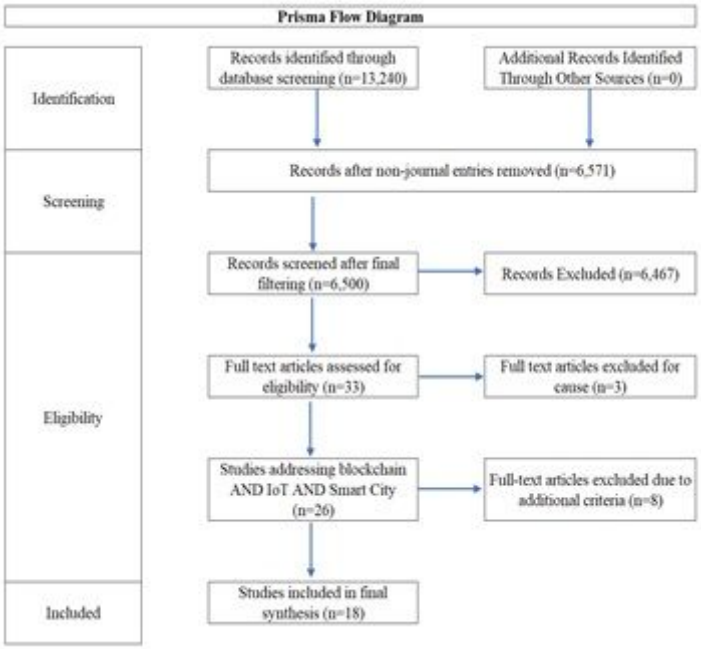

Figure 1

PRISMA Flow Diagram

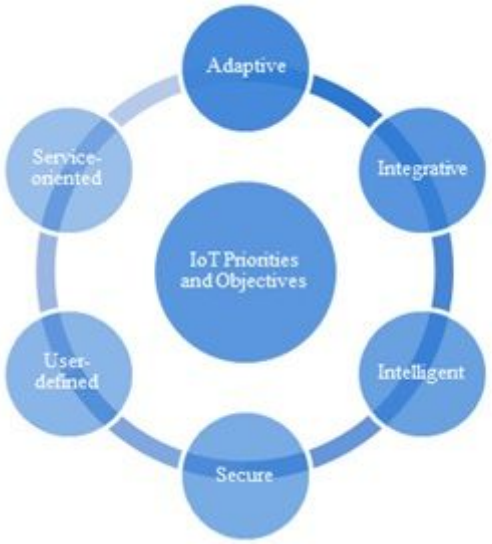

Figure 2

Summary Representation of IoT Priorities and Objectives

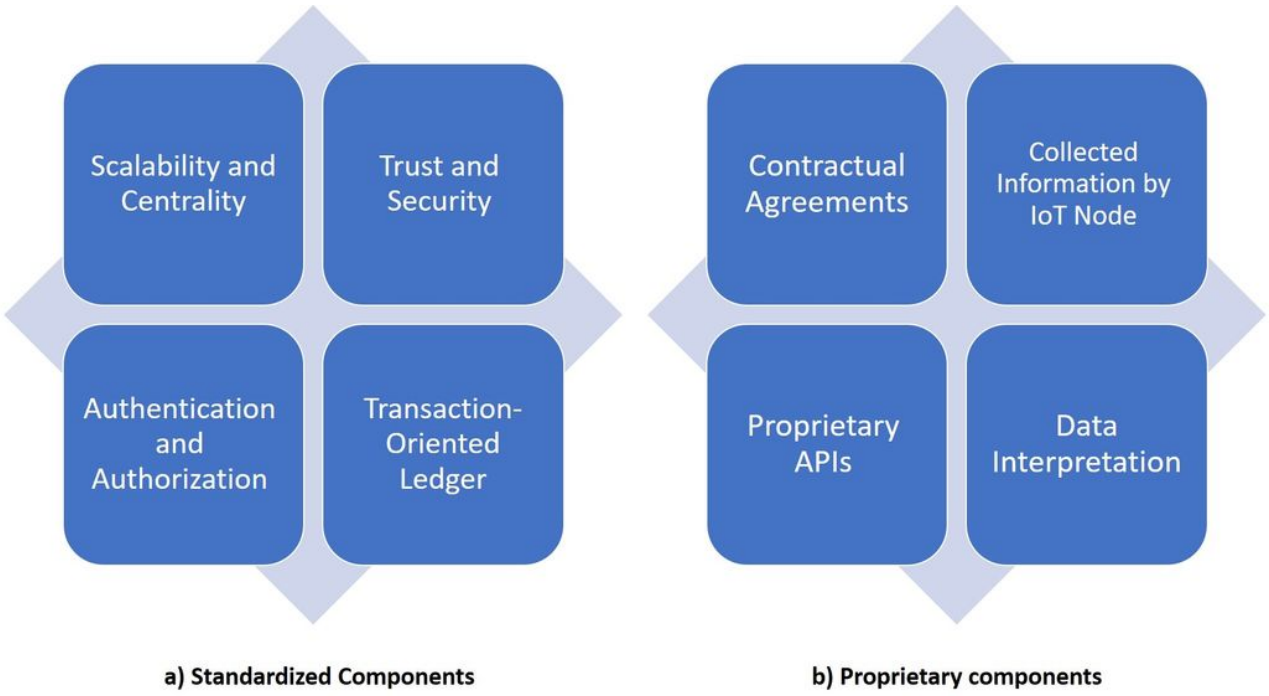

Figure 3

