IEEE Open Journal of Vehicular Technology

Received 9 June 2023; accepted 11 July 2023. Date of publication 13 July 2023;
date of current version 30 August 2023. The review of this article was coordinated by Editor Lina Bariah.

Digital Object Identifier 10.1109/OJVT.2023.3295208

Blockchain-Assisted UAV Communication Systems: A Comprehensive Survey

SANA HAFEEZ (Student Member, IEEE), AHSAN RAZA KHAN, MOHAMMAD M. AL-QURAAN (Student Member, IEEE), LINA MOHJAZI (Senior Member, IEEE), AHMED ZOHA (Senior Member, IEEE), MUHAMMAD ALI IMRAN (Fellow, IEEE), AND YAO SUN (Senior Member, IEEE)

(Invited Paper)

James Watt School of Engineering, Electrical and Electronics Engineering, University of Glasgow, G12 8QQ Glasgow, U.K.

CORRESPONDING AUTHOR: YAO SUN (e-mail: yao.sun@glasgow.ac.uk)

ABSTRACT Unmanned aerial vehicles (UAVs) have recently established their capacity to provide cost-effective and credible solutions for various real-world scenarios. UAVs provide an immense variety of services due to their autonomy, mobility, adaptability, and communications interoperability. Despite the expansive use of UAVs to support ground communications, data exchanges in those networks are susceptible to security threats because most communication is through radio or Wi-Fi signals, which are easy to hack. While several techniques exist to protect against cyberattacks. Recently emerging technology blockchain could be one of promising ways to enhance data security and user privacy in peer-to-peer UAV networks. Borrowing the superiorities of blockchain, multiple entities can communicate securely, decentralized, and equitably. This article comprehensively overviews privacy and security integration in blockchain-assisted UAV communication. For this goal, we present a set of fundamental analyses and critical requirements that can help build privacy and security models for blockchain and help manage and support decentralized data storage systems. The UAV communication system's security requirements and objectives, including availability, authentication, authorization, confidentiality, integrity, privacy, and non-repudiation, are thoroughly examined to provide a deeper insight. We wrap up with a discussion of open research challenges, the constraints of current UAV standards, and potential future research directions.

INDEX TERMS Blockchain, drone communication, federated learning, privacy, security, UAV networks.

I. INTRODUCTION

The use of unmanned aerial vehicles (UAVs) has gained a great attention due to their high mobility, affordability, and ease of use. UAVs are considered valuable service enablers for innovative city applications, healthcare domains, real-time surveillance and monitoring, disaster management, and wireless communication. Approximately 102.4 billion dollars will be spent annually on UAVs by 2030, a compound annual growth rate of 19.6%, surpassing 19.78 billion dollars in 2020 [1].

Solely devoted UAVs could be deployed as aerial base stations (ABSs), access points (APs), or relays to assist terrestrial wireless communications from the sky, resulting in an innovative approach known as UAV-assisted communications. This approach has several upgrading processes, including potential on-demand deployment, high network reconfiguration flexibility, and a high probability of line of sight (LoS) communication links. UAVs have the potential to meet these requirements concerning user mobility, random channel fluctuations, and blocking effects. UAVs can broaden the coverage area, decrease the blind spots of terrestrial BS, and increase the probability of a direct LoS. The environmental challenges UAVs face cannot be solved using conventional optimization techniques.

A. BACKGROUND

In recent years, UAVs have been utilized for various applications such as surveillance, mapping, remote sensing, search and rescue, disaster control, and entertainment, among others [2]. These technical UAVs often work collectively as UAV swarm intelligence. Designing them requires joint optimization problems of UAVs and blockchain, including flight trajectory, time scheduling, altitude optimization, aerial and relay base stations, energy harvesting, power transfer, optimal power consumption, and resource allocation [3]. Specialized drones and swarm units are also used as temporary base stations in disaster areas and emergencies.

It is anticipated that UAVs will become increasingly prevalent and capture a significant market share by 2025 [4]. However, there are still significant barriers to their widespread use in various applications, such as optimal UAV deployment in 3D space, trajectory optimization, wireless and computational resource allocation, and flight duration when deploying UAVs as base stations (BS) in UAV communications. Additionally, wireless network deployment and expansion require considerable time and capital investments. Moreover, the broadcast nature of UAV-assisted wireless networks makes them highly susceptible to privacy and security breaches, including distributed denial-of-service (DDOS), replay, impersonation, message injection, spoofing, malware infection, eavesdropping links, and line-of-interference attacks. Consequently, UAV-assisted communication presents significant privacy and security challenges that must be addressed [5].

Cryptographic keys and hash-based blockchain techniques can provide security against global positioning system (GPS) spoofing, wormhole attacks, jamming, DOS, and eavesdropping in UAV swarm applications [6]. Multiple consensus algorithms are restricted in their capacity to provide high throughput in a distributed network. In addition to the shortcomings of the current architecture, blockchain's security algorithms impose a high computational delay on the UAV swarm network, rendering it unsuitable for applications requiring high availability and low latency. UAV communication faces several challenges and limitations, including:

1) *Security and Privacy:* UAV communication systems are vulnerable to cyber threats, including unauthorized access, data tampering, and spoofing attacks. Ensuring secure and private communication between UAVs and ground stations is crucial to maintaining the integrity and confidentiality of data.
2) *Trust and Accountability:* UAV communication involves multiple stakeholders, including UAV operators, service providers, and regulatory authorities. Establishing trust and accountability among these entities is essential for reliable and transparent operations. Centralized trust models may introduce single points of failure and raise concerns about data manipulation.
3) *Interoperability and Standardization:* UAV communication systems often involve heterogeneous devices and protocols, leading to interoperability challenges. Lack of standardization hinders seamless communication and coordination among UAVs from different manufacturers or service providers.
4) *Spectrum Management:* UAVs require access to radio frequency spectrum for communication and control purposes. Efficient spectrum allocation and management are crucial to prevent interference, ensure reliable communication, and maximize spectrum utilization.

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

1) *Enhanced Security:* Blockchain inherent immutability and cryptographic properties provide a robust security framework for UAV communication. The decentralized nature of blockchain ensures that transactions and data are tamper-proof, enhancing the integrity and security of UAV communications.
2) *Trust and Decentralization:* By utilizing a distributed ledger, blockchain eliminates the need for a centralized authority in UAV communication. This fosters trust and transparency among stakeholders, as transactions and interactions are recorded and verifiable by all participants.
3) *Smart Contracts and Automation:* Smart contracts on the blockchain enable automated and self-executing agreements between UAVs and other entities. This can streamline operations, ensure compliance with regulations, and facilitate secure and transparent transactions.
4) *Data Integrity and Transparency:* Blockchain can provide a secure and transparent platform for recording and sharing UAV data. This ensures data integrity and traceability, enabling auditable and accountable UAV operations.
5) *Interoperability and Standardization:* Blockchain-based protocols can facilitate interoperability and standardization by providing a common framework for communication and data exchange among UAVs and ground systems. This promotes seamless integration and collaboration across different platforms.

Blockchain technologies are a promising security solution for UAVs with limited capacity. However, further research is required as these technologies are still in their preliminary stages of development. Improvements in consensus algorithms and software-based cryptographic key impairments could lead to more effective security solutions for UAVs in the future.

B. MOTIVATIONS

The wireless channel in UAV networks is prone to security vulnerabilities that can impact reliability. Moreover, the current centralized communication and control system for drones is constantly threatened by external attacks. Therefore, in recent times, researchers have paid more attention to making the UAV-assisted network more secure by using different techniques such as differential privacy and homomorphic encryption [7]. Federated Learning (FL) evolved to ensure privacy by training machine learning (ML) models without data sharing. A global model is trained collaboratively in FL [8]

TABLE 1. Comparisons of Existing Survey Papers. 1: 5G-Concentrated, 2: Blockchain-Concentrated, 3: UAV-Concentrated 4: Performance Comparisons With Other Technologies

Ref.	Year	Goals	1	2	3	4
[13]	2019	Presented PHY-layer Security for UAV Communication Networks	✓	X	✓	X
[14]	2019	Concentrated on UAV Energy Constraints, High Altitude, and 3-D Mobility	✓	X	✓	✓
[12]	2020	Detailed Blockchain-envisioned UAV Communication using 6G Networks	X	✓	✓	X
[15]	2020	Discusses the Blockchain Technology in 5G-enabled Networks	X	✓	✓	✓
[16]	2021	UAV Security and 6G/BC Integration are Explained	✓	✓	✓	X
[18]	2021	Overview of Secure Drone Communication	✓	X	✓	X
[19]	2020	Blockchain-Envisioned UAV Communication Using 6G Networks	✓	✓	✓	X
[17]	2022	Blockchain-based Federated Learning in UAVs Beyond 5G Networks	✓	✓	✓	X
Our Work	2023	Blockchain-Assisted UAV Communication Systems	✓	✓	✓	✓

by sharing the model parameters only. Combining FL with a blockchain-assisted UAV network can revolutionize future intelligent applications, especially in healthcare and wireless networks. Consequently, this survey comprehensively analyzes the impact of combining FL, blockchain, and UAV with beyond 5G (B5G) communication networks for privacy and time-sensitive applications.

Some attacks aim to steal information through security holes [9] in communication links; others use obfuscating sensors, such as GPS spoofing. The standard attacks on UAV networks are flight control manipulation and GPS attacks. Though UAVs have many potential applications, they also raise social concerns and challenges related to public safety, privacy, and cyber security. For instance, cyber-attacks like hacking UAV networks are a potential threat that can be misused by malicious entities, resulting in cybercrime [10]. These vulnerabilities lead to information theft, property destruction, and loss of life. In addition, a UAV network must have safe and reliable correspondence for privacy-sensitive and time-sensitive applications. Therefore, considering the broader perspective of combining UAV and blockchain technology for data-driven applications is paramount.

C. RELATED EXISTING SURVEYS

Recently, some surveys in the literature deal with UAV-assisted communication enabled by blockchain. The comparisons of the existing surveys are presented in Table 1. In the literature, a detailed survey [11] provides comprehensive information on the six-generation (6G) network-based blockchain-envisioned UAV communication. In addition, the architecture, specifications, and use cases of 6G technology are discussed. This study also covers the security and communication facets. Finally, it identifies the potential privacy challenges that blockchain can solve. Similarly, another similar survey [12] introduces PHY-layer security to UAV communication networks to address the difficult problem of information leakage caused by potential eavesdropping. A UAV network of this kind aims to achieve information exchange confidentiality. The article [13] first emphasises UAV energy constraints, high altitude, and 3-D mobility, and then the authors present a literature review on 5G communication. The next work [14] specifics on UAV networks and BC technology, including their security problems, limitations, and solutions. Moving on to general blockchain surveys, a very thorough survey [15] covers the integration of 5G and 6G with blockchain in UAV communications. Maintaining the present trend, this article [16] provides a comprehensive overview of recent developments in blockchain-based FL. According to studies, blockchain is widely used to solve the challenges of drone networks. The UAV layer connects drones for specific tasks, such as blockchain mining. On the other hand, the resource layer is about setting up the blockchain and allocating resources. A service provider at the network's edge sets up the management layer to manage resources and make decisions, like sending work to drones to do computation.

While research on blockchain-assisted UAV communication systems is an emerging field, there are still several gaps and limitations that need to be addressed. Some of the key gaps and limitations in existing research include:

- *Scalability:* Blockchain scalability remains a significant challenge, especially in the context of real-time UAV communication systems. As the number of UAVs and transactions increases, the scalability of blockchain networks becomes crucial to ensure timely and efficient communication. More research is needed to develop scalable blockchain solutions specifically tailored for UAV communication systems.

- *Performance and Latency:* Blockchain transactions typically require multiple confirmations, leading to latency issues in UAV communication. Reducing transaction confirmation times and minimizing latency is crucial, especially in time-critical applications. Exploring novel consensus algorithms and optimization techniques to improve the performance of blockchain-assisted UAV communication systems is an area that requires further investigation.
- *Energy Efficiency:* UAVs are often resource constrained in terms of battery life and computing power. Integrating blockchain technology into UAV communication systems can introduce additional energy overhead due to computational requirements and network communication. Developing energy efficient protocols and mechanisms to minimize the energy consumption of blockchain operations in UAV communication is an important research area.
- *Real-World Deployments and Testing:* While there are theoretical studies and simulations exploring blockchain-assisted UAV communication, real-world deployments and comprehensive testing in operational environments are limited. More empirical studies and field trials are necessary to validate the feasibility, performance, and effectiveness of blockchain solutions in practical UAV communication scenarios.
- *Regulatory and Legal Considerations:* Blockchain technology introduces regulatory and legal challenges in UAV communication systems, such as data privacy, compliance, and liability issues. Understanding and addressing these regulatory and legal considerations are essential for the widespread adoption of blockchain-assisted UAV communication systems.
- *Cost and Infrastructure Requirements:* Implementing blockchain technology in UAV communication systems may require significant infrastructure and resource investments. The cost implications and feasibility of deploying blockchain solutions in UAV communication need to be carefully evaluated, especially for small-scale UAV operations and resource-constrained environments. Addressing these gaps and limitations will be crucial for advancing the field of blockchain-assisted UAV communication systems and realizing their full potential in enabling secure, trusted, and efficient UAV operations in various applications.

Whereas our study presents a comprehensive review covers several aspects, including some potential factors.

- *Technical Aspects:* This includes details of the blockchain architecture, the consensus mechanisms used, cryptographic techniques employed, and smart contract design.
- *Security Aspects:* This covers the security benefits of using blockchain technology in UAV communication systems, such as improved data encryption, authentication, access control, and record-keeping. It also discusses potential security risks and challenges.
- *Applications and Use Cases:* The potential applications and use cases, such as surveillance, monitoring, search and rescue, and precision agriculture.
- *Performance Evaluation:* This aspect covers the performance evaluation of blockchain-assisted UAV communication systems, including their scalability, latency, energy consumption, and fault tolerance.
- *Regulatory and Legal Aspects:* This aspect covers data privacy, intellectual property, liability, and safety regulations.
- *Economic Aspects:* This aspect covers the implementing and maintaining the system, the potential cost savings and revenue opportunities, and the impact on the UAV industry.

D. CONTRIBUTIONS AND ORGANIZATION

Few recent research focuses on improving the privacy and security of UAV communication networks using blockchain technology. However, there needs to be more research on combining technologies such as blockchain, UAVs, FL, and B5G communication. This gap motivates us to investigate the potential benefits of these technologies when combined. The key contributions of this article are highlighted as follows:

1) This article provides a comprehensive exploration of the integration of multiple technologies such as UAVs, blockchain, next-generation wireless communication, and FL for future intelligent applications.
2) We also cover the necessary enabling technologies for a reliable UAV network, such as B5G communication for massive connectivity, ultra-reliable low latency (uRLLC), and higher data rates. In addition, blockchain is used for security and privacy, while FL is used for distributed learning and collaborative intelligence.
3) We throughly discuss privacy and security of data in UAV communication as blockchain technology has the potential to enhance the privacy and security of drone communication by providing a decentralized and tamper-proof system for data storage and transmission.
4) Furthermore, this study covers various aspects and provides a holistic view of the technology, its benefits, and potential challenges of more secure and privacy-aware systems capable of integrating distributed learning.

The rest of the article is organized as follows; Section II presents an overview of preliminary topics such as blockchain technologies, data security and privacy concerns in communication systems, and UAV communication systems. Section III explores the role of blockchain in UAV networks, while Section IV analyzes data privacy and security concerns in blockchain-enabled UAV security solutions. Section V discusses the challenges and open research directions. Finally, Section VI provides concluding remarks.

II. BLOCKCHAIN-ENABLED UAV NETWORKS: PRELIMINARIES AND OVERVIEW

This section presents a summary of the blockchain-enabled UAV network and preliminary information. It briefly

discusses the evolution of UAV technology, related applications, a conceptual communication framework, and the challenges that come with it. Furthermore, a primer on the fundamentals of blockchain technology explains.

A. UAV COMMUNICATION SYSTEMS

The UAVs or drones are operated remotely by ground control systems (GCS), also known as ground cockpits, either by human pilots or autonomous systems such as autopilot, which require no human intervention. Initially, UAVs were designed for military and surveillance applications, however, rapid research and development significantly reduced the cost of UAV manufacturing. As a result, UAV technology is being adopted in many commercial and non-military applications like intelligent city surveillance, delivery services, agriculture, search and rescue, weather monitoring, filmmaking [18], photography and innovative healthcare [19]. The communication system is vital to UAV applications because it connects the flying node, the GCS, the stationary nodes, and the infrastructure. Therefore, the entire system has the communication capacity of drone-to-ground communication (D2G), drone-to-drone communication (D2D), drone-to-satellite communication (D2S) and drone-to-cellular communication (D2C).

- *D2G:* In D2G communication, the ground station controller monitors the UAV's flight path. Then, on-duty technicians or field staff start the flight control, upload the path to the flight control, and set up parameters for automatic takeoff and landing, such as closing speed, lift angle, climb height, and end altitude. D2G communication ensures the smooth operation of the task assigned to UAVs. Moreover, the job of the GCS is to collect data captured by the UAVs and send the control command based on adherence. Therefore, a secure connection between the UAV and the GCS is required.
- *D2D:* In most existing applications, multi-UAV systems and ad hoc networks are used, where two or more UAVs participate in completing the task. The fundamental design challenge for the multi-UAV system [20] is communication and coordination among multiple devices. UAVs serve as mobile ad hoc networks (MANETs) for communication while in flight. As a result, in a MANET environment, each UAV is considered a mobile node. An open system interconnection (OSI) framework is commonly used, including the OSI model's data link, network, transport, and application stages, which include the physical layer security [21], data link, network transport, and application stages. The communication of each UAV with the ground station limits the system's capabilities when there are multiple UAVs.
- *D2S:* UAV satellite communication is predominantly used beyond LoS communications. Due to the earth's rotation, standard LoS datalinks are rendered unusable over long distances. Moreover, drones may fly beyond the range of terrestrial networks, including 5G and other cellular services. A satellite can instead relay and amplify radio or microwave frequency signals between a vehicle and its BS. In regions without wireless communication infrastructure, the military-based application uses D2S. GPS devices ensure real-time location tracking for drones and facilitate drone communication via satellite links. However, this setup can also be useful in exceptional emergencies like earthquakes and floods.
- *D2C:* Communication between aircraft, or air-to-air (A2A) communications, occurs during missions involving multiple UAVs. In these cases, UAVs work together and coordinate using low-power wireless technologies (like bluetooth and zigbee) to send and receive data directly or via a series of intermediate nodes. Here, a single UAV operates within a network of UAVs, where they all share information and complete the flight mission. But the throughput and transmission bandwidth of D2D communications is extremely low.

B. DATA SECURITY AND PRIVACY SPECIFICATIONS IN UAV NETWORK

Internet-connected UAVs are prone to cyber-attacks, posing profound uncertainty to the security and privacy of their users. Such attacks fall into five broad categories: confidentiality, integrity, availability, authenticity, and privacy attack. Fig. 2 presents the percentage of attacks compiled in recent surveys [22]. The following section describes the specifications of each intrusion. The risk of passive and active attacks is heightened by the lack of security measures for UAVs operating in the national airspace. In this article, we categorize the potential vulnerabilities of UAVs into four groups: sensor level attacks, hardware level attacks, software level attacks, and communication level attacks. In Fig. 3, we provide a detailed breakdown of the threats and vulnerabilities that UAVs face based on their functional level. We then review the various attacks and their corresponding countermeasures currently available in the literature.

1) *Communication-level Attacks:* UAV flight control and data transmission require effective communication protocols. Typically, UAVs communicate with the GCS wirelessly. This section examines the vulnerabilities, threats and attacks that can compromise the confidentiality, integrity, authenticity, and accessibility of UAV communication. Communication-level vulnerabilities and threats can be categorized based on the following communication layers.
    a) *Physical & MAC Layer Vulnerabilities and Attacks:* The security of UAV communication networks is compromised due to vulnerabilities at different layers of the communication protocol. In this regard, physical MAC layer vulnerabilities and attacks have been identified in the complex D2G wireless communication network. A recent study [23] reports three zero-day attacks on commercial Wi-Fi-based UAVs, including the Parrot Bebop UAV.
    b) *Network Layer Vulnerabilities and Attacks:* Additionally, the ad hoc mode of UAV networks

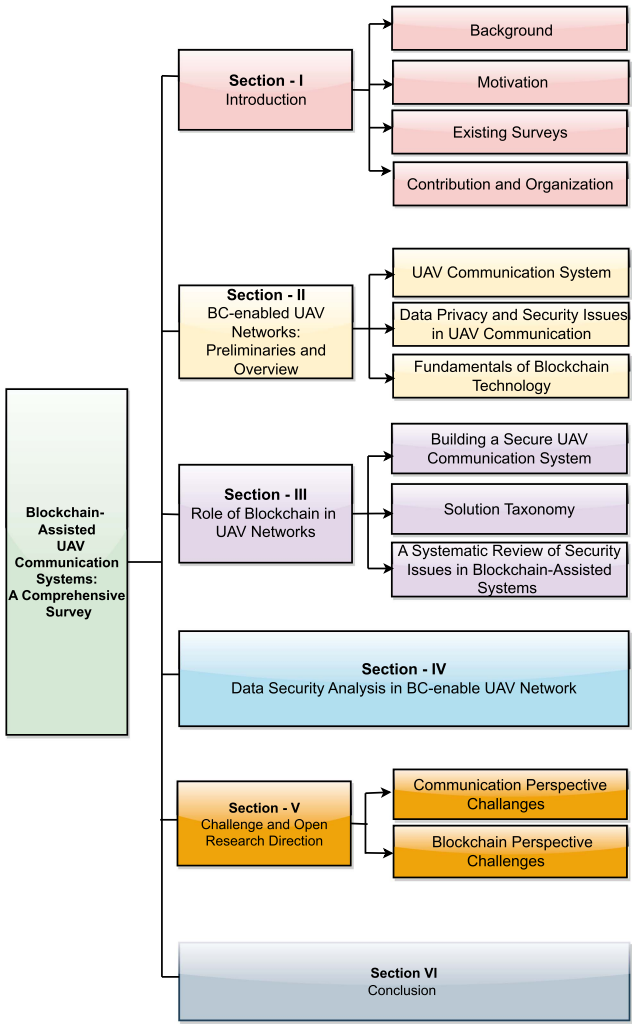

FIGURE 1. Illustrative overview of structure survey and reading map.

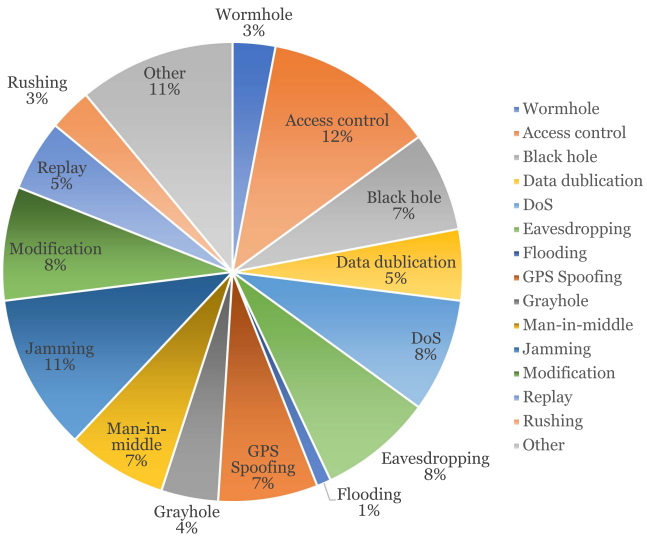

FIGURE 2. Percentage of different attacks on UAV network [22].

known as the flying ad hoc network (FANET) poses serious threats due to its dynamic topology. A previous study [24] highlights the security risks of a UAV public safety network. UAV routing protocols are particularly vulnerable due to the limited resources and lack of wireless encryption in these networks, as discusses in [25].

- *Eavesdropping Attacks:* Sniffing or snooping attacks are like eavesdropping on communication's confidentiality, integrity, authenticity, and availability to access information, which is information theft. The UAV sends or receives data to the user; attacks are undetectable. Typically, this is due to the nature of the operation, i.e., standard network transmission.
- *DoS Attacks:* In the DoS, the communication protocol layers and services during this threat result in a degradation in system performance. This attack will originate from a sole source and deal in several ways. Some commonly used techniques to deal with DoS attacks include network firewalls and intrusion detection systems.
- *Man-in-the-Middle Attacks:* Man-in-the-middle (MITM) attacks involve interfering with user-to-UAV communication. It is also the most effective scenario for an active eavesdropper attack, in which the person conducting the availability communicates directly with the person being eavesdropped upon. Then it starts sending messages back and forth between the two. As a result, the user and the UAV believe they are communicating with one another, but the attacker has complete control over the interaction.
- *Replay Attacks:* Eavesdropping is a potential attack in UAV networks, where the adversary intercepts multiple requests and replays legitimate data to the UAVs. This can result in the UAVs receiving repeated data, and without the implementation of replay protection, they may be unable to distinguish between genuine and malicious requests.
- *Forgery Attacks:* By sending a spoof request to unauthenticated UAVs, an adversary can compromise their ability to communicate securely. An adversary disrupts D2G communication by creating a malicious request that looks legitimate.
- *FANETs Routing Attacks:* MANETs routing protocols are vulnerable to passive and active attacks, such as injecting malicious nodes, controlling network traffic, or interrupting routing features. Most of these

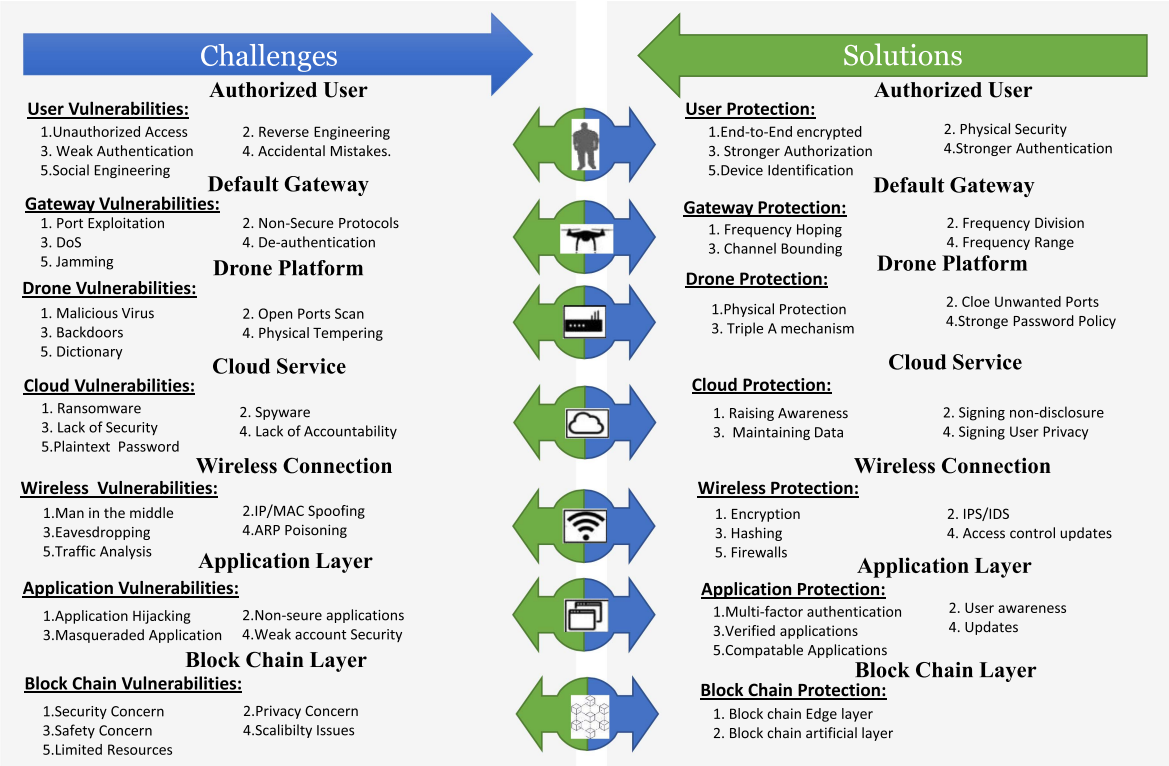

FIGURE 3. Exploitable security gaps and solutions.

attacks can also target routing protocols on FANETs. We categorize these attacks based on their routing functionality into three categories. The first category is path discovery attacks, which aim to control traffic and include blackhole [26], sleep deprivation [27], sybil attacks [28], and wormhole [29] attacks. The second category is route maintenance attacks, which attempt to corrupt routing control packets and include flooding and byzantine [30] attacks. The third category is data forwarding attacks that affect payload traffic, such as real-time video traffic [31].

- *Jamming Attacks:* The UAV network is built with epidemic routing, one of the best delay-tolerant routing protocols. As a result, it is impossible to predict when or where an attack will occur, how long it will last, who it will target, or what tactics will be used. When a UAV goes into autopilot flight mode, communication is lost with the control station, and the drone is vulnerable to a GPS spoofing attack. This type of connection break happens when an attack, jamming, is sent from an enemy's ground station. Even if the drone is still in range of the control unit, a jamming attack will cause it to enter autopilot mode. Attackers use jamming techniques to gain access to the UAV and then spoof GPS signals to ensure it lands in a designated area if the UAV loses contact with the control station, as it would in the more common and unpredictable circumstances, it will be unable to activate the safety return-to-home (RTH) feature.

c) *Transport Layer Vulnerabilities and Attacks:* Communication protocols used by UAVs are vulnerable to attacks if they lack proper security measures to ensure privacy, integrity, availability, and authenticity. The MAVLink protocol is one of the widely used communication protocols for UAVs, and recent studies suggest that it is susceptible to attacks such as internet control message protocol (ICMP) flooding and packet injection. Therefore, it is critical to implement secure transport layer protocols to protect UAV communication from potential attacks.

The authors of [32] classify MAVLink attacks into four types based on how data is compromised includes interception, modification, interruption, and fabrication attacks. Since the MAVLink protocol lacks authentication and encryption, attackers can intercept communication traffic and collect data exchanged between the GCS and UAVs.

On the other hand, uranus link only provides integrity protection through the checksum field in the messages, according to the design and

implementation of uranus link for real-world applications [33]. However, an attacker capable of intercepting exchanged packets can exploit this vulnerability and reveal mission-critical information [34].

2) *Sensor-level Attacks:* GPS data jamming, false sensor data injection, and sensory-channel attacks are examples of sensor-based attacks.
   - *GPS Data Jamming:* During a UAV's mission, the GPS receiver receives coordinates from satellites and sends them to the GCS. However, an adversary can disrupt the GPS signals, causing a GPS data jamming attack that can disorient the UAV [35]. Such attacks can lead to loss of control over the UAV and potential hijacking of the drone.
   - *False Sensor Data Injection:* The injection of false sensor data into a UAV's flight controller can have severe consequences on external sensors such as electro-optical and infrared sensors (EO/IR), leading to instability of the UAV [36]. Such attacks can be initiated by injecting false sensor data into the flight controller system or by sending false signals to the sensors. GPS spoofing is a common technique used for injections or data. As GPS signal broadcasts are typically unencrypted and unauthenticated, attackers can alter the GPS receiver of the UAV and gain control over it [37]. In this study, authors in [38] demonstrates the effect of GPS spoofing on UAVs, which causes the drone to respond to false signals and leads to the malfunction of its navigation system.
   - *Sensory-channel Attacks:* UAVs use a variety of sensors, and their sensory channels (e.g., infrared, acoustic, and light) serve as attack vectors.
3) *Software-level Attacks:* Malicious software and zero-day vulnerabilities contain software-level vulnerabilities and threats on UAVs.
   - *Zero-day Vulnerabilities:* Zero-day vulnerabilities and malicious software pose serious threats to the security and privacy of UAVs. The flight stack or GCS software of UAVs may contain unknown defects, such as buffer overflow or DoS, which can be exploited by adversaries until patches are released by manufacturers. Promptly updating UAV systems for each patch released is therefore essential for operators to mitigate such vulnerabilities.
   - *Malicious Software:* Malicious software, such as UAV malware, can infiltrate the GCS and flight controller, leading to sensitive data loss and loss of control over the UAV system. Attackers who gain access to the UAV's flight stack can shut down the system, causing DoS and disrupting the flight mission. Moreover, malware such as Maldrone, SkyJack, and Snoopy can compromise the security and privacy of UAVs.

     Maldrone infects the flight controller, enabling the attacker to control the UAV and act as a proxy for the drone's flight controller and sensor communications, allowing the compromised drone to land anywhere. SkyJack is a hijacking malware that can be installed on an infected drone, taking over other legitimate drones [39]. Through a Wi-Fi de-authentication attack, compromising the entire system. On the other hand, Snoopy can be installed on a drone to steal personal information from public users. It tricks users into connecting to a fake Wi-Fi network, allowing it to follow its users and collect their personal information. Therefore, UAV operators must be aware of the risks posed by malicious software and take necessary precautions to secure their systems [40].
4) *Hardware-level Attacks:* Hardware-based attacks on UAVs include hijacking, supply chain attacks, battery attacks, and RF module attacks. These attacks target the physical components of the UAV, such as its hardware and electronics, to compromise its security and disrupt its operation.

   In addition to hardware-based attacks, UAVs are also vulnerable to attacks that involve hardware reverse engineering. By analyzing the internal structure and characteristics of the UAV's hard chip, an attacker can gain valuable information about the system and potentially exploit its vulnerabilities. It is essential to implement robust security measures to protect against hardware-based attacks and hardware reverse engineering to ensure the safety and security of UAV operations [41].

C. FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGY

Blockchain is a decentralized, distributed ledger that facilitates secure and transparent tracking of transaction records within a network. Transactions can involve physical assets such as cars and houses or intangible assets such as intellectual property, patents, and copyrights. The core components of blockchain technology include distributed ledgers, immutable records, and smart contracts. Additionally, blockchain's innovation ensures data security and confidentiality, enabling trust without the involvement of third parties. Furthermore, the blockchain system is resistant to monopolies, allowing any node to withstand a monopoly threat and participate in the decision-making process, thus promoting the democratization of blockchain. The key components of blockchain technology are straightforward, despite its distributed nature. Six distinct zones make up the fundamentals of blockchain technology: The transmission control protocol/internet protocol (TCP/IP) network [42], peer-to-peer protocols [43], cryptography algorithms [44], execution, and transactions [45] and smart contract. Additionally, the simplest architecture of blockchain technology consists of digital signatures and hash functions, as well as Dapps and smart contracts. Cryptographic hashing and digital signature systems are employed by blockchain technology for data security. Although blockchains do not always use cryptographic hashing or digital signatures, the distributed ledger system of the technology enhances security

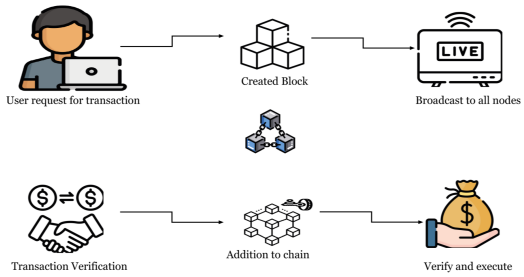

FIGURE 4. Simplified operation of blockchain technology.

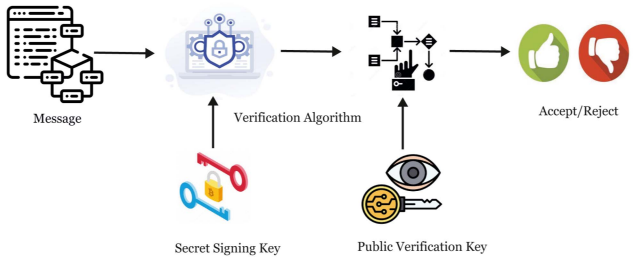

FIGURE 5. Asymmetric key cryptography secure blockchain transactions.

through blockchain hashing, digital signatures, and digital ledgers.

- *Hash Functions:* Each result in the cryptographic hashing process is associated with a unique digital fingerprint. The length of a string can serve as an input for the cryptographic hash function, while the result is always of a fixed length. Moreover, the hash possesses properties that render it collision-free, concealed, and capable of easily solving puzzles.
  The National Security Agency (NSA) developed secure hash algorithms (SHA), namely SHA-256 and SHA-512, as well as message digests such as MD2, MD3, and MD6. As a result, they are unable to obtain the input that was initially introduced or perform the inverse function [46].
- *A Digitized Ledger:* A digitized ledger system was introduced by Satoshi Nakamoto in 2008 [47]. This system facilitates the replication of transactions between computers, linked together to prevent record tampering. An immutable record-keeping system eliminates the need for third parties. Chaining together the hashes of previous blocks create a chain of blocks.
  A single block stores nonces, previous block hashes, merkle roots of timestamps, block numbers, and hashes. Private blockchains fall into two categories: public [48] and consortium blockchains. Fig. 4 illustrates a simplified model of how a blockchain system operates. Integrating drones and blockchain technologies is a practical possibility, with both technologies being investigated and refined simultaneously across many industrial applications. Blockchain technology for drones has the potential to increase operational effectiveness and circumvent many of the current potential barriers to drone attacks, as outlined in this article.
- *Digital Signatures:* Similar to hash functions, digital signatures are an underlying cryptographic building block. As with a digital signature, the key difference is that, unlike a traditional signature, this one cannot be copied and pasted from one manuscript to another. It must instead be signed only once and interpreted by any third party.
- *Decentralization:* The decentralized nature of blockchain is a distinct advantage that is leveraged in all blockchain-related applications. In [49], the authors propose a blockchain-based key management scheme for heterogeneous FANET, in which all drones collectively maintain the public key information through blockchain in a decentralized and distributed way, without any participation from a third party, thus avoiding a single point of failure. If each drone stores the details of the other's flight paths in the blockchain, the effects of jamming attacks can be reduced, as collisions can be avoided.
- *Asymmetric-Key Cryptography:* The Elliptic Curve Digital Signature Algorithm (ECDSA) [50] garners and affirms digital signatures to use public-private vital tuples. Specific domain parameters specified for a particular period are subject to validation. The measures of the advertised blockchain transactions are shown in Fig. 5.
- *Consensus Mechanisms:* The next block acknowledgement is one of the most important parts of blockchain technology. This problem can be tackled by incorporating a consensus model. Different blockchain consensus mechanism and their working is present in Fig. 6. A blockchain network's basic structure must acknowledge that a blockchain network should start with a public genesis block, making it the only pre-configured block. This is required for participation, and the primary objective of the consensus mechanism is to produce an acceptable outcome. For instance, preventing double spending, aligning economic incentives, and objecting to fair, equitable, and fault tolerance [51].
  Consensus algorithms are used in blockchain networks to reach an agreement among various distributed nodes. Blockchain is vital since its distributed ledger keeps track of all module activities and makes the relevant information accessible to anyone using AI for in-depth analysis. Second, there is the potential for adversarial exploitation of smart contract codes that use AI to identify potential contract limitations. Such risks can be reduced by utilizing AI to increase the adaptability and intelligence of the smart contract. Third, more smart contracts and consumption optimization can reduce transaction authentication times by half, making them more sustainable and accessible to more participants. Other benefits include superior energy efficiency, increased reliability, and quicker decision-making.

III. ROLE OF BLOCKCHAIN IN UAV NETWORKS

The use of blockchain technology in UAV networks can have significant meaning the data security and privacy by providing

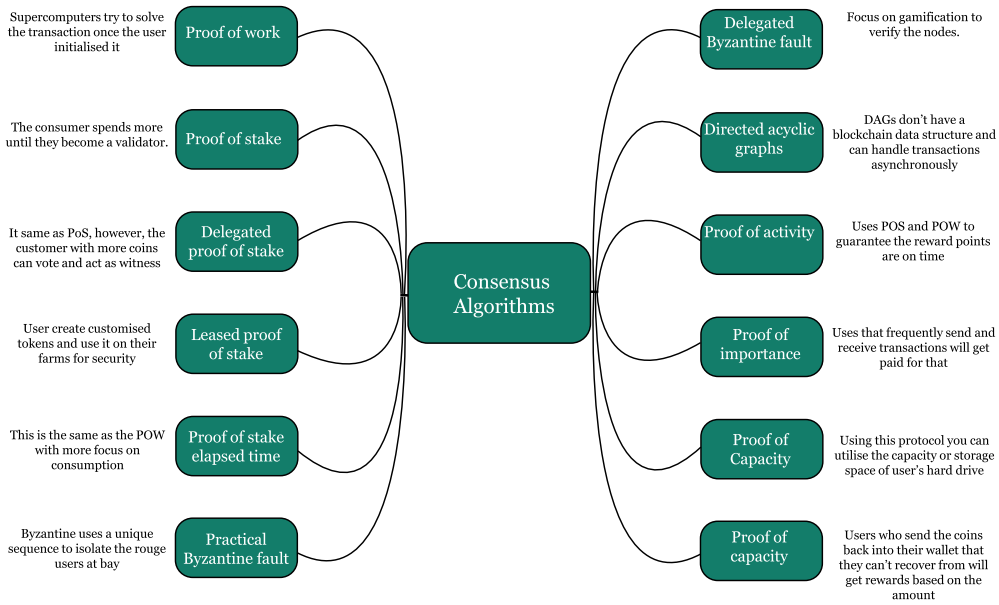

FIGURE 6. **Different blockchain consensus mechanisms.**

immutability, decentralization, encryption, smart contracts, and audibility. To assure data integrity, immutability, and transparency, distributed ledge simultaneously, the technology works together seamlessly to store decentralized data. However, a central server is sometimes required to keep a blockchain framework running smoothly. The decentralization of private and federated blockchains is only partial. In comparison to other centralized platforms, the blockchain provides greater security. It also needs cryptography to protect sensitive data in the ledger system. Cryptography is a complex process for encrypting data as a barrier against malicious cyber-attacks [52]. