Hindawi
Mobile Information Systems
Volume 2022, Article ID 9109300, 11 pages
https://doi.org/10.1155/2022/9109300

Research Article

Rules of Smart IoT Networks within Smart Cities towards Blockchain Standardization

Nada Alasbali,[1,2] **Saaidal Razalli Bin Azzuhri**,[1] **Rosli Bin Salleh**,[1] **Miss Laiha Mat Kiah**,[1] **Ahmad Aliff A. S. Ahmad Shariffuddin**,[3] **Nik Muhammad Izwan bin Nik Mohd Kamel**,[3] **and Leila Ismail**[4]

[1]*Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia*
[2]*College of Computer Science, King Khalid University, Abha, Saudi Arabia*
[3]*Ifcon Technology Sdn Bhd, Kuala Lumpur, Malaysia*
[4]*Intelligent Distributed Computing and Systems Research Laboratory, Department of Computer Science and Software Engineering, College of Information Technology, United Arab Emirates University, Al Ain, Abu Dhabi 15551, UAE*

Correspondence should be addressed to Saaidal Razalli Bin Azzuhri; saaidal@um.edu.my

Received 20 December 2021; Revised 10 January 2022; Accepted 17 January 2022; Published 23 February 2022

Academic Editor: Hasan Ali Khattak

Motivation. Standardization in smart city applications is restricted by the competitive pressures of proprietary innovation and technological compartmentalization. Interoperability across networks, databases, and APIs is essential to achieving the smart objectives of technology-supported urban environments. *Methodology*. The issues that smart cities face, as well as the usage of blockchain in Internet of Things (IoT) applications, are discussed in this research paper. *Problem Statement*. The study shows the obstacles to the establishment of an IoT-driven smart city agenda, including system security, dispersed node interoperability, data resource management, and scalability of a diverse IoT network. *Results*. To resolve these challenges, this research proposes a working infinite loop model for establishing a standardized, intermediary cloud-based blockchain for IoT networking within smart cities. The blockchain intermediary function will resolve critical gaps in the existing, distributed IoT-based smart cities' standards, drawing connections between nodes, users, and service providers that are enabled through autonomous, immutable, and nonrepudiated transactions.

1. Introduction

The ability to create a fluid, adaptable, and information-rich smart city environment requires networked interdependencies. Iterative breakthroughs in the intersection of static and dynamic resources will revolutionize the breadth of technology-enhanced choices in networked urban environments, allowing for smart, behavior-aware, and data-rich transactions [1–3]. Despite these benefits, the competitive incentive for compartmentalized technological innovation has resulted in structural splits in the smart city ecosystem as proprietary modules, networks, and algorithms limit smart node interoperability and network-spanning information sharing [4, 5]. The interoperability as defined by IEEE 2030.5 Ecosystem Steering Committee (ESC) is "a quality of information and communications technology interfaces that enables two or more devices or systems to connect and successfully interact" [6]. Interoperability across networks, databases, and Application Programming Interfaces (APIs) is critical to realizing the smart goals of technology-enabled urban environments. The Internet of Things (IoT) is realizing a comprehensive technological goal of integrated, multinodal communication over scattered networks in these smart cities and through lightweight, low-power, and multifunction gadgets [3].

With various devices collecting usage, behavior, and environmental data, the ability to mine and interpret these data resources is limited due to a lack of interoperability

between proprietary platforms [7]. Economically speaking, IoT is an efficient source of economic profits, which is continuously evolving and growing [8]. Fernández-Caramés and Fraga-Lamas [9] have forecasted growth in Machine-to-Machine (M2M) connection in the coming years from 780 million devices in 2016 to 3.3 billion devices in 2021, which is related to its broad application in defense, transportation, public, safety, home automation, and more [10–12]. Consequently, the smart cities concept has significantly grown given the complex challenges aimed at improving the citizen's quality of life (QoL) and quality of service (QoS). In a report by the United Nations (UN), it is mentioned that there is more than half of the population resides in the urban areas, and an additional growth of 2.5 billion is expected by 2050 [13]. This increased urbanization has substantially affected the living conditions due to the increase in traffic jams, greenhouse gas emission, carbon dioxide, and waste disposal [14].

Some of the cities recognize themselves as smart based on their innovative applications and certain characteristics, including digital inclusion, broadband connectivity, and knowledge workforce [14]. Some examples of smart cities solutions are found globally. For instance, Tangle Technology in Germany is used for automated transportation system [15]. In Amsterdam, IoT application has improved energy conservation, traffic reduction, and security level [16], and in Barcelona, sensor technology is used for evaluating the traffic flow for designing new bus network [17, 18]. Moreover, in Korea, a smart street lighting system is used along with automated building [19] similar to Japan, Netherland, and England [20]. Previous studies have highlighted the benefits and application of the devices and few on the concerns related to smart city vulnerabilities [21–24]. The identification of the concerns related to smart cities is integral for recognizing potential threats. Likewise, Silva et al. [22] have also stressed on identifying the concerns related to smart cities for optimizing the benefits and making necessary improvements for future deployment. Kitchin [21] has also stated that studies have mostly focused on the technological development of the smart cities while neglecting the security and privacy issues when implementing smart city's solutions.

Moreover, Blockchain (BC) technology or Distributed Ledger Technology (DLT) as pointed by [25–27] is likely to change the way we live because it enables the implementation of decentralized, secure, privacy-preserving, and transparent transactions, increasing the trust in smart cities applications and consequently accelerating their adoption and use by citizens [28]. Previously, the database and networks were controlled by an intermediary; in BC, however, every member contributes to the network and serve as a control instance after the development [29]. BC application in the smart cities is proliferated due to its decentralized nature and potential for automation [21]. For example, Rizzo [30] adds that BC is likely to serve as an urban solution to the smart city problem as initiated in the "Smart Dubai" project, which aims to solve all its urban-related areas' problems (pollution, governance, resource shortages, or transportation). The problem of rapid growth management in a sustainable manner has increased due to the increase in the global population by 2050. Blockchain is likely to reshape the lives in diverse areas, including management in the country, consumption of energy, water management, patient-centric healthcare [31], and traffic handling [32]. Despite its vast scope, the application of the BC in the smart city remains surprisingly scarce [28].

The organization of this paper is as follows: the research aim is presented in Section 2 followed by materials and methods. Section 3 presents the research findings on basis of a comparative exploration of prior research, conceptual dynamics, and theoretical relationships related to three domains of smart city innovation, the IoT industry, and blockchain solutions. Then, we proposed a blockchain-based standard for IoT integration for smart cities in Section 4. Finally, we summarize the work contributions and conclude this research in Sections 5 and 6, respectively.

2. Research Aim

Smart city technology interoperability is being restricted by corporate commercial goals; hence, a unifying solution that connects IoT nodes across urban fabric is urgently needed to facilitate technological interoperability [13]. This research paper aims to critically examine the current level of progress in IoT-based smart city solutions and to provide a framework for blockchain integration into IoT-based smart city applications.