(a) Standardized Components versus (b) Proprietary Components of Blockchain Solution

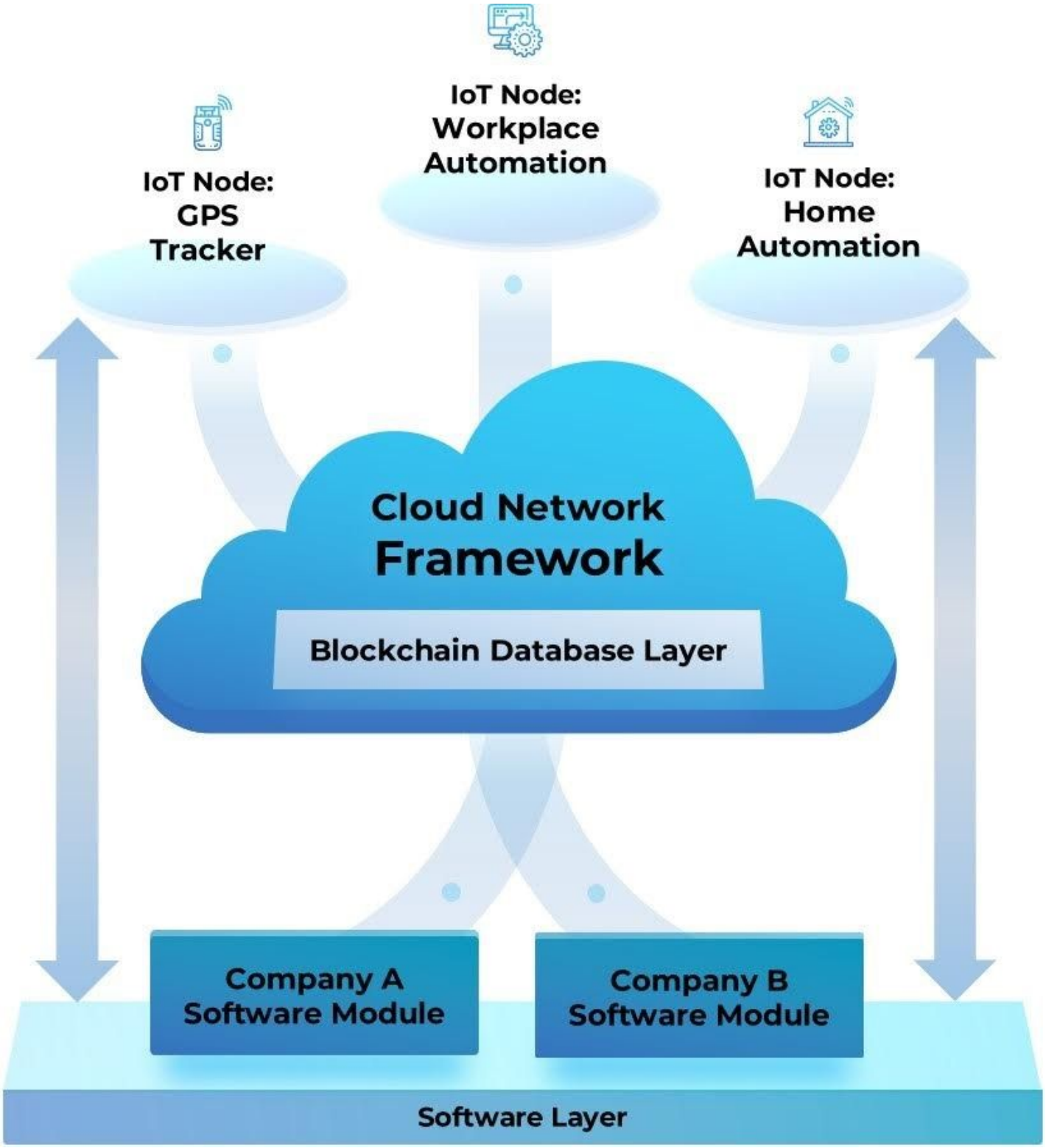

Figure 4

Standardized Blockchain Middleware Solution

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- AppendixA.pdf