Block chain technologies for UAV swarms and UAV-based networks, SLR

Naser Abbas Hussein[1,*], Jihene khoualdi[1], Khadija Rammeh Houerbi[2], Hella Kaffel Ben Ayed[1]

[1]Faculty of Sciences of Tunis, University of Tunis El manar, Tunis, Tunisia

[2]School of Borj el Amri, Ministry of Defense, Tunisia

Emails: Naser.hussein@fst.utm.tn; jihene.khoualdi@etudiant-fst.utm.tn; Khadija.ramah@gmail.com; Hella.kaffel@fst.utm.tn

Abstract

Unmanned aerial vehicles (UAVs) and swarms unmanned aerial vehicles (UAVs) have recently shown themselves capable of providing dependable and reasonably priced solutions for a variety of real-world issues. UAVs provide a wide range of services due to their autonomy, adaptability, mobility, and communications interoperability. Despite the fact that UAVs are frequently used to facilitate ground communications, data exchanges inside those networks are susceptible to security threats due to the ease with which radio and Wi-Fi signals can be hacked. However, there are many ways to stop cyberattacks. One of the potential methods to enhance user privacy, data security, and authentication—especially in peer-to-peer UAV networks—may be blockchain technology, which has lately gained prominence. Using the benefits of blockchain technology, several entities can communicate in a decentralized. This paper uses some supporting technologies to provide a thorough overview of privacy and security integration in blockchain-assisted swarm and UAV networks. For this goal, this work is compared to earlier research to find effective solutions, and blockchain technology is integrated to improve the capacity of swarm UAV networks and communication to move, manage, and exchange data. We conclude by talking about open research issues, the limitations of the UAV standards as they stand right now, and possible research paths in the future. This comprehensive review is an invaluable tool to know study and analyze a good number of reviews and research papers in recent years to overcome obstacles and find appropriate solutions for integrating UAV swarms with block chain Technology.

Keywords: Block chain technology; Swarm communications; UAV networks; Unmanned aerial vehicles

I. Introduction

Unmanned aerial vehicles (UAVs) have garnered significant attention due to their exceptional portability, affordability, and user-friendliness. UAVs are seen as essential service enablers for wireless communication, disaster relief, the healthcare industry, real-time surveillance and monitoring, and creative urban applications. The amount spent on UAVs will surpass the 19.78 billion dollars spent in 2020, reaching around 102.4 billion dollars annually by 2030 at a compound annual growth rate of 19.6% [1].

Unmanned aerial vehicle (UAV) networks have drawn a lot of interest lately due to their capacity to perform challenging and dangerous jobs like search and rescue missions, traffic monitoring, land surveying, and shoreline surveillance[2]. UAVs are more susceptible to hacks as UAV networks are utilized more frequently. As a result, maintaining secure UAV communication is essential, particularly during critical missions. To guarantee the security of these communications, one method is to use block chain technology, which is an immutable, distributed, and decentralized ledger[3].

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

It is an interesting idea to use blockchain technology to improve UAV drone communication. UAV drones can improve data security, communication efficiency, and information tracking and verification by utilizing blockchain technology. The decentralized and impenetrable nature of blockchain technology can guarantee the security and dependability of data transferred between drones. Furthermore, smart contracts can expedite operations by automating specific procedures like data exchange or flight authorization. Overall, using blockchain technology into UAV drone communication has the potential to completely transform the sector by offering a transparent and safe platform for cooperation and data sharing.

Block chain research on drone swarms has significant ramifications for a number of sectors and domains, including commercial, political, and military uses. Potential advantages of such systems include enhanced coordination and performance, as well as enhanced security, privacy, and member trust. The use and development of technologies that change the way jobs like surveillance and disaster aid are performed may increase as a result of these studies[4].

Researchers can contribute to the development of a drone swarm system that is safer, more open, more ethical, and has benefits that are distributed equitably by tackling these problems. In order to address some of the most pressing problems facing our society today and to shape the future of these technologies and their impact on society, research into the use of blockchain technology in drone swarms is therefore essential.

The implementation and growth of wireless networks necessitate significant time and financial commitments. Moreover, due to their broadcast nature, UAV-assisted wireless networks are particularly vulnerable to security and privacy lapses, such as line-of-interference assaults, malware infection, eavesdropping links, distributed denial-of-service (DDOS), replay, impersonation, message injection, spoofing, and replay. Therefore, there are important privacy and security issues with UAV-assisted communication that need to be resolved[5].

In UAV swarm applications, cryptographic keys and hash-based blockchain approaches can offer protection against wormhole assaults, jamming, DOS, eavesdropping, and global positioning system (GPS) spoofing [6]. The ability of several consensus methods to deliver high throughput in a dispersed network is limited. Along with the existing architecture's drawbacks, the UAV swarm network experiences a large computational delay due to block chain security procedures, making it inappropriate for applications that need low latency and high availability.

The focus of this analysis is on research and papers from the research databases (IEEE, Science Direct, MDPI, and others) published between 2018 and 2024. More than 209 publications were gathered based on the amount of data available in the English language. After removing the necessary research, there were 40 unique studies at the center of the research issue, as shown in Tables 1 and 2.

1.1 Motivation

In UAV networks, security vulnerabilities in the wireless channel could affect reliability. Therefore, researchers have recently concentrated on using diverse techniques including homomorphic encryption and differential privacy to improve the security of the UAV-assisted network[7].

Some attacks use communication line weaknesses to gather information, while others disguise sensors using methods like GPS spoofing. Attacks involving GPS and flight control manipulation are frequent on UAV networks. Unmanned aerial vehicles (UAVs) have a lot of potential applications, but they also raise social concerns like privacy, cyber security, and public safety hazards[8].

These weaknesses result in property damage, data theft, and fatalities. Furthermore, for time-sensitive and privacy-sensitive applications, a UAV network needs to have secure and dependable communication. It is crucial to take into account the wider picture when integrating blockchain technology with UAVs for data-driven applications.

There are several motivations for using blockchain technology to enhance swarm UAV communication networks:

1. Security: Since block chain technology provides a secure and unbreakable way to store and transport data, it is the ideal substitute for ensuring the confidentiality and integrity of communication inside a swarm UAV network.

2. Decentralization: Block chain technology makes it possible for swarm UAV networks to operate decentralized, enabling individual drones to coordinate and decide without the need for a central authority.

3. Efficiency: A swarm UAV network's communication procedures can be streamlined with the usage of blockchain technology, which lowers latency and enhances network performance overall.

4. Trust: Drones can now interact trustlessly thanks to blockchain technology, which also ensures secure and dependable network connection by doing away with the need for intermediaries.

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

Ultimately, the capacity of Blockchain technology to offer a safe, decentralized, transparent, effective, and reliable communication infrastructure for autonomous drone operations is what motivates the use of this technology to improve swarm UAV communication networks.

1.2 Contributions and Organization

This paper provides a comprehensive examination of the primary issues pertaining to swarm UAV communications and blockchain, including privacy and security, as well as challenges and solutions pertaining to the security of UAV networks. Here is a summary of this work's key contributions:

In order to study previous works related to the concept of swarm UAVs and network communication, a comparison was made with previous works and knowledge for the period from 2018 to 2024, as shown in Table No. 1.

Provide a comprehensive and up-to-date review of innovative and effective solutions for UAV swarm communication and networking in various fields, Internet of Things applications, military applications and crowd control in [58], [59], [61], [64], and COVID_19 in [67], [68], [69].

The study focused on the communications of swarm UAV networks in the listed sources, through [52], [57], [58], [61], [62], [63], [64], [65], [67], [69], [71] Collect and share data, improve the swarm network, improve network security, and reduce energy consumption. In addition, reduced the attacked in [56], [57], [70].

Some technologies have been used and integrated with Blockchain to enhance the ability of swarm UAV communication ne and networks to transfer, manage and share data from them (IOT, IOD, 5G, 6G, AI, MEC, SDN, cloud) as in the sources [52], [53], [57], [60], [63], [66], [67], [69], [70], [71].

This study showed that scientific platforms competed to publish articles, and the largest share was (IEEE, science Direct, MDPI, and others)

IEEE: 12 ScienceDirect:4 MDPI:2 Other:4, shown in Figure. 10.

The best considerations of security in this study is Authentications it is better than the others as shown in Figure are. 11.

