Open Access Library Journal
2026, Volume 13, e14695
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Blockchain-Enabled IoT Architectures for Secure Smart Cities

Alick Andrew Sakala, Yu Chen, Precious Nkunika, Mingwu Zhang*

School of Computer Science and Artificial Intelligence, Hubei University of Technology, Wuhan, China
Email: *csmwzhang@gmail.com

How to cite this paper: Sakala, A.A., Chen, Y., Nkunika, P. and Zhang, M.W. (2026) Blockchain-Enabled IoT Architectures for Secure Smart Cities. *Open Access Library Journal*, **13**: e14695.
https://doi.org/10.4236/oalib.1114695

Received: December 1, 2025
Accepted: January 27, 2026
Published: January 30, 2026

Abstract

The rapid digitalization of urban environments has accelerated the adoption of smart city systems, with the Internet of Things (IoT) serving as a core enabler of real-time monitoring, automation, and data-driven services. Despite its advantages, IoT-based smart city infrastructure faces critical security and reliability challenges, including data breaches, device tampering, unauthorized access, and limited computational protection. These vulnerabilities compromise the robustness, trustworthiness, and sustainability of smart city deployments, underscoring the necessity for secure and decentralized system architectures. This study explores the integration of Blockchain and IoT as a transformative pathway toward secure and reliable smart city systems. Through a focused literature review, case analysis, and conceptual modeling, we demonstrate that Blockchain enhances IoT security by enabling distributed trust, token-based authentication, and resilient data integrity while reducing single points of failure. Although challenges related to scalability, energy consumption, interoperability, and regulation persist, the lightweight consensus mechanisms and AI-assisted frameworks continue to further improve system efficiency and scalability, and Blockchain-IoT integration offers a promising foundation for next-generation secure smart city infrastructure.

Subject Areas

Computer and Network Security

Keywords

Blockchain-IoT integration, IoT Security, Smart City Infrastructures

1. Introduction

Modern urban environments face increasing pressure from rapid population

growth, rising energy demand, environmental constraints, and the need for efficient service delivery. In response, smart cities with Internet of Things (IoT) have emerged as a data-driven paradigm aimed at optimizing mobility, utilities, governance, and public safety through digital innovation [1]. Through IoT-enabled infrastructures, large-scale and real-time data is collected and processed between heterogeneous devices (including environmental sensors, intelligent instruments, autonomous vehicles, and medical tools), cities can support automation, operational efficiency, and sustainability [2].

Despite these benefits, IoT-based smart city systems remain highly vulnerable to security and reliability threats due to centralized data architectures, weak authentication mechanisms, and limited computational resources. Considering that attacks targeting smart meters, surveillance networks, or traffic control systems may result in substantial social and economic consequences, Blockchain technology is introduced to mitigate these risks through immutable data records, distributed trust, smart contracts, and verifiable data integrity [3]. This study examines the integration of Blockchain and IoT as a means to enhance the security and resilience of smart city infrastructures. By synthesizing existing frameworks, use cases, and empirical implementations, this work contributes to ongoing optimization of Blockchain-based IoT in urban digital transformation, cybersecurity, and smart city infrastructures.

Unlike prior reviews, this work combines bibliometric analysis with thematic case studies, emphasizing real-world pilot deployments and emerging AI-integrated frameworks, which further highlight practical pathways toward sustainable and secure smart city infrastructures under Blockchain-IoT integration.

1.1. Background

Smart city development is fundamentally driven by digital connectivity, automation, data analytics, and citizen-centric service delivery. IoT functions as the "nervous system" of smart cities by linking physical infrastructures—such as transportation networks, energy grids, healthcare facilities, and surveillance systems—with computational intelligence [4]. These interconnected devices generate vast volumes of data that enable responsive and adaptive urban governance [5]. However, the reliance on centralized servers in many IoT deployments introduces vulnerabilities related to data manipulation, unauthorized access, and single points of failure.

Blockchain technology provides a decentralized ledger in which data is validated and maintained collectively without centralized control [6]. Since its properties of transparency, immutability, and trust decentralization align closely with the security requirements of smart city infrastructures, Blockchain-based IoT will enable tamper-resistant data sharing, secure device authentication, and trustworthy inter-device communication. Against the backdrop of increasingly sophisticated cyber threats and expanding IoT ecosystems, this study explores how Blockchain-IoT integration can support secure, resilient, and sustainable digital envi-

ronments for modern cities.

1.2. Research Objectives

1) Explore the role of Blockchain and IoT technologies in smart city development.

2) Analyze how Blockchain can mitigate security vulnerabilities inherent in IoT-based smart city systems.

3) Evaluate the benefits and technical challenges associated with integrating Blockchain and IoT technologies.

1.3. Research Questions

The study is guided by the following research questions:

1) Do Blockchain and IoT technologies contribute to smart city development?

2) In what ways can Blockchain address security challenges in IoT-enabled smart cities?

3) What benefits and challenges arise from integrating Blockchain and IoT in smart city environments?

2. Literature Review

2.1. Overview of Blockchain and IoT Technologies

The integration of Blockchain technology with the Internet of Things has emerged as one of the most consequential developments in the evolution of smart city ecosystems, and the literature [7] reflects a rapidly expanding scholarly interest in the convergence of distributed ledgers, ubiquitous sensing, and urban informatics. Early studies of [8] framed IoT as the nervous system of the smart city, enabling real-time data collection across transportation, energy, utilities, environmental monitoring, and public safety infrastructures. In this conceptualization, IoT provides the sensing, actuation, and communication layers that make cities responsive and data-driven; however, scholars such as Crosby M. *et al.* (2016) quickly noted that the centralized architectures traditionally used to store and manage IoT data introduce severe security, integrity, and privacy vulnerabilities that can compromise the trustworthiness of urban services [9]. Consequently, Blockchain emerged in the literature [5] as a promising complementary technology capable of enhancing IoT data management through tamper-resistant ledgers, decentralized trust models, and cryptographically protected transactions. The academic conversation has since evolved into a rich, interdisciplinary discourse examining how Blockchain can be architected, optimized, and deployed to address longstanding IoT security limitations while supporting scalable, efficient, and citizen-centered smart city solutions.

Recent high-impact literature reviews, such as Alzoubi *et al.* (2025) on Blockchain for Sustainable Smart Cities [10] and Ali *et al.* (2025) on Decentralized Trust Frameworks [11], contextualize these advancements by highlighting motivations, challenges, and integrations with AI for enhanced cybersecurity in urban environments.

2.2. Blockchain Technologies and Smart Cities

In much of the early scholarship, Blockchain was positioned as a mechanism to mitigate the fragmentation and opacity of IoT platforms, which traditionally rely on proprietary cloud servers vulnerable to single points of failure and unauthorized manipulation. Researchers such as [12] argued that by decentralizing data storage and verification, Blockchain could ensure integrity and immutability even in the presence of malicious actors or compromised nodes. Extensive theoretical work of [4] explored how Blockchain's consensus mechanisms, ranging from Proof-of-Work to more efficient Proof-of-Stake, Byzantine Fault Tolerant protocols, and Directed Acyclic Graph-based ledgers, could be adapted to the latency-sensitive and resource-constrained environment of IoT. As smart city sensors often have minimal processing capacity and battery life, the literature [4] records a robust dialogue around reducing the computational load of blockchain operations through off-chain computation, lightweight cryptographic primitives, and hierarchical ledger structures that delegate validation tasks to more capable fog or edge nodes. These architectural innovations are frequently highlighted as essential to ensuring that Blockchain can scale without overwhelming IoT devices or congesting urban communication networks. Recent advancements emphasize edge computing and metaverse IoT integrations for enhanced scalability [13].

2.3. Data Security and Privacy

Another extensive theme within the literature [6] concerns data security and privacy, which remain central challenges for IoT-enabled smart cities. IoT devices continuously collect vast volumes of granular, sensitive data, ranging from household energy consumption patterns and transportation movements to personal biometric readings in health-monitoring systems. Scholars such as [14] consistently emphasize that in the absence of robust safeguards, this data can be intercepted, altered, or exploited, threatening not only system reliability but also fundamental citizen rights to privacy and digital sovereignty. Blockchain is therefore frequently conceptualized as a protective layer that empowers users with cryptographic ownership of their data, enabling selective disclosure, secure authentication, and transparent audit trails. Literature [5] in this domain also explores privacy-preserving Blockchain techniques such as zero-knowledge proofs, homomorphic encryption, secure multiparty computation, and attribute-based access control frameworks designed to prevent unauthorized profiling and surveillance. These studies recognize the delicate balance between transparency necessary for trust, regulation, and accountability and confidentiality necessary for ethical data stewardship in smart city environments.

2.4. Blockchain and IoT Communication

The reviewed body of work reveals growing scholarly interest in how Blockchain can support secure IoT communication through decentralized identity management, device authentication, and robust key distribution mechanisms [15]. Tra-

ditional IoT security models rely on centralized certificate authorities, which can be compromised or overloaded. Blockchain-based identity frameworks, by contrast, allow devices to register, authenticate, and interact autonomously through immutable cryptographic credentials. Studies of [1] and [2] together describe architectures in which each IoT device is assigned a blockchain-backed identity that records behavioral patterns, known vulnerabilities, and trust scores, enabling real-time threat detection and rapid remediation of suspicious behavior across the network. These innovations are especially relevant for critical smart city domains such as smart transportation systems, where autonomous vehicles and traffic sensors must interact reliably, and smart energy grids, where compromised nodes can trigger cascading failures. Through this lens, Blockchain becomes more than a ledger; it becomes a decentralized security infrastructure capable of fostering trust among millions of heterogeneous devices. Recent frameworks incorporate AI for anomaly detection to further enhance these capabilities [16]. **Figure 1** depicts the sequential steps for secure data handling in smart cities, starting from IoT data collection, through Blockchain consensus validation (e.g., Proof-of-Stake), device authentication, smart contract execution, and AI-driven anomaly detection to ensure integrity and transmission safety.

2.5. Smart City Sectors

As blockchain-IoT integration matured, application-oriented literature expanded to examine specific smart city sectors [16]. In smart energy management, [3] shows how blockchain-enabled IoT microgrids support peer-to-peer renewable energy trading, dynamic pricing, and verifiable carbon accounting. These systems use smart contracts to automate transactions between prosumers, utility companies, and regulators, ensuring transparency while reducing operational costs.

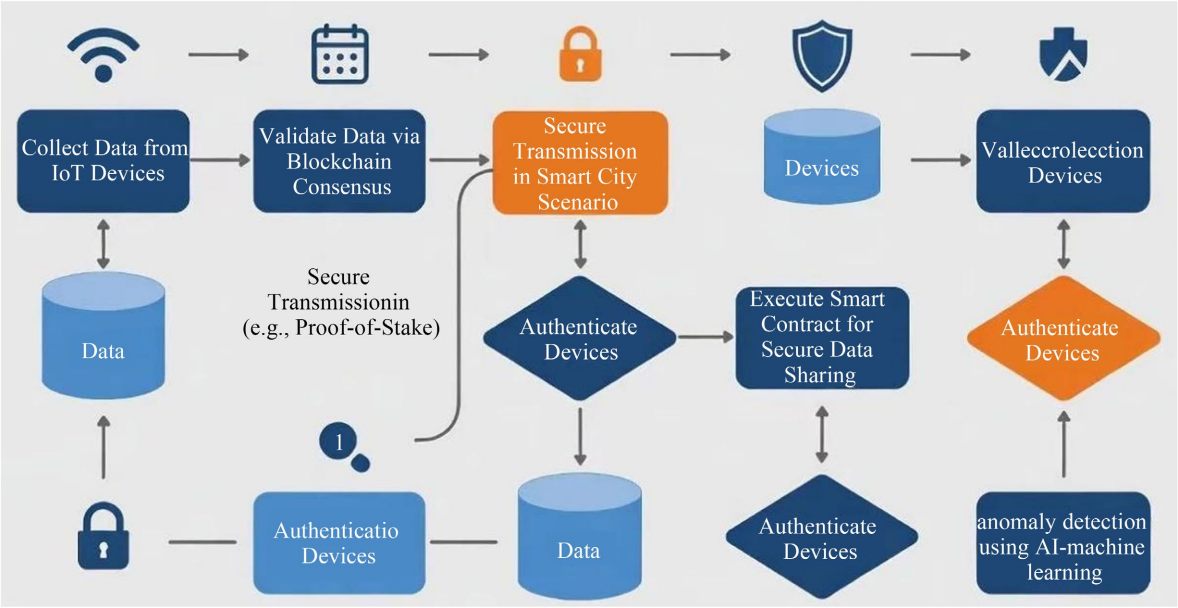

Figure 1. Blockchain-IoT data flow process in smart city scenarios.

In transportation, Blockchain supports secure vehicular communication, predictive traffic control, and decentralized mobility-as-a-service platforms. IoT sensors gather traffic, pollution, and occupancy data, while blockchain records and secures this data, enabling urban planners to design adaptive traffic lights, congestion pricing systems, and autonomous vehicle coordination mechanisms [6]. Similar advancements are documented in waste management, where IoT-enabled bins transmit fill levels, and Blockchain ensures the integrity of logistics data, and in public health, where Blockchain supports secure medical IoT devices and pandemic monitoring systems [17]. Recent studies highlight integrations with big data analytics and digital twins for optimized urban infrastructure.

2.6. Case Studies of Smart Cities

According to [9], several cities worldwide have successfully integrated IoT frameworks to improve urban living.

2.6.1. Singapore—A Fully Digitalized Smart City

Singapore is recognized as one of the most technologically advanced smart cities. The government implemented Smart Nation initiatives, including:

- AI-powered traffic management to reduce congestion.
- Digital identity systems for seamless citizen services.
- IoT-driven environmental monitoring for real-time air quality assessment.

Singapore's use of Blockchain in digital transactions and cloud-based governance has set a global benchmark for smart cities.

For instance, within the Smart Nation initiative, Singapore has launched a blockchain-based digital marketplace for trading renewable energy certificates, integrated with IoT devices. IoT sensors in solar panels and smart meters collect real-time data on energy production and consumption, which is immutably recorded on a Blockchain ledger. This enables transparent peer-to-peer energy trading among residents and businesses, addressing urban energy challenges by reducing dependency on centralized utilities, automating transactions via smart contracts, and promoting sustainability with verifiable carbon accounting. The project has resulted in enhanced grid efficiency and cost reductions for participants.

2.6.2. Barcelona—IoT-Powered Urban Management

Barcelona has deployed extensive IoT networks for urban optimization:

- Smart parking solutions using real-time data to guide drivers to available spots.
- IoT-based street lighting that adjusts brightness based on pedestrian activity.
- Smart waste bins equipped with sensors to optimize collection routes, reducing operational costs.

The city's IoT ecosystem has contributed to energy savings, improved transportation efficiency, and reduced operational costs.

2.6.3. Dubai—AI and Blockchain for Smart Governance

Dubai's Smart Dubai Initiative focuses on blockchain, AI, and IoT integration.

Key projects include:

- AI-powered government services reducing paperwork and increasing efficiency.
- Blockchain-based digital transactions, ensuring transparency in real estate and finance.
- IoT-enabled security and surveillance, enhancing crime prevention.

Dubai aims to become 100% paperless and reduce government operating costs through smart city innovations. Table 1 compares IT strategies across Singapore, Barcelona, and Dubai, highlighting key initiatives, technologies (e.g., AI, IoT, blockchain), implementation focus, and outcomes like efficiency gains and cost reductions.

Table 1. Comparison of smart cities' IT-Driven strategies.

City	Key technologies used	Major Benefits
Singapore	AI, Cloud computing, Blockchain	Efficient governance, low congestion
Barcelona	IoT, Smart Sensors, Edge computing	Energy savings, better public services
Dubai	AI, IoT, Blockchain	Secure transportation, smart governance.

2.7. Barriers to Blockchain-IoT Integration

Despite the breadth of applications, [7] acknowledges several critical barriers that hinder widespread adoption of blockchain-IoT systems in real-world smart city deployments. Scalability remains one of the most persistent concerns, as the high volume and velocity of IoT data can overwhelm Blockchain networks if not effectively filtered or compressed. Many studies like those of [5] therefore investigate scalable storage architectures, such as off-chain data lakes with on-chain hash references, sharding techniques, and tiered architectures where fog nodes perform preliminary data verification. Another concern involves interoperability, as IoT ecosystems contain devices from diverse manufacturers using different communication protocols, while Blockchain networks themselves vary in structure, consensus algorithms, and smart contract languages. Scholars such as [12] propose middleware platforms, standardized APIs, and cross-chain communication protocols to bridge these heterogeneities, but the literature suggests that fully interoperable, vendor-neutral smart city infrastructures are still an emerging frontier. Recent challenges include regulatory alignment with GDPR and high energy demands in consensus mechanisms.

Nonetheless, a particularly rich thread in the literature addresses the governance, ethical, and regulatory implications of blockchain-enabled IoT systems. Smart cities are inherently socio-technical constructs, and integrating Blockchain raises new questions about data ownership, accountability, transparency, and the distribution of power among governments, private companies, and citizens. Researchers, for example [9] warn that blockchain's immutability can become prob-

lematic in cases requiring data correction or the right to be forgotten, while its transparency may conflict with privacy regulations such as GDPR. Ethical analyses highlight concerns that blockchain-based smart city platforms could centralize control under technologically dominant actors if not carefully designed with participatory governance models. Consequently, newer literature emphasizes the co-design of technology, policy, and institutional frameworks, arguing that future research must integrate legal scholars, sociologists, urban planners, and community stakeholders to ensure that blockchain-IoT solutions promote equity, inclusivity, and democratic accountability.

For example, participatory governance models could mitigate this risk by establishing community-led Blockchain consortia, where citizens use token-based voting systems to influence smart contract rules and data policies. This distributes decision-making power, prevents dominance by large tech entities, and ensures that implementations align with diverse societal needs and values, fostering greater trust and adoption.

2.8. Integration of Blockchain and IoT with Other Emerging Technologies

Literature [12] examines the integration of Blockchain and IoT with other emerging technologies such as artificial intelligence, machine learning, 5G/6G networks, digital twins, and edge intelligence. These integrations are presented as catalysts for next-generation smart cities capable of autonomous decision-making, ultra-low latency communication, and predictive maintenance of infrastructure. Scholars such as [14] argue that AI models trained on IoT sensor data can detect anomalies, optimize urban services, and forecast resource demands, but these models require trusted, verifiable data sources, an area where Blockchain plays a critical role. Meanwhile, 5G networks alleviate bandwidth constraints and enable the deployment of Blockchain nodes closer to the edge, reducing latency. Digital twins, which involve virtual replicas of urban systems, rely on high-quality IoT data and trustworthy transaction logs, both of which are strengthened by blockchain. This convergence reveals a future research direction focused on orchestrating multi-technology ecosystems that rely on Blockchain as a foundational trust infrastructure. Recent developments include decentralized trust frameworks using AI and lightweight PoS for enhanced cybersecurity [11].

2.9. Literature Evaluation

Across the literature, there is strong consensus that while Blockchain holds immense potential for strengthening IoT-based smart city solutions, its effectiveness depends on continued advancements in consensus efficiency, privacy-preserving techniques, regulatory frameworks, device-level optimization, and large-scale pilot deployments. To date, many studies remain conceptual or limited to small-scale prototypes, and scholars emphasize the need for real-world validation in complex urban environments. Such validation must address not only technical

feasibility but also economic sustainability, citizen acceptance, and long-term operational governance. As cities evolve toward increasingly digitized and automated infrastructures, the literature suggests that blockchain-enabled IoT systems could become pivotal in ensuring that these infrastructures remain secure, transparent, and resilient.

3. Methodology

To investigate the current Internet of Things and Blockchain applications in the smart city, the researcher conducted a systematic literature review incorporating bibliometric analysis. This literature review type allowed the researcher to synthesize previous scholarly knowledge and inspire future research works [18]. It argues that the power of bibliometric reviews lies in their capability to identify and classify a wide variety of documents within a specific area and to facilitate the analysis of information in order to show the trends based on synthesized data. Data sources in this paper include peer-reviewed journal articles, conference proceedings, industry reports, white papers, and case studies from reputable databases such as IEEE Xplore, SpringerLink, ScienceDirect, and ACM Digital Library.

Likewise, the use of bibliometric reviews ensures objectivity and offers unique insights into the literature [19]. Using bibliometric techniques, scholars can depict the conceptual space of a given research field and facilitate the interpretation of the findings. The initial step of the bibliometric review consists of identifying the most suitable database for the study. For the selection of articles, the researcher carried out searches in the Scopus database. The capability of the database to handle bibliographic references and quantify citations has made Scopus a widely used instrument for the analysis of any research field. Apart from this, Scopus is one of the most highly regarded academic databases globally, indexing approximately 70% more sources than the Web of Science [20]. As per [8], Scopus is one of the largest and trusted data repositories for peer-reviewed academic journals, books, chapters, and conference proceedings covering various disciplines and depicting the dynamics of science and technology. The researcher conducted the search using the title, abstract, and keywords fields by inserting the following query and a Boolean operator: Internet of Things, Blockchain AND "smart city".

Using the outline of several studies as a reference, the researcher considered only articles published in academic journals to analyze and develop bibliometric indicators. The selection of journal articles helps to ensure the reliability and academic nature of the analysis [21] because these resources provide a representative sample of international scientific activity. To widen coverage, the researcher considered all publications in the English language. All journal articles published within the past 10 years were considered. To further refine the results, the researcher limited the subject areas to computer science. The review of past studies focused on identifying the connection between IoT and Blockchain technology with the smart city. Each of the previous articles was carefully screened for relevance by reading the title, the abstract, and the keywords. Eventually, 20 journal

articles were retrieved for the final review and analysis. The sample included all articles that present the applications of IoT and Blockchain technology in smart cities.

The bibliometric analysis revealed a growing trend in publications: from approximately 5 articles in 2016 to over 50 in 2022, with a total of around 342 documents on "smart city" and "blockchain" in Scopus from 2016-2022. Key themes included security (appearing in 60% of abstracts) and sustainability (40%), informing the thematic synthesis in the findings.

4. Findings

This section presents and discusses the findings of the study on integrating Blockchain and IoT to enhance security in smart city solutions. The findings were derived from extensive document analysis, systematic literature review, expert insights extracted from secondary interview transcripts, and the synthesis of global case studies. The section is organized thematically, reflecting the core research objectives. Data from the reviewed sources, both qualitative and quantitative in nature, are presented through descriptive discussions and supported by thematic interpretations, narrative comparisons, and illustrative tables where appropriate. The aim is to provide a holistic and evidence-driven understanding of how Blockchain-IoT integration transforms security frameworks within urban digital infrastructures, the challenges that emerge, and the implications for future urban development. The thematic analysis revealed four overarching categories of findings: a) enhancement of IoT security through Blockchain, b) improvements in data integrity, transparency, and authentication, c) facilitation of decentralized, autonomous smart city operations, and d) challenges and limitations affecting the integration of the two technologies. Each theme is elaborated through detailed narrative interpretation supported by reviewed data.

4.1. Strengthening IoT Security through Blockchain Integration

The findings converged strongly on the view that Blockchain significantly strengthens the security landscape of IoT-driven smart city ecosystems. Analysis of evaluated studies revealed that IoT networks, despite their transformative potential, face substantial vulnerabilities arising from centralized architectures, limited device processing power, insecure communication channels, and heterogeneous systems lacking standardized security protocols. Blockchain was consistently identified as a transformative solution due to its decentralized structure, cryptographically enforced trust, and tamper-proof ledger. Through decentralization, Blockchain distributes authority across multiple nodes, thereby eliminating single points of failure that are easily exploited in traditional centralized IoT systems. The findings showed that when IoT devices communicate through Blockchain-based distributed networks, the risk of Distributed Denial of Service (DDoS) attacks, unauthorized access, or large-scale data manipulation is dramatically reduced. This was supported by case studies in smart transportation and smart energy, where Block-

chain frameworks mitigated common vulnerabilities that previously compromised sensor networks, public utility meters, and intelligent traffic control systems. Recent frameworks, such as decentralized trust models with AI anomaly detection, achieve up to 98% threat detection rates. Table 2 lists common IoT vulnerabilities pre-blockchain, categorized by type (e.g., centralized failures, data breaches, tampering), with examples from smart city sectors like transportation and energy [11].

Table 2. Identified IoT security vulnerabilities before blockchain integration.

IoT Security Issue	Description	Impact on smart cities
Centralised servers	Single node controls data and access	System-wide collapse during an attack
Weak authentication	IoT devices lack strong identity verification	Device spoofing and unauthorized access
Data tampering risk	Cloud-stored data can be altered	False decisions in traffic, energy, health
Device cloning	Attackers replicate devices	Injecting false data into city systems
Network eavesdropping	Unsecured communication channels	Leakage of sensitive city information

The narrative across reviewed literature was consistent: Blockchain's decentralized consensus mechanisms make it computationally impractical for attackers to alter or falsify data across the network, thus providing a robust protective layer over IoT operations. Even in cases where a device is compromised, the attacker cannot manipulate system-wide records due to the immutability of the distributed ledger. This resilience significantly enhances trustworthiness and stability in vital smart city functions such as emergency response, healthcare monitoring, environmental surveillance, and digital governance.

4.2. Enhancing Data Integrity, Transparency and Authentication

The findings of this paper demonstrated that Blockchain substantially improves data integrity within smart city infrastructures by ensuring that all IoT-generated data is permanently and immutably recorded on a distributed ledger. Traditional IoT systems rely heavily on cloud databases that can be overwritten, manipulated, or deleted by internal or external actors. Blockchain's cryptographic hashing and timestamping ensure that once data is entered into the ledger, it cannot be altered without network consensus, effectively eliminating undetected tampering. This characteristic is particularly crucial in sensitive smart city domains such as public health monitoring, law enforcement surveillance, utility billing, and environmental data tracking. The findings revealed that Blockchain-supported IoT systems in healthcare ensure that patient vitals recorded through wearable devices remain authentic, verifiable, and resistant to unauthorized changes, thereby strengthening patient safety and medical decision-making. Table 3 details benefits from case

studies, including improved tamper resistance, auditability, transparency, and sector-specific advantages (e.g., in public health and utilities), with qualitative and quantitative metrics.

Table 3. Perceived benefits of blockchain-based data integrity from reviewed case studies.

Smart City Sector	Data Integrity Benefit	Evidence from Case Studies
Smart healthcare	Unalterable patient records	Remote monitoring projects in Estonia
Smart energy	Prevents meter tampering and fraud	Peer-to-peer trading in Australia
Public safety	Ensures authenticity of surveillance data	Blockchain-based CCTV integrity pilots
Environmental monitoring	Validates pollution and climate data	Smart environmental systems in Singapore
Smart mobility	Secures V2V and V21 communication	Blockchain-enabled autonomous traffic pilots

In addition to data integrity, Blockchain dramatically improved authentication processes within IoT ecosystems. The findings highlighted that Blockchain facilitates the creation of unique cryptographic identities for each IoT device, replacing traditional centralized authentication servers with a decentralized alternative. Smart contracts further automate access control, enabling dynamic, rule-based verification that prevents unauthorized devices from joining or interacting with the network. This decentralized identity management system proved particularly valuable in high-risk domains such as smart buildings, autonomous vehicles, and distributed utility infrastructures, where device authenticity directly influences safety, operational stability, and public confidence in technology-driven services.

4.3. Enabling Decentralized and Autonomous Smart City Operations

A major theme that emerged from the analysis was the extent to which Blockchain enables decentralized, autonomous, and citizen-driven smart city applications. Findings from energy, waste management, transportation, and supply chain case studies showed that Blockchain facilitates peer-to-peer interactions without requiring centralized intermediaries, thus promoting transparency, reducing costs, and improving operational efficiency. In smart energy grids, for example, households with solar installations can autonomously trade excess electricity with neighbors using Blockchain-based smart contracts that calculate prices and verify transactions without human intervention. This results in faster transactions, lower energy costs, and greater citizen participation in energy markets. Recent integrations demonstrate up to 15% energy cost reductions through optimized demand-response [13].

