drones

MDPI

Review

Beyond Flight: Enhancing the Internet of Drones with Blockchain Technologies

Kyriaki A. Tychola [1], Konstantinos Voulgaridis [2] and Thomas Lagkas [2,*]

[1] MLV Research Group, Department of Computer Science, Democritus University of Thrace, 65404 Kavala, Greece
[2] Department of Computer Science, Democritus University of Thrace, 65404 Kavala, Greece
* Correspondence: tlagkas@cs.duth.gr

Abstract: The Internet of Drones (IoD) is a decentralized network linking drones' access to controlled airspace, providing high adaptability to complex scenarios and services to various drone applications, such as package delivery, traffic surveillance, and rescue, including navigation services. Unmanned Aerial Vehicles (UAVs), combined with IoD principles, offer numerous strengths, e.g., high mobility, wireless coverage areas, and the ability to reach inaccessible locations, including significant improvements such as reliability, connectivity, throughput, and decreased delay. Additionally, emerging blockchain solutions integrated within the concept of the IoD enable effective outcomes that surpass traditional security approaches, while enabling decentralized features for smart human-centered applications. Nevertheless, the combination of the IoD and blockchain faces many challenges with emerging open issues that require further investigation. In this work, we thoroughly survey the technological concept of the IoD and fundamental aspects of blockchain, while investigating its contribution to current IoD practices, the impact of novel enabling technologies, and their active role in the combination of the corresponding synergy. Moreover, we promote the combination of the two technologies by researching their collaborative functionality through different use cases and application fields that implement decentralized IoD solutions and highlighting their indicative benefits, while discussing important challenges and future directions on open issues.

Keywords: Artificial Intelligence; blockchain; Internet of Drones; Internet of Things; open issues; security; Unmanned Aerial Vehicles; use cases

check for updates

Citation: Tychola, K.A.; Voulgaridis, K.; Lagkas, T. Beyond Flight: Enhancing the Internet of Drones with Blockchain Technologies. *Drones* **2024**, *8*, 219. https://doi.org/10.3390/drones8060219

Received: 19 April 2024
Revised: 20 May 2024
Accepted: 24 May 2024
Published: 26 May 2024

1. Introduction

Unmanned Aerial Vehicles (UAVs), also known as drones, are pilot-free aircrafts controlled by a remote user or control station. Until recently, drones were operated individually. However, recent technological accomplishments allow a high number of drones to interconnect and accomplish complex missions coordinately [1], aiming for the efficient management of their airspace [2]. Such approaches have led to the rise of the Internet of Drones (IoD) ecosystem [3], leveraging a wide range of applications and deploying various tasks, such as agricultural monitoring, faster package delivery with reduced operational costs [4], drone swarm surveillance with autonomous operations, service relaying (e.g., Internet services to remote locations), and so on [5], due to the increased flexibility, mobility, scalability, and autonomy [6]. The IoD is considered to be a part of the Internet of Things (IoT), equipped with interconnected physical devices and Internet-connected sensors [7,8]. Substantially, the drone network obtains a new perspective, providing more features, while at the same time key IoT properties are maintained [9]. However, it also inherits the security weaknesses of IoT networks [10]. As a typical network architecture, it enables communications between UAVs and devices on the ground [11] in a coordinated manner [12], allowing drones to have flight control and providing navigation services [13] such as the internal transmission and exchange of data, with integrated mobility, portability, and automation [14].

In addition, with drones interacting across a public wireless channel [15], the IoD is integrated with different systems, such as Wireless Sensor Networks (WSNs), i.e., systems spatially separated from UAVs allowing them to function efficiently in an expanding controlled zone, considering connection performance [16], due to congestion prevention, which results in reducing packet loss while ensuring equal bandwidth allocation [12]. Some significant characteristics of the IoD, such as (a) Device to Device (D2D) support and Device to Multi-device (D2M) communications, (b) facilitating connectivity to the contextual networks, and (c) its ability to operate as a data gathering and information management service [9], combined with its small size, high reconfigurability, functionality, and real-time accountability, have led to its adoption by more and more organizations [7]. Nevertheless, the IoD is vulnerable to various risks at different levels, such as radio signals for the communication between drones and users being interrupted, hacking, requested and transmitted data including Global Positioning System (GPS) signals, and vulnerabilities in the drone software to malicious injections [12].

On the other hand, blockchain allows transparent data sharing within a decentralized network, with an immutable ledger facilitating the process of recording transactions and tracking assets [17], as well as providing trust, security, and reliability of data processing [18]. The dominant advantages and capabilities of blockchain were soon recognized and leveraged, with relative solutions being applied in different fields, among them UAVs to tackle emerging problems. Today, the integration of blockchain (public or private) within the IoD ecosystem has gained growing attention, providing many benefits in relation to the enhancement of IoD networks, and mitigating security and safety risks, as well as improving reliability. Consequently, it has been proven that the utilization of a certain amount of fragmented blockchains [19] is highly effective in a multitude of security applications due to its vital features, i.e., decentralization, immutability, transparency, traceability, and auditability [20], as well as cryptographic capabilities. Specifically, blockchain provides extensive solutions to satisfy demanding IoD security requirements, such as authentication, privacy, confidentiality, and integrity, through smart contracts (SCs) and access control [4].

Nevertheless, since the IoD and blockchain are considered to be types of embedded networks, utilizing communication links and smart devices that handle various sensitive information that is collected, transmitted, and exchanged, they are also being undermined by threats and vulnerabilities. Such data leaks lead to trust and privacy issues [21,22], while security breaches between networks and communication links lead to extensive losses of resources, trust, and availability [23,24].

With the constant evolution of the IoD and blockchain approaches, additional emerging digital technologies are being incorporated in the respective synergy as impactful enablers [25], such as (a) Artificial Intelligence (AI) [26]; (b) Cloud Computing (CC) [27]; (c) Edge Computing (EC), including Edge AI for smarter computational systems as well as intellectual tasks of robotic machinery [28]; (d) IoT [29]; and (e) communication technologies, such as 5G/6G for smarter communication, fast and accurate processing of big data, transmission, and handling [30,31].

As the benefits of the corresponding synergy are increasing, improved adjustability has been noted in various use cases. The combinative concept is adaptable to a wide range of industrial and application fields, such as healthcare, finance, government, agriculture, media, and natural disasters, fulfilling their objectives and at the same time ensuring requirements such as security, scalability, and efficiency [32].

To this end, the aim of this study is to provide an exhaustive review and present the current status and role of blockchain for the effective enhancement of the IoD. This work covers a wide range of aspects, summarized in the following distinct points: (1) The referenced frameworks of the IoD and blockchain, (2) a holistic review of IoD- and blockchain-related works, (3) a conceptual architecture model and IoD component requirements, (4) security and privacy issues, (5) the role and contribution of blockchain as an addition to IoD systems, (6) the synergy of the IoD and blockchain with indicative enabling technologies, (7) referenced use cases of IoD and blockchain solutions, (8) the presentation of emerging IoD challenges, (9) proposed potential solutions to face the corresponding challenges, and (10) open issues and future research directions.

The organization of this survey is as follows: Section 1 provides a brief introduction to the IoD and blockchain ecosystems as well as requirements regarding their integration, while highlighting the role of other technologies as conceivable solutions. Section 2 provides the motivation and the contributions of this work. Section 3 presents the research strategy followed. Section 4 provides an overview of the IoD ecosystem, including components, requirements, and a conceptual architecture model, as well as security concerns. Section 5 discusses the concept of blockchain, with an emphasis on its role as an extension of the IoD. Section 6 focuses on the technologies that enable the combination of the IoD and blockchain, such as AI, communication technologies (e.g., 5G/6G), the IoT, and Cloud/Edge Computing. Section 7 investigates indicative use cases—such as supply chains, healthcare, natural disasters, agriculture, charging/refueling, and media—that implement the corresponding synergy. Section 8 includes a thorough discussion based on the research findings, summarizing various challenges at different levels, proposing solutions, and providing open issues and future research directions. Finally, Section 9 presents the conclusions of our research. Figure 1 depicts a visual representation of this paper's structure and related contents.

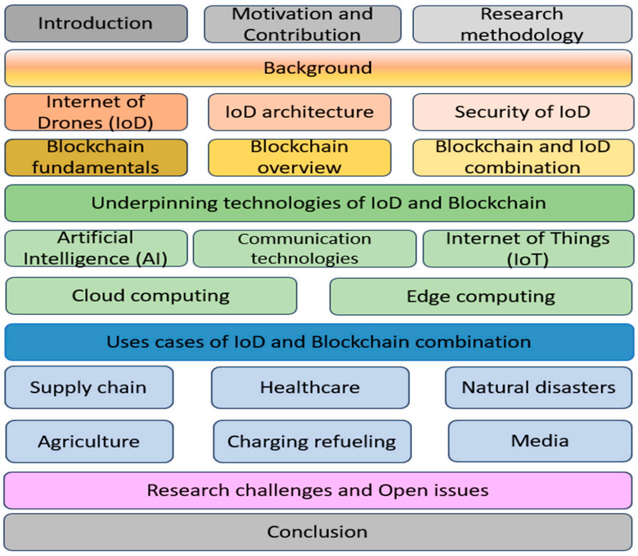


Figure 1. Contents and structure of this paper.

2. Motivation and Contribution

Recently, the leverage of interconnecting drones within the concept of the IoD has revolutionized the proposition of significant infrastructure, aiming towards the control and access of drones over the Internet. However, these systems are vulnerable to infiltration issues, including privacy and security concerns. Nevertheless, the integration of blockchain technology within IoD networks has gained growing attention, providing many benefits related to the security enhancement of IoD networks.

Several review articles can be found in the recent literature. However, most of the surveys are restricted to the individual research of IoD and blockchain technologies, mainly focusing on security issues, with minimal availability on their potential combination. In [33,34], the authors discuss security concerns and challenges of IoD domains while emphasizing authentication issues. In [35], the authors discuss cybersecurity weaknesses and intrusions of the IoD, and they elucidate potential countermeasures. In [36], the authors investigate the role of blockchain in UAV networks in various fields, including the security of systems, attacks on the IoD, and preventive countermeasures, while in [37] the authors discuss the integration of blockchain as a solution to tackle IoD network security issues. In [14], the authors analyze architectures and applications of the IoD, including networking and decentralization, as well as security and privacy issues. In [38], IoD privacy and security challenges derived from drone operations are described, including the impact on an IoD network, particularly on large-scale networks. In [4], the authors provide a systematic literature review, gathering material related to the IoD and blockchain technologies, including security issues of the corresponding technologies. In [39], the researchers focus on the combination of the IoD and blockchain for certain application fields, including a relative communication network. The paper presented in [40] discusses blockchain and robotics technologies, focusing on security concerns. Similarly, Ref. [17] provides an exhausting overview of blockchain technology, including its architecture, components, characteristics, and operational principles, while in [41] the IoD and blockchain technologies are thoroughly described, including applications and security issues. Moreover, Refs. [42,43] describe enabling technologies of IoD, while mentioning blockchain as well. In [44], the authors propose the combination of 5G networks and blockchain by examining security issues, while in [45] the authors discuss AI and blockchain as underpinning technologies, including use cases of the IoD and blockchain. In [46], the authors research blockchain in combination with Edge Computing, emphasizing security issues and indicative solutions, while in [47] the authors focus on security vulnerabilities in drone applications and discuss blockchain as an emerging technology for security solutions for drones.

Table 1 includes the basic features of the aforementioned related works regarding IoD and blockchain technologies, aiming to comparatively highlight the contribution of the present review work in relation to previous ones.

Undoubtedly, the available literature offers significant contributions to the research and academic communities. The majority of studies describe the IoD technology focusing on drone characteristics and requirements, while others discuss security and privacy issues related to networks, including proposed solutions utilizing different technologies, such as blockchain. The corresponding review of the existing literature reveals a significant gap in research focusing on the underpinning technologies, use cases, and challenges associated with the integration of blockchain and IoD systems, with the authors across the previous articles not extensively discussing the role, contribution, and integration of the specific combination. The lack of focus on the underpinning technologies, uses cases, and challenges of combining blockchain with IoD appears to be a common theme in these works. This lack of emphasis on these critical aspects hinders the development and understanding of how blockchain can enhance the functionality and security of IoD systems.

Understanding how blockchain protocols can be adapted and optimized for use in a network of interconnected devices is crucial for ensuring data integrity, privacy, and security. Additionally, identifying the specific challenges and constraints that may arise from implementing blockchain in IoD environments is essential for developing effective solutions and strategies. Moreover, the literature indicates a significant gap in the exploration of use cases for blockchain in the context of the IoD. While some studies briefly mention potential applications or scenarios where blockchain could add value to IoD systems, a more in-depth analysis of real-world examples and industry-specific implementations is needed to demonstrate the practical benefits of this integration.

Furthermore, the lack of focus on challenges and opportunities associated with integrating blockchain with the IoD is a notable gap in the existing research. Issues such as scalability, interoperability, data management, and regulatory compliance are critical considerations that must be addressed to ensure the successful implementation of blockchain technology in IoD environments. Nevertheless, none of them provides a unified approach to presenting and analyzing in detail the significance of blockchain technology within an IoD environment. The lack of complete research acted as a solid motivation to carry out a thorough investigation regarding the contribution of blockchain for impactful IoD enhancement, holistically identifying its related research gaps. Hence, the contribution and innovation of our work lie in a detailed analysis of the role of blockchain, correlated with the field of IoD, including architectures and requirements; underlining attacks; analyzing security and privacy issues, underpinning technologies, and combinative use cases; highlighting challenges and constraints; and responding to the key research questions.

Table 1. Comparative table of the characteristics of the present work versus related available literature.

Characteristics	**Blockchain Integration within the Internet of Drones (IoD)**																		
	[33]	[34]	[35]	[36]	[37]	[14]	[38]	[4]	[39]	[40]	[17]	[41]	[42]	[43]	[44]	[45]	[46]	[47]	**Ours**
IoD	✓	✓	✓	✓	✓	✓	✓	✓	✓[1]	×[2]	×	✓	✓	✓	✓	×	✓	✓	✓
Blockchain	×	×	×	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IoD–blockchain integration	×	×	×	✓	×	×	×	✓	✓	×	×	✓	✓	✓	×	×	×	×	✓
Contribution of blockchain	×	×	×	×	✓	✓	×	×	×	×	×	×	×	✓	✓	×	×	✓	✓
Security issues	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	×	✓	✓	✓		×	×	✓	✓
Underpinnings technologies	×	×	×	×	✓	×	×	×	×	✓	×	×	✓	✓	✓	✓	✓	✓	✓
Uses cases of IoD and blockchain	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓
Challenges	✓	✓	×	✓	✓	✓	✓	×	×	×	×	✓	✓	✓	×	✓	✓	×	✓

[1] ✓included characteristics; [2] × missing characteristics

3. Research Methodology

Within the context of this work, a systematic literature review was carried out by using the Kitchenham approach [48] to identify the status of implementing decentralized solutions within IoD systems, based on the following research questions:

RQ1: Why is blockchain used in the IoD?

RQ2: What are the strengths and weaknesses of using blockchain in the IoD?

RQ3: Which underpinning technologies are integrated within the IoD and blockchain ecosystems?

RQ4: In which cases can the IoD and blockchain be applied together?

RQ5: What are the strengths and weaknesses of combining blockchain and the IoD?

RQ6: What are the challenges and open issues related to the integration of blockchain and the IoD?

In order to have an initial perception of the corresponding research topic, we performed a search of peer-reviewed journal publications in the Scopus database using the query "(TITLE-ABS-KEY (internet AND of AND drones) AND TITLE-ABS-KEY (blockchain)) AND (LIMIT-TO (DOCTYPE, "ar") OR LIMIT-TO (DOCTYPE, "cp") OR LIMIT-TO (DOCTYPE, "ch")) AND (LIMIT-TO (LANGUAGE, "English")) AND (EXCLUDE (PUBYEAR, 2024))". The process returned 201 documents. Figure 2 summarizes the number and the proportion of the total number of published works on the subject in the range from 2017 to 2024, in a full period of 5 years. Although the combination of IoD and blockchain technologies has been researched only in the last five years, the ever-increasing number of publications, arithmetically and proportionally, shows an overall upward trend, indicating the significance of this research topic. Figure 3 illustrates high-frequency keywords used, in terms of the IoD and blockchain within the related literature, based on their occurrence, and with the font size indicating the respective frequency. As can be observed, the majority of the available scientific material focuses on blockchain and UAVs. In addition, network security, IoT, and 5G communication systems, as well as authentication, are the most used for various application fields and investigated issues.

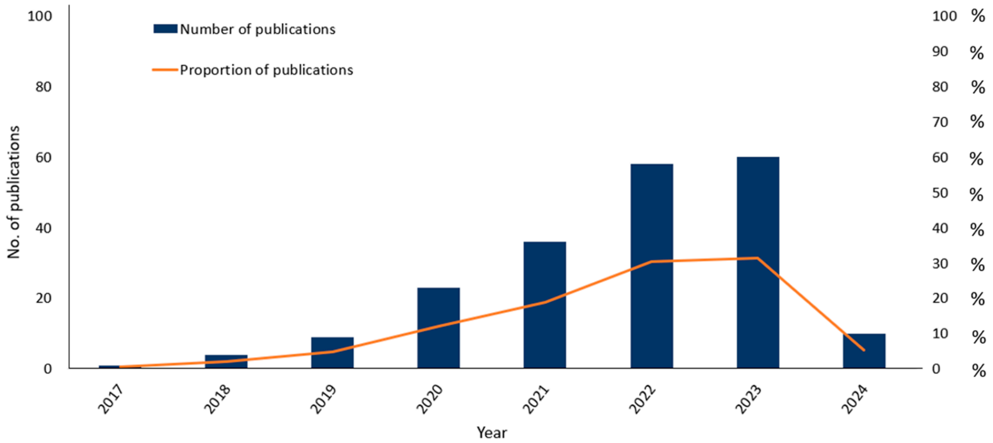


Figure 2. Number of relevant publications per year on the subject of the IoD and blockchain (statistics April 2024).

Based on the literature, since the integration of blockchain within the IoD has not been investigated in depth, we proceeded to a more extensive research analysis of the relation between these emerging technologies. According to Figure 4, concerning the main context of the reports, papers focused on blockchain and the IoD are directly related and, as the core of this subject, occupy a lot of space on the grid, with greater density, and tend to be in the motor theme space. However, different technologies, such as AI and augmented reality (AR), also take place in the corresponding fields as basic themes, while 5G communication technologies are a potential factor for the operating systems of interest. In addition, security issues are illustrated to a lesser extent, combined with related file systems. Furthermore, many use cases, such as agriculture, robotics, and supply chains, also play a significant role. However, learning systems and related topics were identified as a common space between emerging and niche themes, and between emerging and basic ones, respectively, due to their close relation to the IoT. Nevertheless, the IoD is considered to be a byproduct of the IoT, resulting in the inclusion of a variety of applications.

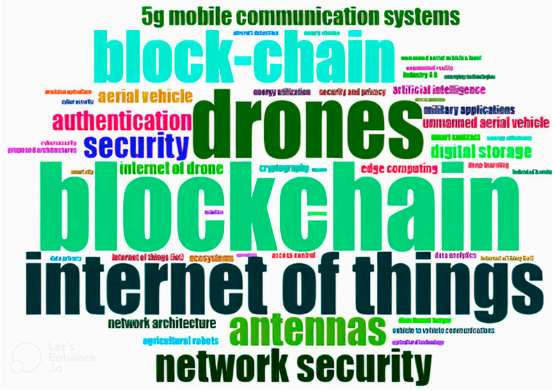


Figure 3. Cloud map of high-frequency terms used in IoD and blockchain works.

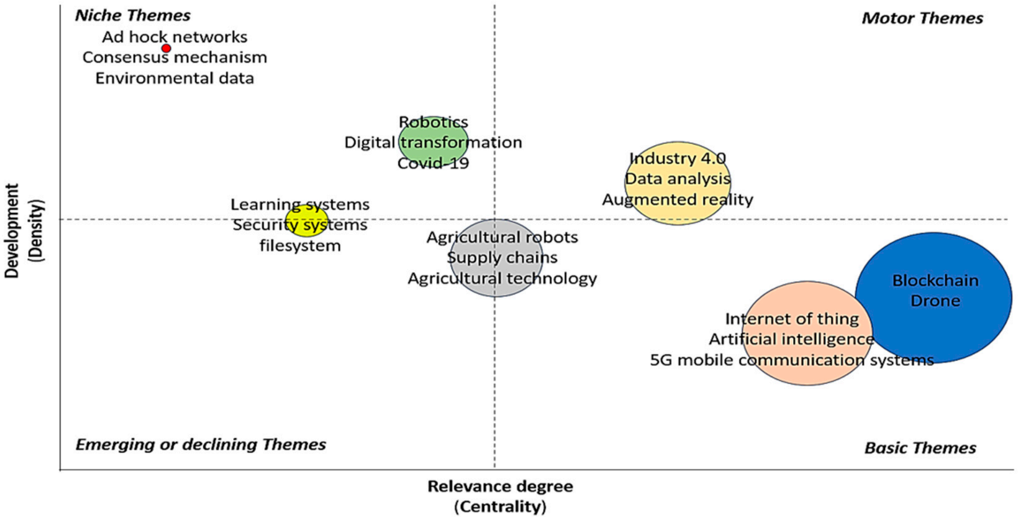


Figure 4. Diagram of centrality and density relations per topic field.

The terms blockchain and drones are utilized at the same frequency and have a notable impact. In more detail, blockchain appears as “block-chain” in 43.8% of the publications and as “blockchain” in 55.6% of them, while the term “drones” appears in 44.1% of the publications. It is evident that these percentages are comparable; hence, there is a clear potential for interconnection and formation as a main research topic. In addition, blockchain and drones, combined with IoT features, exhibit similar appearance percentages of 50% and 52.4%, respectively. However, IoT appears at a higher percentage of 74.3%, due to the inclusion of decentralized principles and UAVs for different types of applications. On the other hand, aerial vehicle–blockchain–convolution also has a partial centrality, but with a different impact in contrast to the previous case. Particularly, convolution with a percentage of 100% denotes that state-of-the-art technologies such as Machine Learning (ML) are implemented in blockchain and IoD solutions. Also, the low percentages of aerial vehicles (41.7%) and blockchain (11.1%) are related to the low utilization frequency of these specific writings. Figure 5 depicts the impact and centrality of the relative affinity percentage of each topic.

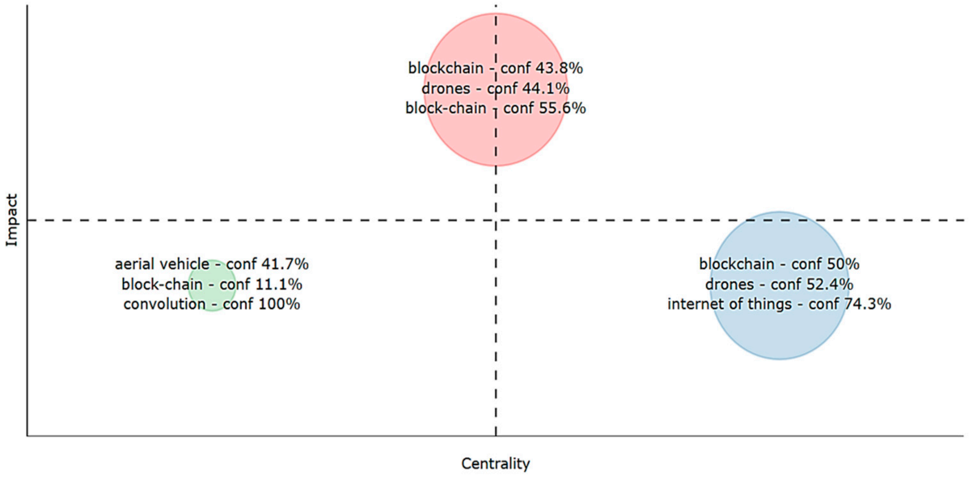


Figure 5. Diagram of clustering by coupling according to the context of the paper.

4. The Internet of Drones (IoD)

The IoD is considered to be a state-of-the-art subfield of the IoT, supporting the coordination and interconnection of drones within a common network [9].

4.1. Background of the Internet of Drones (IoD)

The IoD is a layered network providing controlled and coordinated access to drones, while simultaneously offering important benefits such as scalability, codebase maintenance, and layer modification flexibility, with minimal changes to other interconnected layers [2]. An indicative IoD network consists of three layers with dedicated functionalities: (a) an air traffic control network layer, (b) a cellular network layer, and (c) the Internet [49].

A traditional IoD architecture is divided into certain components for the proper and efficient operational performance of UAVs, through controlling and administering to ensure that the collected data reach the correct destination from the source nodes [2,50] and the utilized communication protocols [51]. Some referenced protocols that support data transmission between nodes are MAVLink and ROSLink [52]. Practically, decision-making tasks are conducted by nodes to establish their required behavior within the network [53] and accelerate the routing between reference and target nodes [54]. The process of data collection, data transmission, stability, and communication methodologies depend on the architectural components with novel methodologies researched and analyzed in [55–57], while further elements in the IoD environment are part of the middleware layer, separated into service-based and cloud-based counterparts, ensuring the abstraction between the various interfaces of the IoD, such as programming languages, operating systems, networks, and architectures [58]. Service-based middleware provides network access, local message delivery, caching, and name resolution to the IoD architecture, while ensuring robust connectivity and collaboration for the entire IoD architecture due to its integration capabilities in other network layers [59]. Cloud-based middleware delivers a response to the requested service rapidly and supports various application operations, such as Robot Operating System (ROS), for their integration within the network architecture [2], while providing reliable communication between the ground network and UAVs [60]. Since multiple drones are interconnected to perform various operations simultaneously, data fusion and sharing is an important element of the IoD infrastructure, allowing the processing and merging of various data sources to further generate and revise data for decision-making tasks. Moreover, IoD data can be classified into distributed (meta-architecture), centralized, and cloud-based data. To begin with, distributed data support their transition into a form of local interaction, leading to their scalability, fault tolerance, interoperability, ease of redesign and reconfiguration, and security against unscheduled drone disconnections [61]. Next, centralized data are defined for their smooth operational flow and share all of the required information through the fusion center, with the support of other interconnected devices of the network leading to more accurate task-related information [62]. Cloud-based data are controlled by cloud interfaces consisting of various services, including safety analytics, collision prevention, and operations concerning risk-aware navigation [63]. Finally, network security issues, such as authentication, privacy, availability, and intrusion detection, as well as considerations for secure data transmission, are the most important factors that should be implemented in the design of IoD architectures and the development of their corresponding applications [36]. Figure 6 depicts an overview of the corresponding elements and features of a traditional IoD infrastructure.

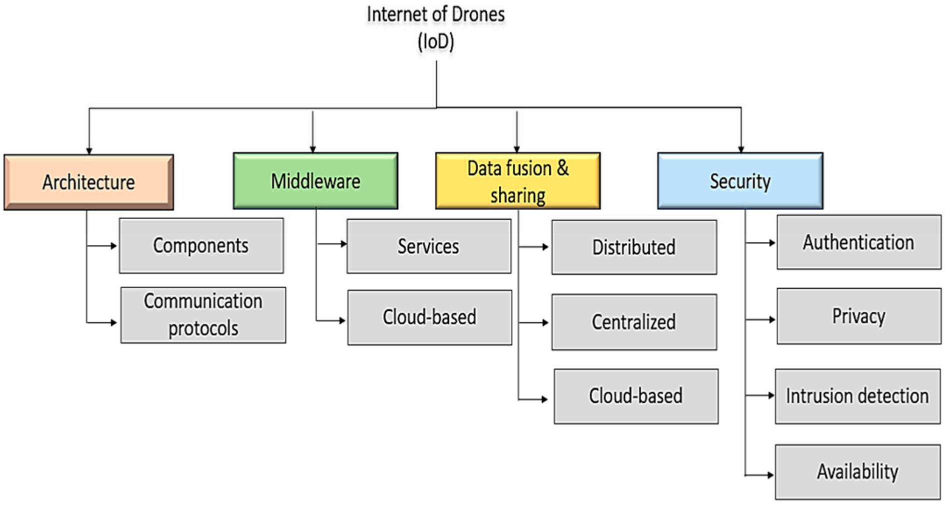


Figure 6. Basic elements and functions of the IoD.

The main requirements of the IoD can be categorized into communication and security requirements, due to drones being the main functional component of the corresponding technology. Figure 7 depicts the respective key IoD requirements.

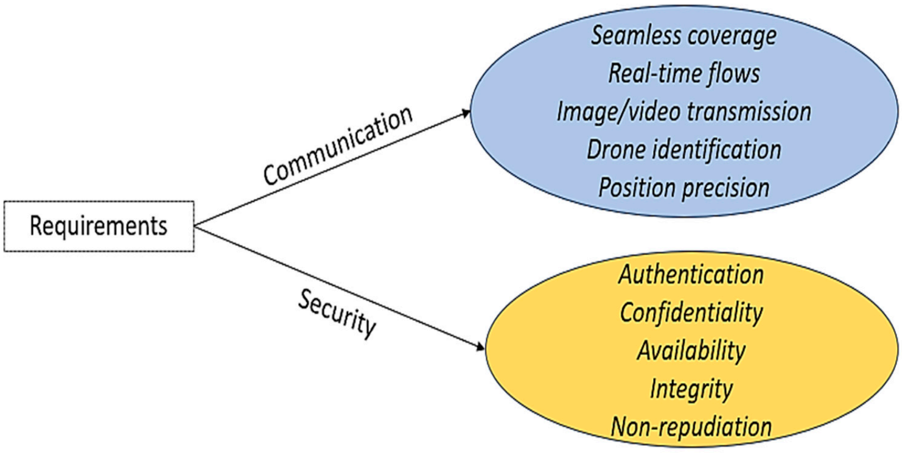


Figure 7. Key requirements of the IoD.

Seamless coverage supports the operations of drones at different altitudes in contrast to networks. For instance, coverage of up to 10 m altitude is appropriate for plant protection, up to 50 to 100 m for power line inspection, and up to 200 to 300 m is sufficient for mapping of agricultural land [64]. Real-time and remote controllers are used for the monitoring of flight conditions, drone tasks, and equipment, as well as emergency control, depending on conditional latency and data rate requirements. Transmission of high-definition images and videos provides a high uplink data rate from the drone to the station, depending on their size and quality, respectively. Also, 5G networks support services such as multi-data rates of 10 Gbps, low-latency operations, increasing wireless communication ranges [65], and additional features as part of the drones' application, including augmented and virtual reality [66]. Mobile networks identify and control drones through the support of (a) registration of flight control serial numbers and legality; (b) detection and monitoring of drone connections and data communications, whereas in real-time tracking additional regulatory protocols are established; and (c) time-sensitive evaluation and warning of flights for risk prevention related to flight paths, traffic, and coordination [13]. Finally, precise vertical or horizontal positioning is significant; however, it is contingent upon application [66].

At the same time, privacy and security issues emerge from the network itself, such as localization errors [67]. Consequently, additional emphasis is required on the authentication of devices, nodes, and users in order to prevent unauthorized access to sensitive information [68], including mutual authentication between a drone and a Ground Control Station (GCS). Such countermeasures are achieved through the utilization of security keys, ensuring absolute secrecy and confidentiality in the protection of wireless communication channels from unauthorized disclosure of information [69], data availability, access control [13], integrity of collected data [68], and non-repudiation aiming to reveal concealed actions [70,71].

4.2. Fundamental IoD Architecture

The IoD, as a network architecture, controls airspace by deploying interconnected UAVs and by establishing their constant coordination, which is achieved through the establishment of a Ground Station (GS) and the deployed drones [2]. An essential task of the UAVs is acquiring and storing data and information from a specific Fly Zone (FZ), which are then transmitted to the assigned GS via wireless communication modules [72,73] based on IoT technologies [26,74,75]. Specifically, the airspace is divided into multiple specific FZs and drone groups, aiming toward the monitoring process of a particular environment for the effective collection of data, which are transmitted to the management server of the GCS. The MS has additional responsibilities, such as the storage of private information pertaining to the user, drone, and air space. In the Control Room (CR), a user monitors the predetermined IoD environment, with all of the network participants being registered prior to the drone deployment in the scheduled FZ [69]. After registration, drones collect data in real-time from their corresponding zone and transmit them to the MS, while being able to share the collected data with their neighbors. Moreover, the CR can assign instructions to drones via the MS to perform any required task. The wireless connectivity is achieved by 5G cellular networks in a specific FZ, in contrast to the connectivity between the GS and wireless access points, which is wired [76]. Figure 8 depicts a conceptual IoD network model, with an overview of the communications and responsibilities of various parties in the IoD environment.

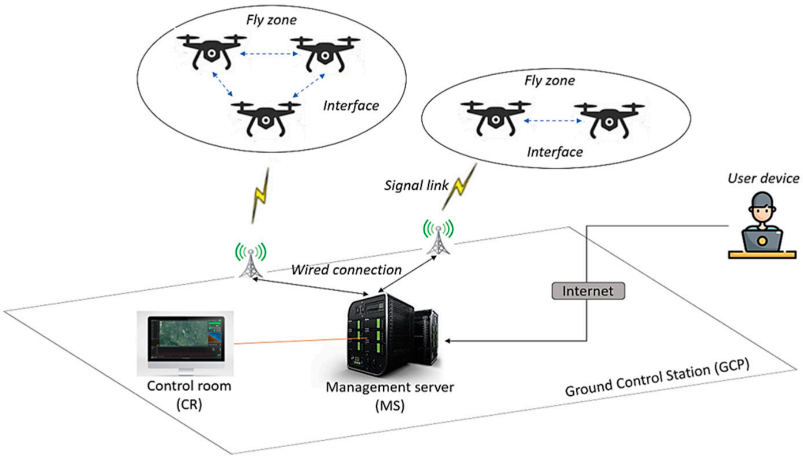


Figure 8. Internet of Drones (IoD) network conceptual model.

4.3. Security in the IoD

With the drone industry developing, the number of UAV-based applications is increasing. Consequently, different risks and vulnerabilities are also increasing. An IoD framework is susceptible to many security and safety issues, which can significantly affect the accomplishment of the predetermined task, the data (acquisition, communication, storage), and the network [39] while taking into consideration transmissions involving sensitive and critical information, as the IoD infrastructure becomes a target for many hostile cyber-attacks [77].

These attacks can be ranked as follows: (a) device attacks, aiming to mimic confidential credentials to access the drones' components; (b) network attacks, where data streams are tampered with and altered; and (c) software attacks, where drones or Ground Stations are injected with malicious data [78]. Thus, the preservation of confidentiality, integrity, availability, authenticity, and privacy are key requirements of the IoD, to properly reflect its capabilities and functions in tackling threats and security breaches [35], i.e., (a) confidentiality of wireless communication channels prevents data leaks, (b) integrity ensures that the collected data remain unchanged, (c) availability of services to authorized users remains even in the case of infiltration, and (d) authentication verifies identities before access or exchange of data, while privacy prevents malicious approaches from disclosing personal data without permission. As a result, data leaks raise serious privacy concerns and threaten location- and identity-related information [13], leading to trust issues among the related stakeholders [22].

Moreover, IoD networks are vulnerable to physical threats, with a great impact on their safety and, as a result, the drones' requirements for accomplishing their predefined objectives [39]. Significant examples of physical threats are theft and vandalism [79], harsh weather conditions (depending on the size of the operating drone), collision among drones due to the nature of IoD applications and the collaborative manner of drone fleets, and possible sensory malfunctions [80].

4.3.1. Localization Error-Based Attacks

One of the main categories of attacks on IoD systems is localization error-based attacks [81]. Specifically, lack of localization for cyber–physical systems, such as the IoD, leads to significant errors that emerge from hindering the estimation of drones' secure location [82]. Figure 9 shows the taxonomy of IoD attacks based on the corresponding category.

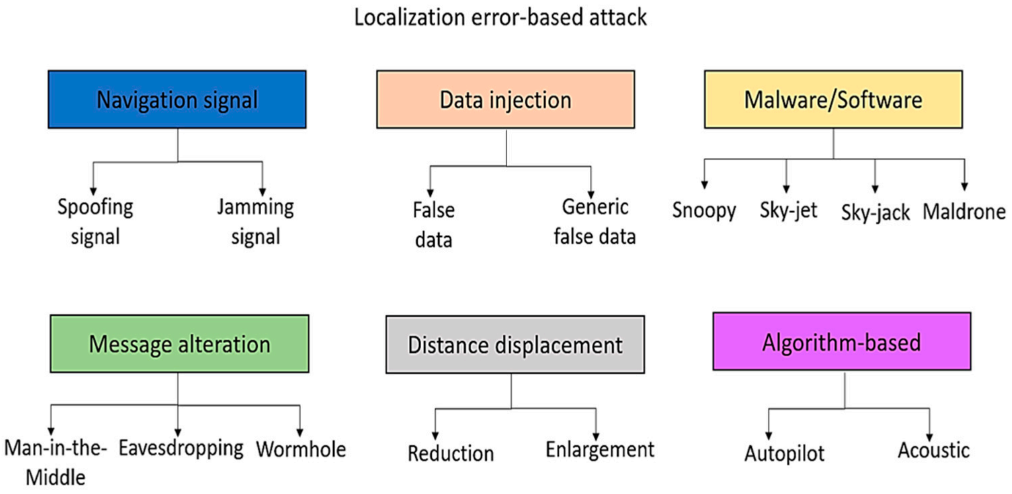


Figure 9. Localization error-based attacks.

According to the scheme, navigational signals are used to estimate precise locations within an IoD network, including the Global Positioning System (GPS), Global Navigation Satellite Systems (GNSSs), and Ground Control Signals (GCSs). GPS spoofing attacks aim to modify the content of the received GPS signals through the generation of spoof

GPS signals with specialized generators. As a result, a significant signal delay is created, causing coordination imbalances and possible midair collisions [83]. Next, channel jamming disrupts communications [84] through the utilization of GNSS signals received by drones, in order to provide incorrect directions, while in the case of GCSs third parties transmit false GC signals for the direction of drones to specific places. Disruptions based on jamming signals cause the collision of UAVs or unavailability of services [85], facilitating efforts of hijacking or physical damage to the drone. In the cases of both GNSS and GCS jamming attacks, all of the signals are interrupted and all of the GCS are obstructed.

Another type of localization error attack is the traditional data injection, resulting in modified instructions for changing the drones' programmed route [86]. A selective forwarding attack, also known as a wormhole attack [87], is a network layer attack on the IoD, where a malicious node selectively drops or alters packets passing through it, disrupting the normal functioning of the network, with the potential of causing malfunctions in drone communications and data interactions [88]. Malware attacks, such as Snoopy software, are installed by third parties for the collection of data related to the utilized Wi-Fi within the IoD system, resulting in navigation control of the drone. Similarly, skyjet attacks are related to the installation of hijacking software for the deactivation of the default and preprogrammed navigation controls [89], while in skyjack attacks the perpetrators attempt to detect and infiltrate utilized wireless networks [90]. The last type of malware attack is Maldrone, disrupting the communication between the drone's flight controls and implemented sensory devices [91]. Tampering attacks on the IoD involve an attacker physically or digitally altering the drone's hardware or software, leading to potential unauthorized control, data theft, or even drone damage [34].

Moving on to message alteration, transmitted data and messages for the efficient control of drones are disrupted through these approaches, such as the case of man-in-the-middle attacks on navigational data, where the communicated data streams between the drone and its corresponding navigational control system are accessed without authorization [53]. Also, eavesdropping is where the communicated navigational messages between the drone of interest and its controller are intercepted through unsecured communication channels [92]. In wormhole attacks, data regarding navigation and controls are recorded, adapted, and retransmitted to the drone's main control system.

Other attacks are related to distance displacement, altering the data on position estimation of the IoD components. In this case, the falsification of data on distance calculation in terms of size or content can vary compared to the real signal [93].

Algorithm-based attacks are the last type of localization error-based infiltrations, defined by infused algorithms that cause impactful misleading of auto-pilot functionalities [94] and distort the acoustic position control algorithm through alteration of the drone's resonant gyroscope frequency [95]. In addition, a collision attack in the context of the IoD can refer to two different scenarios: Starting with physical collision, it refers to the physical impact between two or more drones. This can be mitigated by implementing advanced collision avoidance systems that use real-time sensor data to detect and avoid obstacles. Techniques such as geo-fencing, where drones are programmed to stay within a specific geographical boundary, can also be used. Additionally, drones can be equipped with fail-safe mechanisms that guide them to a safe landing spot in case of a system failure. Meanwhile, data collision refers to the scenario where two or more drones try to transmit data simultaneously over the same frequency, causing the data packets to collide and resulting in loss of data [96]. An impersonation attack in the context of the IoD involves an attacker pretending to be a legitimate drone or control station in order to gain unauthorized access or control [76]. Also, a side-channel attack involves an attacker gaining information from the physical implementation of a system, rather than exploiting software vulnerabilities or cryptographic weaknesses. This can include information leaked through power consumption, electromagnetic emissions, and timing information [97].

4.3.2. Attacks Based on Security and Privacy Requirements

This category of IoD attacks is based on the security and privacy requirements of the corresponding concept, targeting important principles, namely, integrity, availability, authenticity, confidentiality, and privacy, as also shown in Figure 10.

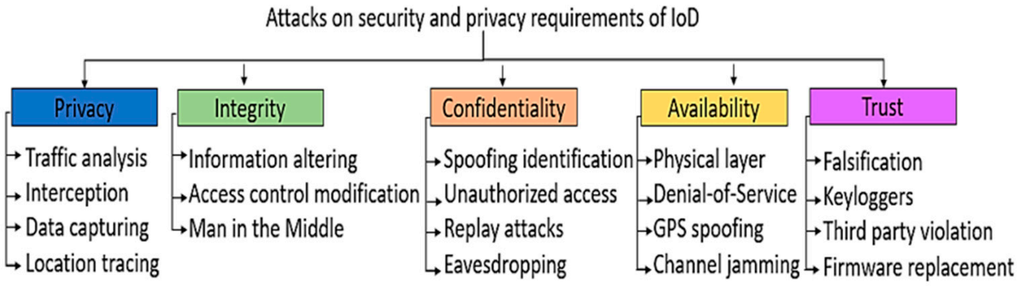


Figure 10. Taxonomy of attacks based on requirements of the IoD.

Starting with privacy, data that are collected and processed through IoD mechanisms can be stolen or disrupted by adversaries [98] with strategies such as traffic analysis, by obtaining information on IoD devices and networks, including location, connected sensory devices, and their captured data that are distributed between the IoD network and GCS, resulting in the interception of network traffic.

Another category of attacks is related to the integrity i.e., the accuracy, trust, and consistency of data [99]. IoD integrity is affected by inserting false data in the communications system, through modification, fabrication, substitutions, and data injections intending to mislead drone users, or utilizing tactics [100].

Confidentiality is affected by unauthorized access of non-legitimate users to the components of the IoD network for the retrieval of targeted information [22]. Indicative examples are spoofing identification, with the attacker pretending to be a legitimate user by spoofing ID credentials; unauthorized access to the IoD server and services using hacked accounts or ID duplication; replay attacks through bypassing and replaying of the established security mechanisms and requests; and eavesdropping for real-time interception of IoD communications, aiming at the retrieval of confidential information [21].

Attacks related to the availability of the IoD aim to cause physical damage to the structure of the drone or its hardware components, e.g., through network interruption (Denial-of-Service, DoS), including flooding, where the attacker overwhelms the drone's network by sending a large amount of unnecessary and unwanted traffic. This can cause the drone's network to become overloaded, leading to a slowdown in performance or even a complete shutdown [101] and normal traffic server disruption (Distributed Denial-of-Service, DDoS), through GPS spoofing and channel jamming, preventing legitimate users from accessing services and essential resources [102].

In terms of trust, several risks may emerge during the development and deployment phases, due to misconfiguration and limited incorporation of security mechanisms [103], through firmware replacements during upgrading processes, or through falsified IoD mechanisms resulting in data leaks [9]. Other strategies worth mentioning are keyloggers, utilized for private data to be forwarded directly to attackers, or regulatory violations by trusted third parties leading to financial and intellectual property losses.

Protecting IoD systems from cyber threats is crucial in ensuring the safety, security, and reliability of drone operations. To defend against potential attacks, robust security measures need to be implemented, including encryption, regular software updates, strong authentication, and continuous monitoring. These measures are essential in safeguarding drone systems from unauthorized access, data interception, DoS attacks, malware injection, GPS spoofing, physical attacks, and signal jamming [9].

Encryption plays a crucial role in safeguarding communication channels between drones and Ground Control Stations while ensuring the confidentiality and integrity of exchanged data. It ensures that the data are scrambled through the utilization of algorithms and can only be decrypted by authorized parties with the necessary keys. This prevents hackers from eavesdropping on the communications and gaining access to sensitive information [104]. Regular security updates and patches are also essential in addressing vulnerabilities in communication. By encrypting data during transmission, even if intercepted, they remain unreadable and meaningless to unauthorized entities [105]. Implementing strong encryption protocols, such as the Advanced Encryption Standard (AES) or Rivest–Shamir–Adleman (RSA) encryption, can effectively protect data from interception attacks. These encryption mechanisms use complex mathematical algorithms to encode data, making it extremely difficult for attackers to decipher the information without the decryption key. Additionally, encryption should be applied not only to data in transit but also to data at rest on drones and GCSs to ensure end-to-end protection [88]

Furthermore, regular auditing and monitoring of communication channels for suspicious activities can help detect and prevent data interception attempts in real time, by setting up intrusion detection. The significance of monitoring traffic for early detection and prevention of DoS attacks cannot be overstated in safeguarding drone systems. By closely monitoring network traffic patterns and behavior, organizations can detect unusual spikes in traffic volume or suspicious activities that may indicate a potential DoS attack. Early detection enables timely response measures to be implemented, such as filtering out malicious traffic, rerouting communications through secure channels, or activating backup systems to ensure uninterrupted drones [33].

To mitigate the risks associated with GPS spoofing attacks, one effective countermeasure is GPS signal authentication. This involves verifying the authenticity of the GPS signals received by drones to ensure their accuracy and integrity. By implementing GPS signal authentication mechanisms, drones can validate the source of the GPS signals and detect any attempts at spoofing or manipulation. There are several techniques that can be used for GPS signal authentication to prevent spoofing attacks. One common method is cryptographic authentication, which involves using cryptographic algorithms and keys to digitally sign the GPS signals. This allows drones to verify the authenticity of the signals by checking the signature against a trusted source [106]. Another approach is to implement secure communication protocols, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), to encrypt the GPS signals and protect them from interception or manipulation. Additionally, the use of redundant navigation systems can assist in enhancing the resilience of drones against GPS spoofing attacks. By integrating multiple sources of navigation data, inertial navigation systems, and visual sensors, drones can cross-validate the information and detect discrepancies [107].

To mitigate the risks associated with signal jamming, countermeasures such as frequency hopping have been developed. Frequency hopping is a technique used to counteract the effects of jamming by rapidly changing the frequency at which data are transmitted. By hopping between different frequencies in a predetermined sequence, drones can avoid prolonged interference and maintain communication with their controllers. This works by dividing the available frequency spectrum into multiple channels and switching between them at regular intervals. This method makes it difficult for attackers to jam the signal effectively, as they would need to jam multiple frequencies simultaneously to disrupt communication. Additionally, frequency hopping can provide a level of encryption by using a unique hopping sequence known only to the drone and its controller, further enhancing the security of the communication link [108,109]. By implementing frequency hopping as a countermeasure against signal jamming, drone operators can significantly enhance the resilience of their communication systems, as it enables drones to adapt to changing interference conditions and maintain reliable connectivity in challenging environments [110].

Moreover, regular software updates are essential for maintaining the security and functionality of drone systems, since software vulnerabilities are commonly exploited by attackers to gain unauthorized access or inject malware into drones. By regularly updating the drone software, security patches can be applied to address known vulnerabilities and strengthen the system's resilience against potential cyber threats. Additionally, software updates can improve the overall performance and stability of drone operations, reducing the risk of system malfunctions and disruptions. Similarly, strong authentication mechanisms are crucial for verifying the identity of users and ensuring secure access to drone systems [111]. By implementing multi-factor authentication, access controls, and user permissions, the risk of unauthorized access to drones can be significantly reduced. Such measures prevent malicious actors from exploiting weak credentials or gaining unauthorized control over drones, protecting the integrity and confidentiality of sensitive data. Finally, continuous monitoring of drone systems is essential for detecting and responding to any unusual activities or security incidents. By monitoring network traffic, system logs, and user behaviors, potential threats can be identified in real time, allowing for prompt mitigation measures to be implemented and helping security teams to stay vigilant against evolving cyber threats and proactively defend against attacks that could compromise the safety and security of drone operations [77,112].

Blockchain technology can provide robust solutions for enhancing the security of the IoD environment in various ways. It can be used to create unique digital identities for individual drones, which are stored and managed on the blockchain, assisting in the prevention of impersonation attacks. Specifically, each drone in the network is given a unique identity, with the identity being stored in the blockchain. When a drone attempts to join the network or perform a transaction (e.g., sending data), it has to prove its identity. This is done through a process called cryptographic verification. The drone provides a digital signature, which is a piece of cryptographic data, while other participants in the network (which could be other drones, or base stations) can use this digital signature to verify the drone's identity. If the identity cannot be verified, the drone is not allowed to join the network or perform transactions [113]. In addition, blockchain can ensure the confidentiality and integrity of the data using encryption, access control, and immutability, with the transmitted data being encrypted using cryptographic algorithms. Only entities with the correct decryption key can access the original data. Moreover, blockchain can be used to implement sophisticated access control mechanisms. For instance, permissions can be set on the blockchain to restrict access to certain data for specific entities, while the immutability of the blockchain ensures that, once data are recorded, they cannot be altered. This can be useful for maintaining a tamper-proof log of drone activities [4]. Moreover, blockchain can secure the communication between drones and control stations, preventing various types of attacks [114] providing access control, ensuring that only authorized drones can access certain resources or perform certain actions, preventing single points of failure, and making the system more resilient to attacks. This can enhance the robustness and reliability of IoD systems and enable the use of smart contracts, which are self-executing contracts with the terms of the agreement directly written into code. These can be used to automatically enforce access control policies, such as automatically revoking a drone's access rights if it behaves maliciously [4]. Regarding integrity, all transactions on a blockchain are transparent and cannot be altered, ensuring data integrity, while the use of consensus algorithms to validate transactions and blocks can prevent fraudulent activities [115].

As a recently emerging and revolutionary technology, blockchain is capable of being integrated within the IoD ecosystem [4], supporting efficient and secure solutions due to its prominent features and cryptographic properties [116]. At its core, blockchain offers decentralized data storage services and the ability to log and secure transactions through cryptography [117], which is achieved through the interconnection and validation of data blocks using cryptographic hash functions. Such principles are beneficial to the design of security mechanisms for tackling the challenges mentioned above [118]. Specifically, blockchain has been integrated with various emerging technologies and concepts, including the IoD, and deployed in critical domains to provide effective and robust cybersecurity [119,120]. Practically, it maintains a distributed ledger, tracking the activity of the UAVs in a swarm network, enabling the collected data to maintain their integrity, making them unable to be tampered with [121]. A significant example of blockchain's applicability as a UAV security mechanism is related to the organizational manner of Ground Stations with regard to the drone's status and availability within the network, based on the related data that can be accessed from the preferred distributed database [122].

4.3.3. Localization Error-Based Attacks

One of the main categories of attacks on IoD systems is localization error-based attacks [78]. Specifically, lack of localization for cyber–physical systems, such as the IoD, leads to significant errors that emerge from hindering the estimation of drones' secure location [81]. Figure 9 shows the taxonomy of IoD attacks based on the corresponding category (localization error-based attacks). Table 2 summarizes the investigated published material on IoD elements, requirements, security issues, and countermeasures.

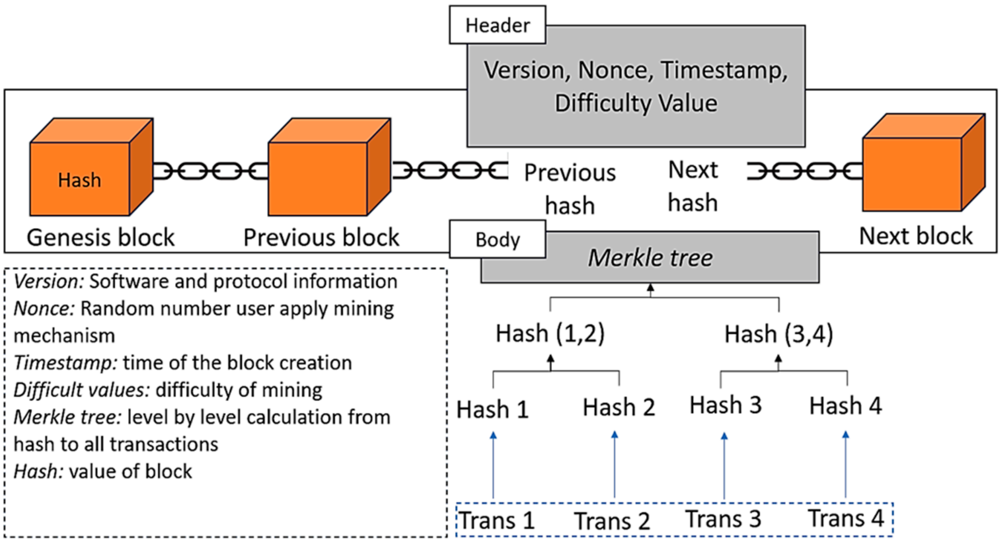
Table 2. Investigated works on the IoD, by scientific topic.

Investigated Works	Scientific Topic
[2,5,26,49–66,72,76]	Basic elements and requirements of the IoD
[13,22,35,39,67,71,77–80]	Privacy and security issues of the IoD
[9,22,34,78,81–103]	IoD attacks
[9,33,77,88,104–115]	Protected countermeasures
[116–122]	Blockchain measures for IoD security

5. Blockchain Fundamentals

5.1. Overview of Blockchain

Blockchain consists of data structures (blocks) that are linked to each other to form a chain based on the hash pointer concept, with each block containing the stored data (or transactions) and the hashes of the previous and current blocks [123]. As a concept, data blocks, identified by their unique codes, wrap the chronological order of transactions (recorded in the block header) and store the related information [124]. Simultaneously, the header contains the result of the Merkle tree [125] and the hash value of its parent block. Figure 11 presents an overview of the overall concept and functionality of blockchain.



Version: Software and protocol information
Nonce: Random number user apply mining mechanism
Timestamp: time of the block creation
Difficult values: difficulty of mining
Merkle tree: level by level calculation from hash to all transactions
Hash: value of block

Figure 11. Basic structure of blockchain.

Due to the established shared ledger throughout the network, the speed of transactions and data exchange among untrusting parties are significantly increased, eliminating manual processes. In addition, blockchain's integrated security features assist the verification and initialization of transactions originated by a trusted party, as well as data encryption during transmission and storage. However, the great merit of blockchain is the rapid identification of weaknesses in the entire network. From the privacy perspective, blockchain, as a decentralized distributed ledger database system, contains cryptographically generated data blocks [126]. Moreover, through smart contracts, the self-execution of a program is performed, with the condition that certain terms are being met.

The blockchain technology consists of five layers in terms of architecture, which are correlated for the creation of a secure, decentralized, and transparent blockchain ecosystem [127,128].

Hardware/infrastructure layer: This layer is the foundational layer of a blockchain system. It comprises all of the physical resources, such as servers, nodes, and specialized hardware like ASICs (Application-Specific Integrated Circuits) for mining in Proof-of-Work blockchains, or hardware security modules for securely storing cryptographic keys. This layer is crucial, as it provides the computational power and storage capacity needed for the operation of the blockchain network. It is the base upon which all other layers of the blockchain architecture are built. Without a robust and secure infrastructure layer, the blockchain network cannot function effectively [129].

Data layer: The data layer involves the storage and management of data within the blockchain network, including transactions, smart contracts, and other related information. This layer is essential for ensuring the security and integrity of transactions. Through the use of cryptographic techniques, decentralized networks, immutability, and data validation mechanisms, this layer plays a pivotal role in safeguarding the integrity of blockchain transactions and maintaining the trust and transparency of the network. Data stored in the blockchain are encrypted using cryptographic hash functions, which are algorithms that convert input data into a fixed-size string of characters. Any changes made to the data will result in a different hash value, alerting the network to the presence of unauthorized modifications. Moreover, the decentralized nature of blockchain technology further reinforces the security and integrity of transactions within the data layer. Furthermore, the data layer employs data validation mechanisms to ensure the accuracy and integrity of transactions. When a transaction is initiated, it undergoes a series of validation checks to confirm its validity and authenticity. These checks may include verifying the digital signatures of the parties involved, checking for double-spending, and ensuring that the transaction complies with the rules and protocols of the blockchain network. The transactions that pass these validation checks are then added to the blockchain, maintaining the integrity of the ledger [130].

Network layer: This layer focuses on the communication protocols and network infrastructure that enable nodes to interact and share information securely across the blockchain network [131]. It handles all aspects of peer-to-peer network communication within the blockchain system. The network layer is responsible for the communication between nodes in the blockchain, including the propagation of new transactions and blocks to all nodes, while nodes communicate with each other via network protocols [132]. This layer ensures that data are correctly transmitted across the network and, thus, it ensures its security by applying protective measures against attacks such as DoS.

Consensus layer: The consensus layer is responsible for ensuring agreement among network participants on the validity of transactions and maintaining the integrity of the blockchain through various consensus mechanisms. This layer ensures that all transactions are validated and that new blocks are added to the blockchain in a manner that maintains the system's security and integrity. There are several types of consensus algorithms used in different blockchain networks [133], including Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT). These algorithms are designed to achieve agreement across all nodes in the network regarding the state of the distributed ledger [134,135].

Application layer: The application layer is the topmost layer that interfaces with users and external systems, providing functionalities such as wallets, decentralized applications (dApps), and user interfaces for interacting with the blockchain network [131]. (a) Wallets:

These are applications that allow users to store, send, and receive digital assets that are secured by the blockchain [136]. (b) Decentralized Applications (dApps): These are applications that run on the blockchain network itself, leveraging its decentralized nature to provide services that are not controlled by a single entity [137]. (c) User interfaces: These are the front-end systems that users interact with. They can be web interfaces, mobile apps, or other types of software that provide a user-friendly way to access the blockchain network [138]. In essence, the application layer is where the capabilities of the blockchain network are made tangible and usable for end-users. It is the bridge between the underlying blockchain infrastructure and the users who benefit from the services that it provides. In addition, this layer enables the tokenization of assets and the issuance of digital tokens on the blockchain network [139], facilitates identity management and authentication services on the blockchain network, enables supply chain traceability and provenance tracking on the blockchain network, and serves as the foundation for decentralized finance (DeFi) applications on the blockchain network [140].

Nevertheless, in a distributed network such as blockchain, partial trust between peers exists, and consensus protocols are established to agree on a single copy of the ledger, whereas, in the case of the participation of multiple nodes, there must be agreement on a standard value [118,141]. Distribution, immutability, and decentralization are the fundamental principles of blockchain, enhancing fault tolerance due to the participants' contribution to the system [142]. Also, fundamental features (characteristics) of blockchain, such as transparency, tamper-proofing, and security, make it a high-potential and innovative technology, capable of being combined with other emerging technologies [143].

- Distribution: Thanks to distribution, independent computers or nodes keep sharing, recording, and synchronizing transactions in their respective electronic ledgers through protocols and supporting infrastructure. In this manner, the process remains transparent, dependable, and reliable.
- Immutability: Since each block is specified with a string of characters obtained by a cryptographic hash function, representing recorded transactions, stored data remain immutable and unable to be manipulated.
- Decentralization: This indicates the transfer of control, authority, and decision-making from an individual, organization, or group to a distributed network or its participants, averting the abuse of power. Consequently, assets can be stored in the network without the oversight or control of a single person or entity.
- Transparency: Each participant in the blockchain system holds a copy of the blockchain for the verification of initiating a transaction by a legitimate user.
- Tamper-proofing: After the verification of each block by (all) participants, it is added to the blockchain through the confirmation of a consensus algorithm. Hence, the blockchain system maintains a tamper-proof ledger shared by the participants, without relying on a trusted third party.
- Security: Blockchain systems use asymmetric cryptographic building blocks to encrypt data, whose security generally relies on the underpinning consensus algorithm, and this is empowered by most of the participants.

Generally, blockchain networks can be categorized based on their permission model and structures into (a) public, (b) private, and (c) consortium. All types of blockchains can be described as permissionless, permitted, or both, since users can join a network with permissionless blockchain. However, permitted blockchains restrict network access to specific nodes with specialized rights. A public blockchain is inherently permissionless, allowing anyone to join, and is completely decentralized. All nodes have equal access to the ledger, as well as the ability to create new transactions and validate the blocks. Private blockchains, known as trust blockchains, are authorized and controlled by a single organization that decides whether a node is permitted to be integrated within the private network. However, every node has the same rights in terms of functionalities. A consortium blockchain is an authorized blockchain controlled by a group of organizations, with a higher degree of decentralization than private blockchains, leading to a higher level of security [4].

Public blockchains are open networks where anyone can participate and have access to the shared ledger, defining its high level of accessibility, as they allow anyone to join the network and contribute to the validation process. This openness also fosters innovation, as developers can build decentralized applications on these platforms. Moreover, public blockchains provide a high degree of security and transparency, as the data are shared across a distributed network of nodes, making it difficult for malicious actors to manipulate the system. In terms of practical applications, public blockchains are well suited for use cases that require a high level of transparency and decentralization. For example, they are often used in the financial sector for peer-to-peer transactions and smart contracts. Public blockchains are also ideal for applications that involve multiple parties with minimal trust, as the decentralized nature of the network ensures that no single entity has control over the data [144,145].

Private blockchains restrict access to selected and verified participants. Unlike public blockchains, which are open to anyone, private blockchains offer more control and privacy, maintaining a certain level of confidentiality and security. The primary purpose of private blockchains is to limit access to sensitive information and transactions within a closed group of participants. As a result, organizations can ensure that only authorized users are able to view or modify the information. This enhanced level of security is particularly important for industries that handle sensitive data, such as financial institutions, healthcare providers, and government agencies. One of the key benefits of private blockchains is the ability to customize the network according to the specific needs and preferences of the participating organizations. This level of customization allows for greater flexibility in terms of scalability, performance, and governance. Private blockchains also tend to have higher transaction speeds and lower latency compared to public blockchains, making them well suited for applications that require real-time processing of transactions. In addition to security and customization, private blockchains offer a range of other benefits to organizations. These include increased efficiency and cost savings, as well as improved transparency and auditability. By using blockchain technology to streamline operations and automate processes, organizations can reduce the risk of errors and fraud, ultimately leading to improved trust and credibility among stakeholders [146–148].

Consortium blockchains represent a unique hybrid model that combines elements of both public and private blockchains. This type of blockchain is characterized by a group of organizations working together to maintain the network, sharing control and responsibility among the participants. In consortium blockchains, multiple preselected entities have the authority to read, write, and validate transactions on the distributed ledger, ensuring a higher degree of control and privacy compared to public blockchains, while still maintaining some level of decentralization. One of the key characteristics of consortium blockchains is the collaborative nature of the network. By bringing together multiple organizations that have mutual trust and shared goals, consortium blockchains enable these entities to interact with each other in a secure and transparent manner. This collaboration fosters innovation and efficiency, as participants can leverage the shared infrastructure to streamline processes, reduce costs, and improve overall operations [149]. Another key benefit of consortium blockchains is the balance that they strike between decentralization and control. While public blockchains prioritize decentralization and openness, and private blockchains prioritize control and privacy, consortium blockchains offer a middle ground that satisfies and caters to varying needs in terms of transparency, control, and collaboration [150,151]. Table 3 shows a comparison of the corresponding blockchain types.

Table 3. Differences among the types of blockchains.

Parameters	Public BC	Private BC	Consortium BC
Accessibility	Anyone can participate in the core activities of the BC network	Selected and verified participants can join the network (restricted access)	Participants need permission to join the network (restricted access)
Visibility	All transactions are visible in the network	Closed or open to a certain number of nodes	Open to a certain number of nodes (preselected nodes)
Control	Decentralized	Centralized	Centralized
Transparency	Transparent, as all transactions are visible to anyone on the network	Private, as only authorized users can view the data and transactions on the network	Private, as only authorized users can view the data and transactions on the network
Scalability	Lower	Higher	Better compared to the public BC
Privacy	Less privacy, as it accessible to everyone	High-level privacy	High level privacy compared to the public BC
Consensus mechanism	PoW	PoW, PoS, etc.	PoW, PoS, etc.
Power consumption	High energy consumption	Low energy consumption	Low energy consumption
Anonymity	Users remain anonymous	Identities of users involved in the transaction	Identities of users involved in the transaction
Security	Highly secure and resistant to attacks, due to the decentralized nature of the network and use of cryptography	Security using cryptography	Enhanced security through access restrictions
Use cases	Mining and exchanging cryptocurrencies, decentralized financial systems, supply chain management, digital arts	Enterprise applications, supply chain management, and internal data sharing	Financial institutions, the healthcare industry, supply chain management, and confidential data sharing among trusted entities

5.2. Contribution of Blockchain to the IoD

The integration of drones and blockchain technologies has the potential to transform the operational manner of the IoD ecosystem, as it has the capacity to provide powerful outcomes, such as enhanced security, as highlighted in Section 4.3, as well as novel applications that are described later on. Specifically, in the case of the IoD, a distributed network maintains an immutable database of the users' actions, data obtained by drones, and GCS commands, with the recorded transactions being shared among the nodes in the network, assisting in the overall support of the network and verification of data blocks [152]. A typical model consists of the user, infrastructure, and an IoD layer [15,61], enabling the interaction between two users, or between a user and a drone, while creating blockchain clusters with a drone being assigned as a master controller. Each cluster controls and coordinates the behavior of the network's drones, and the infrastructure layer specifies the connectivity and control of users and drones through the GCS for efficient and secure data exchange. The result of the corresponding operational flow leads to the storage of the updated data within the specified blockchain framework [153]. Figure 12 presents the basic functionality features of blockchain, integrated with the IoD.

Specifically, blockchain offers significant benefits [4,154] as a main component of distributed systems [155]:

- It overcomes single-point failures due to decentralization features.
- It provides enhanced security to drone communication.
- Drone data are transparently recorded, maintaining their integrity.
- It ensures accountability and traceability.
- It controls multi-signature access and decentralized administration.

- It secures shared data due to the encryption and hashing capabilities.
- It is based on the distributed consensus mechanism, enabling smart agreements, trust, and protection across the utilized decentralized network, with a transaction being validated as authentic [156].

- It ensures data privacy protection through cryptography [153].
- It provides 5G-enabled drone identification and flight mode detection [157], as well as drone communication for the preservation of privacy [158].
- It offloads the provision of dynamical cache data [159].
- It provides a secure and transparent platform for managing valuable information and data obtained by drones [160].
- It ensures the confidentiality of all transactions following decentralized, distributed, and peer-to-peer (P2P) communication networks, with data being stored on each node [161].
- It ensures secure data sharing over a tamper-proof and decentralized ledger [162].

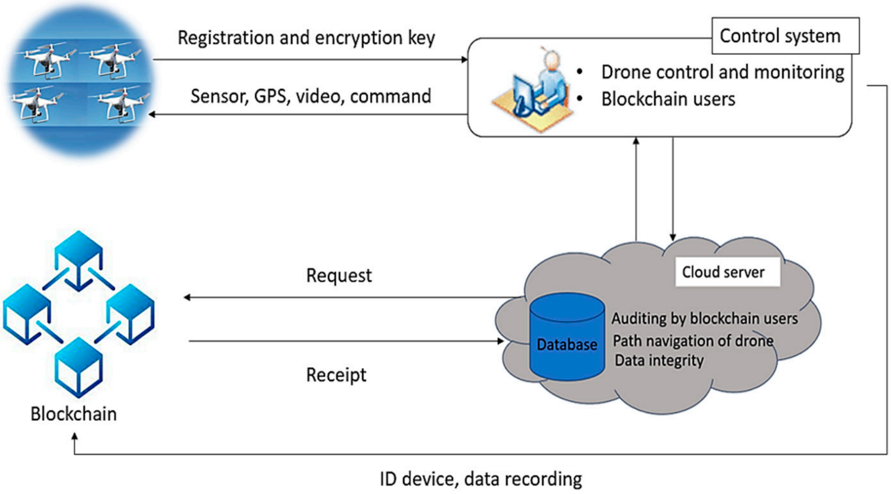

Registration and encryption key
Sensor, GPS, video, command
Control system
Drone control and monitoring
Blockchain users
Request
Receipt
Cloud server
Database
Auditing by blockchain users
Path navigation of drone
Data integrity
Blockchain
ID device, data recording

Figure 12. Blockchain integrated with IoD.

Blockchain facilitates automated privacy preservation [143] at different layers of 5G-enabled drone communications, such as ID management, data privacy, and trajectory protection, as well as the consensus of drones' participation within the network. The drones' ID can be registered to the blockchain-based ID management system covering the entire life cycle of a drone. During this process, trust can be ensured via the decentralized consensus of blockchain-based systems. Similarly, the termination status can be updated in the blockchain for the drone ID to be revoked or removed, i.e., during the entire life cycle of a drone, status changes can be traced through a decentralized ID management system. Furthermore, the automatic ID management process reduces administration costs due to the availability of smart contracts. Concerning privacy conditions, collected data can be violated via Drone-to-Drone (D2D) or Drone-to-Ground (D2G) links, with additional theft risks related to transits, by utilizing Drone-to-Base-Station (D2B) links [163].

At this point, blockchain contributes to different phases, as it is based on authentication mechanisms that verify access authorization protocols assigned to drones, along with cryptographic schemes to minimize the risk of misused data [164]. Also, the blockchain-based consensus of drone networks ensures reliable interconnection between multiple drones. However, the maintenance of its reliability is in its infancy due to the dynamic drone topologies and unreliable wireless communications [165,166]. Additional decentralized security approaches involve data protection in case of theft, air traffic control, and collision prevention through secure sharing of real-time location data [167], as well as insurance in terms of unpredicted damages, with the related data being stored in the ledger without possibilities for alteration [168]. Table 4 presents the investigated research papers that supported the analysis of blockchain, as well as its contribution to IoD systems.

Table 4. Investigated references on blockchain, by scientific topic.

Investigated References	Scientific Topic
[118,123–126,141–144]	Structure of blockchain
[127–140]	Architecture of blockchain
[144–151]	Types of blockchain
[15,61,143,152–168]	Contribution and benefits of blockchain to the IoD

6. Underpinning Technologies for IoD–Blockchain Integration

Due to constant technological evolution, current applications are designed in a collaborative manner, combining features and characteristics and supplementing utilized technologies in order to provide additional benefits on different levels. In this section, various technologies are highlighted in relation to enabling the integration of blockchain and the IoD. Figure 13 shows the essential underpinning technologies of the IoD and blockchain.

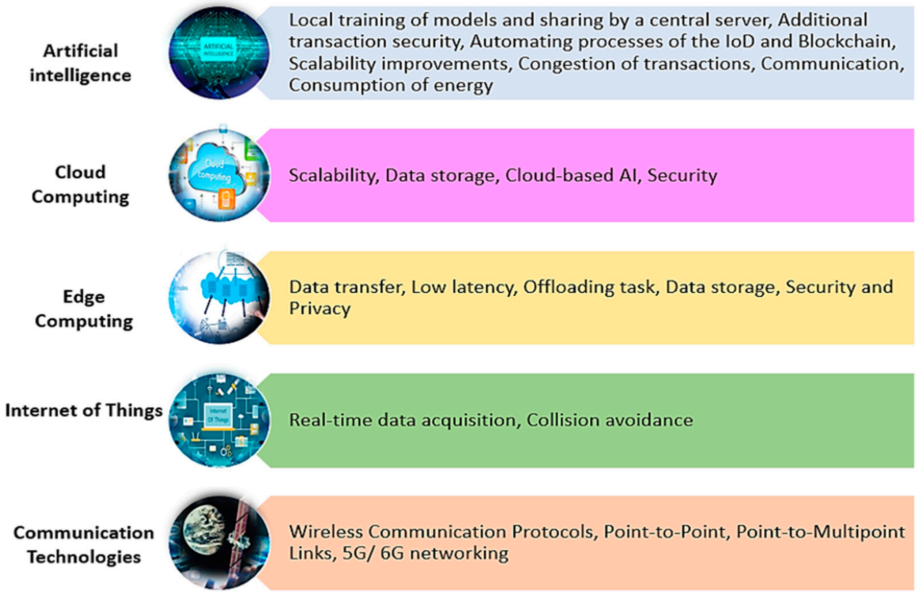

Artificial intelligence
Local training of models and sharing by a central server, Additional transaction security, Automating processes of the IoD and Blockchain, Scalability improvements, Congestion of transactions, Communication, Consumption of energy
Cloud Computing
Scalability, Data storage, Cloud-based AI, Security
Edge Computing
Data transfer, Low latency, Offloading task, Data storage, Security and Privacy
Internet of Things
Real-time data acquisition, Collision avoidance
Communication Technologies
Wireless Communication Protocols, Point-to-Point, Point-to-Multipoint Links, 5G/ 6G networking

Figure 13. The essential underpinning technologies of the IoD and blockchain.

6.1. Artificial Intelligence (AI)

AI, including sub-disciplines such as Machine Learning and Deep Learning, is a key technology enabling the IoD and blockchain to act intelligently, providing trust in unknown environments [169]. AI can enhance the performance, accuracy, and efficiency of the data derived by multiple drones and other sources while providing a unified and coherent view of the environment, with blockchain providing immutable data storage. The implementation of AI algorithms within decentralized IoD systems enables the following:

- Local training of models and sharing by a central server: This allows drones to operate autonomously and contribute to the collective knowledge of the entire network. Specifically, it enables data recording and management, sharing of model updates within the blockchain, coordination between participants, and ensuring transparency, immutability, and trust in the IoD ecosystem.
- Additional transaction security: During the flight of drones, AI-based mechanisms support the safety of drone operations by detecting potential risks, such as collisions or unauthorized intrusions. When data are inserted into the blockchain, an additional

layer of security is added to it, identifying and preventing or minimizing the risk of fraud and detected anomalies in transactions. In this manner, the transparency of the transactions is increased, reducing the need for intermediaries.

- Automating processes of the IoD and blockchain: The key to automatic enhancement is the integration of AI, decentralized decision-making through blockchain, and automation to enable systems to adapt and improve autonomously. Drones operate autonomously without direct human intervention and can dynamically adjust their routes based on real-time data, traffic, weather conditions, and mission priorities. In addition, drones analyze sensor data in real time for object detection, path planning, and decision-making during missions, with the system automatically scheduling maintenance and even ordering replacement parts or services, while blockchain facilitates decentralized coordination among drones, allowing them to share information and collaborate effectively. Smart contracts on the blockchain can govern interactions and decision-making, as they can be designed to adapt and optimize themselves based on changing conditions and performance data [170,171].
- Scalability improvements: Drones collect a vast amount of data that are distributed in a decentralized system towards multiple nodes while optimizing blockchain consensus algorithms, making blockchain networks more efficient and scalable. AI algorithms can allocate resources such as processing power and bandwidth dynamically, based on the specific requirements of each drone's mission, ensuring efficient resource utilization and scalability. In addition, AI facilitates multi-drone coordination, allowing them to collaborate efficiently in various tasks, such as surveillance, search and rescue, or delivery. Moreover, AI analyzes real-time data to optimize the routing of drones, enabling them to avoid congestion [31].
- Congestion of transactions: Congestion in the drones' communication network can result in communication delays, disrupting the execution of drone tasks that rely on real-time data sharing and control commands, as well as malfunctions and errors during drone fleet missions, causing disturbances in their coordination. Taking into consideration the aspect of blockchain, transaction delays are also present. AI can help improve congestion by prioritizing transactions based on their size and urgency, analyzing historical data and network conditions to predict potential congestion, distributing transaction data processing across the network nodes evenly, preventing specific nodes from becoming bottlenecks during congestion, and allocating resources dynamically to drones based on their current tasks and priority levels [172]. This ensures that drones with critical missions are supplied with the required resources during such situations, manage the communication traffic efficiently, reduce congestion by scheduling data transmission, and control the flow of information between drones and central servers [45,173].
- Communication: The wireless communication among the drones and data management within blockchain is secure, thanks to AI providing efficient decentralized intelligence. AI can assist drones in selecting optimal communication paths, optimize the utilization of the available frequencies, and enable drones to dynamically switch to different frequencies or channels to avoid interference, facilitating multi-drone communication coordination. Furthermore, UAVs' robustness, resilience, and efficiency are improved by applying Machine Learning, Deep Learning, and ANN-optimized UAV communication networks [64]. Meanwhile, in the case of blockchain, AI provides efficient and secure data transfer, optimizing the communication and load distribution between wireless nodes [174,175].
- Consumption of energy: During data transmission between drones and Ground Stations, or among drones, a significant amount of energy is consumed. In addition, data processes within blockchain, or features such as the execution of complex smart contracts, contribute to additional energy consumption. AI can optimize drone routes and flight patterns, making them more energy-efficient, reducing operational costs [176],

and establishing intelligent decision-making in relation to data blocks and the overall ledger [177].

6.2. Cloud Computing (CC)

CC provides flexibility, storage, and resource management, sharing rapid elasticity and dynamic scalability of resources [27]. The data collected by drones can be gathered in a cloud capable of maintaining a large amount of data [178]. CC provides the following:

- Scalability: There are platforms with on-demand resources, allowing IoD applications to scale up or down as needed. Thus, CC provides the capability of handling a variable number of drones or accommodating traffic spikes during specific missions, as well as supplementing blockchain storage depending on the resources required by the utilized nodes [179,180].
- Data storage: The IoD generates large volumes of data, such as high-definition images and videos, which can be efficiently stored in the cloud, since blockchain networks often require extensive data storage for the ledger. Cloud storage can provide a reliable and cost-effective solution for storing blockchain data. In addition, CC prevents data losses, offering data copies that are stored in different nodes [181].
- Cloud-based AI: In this case, cloud-based AI and analytics tools can be used to process and analyze the vast amounts of data generated by drones. This is valuable for extracting insights, detecting anomalies, and optimizing operations.
- Security: Cloud providers often offer robust security features, including encryption and access control, to protect the data and communication within IoD and blockchain networks.

6.3. Edge Computing (EC)

Edge Computing is another key technology that can be implemented within IoD and blockchain infrastructures for data processing and storage at the utilized network's edge [182], including the AI known as "edge AI" [183]. EC provides the following:

- Data transfer: It enables drones to perform data processing and decision-making procedures at the edge, reducing the need to transmit large volumes of data to central servers. This reduces network congestion and enhances scalability while minimizing the requirement of transferring massive data volumes over blockchain.
- Low latency: It reduces latency by processing data and making decisions closer to the source, which is crucial for real-time communication, obstacle detection, and collision avoidance in IoD applications, while it accelerates the verification and propagation of blockchain transactions. Consequently, there are significant improvements in the speed of confirmations and transactions [184].
- Offloading tasks: Combined with AI, it facilitates the computational flow of the server to offload tasks and data, providing lower latency, higher reliability, improved security and privacy, and reduced costs and energy consumption [31,185]. Thus, data streams are shortened to remote centralized servers because of the computational services at the edge of the network [182], while blockchain technology is used to further enhance the capabilities of EC, allowing secure communications and data processing by enabling decentralized approaches [186].
- Data storage: Since the data collected can be stored within the blockchain, edge devices can store a copy of the blockchain ledger, reducing the reliance on central servers for data access and ensuring data integrity, while smart contracts can be executed at the edge, allowing for quicker and more responsive automation of contractual agreements without the need for centralized cloud services.
- Security and Privacy: Sensitive data obtained by drones can remain on the edge device or gateway, reducing the exposure to potential security threats and privacy breaches that may occur during data transmissions to a central server. Also, during data transfers within the blockchain, an extra layer of security is included, allowing for localized encryption and data validation at the source.

6.4. Internet of Things (IoT)

The integration of IoT devices into blockchain and IoD ecosystems has a significant impact on data collection and accuracy, automation, and real-time decision-making upgrades. Important IoT features within the combination of the IoD and blockchain include the following [29,187–189]:

- Real-time data acquisition: IoT sensors and devices on drones result in the collection of real-time data—specifically, smart monitoring of environmental factors like temperature, humidity, air quality, and radiation levels, with the data being able to be registered on a blockchain for storage, analysis, and further decision-making tasks. Similarly, depending on the status of the collected data, IoT devices can trigger warning notifications and reports to the related stakeholders, with the history of the reported data being stored in an immutable decentralized ledger. Also, IoT devices can be used for identity verification and access control in blockchain-based systems, enhancing security and privacy.
- Collision Avoidance: IoT sensors can detect nearby objects, including other drones, aircraft, and obstacles, preventing potential collisions, and ensuring their physical integrity and safety during flights. Such an approach is handled with the registration of IoT data within a decentralized system dedicated to the drones' coordination. Drones can share their positions and intentions on a blockchain, and smart contracts can govern their interactions, providing a framework for collision avoidance strategies through immutable flight data, including routes, altitudes, and times, which can be reviewed in case of incidents or accidents. Analyzing these data can help identify the causes of collisions and develop preventive measures.

6.5. Communication Technologies

Effective communication technologies are essential for the IoD and blockchain networks to function efficiently and securely, enabling real-time data sharing, command execution, and secure transactions. In particular, the adoption of 5G and 6G technologies by the IoD can significantly enhance performance, security, and real-time capabilities, opening up new opportunities for innovative applications and use cases. Although 6G is still in the early stages of development, its full capabilities and specifications may change as the technology evolves. The key communication technologies that play crucial roles in these domains are described below:

Wireless Communication Protocols: Drones rely on wireless communication to transmit data and receive commands. Common protocols include Wi-Fi, cellular networks, and LoRa (long range) for long-distance communication. Additionally, Drone-to-Drone (D2D) communication may use ad hoc mesh networks that enable drones to create a self-healing network, where each drone acts as a relay for data transmission and enhances coverage and redundancy [190,191].

Point-to-Point and Point-to-Multipoint Links: These technologies are used for dedicated communication links between drones, Ground Stations, and other devices, while blockchain networks rely on peer-to-peer communication to distribute and validate data, enabling nodes to connect directly to one another, forming the decentralized network. The communication among the nodes in the blockchain is achieved by consensus protocols such as PoW, PoS, and Delegated Proof of Stake (DPoS), whereas, thanks to smart contracts, communication of blockchain with external data sources (oracles) is achieved to execute predefined conditions. Oracles ensure that the smart contract interacts with the real world and receives reliable data [192,193].

Properties of 5G networking:

- Low Latency: 5G offers significantly lower latency (below 1 ms) compared to previous generations of mobile networks, supporting high data transmission rates in the range of Gbps. Since drones collect real-world data, 5G's low latency and high bandwidth can facilitate this procedure of utilizing external data sources when the related data are inserted into a blockchain, with smart contracts enhancing the capabilities of blockchain-based oracles. This is crucial for real-time communication and decision-making in drone operations, while during the data processing in blockchain, low latency in the 5G network provides faster transaction confirmation, propagation, and validation, leading to faster confirmation times [194,195].

- High Bandwidth: The high bandwidth of 5G networks allows drones to transmit large volumes of data, including high-definition video feeds, sensor data, and imagery. When the corresponding data are inserted into the blockchain, a unification is achieved between the security of the decentralized mechanism and the increased bandwidth of 5G, resulting in advanced scalability, encryption, and authentication [196].
- Reliable Connectivity: 5G provides a more reliable and stable connection for drones, reducing the risk of signal loss or interference, which is vital for maintaining control and communication in critical missions, while blockchain provides faster and more reliable 5G networks, improving the cross-chain communication and enabling the transfer of assets and data obtained by drones between different blockchain networks more seamlessly [197].
- Network Slicing: 5G supports network slicing, allowing operators to dedicate specific network slices to IoD ecosystems, ensuring that drones have dedicated resources and guaranteed service quality, and enhancing the overall performance. Meanwhile, the transactions are processed more efficiently, improving the performance of blockchain networks, especially in scenarios with high transaction volumes [192].

Properties of 6G networking:

- Ultra-Low Latency: 6G is expected to provide even lower latency than 5G, potentially enabling near-instantaneous communication between drones and control centers. It is expected that the 6G network will have a transmission rate up to Tbps, i.e., 1000 times faster than 5G, and the ability to provide latency in ms, which is crucial for real-time decision-making and autonomous drone operations. In addition, with 6G's improved connectivity and low latency, drones can operate in swarms with greater autonomy, facilitating collaborative tasks and coordinated missions, while in blockchain 6G can enable faster consensus mechanisms, reducing the time required for transaction validation. Thus, high transaction volumes are handled easily, with the capability of being processed simultaneously, making blockchain networks more efficient and responsive [197,198].
- Terahertz Frequencies: 6G may operate at terahertz frequencies, allowing for higher data rates and more efficient data transmissions. Drones can stream ultra-high-definition videos and sensor data, offering more precise positioning and navigation capabilities, and ensuring accurate location information for drones. In blockchain, 6G frequencies provide faster and more efficient data transmissions and consensus mechanisms, as well as seamless exchange of data and assets between various blockchains [197].
- Secure Communication: 6G is expected to introduce advanced security features, such as quantum-resistant encryption, which can ensure the confidentiality and integrity of data exchanged between drones and other network components. Moreover, blockchain is expected to introduce advanced security mechanisms, including post-quantum cryptography, which can further enhance the security of decentralized networks [199–201].

Table 5 summarizes the studied references related to the underpinning technologies of the blockchain–IoD union.

Table 5. Investigated works on the underpinning technologies regarding blockchain–IoD integration.

Investigated Works	Underpinning Technologies
[169–177]	Artificial Intelligence (AI) within blockchain and the IoD
[178–181]	Cloud Computing (CC) within blockchain and the IoD
[182–186]	Edge Computing (EC) within blockchain and the IoD

Table 5. *Cont.*

Investigated Works	Underpinning Technologies
[29,187–189]	The Internet of Things (IoT) within blockchain and the IoD
[190–193]	Communication technologies
[192,194–198]	5G networks
[197,199–201]	6G networks

7. IoD and Blockchain-Enabled Features and Applied Use Cases

Today, there is a variety of application fields and use cases, integrating core principles of the IoD and blockchain, as well as providing many benefits and the potential for additional novel characteristics, while at the same time enhancing data security, transparency, and automation, enabling various industries to optimize their operations and services while maintaining trust and accountability [45]. Integrating blockchain technology with the IoD devices offers several potential benefits, including the following: (a) Enhanced security: Blockchain's decentralized and tamper-proof nature can provide robust security measures for IoD devices and data, while reducing vulnerabilities to cyber threats. (b) Improved data integrity: By leveraging blockchain's immutable ledger, the integrity and authenticity of data transmitted and stored by IoD devices can be ensured, enhancing trust among stakeholders. (c) Increased transparency: The transparent and traceable nature of blockchain technology can enable real-time monitoring and auditing of IoD device interactions and transactions, promoting accountability and transparency. (d) Efficient automation: Smart contracts on blockchain can automate processes within the IoD ecosystem, facilitating seamless and efficient interactions between devices, without the need for intermediaries. (e) Decentralized control: Integrating blockchain with the IoD can enable devices to operate autonomously, without centralized control, fostering a more distributed and resilient network architecture. (f) Cost savings: Streamlining processes, reducing intermediaries, and enhancing security through blockchain integration can lead to cost savings in IoD operations and maintenance [202–205]. Figure 14 presents key use cases of IoD–blockchain integration.

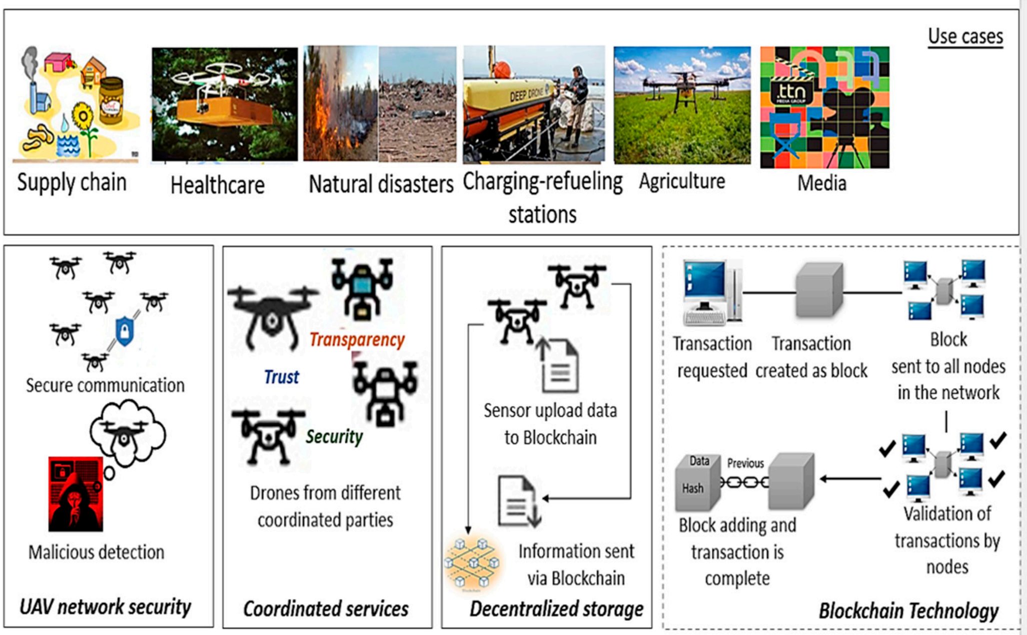

Use cases
Supply chain
Healthcare
Natural disasters
Charging-refueling stations
Agriculture
Media
Secure communication
Malicious detection
UAV network security
Transparency
Trust
Security
Drones from different coordinated parties
Coordinated services
Sensor upload data to Blockchain
Information sent via Blockchain
Decentralized storage
Transaction requested
Transaction created as block
Block sent to all nodes in the network
Data
Hash
Previous
Block adding and transaction is complete
Validation of transactions by nodes
Blockchain Technology

Figure 14. Uses cases of the blockchain-based IoD.

7.1. Supply Chain

A supply chain, also known as an inter-organizational supply chain and intra-organizational supply chain in the broad and narrow sense, respectively [206], is a network of individuals and companies, including all of the raw materials and components aiming towards the development of a product or service and its delivery to the relevant consumers [207]. The integration of the IoD and blockchain technology into supply chains offers numerous benefits, including enhanced transparency, traceability, and security. Specifically, drones are used for supply chain monitoring and logistics, while blockchain ensures the transparency of goods' origins, handling, and delivery, reducing false data and ensuring the authenticity of products. Moreover, in the context of transactions, blockchain enables trustworthiness and shareability of data, as drones can securely transmit them to authorized parties through blockchain-based access control and encryption mechanisms, promoting data privacy and security. For instance, in a supply chain of the food industry, drones equipped with sensors and cameras can monitor and record the pathway of products through the supply chain as well as parameters such as location and handling conditions, which can be stored in a blockchain ledger. In addition, drones can provide real-time monitoring of goods for conditions such as temperature variations, humidity levels, and other environmental factors that might affect the quality of products. This traceability helps in identifying the source(s) of any potential issues, such as contamination or damage, and facilitates product recalls if necessary, while blockchain ensures that these data remain tamper-proof and can be accessed by the relevant stakeholders. Moreover, blockchain-based smart contracts can automate various processes in the supply chain, including payment settlements, customs clearances, and delivery confirmations. These contracts can be triggered automatically when predefined conditions are met, reducing manual intervention and the risk of errors. Drones can be used for aerial inventory checks, which are particularly valuable in large warehouses and outdoor storage areas, with the related reports being recorded on the blockchain, ensuring accuracy and transparency in stock levels and authentication of products at each stage of the supply chain. Furthermore, drones can capture images of product labels or unique identifiers, with the information being stored on a dedicated ledger. This helps in preventing counterfeit products from entering the supply chain, while also conducting quality control inspections during the manufacturing or packaging process. Any deviations from quality standards can be documented on the blockchain, providing a permanent record of product quality. Also, drones can monitor compliance with sustainability and environmental regulations throughout the supply chain, through the collection of data on emissions, waste disposal, and adherence to environmental standards that can be securely recorded on the blockchain, in order to provide access to the related stakeholders [208,209]. Another aspect of the combination of drones and blockchain in the supply chain is the incorporation of cross-blockchain technology for the delivery of physical assets, i.e., a drone includes two blockchains, for the supply chain and the airspace traffic network, respectively. Thus, a correlation between the two ledgers is enabled, with the supply chain data blocks interacting in a collaborative manner with the airspace traffic data blocks through specific algorithmic mechanisms, resulting in efficient shipment tracking, boosted with confidentiality and interoperability [19,210].

7.2. Healthcare

The integration of the IoD and blockchain technology into healthcare offers numerous possibilities to enhance various aspects of the healthcare ecosystem, including the improvement of patient care, enhanced data security, streamlined operations, and addressing some of the key challenges in the healthcare industry, such as data interoperability and fraud prevention. Drones can be used to deliver medical supplies and equipment to remote areas, damaged regions, or healthcare facilities in need of urgent supplies, with installed temperature sensors to monitor the conditions of the supplies during transport. Simultaneously, the collected data are recorded on the system's integrated blockchain to ensure the integrity of the supplies [211]. Another example of a healthcare use case is the utilization of drones with implemented telemedicine capabilities, capable of providing remote consultations to patients in hard-to-reach areas, with the respective patient data (e.g., vital signs or diagnostic documents, diagnostics by healthcare professionals, and records such as medical history, including test results, treatment plans, and prescription histories) to be securely stored and shared on a tamper-proof blockchain platform for future reference [212,213], including a patient-controlled blockchain account, integrated with identity solutions, to ensure privacy and data security. In this manner, patients can grant and revoke consent for healthcare providers to access their medical data via smart contracts [214,215], which can also help in the development of new treatments and drugs [216]. In the context of healthcare, drones can also monitor pandemic (e.g., COVID-19) outbreaks by collecting related data on a blockchain and sharing them with public health agencies for analysis and early intervention [217,218].

7.3. Natural Disasters

The combination of the IoD and blockchain technology can significantly improve disaster prevention and recovery efforts, contributing to efficient and effective management enhancement while simultaneously ensuring transparency and accountability. Drones assist in coordinating resources, tracking data, and supporting survivors in times of crisis, ultimately reducing the impact of natural disasters [214], combined with decentralized solutions, such as smart contracts for resource allocation, based on predefined criteria. Thanks to their various sensors, such as cameras with thermal optics, they can collect real-time data related to information on the extent of damage, weather conditions, and the presence of hazards such as fires or floods in disaster-affected areas, as well as the detection of survivors. The data collected during search-and-rescue operations are securely recorded on the blockchain, aiding coordination efforts among rescue teams, especially through the immutable features of timestamps, to ensure when and where the data were registered in the ledger [219]. As a result, drones can be used to assess long-term recovery needs in the context of post-disaster recovery, such as infrastructure repair, environmental restoration, and rebuilding efforts. The blockchain records data related to recovery projects, ensuring transparency in resource allocation and project progress [220].

7.4. Charging/Refueling Stations

The charging and refueling stations for drones, often referred to as drone hubs or drone service centers, play a crucial role in enabling the sustainable operation of drones, especially in applications such as package delivery, aerial inspections, surveillance, and more [221]. Essentially, drone stations can serve as logistical hubs for managing the movement of drones, their payloads, and supplies, including storage, sorting, and dispatching of drones for various missions, while incorporating sustainability practices such as renewable energy sources and environmentally friendly refueling options for drones. Blockchain can provide a secure platform for processing the respective transactions for fueling services and their recording, by ensuring transparency through automated smart contracts depending on the required service [222], while having proven useful for information exchange between the drone and established ledgers, ensuring data integrity and security with regard to the amount of purchased energy, the amount spent, and information on the charged drone [19]. From the refueling perspective, blockchain can record data on emissions produced during the fueling process and verify the authenticity and quality of the station's utilized fuel, ensuring that it meets quality standards, while in terms of charging stations, data on the energy efficiency of charging equipment can be recorded on the ledger, helping consumers to filter their available options on stations that use energy-efficient technology. For both cases, data related to the maintenance and status of the charging or refueling equipment can be recorded on the blockchain, ensuring that the equipment is well maintained and reducing the risk of service disruptions [223]. Blockchain can also facilitate the integration of smart grid practices by allowing proper load balancing and grid optimization for drones to access only the required amount of resources, as well as accessing available charging or fueling resources from other users in a decentralized network.

7.5. Agriculture

The synergy of the IoD and blockchain in agriculture can revolutionize the industry by enhancing efficiency, transparency, and sustainability, offering benefits such as improved crop yields, reduced resource wastage, supply chain transparency, and enhanced sustainability. Specifically, significant contributions in agriculture include the following [34]: (a) Drones equipped with various sensors, including multispectral cameras and LiDAR, can monitor crop health, detect diseases, and assess nutrient levels, with collected data being recorded on the blockchain through smart contracts to automate tasks such as planting, harvesting, and irrigation, optimizing resource usage and enabling decision-making tasks about irrigation and fertilization. (b) In terms of soil conditions and overall health, drones equipped with soil sensors can assess soil quality, moisture levels, and nutrient contents, as well as identifying and monitoring pests and diseases, with the respective data about locations and health status being recorded on the blockchain, allowing for precise soil and water management. (c) Taking into consideration weather conditions, drones can provide real-time weather data, such as temperature, humidity, wind speed, and precipitation. This information can be shared on the blockchain to support weather forecasting and agricultural planning. (d) Also, drones can be used to assess carbon sequestration and reduce emissions that are generated by traditional farming practices. The corresponding data can be recorded on the blockchain for carbon credit trading [5,45,224]. (e) Finally, drones can be used for transparent monitoring of agricultural supply chains, from planting to the delivery of products, with the related data being registered in an immutable record to ensure product authenticity and quality for relevant stakeholders while automating transactions and providing access to decentralized markets [225].

7.6. Transportation

The corresponding synergy can have a profound impact on various aspects of transportation, including logistics, offering additional safety, increasing transparency, and preventing fraud actions. Drones equipped with sensors and cameras can inspect the condition of vehicles, detecting urgent maintenance needs or damage. The data collected can be stored on the blockchain as a personal maintenance record, with private data on the driver's identity and vehicle information remaining secure and accessible only to the parties responsible, e.g., mechanics, technicians, and corporate owners. Another case of transportation, related to delivery services, enables the utilization of drones for delivering parcels and cargo across specified locations, with the possibility of malfunctions or physical damage occurring during the process [14]. Due to blockchain's integrity, insurance companies have the ability to verify the conditions and reasons for the malfunctions, in order to proceed into further damage assessments [5] while ensuring the reliability of data. In addition, smart contracts on the blockchain can automate cargo insurance claims based on predefined criteria, reducing additional administrative overheads [226].

7.7. Media

The media industry can gain significant enhancements in various aspects of content creation, distribution, and consumption, offering simultaneous content protection, copyright management, decentralized distribution of the generated content, and efficient monetization processes, while benefiting content creators, consumers, and the industry as a whole. Drones equipped with high-quality cameras can capture aerial footage and images, providing unique perspectives for news reporting, documentaries, and entertainment [227]. These media assets can be securely recorded on the blockchain to ensure authenticity and copyright protection, while blockchain-based platforms enable content creators to distribute their captured content directly to their audience, reducing the influence of intermediaries and ensuring proper licensing and distribution. In addition, smart contracts can automate content licensing, royalty payments, and sponsorship agreements, ensuring that content creators are compensated fairly for the use of their work and sponsors receive fair exposure [228]. Additionally, blockchain can facilitate fact-checking and data verification for media reporting, information, and content captured by drones, enabling media organizations to create decentralized archives of historical content, preserving it for future generations, while utilizing the records of content ownership stored in the respective data blocks for piracy prevention [5,229]. Table 6 summarizes the collection of references that were investigated for the analysis of potential use cases, based on the blockchain–IoD union.

Table 6. Investigated references on potential use cases based on the IoD–blockchain union.

Investigated References	IoD–Blockchain Use Cases
[45,200–205]	Integration of blockchain within IoD devices
[206–211]	Supply chain within blockchain and the IoD
[211–218]	Health chain within blockchain and the IoD
[214,219,220]	Natural disasters within blockchain and the IoD
[221–224]	Charging/refueling stations within blockchain and the IoD
[5,34,45,224,227]	Agriculture within blockchain and the IoD
[5,14,228]	Transportation within blockchain and the IoD
[227–229]	Media within blockchain and the IoD

8. Discussion and Open Issues

Despite the benefits of the IoD and blockchain, combined with the valuable contributions of underpinning technologies, many challenges emerge at different levels, such as increased computational costs, latency, and potential security gaps. For example, blockchain is considered to be an emerging technology that faces adaptation difficulties due to its conventional architecture, as it builds trust in trustless environments using a consensus mechanism, involves numerous network communications for the synchronization of P2P networks and, due to the constant addition of new data blocks across the network of interest, may be considered uncontrollable [6].

On the other hand, due to the mobility and energy constraints of UAVs, application circumstances and conditions face additional challenges, such as deployment, required energy consumption, data transmission (communication), security, and privacy [230]. As drones become more prevalent and collect a rising number of data, it is essential to guarantee the protection and responsible utilization of the resulting information [12].

However, although blockchain provides a secure platform for storing and sharing data, the lack of clear guidelines and policies to govern the use of this technology is visible. Therefore, all of these challenges signify the importance of developing an IoD environment with the inclusion of blockchain features in order to fully complement each other and tackle the corresponding challenges with this particular combination [118]. Overcoming these challenges is essential to successfully harness the full potential of the IoD and blockchain, enabling a wide range of applications in various fields. A detailed list of such challenges, with indicative suggested approaches to their resolution, is presented below.

8.1. Security and Privacy

The challenges and open issues that derive from IoD–blockchain integration and are related to security and privacy aspects are listed below:

I. Access control and authentication of UAVs can fail with affected and centralized authentication methods. Thus, secure decentralized communications among drones, and between drones and GSS, should be ensured [16].

II. Due to the lack of robust communication between devices, blockchain should be combined with solutions such as 5G-enabled IoD, utilization of multiple signatures, and smart contracts [231].

III. Regarding security and privacy issues of blockchain in 5G-based IoD environments, a more robust blockchain, in terms of security, would improve data management between communicating entities in the IoD [70].

IV. Although cryptographic functions and a consensus mechanism are available in blockchain, insurance of the integrity of the drone-collected data and the processing rate of transactions are limited. Thus, it would be useful to expand the throughput and develop mechanisms that will support the participation derived by multiple entities [232].

V. Blockchain preserves the privacy of users and drone owners through the implementation of pseudo-random identities. However, transaction data are visible to all participants. A potential solution would be the development of novel encryption methods that prevent correlations with previous data blocks [232].

VI. The development of powerful security protocols enhanced with blockchain cryptographic features will tackle repeated attacks, such as man-in-the-middle infiltrations taking place in the computing environment of the IoD, providing low computational and communication costs [233].

VII. Lack of security and privacy during the design stage requires the construction of suitable strategies, including the forensic mechanism to eliminate attacks, as well as tracing and reconstructing attack events [234].

8.2. Data Communication

The challenges and open issues that derive from IoD–blockchain integration and are related to data communication aspects are listed below:

I. Lack of security mechanisms for cyber–physical systems to guarantee the secure transmission of information between drones, requiring the development of mechanisms focused on the verification of registrations and transactions within the integrated blockchain. Deep Learning approaches are an ideal solution for the protection of flight paths during the exchange of data between drones and GCSs [118].

II. Lack of security of unmanned traffic management in the IoD, requiring mechanisms providing secure and unalterable traffic data between drones and GCSs. A potential solution is logging the respective data into immutable decentralized ledgers [153].

III. The lack of the node's memory in terms of data storage is conflicting due to the constant growth of data blocks being correlated with each other, along with the storage required for the drone to collect the predefined data, resulting in the requirement of additional memory space. Hence, consideration of the node's data storage requirements is essential [235].

IV. In the context of the IoD, many drones collect a vast amount of data. Thus, data collection and storage among a sufficient number of blockchain nodes for load sharing would be a potential solution. The development of aggregation schemes is required to ensure data security, energy efficiency, and reduced communication costs with integrated encryption techniques that can be used to provide confidentiality and access control of data [12].

8.3. Autonomy

The challenges and open issues that derive from IoD–blockchain integration and are related to autonomy aspects are listed below:

I. The lack of reliable infrastructure for an autonomous IoD is tackled by the utilization of decentralized tools for designing and developing IoD solutions. Hence, drone-based autonomous systems will ensure security and safety in the operating phase, avoiding risks and preventing mishaps [236].

II. Avoidance of functionality errors caused by faulty devices is achieved through the development of a decentralized mechanism capable of monitoring malfunctions distributed in the interconnected IoD nodes, along with the comparison of different traditional architectures, to reduce the overall operational time and increase maintenance quality [237].

III. There is a significant lack of drone operational control, causing demotivation of the relevant stakeholders. Thus, the creation of platforms with dedicated anti-spoofing tools, as well as related smart contracts with specific conditions, would improve the overall protection of the IoD system [238].

IV. Energy efficiency is a big challenge due to the requirements for data processing, storage, transmission, and operation of blockchain functionalities. An efficient solution would be the development and adoption of smart systems capable of supplementing the existing IoD solutions for minimal energy consumption [38].

8.4. Wireless Communications/Networking

The challenges and open issues that derive from IoD–blockchain integration and are related to wireless communications and networking aspects are listed below:

I. Security and privacy challenges regarding the broadcasting of wireless communications result in important vulnerability of UAVs. The contribution of enabling technologies, such as AI and blockchain for the design of intelligent decentralized drones, would assist in the overall data security and privacy in different communication layers while controlling and monitoring the operational flow of the IoD system [36].

II. Challenges related to the lack of network maintenance services are tackled with the development of protocols and the distribution of resource allocations. Additional indicative solutions include the availability of models that efficiently monitor and calculate the performance of multi-core CPUs, effective utilization of the related communication channels, distribution of information to the main data storage, and secure blockchain ledgers [239].

III. There is a high possibility of data loss or reception of false data by other nodes, as well as routing issues in the interconnection of drones and IoD networks. To tackle these challenges, a standardized policy and suitable communication protocols should be developed for the utilization of authorized components and effective interconnection and data sharing of the installed sensors, so as to successfully submit the collected data to the integrated blockchain solution [240].

IV. Network communication issues such as high throughput, latency, and delay, due to low-quality hardware components, require solutions that implement IoT infrastructures with smart routing features and integrated 5G networks [240].

V. Due to the lack of upgraded platforms supporting 5G communication networks and AI, the development of novel architectures with decentralized features would ensure the increase in network capacity, communication safety, privacy, and cost reduction for transaction storage [241].

8.5. Regulation and Fairness

The challenges and open issues that derive from IoD–blockchain integration and are related to regulation and fairness aspects are listed below:

I. Security: Different regulatory frameworks lead to uncertainty in terms of researching and leveraging the potentiality of drones and blockchain, as well as lack of access control leading to unfairness in blockchain adaptation. Governments and industry stakeholders should be proactive in developing clear and consistent regulations to accommodate the rapid development and deployment of drones and blockchain technologies [237].

II. Unfair mining issues may lead to further conflicts among stakeholders, with the risk of the blockchain of one party being considered as valid, while others, although legitimate, are identified as invalid. Thus, specific mining metric evaluation models would support the prevention of unfair treatment [242].

8.6. Architecture and Deployment

The challenges and open issues that derive from IoD–blockchain integration and are related to architecture and deployment aspects are listed below:

I. Lack of intelligent techniques to detect possible attacks is a significant challenge. The potential scheme's design will offer cutting-edge solutions for detecting attacks, as well as prevention measures. A suitable mechanism will isolate an attack in real time to reduce localization error, return the drone to its core GS in the case of disconnection, and prevent the collapse of the entire network [37].

II. Due to ongoing technological evolution, more complex attacks appear. However, since the IoD and blockchain incorporate additional technologies, the implementation of AI-based mechanisms mitigates this challenge by using neural networks, Deep Learning, and Machine Learning algorithms to optimize the security and privacy of the IoD network [243].

III. High computational and communication costs remain challenging. However, the IoD architecture may contain devices from the Mobile Edge Computing (MEC) domain, facilitating quicker and more effective communication by offloading messages to the closest verified MEC device for processing. This suggests a decrease in computing costs as well [37].

IV. The lack of reliable real-time detection of obstacles can lead to physical damage to the drone or civil properties due to collisions. Therefore, the development of avoidance mechanisms for the early identification of obstacles would be sufficient [244].

V. Deployment of drones related to the covering area and the completion of the scheduled task requires the programming and training of several UAVs, as well as distributing a suitable number of blockchain nodes to support the decentralized IoD system. Thus, the development of a suitable mechanism focusing on the mobility/trajectory motion to mitigate interference and collision issues would be a sufficient solution [34].

VI. Due to frequent point-to-point network updates and traffic congestion, a noticeable depletion is generated, leading to the prolonged latency of the network. To avoid such implications, enhanced architectures would allow drones to have access to their own assigned data blocks [245].

VII. Authentication schemes suffer from real-time latencies and are vulnerable to potential attacks. Thus, the establishment of a system that performs automated authentication in specific flight zones, with the respective coordinates being registered in a dedicated ledger, would enhance security countermeasures against potential infiltrations [246].

9. Conclusions

This paper researched the technological concept of the IoD, as well as the core principles of blockchain, aiming towards the proper investigation of the potential synergy of the two technologies.

The results of our analysis present the significant impact of blockchain technology as an active component of IoD systems, escaping the traditional utilization of decentralized mechanisms for security purposes, with the option of incorporating additional technologies, e.g., AI or computing variations, to further supplement requirements such as automation, task allocation for efficiency, and improved transmission rates.

Through the investigation of the indicative use cases implementing the corresponding synergy, certain common and impactful features were realized. Initially, drones provide flexible mobility and the collection of different types of data, such as multimedia and numerical data. Simultaneously, integrated blockchain-based frameworks with distributed nodes within the IoD infrastructure and components ensure immutable data processing and storage characteristics. As a whole, the resulting solutions enable secure cryptographic, authenticated, and real-time sharing among the related stakeholders, while validating the value of the captured data.

Regarding proposed future guidelines on the topic, further research on important open issues is required. Significant examples are related to solutions for efficient resource allocation in terms of energy consumption, costs, and computing processes, since both technologies are considered to be individually highly demanding, guaranteeing interconnection between the IoD system and the decentralized ledger, as well as utilizing blockchain data for coordinating aerial tasks of the drones.

Author Contributions: Conceptualization, K.A.T.; methodology, K.A.T. and K.V.; formal analysis, K.A.T. and K.V.; investigation, K.A.T.; resources, K.A.T.; data curation, K.A.T. and K.V.; writing—original draft preparation, K.A.T.; writing—review and editing, K.A.T. and T.L.; visualization, K.A.T. and K.V.; supervision, T.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: This work was supported by the MPhil program "Advanced Technologies in Informatics and Computers", hosted by the Department of Computer Science, Democritus University of Thrace, 65404 Kavala, Greece.

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

References

1. Kang, J.H.; Park, K.J.; Kim, H. Analysis of localization for drone-fleet. In Proceedings of the Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 28–30 October 2015; pp. 533–538. [CrossRef]
2. Gharibi, M.; Boutaba, R.; Waslander, S.L. Internet of Drones. *IEEE Access* **2016**, *4*, 1148–1162. [CrossRef]
3. D'Andrea, R. Guest Editorial Can Drones Deliver? *IEEE Trans. Autom. Sci. Eng.* **2014**, *11*, 647–648. [CrossRef]
4. Harbi, Y.; Medani, K.; Gherbi, C.; Senouci, O.; Aliouat, Z.; Harous, S. A Systematic Literature Review of Blockchain Technology for Internet of Drones Security. *Arab. J. Sci. Eng.* **2023**, *48*, 1053–1074. [CrossRef] [PubMed]
5. Singh, M.P.; Aujla, G.S.; Bali, R.S. Blockchain for the Internet of Drones: Applications, Challenges, and Future Directions. *IEEE Internet Things Mag.* **2021**, *4*, 47–53. [CrossRef]
6. Alzahrani, B.; Oubbati, O.S.; Barnawi, A.; Atiquzzaman, M.; Alghazzawi, D. UAV assistance paradigm: State-of-the-art in applications and challenges. *J. Netw. Comput. Appl.* **2020**, *166*, 102706. [CrossRef]
7. Hall, R.J. An Internet of Drones. *IEEE Internet Comput.* **2016**, *20*, 68–73. [CrossRef]
8. Stankovic, J.A. Research Directions for the Internet of Things. *IEEE Internet Things J.* **2014**, *1*, 3–9. [CrossRef]
9. Choudhary, G.; Sharma, V.; Gupta, T.; Kim, J.; You, I. Internet of Drones (IoD): Threats, Vulnerability, and Security Perspectives. *Res. Briefs Inf. Commun. Technol. Evol.* **2018**, *4*, 64–77. [CrossRef]
10. Nguyen, H.P.D.; Nguyen, D.D. Drone Application in Smart Cities: The General Overview of Security Vulnerabilities and Countermeasures for Data Communication. In *Development and Future of Internet of Drones (IoD): Insights, Trends, and Road Ahead*; Krishnamurthi, R., Nayyar, A., Hassanien, A.E., Eds.; Studies in Systems, Decision and Control; Springer International Publishing: Cham, Switzerland, 2021; Volume 332, pp. 185–210. [CrossRef]
11. Boccadoro, P.; Striccoli, D.; Grieco, L.A. An extensive survey on the Internet of Drones. *Ad Hoc Networks* **2021**, *122*, 102600. [CrossRef]
12. Abdelmaboud, A. The Internet of Drones: Requirements, Taxonomy, Recent Advances, and Challenges of Research Trends. *Sensors* **2021**, *21*, 5718. [CrossRef]
13. Lin, C.; He, D.; Kumar, N.; Choo, K.-K.R.; Vinel, A.; Huang, X. Security and Privacy for the Internet of Drones: Challenges and Solutions. *IEEE Commun. Mag.* **2018**, *56*, 64–69. [CrossRef]
14. Abualigah, L.; Diabat, A.; Sumari, P.; Gandomi, A.H. Applications, Deployments, and Integration of Internet of Drones (IoD): A Review. *IEEE Sensors J.* **2021**, *21*, 25532–25546. [CrossRef]
15. Bera, B.; Chattaraj, D.; Das, A.K. Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment. *Comput. Commun.* **2020**, *153*, 229–249. [CrossRef]
16. Sharma, B.; Srivastava, G.; Lin, J.C.-W. A bidirectional congestion control transport protocol for the internet of drones. *Comput. Commun.* **2020**, *153*, 102–116. [CrossRef]
17. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain Technology Overview. *arXiv* **2019**, arXiv:1906.11078.
18. Golosova, J.; Romanovs, A. The Advantages and Disadvantages of the Blockchain Technology. In Proceedings of the 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), Vilnius, Lithuania, 8–10 November 2018; pp. 1–6.
19. Alkadi, R.; Alnuaimi, N.; Shoufan, A.; Yeun, C. Blockchain Interoperability in UAV Networks: State-of-the-art and Open Issues. *arXiv* **2021**, arXiv:2111.09529.

20. Harbi, Y.; Aliouat, Z.; Refoufi, A.; Harous, S. Recent Security Trends in Internet of Things: A Comprehensive Survey. *IEEE Access* **2021**, *9*, 113292–113314. [CrossRef]
21. Yampolskiy, M.; Horvath, P.; Koutsoukos, X.D.; Xue, Y.; Sztipanovits, J. Taxonomy for description of cross-domain attacks on CPS. In Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems, Philadelphia, PA, USA, 9–11 April 2013; pp. 135–142.
22. Akram, R.N.; Markantonakis, K.; Mayes, K.; Habachi, O.; Sauveron, D.; Steyven, A.; Chaumette, S. Security, privacy and safety evaluation of dynamic and static fleets of drones. In Proceedings of the 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), St. Petersburg, FL, USA, 17–21 September 2017; pp. 1–12.
23. Javaid, A.Y.; Sun, W.; Devabhaktuni, V.K.; Alam, M. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In Proceedings of the 2012 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 13–15 November 2012; pp. 585–590.
24. Mansfield, K.; Eveleigh, T.; Holzer, T.H.; Sarkani, S. Unmanned aerial vehicle smart device ground control station cyber security threat model. In Proceedings of the 2013 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 12–14 November 2013; pp. 722–728.
25. Jain, A.; Singhal, P. Fog computing: Driving force behind the emergence of edge computing. In Proceedings of the 2016 International Conference System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 25–27 November 2016; pp. 294–297.
26. Chen, Y.-J.; Wang, L.-C. Privacy Protection for Internet of Drones: A Network Coding Approach. *IEEE Internet Things J.* **2019**, *6*, 1719–1730. [CrossRef]
27. Biswas, A.R.; Giaffreda, R. IoT and cloud convergence: Opportunities and challenges. In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Republic of Korea, 6–8 March 2014; pp. 375–376.
28. Al-Turjman, F.; Zahmatkesh, H. A Comprehensive Review on the Use of AI in UAV Communications: Enabling Technologies, Applications, and Challenges. In *Unmanned Aerial Vehicles in Smart Cities*; Al-Turjman, F., Ed.; *Unmanned System Technologies*; Springer International Publishing: Cham, Switzerland, 2020; pp. 1–26. [CrossRef]
29. Sobb, T.; Turnbull, B.; Moustafa, N. Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions. *Electronics* **2020**, *9*, 1864. [CrossRef]
30. Taherdoost, H. A Critical Review of Blockchain Acceptance Models—Blockchain Technology Adoption Frameworks and Applications. *Computers* **2022**, *11*, 24. [CrossRef]
31. McEnroe, P.; Wang, S.; Liyanage, M. A Survey on the Convergence of Edge Computing and AI for UAVs: Opportunities and Challenges. *IEEE Internet Things J.* **2022**, *9*, 15435–15459. [CrossRef]
32. Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141. [CrossRef]
33. Wazid, M.; Das, A.K.; Lee, J.-H. Authentication protocols for the internet of drones: Taxonomy, analysis and future directions. *J. Ambient. Intell. Humaniz. Comput.* **2018**, 1–10. [CrossRef]
34. Yang, W.; Wang, S.; Yin, X.; Wang, X.; Hu, J. A Review on Security Issues and Solutions of the Internet of Drones. *IEEE Open J. Comput. Soc.* **2022**, *3*, 96–110. [CrossRef]
35. Hema, N.; Sharma, M. Smart Agriculture Using IoD: Insights, Trends and Road Ahead. In *Development and Future of In-ternet of Drones (IoD): Insights, Trends and Road Ahead*; Krishnamurthi, R., Nayyar, A., Hassanien, A.E., Eds.; Studies in Systems, Decision and Control; Springer International Publishing: Cham, Switzerland, 2021; Volume 332, pp. 79–107. [CrossRef]
36. Alladi, T.; Chamola, V.; Sahu, N.; Guizani, M. Applications of blockchain in unmanned aerial vehicles: A review. *Veh. Commun.* **2020**, *23*, 100249. [CrossRef]
37. Yahuza, M.; Idris, M.Y.I.; Bin Ahmedy, I.; Wahab, A.W.B.A.; Nandy, T.; Noor, N.M.; Bala, A. Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges. *IEEE Access* **2021**, *9*, 57243–57270. [CrossRef]
38. Ilgi, G.S.; Ever, Y.K. Critical analysis of security and privacy challenges for the Internet of drones: A survey. In *Drones in Smart-Cities*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 207–214. [CrossRef]
39. Chen, J.; Wang, W.; Zhou, Y.; Ahmed, S.H.; Wei, W. Exploiting 5G and Blockchain for Medical Applications of Drones. *IEEE Netw.* **2021**, *35*, 30–36. [CrossRef]
40. Arai, K.; Bhatia, R.; Kapoor, S. (Eds.) *Advances in Intelligent Systems and Computing*; Springer International Publishing: Cham, Switzerland, 2019; Volume 881, pp. 1037–1058. [CrossRef]
41. Ahanger, T.A.; Aldaej, A.; Atiquzzaman, M.; Ullah, I.; Yousufudin, M. Distributed Blockchain-Based Platform for Unmanned Aerial Vehicles. *Comput. Intell. Neurosci.* **2022**, *2022*, 4723124. [CrossRef]
42. Hassija, V.; Chamola, V.; Agrawal, A.; Goyal, A.; Luong, N.C.; Niyato, D.; Yu, F.R.; Guizani, M. Fast, Reliable, and Secure Drone Communication: A Comprehensive Survey. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 2802–2832. [CrossRef]
43. Heidari, A.; Navimipour, N.J.; Unal, M.; Zhang, G. Machine Learning Applications in Internet-of-Drones: Systematic Review, Recent Deployments, and Open Issues. *ACM Comput. Surv.* **2023**, *55*, 1–45. [CrossRef]
44. Kang, J.; Xiong, Z.; Niyato, D.; Xie, S.; Kim, D.I. Securing data sharing from the sky: Integrating blockchains into drones in 5G and beyond. *IEEE Netw.* **2021**, *35*, 78–85. [CrossRef]

45. Taherdoost, H. Blockchain Technology and Artificial Intelligence Together: A Critical Review on Applications. *Appl. Sci.* **2022**, *12*, 12948. [CrossRef]
46. Zhu, C.; Zhu, X.; Ren, J.; Qin, T. Blockchain-Enabled Federated Learning for UAV Edge Computing Network: Issues and Solutions. *IEEE Access* **2022**, *10*, 56591–56610. [CrossRef]
47. Renu; Sharma, S.; Saxena, S. Blockchain and UAV: Security, Challenges and Research Issues. In Proceedings of the UASG 2019, Melbourne, Australia, 12–24 April 2019; Jain, K., Khoshelham, K., Zhu, X., Tiwari, A., Eds.; Lecture Notes in Civil Engineering. Springer International Publishing: Cham, Switzerland, 2020; Volume 51, pp. 99–107. [CrossRef]
48. Kitchenham, B. *Procedures for Performing Systematic Reviews*; Keele University: Keele, UK, 2004.
49. Solanki, A.; Tarar, S.; Singh, S.P.; Tayal, A. (Eds.) *The Internet of Drones: AI Applications for Smart Solutions*; CRC Press: Boca Raton, FL, USA, 2022.
50. Zhang, P.; Wang, C.; Qin, Z.; Cao, H. A multidomain virtual network embedding algorithm based on multiobjective optimization for Internet of Drones architecture in Industry 4.0. *Softw. Pract. Exp.* **2022**, *52*, 710–728. [CrossRef]
51. Choudhary, G.; Sharma, V.; You, I. Sustainable and secure trajectories for the military Internet of Drones (IoD) through an efficient Medium Access Control (MAC) protocol. *Comput. Electr. Eng.* **2019**, *74*, 59–73. [CrossRef]
52. Koubâa, A.; Qureshi, B.; Sriti, M.-F.; Allouch, A.; Javed, Y.; Alajlan, M.; Cheikhrouhou, O.; Khalgui, M.; Tovar, E. Dronemap Planner: A service-oriented cloud-based management system for the Internet-of-Drones. *Ad Hoc Netw.* **2019**, *86*, 46–62. [CrossRef]
53. Sanchez-Garcia, J.; Garcia-Campo, J.M.; Arzamendia, M.; Reina, D.G.; Toral, S.L.; Gregor, D. A survey on unmanned aerial and aquatic vehicle multi-hop networks: Wireless communications, evaluation tools and applications. *Comput. Commun.* **2018**, *119*, 43–65. [CrossRef]
54. Bousbaa, F.Z.; Kerrache, C.A.; Mahi, Z.; Tahari, A.E.K.; Lagraa, N.; Yagoubi, M.B. GeoUAVs: A new geocast routing protocol for fleet of UAVs. *Comput. Commun.* **2020**, *149*, 259–269. [CrossRef]
55. Ren, M.; Fu, X.; Pace, P.; Aloi, G.; Fortino, G. Collaborative Data Acquisition for UAV-Aided IoT Based on Time-Balancing Scheduling. *IEEE Internet Things J.* **2024**, *11*, 13660–13676. [CrossRef]
56. Huang, X.; Fu, X. Fresh Data Collection for UAV-Assisted IoT Based on Aerial Collaborative Relay. *IEEE Sensors J.* **2023**, *23*, 8810–8825. [CrossRef]
57. Lagkas, T.; Argyriou, V.; Bibi, S.; Sarigiannidis, P. UAV IoT Framework Views and Challenges: Towards Protecting Drones as "Things". *Sensors* **2018**, *18*, 4015. [CrossRef]
58. Vallejo, D.; Castro-Schez, J.; Glez-Morcillo, C.; Albusac, J. Multi-agent architecture for information retrieval and intelligent monitoring by UAVs in known environments affected by catastrophes. *Eng. Appl. Artif. Intell.* **2020**, *87*, 103243. [CrossRef]
59. López, J.; Royo, P.; Pastor, E.; Barrado, C.; Santamaria, E. A middleware architecture for unmanned aircraft avionics. In Proceedings of the ACM/IFIP/USENIX International Conference on Middleware Companion, Newport Beach, CA, USA, 26–30 November 2007; pp. 1–6.
60. Ribeiro, J.P.; Fontes, H.; Lopes, M.; Silva, H.; Campos, R.; Almeida, J.M.; Silva, E. UAV cooperative perception based on DDS communications network. In Proceedings of the OCEANS 2017-Anchorage, Anchorage, AK, USA, 18–27 September 2017; pp. 1–8.
61. Aggarwal, S.; Shojafar, M.; Kumar, N.; Conti, M. A New Secure Data Dissemination Model in Internet of Drones. In Proceedings of the IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019.
62. Xu, S.; Doğançay, K.; Hmam, H. Distributed pseudolinear estimation and UAV path optimization for 3D AOA target tracking. *Signal Process.* **2017**, *133*, 64–78. [CrossRef]
63. Mohamed, N.; Al-Jaroodi, J.; Jawhar, I.; Idries, A.; Mohammed, F. Unmanned aerial vehicles applications in future smart cities. *Technol. Forecast. Soc. Chang.* **2020**, *153*, 119293. [CrossRef]
64. Sharma, A.; Vanjani, P.; Paliwal, N.; Basnayaka, C.M.; Jayakody, D.N.K.; Wang, H.-C.; Muthuchidambaranathan, P. Communication and networking technologies for UAVs: A survey. *J. Netw. Comput. Appl.* **2020**, *168*, 102739. [CrossRef]
65. Wang, J.; Liu, Y.; Niu, S.; Song, H.; Jing, W.; Yuan, J. Blockchain enabled verification for cellular-connected unmanned aircraft system networking. *Futur. Gener. Comput. Syst.* **2021**, *123*, 233–244. [CrossRef]
66. Yang, G.; Lin, X.; Li, Y.; Cui, H.; Xu, M.; Wu, D.; Rydén, H.; Redhwan, S.B. A Telecom Perspective on the Internet of Drones: From LTE-Advanced to 5G. *arXiv* **2018**, arXiv:1803.11048. [CrossRef]
67. Rahman, M.F.B.A. *Smart CCTVS for Secure Cities: Potentials and Challenges*; Rajaratnam School of International Studies: Singapore, 2017.
68. Nikooghadam, M.; Amintoosi, H.; Islam, S.H.; Moghadam, M.F. A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance. *J. Syst. Arch.* **2021**, *115*, 101955. [CrossRef]
69. Ko, Y.; Kim, J.; Duguma, D.G.; Astillo, P.V.; You, I.; Pau, G. Drone Secure Communication Protocol for Future Sensitive Applications in Military Zone. *Sensors* **2021**, *21*, 2057. [CrossRef] [PubMed]
70. Bera, B.; Saha, S.; Das, A.K.; Kumar, N.; Lorenz, P.; Alazab, M. Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment. *IEEE Trans. Veh. Technol.* **2020**, *69*, 9097–9111. [CrossRef]
71. Ayamga, M.; Akaba, S.; Nyaaba, A.A. Multifaceted applicability of drones: A review. *Technol. Forecast. Soc. Chang.* **2021**, *167*, 120677. [CrossRef]
72. Wazid, M.; Das, A.K.; Kumar, N.; Vasilakos, A.V.; Rodrigues, J.J.P.C. Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment. *IEEE Internet Things J.* **2019**, *6*, 3572–3584. [CrossRef]

73. Srinivas, J.; Das, A.K.; Kumar, N.; Rodrigues, J.J.P.C. TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment. *IEEE Trans. Veh. Technol.* **2019**, *68*, 6903–6916. [CrossRef]
74. Alsamhi, S.H.; Ma, O.; Ansari, M.S.; Almalki, F.A. Survey on Collaborative Smart Drones and Internet of Things for Improving Smartness of Smart Cities. *IEEE Access* **2019**, *7*, 128125–128152. [CrossRef]
75. Zhi, Y.; Fu, Z.; Sun, X.; Yu, J. Security and Privacy Issues of UAV: A Survey. *Mob. Netw. Appl.* **2020**, *25*, 95–101. [CrossRef]
76. Das, A.K.; Bera, B.; Wazid, M.; Jamal, S.S.; Park, Y. iGCACS-IoD: An Improved Certificate-Enabled Generic Access Control Scheme for Internet of Drones Deployment. *IEEE Access* **2021**, *9*, 87024–87048. [CrossRef]
77. Yaacoub, J.-P.; Noura, H.; Salman, O.; Chehab, A. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet Things* **2020**, *11*, 100218. [CrossRef] [PubMed]
78. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 2702–2733. [CrossRef]
79. Mitka, E.; Mouroutsos, S.G. Classification of Drones. *Am. J. Eng. Res.* **2017**, *6*, 36–41.
80. Dahlman, E.; Lagrelius, K. A Game of Drones: Cyber Security in UAVs. 2019. Available online: https://www.semanticscholar.org/paper/A-Game-of-Drones-:-Cyber-Security-in-UAVs-Dahlman-Lagrelius/3119bc3f5f4282210ab46a25ce86b3c6124b26d5 (accessed on 10 April 2024).
81. Nandy, T.; Bin Idris, M.Y.I.; Noor, R.M.; Ahmedy, I.; Bhattacharyya, S. An Enhanced Two-factor Authentication Protocol for V2V Communication in VANETs. In Proceedings of the 3rd International Conference on Information Science and System, Cambridge, UK, 19–22 March 2020.
82. Abdelhafez, A.A.M.A. Localization of Cyber-Physical Systems: Privacy, Security and Efficiency. Doctoral Dissertation, Technische Universität München, Munich, Germany, 2020.
83. Giray, S.M. Anatomy of unmanned aerial vehicle hijacking with signal spoofing. In Proceedings of the 2013 6th International Conference on Recent Advances in Space Technologies (RAST), Istanbul, Turkey, 12–14 June 2013; pp. 795–800.
84. Bhattacharya, S.; Başar, T. Game-theoretic analysis of an aerial jamming attack on a UAV communication network. In Proceedings of the 2010 American Control Conference (ACC 2010), Baltimore, MD, USA, 30 June–2 July 2010; pp. 818–823.
85. Rudinskas, D.; Goraj, Z.; Stankūnas, J. Security analysis of UAV radio communication system. *Aviation* **2009**, *13*, 116–121. [CrossRef]
86. Chen, W.; Dong, Y.; Duan, Z. Manipulating Drone Position Control. In Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 10–12 June 2019; pp. 1–9.
87. Alajmi, N.M.; Elleithy, K.M. Comparative analysis of selective forwarding attacks over Wireless Sensor Networks. *Int. J. Comput. Appl.* **2015**, *111*, 27–38. [CrossRef]
88. Samanth, S.; Prema, K.V.; Balachandra, M. Security in Internet of Drones: A Comprehensive Review. *Cogent Eng.* **2022**, *9*, 2029080. [CrossRef]
89. He, D.; Chan, S.; Guizani, M. Drone-Assisted Public Safety Networks: The Security Aspect. *IEEE Commun. Mag.* **2017**, *55*, 218–223. [CrossRef]
90. Vattapparamban, E.; Güvenç, I.; Yurekli, A.I.; Akkaya, K.; Uluagac, S. Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In Proceedings of the 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), Paphos, Cyprus, 5–9 September 2016; pp. 216–221.
91. Arteaga, S.P.; Hernandez, L.A.M.; Perez, G.S.; Orozco, A.L.S.; Villalba, L.J.G. Analysis of the GPS Spoofing Vulnerability in the Drone 3DR Solo. *IEEE Access* **2019**, *7*, 51782–51789. [CrossRef]
92. Sciancalepore, S.; Ibrahim, O.A.; Oligeri, G.; Di Pietro, R. PiNcH: An effective, efficient, and robust solution to drone detection via network traffic analysis. *Comput. Networks* **2020**, *168*, 107044. [CrossRef]
93. Perazzo, P.; Ariyapala, K.; Conti, M.; Dini, G. The verifier bee: A path planner for drone-based secure location verification. In Proceedings of the 2015 IEEE 16th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Boston, MA, USA, 14–17 June 2015; pp. 1–9.
94. Chen, W.; Dong, Y.; Duan, Z. Compromising Flight Paths of Autopiloted Drones. In Proceedings of the 2019 International Conference on Unmanned Aircraft Systems (ICUAS), Atlanta, GA, USA, 11–14 June 2019; pp. 1316–1325.
95. Son, Y.; Shin, H.; Kim, D.; Park, Y.; Noh, J.; Choi, K.; Choi, J.; Kim, Y. Rocking drones with intentional sound noise on gyroscopic sensors. In Proceedings of the 24th USENIX Security Symposium (USENIX Security 15), Washington, DC, USA, 12–14 August 2015; pp. 881–896.
96. Maurya, S.; Rauthan, M.M.S.; Verma, R. Security Aspects of the Internet of Drones (IoD). In Proceedings of the 2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 21–22 April 2022; pp. 1–6.
97. Jan, S.U.; Abbasi, I.A.; Algarni, F. A Mutual Authentication and Cross Verification Protocol for Securing Internet-of-Drones (IoD). *Comput. Mater. Contin.* **2022**, *72*, 5845–5869. [CrossRef]
98. Pauner, C.; Kamara, I.; Viguri, J. Drones. In Current challenges and standardization solutions in the field of privacy and data protection. In Proceedings of the 2015 ITU Kaleidoscope: Trust in the Information Society (K-2015), Barcelona, Spain, 9–11 December 2015; pp. 1–7.

99. Hartmann, K.; Steup, C. The vulnerability of UAVs to cyber-attacks-An approach to the risk assessment. In Proceedings of the 2013 5th International Conference on Cyber Conflict (CYCON 2013), Tallinn, Estonia, 4–7 June 2013; pp. 1–23.
100. Kamthan, S.; Singh, H.; Meitzler, T. UAVs: On development of fuzzy model for categorization of countermeasures during threat assessment. In Proceedings of the SPIE Defense + Security, Anaheim, CA, USA, 5 May 2017; Karlsen, R.E., Gage, D.W., Shoemaker, C.M., Nguyen, H.G., Eds.; SPIE: Bellingham, WA, USA, 2017; p. 1019518.
101. Osanaiye, O.A.; Alfa, A.S.; Hancke, G.P. Denial of Service Defence for Resource Availability in Wireless Sensor Networks. *IEEE Access* **2018**, *6*, 6975–7004. [CrossRef]
102. Rodday, N.M.; Schmidt, R.d.O.; Pras, A. Exploring security vulnerabilities of unmanned aerial vehicles. In Proceedings of the IEEE/IFIP Network Operations and Management Symposium, Istanbul, Turkey, 25–29 April 2016; pp. 993–994.
103. Oleson, K.E.; Hancock, P.; Billings, D.R.; Schesser, C.D. Trust in unmanned aerial systems: A synthetic, distributed trust model. In Proceedings of the 6th International Symposium on Aviation Psychology, Columbus, OH, USA, 2–5 May 2011; pp. 469–474.
104. Mekdad, Y.; Aris, A.; Babun, L.; El Fergougui, A.; Conti, M.; Lazzeretti, R.; Uluagac, S. A Survey on Security and Privacy Issues of UAVs. *Comput. Netw.* **2023**, *224*, 109626. [CrossRef]
105. Dissanayake, N.; Jayatilaka, A.; Zahedi, M.; Babar, M.A. Software Security Patch Management—A Systematic Literature Review of Challenges, Approaches, Tools and Practices. *Inf. Softw. Technol.* **2021**, *144*, 106771. [CrossRef]
106. Eldosouky, A.R.; Ferdowsi, A.; Saad, W. Drones in Distress: A Game-Theoretic Countermeasure for Protecting UAVs Against GPS Spoofing. *IEEE Internet Things J.* **2020**, *7*, 2840–2854. [CrossRef]
107. Martínez-Rodríguez, B.; Bilbao-Arechabala, S.; Jorge-Hernandez, F. Security Architecture for Swarms of Autonomous Vehicles in Smart Farming. *Appl. Sci.* **2021**, *11*, 4341. [CrossRef]
108. Omolara, A.E.; Alawida, M.; Abiodun, O.I. Drone Cybersecurity Issues, Solutions, Trend Insights and Future Perspectives: A Survey. *Neural Comput. Appl.* **2023**, *35*, 23063–23101. [CrossRef]
109. Siddappaji, B.; Akhilesh, K.B. Role of Cyber Security in Drone Technology. In *Smart Technologies*; Akhilesh, K.B., Möller, D.P.F., Eds.; Springer: Singapore, 2020; pp. 169–178. [CrossRef]
110. Lei, Z.; Ding, P.; Zheng, W.; Fei, X.; Fan, H. UAV Countermeasure Technology Based on Partial-band Noise Jamming. In Proceedings of the 2021 33rd Chinese Control and Decision Conference (CCDC), Kunming, China, 22–24 May 2021; pp. 1456–1461.
111. Altawy, R.; Youssef, A.M. Security, Privacy, and Safety Aspects of Civilian Drones: A Survey. *ACM Trans. Cyber-Physical Syst.* **2017**, *1*, 1–25. [CrossRef]
112. Kumar, C.R.S.; Mohanty, S. Current trends in cyber security for drones. In Proceedings of the 2021 International Carnahan Conference on Security Technology (ICCST) IEEE, Hatfield, UK, 1–15 October 2021; pp. 1–5.
113. Singh, M.; Aujla, G.S.; Bali, R.S. Derived Blockchain Architecture for Security-Conscious Data Dissemination in Edge-Envisioned Internet of Drones Ecosystem. *Clust. Comput.* **2022**, *25*, 2281–2302. [CrossRef]
114. Sachdeva, H.; Gupta, S.; Misra, A.; Chauhan, K.; Dave, M. Privacy and Security Improvement in UAV Network Using Blockchain. *Int. J. Commun. Networks Distrib. Syst.* **2023**, *29*, 383–406. [CrossRef]
115. Alajlan, R.; Alhumam, N.; Frikha, M. Cybersecurity for Blockchain-Based IoT Systems: A Review. *Appl. Sci.* **2023**, *13*, 7432. [CrossRef]
116. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain Technologies for the Internet of Things: Research Issues and Challenges. *IEEE Internet Things J.* **2019**, *6*, 2188–2204. [CrossRef]
117. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on blockchain for Internet of Things. *Comput. Commun.* **2019**, *136*, 10–29. [CrossRef]
118. Singh, M.; Aujla, G.S.; Bali, R.S. A Deep Learning-Based Blockchain Mechanism for Secure Internet of Drones Environment. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 4404–4413. [CrossRef]
119. Das, A.K.; Bera, B.; Saha, S.; Kumar, N.; You, I.; Chao, H.-C. AI-Envisioned Blockchain-Enabled Signature-Based Key Management Scheme for Industrial Cyber–Physical Systems. *IEEE Internet Things J.* **2021**, *9*, 6374–6388. [CrossRef]
120. Vangala, A.; Sutrala, A.K.; Das, A.K.; Jo, M. Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming. *IEEE Internet Things J.* **2021**, *8*, 10792–10806. [CrossRef]
121. Kayalvizhi, M.; Ramamoorthy, S. Blockchain-based Secure Data Transmission for UAV Swarm using Modified Particle Swarm Optimization Path Planning Algorithm. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 554–563. [CrossRef]
122. Li, X.; Wang, Y.; Vijayakumar, P.; He, D.; Kumar, N.; Ma, J. Blockchain-Based Mutual-Healing Group Key Distribution Scheme in Unmanned Aerial Vehicles Ad-Hoc Network. *IEEE Trans. Veh. Technol.* **2019**, *68*, 11309–11322. [CrossRef]
123. Demestichas, K.; Peppes, N.; Alexakis, T.; Adamopoulou, E. Blockchain in Agriculture Traceability Systems: A Review. *Appl. Sci.* **2020**, *10*, 4113. [CrossRef]
124. Herbadji, A.; Gou-midi, H.; Harbi, Y.; Medani, K.; Aliouat, Z. Blockchain for internet of vehicles security. In *Blockchain for Cybersecurity and Privacy*; CRC Press: Boca Raton, FL, USA, 2020; pp. 159–197.
125. Merkle, R. A Digital Signature Based on a Conventional Encryption Function. In Proceedings of the Advances in Cryptology—CRYPTO1987, Santa Barbara, CA, USA, 16–20 August 1987; Springer: Berlin/Heidelberg, Germany, 1988; pp. 369–378.
126. Cheng, L.; Liu, J.; Xu, G.; Zhang, Z.; Wang, H.; Dai, H.-N.; Wu, Y.; Wang, W. SCTSC: A Semicentralized Traffic Signal Control Mode With Attribute-Based Blockchain in IoVs. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1373–1385. [CrossRef]

127. Wang, C.; Jiang, H.; Zeng, J.; Min, Y.U.; Huang, Q.; Zuo, Z. A review of blockchain layered architecture and technology application research. *Wuhan Univ. J. Nat. Sci.* **2021**, *26*, 14.
128. Duan, Z.; Mao, H.; Chen, Z.; Bai, X.; Hu, K.; Talpin, J.-P. Formal Modeling and Verification of Blockchain System. In Proceedings of the 10th International Conference on Computer Modeling and Simulation, Sydney, Australia, 8–10 January 2018; pp. 231–235.
129. Bary, T.A.A.A.A.; Elomda, B.M.; Hassan, H.A. Multiple Layer Public Blockchain Approach for Internet of Things (IoT) Systems. *IEEE Access* **2024**, *12*, 56431–56438. [CrossRef]
130. Zhai, S.; Yang, Y.; Li, J.; Qiu, C.; Zhao, J. Research on the Application of Cryptography on the Blockchain. *J. Phys. Conf. Ser.* **2019**, *1168*, 032077. [CrossRef]
131. Latif, S.; Idrees, Z.; Huma, Z.E.; Ahmad, J. Blockchain Technology for the Industrial Internet of Things: A Comprehensive Survey on Security Challenges, Architectures, Applications, and Future Research Directions. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4337. [CrossRef]
132. Pajooh, H.H.; Rashid, M.; Alam, F.; Demidenko, S. Multi-Layer Blockchain-Based Security Architecture for Internet of Things. *Sensors* **2021**, *21*, 772. [CrossRef]
133. Zhu, Y. Security architecture and key technologies of blockchain. *J. Inf. Secur. Res.* **2016**, *2*, 1090.
134. Hu, Q.; Yan, B.; Han, Y.; Yu, J. An Improved Delegated Proof of Stake Consensus Algorithm. *Procedia Comput. Sci.* **2021**, *187*, 341–346. [CrossRef]
135. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.-Y. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Trans. Syst. Man, Cybern. Syst.* **2019**, *49*, 2266–2277. [CrossRef]
136. Ferreira, M.; Rodrigues, S.; Reis, C.I.; Maximiano, M. Blockchain: A Tale of Two Applications. *Appl. Sci.* **2018**, *8*, 1506. [CrossRef]
137. Singh, H. DApps: Decentralized Applications for Blockchains. In *Distributed Computing to Blockchain*; Elsevier: Amsterdam, The Netherlands, 2023; pp. 87–104. [CrossRef]
138. Dutta, J.; Barman, S.; Sen, S.; Routh, A.; Chattopadhyay, M.; Chattopadhyay, S. Easypay: A user-friendly blockchain-powered payment gateway. *Clust. Comput.* **2024**, 1–20. [CrossRef]
139. Buldas, A.; Draheim, D.; Gault, M.; Laanoja, R.; Nagumo, T.; Saarepera, M.; Shah, S.A.; Simm, J.; Steiner, J.; Tammet, T.; et al. An Ultra-Scalable Blockchain Platform for Universal Asset Tokenization: Design and Implementation. *IEEE Access* **2022**, *10*, 77284–77322. [CrossRef]
140. Schaer, F. Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *FRB St. Louis Rev.* **2020**, *103*, 153–174. [CrossRef]
141. Chaudhry, N.; Yousaf, M.M. Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities. In Proceedings of the 12th International Conference on Open Source Systems and Technologies (ICOSST), Lahore, Pakistan, 19–21 December 2018; pp. 54–63.
142. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *3*, 1–32.
143. Zou, W.; Lo, D.; Kochhar, P.S.; Le, X.-B.D.; Xia, X.; Feng, Y.; Chen, Z.; Xu, B. Smart Contract Development: Challenges and Opportunities. *IEEE Trans. Softw. Eng.* **2021**, *47*, 2084–2106. [CrossRef]
144. Scherer, M. Performance and Scalability of Blockchain Networks and Smart Contracts. 2017. Available online: https://www.semanticscholar.org/paper/Performance-and-Scalability-of-Blockchain-Networks-Scherer/be45a7e01d17cc2e09e7ddecfabb2d28ac2763d9 (accessed on 10 April 2024).
145. Holotescu, C. *Understanding Blockchain Opportunities and Challenges*; Carol I National Defence University Publishing House: Bucharest, Romania, 2018; pp. 275–283. [CrossRef]
146. Dinh, T.T.A.; Wang, J.; Chen, G.; Liu, R.; Ooi, B.C.; Tan, K.-L. BLOCKBENCH: A Framework for Analyzing Private Blockchains. In Proceedings of the International Conference on Management of Data, Chicago, IL, USA, 14–19 May 2017; pp. 1085–1100. [CrossRef]
147. Yang, R.; Wakefield, R.; Lyu, S.; Jayasuriya, S.; Han, F.; Yi, X.; Yang, X.; Amarasinghe, G.; Chen, S. Public and Private Blockchain in Construction Business Process and Information Integration. *Autom. Constr.* **2020**, *118*, 103276. [CrossRef]
148. Mohan, C. State of Public and Private Blockchains: Myths and Reality. In Proceedings of the International Conference on Management of Data, Amsterdam, The Netherlands, 30 June–5 July 2019; pp. 404–411.
149. Dib, O.; Brousmiche, K.-L.; Durand, A.; Thea, E.; Hamida, E.B. Consortium blockchains: Overview, applications and challenges. *Int. J. Adv. Telecommun.* **2018**, *11*, 51–64.
150. Meng, T.; Zhao, Y.; Wolter, K.; Xu, C.-Z. On Consortium Blockchain Consistency: A Queueing Network Model Approach. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *32*, 1369–1382. [CrossRef]
151. Yao, W.; Deek, F.P.; Murimi, R.; Wang, G. SoK: A Taxonomy for Critical Analysis of Consensus Mechanisms in Consortium Blockchain. *IEEE Access* **2023**, *11*, 79572–79587. [CrossRef]
152. Allouch, A.; Cheikhrouhou, O.; Koubâa, A.; Toumi, K.; Khalgui, M.; Gia, T.N. UTM-Chain: Blockchain-Based Secure Unmanned Traffic Management for Internet of Drones. *Sensors* **2021**, *21*, 3049. [CrossRef] [PubMed]
153. Bera, B.; Das, A.K.; Sutrala, A.K. Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment. *Comput. Commun.* **2021**, *166*, 91–109. [CrossRef]
154. Niranjanamurthy, M.; Nithya, B.N.; Jagannatha, S. Analysis of Blockchain technology: Pros, cons and SWOT. *Clust. Comput.* **2019**, *22*, 14743–14757. [CrossRef]