3. Research Findings

3.1. Smart City Solutions. The incorporation of smart city solutions in urban areas is evidence of the unsustainable and coordinated weight of human activity [33]. Given that the world's largest 600 cities will contribute to more than 60% of global GDP by 2025, efficient and integrated hubs of connected technical and informational resources are critical [33]. Almirall et al. [33] suggest that in order to achieve such goals, urban ecology must be substantially transformed by networked technologies that give access to and control over datasets throughout the human-system network. While the fabric of current urban areas is an enabler of communal action, Finger and Razaghi [34] contend that it is the complex and dynamic sociotechnical interface between individuals and systems that generates chances for smart, data-driven city characteristics. The concept of smart city ecology is based on the "pervasive penetration of cities by ICTs" (Information and Communication Technologies) as a system approach to the digitalization of the infrastructure nodes, connections, and interfaces essential for human-technology convergence [35]. While such definitions may eventually appear in the digital lifestyles of mobile device users or technological breakthroughs in ICT-connected vehicles, the entire ecological framework of the urban center determines the city's relative smartness or integrated nature. A richness of dynamic and static resources is regarded as underscoring the fundamental purpose of the smart city [36]. Stone et al. [36] propose that the technological underpinnings for most early-phase smart city applications are built on static data mining and information management resources, rather than the practical initiatives associated with

more dynamic network interactions. From the standpoint of development, this developing technology ecosystem is mapping the breadth of human-system interactions, identifying the scope of crucial nodes, triggers, and responses that will eventually appear in smart city design [37, 38].

Sun et al. [13] and Alasbali et al. [39, 40] recognize that smart cities must satisfy requirements of trust, accessibility, and security in order to provide efficient, high-value resources to the central user population. Snow et al. [38] note a formative collaboration of public and private organizations striving towards a singular, integrated objective by highlighting Aarhus, Denmark, as a modern, smart city repleted with integrated technologies and connections. The smart initiatives' holistic design was built on mutual benefits and network communications that are unified and feature a central database as well as outlying software-supported connection points and monitoring nodes [33]. Finger and Razaghi [34] argue that by acknowledging the simplistic constructs of smart cities' physical infrastructure layer, a broader spectrum of innovative, purposeful, and dynamic services can be developed that not only extend the reach of integrated technologies but also redefine the purposes and human-technology relationships that have evolved over time.

3.2. IoT and Smart Cities. Commonly, the Internet of Things is explained as a broad real-to-object with limited storage and processing capabilities. The goal of IoT for smart cities is to improve the infrastructure's performance, reliability, and security [8]. Figure 1 shows the conventional network architecture for data centers. In the presence of internet-enabled devices, information is perceived, detected, and collected. It also distributes data by way of an internet-based communications network to various devices. Global Positioning Systems, Radio Frequency Identification Devices, cameras, and sensors are a few examples. In terms of network capability and device limits, the network layer is in charge of moving data from the application layer's viewpoint. For transporting information from the perception device to the close by a gateway that utilizes communicative capabilities, it integrates into a combination of multiple short-range networks like ZigBee and Bluetooth. Wi-Fi, 4G, and Power Line Communication (PLC) are employed for longer data transfers [42].

3.3. IoT and the Network Advantage of Connectivity. Since the IoT is made up of autonomous nodes, it may fulfill specific demands or obligations based on input from users (both active and passive) [43]. Application, middleware, network, and perception all have hierarchical layers in the Internet of Things (IoT) architecture [43, 44]. Applications are implemented according to a wide range of situations at the application layer and data from the middleware layer is managed and processed [45, 46]. Using the network layer, the middleware layer gathers data, links the system to the cloud and database, performs data processing and storage, and offers the APIs required to meet application layer requests. As previously stated, this network layer is in charge of connecting the IoT infrastructure and collecting data from the perception layer, which is subsequently sent up the stack [46, 47].

Another study by Reilly et al. [48] indicated that the use of IoT aids in the sharing of critical information about urban infrastructure, which aids in the smooth operation of smart cities. Integrated communication is essential for establishing a secure urban environment and, eventually, preventing cyberattacks on smart cities. Furthermore, Pardini et al. [49] illustrated how cloud computing and the Internet of Things could help cities enhance waste management by enabling for the tracking of waste, containers, garbage deposit monitoring, and detecting high-demand areas. Almirall et al. [33] also discover a fragmented information governance and oversight framework that confines data resources to silos. Private firms impede the potential for city-wide integration and quick technoinnovation based on the IoT's cooperative and integrated potential by hoarding and restricting access to collected-IoT data. According to Chen et al. [43], the lack of integration and definitions support systems in IoT systems leads to functional and effectiveness gaps in the security architecture. Bruneo et al. [50] as shown in Figure 2 propose that output services can be integrated, reducing the dependency on proprietary networks. Emerging technologies, such as those presented by Collen et al. [51] and Alasbali et al. [39], anticipate an IoT standard that is secure and adaptable to changing ontologies of security threats by developing architectural solutions and data authentication standards that limit unauthorized access and automate information exchange.

Overlapping hardware solutions are being studied for IoT to be scalable and effective across big technology-supported networks. Historically, RFID tags provided a low-tech version of IoT connectivity, generating static nodes that maintained onboard information for sharing with device readers once sufficient authorizations were received [52]. A variety of network-connected technologies, such as 3G, LTE, Bluetooth, ZigBee, Z-Wave, and Sigfox, have been identified as scalable technological solutions that can be modified to the system's, users', and network's particular needs [52]. Virtual SIM or eSIM technologies, as a significant innovation in IoT connectivity, will enable the IoT to extend internationally, creating network connectivity that is scalable, mobile, and unregulated by network or service provider [49]. Such technologies require what Sachs et al. [53] refer to as redundant capillary networks, which use several gateways to transport data from mobile networks to the cloud. The benefit of these overlapping gateways is that they ensure that, regardless of network growth or technology advancements, slack built into the system design allows for adaptability and innovation throughout time [54]. Network communications can be regulated by automating gateway switching behavior, and a persistent state of connectivity will offer the quality of service (QoS) requirements required to fulfill long-term network solutions [54].