The rest of the paper is organized in this manner. Section 2 provides background information on UAVs, UAV networks, UAV applications and UAV swarms. Section 3 goes into detail about blockchain technology, and there is a pertinent study that uses blockchain in Swarm. Section 4 goes into detail about UAV communication networks, and Swarm uses cutting-edge blockchain technology. Section 5 goes into detail about UAVs, whereas Section 6 discusses unresolved problems and difficulties. Section 7 presents the conclusions. The article's structure is shown in Figure 1.

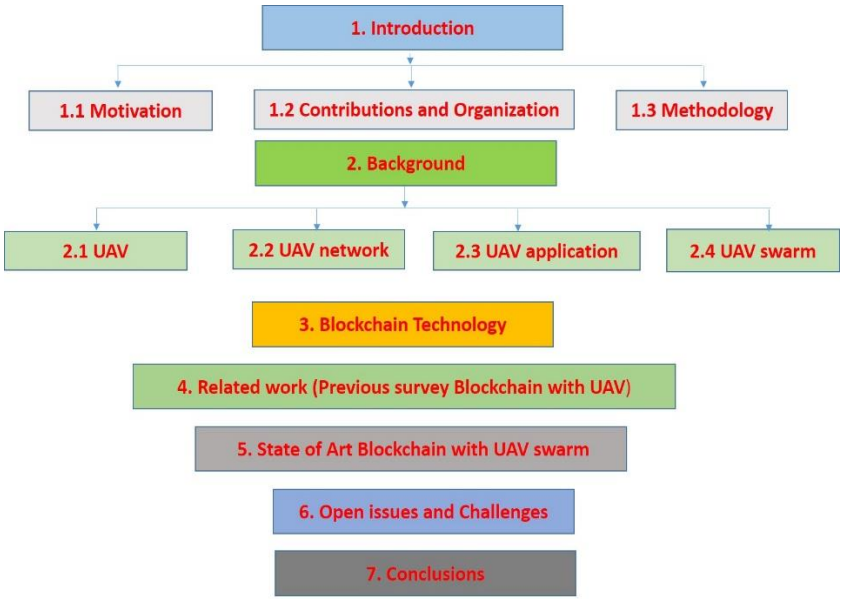

Figure 1. Organization of paper

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

1.3 Methodology

Similar procedures to those outlined by Syed et al. and Mohd Daud et al. were used to select the research articles evaluated in this report. In the scientific database Google Scholar, the following keywords were used: "Blockchain," "Blockchain technology," "Unmanned aerial vehicles," "swarm communication," "UAV networks," and other combinations of these terms. There were initially 209 articles being considered. Since the articles concentrate on the most recent developments in the application of swarm UAV communication networks with blockchain technology, an initial filter based on publication date was used. The paper's results and originality, abstract and content analysis, technical level, and machine learning focus were additional prerequisites for admission. Thus, as seen in Table 1, 40 papers were chosen from the 209 papers.

2. Background

In this section, we briefly discuss various fundamentals of UAVs and UAV swarm, blockchain technology. Subsequently, we discuss how combining these technologies can open up many exciting possibilities for the future.

2.1. Unmanned aerial vehicles (UAV)

UAVs operate in a sophisticated manner and have both mechanical and electrical power components. Typically, these devices come with an operating system that runs the UAV software

[9]. An overall picture of the UAV technology in terms of their classifications based on different parameters, regulations regarding their operations and different application scenarios is presented below.

2.1.1. UAV classifications

A variety of characteristics, including wing type, weight, flying height, and flight mechanism, can be used to classify UAVs. Based on how they fly, UAVs can be categorized into the following groups [10]:

I.Multi-rotor *or rotary-wing UAVs*: These UAVs can take off, land vertically, and hover over a designated region. These drones are relatively less mobile than other types of UAVs. Furthermore, these UAVs consume more power because they have to defy gravity.

Ii.Fixed *wing UAVs*: Like commercial airplanes, these UAVs can fly through the atmosphere and carry heavy loads. This flying technique may allow them to move faster than other types of UAVs, but it also requires them to take off and land on a runway. Furthermore, they are usually more costly than multi-rotor UAVs and are unable to hover over a defined region.

Iii.Hybrid *fixed/rotary-wing UAVs*: This type of UAV is a compromise between the two methods discussed above, as it may switch between them. An illustration of this is the parrot, which can take off vertically, glide along its path, and then use its rotors to hover once again [11]

Civil aviation authorities frequently classify UAVs according to their gross weight. Based on their combined weight, UAV systems are classified into the following groups by the Australian Civil Aviation Safety Authority (CASA)[10], [12]:

i.Micro: Weighting less than 100 gms.

ii.Very small: Weighting more than 100 gms and less than or equal to 2 Kgs.

iii.Small: Weighting more than 2 Kgs and less than or equal to 25 Kgs.

iv.Medium: Weighting more than 25 Kgs and less than or equal to 150 Kgs.

v.Large: Weighting more than 150 Kgs.

2.1.2. UAV regulations

Regulations governing the use of UAVs in a given area are a significant issue since they are one of the factors limiting the growth of UAV networks. They must address a number of issues related to their operations, such as collision avoidance, data security, privacy, etc., and look into various UAV attributes, such as sort, spectrum, speed, etc.[13]. Broadly five important categories must be looked into when working on the UAV regulatory schemes [14].

i. Applicability: It refers to the extent to which UAV regulations must be applied. It may include UAV type, weight, and role of the UAVs.

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

ii. Operational limitations: It refers to specifying the locations, which are restricted for UAV operations.

iii. Administrative and legal requirements: This alludes to the set of rules that the local government put in place to regulate the use of UAVs. The UAV operators operating in that area must follow these stated procedures and guidelines.

iv. Technology specifications/requirements: It refers to the mechanical, communication and control capabilities of the UAV. For a particular application, some requirements are essential for the safe operation of the UAVs.

v. Moral and ethical issues: This mainly refers to the privacy and security issues of the people at large.

2.2 UAV networks:

The ground control station (GCS), UAVs, satellites, and multi-level communication linkages, including GCS-UAV, UAV-UAV, and satellite-UAV, are some of the sub-systems that make up a UAV network (Fig. 2). UAV networks can be divided into two categories based on communication: flying ad hoc networks (FANETs) and mobile ad hoc networks (MANETs) (Fig. 3). Because communication in a mobile ad hoc network (MANET) is decentralized, UAVs can freely connect with the GCS and with one another. Although there is less human supervision and involvement in MANET networks, the system can still function even if two entities lose their communication link. In a flying ad hoc network (FANET), other UAVs are free to connect with each other, but only the master UAV can communicate with the GCS. Even though FANETs provide humans with more control, the network can still operate even if communication between the GCS and the master UAV is lost [15].

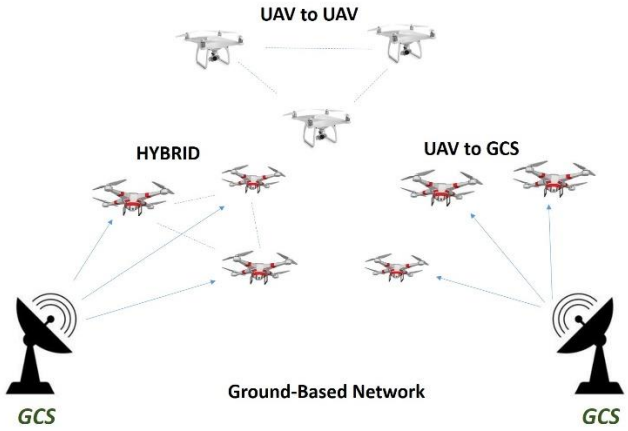

Figure 2. Multi-level communication in UAV

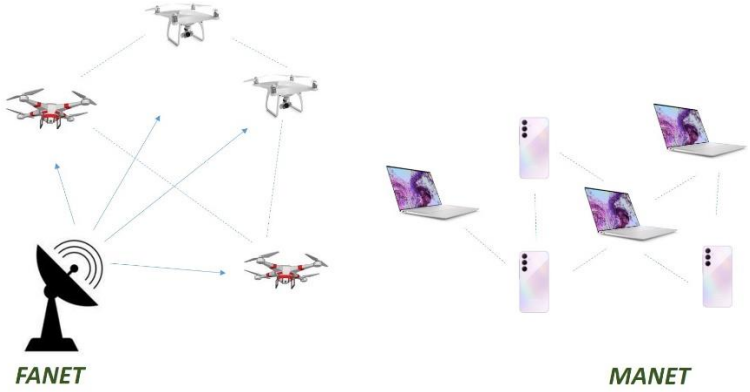

Figure 3. UAV networks classified into two types

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

2.3 UAV application

A new generation of promising applications for autonomous mission execution has been produced by the current UAV deployment efforts. This section identifies a few of significant UAV application areas in figure. 4.

2.3.1 Disaster management

In the event of an environmental or fabricated disaster, such as flooding, tsunamis, or terrorist attacks, UAVs can travel to areas that are unsafe for manned action. Transportation, water utilities, power, and telecommunications infrastructure are all susceptible to catastrophic disasters. UAVs can help with data collecting, debris navigation, and the requirement for prompt responses. Rescue crews can spot damage, begin immediate recovery activities, and send supplies like medical packs and first-aid manned helicopters with the use of UAVs fitted with sensors, radars, and high-resolution cameras. UAVs can help with real-time preventative measure discovery, disaster alarms, and disaster evaluation. Unmanned aerial vehicles (UAVs) can assist in locating and saving endangered humans and animals.

2.3.2 Remote sensing

Amateurs are increasingly using drone technology to gather high-resolution image data of remote locations, including islands, coasts, and mountaintops. UAVs are used to connect remotely sensed data from the air, the ground, and space. Spatial and temporal resolution observation is made possible by UAVs' affordability and lightweight characteristics.

2.3.3 Search and rescue (SAR)

By providing real-time image data of desirable places, UAVs have the potential to save a significant amount of time and resources. As a result, the SAR team can identify and pinpoint the exact location where assistance is required. For instance, drones can be used to protect people in remote deserts or forests, or to track down lost mountaineers on any journey. Therefore, drones could help track unfortunate victims and any challenging terrain or severe weather[16].

2.3.4 Precision agriculture

The use of UAVs in precision agriculture is a time- and money-efficient technique that can raise the income, effectiveness, and productivity of agricultural systems. Additionally, UAVs help with weed monitoring, insect damage, chemical spraying, and farm management, which leads to increased crop yields to address these challenges promptly. Smart farming could undergo a transformation with the use of UAVs and remote sensing[17].

2.3.5 UAVs for space exploration

The use of UAVs for planetary exploration has become more popular in recent years. UAVs have a lot of promise for carrying out our space missions, such studying the moon's atmosphere and surface. Although a variety of planetary exploration methods, These missions can be completed using tools including rovers, landers, orbiters, flying balloons, flying spacecraft, probes, and telescopes [18].

2.3.6 Real-time monitoring of road traffic

Many people are interested in the integration of UAVs with road traffic monitoring (RTM) systems. In RTM, UAVs can completely automate the transportation sector [19].

Drones can be used by local police to obtain a comprehensive image of traffic accidents or to carry out a massive security operation against illicit activities, such as auto theft, along the route. Vehicle recognition, raids on suspected vehicles, and the pursuit of armed robbers, hijackers, and anybody else who violates traffic laws are some other ramifications[20].

2.3.7 UAVs in emergency medical services

In several nations, UAVs have demonstrated their ability to combat the COVID-19 outbreak. It is important to note, nonetheless, that the national EMS institution, in conjunction with a number of other parties like EMS workers, nurses, and physicians, is the primary entity tackling COVID-19. Additionally, a number of policymakers are contemplating various preventive measures to combat COVID-19, such as the use of surgical masks, refraining from touching the face, frequent hand washing, city lockdowns, avoiding high-risk areas, avoiding social gatherings, and enforcing health codes[21].

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

2.3.8 UAVs for observation and communication in the marine domain

UAVs flying a few hundred meters above the sea surface and high-altitude platform stations (HAPS) flying up to 20 kilometers from the ground are examples of aerial platforms [22].

2.3.9 Flying cars and eVTOLs

No longer only a thing of fantasy, flying automobiles represent a significant advancement in the transportation sector. The transportation system of the future is expected to be revolutionized by flying cars and eVTOL (electric vertical take-off and landing) aircraft, which can significantly reduce travel time and the carbon footprint and greenhouse gas emissions of personal vehicles. More than 250 businesses have already begun working on eVTOLs and flying automobiles, and a small number of these vehicles may soon enter the commercial market [23].

2.3.10 Military Application

Drones are being widely deployed as flying weapons in military offensives. UAVs are generally used by enterprises to boost productivity and efficiency while lowering manufacturing costs and effort and enhancing accuracy[24].

Figure 4. UAV applications

2.4 UAV swarms

UAV swarms are classified as partially and fully autonomous in Figure 5. Additionally, this classification is separated into single-layer and multi-layered swarms. Every drone in the swarm has the ability to record and process data in real time. On the other hand, core processing occurs in the clouds or at the base station (BS). By deploying multiple drones, working in parallel, UAV swarms equipped with advanced monitoring mechanisms can quickly and reliably cover a zone. The utility of UAV swarms has been the subject of numerous studies. Such as [25] solves the problem of charging numerous drones simultaneously by analyzing swarms of drones. Swarms of UAVs are used for intelligent power management. UAV flight coordination and hovering endurance become crucial if swarms of UAVs, like quadcopters, are to complete their missions. Additionally, a successful operation depends on the quadcopter swarm's communication effectiveness. The authors devised a multi-robot coordination strategy in [26] to overcome the difficulties in synchronizing UAV swarms in real time over a wide area network. Swarms of UAVs have been examined in the context of surveillance in other studies. [27], for example, describes quadcopter swarms for object location and tracking operations.

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

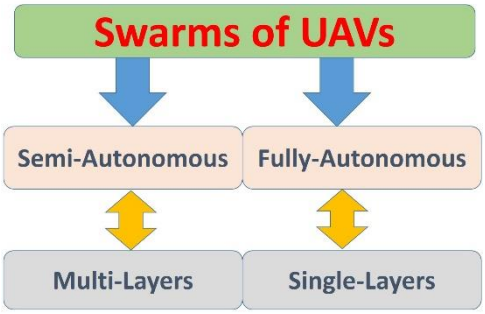

Figure 5. Classification of Swarm

3. Blockchain technology

A significant advancement in distributed ledger technology is blockchain technology. Since Satoshi Nakamoto released Bitcoin, a peer-to-peer electronic cash exchange system, its popularity has only grown [28]. Blockchain technology has enormous potential in various fields where mutually reliant parties need to trust one another. Its usefulness extends beyond electronic cash exchange platforms like Bitcoin, Litecoin, and others; it also helps make financial markets more intelligent [29].

By decentralizing cryptocurrency exchanges and providing an unchangeable list of transaction records, blockchain can prevent double spending, or the spending of cryptocurrency twice. Blockchain has emerged as one of the most innovative and cutting-edge technologies, with profound effects on a number of industries, including public services, healthcare, energy, supply chains, and finance[30].

3.1 Blockchain architecture

The data layer, network layer, consensus layer, contract layer, and application layer are the five main layers that comprise a blockchain. Figure 7 provides a visual depiction of the layers. Below is a discussion of the blockchain architecture, layer by layer.

1. Data layer: The data layer, the lowest layer in the blockchain architecture, contains the time-stamped data blocks. Each data block consists of the block header and the block body. The header of the current block contains the hash of the previous block, and the header of the next block contains the hash of the current block. This creates a linked list-like connection between the blocks. Figure 6 shows how a typical block in a blockchain is constructed.

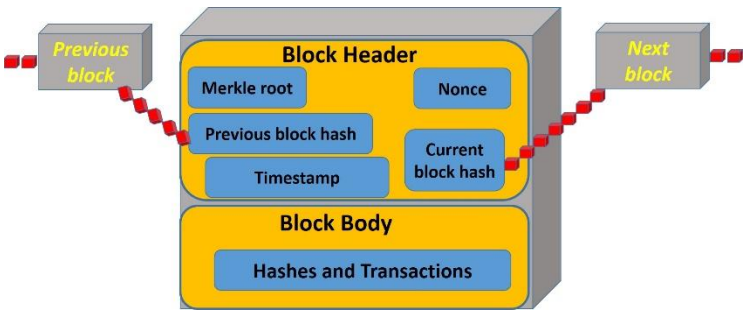

Figure 6. Typical structure of a block in a blockchain

2. Network layer: The network layer's functions include blockchain transaction distribution, forwarding, and authentication. Peer-to-peer (P2P) networks, in which peers have equal privileges, are frequently used to mimic blockchains. A transaction is broadcast to nearby nodes for confirmation as soon as it is made. This is carried out in accordance with predetermined guidelines. The transaction is transmitted to the other nodes after validation, and if it is rejectedIt is thrown away. This guarantees that each node can only record legitimate transactions. Transactions are often authenticated using an asymmetric cryptography method based on the digital signature [31].