155. Bera, B.; Wazid, M.; Das, A.K.; Rodrigues, J.J.P.C. Securing Internet of Drones Networks Using AI-Envisioned Smart-Contract-Based Blockchain. *IEEE Internet Things Mag.* **2021**, *4*, 68–73. [CrossRef]
156. Huang, R.; Yang, X.; Ajay, P. Consensus mechanism for software-defined blockchain in internet of things. *Internet Things Cyber-Physical Syst.* **2023**, *3*, 52–60. [CrossRef]
157. 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]
158. Wu, Y.; Dai, H.-N.; Wang, H.; Choo, K.-K.R. Blockchain-Based Privacy Preservation for 5G-Enabled Drone Communications. *IEEE Netw.* **2021**, *35*, 50–56. [CrossRef]
159. Luo, S.; Li, H.; Wen, Z.; Qian, B.; Morgan, G.; Longo, A.; Rana, O.; Ranjan, R. Blockchain-Based Task Offloading in Drone-Aided Mobile Edge Computing. *IEEE Netw.* **2021**, *35*, 124–129. [CrossRef]
160. Nguyen, T.; Katila, R.; Gia, T.N. An advanced Internet-of-Drones System with Blockchain for improving quality of service of Search and Rescue: A feasibility study. *Futur. Gener. Comput. Syst.* **2023**, *140*, 36–52. [CrossRef]
161. Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mech. Syst. Signal Process.* **2019**, *135*, 106382. [CrossRef]
162. Kang, J.; Xiong, Z.; Niyato, D.; Ye, D.; Kim, D.I.; Zhao, J. Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2906–2920. [CrossRef]
163. Wu, Q.; Mei, W.; Zhang, R. Safeguarding Wireless Network with UAVs: A Physical Layer Security Perspective. *IEEE Wirel. Commun.* **2019**, *26*, 12–18. [CrossRef]
164. Cao, B.; Li, Y.; Zhang, L.; Zhang, L.; Mumtaz, S.; Zhou, Z.; Peng, M. When Internet of Things Meets Blockchain: Challenges in Distributed Consensus. *IEEE Netw.* **2019**, *33*, 133–139. [CrossRef]
165. Yanmaz, E.; Yahyanejad, S.; Rinner, B.; Hellwagner, H.; Bettstetter, C. Drone networks: Communications, coordination, and sensing. *Ad Hoc Netw.* **2018**, *68*, 1–15. [CrossRef]
166. Dai, H.-N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A Survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094. [CrossRef]
167. Ossamah, A. Blockchain as a solution to Drone Cybersecurity. In Proceedings of the IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2–16 June 2020; pp. 1–9.
168. Kantur, H.; Bamuleseyo, C. How Smart Contracts Can Change the Insurance Industry: Benefits and Challenges of Using Blockchain Technology. 2018. Available online: http://www.diva-portal.org/smash/record.jsf?pid=diva2:1214254&dswid=8446 (accessed on 10 April 2024).
169. Tyagi, A.K.; Chandrasekaran, S.; Sreenath, N. Blockchain Technology:– A New Technology for Creating Distributed and Trusted Computing Environment. In Proceedings of the International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 9–11 May 2022; pp. 1348–1354.
170. Rajagopal, B.R.; Anjanadevi, B.; Tahreem, M.; Kumar, S.; Debnath, M.; Tongkachok, K. Comparative Analysis of Blockchain Technology and Artificial Intelligence and its impact on Open Issues of Automation in Workplace. In Proceedings of the 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 28–29 April 2022; pp. 288–292.
171. Gupta, R.; Reebadiya, D.; Tanwar, S.; Kumar, N.; Guizani, M. When Blockchain Meets Edge Intelligence: Trusted and Security Solutions for Consumers. *IEEE Netw.* **2021**, *35*, 272–278. [CrossRef]
172. Yang, R.; Yu, F.R.; Si, P.; Yang, Z.; Zhang, Y. Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges. *IEEE Commun. Surv. Tutorials* **2018**, *21*, 1508–1532. [CrossRef]
173. Wang, Z.; Li, M.; Lu, J.; Cheng, X. Business Innovation based on artificial intelligence and Blockchain technology. *Inf. Process. Manag.* **2022**, *59*, 102759. [CrossRef]
174. Mendis, G.J.; Wu, Y.; Wei, J.; Sabounchi, M.; Roche, R. A Blockchain-Powered Decentralized and Secure Computing Paradigm. *IEEE Trans. Emerg. Top. Comput.* **2020**, *9*, 2201–2222. [CrossRef]
175. Nassar, M.; Salah, K.; Rehman, M.H.U.; Svetinovic, D. Blockchain for explainable and trustworthy artificial intelligence. *WIREs Data Min. Knowl. Discov.* **2019**, *10*, e1340. [CrossRef]
176. Wang, K.; Dong, J.; Wang, Y.; Yin, H. Securing Data with Blockchain and AI. *IEEE Access* **2019**, *7*, 77981–77989. [CrossRef]
177. Zuo, Y.; Guo, J.; Gao, N.; Zhu, Y.; Jin, S.; Li, X. A Survey of Blockchain and Artificial Intelligence for 6G Wireless Communications. *IEEE Commun. Surv. Tutorials* **2023**, *25*, 2494–2528. [CrossRef]
178. Saini, S.; Jangra, A.; Singh, G. Real-Time Agent-Based Load-Balancing Algorithm for Internet of Drone (IoD) in Cloud Computing. In *Internet of Things*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2022; pp. 81–94. [CrossRef]
179. Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Wills, G.B. Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. *Int. J. Intell. Syst. Appl.* **2018**, *10*, 40–48. [CrossRef]
180. Reyna, A.; Martin, C.; Chen, J.; Soler, E.; Diaz, M. On blockchain and its integration with loT. Challenges and opportunities. *Futur. Gener. Comput. Syst.* **2018**, *88*, 173–190. [CrossRef]
181. Habib, G.; Sharma, S.; Ibrahim, S.; Ahmad, I.; Qureshi, S.; Ishfaq, M. Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Futur. Internet* **2022**, *14*, 341. [CrossRef]
182. Khan, W.Z.; Ahmed, E.; Hakak, S.; Yaqoob, I.; Ahmed, A. Edge computing: A survey. *Futur. Gener. Comput. Syst.* **2019**, *97*, 219–235. [CrossRef]

183. Zhang, X.; Wang, Y.; Lu, S.; Liu, L.; Xu, L.; Shi, W. OpenEI: An Open Framework for Edge Intelligence. In Proceedings of the IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–10 July 2019; pp. 1840–1851.
184. Zhou, S.; Jadoon, W.; Khan, I.A. Computing Offloading Strategy in Mobile Edge Computing Environment: A Comparison between Adopted Frameworks, Challenges, and Future Directions. *Electronics* **2023**, *12*, 2452. [CrossRef]
185. Yuan, X.; Xie, Z.; Tan, X. Computation Offloading in UAV-Enabled Edge Computing: A Stackelberg Game Approach. *Sensors* **2022**, *22*, 3854. [CrossRef]
186. Xue, H.; Chen, D.; Zhang, N.; Dai, H.-N.; Yu, K. Integration of blockchain and edge computing in internet of things: A survey. *Futur. Gener. Comput. Syst.* **2023**, *144*, 307–326. [CrossRef]
187. Nayyar, A.; Kumar, A. (Eds.) *A Roadmap to Industry 4.0: Smart Production, Sharp Business and Sustainable Development*; Springer International Publishing: Cham, Switzerland, 2020. [CrossRef]
188. Keshk, M.; Sitnikova, E.; Moustafa, N.; Hu, J.; Khalil, I. An Integrated Framework for Privacy-Preserving Based Anomaly Detection for Cyber-Physical Systems. *IEEE Trans. Sustain. Comput.* **2019**, *6*, 66–79. [CrossRef]
189. Kang, S.; Fu, X. Blockchain-Enabled Infection Sample Collection System Using Two-Echelon Drone-Assisted Mechanism. *Drones* **2024**, *8*, 14. [CrossRef]
190. Ulusar, U.D.; Al-Turjman, F.; Celik, G. An overview of Internet of things and wireless communications. In Proceedings of the International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey, 5–8 October 2017; pp. 506–509.
191. Khanh, Q.V.; Hoai, N.V.; Manh, L.D.; Le, A.N.; Jeon, G. Wireless Communication Technologies for IoT in 5G: Vision, Applications, and Challenges. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 3229294. [CrossRef]
192. Gemeliarana, I.G.A.K.; Sari, R.F. Evaluation of Proof of Work (POW) Blockchains Security Network on Selfish Mining. In Proceedings of the 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 21–22 November 2018; pp. 126–130.
193. Saad, S.M.S.; Radzi, R.Z.R.M.; Othman, S.H. Comparative Analysis of the Blockchain Consensus Algorithm Between Proof of Stake and Delegated Proof of Stake. In Proceedings of the International Conference on Data Science and Its Applications (ICoDSA), Bandung, Indonesia, 21–22 November 2018; pp. 175–180.
194. Aloqaily, M.; Bouachir, O.; Boukerche, A.; Al Ridhawi, I. Design Guidelines for Blockchain-Assisted 5G-UAV Networks. *IEEE Netw.* **2021**, *35*, 64–71. [CrossRef]
195. Tychola, K.A.; Voulgaridis, K.; Lagkas, T. Tactile IoT and 5G & beyond schemes as key enabling technologies for the future metaverse. *Telecommun. Syst.* **2023**, *84*, 1–23. [CrossRef]
196. Khan, F. *LTE for 4G Mobile Broadband: Air Interface Technologies and Performance*; Cambridge University Press: Cambridge, UK, 2009.
197. Gupta, R.; Nair, A.; Tanwar, S.; Kumar, N. Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges. *IET Commun.* **2021**, *15*, 1352–1367. [CrossRef]
198. Andrews, J.G.; Buzzi, S.; Choi, W.; Hanly, S.V.; Lozano, A.; Soong, A.C.K.; Zhang, J.C. What Will 5G Be? *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1065–1082. [CrossRef]
199. Raja, G.; Senthivel, S.G.; Balaganesh, S.; Rajakumar, B.R.; Ravichandran, V.; Guizani, M.; Ganesh, S. MLB-IoD: Multi Layered Blockchain Assisted 6G Internet of Drones Ecosystem. *IEEE Trans. Veh. Technol.* **2022**, *72*, 2511–2520. [CrossRef]
200. Zhang, S.; Zhang, H.; Song, L. Beyond D2D: Full Dimension UAV-to-Everything Communications in 6G. *IEEE Trans. Veh. Technol.* **2020**, *69*, 6592–6602. [CrossRef]
201. Piran, J.; Suh, D.Y. Learning-Driven Wireless Communications, towards 6G. In Proceedings of the International Conference on Computing, Electronics & Communications Engineering (iCCECE), London, UK, 22–23 August 2019; pp. 219–224.
202. Porkodi, S.; Kesavaraja, D. Integration of Blockchain and Internet of Things. In *Handbook of Research on Blockchain Technology*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 61–94. [CrossRef]
203. Zafar, S.; Bhatti, K.M.; Shabbir, M.; Hashmat, F.; Akbar, A.H. Integration of Blockchain and Internet of Things: Challenges and Solutions. *Ann. Telecommun.* **2022**, *77*, 13–32. [CrossRef]
204. Alsharari, N. Integrating Blockchain Technology with Internet of Things to Efficiency. *Int. J. Technol. Innov. Manag. (IJTIM)* **2021**, *1*, 1–13. [CrossRef]
205. Sharma, D.K.; Kaushik, A.K.; Goel, A.; Bhargava, S. Internet of Things and Blockchain: Integration, Need, Challenges, Applications, and Future Scope. In *Handbook of Research on Blockchain Technology*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 271–294. [CrossRef]
206. Stadtler, H. Supply Chain Management: An Overview. In *Supply Chain Management and Advanced Planning*; Stadtler, H., Kilger, C., Meyr, H., Eds.; Springer Texts in Business and Economics; Springer: Berlin/Heidelberg, Germany, 2015; pp. 3–28. [CrossRef]
207. Beamon, B.M. Supply chain design and analysis: Models and methods. *Int. J. Prod. Econ.* **1998**, *55*, 281–294. [CrossRef]
208. Druehl, C.; Carrillo, J.; Hsuan, J. Technological Innovations: Impacts on Supply Chains. In *Innovation and Supply Chain Management*; Moreira, A.C., Ferreira, L.M.D.F., Zimmermann, R.A., Eds.; Contributions to Management Science; Springer International Publishing: Cham, Switzerland, 2018; pp. 259–281. [CrossRef]
209. Rejeb, A.; Rejeb, K.; Simske, S.J.; Treiblmaier, H. Drones for supply chain management and logistics: A review and research agenda. *Int. J. Logist. Res. Appl.* **2023**, *26*, 708–731. [CrossRef]
210. Amiri, M.J.; Agrawal, D.; El Abbadi, A. CAPER: A cross-application permissioned blockchain. *Proc. VLDB Endow.* **2019**, *12*, 1385–1398. [CrossRef]

211. Gupta, R.; Bhattacharya, P.; Tanwar, S.; Kumar, N.; Zeadally, S. GaRuDa: A Blockchain-Based Delivery Scheme Using Drones for Healthcare 5.0 Applications. In *IEEE Internet of Things Magazine*; IEEE: Piscataway, NJ, USA, 2021; Volume 4, pp. 60–66. [CrossRef]
212. Haleem, A.; Javaid, M.; Singh, R.P.; Suman, R.; Rab, S. Blockchain technology applications in healthcare: An overview. *Int. J. Intell. Networks* **2021**, *2*, 130–139. [CrossRef]
213. Ellingsen, G.; Hertzum, M. User requirements meet large-scale EHR suites: Norwegian preparations for Epic. *Stud. Health Technol. Inform.* **2020**, *270*, 703–707. [CrossRef]
214. Claesson, A.; Svensson, L.; Nordberg, P.; Ringh, M.; Rosenqvist, M.; Djarv, T.; Samuelsson, J.; Hernborg, O.; Dahlbom, P.; Jansson, A.; et al. Drones may be used to save lives in out of hospital cardiac arrest due to drowning. *Resuscitation* **2017**, *114*, 152–156. [CrossRef]
215. Rosser, J.C.; Vignesh, V.; Terwilliger, B.A.; Parker, B.C. Surgical and Medical Applications of Drones: A Comprehensive Review. *J. Soc. Laparosc. Robot. Surg.* **2018**, *22*, e2018.00018. [CrossRef]
216. Braun, J.; Gertz, S.D.; Furer, A.; Bader, T.; Frenkel, H.; Chen, J.; Glassberg, E.; Nachman, D. The promising future of drones in prehospital medical care and its application to battlefield medicine. *J. Trauma Inj. Infect. Crit. Care* **2019**, *87*, S28–S34. [CrossRef]
217. Aujla, G.S.; Jindal, A. A Decoupled Blockchain Approach for Edge-Envisioned IoT-Based Healthcare Monitoring. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 491–499. [CrossRef]
218. Singh, M.P.; Aujla, G.S.; Bali, R.S. An Unorthodox Security Framework using Adapted Blockchain Architecture for Internet of Drones. In Proceedings of the IEEE Globecom Workshops (GC Wkshps), Madrid, Spain, 7–11 December 2021; pp. 1–6.
219. Khan, A.; Gupta, S.; Gupta, S.K. Emerging UAV technology for disaster detection, mitigation, response, and preparedness. *J. Field Robot.* **2022**, *39*, 905–955. [CrossRef]
220. Panda, K.G.; Das, S.; Sen, D.; Arif, W. Design and Deployment of UAV-Aided Post-Disaster Emergency Network. *IEEE Access* **2019**, *7*, 102985–102999. [CrossRef]
221. Pinto, R.; Lagorio, A. Point-to-point drone-based delivery network design with intermediate charging stations. *Transp. Res. Part C Emerg. Technol.* **2022**, *135*, 103506. [CrossRef]
222. Torky, M.; El-Dosuky, M.; Goda, E.; Snášel, V.; Hassanien, A.E. Scheduling and Securing Drone Charging System Using Particle Swarm Optimization and Blockchain Technology. *Drones* **2022**, *6*, 237. [CrossRef]
223. Boukoberine, M.N.; Zhou, Z.; Benbouzid, M. Power Supply Architectures for Drones–A Review. In Proceedings of the 45th Annual Conference of the IEEE Industrial Electronics Society, Lisbon, Portugal, 14–17 October 2019; pp. 5826–5831.
224. Krithika, L.B. Survey on the Applications of Blockchain in Agriculture. *Agriculture* **2022**, *12*, 1333. [CrossRef]
225. A Mukherjee, A.; Singh, R.K.; Mishra, R.; Bag, S. Application of blockchain technology for sustainability development in agricultural supply chain: Justification framework. *Oper. Manag. Res.* **2021**, *15*, 46–61. [CrossRef]
226. Zhang, Z.; Song, X.; Liu, L.; Yin, J.; Wang, Y.; Lan, D. Recent Advances in Blockchain and Artificial Intelligence Integration: Feasibility Analysis, Research Issues, Applications, Challenges, and Future Work. *Secur. Commun. Netw.* **2021**, *2021*, 1–15. [CrossRef]
227. Bilow, S.C. Introduction: Blockchain in Media and Entertainment. *SMPTE Motion Imaging J.* **2020**, *129*, 20–21. [CrossRef]
228. Cho, S.; Jeong, C. A blockchain for media: Survey. In Proceedings of the International Conference on Electronics, Information, and Communication (ICEIC), Auckland, New Zealand, 22–25 January 2019.
229. Peng, C.; Liu, Z.; Wen, F.; Lee, J.-Y.; Cui, F. Research on Blockchain Technology and Media Industry Applications in the Context of Big Data. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 3038436. [CrossRef]
230. Zaidi, S.; Atiquzzaman, M.; Calafate, C.T. Internet of Flying Things (IoFT): A Survey. *Comput. Commun.* **2021**, *165*, 53–74. [CrossRef]
231. Feng, C.; Liu, B.; Guo, Z.; Yu, K.; Qin, Z.; Choo, K.-K.R. Blockchain-Based Cross-Domain Authentication for Intelligent 5G-Enabled Internet of Drones. *IEEE Internet Things J.* **2022**, *9*, 6224–6238. [CrossRef]
232. Uddin, A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A survey on the adoption of blockchain in IoT: Challenges and solutions. *Blockchain Res. Appl.* **2021**, *2*, 100006. [CrossRef]
233. Wazid, M.; Bera, B.; Das, A.K.; Garg, S.; Niyato, D.; Hossain, M.S. Secure Communication Framework for Blockchain-Based Internet of Drones-Enabled Aerial Computing Deployment. *IEEE Internet Things Mag.* **2021**, *4*, 120–126. [CrossRef]
234. Ab Rahman, N.H.; Glisson, W.B.; Yang, Y.; Choo, K.-K.R. Forensic-by-Design Framework for Cyber-Physical Cloud Systems. *IEEE Cloud Comput.* **2016**, *3*, 50–59. [CrossRef]
235. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
236. Muram, F.U.; Javed, M.A. Drone-based Risk Management of Autonomous Systems Using Contracts and Blockchain. In Proceedings of the IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), Honolulu, HI, USA, 9–12 March 2021; pp. 679–688.
237. Dawaliby, S.; Aberkane, A.; Bradai, A. Blockchain-based IoT platform for autonomous drone operations management. In Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, London, UK, 25 September 2020; pp. 31–36. [CrossRef]
238. Kumar, M.S.; Vimal, S.; Jhanjhi, N.; Dhanabalan, S.S.; Alhumyani, H.A. Blockchain based peer to peer communication in autonomous drone operation. *Energy Rep.* **2021**, *7*, 7925–7939. [CrossRef]

239. Idries, A.; Mohamed, N.; Jawhar, I.; Mohamed, F.; Al-Jaroodi, J. Challenges of developing UAV applications: A project management view. In Proceedings of the International Conference on Industrial Engineering and Operations Management (IEOM), Dubai, United Arab Emirates, 3–5 March 2015; pp. 1–10.
240. Kriz, V.; Gabrlik, P. UranusLink–Communication Protocol for UAV with Small Overhead and Encryption Ability. *IFAC-PapersOnLine* **2015**, *48*, 474–479. [CrossRef]
241. 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]
242. Kędziora, M.; Kozłowski, P.; Szczepanik, M.; Jóźwiak, P. Analysis of Blockchain Selfish Mining Attacks. In *Information Systems Architecture and Technology, Proceedings of the 40th Anniversary International Conference on Information Systems Architecture and Technology–ISAT 2019, Wrocław, Polska, 15–17 September 2019*; Borzemski, L., Świątek, J., Wilimowska, Z., Eds.; Advances in Intelligent Systems and Computing; Springer International Publishing: Cham, Switzerland, 2020; Volume 1050, pp. 231–240. [CrossRef]
243. Mazhar, T.; Talpur, D.B.; Al Shloul, T.; Ghadi, Y.Y.; Haq, I.; Ullah, I.; Ouahada, K.; Hamam, H. Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. *Brain Sci.* **2023**, *13*, 683. [CrossRef]
244. Sawalmeh, A.H.; Othman, N.S. An Overview of Collision Avoidance Approaches and Network Architecture of Unmanned Aerial Vehicles (UAVs). *arXiv* **2021**. [CrossRef]
245. Singh, M.; Aujla, G.S.; Bali, R.S. ODOB: One Drone One Block-based Lightweight Blockchain Architecture for Internet of Drones. In Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 249–254. [CrossRef]
246. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H.; Srivastava, G.; Aledhari, M. Enabling Drones in the Internet of Things With Decentralized Blockchain-Based Security. *IEEE Internet Things J.* **2020**, *8*, 6406–6415. [CrossRef]

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