3.4. Challenges of IoT Data and Smart City Burden. Human actions are now being exposed to service providers and other unknown third-parties on an unprecedented scale

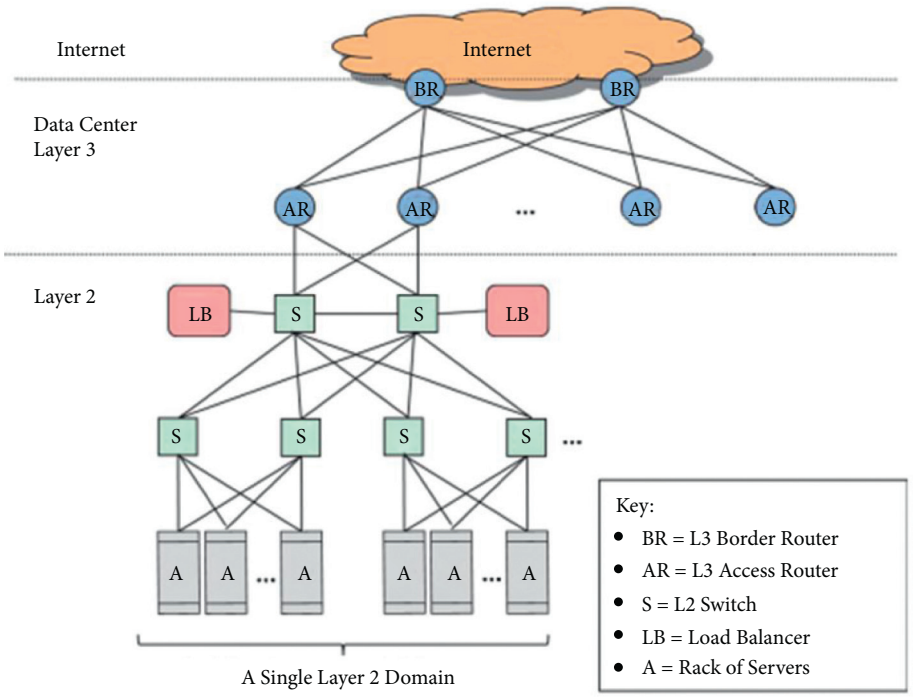

Figure 1: The conventional network architecture for data centers (source: [41]).

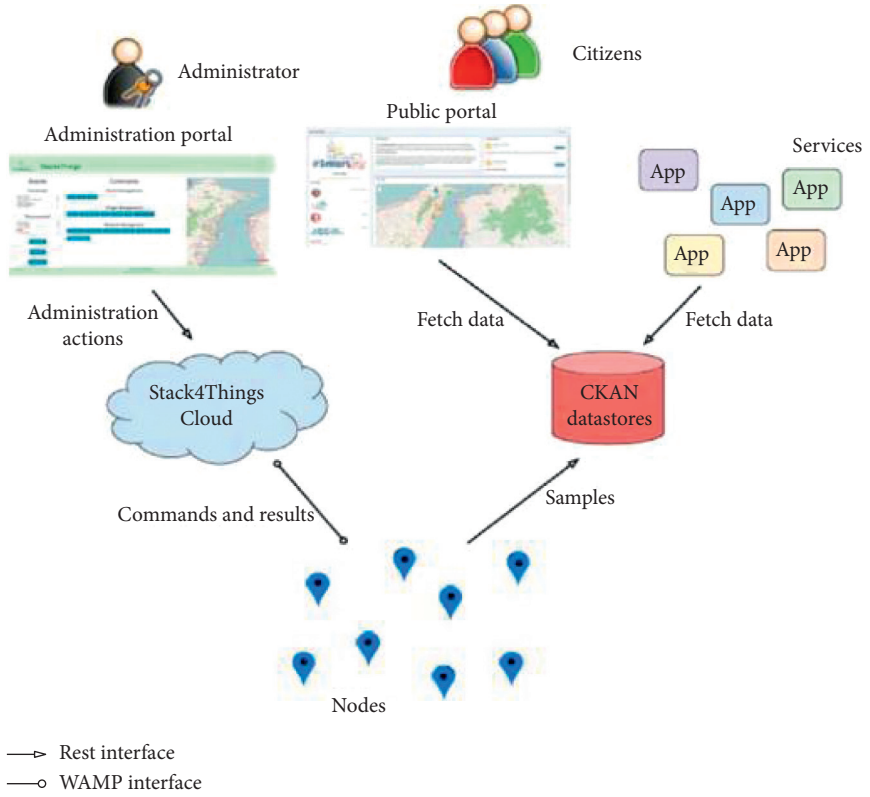

Figure 2: Proposed architecture of the smartme IoT network (source: [50]).

as a result of the emergence of big data mining. Given the importance of a smart city ecosystem's ability to mine and analyze user data, security and trust concerns connected to information security and user data rights are becoming more widespread [55, 56]. Interconnectivity, for example, might expose users' data to malicious attacks or unauthorized access through a plethora of interfaces and connecting points [57]. That is why trust-based certificates, which link

user activities to meaningful triggers and downstream network reactions, are critical in smart city security [55].

The application programming interface (API) is the software that translates user data into triggers and downstream actions [37]. However, as IoT data moves across the network and via the software suite, the danger of data corruption, unauthorized access, and malicious assaults increases, as these layers are exposed to a variety of accessibility and authorization concerns [36]. One feasible answer to the security needs for smart city interconnectivity is the creation of an encryption or encoding standard for network communication that eliminates plain text accessibility and corruptibility of user data. According to Shafagh and Hithnawi [57], smart networks can be secured in a predictable and trust-based manner by incorporating a database-level service capable of encrypting incoming and outgoing data. The Internet of Things (IoT) is fraught with security risks. Multilayer security interference is increasing in proportion to the network's size, exacerbated by a number of physical, access, and technology-based threats (e.g., DDoS attack).

The more connected an IoT device is, the more vulnerable human users are to data disclosure and third-party attacks [58]. However, from a communications perspective, this type of low-power wide area network (LPWAN) enables the development of a mesh network of IoTs within a dedicated regional space, enabling interoperability and cross-node communication based on proximity interactions (e.g., entering and exiting a space) or network-triggered stimuli (e.g., beginning a journey home) [59]. Numerous intermediary methods have been proposed to safeguard IoT-collected data. For example, Hadar et al. [60] have developed a security mitigation framework that consists of a lightweight IoT security appliance, a cloud-based service, and mechanisms for synchronization and communication. The problems that smart cities must overcome are summarized in Table 1.

3.5. BC and IoT Domains. The BC is essentially an electric ledger that includes a credit transaction for incoming data, a debit transaction for outgoing data, and an immutable, shared ledger transaction for the centralized database layer [67, 68]. One of the benefits of BC technology for IoT-based systems is its public or private nature, which allows for the participation of trusted or public players in validation and transaction processes [50]. Ibba et al. [4] offer a contractual database that measures and models behavioral data over time in an assessment of the practical benefits of BC in facilitating IoT connectivity and data management. This networked backbone for IoT-enabled nodes controls numerous information flow paths via acquisition and sorting contracts (ASCs) and geographical contracts (GCs), classifying datasets by typology, timestamps, and values [50]. At the nodes' periphery, data-specific APIs are then able to translate data flows into meaningful triggers or outputs, either by applying responses to individual IoT components or by creating smart models of behavioral patterns that can interpret demand, needs, and gaps over extended time periods [50]. Popov [68] examined the mathematical function of IOTA, a cryptocurrency used in the IoT market. It stores transaction details in a directed acyclic graph (DAG) and provides a novel and evolutionary approach to constructing machine-to-machine micropayment systems. On the other hand, Sagirlar et al. [69] proposed a hybrid BC architecture for the Internet of Things, which was found to be effective in addressing security issues. Li et al. [70] have presented a secure and authenticated IoT block chained paradigm. It implemented a Hyperledger Fabric-based prototyping system. The platform's low cost of ownership, its deployment on lightweight devices, and enhanced security protection all contribute to its implementation prospects. Jiang et al. [27] also presented a system for integrating various blockchains for the purpose of managing secure IoT data. This framework introduces a new type of control station that operates on a decentralized access approach. According to Jiang et al.'s [27] study, this framework consumes fewer resources and is simple to install across numerous consortia.

For the IoT, there are numerous central criteria for achieving the distributed, multinodal system's central security objectives, and information control requirements. Reference [67] argues that systems must protect the integrity of incoming and outgoing communications/transactions while also preserving data integrity by allowing only authorized users to access and save data on the database/ledger. Additionally, the blockchain-based IoT database's resources must be on demand and sufficiently scalable to maintain constant and predictable quality of service (QoS) across time [66]. Due to the fact that the blockchain solution is based on multiple layers of authentication, it is a mutually verifiable solution that not only ensures the security of IoT data exchange, but also enables the software to determine which nodes are communicating in accordance with the given system specifications/permissions [71].

The gap between conventional IoT solutions and blockchain innovation is evident across numerous critical aspects, including the trust model (decentralized), the level of security (high), and the underlying privacy controls (high) [72]. By routing IoT traffic through the distributed blockchain, the data's trustworthiness and immutability ensure that the underlying transactions' integrity and validity are verifiable [72]. Despite these benefits, there are some inherent hurdles to integrating blockchain technologies into the smart city ecosystem that must be addressed architecturally and systemically to enhance the possibility of success:

(i) Scalability: the blockchain solution's architecture will eventually decide the system's overall scalability [73].

(ii) Public versus private blockchain deployment: decisions about the blockchain's public versus private and permission versus permission-less status must be made in light of the smart city and IoT's underlying aims in order to achieve optimality [72].

(iii) Architecture: the architecture of the blockchain solution, which can range from entirely centralized

Table 1: Smart city challenges.

Challenges	Consequences	Reference
Security challenges in the smart city	Cyberattacks	[21, 23, 61]
	Lack of security testing	[23, 62]
	Inadequate knowledge and awareness	[63]
Privacy challenges in the smart city	Data sharing, data mining, mashup data	[62, 64]
	Location data	[21, 65]
	Big data	[23, 66]
Security and privacy challenge consequences	Critical systems	[62, 65]
	Datafication	[21]

to fully distributed, has an effect on the nature of data management and the reconciliation of edge device communications. A hybrid architecture including a core network based on proof-of-work blockchain technology and a second layer capable of refining and transferring IoT-collected data to the core network has been demonstrated to provide an efficient smart city solution [74].

(iv) Data management and storage: data collection and rationalization are essential functions of blockchain systems, as are optimal storage options [72]. The data storage system provided by Yu et al. [74] is based on Ethereum, although data management is only optimized for datasets less than 20 MB in size. This study proposes storage methods based on data features and categorization that can be tailored to meet unique data gathering demands by using internal classification measures developed by Xu et al. [75].

3.6. BC and Smart Cities' Ecosystems. Human behavior, technical nodes, and institutional administration are all integrated into a single service architecture as shown in Figure 3 as a core pillar of the smart city ecosystem. To meet the system's service delivery requirements, this model identifies six key aspects of effective BC data management: automatic data collection, distributed data security, transparency and privacy, trust-free governance, and democratization [13]. Zheng et al. [5] view the BC solution as a technology-supported intervention capable of scalable, secure, and efficient data management across cloud-supported or decentralized network channels that can be coordinated to provide a robust output of informational resources to achieve this broad spectrum of expectations.

The immediate repercussions of IoT security concerns drive academics to create and implement a more productive, efficient security standard based on a centralized blockchain solution. According to Chen et al. [43], efficiency and system performance are demonstrated through small-scale trials and then gradually scaled up to satisfy the requirements of large-scale systems. In Brooklyn, a blockchain-based energy grid was built to enable solar-paneled households to track their energy output and consumption, simplifying the accounting for system credits and debits [76]. While similar solutions have been offered for other service-level billing opportunities, such as healthcare, it is the implementation of a decentralized, intermediary-free charging system that will ultimately generate the efficiencies necessary to minimize network costs [26]. Kundu [26] proposes that by aggregating data on healthcare expenses, insurance firms, and service providers will be able to engage with client data, monitoring demand and offering discounts based on health, payment performance, and network involvement (e.g., visiting their primary care provider). Similarly, in the integrated IoT solution developed by Bruneo et al. [50], it is the consolidation of data management services via centralized cloud-based, network-routed authorizations that ensures seamless integration as consumers add additional layers of technology and information resources to their network connections.

In the European Union, the DECODE project was developed in collaboration with regional governments in major urban centers such as Barcelona, Catalonia, and Amsterdam to enable consumers to not only access data collected via the IoT, but also to exercise control over how that data is exposed to third-party organizations and service providers [55]. According to [76], DECODE is motivated by the assumption that if the technology is exclusive and restricted to corporate services, it will not be freely available in the global marketplace. Consumers obtain access to network data using the DECODE solution by confirming their identity online, allowing them to engage directly with software solutions for identity management, payment, and record keeping [76]. For consumers, privacy controls and monitoring capabilities would not only provide protection, but would also encourage businesses to establish more transparent information management standards in response to consumer and industry pressures [45].

4. The Solution: An Integrated BC Standard for IOT-Based Smart Cities

Due to the IoT's scale, the limited processing capacity of individual nodes, and the vulnerability of always-on or on-demand network connections, it is critical that any coordinating solution handles the IoT's unique scalability and security problems [77]. As "restricted nodes," each IoT hardware device has limited computation and communication capabilities, limiting its capacity to effectively secure and monitor against security breaches and illegal activity [49]. While BC solutions have the ability to alleviate the IoT's authentication burden, it is required to reduce code size incrementally by rewriting the design of the connection network via a distributed solution that includes both full