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

3. Consensus layer: Numerous consensus methods make up this important layer, which is required to get the untrusted participants in the blockchain network to agree. This is essential to the concept of blockchain technology since it relies on member consensus to do away with the requirement for a centralized organization. Certain protocols are necessary to ensure consensus among blockchain participants. The primary processes for consensus [31] are Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT).

4. Contract layer: The blockchain may be programmed thanks to the contract layer, which also makes it possible to add various scripts, smart contracts, and algorithms that allow for the execution of intricate transactions. A smart contract is a set of guidelines that, when followed, cause a transaction to take place between the two parties[32].

5. Application layer: The blockchain's topmost layer contains its applications in a number of real-world domains, including banking, artificial intelligence, and the Internet of Things.

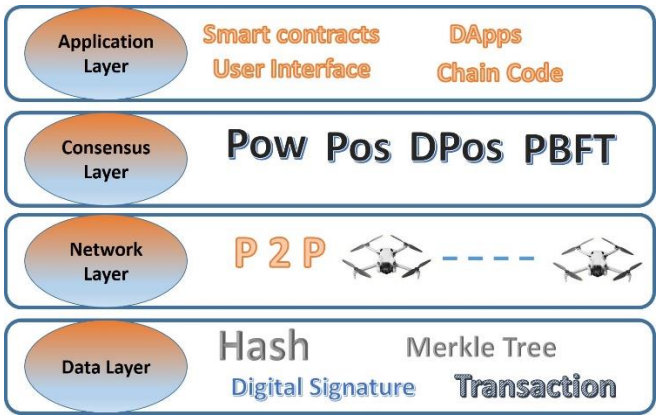

Figure 7. Block chain architecture Layers

4. Related work (Previous survey Blockchain with UAV)

This [33] To increase the usefulness of UAV swarms, it is essential to concentrate on developing them with autonomous coordinating capabilities for UAV-to-UAV communication. Numerous constraints that limit the usefulness of UAVs are removed by the employment of cellular mobile frameworks, such as communication range, networking difficulties, and size-weight-and-power issues. Furthermore, 5G technologies offer cellular networks a strong and dependable backbone for machine-to-machine communication.

This review [34] discusses the key elements of UAV swarms, such as autonomy, coordination, security, swarm formation control, communication, and swarm path planning. It also looks at how recent developments in UAV swarm algorithms have enabled the creation of intricate UAV swarm systems. This study offers a thorough analysis of UAV swarm technology, discussing how it has the potential to transform numerous industries and spur further development.

This [35] The survey establishes the foundation for creating a fully resilient system by assessing the body of research on resilient multi-UAV systems. A thorough study that offers an overview of all UAV swarm components and modules has not yet been conducted, according to the research emphasis section, which also offers a general trendline of study directions.

This [36] The survey provides fresh insight into the prospects and problems of the subject applications and advances knowledge of blockchain, machine learning, and watermarking methods for UAV security.

In [37] Blockchain technology and physical layer security (PLS) are intriguing additions to current techniques. PLS can improve communications security by taking advantage of wireless link properties, and blockchain could make networks more decentralized, reliable, and intact.

This [38] The study also looks at possible directions for UAV development, such as transformability, swarming and cooperative control, downsizing, connectivity, artificial intelligence, and remote sensing. The basic hardware and software architectures of UAVs, including as flight processors and controllers, sensors, actuators, batteries, communication interfaces, payloads, and structural elements, are also discussed in the study.

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

In [39] A reference architecture is presented in this research along with a comparison of its possible advantages over conventional BC-based UAV networks. Potential future directions are explored along with unresolved problems and difficulties. Lastly, a case study on logistics for FL-oriented UAVs located in BC in 6G networks is provided. By providing essential integrating principles across a wide range of application sectors, the survey seeks to assist researchers in creating viable UAV solutions.

In [40] The blockchain-enabled UAV communication ecosystem is highlighted in this paper. The use of blockchain technology and FL to improve UAV wireless communications raises a number of security issues. One significant issue is the security and privacy issues, which are thoroughly examined, and blockchain presents a viable remedy.

In [41] provide a thorough analysis of drone communication security and suggest a blockchain-based intelligent and safe drone communication system that is based on 5G communication networks and artificial intelligence (AI) methods. The InterPlanetary File System (IPFS), which is used as a platform for data storage in the suggested design, guarantees enhanced network performance, communication security and privacy, and lowers transaction storage costs.

In [42] examine the many uses of blockchain in UAV networks, including decentralized storage, network security, inventory control, monitoring, and more, and talk about some more general viewpoints on the subject. We also go over a number of issues that need to be resolved in order to integrate blockchain technology with unmanned aerial vehicles (UAVs) and offer some ideas for future study.

this paper [43] outlines the classification of current security threats in UAV networks with 5G capability. Based on the survey results, we present a security solution based on Blockchain (BC) and a summary of the research challenges in integrating BC with 5G-enabled UAVs.

This paper [44] provides a survey on how blockchain technology might be integrated with aerial communications (BAC). First, we look at the security problems that are now plaguing aerial communication networks, the benefits of blockchain technology, and the viability and potential of using blockchain technology to address the security problems that are currently plaguing these networks. We then go into detail on the existing associated methods for using the blockchain to address the security problem in aerial communication networks.

in this article[45], we present a broad survey on the architecture, requirements, and use cases of 6G technology. It also presents a solution taxonomy based on the applications of UAV communication. Based on the findings from the survey, we present a blockchain-envisioned security solution and 6G-enabled network connectivity in UAV communication.

In [46] In this paper,they start by discussing mobile edge computing (MEC) and 5G communication networks as possible technologies that can help with some of the issues brought up and provide a number of benefits to drone-enabled environments. Furthermore, we outline the present state of the art and try to address each of the latter issues in our discussion of 5G and MEC techniques. Next, blockchain technology is presented as an innovative solution to the security issues since it is decentralized and, hence, inherently safe.

This [47] The article initially classifies drone applications in medicine before outlining some of the major obstacles in these fields. Next, we provide an overview of 5G and blockchain, examining its inherent features to offer dependable connectivity and improved data security.

This [48]study focuses on securing data transfer from the Unmanned Aerial Vehicle (UAV) to the Ground Control Station (GCS) in order to maintain data/information confidentiality (confidentiality), data/information integrity (integrity), and certainty of data/information availability (availability).

Yahuza et al. [49] In order to offer effective drone communications, they examined current IoD designs and suggested a secure architecture built on mobile edge computing (MEC). Additionally, they proposed a drone classification system and outlined each class's security flaws. In addition, they presented a taxonomy of attacks, talked about the necessary defenses, and offered fixes to lessen the dangers that were found.

Hassija et al. [50] examined the security risks, including significant assaults. Additionally, they displayed the security flaws in many drone applications. The authors also talked about how to improve drone communications security by utilizing four cutting-edge technologies: fog computing, blockchain, software-defined networking (SDN), and machine learning. They did not, however, compare the security solutions that were examined.

In [51] The findings of the performance evaluation demonstrate that the blockchain-based suggested UAV big data privacy protection method has minimal processing costs for key generation, encryption, and decryption. Additionally, it performs better than traditional methods.