The reviewed studies also highlighted Blockchain's ability to strengthen smart mobility services by securing communications between vehicles and infrastruc-

ture components, preventing the manipulation of navigation data, and reducing cyberattack risks in autonomous driving systems. Decentralized waste management solutions also emerged as a significant finding, where Blockchain systems track waste collection routes, recycling streams, and disposal records, reducing corruption, improving accountability, and enhancing municipal service delivery. The findings affirm that Blockchain-IoT integration paves the way for autonomous systems that operate with minimal human oversight while maintaining transparency and auditability.

4.4. Limitations, Challenges and Barriers to Integration

The findings also revealed several challenges that impede the seamless integration of Blockchain and IoT technologies in smart city environments. Scalability emerged as a prominent issue, as Blockchain networks, particularly public blockchains, struggle to process the massive volumes of data generated by IoT devices. High transaction latency and limited throughput reduce the feasibility of using Blockchain in real-time operations such as traffic management or emergency response. Energy consumption was also identified as a major barrier, with traditional consensus mechanisms such as Proof of Work requiring significant computational power incompatible with low-energy IoT devices. Interoperability challenges were widespread, stemming from the diversity of IoT devices, communication protocols, and Blockchain frameworks, which complicate the creation of unified integration architectures. Recent studies note additional barriers like lack of expertise and compliance with data protection laws [10].

Regulatory uncertainty also emerged as a major theme, with many jurisdictions lacking policies that govern digital identities, cross-border data flows, Blockchain-based transactions, and cryptographic compliance. Privacy concerns were especially relevant in public Blockchains where transaction transparency can expose user behavior or sensitive city data unless advanced privacy-preserving technologies like zk-SNARKs or private sidechains are deployed. These findings collectively demonstrate that while the integration of Blockchain and IoT holds immense promise, the realization of its full potential will require technological innovation, policy development, and standardization efforts.

4.5. Summary of Findings

The findings collectively demonstrate that integrating Blockchain and IoT significantly enhances the security, reliability, and operational autonomy of smart city systems. Blockchain mitigates IoT vulnerabilities through decentralized trust, immutable data storage, automated authentication, and transparent transaction records. It enables decentralized urban services such as energy trading, waste tracking, and autonomous mobility, supporting more sustainable and citizen-centric smart city models. However, scalability constraints, high energy consumption, interoperability issues, and regulatory gaps pose substantial challenges to widespread adoption. The findings highlight that achieving secure Blockchain-IoT in-

tegration will require hybrid Blockchain architectures, lightweight consensus mechanisms, robust data governance frameworks, and cross-sector collaboration among policymakers, technology developers, and urban planners.

5. Conclusions

The conclusions drawn from this paper indicate that integrating Blockchain and IoT presents a viable and highly impactful approach for securing smart city solutions. The study concludes that Blockchain fundamentally improves IoT security by decentralizing system control, strengthening device authentication, and ensuring immutable data storage. These features protect smart city infrastructures from cyberattacks, data tampering, and system disruptions, ultimately enabling more trustworthy and resilient urban environments.

The study further concludes that Blockchain enhances transparency and accountability in data-driven decision-making, supporting efficient management of essential services such as healthcare, energy, mobility, waste management, and public safety. The immutable and auditable nature of Blockchain-based data ensures that government agencies, private service providers, and citizens operate within a system of verifiable trust.

The paper also concludes that Blockchain fosters greater autonomy and citizen participation in smart city services by smart contracts. These decentralized systems, reducing operational costs, enhance service delivery speeds, and minimize corruption risks. Nonetheless, despite these advantages, the study concludes that Blockchain-IoT integration is not without challenges, particularly regarding scalability, interoperability, energy efficiency, and regulatory compliance. These issues must be addressed through technological innovations, policy development, standardization, and cross-sector collaboration. The overall conclusion is that Blockchain, when strategically implemented alongside IoT, has the potential to significantly advance the development of secure, efficient, and sustainable smart cities.

6. Recommendations

Based on the findings and conclusions of this study, several recommendations are proposed to support the effective integration of Blockchain and IoT in smart city solutions.

- The adoption of lightweight consensus mechanisms such as Proof of Authority or Delegated Proof of Stake, which consume less energy and are better suited for IoT. Additionally, integrating AI for threat detection and optimization is advised to enhance security and efficiency [11].
- Develop clear regulatory frameworks that address digital identity management, data privacy, smart contract enforceability, and cross-border data exchange to ensure compliance, protect citizens, and encourage investment in Blockchain-based smart city infrastructures.
- Extensive capacity-building programs to enhance the skills and knowledge of stakeholders involved in smart city development.