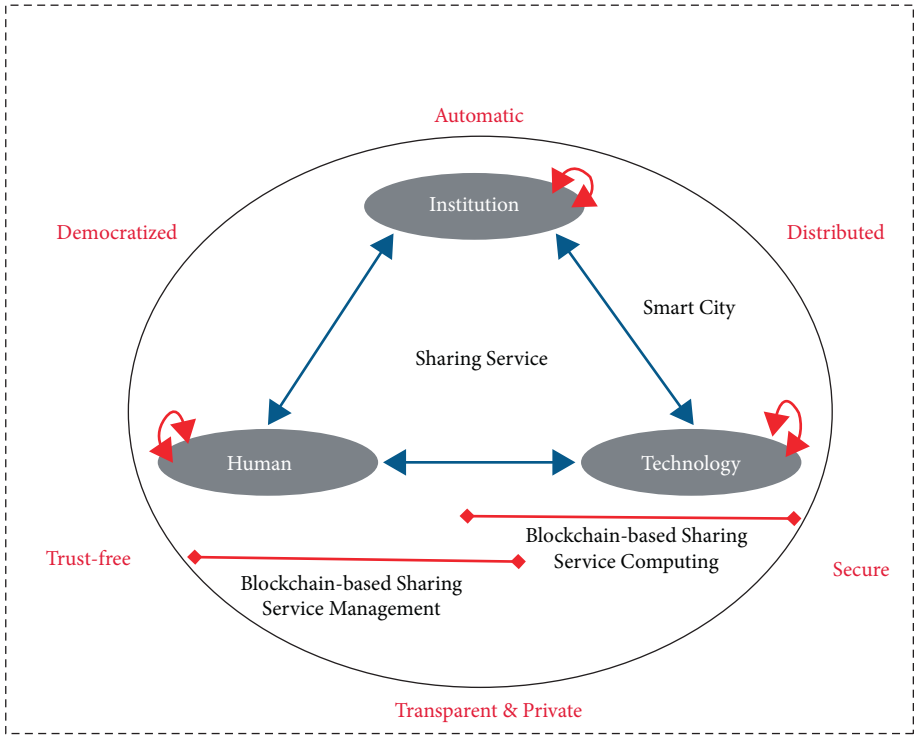

Figure 3: Features of the management and computing of blockchain-based sharing services (source: [13]).

(transacting) and light (adding) nodes [49]. This network design, which is based on an edge computing protocol, is dependent upon what [27] refer to as a centralized consortium network and outlying sidechain networks that connect IoT devices to intermediary notary nodes on the BC. This cross-transaction verification architecture, which is derived from the central conceptual basis for the Helium network [78] and the Tangle proposed by [68], enables parallel consensus and transaction-verified authentication while ensuring that there is no conflict between the current and any previous transactions [27]. BC technologies were created as a decentralized answer to the inherent vulnerability of online transactional systems to abuse, double-spending, and security breaches [26]. As a result, the solution to the security, trust, and integration problems associated with proprietary network architecture in smart city innovation is to construct the BC as a functional, standardized intermediary database [39, 40].

As can be seen in Figure 4, this research presents an integrated framework for BC technology in the context of IoT-based smart cities. The idea centralizes the data transmission process in a homogeneous, network-accessible cloud, where data owners and/or data consumers can grant or restrict access. As a transactional ledger, the BC acts as a central data warehouse, monitoring the inflow and outflow of user-triggered data. While concerns about anonymity and user monitoring are real, the BC sensing system will avoid the need for central authentication by providing access-restricted and purpose-monitored user-specific datasets. The system requires a contractual agreement between the user and the IoT-enabled software node, which is accomplished through transparent and adaptive privacy contracts embedded into the blockchain solution. As a result, the suggested architecture provides a central BC database as the underlying agent for receiving and disseminating user behavior information. APIs and proprietary software connect the database's periphery, routing user data through an integrated ecosystem of hardware nodes. BC authentication ensures the reliability of user information and the preservation of behavior-specific data by digitally validating user agreements and contracts using a universal language standard. Integration suggestions based on this unique paradigm include GPS-based journey tracking integration between, for example, home automation, user automobiles, and user workstations, thereby establishing a three-point assessment mechanism for predicting system efficiency and responsiveness.

The concept in Figure 5 illustrates the proposed BC service solution, which maintains compatibility for both open source and proprietary software design for user interfaces and APIs while consolidating data management operations into a single, centralized ledger. Thus, IoTs will work within their own native software but will initiate data exchange in accordance with the sharing protocol, populating the blockchain with the necessary datasets. Although it is dependent on the transactional modality being tested and examined in practice, a BC solution based on an established standard of exchange, such as Ethereum, provides an infinite-loop foundation for IoT consortium-based integration.

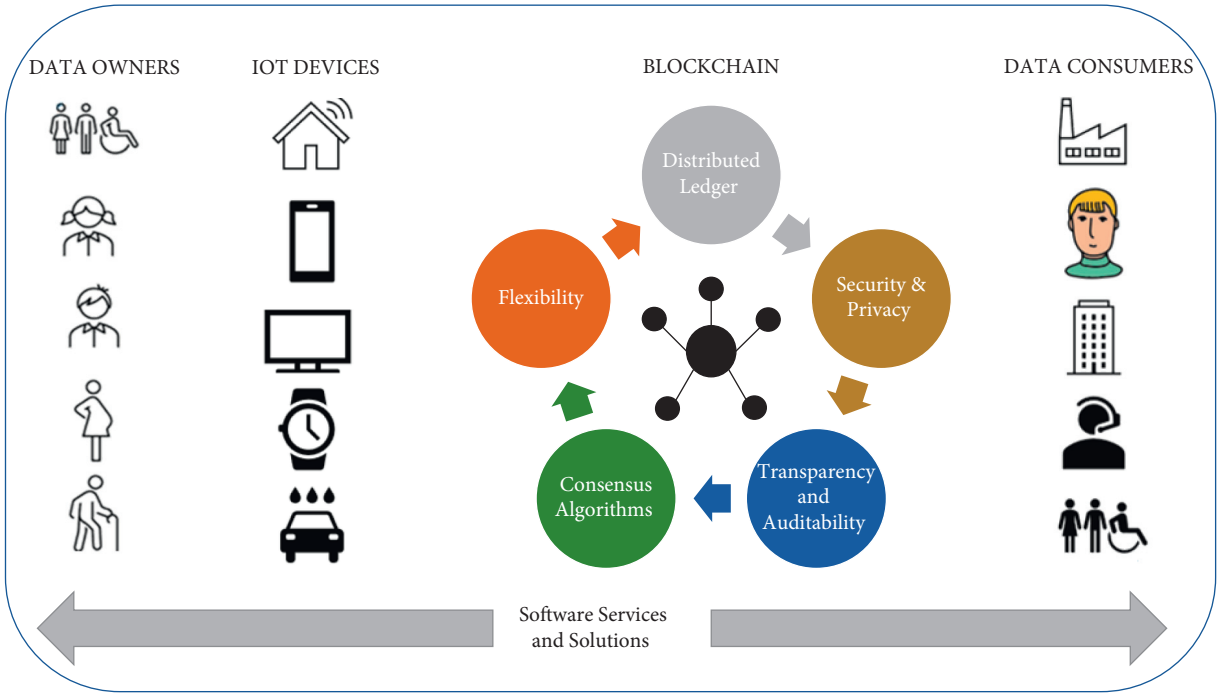

Figure 4: High-level model of blockchain integration within IoT-based smart city.

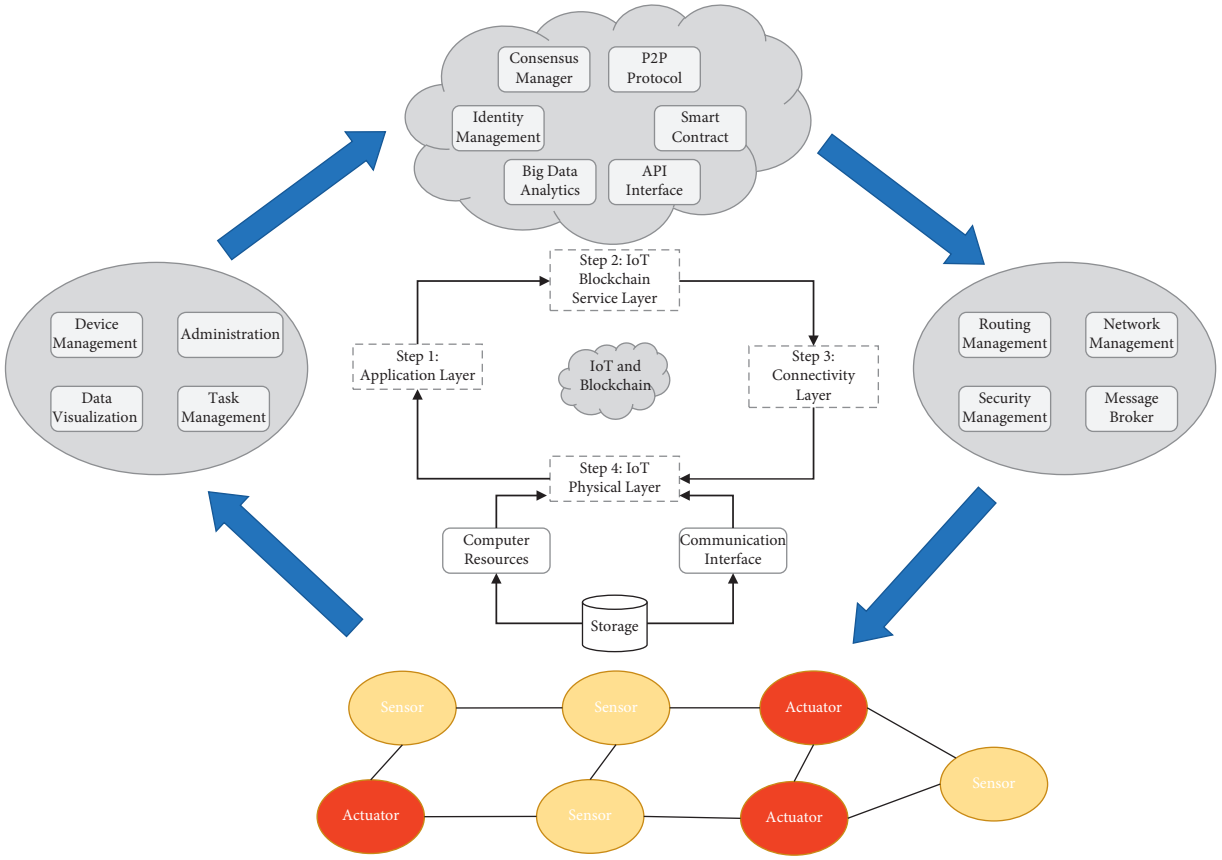

Figure 5: Application of blockchain integration within IoT-based smart city.

5. Research Contributions

This research paper's contributions can be stated as follows: the Internet of Things (IoT) operates as the digital nodes required for smart city solution interoperability, providing contractual precedence for trigger-response behavior across the dispersed smart network. Also, current technologies limit smart-city interoperability as inventive developers and hardware engineers attempt to gain a competitive advantage by establishing proprietary databases and repurposing existing ones. Hence, a realistic infinite loop smart network concept was proposed for building a standardized, cloud-based blockchain-based intermediate for IoT networking in smart cities.

6. Conclusions

This research paper summarizes the conceptual underpinnings of smart city solutions, IoT integration, and database administration using blockchain technology. Previous research studies indicated that the obstacles associated with BC integration are persistent and multidimensional, as experimentation is unable to resolve a large number of the challenges associated with variability. It is critical to ensure that IoT connections are meaningful, valuable, and responsive during the process of privatizing APIs and software solutions. A more immediate requirement is for a decentralized, widely available security validation and authentication standard. This research has demonstrated the benefits of BC serving in this capacity as a standard proof-of-work concept for legitimizing intranetwork information flows. Additionally, strategies for overcoming recognized obstacles are critical for advancing the notion of smart cities. This study verified also that in order for IoT-based smart city solutions to progress beyond its systemic constraints, there is an urgent need for a revised standard of practice that exists outside the existing private state of developer-restricted data management systems [79–85].

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of the present study.

Acknowledgments

The authors are very thankful to all the associated personnel in any reference and the anonymous reviewers that contributed in/for improving the content and presentation of this research.

References

[1] A. Gupta, R. Christie, and R. Manjula, "Scalability in the Internet of Things: features, techniques, and research challenges," *International Journal of Computational Intelligence Research*, vol. 13, no. 7, pp. 1617–1627, 2017.

[2] F. Lingjun, J. R. Gil-Garcia, D. Werthmuller, G. B. Burke, and X. F. Hong, "Investigating blockchain as a data management tool for IoT devices in smart city initiatives," in *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, pp. 1-2, Delft, The Netherlands, May 2018.

[3] M. 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.

[4] S. Ibba, A. Pinna, M. Seu, and F. E. Pani, "CitySense: blockchain-oriented smart cities," in *Proceedings of the XP2017 Scientific Workshops*, vol. 12, pp. 1–5, Cologne, Germany, May 2017.

[5] B. K. Zheng, L. H. Zhu, M. Shen et al., "Scalable and privacy-preserving data sharing based on blockchain," *Journal of Computer Science*, vol. 33, no. 33, pp. 557–567, 2018.

[6] "Interoperability maturity roadmap--IEEE std 2030.5," in *Interoperability Maturity Roadmap--IEEE Std 2030*, IEEE, Available [Online] at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8894220&isnumber=8894219, 2019.

[7] R. 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, 2019.

[8] S. Talari, M. Shafie-Khah, P. Siano, V. Loia, A. Tommasetti, and J. Catalão, "A review of smart cities based on the internet of things concept," *Energies*, vol. 10, no. 4, p. 421, 2017.

[9] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[10] P. Fraga-Lamas, T. Fernández-Caramés, M. Suárez-Albela, L. Castedo, and M. González-López, "A review on internet of things for defense and public safety," *Sensors*, vol. 16, no. 10, p. 1644, 2016.

[11] M. Höjer and J. Wangel, "Smart sustainable cities: definition and challenges," in *Proceedings of the ICT innovations for sustainability*Cham, Springer, 2015.

[12] United Nations, *World Urbanization Prospects The Population Division of the Department of Economic and Social Affairs of the United Nations*, Available [Online] at: https://population.un.org/wup/, 2014.

[13] J. Sun, J. Yan, and K. Z Zhang, "Blockchain-based sharing services: what blockchain technology can contribute to smart cities," *Financial Innovation*, vol. 2, pp. 1–9, 2016.

[14] D. Cox, *IOTA Smoothens Transport Management in Germany as Trive"*, Park Collaborates with Tangle, 2019.