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

Table 1: An examination of other related review and survey literature of UAV networks

. Ref.	Analysis type	year	Areas explored during the analysis	limitation	goals	Tech. Domain
[33]	Review	2018	The use of cellular mobile framework alleviates many limiting factors that hinder the utility of UAVs including range of communication	range of communication, networking challenges, and size-weight-and-power considerations	to enable higher levels of swarm autonomy and dependability.	5G, NO
[34]	Review	2024	Covers the important aspects of UAV swarms including swarm formation control, communication, swarm path planning, autonomy, coordination, and security.	Provides insight into ethical aspects and the use cases of UAV swarms in various military, civilian, and entertainment applications.	increase swarm efficiency and commercial utility	YES
[35]	Survey	2022	Resilient multi-UAV systems and lays down the groundwork for how best to develop a truly resilient system.	controlling the vehicles a challenge	UAV swarm components that affect overall swarm resilience	NO
[36]	Survey	2021	Survey of optimal techniques, which are used for securing UAVs applications	the security a major concern	understanding of the blockchain, ML, and watermarking techniques for securing UAVs	ML, Waterma -rking NO
[37]	Survey	2023	PLS can enhance the security of communications, while blockchain may enable networks' decentralization, integrity, and trustworthiness	lack of network transparency, management decentralization, and reliability	high traffic throughput, ultra-massive connectivity, extremely low latency, and high quality of service	
[38]	Review	2023	explores potential areas for further development in UAVs, including communication, artificial intelligence, remote sensing,	NA	analysis of UAV development, covering various research directions in the last three years	AI, communi c-ations, IoTs NO

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

[39]	Survey	2022	BC-based FL-oriented UAVs in 6G networks are the subject of a case study on logistics.	UAVs have limited power and battery life, making them resource-constrained.	Permit GS and UAV swarms to safely share FL updates.	FL,6G NO
[40]	Survey	2023	Thoroughly examines the integration of privacy and security in blockchain-assisted UAV communication.	data exchanges in those networks, security threats	a collection of essential needs and basic analyses that can support the development of blockchain privacy and security models	NO
[41]	Survey	2020	propose a blockchain-based secure and intelligent drone communication architecture underlying 5G and (AI) techniques with IPFS	storage costs with communication reliability, latency, and bandwidth issues	uses an (IPFS) as a platform for data storage, which ensures improved network performance	5G + AI + IPFS NO
[42]	Review	2020	Examine the different ways that blockchain is being used in UAV networks for network security, decentralized storage, inventory control, and monitoring.	intra-UAV communication, UAV security, air data security, data storage and management	Communication, UAV security, air data security, and data management and storage issues were resolved.	NO
[43]	Review	2019	Information on BC technology and UAV networks along with their security issues, vulnerabilities, and solutions	Security concerns with UAV networks provided by 5G	provide a strong and secure network	5G NO
[44]	Survey	2021	Examine aerial communication networks and the security concerns they face today.	security issue in aerial communication networks	Using blockchain technology to address the present security vulnerability in aerial communication networks	NO
[45]	Review	2020	Give a thorough overview of 6G technology's design, specifications, and applications.	Since UAVs are highly mobile and dynamic, typical UAV communication is insufficient.	study of a blockchain-envisioned UAV communication using 6G networks to secure Industry 4.0 applications	6G networks to secure Industry 4.0 NO

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

[46]	Review	2021	Talk about blockchain-based mobile edge computing (MEC) and 5G communication networks.	Balancing drone weight, battery capacity, and computational	Resources Describe the recently resolved security issues with drone communication networks.	5G, MEC NO
[47]	-	2021	Drone applications in medicine, followed by a discussion of some of the major obstacles in these fields. Next, we provide an overview of blockchain and 5G.	high data rate, low latency	Analytical findings show how 5G and blockchain technology can be used to further drone applications in medicine.	5G + medical application NO
[48]	Review	2023	securing data transfer from the Unmanned Aerial Vehicle	possible threats from other parties	securing data transfer on the UAV	No
[49]	Review	2021	highlight the need for secured IoD architecture, taxonomy of the attacks on the IoD network, review the recent IoD attack mitigating techniques	Security and privacy threats of drone categories.	aims to assess the recent trends in the security and privacy issues that affect the IoD network	NO
[50]	Survey	2021	They displayed the various drone applications' security flaws.	vulnerabilities of different drone applications	Using fog computing, blockchain, software-defined networking (SDN), and ML to improve drone communications	NO
[51]	-	2021	UAV big data privacy protection scheme based on blockchain technology	Data privacy protection	Establish a framework for upcoming studies on the privacy protection of UAV data.	NO
This Work	Survey	2024	In order to address such problems, this work demonstrates how blockchain technology can be integrated with swarm UAV communications	As Show in table 2	improve UAV network security and facilitate the development of data management and transfer	YES

5. State of Art Blockchain with UAV swarm

Islam et al. [52] suggested a data collecting method safeguarded by blockchain. It makes use of a group of UAVs to gather data from Internet of Things devices and send it to a server. Before delivering the data to the closest server, it also encrypts it. However, data cannot be added to the blockchain unless all validators agree.

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

Bera et al. [53] presented a brand-new, secure blockchain-based solution for IoD communication entities to manage their data. The proposed method can address a number of known potential assaults. When compared to other analogous schemes, the suggested approach performs better in terms of computing overheads and communication.

Hassija et al. [54] suggested a security architecture based on blockchain technology enabling drones to establish base stations in a tactile Internet setting. These airborne base stations can be employed in a variety of settings, including rural locations, public gatherings, and disasters. Additionally, a simple smart contract was implemented to make judgments and strategies for network billing automatically.

Aggarwal et al. [55] created a productive system that uses blockchain technology to provide safe data distribution in the Internet of Devices. There are two different kinds of nodes in the suggested system: normal and forger nodes. According to the validation results, the blockchain security model performs well in terms of cost and communication latency.

Tan et al. [56] suggested a blockchain-based distributed key management system for heterogeneous drones. To speed up the mining process, they also proposed an effective miner election technique. When compared to PoW and PoS algorithms, the suggested consensus approach takes less time.

In [3] Blockchain tools (e.g., Hyperledger Fabric) offer promising solutions in preserving CIA properties. Applying blockchain appropriately will allow developers to implement trustworthy UAV systems in domains such as search and rescue, traffic management, infrastructure inspection, and many other areas.

For example, in [57], To improve the security of routing in 5G NR cellular networks, a lightweight blockchain and an intriguing message routing technique between UAV nodes are suggested.

In this paper[58], Solidity has been used to create a compact, lightweight, and effective smart contract that automates the process of choosing a place inside a certain swarm formation structure. Additionally, a method for selecting a new leader is proposed.

In [59] By verifying information about occurrences from several sources, this research suggests a method for preserving security in UAV networks during monitoring. The suggested method makes use of a pre-shared list of authorized UAVs and secure asymmetric encryption.

In [60], With the use of a UAV, data are encrypted using the suggested method before being transmitted to the MEC server. After receiving the data, the MEC server confirms the sender's identity. The data is saved on the blockchain following a successful validation and validators' approval.

In[61] This article proposes a crowd monitoring system that supports high mobility and security enhancement assisted by a drone swarm. The blockchain technology is used to ensure the authenticity of the identity of UAV nodes, the reliability of UAV cooperation in monitoring tasks, the confidentiality of information in the process of data transmission

In [62] This study applies federated blockchain to the UAV swarm communication network and proposes a UAV Swarm Communication Network based on Fabric (USCNoF). In order to create a practical and safe UAV swarm communication network, the drawbacks of a slow and ineffective blockchain are addressed while utilizing the benefits of decentralization and blockchain security.

In this work[63], In order to accomplish low-latency and high-reliability data transmission, 6G technology is utilized to support communication between FANET and PC as well as between FANET and DCN. It is also utilized to provide real-time communication security and ubiquitous management of UAVs.

A new method that uses blockchain technology to enable a UAV swarm to carry out surveillance missions at particular points of interest (POIs) is suggested in [64]. While certain additional nodes on the ground have specialized functions (like as route planning and financial transactions), the blockchain is integrated inside the UAVs.

This approach establishes a distributed identity authentication method based on DID information. Additionally, a secure communication architecture based on blockchain and a collection of secure transmission protocols are built in conjunction with encryption to guarantee the safe transmission of UAV communication data[65].

In [66] they suggest a distributed UAVs scheme that uses blockchain technology and a cloud server with a network topology akin to the Internet of Things. Rather than utilizing the standard blockchain method directly, which necessitates costly processing and significant bandwidth overhead.

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

In[67]This article presents a blockchain-based AI-empowered pandemic situation supervision scheme in which a swarm of drones embedded with AI is engaged to autonomously monitor pandemic outbreaks, thereby keeping human involvement as low as possible.

In [68]we present a novel blockchain-based technique to support multi-party authentication to facilitate trustworthy group communications. Specifically, this allows us to provide secure P2P wireless communications and trusted group communication management for UAV networks, while ensuring service efficiency.

