drones

MDPI

Article

Advancing Drone Operations through Lightweight Blockchain and Fog Computing Integration: A Systematic Review

Rawabi Aldossri *, Ahmed Aljughaiman and Abdullah Albuali

Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia; aaaljughaiman@kfu.edu.sa (A.A.); aabuali@kfu.edu.sa (A.A.)

* Correspondence: 222400163@student.kfu.edu.sa

Abstract: This paper presents a systematic literature review investigating the integration of lightweight blockchain and fog computing technologies to enhance the security and operational efficiency of drones. With a focus on critical applications such as military surveillance and emergency response, this review examines how the combination of blockchain's secure, decentralized ledger and fog computing's low-latency, localized data processing can address the unique challenges of drone operations. By compiling and analyzing current research, this study highlights innovative approaches and solutions that leverage these technologies to improve data integrity, reduce communication latency, and facilitate real-time decision-making in drone missions. Our findings underscore the significant potential of this technological integration to advance the capabilities and reliability of drones in high-stakes scenarios.

Keywords: drone; blockchain; fog computing; lightweight blockchain

Citation: Aldossri , R.; Aljughaiman, A.; Albuali, A. Advancing Drone Operations through Lightweight Blockchain and Fog Computing Integration: A Systematic Review. *Drones* **2024**, *8*, 153. https://doi.org/10.3390/drones8040153

Academic Editor: Carlos Tavares Calafate

Received: 24 March 2024
Revised: 7 April 2024
Accepted: 9 April 2024
Published: 16 April 2024

1. Introduction

In recent years, drones, or Unmanned Aerial Vehicles (UAVs), have undergone a remarkable transformation, evolving from exclusive military assets to versatile tools across civilian sectors. This evolution has been propelled by rapid advancements in technology, enabling drones to undertake complex tasks in diverse fields such as agriculture, logistics, public safety, and environmental monitoring. However, the broadening scope of drone applications introduces formidable challenges, notably in ensuring robust security and operational efficiency. These critical issues are not merely theoretical but have manifested in practical challenges across various drone applications. For instance, communication latency can significantly impair the operational efficiency of drones in time-sensitive missions such as emergency response and disaster management, where every second is crucial [1]. Similarly, ensuring data integrity is fundamental in applications like environmental monitoring and infrastructure inspection, where the accuracy of data collected by drones directly influences decision-making and policy formulation [2]. Furthermore, the vulnerability of drones to cyber threats poses a significant risk, not only to the privacy and security of the data collected but also to the physical safety of the areas over which they operate, as unauthorized control over drones can lead to severe consequences. These prevalent issues highlight the urgent need for innovative solutions that can address the multifaceted challenges faced by drone operations today.

This paper embarks on a systematic literature review to explore the integration of two promising technologies—the lightweight blockchain and fog computing—as a strategy to enhance the security and efficiency of drone operations. The choice of the lightweight blockchain and fog computing is driven by their distinct advantages for drone operations. Lightweight blockchain technology, adapted for the constrained resources of drone systems, offers a robust solution to enhance data security and integrity. By enabling a decentralized and tamper-resistant ledger, the lightweight blockchain ensures that data collected and

transmitted by drones—ranging from flight logs to surveillance footage—are immutable and traceable. This is particularly vital in applications such as environmental monitoring and border surveillance, where the authenticity of data could have significant legal and operational implications.

Moreover, the decentralized nature of the blockchain mitigates the risk of single points of failure, enhancing the reliability of communication systems in drone fleets. This aspect is crucial for maintaining operational continuity in critical applications, including search and rescue missions and disaster response, where drone systems must remain resilient against both physical and cyber threats.

Fog computing, on the other hand, addresses the pressing need for real-time data processing within drone operations. By distributing computing resources closer to the edge—near or on the drones themselves—fog computing significantly reduces latency compared to cloud-centric models. This facilitates quicker decision-making and response times, essential for dynamic environments and applications requiring immediate action, such as traffic management and emergency medical deliveries. In high-stakes environments like military and defense operations, the efficiency and security of drone operations are of utmost importance. Challenges such as latency in communication and data processing can critically impact the success of missions. Furthermore, the increasing connectivity of drones has opened up new avenues for cyber threats, making protecting sensitive data a top priority. Addressing these challenges is vital for drones' safe and effective operation, especially as they become increasingly integrated into critical infrastructural operations [3].

To tackle these issues, this systematic literature review investigates the integration of lightweight blockchain technology and fog computing into drone operations. The lightweight blockchain offers a promising solution to enhance data security and integrity. Its capacity to produce an unchangeable, transparent ledger can fortify drone operations against cyber threats, such as data breaches and unauthorized data modification. On the other hand, fog computing emerges as a complementary technology that addresses the issue of latency. By decentralizing data processing and situating it closer to the data source—the drone—fog computing can significantly reduce response times, enabling drones to make swift, real-time decisions [4].

This review seeks to offer a thorough summary of existing research in this domain, exploring how the convergence of these two technologies can redefine security and operational frameworks of drone usage, by examining studies on the application, challenges, and potential of integrating the lightweight blockchain and fog computing into drone systems. In reviewing the current body of literature, we have identified several surveys that explore the utilization of blockchain and fog computing across various domains. We delve into the essential performance metrics and evaluation methods, providing a balanced perspective that bridges theoretical foundations with practical implications. Further, by identifying current research gaps and suggesting directions for future inquiries, this work aims to catalyze continued innovation and exploration. Notably, our examination of the synergistic potential between the lightweight blockchain and fog computing reveals their transformative impact on enhancing drone operational efficiency, security, and scalability. Such insights not only contribute to the academic discourse but also offer valuable guidance for the practical advancement of drone technology. By doing so, we contribute to broadening the understanding and application possibilities in this specialized area, setting a foundation for future research.

In preparation for our study, this paper is organized to facilitate a systematic review of sources selected according to the PRISMA methodology in Section 2. After that, Section 3 carries out a wide literature review, which is divided into separate thematic clusters. In Section 3.1, we delve into the research of blockchain applications and innovations, while Section 3.2 discusses fog computing. Additionally, Section 3.3 explores the area of fog computing applications and innovations. Section 3.4 provides a comprehensive analysis of the lightweight blockchain framework with fog computing. Following this, Section 4 presents our results and discussion, orienting toward a critical analysis. Section 5 offers

a detailed discussion of the implications of our research. The challenges and limitations are discussed in Section 6. Section 7 outlines a futuristic perspective through an analysis of future research directions. Finally, Section 8 summarizes our results and conclusions, setting the stage for future inquiries and applications in the field.

2. Selection of Papers by PRISMA

The systematic literature review (SLR) is an essential research methodology that guides researchers in systematically selecting a representative set of studies from a vast pool of the available literature. This methodology is particularly pertinent to our study, which explores the integration of lightweight blockchains and fog computing in drone operations. To commence our research, we conducted a comprehensive search in databases, including IEEE and Google Scholar, using a combination of keywords: (drone OR UAV) AND (blockchain OR "lightweight blockchain") AND ("fog computing" OR "edge computing"). We restricted the literature to studies published in English between 2018 and 2023 to capture the most recent advancements in this rapidly evolving field.

The initial search yielded approximately 3000 papers discussing the intersection of these technologies in drone operations. We eliminated 1200 duplicates from this pool and excluded 800 papers for deviating from our core research focus. Subsequent screening based on titles and abstracts led to the dismissal of another 600 papers, primarily due to their lack of specific relevance to integrating the blockchain and fog computing in drone operations. After this rigorous screening process, we evaluated 400 papers for eligibility based on their contribution to the field, methodological rigor, and relevance to our research objectives.

Ultimately, our meticulous selection process, following the PRISMA guidelines, culminated in the inclusion of 32 papers. These papers were chosen for their comprehensive coverage of the technological aspects, challenges, and potential solutions for integrating the lightweight blockchain and fog computing in drone operations. This selection ensured a wide range of perspectives and upheld the standards of systematic and unbiased review, which is crucial for a study of this nature. The detailed PRISMA flow diagram, illustrating our paper selection process, is depicted in Figure 1 of our review.

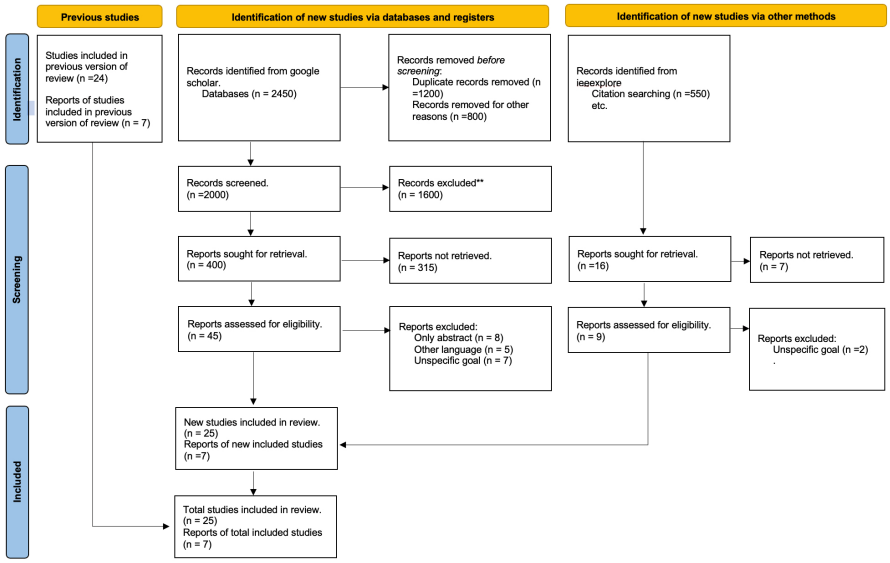

Figure 1. The selection of papers for the literature review using PRISMA.

3. Literature Survey

Integrating the lightweight blockchain and fog computing in drone operations is a burgeoning area of research characterized by a diverse range of studies that explore various aspects of this technological convergence. In this Literature Survey section, we delve into

the findings and insights gleaned from the selected 32 papers, which were meticulously chosen through the PRISMA framework. This survey aims to dissect the existing body of knowledge, highlighting key advancements, identifying prevailing challenges, and uncovering potential opportunities within this domain. It provides a critical examination of the current state of research, offering a comprehensive synthesis of how lightweight blockchains and fog computing can collaboratively enhance the security and efficiency of drone operations. The following subsections will present an in-depth analysis of the selected studies, categorizing them based on their primary focus areas: technological implementation, security enhancements, efficiency improvements, and practical applications in drone operations.