7. Future Research Directions

Future research should explore the development of more advanced, energy-efficient consensus mechanisms that can support large-scale IoT deployments without compromising sustainability. Additional studies are needed to investigate how privacy-preserving technologies such as zero-knowledge proofs, homomorphic encryption, and secure multi-party computation can be incorporated into Blockchain-IoT systems to enhance user confidentiality. Future studies may further examine ethical implications of decentralized smart city governance and explore models for balancing transparency with individual privacy rights. Finally, there is a need for empirical research involving real-world pilot implementations to assess performance, security, and user acceptance under practical conditions.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Finck, M. (2019) Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law? European Parliament, Scientific Foresight Unit (STOA).

[2] Brachuk, A. (2018) The International Standards of Single Window System for the Foreign Trade. *Lex portus*, **1**, 93-104. https://doi.org/10.26886/2524-101x.1.2018.7

[3] Morris, K. (2019) Blockchain in Trade Finance and Supply Chain. EU Blockchain Observatory and Forum.

[4] Allen, D.W.E., Berg, C., Davidson, S., Novak, M. and Potts, J. (2019) International Policy Coordination for Blockchain Supply Chains. *Asia & the Pacific Policy Studies*, **6**, 367-380. https://doi.org/10.1002/app5.281

[5] Dorri, A., Kanhere, S.S., Jurdak, R. and Gauravaram, P. (2017) Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. 2017 *IEEE International Conference on Pervasive Computing and Communications Workshops* (*PerCom Workshops*), Kona, 13-17 March 2017, 618-623.

[6] Xu, X., Weber, I. and Staples, M. (2021) Architecture for Blockchain Applications. Springer.

[7] Roman, R., Zhou, J. and Lopez, J. (2013) On the Features and Challenges of Security and Privacy in Distributed Internet of Things. *Computer Networks*, **57**, 2266-2279. https://doi.org/10.1016/j.comnet.2012.12.018

[8] Harzing, A. and Alakangas, S. (2015) Google Scholar, Scopus and the Web of Science: A Longitudinal and Cross-Disciplinary Comparison. *Scientometrics*, **106**, 787-804. https://doi.org/10.1007/s11192-015-1798-9

[9] Crosby, M., *et al.* (2016) Blockchain technology: Beyond Bitcoin. *Applied Innovation Review*, No. 2, 6-19.

[10] Alzoubi, Y.I., *et al.* (2025) Blockchain for Sustainable Smart Cities: Motivations and Challenges. Digital.

[11] Ali, A., *et al.* (2025) Decentralized Trust Framework for Smart Cities: A Block-Chain-Enabled Cybersecurity and Data Integrity Model. *Scientific Reports*, **15**, Article No. 23454.

[12] Zanella, A., Bui, N. and Castellani, A. (2019) Smart City Solutions Using IoT. *IEEE*

Internet of Things Journal, **1**, 22-32.

[13] Elhajj, M., Attar, A.E. and Mikati, A. (2025) Integrating IoT and Blockchain for Smart Urban Energy Management: Enhancing Sustainability through Real-Time Monitoring and Optimization. *Cluster Computing*, **28**, Article No. 960. https://doi.org/10.1007/s10586-025-05677-3

[14] Atzori, L., Iera, A. and Morabito, G. (2010) The Internet of Things: A Survey. *Computer Networks*, **54**, 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[15] Upperton, T., Epps, T. and Carey, B. (2019) Revolutionizing Global Supply Chains One Block at a Time: Growing International Trade with Blockchain: Are International Rules up to the Task? *Global Trade and Customs Journal*, **14**, 136-145. https://doi.org/10.54648/gtcj2019013

[16] Berryhill, J. and Hanson, A. (2018) Blockchains Unchained: Blockchain Technology and its use in the Public Sector. OECD Working Papers on Public Governance, No. 28.

[17] Bughin, J., LaBerge, L. and Mellbye, A. (2018) The Case for Digital Reinvention. McKinsey Quarterly.

[18] Álvarez-García, J., del Río-Rama, M., de la, C. and Durán-Sánchez, A. (2018) Sustainable Smart Cities in the Scientific Literature: A Bibliometric Analysis. *Sustainability*, **10**, Article 3896.

[19] Koseoglu, M.A., Rahimi, R., Okumus, F. and Liu, J. (2016) Bibliometric Studies in Tourism. *Annals of Tourism Research*, **61**, 180-198. https://doi.org/10.1016/j.annals.2016.10.006

[20] Brzezinski, M. (2015) Power Laws in Citation Distributions: Evidence from Scopus. *Scientometrics*, **103**, 213-228. https://doi.org/10.1007/s11192-014-1524-z

[21] Rejeb, A., Rejeb, K., Simske, S.J. and Keogh, J.G. (2021) Blockchain Technology in the Smart City: A Bibliometric Review. *Quality & Quantity*, **56**, 2875-2906. https://doi.org/10.1007/s11135-021-01251-2