[15] A.S. City: https://amsterdamsmartcity.com/.

[16] T.A. Traffic and IOS, "The best app selection for Barcelona, Apps4bcn," *All the Apps You Need for Barcelona*, Available [Online]: http://apps4bcn.cat/en/apps/index/Category:transport-i-tr-nsit.

[17] S. City and S. de Premsa, "El web de la Ciutat de Barcelona," Available [Online]: http://ajuntament.barcelona.cat/premsa/tag/smart-city/.

[18] E. Strickland, "Cisco bets on South Korean smart city," *IEEE Spectrum*, vol. 48, pp. 2011 11–12.

[19] G. Hancke, B. Silva, and G. Hancke Jr., "The role of advanced sensing in smart cities," *Sensors*, vol. 13, pp. 393–425, 2013.

[20] T. Bakıcı, E. Almirall, and J. Wareham, "A smart city initiative: the case of Barcelona," *ISSN*, vol. 4, pp. 135–148, 2013.

[21] R. Kitchin, *Getting Smarter about Smart Cities: Improving Data Privacy and Data Security*, Department of the Taoiseach, Ireland, 2016, https://www.researchgate.net/publication/293755608_Getting_smarter_about_smart_cities_Improving_data_privacy_and_data_security.

[22] B. N. Silva, M. Khan, and K. Han, "Towards sustainable smart cities: a review of trends, architectures, components, and open challenges in smart cities," *Sustainable Cities and Society*, vol. 38, pp. 697–713, 2018.

[23] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: challenges and opportunities," *IEEE access*, vol. 6, pp. 46134–46145, 2018.

[24] L. Edwards, "Privacy, security and data protection in smart cities:," *European Data Protection Law Review*, vol. 2, no. 1, pp. 28–58, 2016.

[25] L. Ismail and H. Materwala, "Article A review of blockchain architecture and consensus protocols: use cases, challenges, and solutions," *Symmetry*, vol. 11, no. 10, p. 1198, 2019.

[26] D. Kundu, "Blockchain and trust in a smart city," *Environment and Urbanization ASIA*, vol. 10, no. 1, pp. 31–43, 2019.

[27] Y. 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, 2019.

[28] R. Beck, J. Stenum Czepluch, N. Lollike, and S. Malone, "Blockchain–the gateway to trust-free cryptographic transactions," in *Proceedings of the Twenty-Fourth European Conference on Information Systems (ECIS)*, İstanbul,Turkey, 2016.

[29] C. Harrison and I. A. Donnelly, "A theory of smart cities," in *Proceedings of the 55th Annual Meeting of the ISSS-2011*, Hull, UK, 2011.

[30] P. Rizzo, "Dubai government taps IBM for city-wide blockchain pilot push," 2017, http://www.coindesk.com/dubai-government-ibm-city-blockchain-pilot/.

[31] L. Ismail, H. Materwala, and A. Hennebelle, "A scoping review of integrated blockchain-cloud (BcC) architecture for healthcare: applications, challenges and solutions," *Sensors*, vol. 21, no. 11, p. 3753, 2021.

[32] H. Chourabi, T. Nam, S. Walker et al., "Understanding smart cities: an integrative framework," in *Proceedings of the 2012 45th Hawaii international conference on system sciences*, January 2012.

[33] E. Almirall, J. Wareham, C. Ratti et al., "Smart cities at the crossroads: new tensions in city transformation," *California Management Review*, vol. 59, pp. 140–152, 2016.

[34] M. Finger and M. Razaghi, "Conceptualizing "smart cities"," *Informatik-Spektrum*, vol. 40, no. 1, pp. 6–13, 2017.

[35] X. Liu, W. Wang, T. Zhu, Q. Zhang, and P. Yi, "Poster: smart object-oriented dynamic energy management for base stations in smart cities," in *Proceedings of the 3rd Workshop on Experiences with the Design and Implementation of Smart Objects*, vol. 17, pp. 27-28, Snowbird, UT, USA, 2017.

[36] M. Stone, J. Knapper, G. Evans, and E. Aravopoulou, "Information management in the smart city," *The Bottom Line*, vol. 31, no. 11, 2018.

[37] M. Body, "Napster creator's blockchain firm Helium releases IoT hotspots," 2019, https://cointelegraph.com/news/napster-creators-blockchain-firm-helium-releases-iot-hotspots accessed on.

[38] C. 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, 2016.

[39] N. Alasbali, S. R. Azzuhri, and R. Salleh, "Stakeholders' viewpoints toward blockchain integration within IoT-based smart cities," *Journal of Sensors*, vol. 2021, pp. 1–17, 2021.

[40] N. Alasbali, S. R. Azzuhri, and R. Salleh, "A blockchain-based smart network for IoT-driven smart cities," in *Proceedings of the 2020 2nd International Electronics Communication Conference (IECC 2020)*, pp. 17–23, Association for Computing Machinery, Singapore, July 2020.

[41] A. Greenberg, P. Lahiri, D. A. Maltz, P. Patel, and S. Sengupta, "Towards a next generation data center architecture," in *Proceedings of the ACM workshop on Programmable routers for extensible services of tomorrow - PRESTO '08*, pp. 57–62, WA, Seattle, USA, August 2008.

[42] J.-H. Lee, K. D. Singh, Y. Hadjadj-Aoul, and N. Kumar, "Wireless and mobile technologies for the internet of things," *Mobile Information Systems*, vol. 2016, pp. 1-2, Article ID 8206548, 2016.

[43] K. Chen, S. Zhang, Z. Li et al., "Internet-of-Things security and vulnerabilities: taxonomy, challenges, and practice," *Journal of Hardware and Systems Security*, vol. 2, no. 2, pp. 97–110, 2018.

[44] M. F. Muhammad, W. Anjum, and K. S. Mazhar, "A critical analysis on the security concerns of internet of things (IoT)," *International Journal of Computer Application*, vol. 111, pp. 1–6, 2015.

[45] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in *Proceedings of the 2012 10th international conference on frontiers of information technology*, pp. 257–260, IEEE, Islamabad, Pakistan, 2012.

[46] M. Wu, T. L. Lu, S. ling, and Du. Hui-Ying, "Research on the architecture of Internet of things," in *Proceedings of the Advanced Computer Theory and Engineering (ICACTE)*, pp. 484–487, Chengdu, 2010.

[47] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in internet of things (IoT)," in *Proceedings of the 2012 2nd international conference on consumer electronics, communications and networks (CECNet)*, pp. 1282–1285, IEEE, Yichang, China, 2012.

[48] E. Reilly, M. Maloney, M. Siegel, and G. Falco, "A smart city IoT integrity-first communication protocol via an Ethereum blockchain light client," in *Proceedings of the International Workshop on Software Engineering Research and Practices for the Internet of Things, (SERP4IoT 2019)*, pp. 15–19, Marrakech, Morocco, 2019.