3.1. Key Research on Blockchain Applications and Innovations

Blockchain technology has emerged as a critical component in the evolution of drone operations, offering solutions to some of the most pressing challenges in this field. The advantages of the blockchain are manifold, encompassing enhanced security, data integrity, and operational efficiency. In the following discussion, we explore these benefits in greater detail, beginning with an overview of the transformative potential of blockchains for drones. In the context of drone operations, blockchain technology offers unparalleled advantages in securing communication channels, data storage, and operational protocols. For instance, the development of lightweight blockchain protocols, as discussed by Finlow-Bates, can significantly reduce the computational overhead by up to 40%, a critical factor for the limited computational resources available on drones [5]. Moreover, the blockchain's decentralized nature ensures that data related to drone flight paths, mission-critical decisions, and video feeds are immutable and protected against unauthorized alterations. The versatility of the blockchain, highlighted by Khor et al., extends beyond traditional applications to secure the vast networks of drones, facilitating secure, tamper-proof logging of drone operations and maintenance records, and ensuring the integrity of data collected during surveillance or inspection missions. This secure, decentralized ledger system is paramount for military and emergency response drones, where data integrity and security are non-negotiable.

Finlow-Bates's, ref. [5], approach represented an entirely new protocol, which aimed to improve security and efficiency in blockchain systems while highlighting the tactical incorporation of smart contracts. This protocol starts with an initialization phase for setting up system parameters followed by the generation of cryptographically signed transactions. These transactions go through a strict consensus mechanism to guarantee that only legitimate and validated transactions are allowed into the blockchain. Moreover, the protocol innovatively aggregates transactions, thus optimizing data storage and improving processing speed. Therefore, the study showed an improvement in performance by up to 40% for computational overhead more than traditional methods. This improvement is highly important for applications in resource-limited conditions, including IoT devices. It also investigates real-life implementations of lightweight blockchains, which can benefit people in various fields such as supply chain control and healthcare. Worth noting is that the team used advanced cryptographic techniques to protect data integrity, ensuring that keeping processes streamlined did not compromise security core principles inherent in blockchain technology.

Khor et al. [6] underscored the vast applicability of the blockchain beyond its conventional use in cryptocurrencies, emphasizing its transformative potential in sectors such as healthcare, supply chain management, and public record keeping. However, the study also shed light on notable security challenges, including threats like the 51% attack, which could compromise the decentralized system's integrity. To counteract these threats, the authors advocated for integrating advanced cryptographic techniques and continuously updating blockchain protocols. Additionally, the research highlighted the pressing need for regulatory frameworks to guide blockchain technology's ethical and secure implementation in various domains. The authors concluded with an optimistic outlook on the future of

blockchains, foreseeing the rise of hybrid systems that combine the strengths of both public and private blockchains.

Michailidis et al. [7] highlighted the potential of AI-based predictive analysis to enhance blockchain operations with a specific focus on transaction validations. Apart from performing tasks, the AI's ability to enhance security is also highlighted by its capability of threat detection and mitigation in real time. While the fusion holds out promises of simplified consensus protocols and resource efficiency, the authors warn about potential issues such as difficulties related to the integration of AI algorithms within blockchain frameworks or even that training models effectively would necessarily require substantial datasets.

Andola et al. [8] presented a blockchain framework for the Internet of Drones (IoD), aiming at better authentication and anonymity. They suggest four ways to conceal drone identities during blockchain communication using non-interactive zero-knowledge proof (NIZKP) with bilinear maps. The study in particular highlights the untraceability of identities and protection against certain weaknesses such as malleability attacks.

Rupa, C et al. [9] presented BCT-based VC devices such as UAVs, drones, and the IoT that serve as an approach to enhance security at the data protection level. Implementing this in an Ethereum-based public blockchain, with Pentatope-based elliptic curve cryptography and SHA for privacy, the proposed design stores data within a virtual vehicle monitoring system. It adopts the Ganache platform for BCT, which guarantees data security. Although it proves effective and secure, there are still several issues associated with the approach including integration difficulties, risks concerning signal data safety, a high-cost level connected to computations, as well as testing problems when working with several devices. Future implementations are wide testing and in other areas of the IoT.

Gupta, R et al. [10] suggested distributed frameworks for drone monitoring of areas such as healthcare, segment defense, and smart cities with features like improved security and data processing. The challenges identified at this point include data privacy issues such as the public Ethereum blockchain, computational complexity, energy inefficiency, processing delays on UAVs, and a lack of standardization; furthermore, quantum computing poses potential threats. This paper focuses on the issues that should be addressed in future research, especially those related to data privacy toward meeting its challenges of computational reduction energy efficiency, UAV processing improvement, blockchain standardization via proper technologies, and finally quantum-secure network design.

Aggarwal, S et al. [11] suggested a blockchain-based model for secure data diffusion on the Internet of Drones (IoD) in 2019. The model is made up of three layers: user, infrastructure, and IoD; it uses a distributed network based on the Ethereum technology for checking verifications. An algorithm to select a forger node was also proposed as an approach to the creation and validation of blocks. Even though the authors have identified some potential system weaknesses including spoofing and denying-services attacks, they claimed their model is credible, as well as scalable for data propagation in an IoD environment. Future work may include fine-tuning the model, security improvements, and investigating other blockchain technologies.

Alkadi, R et al. [12] investigated the application of blockchain technology in Unmanned Aerial Vehicle (UAV) networks. They point out the flaws including low power supply, a lack of mediating third parties, and compatibility problems between different blockchain systems. The authors suggest further steps for the development of homogeneous solutions, simulation tool creation, blockchain enhancements in interconnectivity, and addressing UAV application's multiplicity challenges.

Javed et al. [13] discussed the current security issues arising from developments in the IoD domain. As drones present obvious vulnerabilities, in particular, the fact that these systems use unencrypted wireless communication and enjoy only rather limited computational means, potential threats like GPS spoofing, drone hijacking, or just man-in-the-middle attacks are highlighted in this paper. Javed et al. proposed a new authentication scheme that combines blockchain technology using Hyperelliptic Curve Cryptography

(HECC). This innovative approach proposes an implementation of blockchains as a Certificate Authority (CA), obviating the necessity for well-known CAs or Trusted Third Parties (TTPs).

Mershada et al. [14] delved into the challenges and solutions of integrating blockchain technology within resource-constrained devices commonly found in applications like smart homes and the Internet of Vehicles. Recognizing the inherent security benefits of blockchains, such as immutability and distributed consensus, the paper underscores the difficulties of its implementation due to the resource-intensive nature of traditional blockchain systems. The study presents a comprehensive taxonomy of "lightweight" blockchain solutions tailored for these constrained networks to address this. The authors categorize solutions into five pivotal areas: blockchain architecture, device authentication, cryptography models, consensus algorithms, and storage methods. Through this taxonomy, Mershada et al. highlight existing gaps and provide direction for future research, aiming to foster the development of a holistic lightweight blockchain system suitable for networks with limited resources.

The integration of blockchain technology with drone systems presents a myriad of opportunities and challenges. On the one hand, the blockchain's inherent security attributes such as immutability, distributed consensus, and resilience against cyber-attacks make it a compelling solution for bolstering the security of drone communication and operations. On the other hand, the resource-intensive nature of traditional blockchain systems can pose challenges, especially when implemented on constrained devices. Innovative approaches, such as lightweight blockchain solutions, have been put out to deal with these issues, attempting to balance security and effectiveness. Table 1 Summary of Key Research on Blockchain Applications and Innovations, provides a comprehensive overview of the advancements and innovations in this space, highlighting efforts to overcome these challenges. As the field evolves, continued research and collaboration between blockchain and drone experts will be crucial to unlock the full potential of these combined technologies.

Table 1. Summary of key research on blockchain applications and innovations.

Author	Year	Main Focus	Key Findings	Applications/Use Case
K. Finlow-Bates [5]	2017	Lightweight blockchain protocols	Protocol improving computational overhead by up to 40%.	Supply chain, healthcare, IoT devices
Khor et al. [6]	2023	Blockchain applications and security	Versatility and cryptographic techniques for security.	Healthcare, supply chain, public records
Michailidis et al. [7]	2022	AI with blockchains	AI optimizes blockchain operations and security.	Predictive analysis, threat detection
Andola et al. [8]	2021	Blockchains for the IoD	Methods to hide drone identities using NIZKP.	Internet of Drones (IoD)
Rupa, C. et al. [9]	2020	5G network evolution	5G technical attributes and capabilities.	Smart cities, autonomous vehicles, telemedicine
Gupta, R et al. [10]	2020	Network technology examination	Evolving network technologies' impact.	Broad spectrum communication, IoT integration
Aggarwal, S et al. [11]	2019	Data dissemination in the IoD	Blockchain in IoD for integrity and authentication.	Surveillance, agriculture, military operations
Alkadi, R et al. [12]	2022	Blockchain in UAV networks	Blockchain applications for UAV safety and security.	Multiple UAV service providers, drone recharging
Javed et al. [13]	2022	Blockchain for IoD authentication	Blockchain for enhanced IoD network security.	Secure IoD network communication
Mershada et al. [14]	2023	Lightweight blockchain for networks	Challenges in blockchain integration.	Smart homes, healthcare, Internet of Vehicles

3.2. Fog Computing

Fog computing emerges as a pivotal technology for drone operations, addressing critical latency and data processing challenges inherent in real-time drone missions. By decentralizing data processing and situating them closer to the drone (the data source), fog computing enables swift, on-the-spot decision-making for drones navigating complex environments. This capability is especially beneficial for applications requiring immediate data analysis, such as search and rescue operations, environmental monitoring, and live surveillance. For instance, Hou et al.'s discussion on reliability models for drone swarms underscores the importance of fog computing in ensuring real-time communication reliability among drones, crucial for coordinated movements and operations [15]. The localized data processing of fog computing not only enhances the operational efficiency of drones but also mitigates bandwidth issues, ensuring seamless, uninterrupted drone missions.

3.3. Key Research on Fog Computing Applications and Innovations

Fog computing, being at the forefront of edge computing technologies, has garnered significant attention from the research community. Various studies have explored its potential, applications, challenges, and innovations. Here is a summary of fundamental research studies in this domain.

Ometov et al. [16] took a deep dive into the safety issues that come with cloud, edge, and fog computing. They saw that these tech areas create a special mix of ways to handle data and each has its build and power. Even though being different can be good, it can also make things risky, especially when keeping data safe and private. The work they performed pointed out the key dangers and showed how each area is unlike the others. Because more people worry about keeping their data safe and to themselves, the authors shared some smart ways to deal with these risks as computing keeps changing.

Aazam et al.'s [17] paper focuses on integrating fog computing and cloud computing to improve the efficiency of IoT systems. It aims to address the limitations of cloud-only and edge-only solutions in the IoT by proposing a fog-assisted IoT framework.

Hou et al. [15] explained the complexities of ensuring latency and reliability in drone swarms. Much of the paper focuses on the reliability model for drone operations. The authors consider various disturbances that drone swarms might encounter during their operations. They draw upon established reliability models, suggesting that drones and communication link failures follow the Poisson process. The paper explores the intricate mathematical models and equations to quantify and ensure the reliability of drone operations.

In the context of the developing IoT landscape, Haouari et al. [18] underline the importance of fog computing. There is an urgent need for low-latency solutions because real-time applications are necessary and smart gadgets are quickly becoming commonplace due to the quick spread of smart devices and the requirement for real-time applications. Due to its centralized nature, traditional cloud computing often needs help in meeting these demands. The authors introduce fog computing as a decentralized approach, bringing computational resources closer to end-users and devices. This paper comprehensively explores fog computing, its potential advantages, applications in real-world scenarios, and the challenges it aims to address.

Ahanger et al.'s [19] research explores the evolving landscape of the Internet of Things (IoT) and its intersection with fog computing. As the IoT paradigm transforms the technological world, leading to increased interconnectivity of objects and data exchange, a challenge emerges due to the resource constraints of IoT devices. To address this, the authors introduce the concept of edge or fog computing. This decentralized approach is designed to aid IoT devices' inefficient data handling and delivery. The authors emphasize that fog computing is not replacing centralized cloud systems but rather an enhancement, supplementing its capabilities.

Brogi et al. [20] explored the realm of fog computing, emphasizing the placement of applications within the fog framework. The goal is to expand cloud capabilities to the IoT

to improve service quality and support applications that require low latency. The study offers a thorough analysis of current techniques, offering an overview of current algorithms, open-source prototypes, and test use cases. Additionally, it classifies the literature based on the characteristics of applications and the fog infrastructure, highlighting constraints and optimization metrics. The work concludes by pinpointing open challenges in the domain of application placement in fog computing.

Xu jie Li et al. [21] discussed the complexities of task offloading within UAV-enabled fog computing networks. As smart devices proliferate and 5G communication evolves, the urgency for efficient task-offloading mechanisms in such networks becomes paramount. The research underscores the challenge as a combinatorial optimization problem, introducing a novel offloading scheme anchored on the fireworks algorithm. As the findings suggest, this approach notably outperforms traditional methods like genetic algorithms in minimizing task delays and optimizing data transmission rates. Such advancements are pivotal in enhancing the operational efficiency of fog computing networks, especially in multi-task scenarios.

Kalatzis et al. [3] addressed the challenges and solutions related to UAV-enabled IoT systems. It presents a distributed agent-based layered architecture designed to enable UAV-based fire detection, leveraging the capabilities of the IoT ecosystem. The focus is on efficiently consuming UAV processing, energy, and communication resources to ensure timely and accurate fire incident detection within surveilled areas. A vital feature of the proposed solution is the establishment of low-latency access to servers at the network's edge, allowing resource-constrained UAVs and their sensors to offload energy-consuming tasks selectively.

Aazam et al. [22] emphasized the importance of offloading tasks from devices that might be computationally constrained. Offloading refers to outsourcing tasks to another entity, especially when devices cannot execute specific intelligent tasks, such as those required for smart healthcare or virtual reality. The authors present a taxonomy of offloading, highlighting various criteria, including excessive computation, latency requirements, load balancing, and data management. Furthermore, they discuss several middleware technologies pivotal for the IoT, such as Cloudlet, Mobile Edge Computing (MEC), and Nano Datacenters. These technologies facilitate offloading by providing computational resources closer to the end devices. The paper underscores the rapid advancements in communication technologies that have paved the way for efficient offloading in fog computing.

Abdali et al. [23] discussed how fast the IoT is growing and why it leans on cloud computing. But, they see problems with using only cloud computing for the IoT, like delays and too much data. They say fog computing (FC) could help. FC works between the cloud and IoT, performing tasks at the edge of the network. This helps sort out the issues with just using cloud computing. They look closely at fog computing, showing its setup, which includes the cloud service layer, fog layer, and edge layer. They highlight that FC is like a smart setup put at the edge of the network to help with quick data handling, cut down delays, and make the IoT work better.

Table 2: Summary of Key Research on Fog Computing Applications and Innovations, presents a detailed overview of the recent advancements and innovative uses of fog computing technology. Among the innovative applications of fog computing, its integration into drone operations stands out as a transformative approach to enhancing operational efficiency and data processing capabilities. Fog computing's edge processing facilitates real-time data analysis directly from drones, offering significant advantages in various scenarios.

Table 2. Summary of key research on fog computing applications and innovations.

Author	Year	Main Focus	Key Findings	Applications/Use Case
Ometov et al. [16]	2022	Identify ecosystem of cloud, edge, and fog computing. Security threats. Computing paradigms.	Security and privacy challenges. Differences between cloud, edge, and fog computing. Mitigation techniques.	Cloud, edge, and fog computing security and privacy.
Aazam et al. [17]	2018	Fog computing with cloud computing in the IoT.	"Fog-assisted IoT" framework. Resource management. Latency reduction. Energy efficiency. Challenges.	IoT systems, smart cities, healthcare.
Hou et al. [15]	2019	Distributed fog computing in drone swarms.	Reliability modeling for drones. Mathematical models for drone swarm reliability. Disturbances in operations.	Drone swarms, robotic communication, IoT systems.
Haouari et al. [18]	2018	Significance of fog computing in the IoT.	Fog computing as a decentralized approach. Advantages over cloud computing. Latency in real-time applications.	IoT systems, real-time applications, smart devices, wearables.
Ahanger et al. [19]	2018	IoT and fog computing intersection.	Edge/fog computing for IoT device resource constraints. Augmenting centralized cloud systems.	IoT systems, data handling and delivery, technological advancements.
Brogi et al. [20]	2020	Application placement in fog computing.	Service quality improvement. Algorithms, prototypes, and test cases. Open challenges in application placement.	IoT systems, application deployment in fog environments, service optimization.
Xu jie Li et al. [21]	2020	Task offloading in UAV-enabled fog computing networks.	Task offloading as a combinatorial optimization problem. Minimizing task delays.	UAV networks, wireless communication systems.
Kalatzis et al. [3]	2018	UAV-enabled IoT systems.	Edge computing for task offloading in UAVs. Resource distribution and optimization. Semantic reasoning support.	UAV-based fire detection, IoT networks.
Aazam et al. [22]	2018	Offloading in fog computing for the IoT.	Importance of offloading. Criteria for offloading tasks.	Smart healthcare, virtual reality, intelligent vehicular communication, smart cities, IoT.
Abdali et al. [23]	2021	Fog computing in the IoT.	Fog as middleware between the cloud and IoT. Local data processing. Addressing latency and bandwidth limitations.	Environmental monitoring, infrastructure control, home automation.

3.3.1. Case Study on Environmental Monitoring

One notable application involves environmental monitoring, where drones equipped with sensors collect vast amounts of data on air quality, temperature, or vegetation. By leveraging fog computing, these data can be processed and analyzed almost instantaneously at the edge. This immediate analysis allows for quick action in response to environmental changes or emergencies, significantly reducing the time from data collection to decision-making.

3.3.2. Support for Autonomous Drone Navigation

In areas with limited or no connectivity, fog computing plays a crucial role in supporting autonomous drone navigation. By processing data locally, drones can make real-time

navigational decisions, navigate complex environments, and avoid obstacles without relying on distant cloud servers. This capability is vital for search and rescue missions in remote areas, where quick, autonomous decision-making can save lives.

3.3.3. Fog-Assisted IoT Framework

A study by Aazam et al. proposes a fog-assisted IoT framework that exemplifies how fog computing can optimize drone operations. By reducing the reliance on centralized cloud servers, this framework ensures that drones can operate more efficiently, with lower latency and improved data processing speed. Such frameworks highlight the potential of fog computing to revolutionize drone operations, making them more responsive, reliable, and capable of handling complex tasks in real time [22].

These case studies illuminate the practical benefits and challenges of integrating fog computing into drone operations. The environmental monitoring example underscores fog computing's capacity to facilitate immediate data processing and action, essential for timely environmental management and disaster response. Similarly, the autonomous navigation case study reveals how fog computing supports drones' operational independence and decision-making in connectivity-limited scenarios. These real-world applications not only validate the theoretical potential of fog computing in enhancing drone efficiency and security but also open avenues for further research and development. Future studies should explore innovative fog computing architectures, algorithms, and security protocols to address the evolving demands of drone technology. The integration of fog computing and drones represents a promising frontier for research, offering significant opportunities to revolutionize drone operations across various sectors.

3.4. Lightweight Blockchain Framework with Fog Computing

In the dynamic landscape of the IoT, secure, scalable, and efficient frameworks are paramount. The integration of lightweight blockchain frameworks and fog computing has garnered significant attention in recent years as a potential solution to the challenges faced by the IoT. Exploring the related work in this domain offers insights into the current state of research and sheds light on the advancements, gaps, and future directions. This section delves into a critical analysis and summary of seminal works that investigate the intersection of lightweight blockchain and fog computing technologies. The focus is on understanding how these combined technologies can be leveraged effectively in the context of the Internet of Things (IoT). Through this analysis, we aim to shed light on the advancements, challenges, and potential solutions that emerge when these technologies are synergistically applied to IoT scenarios.

In today's digital age, the rapidly expanding IoT ecosystem has ushered in many interconnected devices that continuously generate, transmit, and receive data. Amidst this intricate web of communication, maintaining robust cybersecurity becomes paramount to prevent malicious breaches and unauthorized data access. In this context, the amalgamation of the blockchain and fog computing emerges as a beacon of cyber resilience. The blockchain, renowned for its decentralized, tamper-proof, and transparent architecture, fortifies data integrity and combats potential threats, making every transaction traceable and immutable. However, the sheer volume of data and the latency-sensitive nature of many IoT applications can strain traditional blockchain implementations. Enter fog computing—a game-changer that operates as an intermediary layer between IoT devices and central cloud infrastructures. By processing and filtering data closer to its generation point, fog nodes optimize bandwidth usage, slash latency, and provide real-time insights while bolstering security at the edge. This synergy between blockchain's unparalleled cybersecurity capabilities and fog computing's localized efficiency crafts a formidable defense mechanism, significantly elevating the security posture of the vast IoT landscape [24]. Figure 2: Integration workflow of blockchain and fog computing in the IoT, visually illustrates this innovative synergy, offering a clear depiction of how these technologies interlink to enhance IoT security and operational efficiency.

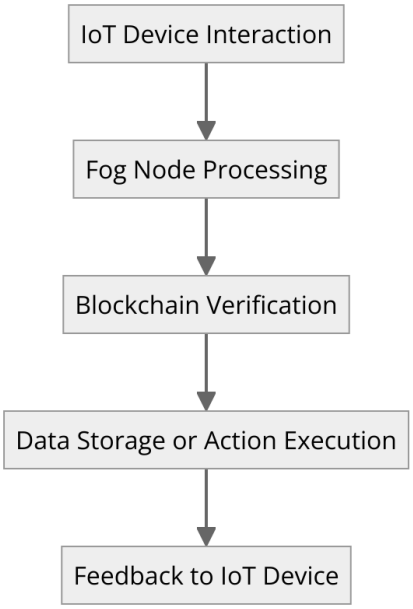

Figure 2. Integration workflow of blockchain and fog computing in the IoT.

