future internet

Review

Machine Learning for Blockchain and IoT Systems in Smart Cities: A Survey

Elias Dritsas * and **Maria Trigka**

Athena Research and Innovation Center, Industrial Systems Institute (ISI), 26504 Patras, Greece; trigka@isi.gr
* Correspondence: dritsas@isi.gr

Abstract: The integration of machine learning (ML), blockchain, and the Internet of Things (IoT) in smart cities represents a pivotal advancement in urban innovation. This convergence addresses the complexities of modern urban environments by leveraging ML's data analytics and predictive capabilities to enhance the intelligence of IoT systems, while blockchain provides a secure, decentralized framework that ensures data integrity and trust. The synergy of these technologies not only optimizes urban management but also fortifies security and privacy in increasingly connected cities. This survey explores the transformative potential of ML-driven blockchain-IoT ecosystems in enabling autonomous, resilient, and sustainable smart city infrastructure. It also discusses the challenges such as scalability, privacy, and ethical considerations, and outlines possible applications and future research directions that are critical for advancing smart city initiatives. Understanding these dynamics is essential for realizing the full potential of smart cities, where technology enhances not only efficiency but also urban sustainability and resilience.

Keywords: smart cities; machine learning; blockchain technology; internet of things; analysis

check for updates

Citation: Dritsas, E.; Trigka, M. Machine Learning for Blockchain and IoT Systems in Smart Cities: A Survey. *Future Internet* **2024**, *16*, 324. https://doi.org/10.3390/fi16090324

Academic Editors: Dinh-Thuan Do and Cheng-Chi Lee

Received: 22 August 2024
Revised: 2 September 2024
Accepted: 4 September 2024
Published: 6 September 2024

1. Introduction

The rapid and ongoing urbanization of global populations has fundamentally transformed the dynamics of modern cities, necessitating the development of advanced technological infrastructure capable of managing the increasing complexity of urban environments. At the heart of this transformation is the concept of smart cities—urban ecosystems that leverage cutting-edge technologies to optimize the efficiency of city services, enhance the quality of life for residents, and ensure sustainable development. The IoT and blockchain technologies constitute central concepts to this vision, serving as the backbone for data collection, processing, and secure management across diverse urban domains [1,2].

IoT systems enable the pervasive monitoring of urban infrastructure, generating an unprecedented volume of real-time data that can be used to make informed decisions in areas such as traffic management, energy distribution, waste disposal, and public safety. However, the sheer scale and complexity of IoT-generated data present significant challenges to processing, analysis, and security. The integration of ML within this framework offers a powerful means to address these challenges. ML algorithms, due to their ability to learn from data, identify patterns, and make predictions, are uniquely suited to extracting actionable insights from the vast and heterogeneous datasets produced by IoT devices [3,4].

Moreover, the decentralized nature of IoT systems introduces vulnerabilities, particularly related to data integrity, privacy, and security. Blockchain technology, thanks to a decentralized and immutable ledger system, provides a robust solution to these challenges, ensuring the secure and transparent management of data across the smart city ecosystem. The cooperation of ML, blockchain, and IoT thus presents a transformative approach to the development of smart cities, where data-driven decision-making is enhanced by secure and trustworthy information management [5,6].

Capitalizing on the previous studies, several focus areas were identified i.e., the importance of secure and scalable frameworks and data-driven decision-making, which guided the further exploration of how ML, blockchain, and IoT collaborate to create intelligent and resilient urban infrastructure. Nowadays, with IoT generating large-scale data, ML is essential for deriving insights, while blockchain ensures the need for data integrity and security. The insights gained from these studies helped to frame the survey's focus on the synergies and challenges of these technological fields. These areas are reflected in the structure and content of the paper and direct the literature review. The executed study was motivated by the need to make a focused presentation of works aimed at analyzing how the combination of ML, blockchain, and IoT can address these rising issues in smart cities in the era of rapid urbanization. More specifically, this survey makes the following contributions:

- It examines the application of ML in IoT systems and the role of blockchain in enhancing security within smart cities.
- The survey identifies potential synergies between ML, blockchain, and IoT to create more intelligent and secure urban environments.
- It highlights key challenges, such as scalability and ethical considerations, and outlines future research directions.

The key topics explored in the subsequent sections are depicted in Figure 1, which reflects the structure of the work. The paper is organized as follows. Section 2 details the integration of ML into IoT systems for smart cities. Section 3 explores blockchain for security and data integrity in smart cities. Moreover, Section 4 discusses the synergy of ML, blockchain, and IoT in smart cities. Section 5 outlines challenges and future directions. Finally, Section 6 summarizes the findings of this survey.

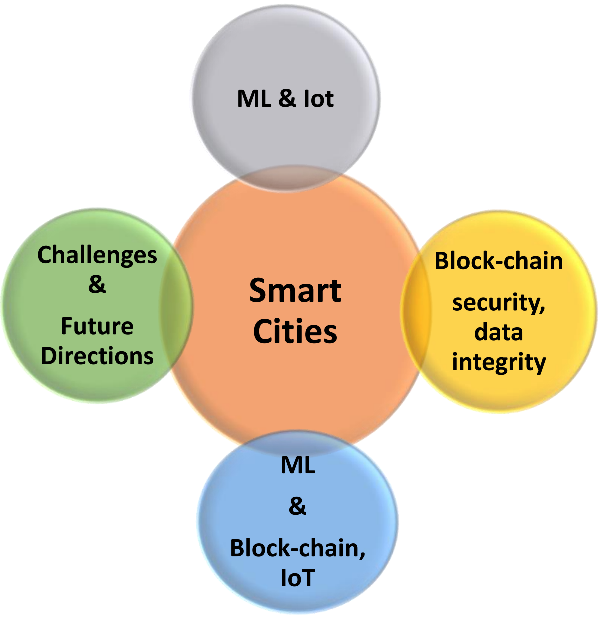
ML & Iot
Challenges & Future Directions
Smart Cities
Block-chain security, data integrity
ML & Block-chain, IoT

Figure 1. Overview of the survey focus areas.

2. Machine Learning in IoT Systems for Smart Cities

In the context of smart cities, the integration of ML into IoT systems transcends conventional data processing and analytics, offering sophisticated mechanisms for real-time decision-making, anomaly detection, and system optimization. The complexity and scale of urban IoT networks necessitate the deployment of advanced ML models that can operate efficiently under constraints such as limited computational power, varying network conditions, and the need for real-time responsiveness [7–10].

Deep learning (DL) models, particularly convolutional neural networks (CNNs) and recurrent neural networks (RNNs), are pivotal in extracting high-level features from vast, heterogeneous IoT data streams. For instance, CNNs are instrumental in processing visual data from city-wide surveillance systems, enabling real-time recognition of patterns related to traffic density, pedestrian movement, and even criminal activity [11–14]. RNNs, with their ability to handle sequential data, excel in predictive maintenance scenarios, where they can analyze time-series data from sensors to forecast equipment failures with high accuracy [15–18].

Moreover, the advent of federated learning (FL) has addressed the challenges of data privacy and decentralized data processing in smart cities. FL allows ML models to be trained across multiple edge devices—such as sensors, cameras, and actuators—without the need to centralize data. This approach not only mitigates privacy concerns by ensuring that sensitive data remain on the device but also reduces the latency and bandwidth requirements associated with transmitting data to a central server for processing. In smart cities, FL facilitates the creation of robust, localized models that are capable of adapting to the specific conditions of different urban areas, thereby enhancing the overall efficiency and responsiveness of IoT systems [19–22].

In addition to predictive analytics, reinforcement learning (RL) has emerged as a powerful tool for dynamic optimization in smart city IoT systems. RL algorithms enable IoT devices to learn optimal strategies through trial and error, continuously improving their performance in dynamic environments. For example, in smart traffic management, RL-based systems can dynamically adjust traffic signal timings in response to real-time traffic conditions, leading to significant reductions in congestion and travel time. Similarly, in smart energy grids, RL can optimize the distribution of energy in real time, balancing supply and demand while minimizing energy loss and maximizing the use of renewable sources [23–27].

Another critical aspect of ML in IoT for smart cities is anomaly detection. As urban IoT systems are inherently complex and operate in unpredictable environments, the ability to detect anomalies—such as unusual traffic patterns, abnormal energy consumption, or unauthorized access to sensitive areas—is crucial for maintaining the security and efficiency of the city. Advanced ML techniques, including unsupervised learning and deep anomaly detection methods, are particularly effective in identifying these anomalies. These techniques can autonomously learn the normal operating patterns of various systems and flag deviations that may indicate potential issues or security threats. For instance, autoencoders—a type of neural network—can be employed to compress and reconstruct data, with significant reconstruction errors signaling potential anomalies that require further investigation [28–32].

What is more, integrating transfer learning into IoT systems enables the adaptation of pre-trained ML models to new urban environments with minimal additional data. This capability is especially valuable in smart cities, where the conditions and requirements can vary significantly across different regions. Transfer learning allows models trained on data from one part of the city—or even from another city entirely—to be quickly adapted to new contexts, thereby accelerating the deployment of intelligent IoT solutions and reducing the time and resources needed for training [33–37].

In summary, applying advanced ML techniques in IoT systems for smart cities extends far beyond traditional analytics, enabling real-time, adaptive, and context-aware solutions that can handle the complexities of modern urban environments. These capabilities are essential for the continuous improvement and optimization of smart city systems, ensuring that they can meet the evolving needs of urban populations while maintaining security, efficiency, and resilience [38–41]. Table 1 provides a comprehensive summary of the artificial intelligence (AI), ML, and DL approaches employed in smart cities, detailing the methodologies and innovations that drive these intelligent systems. By encapsulating the key contributions of each approach, the table offers a clear comparison of their impact on enhancing urban management and the overall functionality of smart city ecosystems.

Table 1. Use of AI, ML, and DL approaches in IoT for smart cities.

Approach	References	Summary
AI & ML	[7–10]	Application of AI and ML for smart governance, traffic control, healthcare, crime forecasting, and more in smart cities.
CNN-based	[11–14]	Use of CNNs for pedestrian detection, traffic signal optimization, crime prediction, and malware detection.
RNN-based	[15–18]	Application of RNNs for time-series prediction, environmental noise prediction, and small-object detection in industrial settings.
FL	[19–22]	Privacy-preserving data analysis and decentralized data processing in smart cities using FL techniques.
RL-based	[23–27]	Use of RL for optimizing traffic signal control, autonomous vehicles, smart energy grids, and other IoT systems in smart cities.
Deep & Unsupervised Learning	[28–32]	Application of deep and unsupervised learning techniques for anomaly detection in IoT systems within smart cities.
Transfer Learning	[33–37]	Research on the application of transfer learning for IoT, smart buildings, IoT attack detection, and secure data fusion in industrial IoT.
IoT and Smart Cities—Overview	[38–41]	Overview of technologies, practices, and challenges related to IoT in smart cities, including a broad analysis of IoT ecosystems and their development in urban settings.

3. Blockchain for Security and Data Integrity in Smart Cities

In the intricate landscape of smart cities, where millions of interconnected IoT devices continuously generate and exchange data, ensuring the security and integrity of these data is paramount. Blockchain technology emerges as a critical solution, providing a decentralized and immutable framework that addresses these pressing concerns [42].

The decentralized nature of blockchain aligns seamlessly with the distributed architecture of IoT systems, creating a robust foundation for secure data management. Each transaction or data exchange in a blockchain network is recorded in a cryptographically secured block, which is then linked to the previous block, forming a chain. This immutable ledger ensures that once data are recorded they cannot be altered or tampered with, providing an unprecedented level of data integrity. This characteristic is particularly vital in smart cities, where the reliability of data directly impacts the efficacy of urban management systems, from traffic control to energy distribution [43–46].

Blockchain also enhances security through its consensus mechanisms, which require network participants to agree on the validity of transactions before they are added to the blockchain. This consensus process significantly reduces the risk of data manipulation, as altering the blockchain would require the collusion of a majority of participants, which is computationally infeasible in well-designed networks. This property is crucial in protecting against various cyber threats that target centralized databases, such as Distributed Denial of Service (DDoS) attacks, data breaches, and unauthorized data modifications [47–51].

While blockchain technology excels in ensuring data integrity and transparency through its decentralized ledger system, it faces significant challenges, particularly in terms of scalability and privacy. FL offers an alternative decentralized approach that focuses on maintaining data privacy by keeping data localized on edge devices. Unlike blockchain, which requires data to be recorded on a public ledger, FL trains machine learning models directly on the devices without transferring the raw data, thereby inherently preserving privacy through techniques such as differential privacy [52–55].

However, while FL enhances privacy and reduces the risks of data breaches, it comes with its own set of vulnerabilities, such as potential exposure to model poisoning attacks where malicious participants can compromise the model's integrity. This contrasts with blockchain's strength in data integrity and security, which is ensured through cryptographic mechanisms and consensus protocols. Therefore, the choice between implementing blockchain or FL in IoT systems should be based on the specific needs of the application, particularly in balancing the demands for privacy, security, and scalability [56–59].

Moreover, blockchain's role in ensuring data provenance and traceability is indispensable in smart cities. In complex urban environments, where data from multiple sources are continuously integrated and analyzed, the ability to trace the origin and modifications of data becomes essential for accountability and transparency. Blockchain provides an unalterable history of data transactions, enabling city administrators and stakeholders to verify the authenticity and source of the data. This traceability is particularly beneficial in critical applications such as public health monitoring, where accurate data provenance is necessary to make informed decisions during emergencies, such as disease outbreaks or environmental hazards [60–63].

Smart contracts, another pivotal feature of blockchain, further augment security and operational efficiency in smart cities. These self-executing contracts with predefined rules and conditions automate and enforce agreements between parties without the need for intermediaries. In smart city applications, smart contracts can streamline a wide range of processes, from automated billing and payments in smart utilities to real-time traffic management systems. By embedding these contracts into blockchain, cities can ensure that all transactions and processes are executed as intended, with full transparency and without the risk of human error or corruption [64–68].

However, the integration of blockchain in smart cities is not without challenges. The scalability of blockchain networks is a significant concern, especially as the number of IoT devices continues to grow exponentially. Traditional blockchain systems, such as Bitcoin or Ethereum, face limitations in transaction throughput and latency, which could hinder their application in high-density urban environments. To address these challenges, advancements in blockchain technologies, such as sharding, sidechains, and layer-two solutions, are being explored. These innovations aim to enhance the scalability and performance of blockchain networks, making them more suitable for the demands of smart cities [69–72].

Furthermore, the energy consumption of blockchain, particularly in proof-of-work consensus mechanisms, poses a sustainability challenge in the context of smart cities. Since smart cities are designed to promote sustainability and energy efficiency, integrating energy-intensive blockchain systems could be counterproductive. Therefore, there is a growing interest in alternative consensus mechanisms, such as proof of stake or proof of authority, which offer lower energy footprints while maintaining security and decentralization [73–75].