[49] K. Pardini, J. J. P. C. Rodrigues, S. A. Kozlov, N. Kumar, and V. Furtado, "IoT-based solid waste management solutions: a survey," *Journal of Sensor and Actuator Networks*, vol. 8, no. 1, p. 5, 2019.

[50] D. Bruneo, F. Longo, G. Merlino, A. Puliafito, and N. Kushwaha, "Integrating IoT and cloud in a smart city context: the# SmartME case study," *International Journal of Computer Application*, vol. 57, pp. 267–280, 2018.

[51] A. Collen, N. A. Nijdam, J. Augusto-Gonzalez et al., "Ghost - safe-guarding home IoT environments with personalised real-time risk control," in *Proceedings of the International ISCIS Security Workshop*, Springer, Cham, pp. 68–78, 2018.

[52] GSMA, *eSIM: The SIM for the Next Generation of Connected Consumer Devices*, GSMA, Retrieved from: https://www.gsma.com/esim/, 2019.

[53] J. O. Sachs, N. I. Beijar, P. Elmdahl, J. Melen, F. R. Militano, and P. A. Salmela, "Capillary networks–a smart way to get things connected," *Ericsson Review*, vol. 8, pp. 1–8, 2014.

[54] K. Finch and O. Tene, "Smart cities: privacy, transparency, and community," *The Cambridge Handbook of Consumer Privacy*, p. 125, Cambridge University Press, 2018.

[55] A. M. Townsend, *Smart Cities: Big Data, Civic Hackers, and the Quest for a New utopia*, WW Norton & Company, New York, NY, USA, 2013.

[56] L. Hu and X. Xia, "5G-Oriented IoT big data analysis method system," *Mobile Information Systems*, vol. 2021, pp. 1–9, Article ID 3186696, 2021.

[57] H. Shafagh and A. Hithnawi, "Privacy-preserving quantified self: secure sharing and processing of encrypted small data," in *Proceedings of the Workshop on Mobility in the Evolving Internet Architecture*, pp. 25–30, CA, Los Angeles, USA, August 2017.

[58] K. R. Özyılmaz and A. Yurdakul, "Integrating low-power IoT devices to a blockchain-based infrastructure: work-in-progress," in *Proceedings of the Thirteenth ACM International Conference on Embedded Software 2017 Companion*, pp. 1-2, Seoul, Republic of Korea, October 2017.

[59] O. 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*, vol. 32, no. 12, p. 5238, 2020.

[60] N. Hadar, S. Siboni, and Y. Elovici, "A lightweight vulnerability mitigation framework for IoT devices," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, pp. 71–75, Texas, Dallas, USA, November 2017.

[61] P. W. Singer and A. Friedman, *Cybersecurity: What Everyone Needs to Know*, OUP, USA, 2014.

[62] S. Ijaz, M. A. Shah, A. Khan, and M. Ahmed, "Smart cities: a survey on security concerns," *International Journal of Advanced Computer Science and Applications*, vol. 7, pp. 612–625, 2016.

[63] M. Harbers, M. Bargh, R. Pool, J. Van Berkel, S. Van den Braak, and S. Choenni, "A conceptual framework for addressing IoT threats: challenges in meeting challenges," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, HICSS 2018, Hilton Waikoloa Village, HI, USA, January 2018.

[64] A. AlDairi and L. a. Tawalbeh, "Cyber security attacks on smart cities and associated mobile technologies," *Procedia Computer Science*, vol. 109, pp. 1086–1091, 2017.

[65] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in Smart Cities: safety, security and privacy," *Journal of Advanced Research*, vol. 5, no. 4, pp. 491–497, 2014.

[66] H. Demirkan and D. Delen, "Leveraging the capabilities of service-oriented decision support systems: putting analytics and big data in cloud," *Decision Support Systems*, vol. 55, no. 1, pp. 412–421, 2013.

[67] M. 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, 2018.

[68] S. Popov, *The Tangle*, Iota, 2018, https://www.iota.org/research/academic-papers accessed on 2020.

[69] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, "Hybrid-IoT: hybrid blockchain architecture for internet of things-pow sub-blockchains," in *Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1007–1016, IEEE, Halifax, NS, Canada, 2018.

[70] D. Li, W. Peng, W. Deng, and F. Gai, "A blockchain-based authentication and security mechanism for IoT," in *Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–6, IEEE, Hangzhou, China, 2018.

[71] V. Rakovic, J. Karamachoski, V. Atanasovski, and L. Gavrilovska, "Blockchain paradigm and internet of things," *Wireless Personal Communications*, vol. 106, no. 1, pp. 219–235, 2019.

[72] N. El Ioini, C. Pahl, and S. Helmer, "A decision framework for blockchain platforms for IoT and edge computing," in *Proceedings of 3rd International Conference on Internet of Things, Big Data and Security*, Funchal, Madeira, Portugal, March 2018.

[73] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Generation Computer Systems*, vol. 86, pp. 650–655, 2018.

[74] X. L. Yu, X. Xu, and B. Liu, "EthDrive: a peer-to-peer data storage with provenance," in *Proceedings of the 29th International Conference on Advanced Information Systems Engineering*, pp. 25–32, 2017.

[75] Q. Xu, K. M. M. Aung, Y. Zhu, and K. L. Yong, "A blockchain-based storage system for data analytics in the internet of things," in *New Advances in the Internet of Things*, pp. 119–138, Springer, Cham, 2018.

[76] E. Copeland, *Blockchain powers a Personal Data Revolution"*, DECODE, 2017, https://decodeproject.eu/blog/blockchain-powers-personal-data-revolution.

[77] S. 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, 2019.

[78] A. Haleem, A. Allen, A. Thompson, M. Nijadam, and R. Garg, *Helium: A Decentralized Wireless Network*, Helium, 2018, http://whitepaper.helium.com.

[79] G. V. Pereira, P. Parycek, E. Falco, and R. Kleinhans, "Smart governance in the context of smart cities: a literature review," *Information Polity*, vol. 23, no. 2, pp. 143–162, 2018.

[80] A. Cocchia, "Smart and digital city: a systematic literature review," in *Smart City*, pp. 13–43, Springer, Cham, 2014.

[81] R. Novotný, R. Kuchta, and J. Kadlec, "Smart city concept, applications and services," *Journal of Telecommunications System & Management*, vol. 3, no. 2, pp. 1–5, 2014.

[82] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *White Paper*, Available online at: http://bitcoin.org/bitcoin.pdf, 2008.

[83] A. Menon, "Smart cities, livable cities," *NIM Marketing Intelligence Review*, vol. 9, no. 1, pp. 48–52, 2017.

[84] V. Skwarek, "Blockchains as security-enabler for industrial IoT-applications," *Asia Pacific Journal of Innovation and Entrepreneurship*, vol. 11, no. 3, pp. 301–311, 2017.

[85] A. Saeed, A. Ahmadinia, A. Javed, and H. Larijani, "Intelligent intrusion detection in low-power IoTs," *ACM Transactions on Internet Technology*, vol. 16, no. 4, pp. 1–25, 2016.