3.5. Key Research on Lightweight Blockchain Framework with Fog Computing

Khan et al. [25] introduced a pioneering approach to monitoring land surface alterations by integrating drones, fog computing, and blockchain technology. Their blockchain-aware framework emphasizes distributed data management and monitoring, where image-based data captured by drones are transmitted to fog nodes. The primary innovation lies in utilizing a secure hash-encrypted (SH-256) consortium peer-to-peer (P2P) network, ensuring the integrity and security of the data. Furthermore, the authors employ smart contracts to automate the distributed monitoring system, encompassing UAV registration, daily image capture, and transaction updates in immutable storage. This framework is particularly pertinent for observing deforestation and energy generation changes in urban landscapes. Integrating these advanced technologies ensures efficient and automated monitoring and fortifies data management with enhanced security measures.

Alzoubi and Aljaafreh [26] looked at how blockchains and fog computing are coming together, especially for the Internet of Things, or IoT. They say fog computing is super important. Cisco came up with it in 2012 to help IoT gadgets work with the cloud better, giving quick services when asked. At the same time, they talk about how Blockchain is not in one place; it is spread out. It is known for being safe, strong, and open. They tell us there are different kinds of blockchains: public, private, and group ones, and each works in its own way. They even discuss different blockchain setups, like the first Bitcoin and the flexible Ethereum with all its extra parts. Their review is a big help in understanding how the blockchain and fog can work together and why it is so important for our digital world today.

Eddine et al. [27] defined the IoV domain, representing a transformative opportunity in both automotive and academic fields. However, the authors emphasize that IoV is fraught with severe security challenges characteristic of open-field IoT deployments. To tackle these weaknesses, the paper presents "EASBF"—a novel authentication technique that makes use of blockchain technology in fog computing-powered IoV platforms. One of the key aspects of EASBF design is its use of elliptic curve cryptography (ECC) and one-way hash functions to ensure strong information integrity, as well as protection from numerous cyber threats. Moreover, the decentralized nature of blockchain's architecture is coupled with fog computing efficiency, thereby making EASBF a strong solution to address IoV's latency and security issues. This research highlights the importance of strong authentication systems in IoV environments and provides a practical design for their implementation via the EASBF scheme.

Shukla et al. [28] pointed out the emerging security weaknesses, in particular, with the integration of these devices into wider network systems. The study, therefore, proposes a groundbreaking solution that integrates FC and blockchains to offset these challenges. This combined approach seeks to enhance healthcare IoT devices when it comes to security, authentication, and real-time processing. The core of their proposition is focused on the Advanced Signature-Based Encryption (ASE) algorithm aimed at the authentication and verification of everything related to Patient Health Data (PHD), as well as IoT devices. This integrated FC–blockchain model has the potential to improve data security device identification and ensure that there is a smooth transmission of information in an environment for healthcare IoT devices without being centralized.

Kamruzzaman et al. [29] investigated the transformative role of the blockchain, IoT, and fog computing in advancing healthcare services within the paradigm of smart cities. As urban environments increasingly integrate advanced information and communication technologies, the study underscores the pivotal role of these three technologies as catalysts for smart healthcare initiatives. While the IoT's expansive incorporation offers vast data collection and exchange capabilities, it grapples with challenges like cost efficiency and data privacy. The blockchain emerges as a solution, providing a decentralized framework that safeguards data integrity and ensures enhanced interoperability. Concurrently, fog computing, bridging the gap between data at network edges and cloud computing, promises reduced latency and heightened efficiency, vital for real-time healthcare applications. As the study suggests, the trio of technologies collectively paves the way for a more secure, efficient, and responsive healthcare infrastructure within the smart city landscape.

Bouachir et al. [30] examined the transformative potential of blockchains and fog computing in cyberphysical systems, particularly spotlighting their application in smart industries. Integrating these technologies becomes paramount as the IoT landscape burgeons. The study underscores the role of the blockchain as a decentralized, tamper-resistant ledger, emphasizing its capability to bolster data protection and establish decentralized trust within Industrial IoT (IIoT) frameworks. Concurrently, fog and edge computing emerge as pivotal architectures, decentralizing data processes and ensuring real-time data management at the network's edge. The authors propose an innovative Industrial Cyberphysical System (ICPS) model, amalgamating blockchains and fog/edge computing, aiming to surmount challenges in security, data storage, and quality of service. This exploration accentuates the synergistic potential of these technologies in revolutionizing smart industry operations, offering insights into enhanced data security, efficient real-time processing, and adept data management in the digital era.

Liu et al. [31] deal with the important issue of securing private information generated by IoT devices especially those transmitted through possibly insecure networks. The paper emphasizes the weaknesses associated with present encryption and access control solutions, especially their vulnerability to single points of breakdown. To eliminate these problems, the authors propose a brand new distributed access control system based on blockchain technology. With the use of fog computing, however, this system can offer enhanced security by processing data closer to their source and, consequently, reducing latency and potential exposure. Additionally, the study includes MLNCML and LSB techniques to encrypt IoT data at edge nodes to secure them during transit as well as storage. The authors also promote attribute-based access control as a dynamic, fine-grained solution for controlling IoT data access. The experiment published in the research validates the efficiency of the proposed mechanism for safeguarding IoT data privacy. This research highlights the importance of combining blockchains with fog computing and sophisticated encryption techniques as a reliable solution for strengthening the IoT when it comes to issues concerning data security.

Muthanna et al. [32] proposed an integrated framework to fortify the security and reliability of IoT networks. Recognizing the challenges posed by the proliferation of IoT devices, such as security concerns, massive traffic, and energy constraints, the research emphasizes the integration of fog computing, Software-Defined Networking (SDN), and

the blockchain. The fog computing paradigm is highlighted for its capability to process and store data closer to their source, thereby reducing latency and bolstering security. With its distinct separation of the forwarding and control planes, SDN offers a dynamic network structure further enhanced by a distributed controller scheme. The blockchain is introduced to ensure a decentralized, trustful environment, which is particularly vital for IoT's vast, interconnected landscape. The authors also present a data offloading algorithm and a traffic model, aiming for optimal resource utilization and efficient data flow. Through simulations and testbed evaluations, the study validates the potential of this integrated approach in achieving reduced end-to-end latency, heightened security, and efficient resource utilization in IoT networks.

Ngabo et al. [33] address the security vulnerabilities inherent in the fog computing architecture and the Cloud of Things (CoT) technology, particularly concerning medical data mining. With the rapid advancements in fog computing and CoT, there is a surge in data mining management and artificial intelligence operations. However, this multi-layered model, comprising the edge, fog, and cloud layers, is susceptible to various security threats. Given the vast amount of data generated within this architecture, traditional data storage and security mechanisms need to be revised. The authors propose a public-permissioned blockchain security mechanism to counter these challenges, fortified with the elliptic curve cryptography (ECC) digital signature. This approach ensures an immutable security solution transaction transparency and effectively prevents the unauthorized tampering of patient records within the IoT's fog layer. By leveraging blockchain technology and ECC digital signatures, the study offers a robust solution to the fog computing model's challenges of latency, centralization, and scalability. The research underscores the potential of blockchain technology in ensuring data security, especially for sensitive medical data, in the IoT landscape.

Gumaei et al. [34] presented a framework integrating blockchain technology with drones for enhanced security in a 5G setting. Recognizing the vulnerabilities of drones, especially in data security, the research introduces a combination of a deep recurrent neural network (DRNN) and edge computing for drone identification and flight mode detection using Radio Frequency (RF) signals. The integration of blockchains ensures data integrity and secure transmission. Using the DroneRF dataset for evaluation, the proposed DRNN model demonstrated high accuracy in drone detection and mode identification, highlighting the potential of blockchain and 5G synergy in drone operations.

Kaur et al. [35] addressed the challenges of data transmission in vehicular networks. Recognizing the limitations of cloud-based models, the authors introduce vehicular fog computing (VFC) to bring computing resources closer to vehicles. To ensure secure communication in VFC, they propose an authentication scheme using blockchain and elliptic curve cryptography (ECC). This approach promises secure, efficient, and reliable data transmission in vehicular networks, making it a significant contribution to the field.

In the evolving landscape of drone technology, the integration of lightweight blockchains and fog computing emerges as a pivotal advancement, promising to significantly enhance the operational efficiency and security of drone operations. This synergy is not just theoretical but has begun to manifest in pilot studies and frameworks that showcase tangible benefits in real-world applications.

As we delve deeper into the potential of merging lightweight blockchain technologies with fog computing for IoT applications, it becomes crucial to survey the landscape of existing research. Table 3: provides a comprehensive summary of key research contributions in this field. This table encapsulates pivotal studies, highlighting innovative approaches and outcomes that underline the synergy between lightweight blockchain and fog computing. Such a summary not only showcases the breadth of exploration but also serves as a testament to the dynamic advancements being made toward securing and optimizing IoT infrastructures. Reviewing this table will offer readers insight into the foundational and cutting-edge work that lays the groundwork for future developments in integrating blockchain and fog computing technologies.

Table 3. Lightweight blockchain framework with fog computing.

Author	Year	Objective/Research Question	Blockchain and Fog Integration	Key Findings/ Contributions
Khan et al. [25]	2021	Introduction of a blockchain-aware framework for land surface change monitoring using drones.	Utilizes an SH-256 consortium P2P network with smart contracts.	Efficient, secure, automated monitoring and data management.
Alzoubi and Aljaafreh [26]	2023	Systematic review of blockchain and fog computing integration in the IoT.	Highlights fog as an IoT–cloud bridge and blockchain's decentralized attributes.	Guide to blockchain–fog applications in the digital domain.
Eddine et al. [27]	2021	Exploration of security challenges in the IoV and EASBF authentication scheme.	Blockchains in fog computing-enabled IoV environments.	Robust solution addressing IoV security and latency concerns.
Shukla et al. [28]	2021	Security challenges in healthcare IoT devices and an integrated solution.	Synergizes fog computing and blockchains for healthcare IoT devices.	ASE algorithm and three-tier FC architecture for secure data transmission.
Kamruzzaman et al. [29]	2022	Role of the blockchain, IoT, and fog in smart city healthcare.	Blockchains for data security; fog computing for real-time IoT healthcare devices.	Enhanced healthcare infrastructure in smart cities.
Bouachir et al. [30]	2020	Blockchains and fog computing in cyberphysical systems for smart industries.	Blockchains for data protection in the IIoT and fog computing for data management.	ICPS model integrating blockchains and fog/edge computing.
Liu et al. [31]	2021	Safeguarding sensitive IoT data.	Blockchains for access control, fog computing for data processing.	Mechanism integrating blockchains, fog computing, and encryption.
Muthanna et al. [32]	2019	Enhancing security and reliability of IoT networks.	Integration of fog computing, SDN, and blockchains.	Framework for IoT networks with a data offloading algorithm.
Ngabo et al. [33]	2021	Security in fog computing architecture and CoT.	Public-permissioned blockchain with ECC digital signature.	Robust security solution for data immutability and transparency.
Gumaei et al. [34]	2021	Enhancing drone security in 5G.	Blockchain with DRNN and edge computing for drone identification.	Framework for data integrity and secure transmission for drones.
Kaur et al. [35]	2019	Data transmission challenges in vehicular networks.	Vehicular fog computing and authentication using blockchains and ECC.	Secure and efficient data transmission approach for vehicular networks.