In conclusion, blockchain technology plays a critical role in securing IoT systems and ensuring data integrity in smart cities. Its decentralized, immutable, and transparent nature provides robust protection against data tampering and cyber threats, while smart contracts streamline and secure urban processes. However, the successful implementation of blockchain in smart cities will require addressing the challenges of scalability and energy consumption, ensuring that these systems can meet the demands of rapidly growing urban environments while supporting the broader goals of sustainability and resilience [76–78]. Table 2 offers an overview of the contributions of blockchain technology within smart cities, highlighting its applications in enhancing security, data integrity, and operational efficiency. This table illustrates the studies discussed in this section, providing a compact summary of blockchain's role and impact across smart city infrastructure.

Table 2. Use of blockchain in smart cities.

Topic	References	Description
Blockchain for Security & Data Integrity	[42–46]	Discusses the role of blockchain in enhancing security and ensuring data integrity within IoT systems in smart cities, focusing on aspects like cryptographic security and protection against cyber threats.
Blockchain & Cybersecurity	[47–51]	Focuses on how blockchain can be used to prevent cyber threats, such as DDoS attacks, data breaches, and unauthorized data modifications in IoT networks.
FL vs Blockchain for Privacy	[52–55]	Compares FL to blockchain, focusing on how these technologies maintain data privacy and security in smart city environments, with blockchain ensuring data integrity through decentralized ledgers.
Blockchain & FL Integration Challenges	[56–59]	Discusses the challenges of integrating blockchain with FL in IoT systems, including issues like model poisoning and balancing privacy with security.
Blockchain Integration in Smart Cities	[60–63]	Examines the integration of blockchain technology into smart city infrastructure, highlighting its use in public health monitoring, energy management, and urban governance.
Smart Contracts & Blockchain	[64–68]	Explores the application of smart contracts within blockchain frameworks in smart cities, enabling automated processes like energy trading and enhancing transparency in urban management.
Blockchain Scalability & Performance	[69–72]	Discusses challenges related to the scalability of blockchain networks in smart cities, and explores solutions like sharding and layer-two protocols to improve performance.
Consensus Mechanisms in Blockchain	[73–75]	Evaluates different blockchain consensus mechanisms (e.g., proof of stake, sharding) and their impact on scalability, energy efficiency, and security in smart cities.
Blockchain & Smart City Applications	[76–78]	Provides insights into the practical applications of blockchain in smart cities, including challenges and opportunities for enhancing urban resilience and sustainability through blockchain technology.

4. Synergy of Machine Learning, Blockchain, and IoT in Smart Cities

This section emphasizes (i) in the first part, the shared aspects of ML, blockchain, and IoT, emphasizing how these technologies complement each other in the context of smart cities, and, in the second part, following the discussion of their shared characteristics, and (ii) the unique contributions and specific roles each technology plays in the broader smart city ecosystem.

4.1. Similar Aspects

The technological integration of ML, blockchain, and IoT in smart cities is driven by several key similarities. First, all three technologies drive data-driven decision-making. ML analyzes vast datasets from IoT devices to optimize urban operations in real-time, while IoT continuously collects essential data across city services. Blockchain ensures the integrity and security of these data, enabling reliable decision-making processes. Another commonality is decentralization; ML benefits from decentralized data processing methods like FL, which reduces latency and enhances privacy. Similarly, IoT networks are inherently decentralized, with numerous devices operating autonomously. Blockchain complements these by providing a decentralized, secure framework that ensures no single point of control over data, aligning perfectly with the distributed nature of IoT and ML. In addition to data-driven decision-making and decentralization, scalability and adaptability are shared challenges and goals. ML models need to scale and adapt to growing data volumes and varying urban conditions, as IoT systems do, and must handle increasing devices and fluctuating network demands. Finally, although blockchain faces scalability challenges, particularly with the rise in IoT transactions, advanced solutions are being developed to enhance its scalability and performance.

4.2. Distinct Interactions and Complementary Roles

While ML, blockchain, and IoT share several similarities in their approach to enhancing smart city infrastructure, each technology also brings distinct capabilities and plays complementary roles, essential for developing intelligent urban environments. The cooperation between ML, blockchain, and the IoT in smart cities goes beyond mere technological integration; it embodies a sophisticated interplay of advanced computational models, decentralized frameworks, and interconnected systems that collectively enable the evolution of urban environments into intelligent, adaptive, and secure ecosystems. The confluence of these technologies empowers smart cities to operate at an unprecedented level of efficiency and resilience by facilitating real-time decision-making, enhancing data security, and enabling seamless collaboration across diverse urban subsystems [79–82].

At the core of this synergy lies the ability of ML algorithms to extract actionable insights from the vast, heterogeneous data generated by IoT devices. These insights drive autonomous decision-making processes that are crucial for managing the dynamic and complex nature of urban systems. For example, ML models can continuously learn from traffic sensor data, optimizing traffic flows and reducing congestion in real time. In energy grids, ML predicts consumption patterns, optimizing energy distribution and reducing waste, which are vital for sustainability in densely populated urban areas [83–86].

Blockchain technology, with its decentralized and immutable ledger, complements ML by ensuring that the data feeding these models are both secure and trustworthy. The integrity of data is paramount in smart cities, where decisions impact millions of lives. Blockchain's consensus mechanisms and cryptographic protocols ensure that data originating from IoT devices remain unaltered and verifiable, which is critical when ML models are used to automate crucial services like emergency response, healthcare, or financial transactions [87–90].

Moreover, the integration of smart contracts within blockchain frameworks allows for the automation of processes based on predefined conditions, further enhancing the efficiency of IoT systems. For instance, in smart grids, blockchain-enabled smart contracts can automatically execute transactions between energy producers and consumers, based on real-time data processed by ML algorithms. This not only streamlines operations but also minimizes human intervention, reducing the potential for errors and fraud [91–94].

The interoperability between these technologies facilitates a level of collaboration across different sectors of a smart city that would be impossible with siloed systems. For example, ML can be employed to forecast maintenance needs for infrastructure, while blockchain securely records all relevant data and transactions, ensuring transparency and accountability. This creates a feedback loop where data are continuously refined and used to improve both the efficiency and security of urban systems [95–98].

Additionally, the combination of ML, blockchain, and IoT fosters an environment where data privacy is rigorously protected while enabling the data-driven innovation that smart cities require. FL, an advanced ML technique that allows models to be trained on decentralized data, can be coupled with blockchain to ensure that sensitive data never leave their source while contributing to global models. This is particularly crucial in areas such as healthcare, where privacy concerns are paramount [99–102].

In a nutshell, the synergy of ML, blockchain, and IoT in smart cities is not merely a combination of technologies but a sophisticated ecosystem where data-driven intelligence, security, and autonomy are seamlessly integrated to create urban environments that are not only smart but also resilient, sustainable, and responsive to the needs of their inhabitants. This triad of technologies holds the potential to redefine urban life, paving the way for cities that are not only more efficient and secure but also more equitable and inclusive [103–106]. Table 3 offers a comprehensive overview of this collaboration, illustrating how these technologies interact to transform various facets of smart city infrastructure. The table highlights key applications and demonstrates the combined strengths of ML, blockchain, and IoT in driving forward innovation, resilience, and sustainable urban development.

Table 3. The synergy of ML, blockchain, and IoT in smart cities.

Topic	References	Description
ML, Blockchain & IoT	[79–82]	Discussion on the synergy and integration of ML, blockchain, and IoT in smart cities.
ML in IoT	[83–86]	Application of ML within IoT systems for smart city services like traffic management, energy optimization, and anomaly detection.
Blockchain for Automation & Integrity	[87–94]	Use of blockchain and smart contracts to automate processes and ensure data integrity in smart cities.
Interoperability & Data Privacy	[95–98]	Challenges and solutions related to interoperability among systems and maintaining data privacy in smart city integrations.
FL & Security	[99–102]	Use of FL in IoT environments to enhance security and privacy with blockchain integration.
Privacy-Preserving Frameworks	[103–106]	Focuses on privacy-preserving frameworks using blockchain and ML to ensure secure and private data management in IoT-driven smart cities.

5. Challenges and Future Directions

The integration of ML, blockchain, and IoT in smart cities, while promising, encounters a myriad of sophisticated challenges that demand careful consideration and innovative solutions. One of the foremost challenges lies in the computational demands of ML algorithms, particularly in the context of large-scale IoT networks. These networks generate immense numbers of data that must be processed in real time to maintain the efficacy of smart city operations. The complexity of deploying ML models on resource-constrained devices at the edge of the network exacerbates this issue. Current advancements in edge computing, while notable, remain insufficient for the seamless execution of ML algorithms that require significant processing power and memory. Consequently, there is a pressing need for the development of more efficient, lightweight ML models that can operate under the stringent constraints of IoT environments without compromising performance [107–109].

Scalability poses another critical challenge, particularly in the context of blockchain technology. As the proliferation of IoT devices in smart cities accelerates, blockchain networks must contend with an ever-increasing number of transactions. Traditional blockchain architectures, reliant on resource-intensive consensus mechanisms like proof of work, struggle to maintain performance and throughput at scale. This scalability bottleneck not only hampers the real-time processing of transactions but also raises concerns about energy consumption and latency. Emerging solutions such as sharding and layer-2 protocols, and alternative consensus mechanisms like proof of stake offer potential pathways to enhanced scalability. However, these innovations must be rigorously tested and optimized for integration within the complex, multi-layered ecosystems of smart cities, where the interplay between various subsystems demands seamless, high-throughput communication [110–112].

Interoperability represents yet another significant hurdle. The diversity of IoT devices, blockchain platforms, and ML frameworks within a smart city ecosystem introduces challenges related to standardization and compatibility. The lack of standardized protocols for data exchange and integration can lead to fragmented systems that fail to communicate effectively, undermining the overall coherence and efficiency of smart city operations. Addressing this issue requires the development of universal standards and protocols that facilitate interoperability across heterogeneous systems. Furthermore, cross-chain interoperability within blockchain networks must be advanced to enable the seamless transfer of data and value across different blockchain platforms, which is crucial for the decentralized management of smart city resources [113–115].

The convergence of these technologies also introduces profound ethical and governance challenges. The deployment of ML algorithms in critical decision-making processes within smart cities raises concerns about transparency, accountability, and algorithmic bias. These issues are further compounded by the immutable nature of blockchain, which, while enhancing data security, also risks perpetuating errors or biases embedded in the data or smart contracts. To mitigate these risks, it is essential to establish robust ethical frameworks and governance structures that ensure the responsible development and deployment of these technologies. This includes implementing mechanisms for auditing ML models and blockchain-based systems, as well as developing strategies for the equitable distribution of the benefits derived from smart city innovations [116–118].

Privacy concerns are paramount in the smart city context, where the aggregation and analysis of vast amounts of personal data are necessary for the optimization of urban services. The tension between the need for data-driven insights and the protection of individual privacy is a significant challenge. While blockchain offers potential solutions through decentralized identity management and encrypted data storage, these approaches must be carefully balanced against the need for transparency and accountability in public systems. The development of privacy-preserving technologies, such as homomorphic encryption and FL, is crucial to enabling secure, privacy-respecting data analysis in smart cities. However, these technologies are still in their infancy and require substantial research and development to become viable at scale [119–121].

Overall, while the integration of ML, blockchain, and IoT in smart cities holds immense potential, it is accompanied by complex challenges that necessitate ongoing research and innovation. Addressing the computational demands of ML, enhancing the scalability and interoperability of blockchain, and establishing robust ethical and governance frameworks are critical to realizing the vision of truly intelligent and secure urban environments. As these technologies continue to mature, their successful convergence will be pivotal in shaping the future of urbanization, driving not only technological advancement but also societal transformation [122–124]. Table 4 provides a detailed taxonomy of these key challenges, serving as a reference and offering insights into the obstacles that need to be overcome to ensure the successful deployment of these technologies in urban environments.

Table 4. A taxonomy of topics in key challenges and reference works.

Topic	References	Description
Computational Demands in ML	[107–109]	Discusses the challenges related to the computational demands of ML algorithms in IoT environments.
Scalability in Blockchain	[110–112]	Explores issues related to the scalability of blockchain technologies, especially in the context of IoT networks in smart cities, and potential solutions.

Table 4. *Cont.*

Topic	References	Description
Interoperability in Smart Cities	[113–115]	Focuses on the challenges and solutions related to interoperability among diverse systems in smart cities.
Ethical & Governance Challenges	[116–118]	Addresses the ethical implications and governance challenges of integrating ML, blockchain, and IoT in smart cities, including issues of transparency and bias.
Privacy-Preserving Technologies	[119–121]	Covers the use of privacy-preserving technologies, such as homomorphic encryption and FL, in ensuring secure and private data handling in smart cities.
Trustworthy & Secure Frameworks	[122–124]	Focuses on developing secure and trustworthy frameworks that leverage blockchain, ML, and IoT for smart cities, ensuring robust security and privacy measures.

6. Conclusions

This paper has examined the integration of ML, blockchain, and IoT in smart city ecosystems, demonstrating how these technologies can collaboratively transform urban management and infrastructure. The synergy of these technologies represents more than just a technological advancement; it embodies a new approach to addressing the complexities of modern urbanization. By harnessing the analytical power of ML, the security and transparency of blockchain, and the real-time data collection capabilities of IoT, smart cities can achieve unprecedented levels of efficiency, resilience, and adaptability. When integrated, these technologies create a synergistic effect that amplifies their individual strengths, resulting in a holistic framework capable of managing the dynamic challenges of urban growth.

A key benefit of this synergy is its ability to tackle critical urban challenges such as scalability, interoperability, and ethical governance. By enabling more accurate and secure data-driven decision-making, these technologies ensure that smart cities can evolve sustainably and equitably. The implications are extensive, offering new opportunities for innovation in urban planning, resource management, and public service delivery.

The future of smart cities will depend on experts' ability to fully exploit this technological synergy. Continued research and interdisciplinary collaboration will be crucial in overcoming the challenges that arise. Prioritizing the development of advanced scalability solutions will be essential to enhance blockchain's capacity to support the dynamic and high-volume demands of smart cities. Concurrently, innovations in privacy-preserving technologies will be vital to safeguarding individual data while allowing for the effective use of ML in decentralized environments. Additionally, establishing robust ethical and governance frameworks will ensure that the deployment of these technologies aligns with societal values and public interest. By addressing these challenges, the field can make significant strides toward creating smart cities that are not only technologically advanced but also socially responsible, sustainable, and inclusive. These advancements will ultimately redefine urban life, making cities smarter, safer, and more responsive to the needs of their inhabitants.

In summary, the foundations laid in this paper highlight the potential for significant advancements in smart city technologies and offer a roadmap for future exploration. This study emphasizes the importance of integrating ML, blockchain, and IoT while emphasizing the need for ongoing innovation to ensure that these technologies meet the ever-evolving demands of urban life. By deepening the understanding of these interconnected systems, we can pave the way for smarter, more sustainable cities that enhance the quality of life for all residents.

Author Contributions: E.D. and M.T. conceived of the idea, designed and performed the experiments, analyzed the results, drafted the initial manuscript and revised the final manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Majeed, U.; Khan, L.U.; Yaqoob, I.; Kazmi, S.A.; Salah, K.; Hong, C.S. Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. *J. Netw. Comput. Appl.* **2021**, *181*, 103007. [CrossRef]
2. Mohanty, R.; Kumar, B.P. Urbanization and smart cities. In *Solving Urban Infrastructure Problems Using Smart City Technologies*; Elsevier: Amsterdam, The Netherlands, 2021; pp. 143–158.
3. Corchado, J.M.; Chamoso, P.; Hernández, G.; Gutierrez, A.S.R.; Camacho, A.R.; González-Briones, A.; Pinto-Santos, F.; Goyenechea, E.; García-Retuerta, D.; Alonso-Miguel, M.; et al. Deepint. net: A rapid deployment platform for smart territories. *Sensors* **2021**, *21*, 236. [CrossRef]
4. Dash, B.; Sharma, P. Role of artificial intelligence in smart cities for information gathering and dissemination (a review). *Acad. J. Res. Sci. Publ.* **2022**, *4*, 1–15. [CrossRef]
5. Bobde, Y.; Narayanan, G.; Jati, M.; Raj, R.S.P.; Cvitić, I.; Peraković, D. Enhancing Industrial IoT Network Security through Blockchain Integration. *Electronics* **2024**, *13*, 687. [CrossRef]
6. Alajlan, R.; Alhumam, N.; Frikha, M. Cybersecurity for blockchain-based IoT systems: A review. *Appl. Sci.* **2023**, *13*, 7432. [CrossRef]
7. Kumar, S.; Verma, A.K.; Mirza, A. Artificial Intelligence-Driven Governance Systems: Smart Cities and Smart Governance. In *Digital Transformation, Artificial Intelligence and Society: Opportunities and Challenges*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 73–90.
8. Ullah, Z.; Al-Turjman, F.; Mostarda, L.; Gagliardi, R. Applications of artificial intelligence and machine learning in smart cities. *Comput. Commun.* **2020**, *154*, 313–323. [CrossRef]
9. Javed, A.R.; Ahmed, W.; Pandya, S.; Maddikunta, P.K.R.; Alazab, M.; Gadekallu, T.R. A survey of explainable artificial intelligence for smart cities. *Electronics* **2023**, *12*, 1020. [CrossRef]
10. Deep, G.; Verma, J. Embracing the future: AI and ML transforming urban environments in smart cities. *J. Artif. Intell* **2023**, *5*, 57–73. [CrossRef]
11. Sha, M.; Boukerche, A. Performance evaluation of CNN-based pedestrian detectors for autonomous vehicles. *Ad Hoc Netw.* **2022**, *128*, 102784. [CrossRef]
12. Allu, A.R.; Mesapam, S. Real-Time Optimization of Traffic Signaling Time Using CNN. *Suranaree J. Sci. Technol* **2021**, *28*, 8.
13. Muthamizharasan, M.; Ponnusamy, R. Forecasting crime event rate with a CNN-LSTM model. In *Innovative Data Communication Technologies and Application: Proceedings of ICIDCA 2021*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 461–470.
14. Li, Q.; Mi, J.; Li, W.; Wang, J.; Cheng, M. CNN-based malware variants detection method for internet of things. *IEEE Internet Things J.* **2021**, *8*, 16946–16962. [CrossRef]
15. Rahhal, J.S.; Abualnadi, D. IOT based predictive maintenance using LSTM RNN estimator. In Proceedings of the 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey, 12–13 June 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–5.
16. Hewamalage, H.; Bergmeir, C.; Bandara, K. Recurrent neural networks for time series forecasting: Current status and future directions. *Int. J. Forecast.* **2021**, *37*, 388–427. [CrossRef]
17. Zhang, X.; Zhao, M.; Dong, R. Time-series prediction of environmental noise for urban IoT based on long short-term memory recurrent neural network. *Appl. Sci.* **2020**, *10*, 1144. [CrossRef]
18. Saeed, F.; Ahmed, M.J.; Gul, M.J.; Hong, K.J.; Paul, A.; Kavitha, M.S. A robust approach for industrial small-object detection using an improved faster regional convolutional neural network. *Sci. Rep.* **2021**, *11*, 23390. [CrossRef] [PubMed]
19. Zhang, C.; Xie, Y.; Bai, H.; Yu, B.; Li, W.; Gao, Y. A survey on federated learning. *Knowl.-Based Syst.* **2021**, *216*, 106775. [CrossRef]
20. Pandya, S.; Srivastava, G.; Jhaveri, R.; Babu, M.R.; Bhattacharya, S.; Maddikunta, P.K.R.; Mastorakis, S.; Piran, M.J.; Gadekallu, T.R. Federated learning for smart cities: A comprehensive survey. *Sustain. Energy Technol. Assess.* **2023**, *55*, 102987. [CrossRef]
21. Jiang, J.C.; Kantarci, B.; Oktug, S.; Soyata, T. Federated learning in smart city sensing: Challenges and opportunities. *Sensors* **2020**, *20*, 6230. [CrossRef]
22. Zheng, Z.; Zhou, Y.; Sun, Y.; Wang, Z.; Liu, B.; Li, K. Applications of federated learning in smart cities: Recent advances, taxonomy, and open challenges. *Connect. Sci.* **2022**, *34*, 1–28. [CrossRef]
23. Joo, H.; Ahmed, S.H.; Lim, Y. Traffic signal control for smart cities using reinforcement learning. *Comput. Commun.* **2020**, *154*, 324–330. [CrossRef]

24. Louati, A.; Louati, H.; Kariri, E.; Neifar, W.; Hassan, M.K.; Khairi, M.H.; Farahat, M.A.; El-Hoseny, H.M. Sustainable Smart Cities through Multi-Agent Reinforcement Learning-Based Cooperative Autonomous Vehicles. *Sustainability* **2024**, *16*, 1779. [CrossRef]
25. Dhaya, R.; Kanthavel, R.; Algarni, F.; Jayarajan, P.; Mahor, A. Reinforcement learning concepts ministering smart city applications using iot. In *Internet of Things in Smart Technologies for Sustainable Urban Development*; Springer: Cham, Switzerland, 2020; pp. 19–41.
26. Damadam, S.; Zourbakhsh, M.; Javidan, R.; Faroughi, A. An intelligent IoT based traffic light management system: Deep reinforcement learning. *Smart Cities* **2022**, *5*, 1293–1311. [CrossRef]
27. Chen, W.; Qiu, X.; Cai, T.; Dai, H.N.; Zheng, Z.; Zhang, Y. Deep reinforcement learning for Internet of Things: A comprehensive survey. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 1659–1692. [CrossRef]
28. Islam, M.; Dukyil, A.S.; Alyahya, S.; Habib, S. An IoT enable anomaly detection system for smart city surveillance. *Sensors* **2023**, *23*, 2358. [CrossRef]
29. Al-amri, R.; Murugesan, R.K.; Man, M.; Abdulateef, A.F.; Al-Sharafi, M.A.; Alkahtani, A.A. A review of machine learning and deep learning techniques for anomaly detection in IoT data. *Appl. Sci.* **2021**, *11*, 5320. [CrossRef]
30. Reddy, D.K.; Behera, H.S.; Nayak, J.; Vijayakumar, P.; Naik, B.; Singh, P.K. Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4121. [CrossRef]
31. Agrawal, A.P.; Singh, N. Comparative analysis of SVM kernels and parameters for efficient anomaly detection in IoT. In Proceedings of the 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 22–23 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.
32. Chatterjee, A.; Ahmed, B.S. IoT anomaly detection methods and applications: A survey. *Internet Things* **2022**, *19*, 100568. [CrossRef]
33. Gomez-Rosero, S.; Capretz, M.A.; Mir, S. Transfer learning by similarity centred architecture evolution for multiple residential load forecasting. *Smart Cities* **2021**, *4*, 217–240. [CrossRef]
34. Pinto, G.; Wang, Z.; Roy, A.; Hong, T.; Capozzoli, A. Transfer learning for smart buildings: A critical review of algorithms, applications, and future perspectives. *Adv. Appl. Energy* **2022**, *5*, 100084. [CrossRef]
35. Abbas, Q.; Ahmad, G.; Alyas, T.; Alghamdi, T.; Alsaawy, Y.; Alzahrani, A. Revolutionizing Urban Mobility: IoT-Enhanced Autonomous Parking Solutions with Transfer Learning for Smart Cities. *Sensors* **2023**, *23*, 8753. [CrossRef]
36. Vu, L.; Nguyen, Q.U.; Nguyen, D.N.; Hoang, D.T.; Dutkiewicz, E. Deep transfer learning for IoT attack detection. *IEEE Access* **2020**, *8*, 107335–107344. [CrossRef]
37. Lin, H.; Hu, J.; Wang, X.; Alhamid, M.F.; Piran, M.J. Toward secure data fusion in industrial IoT using transfer learning. *IEEE Trans. Ind. Inform.* **2020**, *17*, 7114–7122. [CrossRef]
38. Syed, A.S.; Sierra-Sosa, D.; Kumar, A.; Elmaghraby, A. IoT in smart cities: A survey of technologies, practices and challenges. *Smart Cities* **2021**, *4*, 429–475. [CrossRef]
39. Kirimtat, A.; Krejcar, O.; Kertesz, A.; Tasgetiren, M.F. Future trends and current state of smart city concepts: A survey. *IEEE Access* **2020**, *8*, 86448–86467. [CrossRef]
40. Lai, C.S.; Jia, Y.; Dong, Z.; Wang, D.; Tao, Y.; Lai, Q.H.; Wong, R.T.; Zobaa, A.F.; Wu, R.; Lai, L.L. A review of technical standards for smart cities. *Clean Technol.* **2020**, *2*, 290–310. [CrossRef]
41. Bauer, M.; Sanchez, L.; Song, J. IoT-enabled smart cities: Evolution and outlook. *Sensors* **2021**, *21*, 4511. [CrossRef]
42. Xihua, Z.; Goyal, S. Security and privacy challenges using IoT-blockchain technology in a smart city: Critical analysis. *Int. J. Electr. Electron. Res* **2022**, *10*, 190–195. [CrossRef]
43. Eghmazi, A.; Ataei, M.; Landry, R.J.; Chevrette, G. Enhancing IoT data security: Using the blockchain to boost data integrity and privacy. *IoT* **2024**, *5*, 20–34. [CrossRef]
44. Cong, R.; Liu, Y.; Tago, K.; Li, R.; Asaeda, H.; Jin, Q. Individual-initiated auditable access control for privacy-preserved IoT data sharing with blockchain. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 14–23 June 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.
45. Padma, A.; Ramaiah, M. Blockchain based an efficient and secure privacy preserved framework for smart cities. *IEEE Access* **2024**, *12*, 21985–22002. [CrossRef]
46. Tyagi, A.K. Decentralized everything: Practical use of blockchain technology in future applications. In *Distributed Computing to Blockchain*; Elsevier: Amsterdam, The Netherlands, 2023; pp. 19–38.
47. Ajayi, O.J.; Rafferty, J.; Santos, J.; Garcia-Constantino, M.; Cui, Z. BECA: A Blockchain-Based Edge Computing Architecture for Internet of Things Systems. *IoT* **2021**, *2*, 610–632. [CrossRef]
48. Lashkari, B.; Musilek, P. A comprehensive review of blockchain consensus mechanisms. *IEEE Access* **2021**, *9*, 43620–43652. [CrossRef]
49. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Garg, S.; Hassan, M.M. A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. *J. Parallel Distrib. Comput.* **2022**, *164*, 55–68. [CrossRef]
50. Ansar, K.; Ahmed, M.; Helfert, M.; Kim, J. Blockchain-Based Data Breach Detection: Approaches, Challenges, and Future Directions. *Mathematics* **2023**, *12*, 107. [CrossRef]

51. Rahman, A.; Islam, M.J.; Khan, M.S.I.; Kabir, S.; Pritom, A.I.; Karim, M.R. Block-sdotcloud: Enhancing security of cloud storage through blockchain-based sdn in iot network. In Proceedings of the 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 19–20 December 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.
52. Khan, D.; Jung, L.T.; Hashmani, M.A. Systematic literature review of challenges in blockchain scalability. *Appl. Sci.* **2021**, *11*, 9372. [CrossRef]
53. Li, Z.; Sharma, V.; Mohanty, S.P. Preserving data privacy via federated learning: Challenges and solutions. *IEEE Consum. Electron. Mag.* **2020**, *9*, 8–16. [CrossRef]
54. Zheng, Z.; Wang, T.; Bashir, A.K.; Alazab, M.; Mumtaz, S.; Wang, X. A decentralized mechanism based on differential privacy for privacy-preserving computation in smart grid. *IEEE Trans. Comput.* **2021**, *71*, 2915–2926. [CrossRef]
55. Hassan, M.U.; Rehmani, M.H.; Chen, J. Differential privacy in blockchain technology: A futuristic approach. *J. Parallel Distrib. Comput.* **2020**, *145*, 50–74. [CrossRef]
56. Yazdinejad, A.; Dehghantanha, A.; Karimipour, H.; Srivastava, G.; Parizi, R.M. A robust privacy-preserving federated learning model against model poisoning attacks. *IEEE Trans. Inf. Forensics Secur.* **2024**, *19*, 6693–6708. [CrossRef]
57. Rahman, M.S.; Chamikara, M.; Khalil, I.; Bouras, A. Blockchain-of-blockchains: An interoperable blockchain platform for ensuring IoT data integrity in smart city. *J. Ind. Inf. Integr.* **2022**, *30*, 100408. [CrossRef]
58. Ali, M.; Karimipour, H.; Tariq, M. Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges. *Comput. Secur.* **2021**, *108*, 102355. [CrossRef]
59. Zhao, Y.; Zhao, J.; Jiang, L.; Tan, R.; Niyato, D.; Li, Z.; Lyu, L.; Liu, Y. Privacy-preserving blockchain-based federated learning for IoT devices. *IEEE Internet Things J.* **2020**, *8*, 1817–1829. [CrossRef]
60. Ali, A.; Al-Rimy, B.A.S.; Almazroi, A.A.; Alsubaei, F.S.; Almazroi, A.A.; Saeed, F. Securing secrets in cyber-physical systems: A cutting-edge privacy approach with consortium blockchain. *Sensors* **2023**, *23*, 7162. [CrossRef] [PubMed]
61. Villarreal, E.R.D.; García-Alonso, J.; Moguel, E.; Alegría, J.A.H. Blockchain for healthcare management systems: A survey on interoperability and security. *IEEE Access* **2023**, *11*, 5629–5652. [CrossRef]
62. Rehman, A.; Naz, S.; Razzak, I. Leveraging big data analytics in healthcare enhancement: Trends, challenges and opportunities. *Multimed. Syst.* **2022**, *28*, 1339–1371. [CrossRef]
63. Dedeoglu, V.; Malik, S.; Ramachandran, G.; Pal, S.; Jurdak, R. Blockchain meets edge-AI for food supply chain traceability and provenance. In *Comprehensive Analytical Chemistry*; Elsevier: Amsterdam, The Netherlands, 2023; Volume 101, pp. 251–275.
64. Sedlmeir, J.; Buhl, H.U.; Fridgen, G.; Keller, R. The energy consumption of blockchain technology: Beyond myth. *Bus. Inf. Syst. Eng.* **2020**, *62*, 599–608. [CrossRef]
65. Sarker, I.H. Smart City Data Science: Towards data-driven smart cities with open research issues. *Internet Things* **2022**, *19*, 100528. [CrossRef]
66. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H.; Srivastava, G.; Aledhari, M. Enabling drones in the internet of things with decentralized blockchain-based security. *IEEE Internet Things J.* **2020**, *8*, 6406–6415. [CrossRef]
67. Khan, S.N.; Loukil, F.; Ghedira-Guegan, C.; Benkhelifa, E.; Bani-Hani, A. Blockchain smart contracts: Applications, challenges, and future trends. *Peer- Netw. Appl.* **2021**, *14*, 2901–2925. [CrossRef] [PubMed]
68. Hewa, T.M.; Hu, Y.; Liyanage, M.; Kanhare, S.S.; Ylianttila, M. Survey on blockchain-based smart contracts: Technical aspects and future research. *IEEE Access* **2021**, *9*, 87643–87662. [CrossRef]
69. Liu, Y.; Liu, J.; Li, D.; Yu, H.; Wu, Q. Fleetchain: A secure scalable and responsive blockchain achieving optimal sharding. In Proceedings of the International Conference on Algorithms and Architectures for Parallel Processing, New York City, NY, USA, 2–4 October 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 409–425.
70. Zheng, P.; Xu, Q.; Zheng, Z.; Zhou, Z.; Yan, Y.; Zhang, H. Meepo: Sharded consortium blockchain. In Proceedings of the 2021 IEEE 37th International Conference on Data Engineering (ICDE), Chania, Greece, 19–22 April 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1847–1852.
71. Aiyar, K.; Halgamuge, M.N.; Mohammad, A. Probability distribution model to analyze the trade-off between scalability and security of sharding-based blockchain networks. In Proceedings of the 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.
72. Hong, Z.; Guo, S.; Li, P.; Chen, W. Pyramid: A layered sharding blockchain system. In Proceedings of the IEEE INFOCOM 2021-IEEE Conference on Computer Communications, Vancouver, BC, Canada, 10–13 May 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–10.
73. Platt, M.; Sedlmeir, J.; Platt, D.; Xu, J.; Tasca, P.; Vadgama, N.; Ibañez, J.I. The energy footprint of blockchain consensus mechanisms beyond proof-of-work. In Proceedings of the 2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C), Hainan, China, 6–10 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1135–1144.
74. Gallersdörfer, U.; Klaaßen, L.; Stoll, C. Energy consumption of cryptocurrencies beyond bitcoin. *Joule* **2020**, *4*, 1843–1846. [CrossRef]
75. Zhang, R.; Chan, W.K.V. Evaluation of energy consumption in block-chains with proof of work and proof of stake. *J. Phys. Conf. Ser.* **2020**, *1584*, 012023. [CrossRef]
76. Riđić, O.; Jukić, T.; Riđić, G.; Mangafić, J.; Bušatlić, S.; Karamehić, J. Implementation of blockchain technologies in smart cities, opportunities and challenges. In *Blockchain Technologies for Sustainability*; Springer: Singapore, 2022; pp. 71–89.

77. Zhou, S.; Li, K.; Xiao, L.; Cai, J.; Liang, W.; Castiglione, A. A systematic review of consensus mechanisms in blockchain. *Mathematics* **2023**, *11*, 2248. [CrossRef]
78. Wen, Y.; Lu, F.; Liu, Y.; Cong, P.; Huang, X. Blockchain consensus mechanisms and their applications in iot: A literature survey. In Proceedings of the Algorithms and Architectures for Parallel Processing: 20th International Conference, ICA3PP 2020, New York City, NY, USA, 2–4 October 2020; Proceedings, Part III 20; Springer: Berlin/Heidelberg, Germany, 2020; pp. 564–579.
79. Ullah, Z.; Naeem, M.; Coronato, A.; Ribino, P.; De Pietro, G. Blockchain applications in sustainable smart cities. *Sustain. Cities Soc.* **2023**, *97*, 104697. [CrossRef]
80. Kumar, R.; Jain, V.; Yie, L.W.; Teyarachakul, S. *Convergence of IoT, Blockchain, and Computational Intelligence in Smart Cities*; CRC Press: Boca Raton, FL, USA, 2024.
81. Ullah, A.; Anwar, S.M.; Li, J.; Nadeem, L.; Mahmood, T.; Rehman, A.; Saba, T. Smart cities: The role of Internet of Things and machine learning in realizing a data-centric smart environment. *Complex Intell. Syst.* **2024**, *10*, 1607–1637. [CrossRef]
82. Alrashdi, I.; Alqazzaz, A. Synergizing AI, IoT, and Blockchain for Diagnosing Pandemic Diseases in Smart Cities: Challenges and Opportunities. *Sustain. Mach. Intell. J.* **2024**, *7*, 1–6. [CrossRef]
83. Goyal, S.; Goyal, I.; Ahmed, T. A Review on Machine Learning Techniques in IoT-Based Smart Grid Applications. In *Proceedings of the International Conference on Recent Trends in Image Processing and Pattern Recognition*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 151–164.
84. Abir, S.A.A.; Anwar, A.; Choi, J.; Kayes, A. Iot-enabled smart energy grid: Applications and challenges. *IEEE Access* **2021**, *9*, 50961–50981. [CrossRef]
85. Saleem, M.; Abbas, S.; Ghazal, T.M.; Khan, M.A.; Sahawneh, N.; Ahmad, M. Smart cities: Fusion-based intelligent traffic congestion control system for vehicular networks using machine learning techniques. *Egypt. Inform. J.* **2022**, *23*, 417–426. [CrossRef]
86. Sharma, A.; Podoplelova, E.; Shapovalov, G.; Tselykh, A.; Tselykh, A. Sustainable smart cities: Convergence of artificial intelligence and blockchain. *Sustainability* **2021**, *13*, 13076. [CrossRef]
87. Kayikci, S.; Khoshgoftaar, T.M. Blockchain meets machine learning: A survey. *J. Big Data* **2024**, *11*, 9. [CrossRef]
88. Masa'deh, R.; Jaber, M.; Sharabati, A.A.A.; Nasereddin, A.Y.; Marei, A. The Blockchain Effect on Courier Supply Chains Digitalization and Its Contribution to Industry 4.0 within the Circular Economy. *Sustainability* **2024**, *16*, 7218. [CrossRef]
89. Salimitari, M.; Chatterjee, M.; Fallah, Y.P. A survey on consensus methods in blockchain for resource-constrained IoT networks. *Internet Things* **2020**, *11*, 100212. [CrossRef]
90. André, M.; Margarida, J.; Garcia, H.; Dante, A. Complexities of Blockchain technology and distributed ledger technologies: A detailed inspection. *Fusion Multidiscip. Res. Int. J.* **2021**, *2*, 164–177.
91. Shurman, M.; Obeidat, A.A.R.; Al-Shurman, S.A.D. Blockchain and smart contract for IoT. In Proceedings of the 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 7–9 April 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 361–366.
92. Jamil, F.; Iqbal, N.; Ahmad, S.; Kim, D. Peer-to-peer energy trading mechanism based on blockchain and machine learning for sustainable electrical power supply in smart grid. *IEEE Access* **2021**, *9*, 39193–39217. [CrossRef]
93. Esmat, A.; de Vos, M.; Ghiassi-Farrokhfal, Y.; Palensky, P.; Epema, D. A novel decentralized platform for peer-to-peer energy trading market with blockchain technology. *Appl. Energy* **2021**, *282*, 116123. [CrossRef]
94. Muneeb, M.; Raza, Z.; Haq, I.U.; Shafiq, O. Smartcon: A blockchain-based framework for smart contracts and transaction management. *IEEE Access* **2021**, *10*, 23687–23699. [CrossRef]
95. Hemashree, P.; Kavitha, V.; Mahalakshmi, S.; Praveena, K.; Tarunika, R. Machine Learning Approaches in Blockchain Technology-Based IoT Security: An Investigation on Current Developments and Open Challenges. In *Blockchain Transformations: Navigating the Decentralized Protocols Era*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 107–130.
96. Matei, A.; Cocoșatu, M. Artificial Internet of Things, Sensor-Based Digital Twin Urban Computing Vision Algorithms, and Blockchain Cloud Networks in Sustainable Smart City Administration. *Sustainability* **2024**, *16*, 6749. [CrossRef]
97. Ahmed, I.; Zhang, Y.; Jeon, G.; Lin, W.; Khosravi, M.R.; Qi, L. A blockchain-and artificial intelligence-enabled smart IoT framework for sustainable city. *Int. J. Intell. Syst.* **2022**, *37*, 6493–6507. [CrossRef]
98. Tsampoulatidis, I.; Komninos, N.; Syrmos, E.; Bechtsis, D. Universality and interoperability across smart city ecosystems. In Proceedings of the International Conference on Human-Computer Interaction, Virtual Event, 26 June–1 July 2022; Springer: Berlin/Heidelberg, Germany, 2022; pp. 218–230.
99. Cui, L.; Qu, Y.; Xie, G.; Zeng, D.; Li, R.; Shen, S.; Yu, S. Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3492–3500. [CrossRef]
100. Otoum, S.; Al Ridhawi, I.; Mouftah, H. Securing critical IoT infrastructures with blockchain-supported federated learning. *IEEE Internet Things J.* **2021**, *9*, 2592–2601. [CrossRef]
101. Yu, F.; Lin, H.; Wang, X.; Yassine, A.; Hossain, M.S. Blockchain-empowered secure federated learning system: Architecture and applications. *Comput. Commun.* **2022**, *196*, 55–65. [CrossRef]
102. Ruzbahani, A.M. AI-Protected Blockchain-based IoT environments: Harnessing the Future of Network Security and Privacy. *arXiv* **2024**, arXiv:2405.13847.

103. Kumar, P.; Kumar, R.; Srivastava, G.; Gupta, G.P.; Tripathi, R.; Gadekallu, T.R.; Xiong, N.N. PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 2326–2341. [CrossRef]
104. Makhdoom, I.; Zhou, I.; Abolhasan, M.; Lipman, J.; Ni, W. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Comput. Secur.* **2020**, *88*, 101653. [CrossRef]
105. Sezer, B.B.; Turkmen, H.; Nuriyev, U. PPFchain: A novel framework privacy-preserving blockchain-based federated learning method for sensor networks. *Internet Things* **2023**, *22*, 100781. [CrossRef]
106. Simonet-Boulogne, A.; Solberg, A.; Sinaeepourfard, A.; Roman, D.; Perales, F.; Ledakis, G.; Plakas, I.; Sengupta, S. Toward blockchain-based fog and edge computing for privacy-preserving smart cities. *Front. Sustain. Cities* **2022**, *4*, 846987. [CrossRef]
107. Valencia-Arias, A.; González-Ruiz, J.D.; Verde Flores, L.; Vega-Mori, L.; Rodríguez-Correa, P.; Sánchez Santos, G. Machine Learning and Blockchain: A Bibliometric Study on Security and Privacy. *Information* **2024**, *15*, 65. [CrossRef]
108. Tong, Z.; Ye, F.; Yan, M.; Liu, H.; Basodi, S. A survey on algorithms for intelligent computing and smart city applications. *Big Data Min. Anal.* **2021**, *4*, 155–172. [CrossRef]
109. Tang, S.; Chen, L.; He, K.; Xia, J.; Fan, L.; Nallanathan, A. Computational intelligence and deep learning for next-generation edge-enabled industrial IoT. *IEEE Trans. Netw. Sci. Eng.* **2022**, *10*, 2881–2893. [CrossRef]
110. Zhou, Q.; Huang, H.; Zheng, Z.; Bian, J. Solutions to scalability of blockchain: A survey. *IEEE Access* **2020**, *8*, 16440–16455. [CrossRef]
111. Singh, S.K.; Rathore, S.; Park, J.H. Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Gener. Comput. Syst.* **2020**, *110*, 721–743. [CrossRef]
112. Auhl, Z.; Chilamkurti, N.; Alhadad, R.; Heyne, W. A Comparative study of consensus mechanisms in blockchain for IoT networks. *Electronics* **2022**, *11*, 2694. [CrossRef]
113. Biswas, S.; Yao, Z.; Yan, L.; Alqhatani, A.; Bairagi, A.K.; Asiri, F.; Masud, M. Interoperability benefits and challenges in smart city services: Blockchain as a solution. *Electronics* **2023**, *12*, 1036. [CrossRef]
114. Rejeb, A.; Rejeb, K.; Simske, S.J.; Keogh, J.G. Blockchain technology in the smart city: A bibliometric review. *Qual. Quant.* **2022**, *56*, 2875–2906. [CrossRef]
115. Jeong, S.; Kim, S.; Kim, J. City data hub: Implementation of standard-based smart city data platform for interoperability. *Sensors* **2020**, *20*, 7000. [CrossRef] [PubMed]
116. Ahmad, K.; Maabreh, M.; Ghaly, M.; Khan, K.; Qadir, J.; Al-Fuqaha, A. Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. *Comput. Sci. Rev.* **2022**, *43*, 100452. [CrossRef]
117. Ahmad, K.; Maabreh, M.; Ghaly, M.; Khan, K.; Qadir, J.; Al-Fuqaha, A. Developing future human-centered smart cities: Critical analysis of smart city security, interpretability, and ethical challenges. *arXiv* **2020**, arXiv:2012.09110.
118. Ziosi, M.; Hewitt, B.; Juneja, P.; Taddeo, M.; Floridi, L. Smart cities: Mapping their ethical implications. *SSRN Electron. J.* **2022**, *10*. [CrossRef]
119. Park, J.; Lim, H. Privacy-preserving federated learning using homomorphic encryption. *Appl. Sci.* **2022**, *12*, 734. [CrossRef]
120. Yang, R.; Zhao, T.; Yu, F.R.; Li, M.; Zhang, D.; Zhao, X. Blockchain-Based Federated Learning with Enhanced Privacy and Security Using Homomorphic Encryption and Reputation. *IEEE Internet Things J.* **2024**, *11*, 21674–21688. [CrossRef]
121. Singh, P.; Masud, M.; Hossain, M.S.; Kaur, A. Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid. *Comput. Electr. Eng.* **2021**, *93*, 107209. [CrossRef]
122. Kumar, P.; Gupta, G.P.; Tripathi, R. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. *J. Syst. Archit.* **2021**, *115*, 101954. [CrossRef]
123. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet Things* **2020**, *11*, 100227. [CrossRef]
124. Rathore, S.; Park, J.H. A blockchain-based deep learning approach for cyber security in next generation industrial cyber-physical systems. *IEEE Trans. Ind. Inform.* **2020**, *17*, 5522–5532. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.