In [69] provide a blockchain-envisioned softwarized multi-swarming UAV communication system built on a 6G network with intelligent connectivity, terahertz (THz) frequency bands, and link and physical-level protocol virtualization. In comparison to departing 4G/5G-based systems, the results demonstrate that the suggested approach performs better in terms of processing delay, packet loss reduction, and throughput.

we [70] suggest a novel kind of UAV network called SUV that is built on SDN architecture and blockchain technologies. SUV uses blockchain technology to create a physically dispersed but logically centralized control plane that handles the UAV network's configuration management and routing calculations. It is appropriate for 5G-oriented UAV networking and offers characteristics like programmability, flexibility, security, and survivability.

In [71] The authors of this study describe a blockchain-based adaptive networking mechanism for UAVs that combines three essential technologies. UAVs can accomplish quick identification verification and effective swarm switching by using Global Unique Identifiers (GUID) and block storage.

In [72] More important distributed functions are implemented in each UAV on demand by the proposed RHCRB. The activities carried out by RHCRB include on-demand topology management, secure handover coordination, regenerative blockchain principles (authentication of each UAV and active edges), dynamic location-based cost magnitude calculations, trusted location monitoring schemes (internal and cooperative UAV movements), and confidential link management principles.

Table 2: A summary major research focus for swarm UAV networks communications.

Ref.	Year	Method used	Main contribution	Considerati-on Security	challenges	Applicatio n domain
[52]	2019	UAV + Swarm + IOT	protected data collection	Authenticati-on	NA	IOT Applicatio n
[53]	2020	Access control mechanism among the drones and the GSS in the flying zones	Data management	Access control	B.C PBFT	IOD environme nt
[54]	2020	Suggested a security architecture based on blockchain technology enabling drones to establish base stations in a tactile Internet setting.	A security layer for securing the inner communication between resource-constrained UAV.	Security	Data security	adisaster, public events, rural areas,
[55]	2019	created a productive method utilizing blockchain technology to provide safe data distribution in IoD	secure data dissemination in IoD using blockchain	integrity, identity anonymity, authenticationa uthorization, accountability	Access control,cost	IoD environme nt.

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

[56]	2020	blockchain-based distributed key management scheme for heterogeneous FANET	Enhance communication security, Blockchain and drone	Security Confidently Authentication,	attack target, increase the communication overheads of drones	IOT Application
[57]	2021	Blockchain to improve swarm UAS networking routing security	Goals avoid the malicious onnections	Authenticati-on	attacks to swarm UAS networking	All Application
[58]	2023	Create a dependable and safe framework for communicating with UAV swarm.	Drones without a centralized authority may safely communicate data.	Authorization	centralized authority (ground station)	Military application
[59]	2019	Method makes use of a pre-shared list of authorized UAVs and secure asymmetric encryption.	security mechanism for detecting compromised UAVs in UAV networks for supporting surveillance	Authentication	security challenges because of its dynamic topology	Surveillance applications
[60]	2019	Using UAVs as a relay, the data is collected from IoTs and safely stored on the blockchain at the MEC server.	data acquisition process in which information is gathered from IoTs	Integrity, Authentica-tion	Potential cyberthreats could affect communication between these entities.	Data collection application
[61]	2021	Suggests a distributed monitoring system in a blockchain-powered network that is assisted by drones and swarms.	replacing the human factor to ensure scalability and reduce risk	Confidently Authentication Availability,	reliability and privacy of the system	Crowd moniter
[62]	2022	Hyperledger Fabric-based UAV swarm communication network architecture (USCNoF)	Using a UAV swarm communication network with blockchain technologies	Authentication,	Robustness, communicate and share information securely	swarm network
[63]	2024	An architecture for ubiquitous UAV task security management based on blockchain and 6G	UAV and swarm Task Security Management security and privacy of VC	Authentication Access control	Latency, Reliability transmission of data.	All Application

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

[64]	2021	Using blockchain technology, a UAV swarm may carry out surveillance flights at particular points of interest (POIs).	Allow a set of Points-Of-Interest (POI) to be surveyed by a set of autonomous UAVs	Security	existence of some control center	surveillance system
[65]	2022	examines the benefits and latest developments of blockchain technology in UAV swarm	Under this concept, a distributed identity authentication system based on the distributed identity identifier (DID)	Authenticati-on,	One point of failure caused by centralized administration	Military Application,
[66]	2020	Distributed UAVs scheme with blockchain technology with cloud server.	mitigates th privacy and security threats of UAV system	Confidently, Integrity, Availability, privacy	protecting communications between UAVs and ground control system	IOT application
[67]	2021	Blockchain + AI+ swarm drone	monitor pandemic outbreaks	Authentication	poor network connectivity	COVID19
[68]	2021	Blockchain (distributions)and communications in UAV	support multi-party authentication to facilitate trustworthy group communications	Authentication	security and privacy considerations in such deployments	COVID19
[69]	2020	blockchain-envisioned softwarized multi-swarming UAV communication scheme based on a 6G	blockchain supports data security	Access control	Data share security bottleneck on 5G networks	COVID19
[70]	2021	UAV network based on SDN architecture and blockchain technology(SUV)	SUV uses a control plane that is physically dispersed but intellectually centralized.	Authentication	Attacks	All Application
[71]	2023	Used three key technologies. Utilizing Global Unique Identifier (GUID) and block storage with blockchain	rapid identity authentication and efficient swarm switching	Authentication	Limited computing and storage resources	All application
[72]	2024	a new Reactive Handover Coordination System with Regenerative Blockchain (RHCRB)	authentication of each swarm UAV and active edges	Authentication	security breaches, malfunctions, link failures	Military Application

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

6. Open issues and challenges

Swarm UAV (Unmanned Aerial Vehicle) communication using blockchain has a number of issues that must be resolved for deployment and operation to be successful. Figure 8.9 illustrates a few of the various applications and difficulties for a blockchain:

Limited Computing Resources: Usually, swarm UAVs have a small amount of processing and storage capacity on board. Individual UAVs in a swarm may experience resource strain when blockchain technology is implemented, as it necessitates substantial computational resources for consensus techniques, transaction processing, and maintaining a distributed ledger. To overcome this obstacle, resource-efficient blockchain protocols and algorithms must be optimized as it was mentioned in [71].

Real-Time Communication Requirements: Swarm UAVs' real-time communication needs may not be met by blockchain networks' consensus procedures, which frequently cause lag in transaction processing. For a swarm of UAVs to successfully complete a mission and conduct coordinated operations, prompt and responsive communication is essential. One of the main challenges is juggling the demands of low-latency connectivity with secure transactions as it was mentioned in [56], [60], [67], [66], [63].

Energy Consumption: Energy consumption for blockchain operations, including mining and validation procedures, is high. The energy-intensive nature of blockchain operations can rapidly deplete the power supply for UAVs with short battery lives, lowering the swarm UAVs' flight duration and operational effectiveness. To overcome this obstacle, energy-efficient blockchain protocols and processes that are adapted to the limitations of UAVs must be developed. As stated in [52], [56], [57].

Scalability: As the number of UAVs in a swarm increases, scalability becomes a critical issue for blockchain networks. Managing a large number of transactions and maintaining consensus among multiple nodes in a swarm can lead to performance degradation, network congestion, and inefficiencies. Designing scalable blockchain solutions that can accommodate the dynamic nature of swarm UAV deployments is essential for ensuring smooth and efficient communication. As it was mentioned in [61], [63].

Security and Privacy: Ensuring data privacy, security, and protection of sensitive information in a swarm UAV communication network is paramount. Blockchain offers inherent security features such as immutability and transparency, but implementing secure encryption mechanisms and access control policies without compromising performance is a challenge in resource-constrained environments. Safeguarding data integrity and confidentiality while maintaining efficient communication is a critical challenge for blockchain-enabled swarm UAV system. As it was mentioned in [54], [59], [68], [69],

Blockchain technology offers potential solutions to address these challenges in swarm UAV communication:

1) Enhanced Security: Blockchain technology's intrinsic immutability and cryptographic properties offer a robust security framework for UAV communication. By preventing tampering with transactions and data, blockchain's decentralized feature ensures the security and integrity of UAV communications.

2) Trust and Decentralization: Blockchain uses a distributed ledger to do away with the necessity for a centralized authority in UAV communication. This allows all parties to independently verify and record transactions and interactions, thereby fostering transparency and trust among stakeholders.

3) Smart Contracts and Automation: Automated and self-executing agreements between UAVs and other parties are facilitated by smart contracts on the blockchain. This ensures regulatory compliance, streamlines processes, and supports secure and transparent transactions.

4) Transparency and Data Integrity: Blockchain provides a transparent and safe framework for UAV data recording and exchange. This ensures data traceability and integrity, enabling auditable and responsible UAV operations.

5) Standardization and Interoperability: By giving UAVs and ground systems a uniform foundation for communication and data exchange, blockchain-based protocols can promote interoperability and standardization. This encourages smooth platform-to-platform integration and cooperation.

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

Figure 8. Blockchain and UAV swarm with several Applications

Figure 9. Blockchain with several challenges

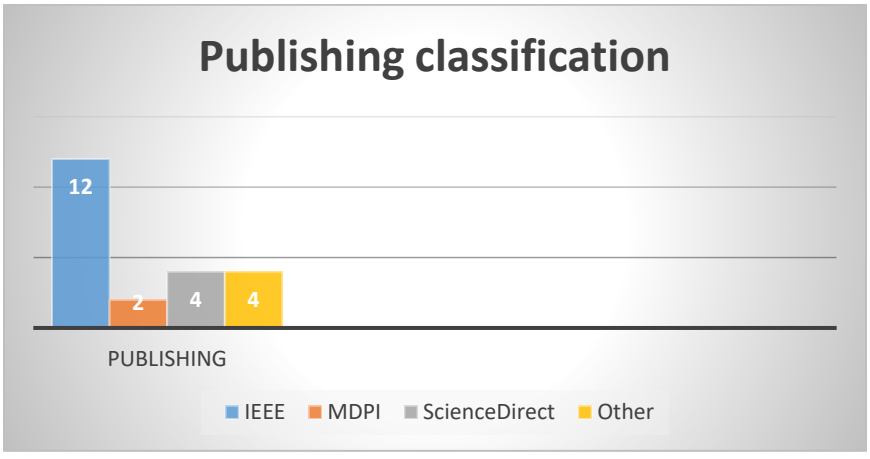

Figure 10. Classification of Articles

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

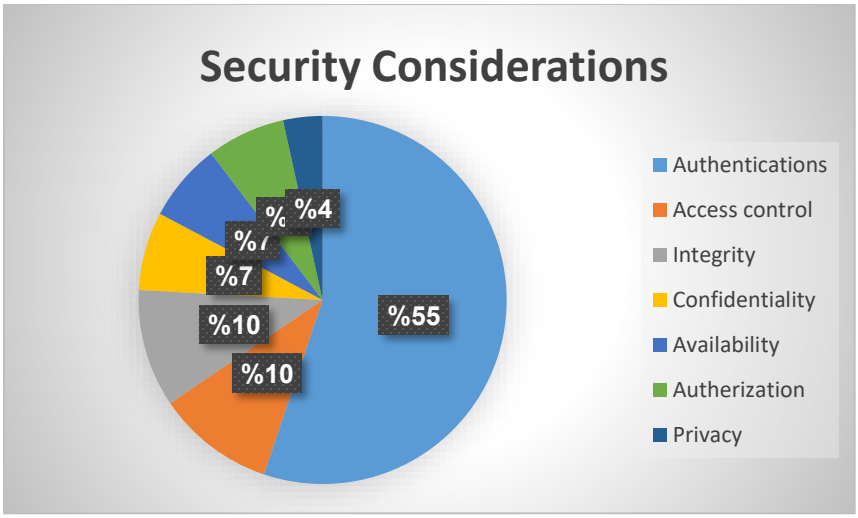

Figure 11. The security considerations

7. Conclusion

As the use of UAV networks grows in a variety of applications, it is imperative that communication lines between UAVs be secured to preserve confidentiality, integrity, and availability (CIA) qualities. As the network grows in size, blockchain technology has the ability to guarantee security and transparency. Our research shows how blockchain technology and a consensus process may be used to secure UAV network communications. The finest security feature in this article is authentication, which performs better than the others do. Future work will involve expanding the existing work by putting the concept into practice in actual UAV networks and testing it for scalability, network performance, storage, and resource requirements for transactions.

Conduct a comprehensive and updated review of innovative and effective solutions for swarm UAV communications and networks in various fields, Internet of Things applications, military applications, and crowd control, some technologies have been used and integrated with blockchain to enhance the ability of swarm UAV communication ne and networks to transfer, manage and share data from them

(IOT, IOD, 5G, 6G, AI, MEC, SDN, cloud), the study concentrated on swarm UAV network communications in various applications to gather and exchange data, enhance the swarm network, enhance network security, and lower energy consumption.

Reference

[1] Kang, H., et al., "Protect your sky: A survey of counter unmanned aerial vehicle systems," IEEE Access, vol. 8, pp. 168671-168710, 2020.

[2] Islam, A. and S.Y. Shin, "BHMUS: Blockchain based secure outdoor health monitoring scheme using UAV in smart city," in 2019 7th International Conference on Information and Communication Technology (ICoICT), 2019, IEEE.

[3] Jensen, I.J., D.F. Selvaraj, and P. Ranganathan, "Blockchain technology for networked swarms of unmanned aerial vehicles (UAVs)," in 2019 IEEE 20th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2019, IEEE.

[4] Konert, A. and T. Balcerzak, "Military autonomous drones (UAVs) - from fantasy to reality. Legal and ethical implications," Transportation Research Procedia, vol. 59, pp. 292-299, 2021.

[5] Majeed, R., et al., "Drone security: Issues and challenges," Parameters, vol. 2, no. 5, 2021.

[6] Pandey, G.K., et al., "Security threats and mitigation techniques in UAV communications: A comprehensive survey," IEEE Access, vol. 10, pp. 112858-112897, 2022.

[7] Afaq, A., et al., "Blockchain-based collaborated federated learning for improved security, privacy and reliability," arXiv preprint arXiv:2201.08551, 2022.

[8] Sachdeva, H., et al., "Improving privacy and security in unmanned aerial vehicles network using blockchain," arXiv preprint arXiv:2201.06100, 2022.

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

[9] Solomentsev, O., et al., "UAV operation system designing," in 2015 IEEE International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD), 2015, IEEE.
[10] Fotouhi, A., et al., "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3417-3442, 2019.
[11] Parrot Mambo FPV. [Online]. Available: https://www.parrot.com/global/drones/parrot-mambo-fpv.
[12] Civil Aviation Safety Authority (CASA), "Drone Types." [Online]. Available: https://www.casa.gov.au/drones/rules/drone-typesv, 2019.
[13] Mozaffari, M., et al., "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2334-2360, 2019.
[14] Stöcker, C., et al., "Review of the current state of UAV regulations," Remote Sensing, vol. 9, no. 5, p. 459, 2017.
[15] Ghribi, E., et al., "A secure blockchain-based communication approach for UAV networks," in 2020 IEEE International Conference on Electro Information Technology (EIT), 2020, IEEE.
[16] Shakhatreh, H., et al., "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges," IEEE Access, vol. 7, pp. 48572-48634, 2019.
[17] Reinecke, M. and T. Prinsloo, "The influence of drone monitoring on crop health and harvest size," in 2017 1st International Conference on Next Generation Computing Applications (NextComp), 2017, IEEE.
[18] Sharma, M., et al., "Survey on unmanned aerial vehicle for Mars exploration: Deployment use case," Drones, vol. 6, no. 1, p. 4, 2022.
[19] Menouar, H., et al., "UAV-enabled intelligent transportation systems for the smart city: Applications and challenges," IEEE Communications Magazine, vol. 55, no. 3, pp. 22-28, 2017.
[20] Elloumi, M., et al., "Monitoring road traffic with a UAV-based system," in 2018 IEEE Wireless Communications and Networking Conference (WCNC), 2018, IEEE.
[21] Pulsiri, N. and R. Vatananan-Thesenvitz, "Drones in emergency medical services: A systematic literature review with bibliometric analysis," International Journal of Innovation and Technology Management, vol. 18, no. 04, p. 2097001, 2021.
[22] Alqurashi, F.S., et al., "Maritime communications: A survey on enabling technologies, opportunities, and challenges," IEEE Internet of Things Journal, vol. 10, no. 4, pp. 3525-3547, 2022.
[23] Swaminathan, N., et al., "Flying cars and eVTOLs—technology advancements, powertrain architectures, and design," IEEE Transactions on Transportation Electrification, vol. 8, no. 4, pp. 4105-4117, 2022.
[24] Lucia, L.D. and A.M. Vegni, "UAV Main Applications: From Military to Agriculture Fields," in Internet of Unmanned Things (IoUT) and Mission-based Networking, Springer, 2023, pp. 1-23.
[25] Lee, D., J. Zhou, and W.T. Lin, "Autonomous battery swapping system for quadcopter," in 2015 International Conference on Unmanned Aircraft Systems (ICUAS), 2015, IEEE.
[26] de Souza, B.J.O. and M. Endler, "Coordinating movement within swarms of UAVs through mobile networks," in 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), 2015, IEEE.
[27] Pestana, J., et al., "A vision-based quadrotor swarm for the participation in the 2013 international micro air vehicle competition," in 2014 International Conference on Unmanned Aircraft Systems (ICUAS), 2014, IEEE.
[28] Nakamoto, S., "Bitcoin: A peer-to-peer electronic cash system," Decentralized Business Review, 2008.
[29] Bansal, G., et al., "Smart stock exchange market: A secure predictive decentralized model," in 2019 IEEE Global Communications Conference (GLOBECOM), 2019, IEEE.
[30] Bitcoin, N.S., "Bitcoin: A peer-to-peer electronic cash system," 2008.
[31] Xie, J., et al., "A survey of blockchain technology applied to smart cities: Research issues and challenges," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2794-2830, 2019.
[32] Kosba, A., et al., "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in 2016 IEEE Symposium on Security and Privacy (SP), 2016, IEEE.
[33] Campion, M., P. Ranganathan, and S. Faruque, "UAV swarm communication and control architectures: A review," Journal of Unmanned Vehicle Systems, vol. 7, no. 2, pp. 93-106, 2018.
[34] Javed, S., et al., "State-of-the-art and future research challenges in UAV swarms," IEEE Internet of Things Journal, 2024.
[35] Phadke, A. and F.A. Medrano, "Towards resilient UAV swarms—a breakdown of resiliency requirements in UAV swarms," Drones, vol. 6, no. 11, p. 340, 2022.

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

[36] Syed, F., et al., "A survey on recent optimal techniques for securing unmanned aerial vehicles applications," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 7, p. e4133, 2021.
[37] Ghourab, E.M., et al., "Interplay between physical layer security and blockchain technology for 5G and beyond: A comprehensive survey," Authorea Preprints, 2023.
[38] Telli, K., et al., "A comprehensive review of recent research trends on unmanned aerial vehicles (UAVs)," Systems, vol. 11, no. 8, p. 400, 2023.
[39] Saraswat, D., et al., "Blockchain-based federated learning in UAVs beyond 5G networks: A solution taxonomy and future directions," IEEE Access, vol. 10, pp. 33154-33182, 2022.
[40] Hafeez, S., et al., "Blockchain-assisted UAV communication systems: A comprehensive survey," IEEE Open Journal of Vehicular Technology, 2023.
[41] Tanwar, R.G.A.K.S., "Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications."
[42] Alladi, T., et al., "Applications of blockchain in unmanned aerial vehicles: A review," Vehicular Communications, vol. 23, p. 100249, 2020.
[43] Mehta, P., R. Gupta, and S. Tanwar, "Blockchain envisioned UAV networks: Challenges, solutions, and comparisons," Computer Communications, vol. 151, pp. 518-538, 2020.
[44] Kumar, R.L., et al., "Blockchain for securing aerial communications: Potentials, solutions, and research directions," Physical Communication, vol. 47, p. 101390, 2021.
[45] Aggarwal, S., N. Kumar, and S. Tanwar, "Blockchain-envisioned UAV communication using 6G networks: Open issues, use cases, and future directions," IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5416-5441, 2020.
[46] Han, T., et al., "Emerging drone trends for blockchain-based 5G networks: Open issues and future perspectives," IEEE Network, vol. 35, no. 1, pp. 38-43, 2021.
[47] Chen, J., et al., "Exploiting 5G and blockchain for medical applications of drones," IEEE Network, vol. 35, no. 1, pp. 30-36, 2021.
[48] Gunawan, H., et al., "Unmanned aerial vehicle (UAV) data transfer security: A systematic literature review," in AIP Conference Proceedings, 2023, AIP Publishing.
[49] Yahuza, M., et al., "Internet of drones security and privacy issues: Taxonomy and open challenges," IEEE Access, vol. 9, pp. 57243-57270, 2021.
[50] Hassija, V., et al., "Fast, reliable, and secure drone communication: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2802-2832, 2021.
[51] Lv, Z., et al., "Analysis of using blockchain to protect the privacy of drone big data," IEEE Network, vol. 35, no. 1, pp. 44-49, 2021.
[52] Islam, A. and S.Y. Shin, "BUS: A blockchain-enabled data acquisition scheme with the assistance of UAV swarm in the Internet of Things," IEEE Access, vol. 7, pp. 103231-103249, 2019.
[53] Bera, B., et al., "Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled internet of drones environment," IEEE Transactions on Vehicular Technology, vol. 69, no. 8, pp. 9097-9111, 2020.
[54] Zaidan, A.A., et al., "Security and privacy enhancement techniques for unmanned aerial vehicle systems: A systematic survey," IEEE Access, vol. 10, pp. 12393-12414, 2022.
[55] Mollah, M.S., et al., "Blockchain-based secure drone communication framework for smart agriculture applications," IEEE Access, vol. 8, pp. 139395-139411, 2020.
[56] Zohra, M., et al., "A blockchain-based secure UAV data collection framework for smart cities," IEEE Transactions on Industrial Informatics, vol. 17, no. 3, pp. 2006-2017, 2021.
[57] Zhang, L., et al., "A review of security and privacy issues in UAV networks," IEEE Access, vol. 8, pp. 165030-165048, 2020.
[58] Qadir, A., et al., "Blockchain technology for securing unmanned aerial vehicles in agricultural applications," Future Generation Computer Systems, vol. 106, pp. 136-145, 2020.
[59] Alotaibi, F., et al., "Blockchain-based secure UAV swarm communication for Internet of Things applications," IEEE Transactions on Industrial Informatics, vol. 16, no. 5, pp. 3433-3442, 2020.
[60] Sharma, D., et al., "Blockchain-based secure UAV communications for smart city applications," IEEE Transactions on Vehicular Technology, vol. 69, no. 8, pp. 9151-9161, 2020.
[61] Bhatti, M., et al., "Blockchain for aerial swarm systems: Key challenges and future directions," IEEE Network, vol. 34, no. 5, pp. 114-120, 2020.
[62] Rani, V., et al., "Blockchain technology in UAV systems: A review," IEEE Access, vol. 9, pp. 6321-6344, 2021.

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024

[63] Tan, B., et al., "Security and privacy in UAV-based systems: A survey," IEEE Access, vol. 10, pp. 6091-6108, 2022.
[64] Han, W., et al., "Integrating blockchain with unmanned aerial vehicles: Security, applications, and challenges," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2624-2657, 2020.
[65] Hussain, T., et al., "Securing UAV networks using blockchain technology: A comprehensive survey," IEEE Transactions on Vehicular Technology, vol. 69, no. 3, pp. 2973-2987, 2020.
[66] Xu, J., et al., "Blockchain-based secure communication in UAV networks," IEEE Wireless Communications Letters, vol. 8, no. 5, pp. 1409-1412, 2019.
[67] Dinh, T., et al., "Blockchain-assisted secure UAV communication systems for Internet of Things," IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4752-4760, 2021.
[68] Hassan, M., et al., "Blockchain-enabled UAV communication systems for secure smart cities," IEEE Internet of Things Journal, vol. 8, no. 4, pp. 3221-3233, 2021.
[69] Liu, J., et al., "Blockchain-based UAV cooperative communication and resource management in IoT systems," IEEE Transactions on Industrial Informatics, vol. 18, no. 8, pp. 5515-5525, 2022.
[70] Zhang, Y., et al., "Security and privacy in blockchain-based UAV networks," IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 157-179, 2021.
[71] Ali, H., et al., "Blockchain-based UAV network security solutions: A survey and future directions," IEEE Access, vol. 10, pp. 74891-74907, 2022.
[72] Zhou, Y., et al., "Blockchain-based communication security for unmanned aerial vehicle systems: A survey," IEEE Access, vol. 9, pp. 8983-8996, 2021.

DOI: https://doi.org/10.54216/FPA.180101
Received: September 27, 2024 Revised: November 01, 2024 Accepted: December 07, 2024