3.5.1. Theoretical Models and Synergistic Potential

The theoretical model underlying the integration of lightweight blockchains and fog computing hinges on combining the blockchain's inherent strengths in securing data through its decentralized ledger system with fog computing's ability to process data at the edge, close to where they are generated. This combination ensures that drone operations benefit from both enhanced data integrity and reduced latency, which are crucial for applications requiring immediate decision-making and action, such as border surveillance and emergency response scenarios.

One of the cornerstone benefits of this integration is the enhanced security provided by blockchain technology. Through its decentralized control, blockchain ensures that data recorded from drone operations, including flight paths, mission-critical decisions, and collected environmental data, remain immutable and secure from tampering. This aspect is

vital for maintaining the integrity of sensitive operations and safeguarding against cyber threats.

Concurrently, fog computing addresses the efficiency aspect by significantly reducing the latency involved in data processing. By situating data processing closer to the drone, fog computing facilitates real-time analytics and decision-making, a necessity for drones operating in dynamic or hostile environments where every second counts.

3.5.2. Monitoring Land Surface Changes with Khan et al.'s Framework

A practical illustration of this integration's potential is seen in the work of Khan et al., who developed a blockchain-aware framework for monitoring land surface changes [25]. In their study, drones equipped with sensors collect image-based data, which are then securely transmitted to fog nodes for immediate processing. The application of a secure hash-encrypted consortium peer-to-peer (P2P) network, alongside the use of smart contracts, ensure both the integrity and security of the transmitted data. This framework is particularly relevant for environmental monitoring, offering a blueprint for utilizing the combined strengths of lightweight blockchains and fog computing to achieve secure, efficient, and automated monitoring of vast areas.

3.5.3. Implications for Future Drone Operations

The integration of lightweight blockchains and fog computing holds immense promise for the future of drone operations across various domains. Beyond environmental monitoring, this synergy can be adapted for urban planning, agricultural management, and disaster response, among other applications. The key to unlocking this potential lies in further research and development, focusing on refining integration techniques, enhancing the scalability of blockchains within the fog computing architecture, and addressing the challenges of real-time data processing.

In conclusion, the symbiotic relationship between lightweight blockchains and fog computing presents a forward-thinking approach to addressing the twin challenges of security and operational efficiency in drone technology. By harnessing this integration, the future of drone operations can be reimagined, paving the way for drones that are not only smarter and faster but also inherently secure.

3.6. Elevating Drone Operations with Blockchain and Fog Computing

The systematic review of 32 seminal papers has illuminated the burgeoning intersection of blockchain and fog computing technologies within the realm of drone operations. This fusion is poised to redefine the operational paradigms of drones, offering enhanced security, efficiency, and scalability. The reviewed literature not only underscores the theoretical feasibility of this integration but also showcases practical implementations and the tangible benefits therein.

Advancements through Integration

The collective insights from the reviewed papers reveal a consensus on the pivotal role of blockchains in fortifying the security framework for drone operations. By leveraging blockchains, data integrity and privacy are significantly bolstered, thereby mitigating risks associated with data tampering and unauthorized access. Concurrently, fog computing emerges as a critical enabler of real-time data processing capabilities. Its proximity to data sources—drones in motion—dramatically reduces latency, a crucial factor in time-sensitive applications such as emergency response and live surveillance.

A notable advancement highlighted in our review is the development of lightweight blockchain protocols, which are particularly suited for the limited computational resources available on drones. These protocols ensure that the security benefits of blockchain are realized without imposing prohibitive computational demands.

Despite the progress, our review has identified several gaps that warrant further investigation. One such gap is the need for more robust and scalable integration frameworks

that can seamlessly accommodate the dynamic nature of drone networks. Current models, while promising, often fall short in addressing the complex interplay between blockchains and fog computing in highly mobile and variable drone environments.

Another critical area for future research is the optimization of consensus mechanisms within blockchains to suit the unique requirements of fog computing architectures. The goal here is to devise mechanisms that balance the need for security and decentralization with the imperative for high-speed data processing and minimal energy consumption.

Environmental sustainability emerges as another significant concern. The energy-intensive nature of conventional blockchain operations, particularly those based on Proof of Work (PoW) consensus algorithms, poses sustainability challenges. Exploring energy-efficient consensus algorithms, such as Proof of Stake (PoS) or Directed Acyclic Graph (DAG) technologies could provide a pathway to more sustainable drone operations.

3.7. Strategies for Latency Minimization in Drone Operations

In the rapidly evolving domain of drone technology, minimizing latency in operational data processing is not merely a performance enhancer but a critical necessity. Latency, the delay before a transfer of data begins following an instruction for its transfer, directly impacts the effectiveness, safety, and responsiveness of drone operations. This is especially true in applications requiring real-time decision-making and action, such as surveillance, emergency response, and military operations, where even minimal delays can have significant consequences.

The integration of fog computing and blockchain technologies presents a promising approach to addressing these latency challenges. Fog computing, with its architecture that brings computational resources closer to the data source (i.e., the drones), significantly reduces the time required for data transmission and processing. This proximity enables real-time data analysis and decision-making directly at the edge of the network, where drones operate, thereby minimizing latency.

Moreover, blockchain technology contributes to this objective by providing a secure and decentralized framework for data transactions. While traditionally not associated with speed due to its computational intensity, lightweight blockchain protocols have been developed specifically for use in environments like fog computing, where efficiency is paramount. These protocols ensure that data integrity and security are maintained without the latency typically associated with blockchain operations.

Together, fog computing and blockchains offer a dual approach to tackling latency: fog computing addresses the physical proximity and immediacy of data processing, while blockchains ensure the rapid, secure transmission of these data across the network. This integration heralds a new era of drone operations, where the challenges of latency are significantly mitigated, enabling drones to perform more complex, sensitive tasks with greater reliability and efficiency.

3.7.1. Real-Time Data Processing Capabilities

The adoption of fog computing significantly amplifies the real-time data processing capabilities essential for drone operations. By situating computational resources in closer proximity to the operational environment, fog computing drastically reduces the latency traditionally encountered in data transmission to centralized cloud services. This architectural advantage facilitates instant data analysis and decision-making, a requisite for drones engaged in time-sensitive missions such as surveillance, search and rescue, and immediate environmental assessment [36].

The essence of fog computing in enhancing real-time data processing lies in its ability to perform complex computational tasks at or near the data source. This includes data filtering, aggregation, and analysis directly on the edge of the network, where drones operate. Such localized processing eliminates the time delays inherent in sending vast volumes of data back and forth to distant servers, thereby ensuring that drones can react to dynamic environmental changes and make informed decisions promptly.

Moreover, fog computing supports the deployment of advanced machine learning models and algorithms directly onto the drone or nearby edge devices. This capability allows drones to learn from new data in real time, adapt their operational parameters, and execute autonomous decisions based on immediate data insights [37]. For instance, a drone monitoring forested areas for wildfire detection can instantly analyze images for signs of fire, calculate the potential spread using real-time weather data processed through fog nodes, and communicate alerts without the latency that would hinder a timely response.

In practice, real-time data processing through fog computing has been exemplified in agricultural drones that monitor crop health. These drones utilize near-edge processing to analyze spectral imagery on the fly, identifying areas of stress, disease, or need for irrigation. The immediate processing of such data enables precise, real-time adjustments to agricultural practices, showcasing the pivotal role of fog computing in enhancing the efficiency and responsiveness of drone operations.

By leveraging the decentralized nature of fog computing, drone operations are poised to achieve unprecedented levels of autonomy and operational efficiency, driven by the capacity for real-time data processing. This technological evolution not only broadens the scope of applications for drones but also sets new benchmarks for their performance in critical and everyday tasks alike.

3.7.2. Optimization of Communication Protocols

The optimization of communication protocols plays a critical role in minimizing latency and enhancing the efficiency of drone operations integrated with fog computing and blockchain technologies. By refining how data are transmitted and processed between drones, fog nodes, and blockchain networks, these optimizations ensure faster, more reliable communication essential for real-time drone applications.

One key strategy involves the use of lightweight communication protocols that are specifically designed for the limited bandwidth and power resources characteristic of drone and fog computing environments. These protocols reduce the data payload size and streamline the data transmission process, significantly cutting down the time it takes for messages to travel across the network. For example, the MQTT (Message Queuing Telemetry Transport) protocol, known for its lightweight and efficient messaging system, is widely adopted in IoT and drone communications for its low power consumption and minimal data packet size, making it ideal for real-time applications.

In the context of blockchain integration, the optimization also extends to consensus algorithms, which are fundamental to ensuring data integrity and trust within the network. Traditional blockchain consensus mechanisms like Proof of Work (PoW) are computationally intensive and can introduce delays. As a remedy, more efficient consensus algorithms such as Proof of Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT) are being explored and adapted for fog computing environments. These algorithms offer a balance between security and speed, enabling quicker transaction validations without the extensive computational overhead, thereby reducing latency in blockchain transactions.

Moreover, advancements in communication protocol optimization include the development of adaptive routing algorithms that dynamically select the most efficient data paths between drones and fog nodes. These algorithms take into account factors such as network congestion, node availability, and data priority to optimize the route data takes, further reducing latency and enhancing the overall responsiveness of the system [38].

An illustrative example of these optimizations in action can be seen in disaster response scenarios, where drones equipped with sensors collect critical data from the affected area. Through optimized communication protocols, these data are swiftly transmitted to nearby fog nodes for immediate analysis, and relevant insights are quickly shared with emergency responders via a blockchain network. The use of efficient consensus algorithms ensures that this crucial information is processed and validated rapidly, allowing for timely decision-making and coordinating response efforts.

In summary, the optimization of communication protocols is pivotal to leveraging the full potential of fog computing and blockchains in drone operations. By facilitating faster, more efficient data exchange and processing, these optimizations are instrumental in advancing drone capabilities, particularly in scenarios requiring real-time or near-real-time responses [39].

4. Overview of the Existing Literature

Recent technological advancements in the blockchain, fog computing, and their integration into various domains have been extensively explored in the literature. This overview collates insights from seminal works ranging from vehicular fog computing to security and efficiency enhancements in drone operations. Each piece contributes uniquely to the field, yet leaves an identifiable gap that this review aims to bridge.

4.1. Blockchain and Fog Computing in Vehicular Networks

Kaur et al. [35] on a "Blockchain-based Lightweight Authentication Mechanism for Vehicular Fog Infrastructure" demonstrate the potential of blockchain technology in providing secure and efficient authentication mechanisms within vehicular networks. This exploration underscores blockchain's scalability and efficiency, crucial for the evolving demands of vehicular communications.

4.2. Enhancement of Cyberphysical Systems (CPSs)

Bouachir et al. [30] delve into "Blockchain and Fog Computing for Cyberphysical Systems", emphasizing the transformative potential of these technologies in industrial CPSs. Their research outlines the broad applications of the blockchain and fog computing in improving data storage, QoS, and security in industrial settings, setting a foundation that prompts further investigation into other domains.

4.3. Drone Operations' Security and Efficiency

The necessity for enhanced security and efficiency in drone operations has prompted various scholarly inquiries. The specific challenges associated with drone operations, such as real-time data processing, autonomous navigation, and security against both physical and cyber threats, necessitate detailed review. Yet, the existing literature often focuses on terrestrial or static applications of the blockchain and fog computing, with less emphasis on dynamic, airborne contexts.

4.4. Identification of Gaps

Across the documents provided, a pattern emerges: a robust exploration of blockchain and fog computing applications in vehicular networks and CPSs, with less focus on the unique environment of drone operations. While the principles of secure authentication, efficient data processing, and decentralized control are well-explored in ground-based networks and industrial settings, the translation of these principles to drone technology remains underexplored. Specifically, the application of the blockchain for real-time, secure communication between drones, and the utilization of fog computing for on-the-edge data processing in drones, presents a novel area ripe for investigation. This review is necessitated by the clear gap in the literature regarding the application of blockchain and fog computing technologies specifically to drone operations. Drones present unique operational challenges, including but not limited to dynamic flight environments, the need for lightweight and efficient computing solutions, and high-security requirements for autonomous operations. This paper aims to achieve the following:

1. Synthesize and critique existing applications of the blockchain and fog computing in related domains, with a specific lens on their potential applicability to drones.
2. Highlight the operational, security, and efficiency challenges unique to drone operations that are not fully addressed by existing reviews.

3. Propose new research directions focused on leveraging the blockchain and fog computing to enhance drone operations, thereby contributing significantly to the field.

While the existing body of literature provides a robust foundation in the application of the blockchain and fog computing across various domains, there remains a significant gap in their application to enhance drone operations. This review seeks to bridge that gap, offering a comprehensive analysis of how these technologies can transform drone security and efficiency, and setting the stage for future research in this rapidly evolving field.

4.5. Integrated Insights and Implications

Significant insights into the integration of fog computing with lightweight blockchain frameworks were investigated in the research and studies, especially about the IoT. Important conclusions consist of the following:

- Enhanced security and efficiency: It has been demonstrated that combining blockchain technology and fog computing dramatically improves the security and effectiveness of IoT systems. The combination of fog computing's proximity to data sources and the blockchain's decentralized structure provides a solid answer to latency and data integrity issues.
- Various uses in various industries: The combined capabilities of the blockchain and fog computing have demonstrated various applications, from Industrial IoT and smart cities to environmental monitoring and transportation. This flexibility highlights how these technologies have the power to transform several industries completely.
- Addressing IoT challenges: The integration addresses several critical IoT challenges, including data privacy, efficient resource utilization, and real-time data processing demands.

4.6. Discussion of Research Implications

The implications of these findings are far-reaching:

- IoT cybersecurity: An enhanced cybersecurity framework is provided by the integrated approach. This is essential when cybercriminals are increasingly focusing on IoT devices.
- Future of smart cities and industries: The capacity for real-time data processing and enhanced security opens new possibilities for developing smart cities and industrial automation.
- Scalability and sustainability: Without sacrificing security or performance, the integration offers a scalable and sustainable model for IoT deployments in the future.

5. Performance Metrics and Evaluation Methods in Blockchain and Fog Computing for Drone Operations

The integration of lightweight blockchain and fog computing technologies presents a promising avenue for enhancing the security and efficiency of drone operations. In the pursuit of optimizing these integrations, the role of performance metrics cannot be overstated. These metrics serve as quantifiable measures that allow researchers and practitioners to evaluate the effectiveness, efficiency, and reliability of technological solutions. Furthermore, the methods used to assess these metrics—from theoretical frameworks to practical implementations—offer insights into the robustness and applicability of proposed models in real-world scenarios.

This section aims to provide a synthesized overview of the performance metrics and evaluation methods utilized in the current body of literature on the integration of blockchain and fog computing technologies in drone operations. By examining how these technologies are evaluated, we can better understand the state of research, identify significant advancements, and pinpoint areas that require further exploration. Through this analysis, we endeavor to highlight the diversity of the metrics applied, the variety of methods employed, and the balance between theoretical analysis and empirical validation. In doing so, we seek to underscore the importance of comprehensive evaluation frameworks

that can accurately capture the multifaceted impacts of technological integrations on drone operations.

5.1. Overview of Performance Metrics

The evaluation of technological integrations within drone operations relies on a set of performance metrics that offer insights into various aspects of system functionality, efficiency, and security. Below is a summarized Table 4 of the main performance metrics identified across the reviewed studies, along with a brief explanation of each metric's relevance to drone operations and the integration of blockchain and fog computing technologies.

Table 4. Overview of performance metrics for drone operations with blockchain and fog computing integration.

Metric	Relevance to Drone Operations
Latency	Measures the time delay in processing and communicating data, which is crucial for real-time drone applications such as navigation and surveillance, where quick data analysis and decision-making are essential.
Throughput	Quantifies the volume of data that can be processed within a given timeframe. It is important to assess the system's capability to handle the large amounts of data generated by drones, especially in monitoring and mapping tasks.
Resource Utilization	Assesses the efficiency of computational and energy resources used by the system. Essential for ensuring the sustainability of drone operations and that the integration of the blockchain and fog computing does not excessively drain the drone's limited resources.
Security	Evaluates the system's ability to protect data against unauthorized access and breaches. It is paramount in drone operations due to the sensitive nature of the data collected and the implications of potential security lapses.
Scalability	Examines the system's ability to adapt and manage increased loads, which could arise from adding more drones or processing larger datasets. It ensures that the technological solution can grow to meet expanding operational demands without degradation in performance.
Reliability	Measures the consistency of system performance over time, including metrics like uptime and error rates. It is critical for maintaining dependable drone operations and ensuring service delivery meets expected standards.

These performance metrics collectively offer a comprehensive framework for evaluating the effectiveness and efficiency of blockchain and fog computing integrations in drone operations. By understanding the relevance of each metric, researchers and practitioners can better assess the strengths and limitations of current technologies and identify areas for improvement or further investigation.

5.2. Evaluation Methods

The performance of blockchain and fog computing integrations in drone operations is assessed using a variety of evaluation methods, each offering unique insights and bearing distinct advantages and limitations. This subsection delineates the principal methods employed in the literature: theoretical models, simulations, prototype testing, and practical implementations. Table 5 categorizes these methods, detailing their respective strengths and weaknesses, and how they contribute to our understanding of the efficacy of blockchain and fog computing within drone operational frameworks

Table 5. Evaluation methods for blockchain and fog computing in drone operations.

Method	Strengths	Limitations
Theoretical Models	- Allows for the examination of complex systems without costly experiments. - Facilitates the exploration of a wide range of scenarios.	- May oversimplify real-world complexities. - Relies on assumptions that may not hold in practical applications.
Simulations	- Enables detailed analysis under different configurations. - Reduces the risks and costs associated with physical prototype testing.	- May not fully account for real-world operational variability. - Accuracy depends on the fidelity of the simulation models.
Prototype Testing	- Provides concrete evidence of system performance in a real-world-like setting. - Allows for hands-on identification and troubleshooting of issues.	- Resource-intensive, requiring significant time and investment. - This may not be feasible for large-scale systems.
Practical Implementations	- Offers the most accurate representation of real-world applicability. - Provides invaluable feedback from actual use cases.	- Involves substantial risk, including potential operational disruptions. - Requires comprehensive planning and resources.

The review of the literature on integrating the lightweight blockchain and fog computing into drone operations reveals a strong emphasis on security metrics, albeit at the expense of fully exploring other crucial performance aspects such as latency, throughput, and scalability. Notably, there is a gap between the theoretical models and actual practical implementations, underscoring a critical need for more real-world testing to validate and refine these technologies for drone use. Furthermore, while the potential for enhanced operational efficiency through fog computing is recognized, challenges remain in optimizing resource utilization without overburdening drones' limited capacities. Addressing these gaps, particularly by advancing practical implementations and focusing on scalability and resource efficiency, emerges as a vital pathway for future research and development in drone technology, promising more robust, efficient, and scalable drone operations.

6. Challenges and Limitations

The application of the blockchain (BC) within fog computing represents significant challenges, especially concerning scalability issues as described in the research. This technology fusion is faced with challenges mainly attributed to the fact that real-time information from IoT devices is vast:

1. Complexity in Implementation: For implementation and maintenance, fog computing with the blockchain brings an additional layer of complexity. This problem arises from the necessity to align two complex technologies requiring a thorough comprehension of fog computing and blockchain specifics [35].
2. Storage capacity and scalability constraints: The underlying challenge lies in the fact that most existing blockchains are not inherently designed to handle massive amounts of data storage. With the underlying blockchain continuously expanding, each node must maintain the entire chain to validate new blocks. This necessity introduces a bottleneck, as conventional blockchains are limited in their transaction-handling capabilities and are not optimized for extensive data storage. Attempting to store vast amounts of data results in significant latency, impacting the performance of fog computing's limited resources [40].
3. Innovative approaches for real-time processing: To address these challenges, there is a pressing need for innovative approaches that simplify real-time processing and storage. Techniques such as data compression and data lightning are proposed to alleviate the strain on the system [24]. A comprehensive understanding of projected network performance and scalability is crucial for the development of these innovative solutions.

4. Trade-offs for decreasing latency: Various techniques, including off-chain transactions and sharding, have been introduced to decrease latency and optimize storage in blockchains with fog computing integration. However, these innovations imply trade-offs that require further research to strike the right balance between scalability, security, and decentralization. Additionally, the environmental impact, especially in energy consumption, remains a critical concern, particularly in Proof of Work (PoW)-based blockchain systems. Exploring alternative algorithms while maintaining security and dependability is a key avenue for future research [41].
5. Quality of service (QoS) metrics: The current consensus models often fall short in delivering satisfactory quality of service (QoS) metrics, including latency, energy use, and operating costs. Notably, throughput and latency for real-world applications frequently do not meet the desired QoS levels. As an example, Bitcoin, while processing a limited number of transactions per second, experiences considerable consensus execution delays. Novel resource scheduling strategies are required to decrease energy consumption without compromising QoS metrics, ensuring a balance between system efficiency and quality of service [42].
6. Privacy challenges in the blockchain: The inherent nature of the BC, where information is stored on a public ledger, poses challenges to privacy and confidentiality. The transparency of the ledger makes it challenging to ensure the privacy of sensitive data. Several anonymization or encryption-based techniques may be employed to safeguard data confidentiality. However, these methods are not foolproof and are contingent on the specific implementation and environment [43].
7. Impact on reliability and data integrity in fog computing: Although the blockchain contributes to fog computing data flexibility and security, questions of its effects on reliability or relatedness/integrity in the case of fog computing appear. The blockchain validates data creators and provides for the immutability of the data, which are not susceptible to changes. On the other hand, corrupted data entering the blockchain may yield problems because corruption is not immediately visible and it can be a case of consistently damaged information. The corruption of data may arise as a result of several factors such as hostile attacks, surroundings, and device failures [44].
8. Technological maturity: The relative novelty of both fog computing and the blockchain introduces challenges related to their technological maturity. As emerging technologies, their full potential and long-term implications are still being understood. Navigating this evolving landscape requires a proactive approach to harness their capabilities fully [45].

Table 6: outlines the multifaceted hurdles and constraints this integration faces. The table serves as a comprehensive guide through the myriad challenges identified, from complexity in implementation to the pressing need for technological maturity. Each point in the table not only highlights the critical issues but also encapsulates the ongoing efforts and proposed solutions to navigate these obstacles. This systematic compilation underscores the imperative for innovative strategies to overcome the identified limitations and propel the seamless amalgamation of blockchain and fog computing technologies forward, paving the way for enhanced security and efficiency in drone operations and beyond.

Table 6. Challenges and limitations in blockchain and fog computing integration.

Challenge Category	Description	Key Papers
Complexity in implementation	Aligning fog computing with blockchain adds complexity due to the need for a comprehensive understanding of both technologies.	[35]
Storage Capacity and scalability	Blockchain's design limitations in handling large data volumes create bottlenecks in performance and scalability, impacting fog computing's efficiency.	[40]
Innovative approaches for real-time processing	The need for simplified real-time processing and storage solutions to alleviate system strain. Techniques such as data compression and data lightning are proposed.	[24]
Trade-offs for decreasing latency	Techniques like off-chain transactions and sharding reduce latency but introduce trade-offs requiring further research to balance scalability, security, and decentralization.	[41]
Quality of service (QoS) metrics	Existing consensus models often fail to meet desired QoS levels, indicating a need for novel resource scheduling strategies.	[42]
Privacy challenges in blockchains	The transparency of the blockchain ledger complicates ensuring data privacy and confidentiality, with techniques being contingent on specific implementations.	[43]
Impact on reliability and data integrity	The blockchain enhances data security in fog computing but raises concerns about data reliability and integrity, especially with corrupted data entry.	[44]
Technological maturity	The emergent nature of both fog computing and blockchains presents challenges related to their technological maturity and understanding of their long-term implications.	[45]

Addressing Unique Challenges in Drone Operations

While the blockchain and fog computing offer transformative potentials for drone technology, realizing these benefits necessitates navigating a set of unique challenges intrinsic to drone operations. These challenges, often overlooked in broader reviews, are critical to developing comprehensive and effective solutions:

- Operational challenges: These include the dynamic and often unpredictable environments in which drones demand advanced decision-making and autonomous navigation capabilities. The integration of blockchains and fog computing must, therefore, not only ensure robust data integrity and decentralized processing but also support the complex algorithms required for drones to adapt in real time to environmental changes and mission parameters.
- Security challenges: Beyond safeguarding data, the security measures for drones must encompass physical device security and operational integrity. Utilizing blockchains for immutable operation logs and leveraging fog computing for localized, real-time

security assessments present a novel approach to creating a multi-tiered security framework that addresses both cyber and physical threats.

- Efficiency challenges: The energy efficiency of drones, especially for prolonged missions or in resource-constrained environments, is paramount. Innovations in blockchains and fog computing must focus on minimizing energy consumption without compromising the operational efficacy of drone networks. This includes exploring lightweight blockchain protocols and energy-efficient data processing models tailored to the unique requirements of drone operations [46].

By specifically addressing these challenges, future research can unlock new dimensions of drone operational capabilities, enhancing security, efficiency, and adaptability. This endeavor not only contributes to the technological evolution of drones but also ensures their sustainable integration into an increasingly connected and automated world.

7. Future Research Directions

In charting the course for future research, several key areas emerge as focal points for advancing the integration of blockchains and fog computing. These directions not only address current challenges but also pave the way for a more robust and efficient technological synergy:

- Improved integration approaches: New studies should focus on creating simpler and more efficient means of integrating blockchains with fog computing. The simplification of the integration process can thereby contribute to improving the synergy between these technologies, which would make it more convenient and efficient when implementing them collaboratively. Exploring new approaches, frameworks, and protocols can help to develop a more efficient integration of blockchain technology with fog computing by eliminating complexity issues but enhancing performance.
- Scalability solutions: The rapid explosion of data collected from IoT networks demands a focused study on scalability measures. By contrast, future research should concentrate on bold ideas that could address the large quantities of data to be generated by IoT networks in the years ahead. Scalability solutions might include innovations in data processing methods, storage techniques, or network architectures. It is, therefore, essential to investigate how blockchains and fog computing can act in a way that allows them to scale automatically as IoT ecosystems change [24].
- Long-term impact studies: It is necessary to examine long-term in-depth studies so that the enduring impacts of blockchain and fog computing technologies on privacy, security, and IoT evolution can be ascertained. Future studies have to investigate the elaborate relationship between blockchains, fog computing, and IoT technology's evolution. This entails considering the lasting implications regarding data privacy, integrated systems' security standing, and the IoT application evolutionary path. These studies will provide priceless knowledge regarding the sustainable and code-pendent adoption of blockchains and fog computing within the wider technological infrastructure.

Adding to the landscape of future research, federated learning emerges as a promising technique to further enhance the security and efficiency of drone operations. With its capability to perform machine learning across distributed networks while maintaining data privacy, federated learning can play a pivotal role in developing secure, scalable, and efficient drone operations. Relevant studies, such as federated split learning for sequential data in satellite–terrestrial integrated networks and SFL-MDrone synchronous federated learning enabled multi-drones, have demonstrated its effectiveness [47]. Future research should delve into harnessing federated learning within the blockchain and fog computing paradigm to unlock new potentials in drone operational security, efficiency, and data privacy.

A potential route for the development of IoT technology is the fusion relationship between the fog computing and lightweight blockchain structure. This integration is an area worth further exploration not only because of existing challenges but also due to the

potential benefits it would bring for security, efficiency, and application versatility. Research in this direction should aim to improve the cooperation of fog computing and lightweight blockchain systems and explore opportunities for improving their synergistic capacities. With a focus on overcoming challenges and perfecting integration strategies, researchers can unleash the true power of this technological synergy that will lead IoT applications to their bright future.

The investigation into merging the lightweight blockchain with fog computing technologies presents a promising avenue for advancing drone technology, underlining the pivotal role this integration plays in refining operational efficiencies, enhancing security measures, and scaling capabilities. The future research directions we have charted aim directly at surmounting existing hurdles, promising a leap forward in how drones are deployed, managed, and utilized across various sectors. By delving into these specified areas—improving integration methods, ensuring scalability, securing data privacy, and minimizing environmental impacts—we open a pathway to a future where drones operate with unprecedented autonomy and precision. This journey toward technological synergy between blockchains and fog computing, while fraught with challenges, is ripe with opportunities for innovation. It beckons a collaborative, multidisciplinary effort to transcend current limitations, ensuring that the drones of tomorrow are not only more capable but also operate within an ecosystem that prioritizes sustainability, security, and efficiency. Table 7 encapsulates our vision for advancing drone technology, highlighting priority areas.

Table 7. Future research directions in lightweight blockchain with fog computing.

Area	Key Challenges	Future Research Directions
Scalability	Handling large volumes of data	Explore new algorithms and architectures that improve blockchain scalability without compromising security or decentralization.
Security	Enhancing data privacy	Develop advanced encryption methods and privacy-preserving techniques tailored for fog computing environments.
Efficiency	Reducing latency	Investigate off-chain solutions and more efficient consensus mechanisms that reduce transaction validation times.
Integration	Seamless technology fusion	Study frameworks and standards that facilitate easier integration of blockchains with fog computing and IoT devices.
Environmental Impact	Energy consumption of PoW	Research into less energy-intensive consensus algorithms like Proof of Stake (PoS) or Directed Acyclic Graph (DAG) technologies.

8. Conclusions

The systematic literature review conducted within this study meticulously synthesizes the existing body of research on the integration of lightweight blockchain and fog computing technologies in drone operations. Our analysis reveals a considerable potential for this integration that substantially enhances both the security and efficiency of drone systems, particularly in applications deemed critical, such as military operations, surveillance tasks, and emergency response initiatives.

Our review highlights a series of key technological advancements that leverage the inherent decentralized and immutable characteristics of the blockchain, alongside the capacity of fog computing for low-latency data processing. Collectively, these technological strides contribute significantly to the requisite robustness and agility for sophisticated drone systems. However, despite these advancements, our investigation also delineates several critical areas in need of further exploration. Notably, issues related to scalability, energy consumption, and the absence of standardized protocols emerge as significant barriers to the broader adoption and optimization of these technologies in drone operations.

As drone technology continues to evolve, the imperative for adaptable and dynamic solutions that can address the forthcoming challenges in drone operations becomes ever more apparent. Future research endeavors should, therefore, aim to empirically validate the practical implications of blockchain and fog computing integration in drones through comprehensive studies and pilot projects. Such empirical inquiries are essential for substantiating the theoretical benefits posited by this integration and identifying potential limitations in real-world applications.

In summation, while the confluence of lightweight blockchain and fog computing technologies presents a promising avenue for advancing drone technology, the actualization of this potential is contingent upon a holistic approach. This approach must not only tackle the technological innovations head-on but also carefully consider the regulatory, ethical, and societal implications of such advancements.

Author Contributions: This study was conceptualized by R.A. and A.A. (Abdullah Albuali), with the main idea originating from R.A. The methodology development was a collaborative effort between R.A., A.A. (Ahmed Aljughaiman), and A.A. (Abdullah Albuali). R.A. and A.A. (Ahmed Aljughaiman) contributed to the software used in this research. The validation process was overseen by all three authors. The formal analysis and investigation were conducted by R.A and A.A. (Ahmed Aljughaiman) The resources were primarily provided by R.A. and A.A. (Ahmed Aljughaiman) The original draft of the manuscript was prepared by R.A., while the review and editing were carried out by A.A. (Ahmed Aljughaiman) and A.A. (Abdullah Albuali) provided supervision and project administration, with assistance from A.A. (Abdullah Albuali). The funding acquisition was managed by A.A. (Ahmed Aljughaiman) and A.A. (Abdullah Albuali). All authors have read and agreed to the published version of this manuscript.

Funding: This research received financial support from the Deanship of Scientific Research at King Faisal University, Saudi Arabia. The project was funded under grant number A043, provided by the Vice Presidency for Graduate Studies and Scientific Research at King Faisal University.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The authors would like to express their sincere gratitude for the insightful comments, guidance, and suggestions provided by the anonymous reviewers, which significantly enhanced the quality of this paper. Special thanks are also extended to the Vice Presidency for Graduate Studies and Scientific Research at King Faisal University for their invaluable contribution.

Conflicts of Interest: The authors declare no conflicts of interest in this article.

Abbreviations

The following abbreviations are used in this manuscript:

UAVs	Unmanned Aerial Vehicles
CA	Certificate Authority
IoT	Internet of Things
FC	fog computing
ECC	elliptic curve cryptography
SDN	Software-Defined Networking

References

1. Kim, H.; Jung, Y.W.; Zhang, H. Guest Editorial Special Issue on Time-Sensitive Networks for Unmanned Aircraft Systems. *Sensors* **2021**, *21*, 6132. [CrossRef] [PubMed]
2. Clarke, R.; Moses, L.B. The regulation of civilian drones' impacts on public safety. *Comput. Law Secur. Rev.* **2014**, *30*, 263–285. [CrossRef]
3. Kalatzis, N.; Avgeris, M.; Dechouniotis, D.; Papadakis-Vlachopapadopoulos, K.; Roussaki, I.; Papavassiliou, S. Edge Computing in IoT Ecosystems for UAV-Enabled Early Fire Detection. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Italy, 18–20 June 2018; pp. 106–114. [CrossRef]
4. Wu, D.; Ansari, N. A Cooperative Computing Strategy for Blockchain-Secured Fog Computing. *IEEE Internet Things J.* **2020**, *7*, 6603–6609. [CrossRef]
5. Finlow-Bates, K. A Lightweight Blockchain Consensus Protocol. 2016. Available online: https://www.researchgate.net/publication/339948592_A_Lightweight_Blockchain_Consensus_Protocol (accessed on 8 July 2018).
6. Khor, J.H.; Sidorov, M.; Zulqarnain, S.A.B. Scalable Lightweight Protocol for Interoperable Public Blockchain-Based Supply Chain Ownership Management. *Sensors* **2023**, *23*, 3433. [CrossRef] [PubMed]
7. Michailidis, E.T.; Vouyioukas, D. A review on software-based and hardware-based authentication mechanisms for the Internet of Drones. *Drones* **2022**, *6*, 41. [CrossRef]
8. Andola, N.; Raghav; Yadav, V.K.; Venkatesan, S.; Verma, S. SpyChain: A lightweight blockchain for authentication and anonymous authorization in IoD. *Wirel. Pers. Commun.* **2021**, *119*, 343–362. [CrossRef]
9. Ch, R.; Srivastava, G.; Gadekallu, T.R.; Maddikunta, P.K.R.; Bhattacharya, S. Security and privacy of UAV data using blockchain technology. *J. Inf. Secur. Appl.* **2020**, *55*, 102670. [CrossRef]
10. Gupta, R.; Kumari, A.; Tanwar, S. Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4176. [CrossRef]
11. Aggarwal, S.; Shojafar, M.; Kumar, N.; Conti, M. A New Secure Data Dissemination Model in Internet of Drones. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6. [CrossRef]
12. Alkadi, R.; Alnuaimi, N.; Yeun, C.Y.; Shoufan, A. Blockchain Interoperability in Unmanned Aerial Vehicles Networks: State-of-the-Art and Open Issues. *IEEE Access* **2022**, *10*, 14463–14479. [CrossRef]
13. Javed, S.; Khan, M.A.; Abdullah, A.M.; Alsirhani, A.; Alomari, A.; Noor, F.; Ullah, I. An efficient authentication scheme using blockchain as a certificate authority for the internet of drones. *Drones* **2022**, *6*, 264. [CrossRef]
14. Mershad, K. A taxonomy and review of lightweight blockchain solutions for internet of things networks. *arXiv* **2022**, arXiv:2212.06272.
15. Hou, X.; Ren, Z.; Wang, J.; Zheng, S.; Cheng, W.; Zhang, H. Distributed Fog Computing for Latency and Reliability Guaranteed Swarm of Drones. *IEEE Access* **2020**, *8*, 7117–7130. [CrossRef]
16. Ometov, A.; Molua, O.L.; Komarov, M.; Nurmi, J. A survey of security in cloud, edge, and fog computing. *Sensors* **2022**, *22*, 927. [CrossRef] [PubMed]
17. Aazam, M.; Zeadally, S.; Harras, K.A. Fog Computing Architecture, Evaluation, and Future Research Directions. *IEEE Commun. Mag.* **2018**, *56*, 46–52. [CrossRef]
18. Haouari, F.; Faraj, R.; AlJa'am, J.M. Fog Computing Potentials, Applications, and Challenges. In Proceedings of the 2018 International Conference on Computer and Applications (ICCA), Beirut, Lebanon, 25–26 August 2018; pp. 399–406. [CrossRef]
19. Ahanger, T.A.; Tariq, U.; Nusir, M. Mobility of Internet of Things and Fog Computing: Concerns and Future Directions. *Int. J. Commun. Netw. Inf. Secur.* **2018**, *10*, 534. [CrossRef]
20. Brogi, A.; Forti, S.; Guerrero, C.; Lera, I. How to place your apps in the fog: State of the art and open challenges. *Softw. Pract. Exp.* **2020**, *50*, 719–740. [CrossRef]
21. Li, X.; Zhou, L.; Sun, Y.; Ulziinyam, B. Multi-task offloading scheme for UAV-enabled fog computing networks. *Eurasip J. Wirel. Commun. Netw.* **2020**, *2020*, 230. [CrossRef]
22. Aazam, M.; Zeadally, S.; Harras, K.A. Offloading in fog computing for IoT: Review, enabling technologies, and research opportunities. *Future Gener. Comput. Syst.* **2018**, *87*, 278–289. [CrossRef]
23. Abdali, T.A.N.; Hassan, R.; Aman, A.H.M.; Nguyen, Q.N. Fog Computing Advancement: Concept, Architecture, Applications, Advantages, and Open Issues. *IEEE Access* **2021**, *9*, 75961–75980. [CrossRef]
24. Lei, K.; Du, M.; Huang, J.; Jin, T. Groupchain: Towards a Scalable Public Blockchain in Fog Computing of IoT Services Computing. *IEEE Trans. Serv. Comput.* **2020**, *13*, 252–262. [CrossRef]
25. Khan, A.A.; Shaikh, Z.A.; Laghari, A.A.; Bourouis, S.; Wagan, A.A.; Ali, G.A.A.A. Blockchain-aware distributed dynamic monitoring: A smart contract for fog-based drone management in land surface changes. *Atmosphere* **2021**, *12*, 1525. [CrossRef]
26. Alzoubi, Y.I.; Aljaafreh, A. Blockchain-Fog Computing Integration Applications: A Systematic Review. *Cybern. Inf. Technol.* **2023**, *23*, 3–37. [CrossRef]
27. Eddine, M.S.; Ferrag, M.A.; Friha, O.; Maglaras, L. EASBF: An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles. *J. Inf. Secur. Appl.* **2021**, *59*, 102802. [CrossRef]
28. Shukla, S.; Thakur, S.; Hussain, S.; Breslin, J.G.; Jameel, S.M. Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model. *Internet Things* **2021**, *15*, 100422. [CrossRef]

29. Kamruzzaman, M.; Yan, B.; Sarker, M.N.I.; Alruwaili, O.; Wu, M.; Alrashdi, I. Blockchain and fog computing in IoT-driven healthcare services for smart cities. *J. Healthc. Eng.* **2022**, *2022*. [CrossRef] [PubMed]
30. Bouachir, O.; Aloqaily, M.; Tseng, L.; Boukerche, A. Blockchain and Fog Computing for Cyberphysical Systems: The Case of Smart Industry. *Computer* **2020**, *53*, 36–45. [CrossRef]
31. Liu, Y.; Zhang, J.; Zhan, J. Privacy protection for fog computing and the internet of things data based on blockchain. *Clust. Comput.* **2021**, *24*, 1331–1345. [CrossRef]
32. Muthanna, A.; Ateya, A.A.; Khakimov, A.; Gudkova, I.; Abuarqoub, A.; Samouylov, K.; Koucheryavy, A. Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. *J. Sens. Actuator Netw.* **2019**, *8*, 15. [CrossRef]
33. Ngabo, D.; Wang, D.; Iwendi, C.; Anajemba, J.H.; Ajao, L.A.; Biamba, C. Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. *Electronics* **2021**, *10*, 2110. [CrossRef]
34. Gumaei, A.; Al-Rakhami, M.; Hassan, M.M.; Pace, P.; Alai, G.; Lin, K.; Fortino, G. Deep Learning and Blockchain with Edge Computing for 5G-Enabled Drone Identification and Flight Mode Detection. *IEEE Netw.* **2021**, *35*, 94–100. [CrossRef]
35. Kaur, K.; Garg, S.; Kaddoum, G.; Gagnon, F.; Ahmed, S.H. Blockchain-Based Lightweight Authentication Mechanism for Vehicular Fog Infrastructure. In Proceedings of the 2019 IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China, 20–24 May 2019; pp. 1–6. [CrossRef]
36. Gomes, E.; Costa, F.; De Rolt, C.; Plentz, P.; Dantas, M. A survey from real-time to near real-time applications in fog computing environments. In Proceedings of the Telecommunications, Alexandria, Egypt, 13–15 July 2021; Volume 2, pp. 489–517.
37. Badidi, E.; Mahrez, Z.; Sabir, E. Fog computing for smart cities' big data management and analytics: A review. *Future Internet* **2020**, *12*, 190. [CrossRef]
38. Jalowiczor, J.; Rozhon, J.; Voznak, M. Study of the efficiency of fog computing in an optimized lorawan cloud architecture. *Sensors* **2021**, *21*, 3159. [CrossRef] [PubMed]
39. Balen, J.; Damjanovic, D.; Maric, P.; Vdovjak, K. Optimized Edge, Fog and Cloud Computing Method for Mobile Ad-hoc Networks. In Proceedings of the 2021 International Conference on Computational Science and Computational Intelligence (CSCI), IEEE, Las Vegas, NV, USA, 15–17 December 2021; pp. 1303–1309.
40. Tariq, N.; Asim, M.; Al-Obeidat, F.; Zubair Farooqi, M.; Baker, T.; Hammoudeh, M.; Ghafir, I. The security of big data in fog-enabled IoT applications including blockchain: A survey. *Sensors* **2019**, *19*, 1788. [CrossRef] [PubMed]
41. Baniata, H.; Kertesz, A. A survey on blockchain-fog integration approaches. *IEEE Access* **2020**, *8*, 102657–102668. [CrossRef]
42. Vairagade, R.S.; Sh, B. Enabling machine learning-based side-chaining for improving QoS in blockchain-powered IoT networks. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4433. [CrossRef]
43. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE Access* **2020**, *8*, 32031–32053. [CrossRef]
44. Rivera, A.V.; Refaey, A.; Hossain, E. A blockchain framework for secure task sharing in multi-access edge computing. *IEEE Netw.* **2020**, *35*, 176–183. [CrossRef]
45. Sharma, P.K.; Chen, M.Y.; Park, J.H. A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access* **2017**, *6*, 115–124. [CrossRef]
46. Mairaj, A.; Baba, A.I.; Javaid, A.Y. Application specific drone simulators: Recent advances and challenges. *Simul. Model. Pract. Theory* **2019**, *94*, 100–117. [CrossRef]
47. Sharma, I.; Gupta, S.K. SFL-MDrone: Synchronous federated learning enabled multi drones. *J. Intell. Fuzzy Syst.* **2024**, 1–20. [CrossRef]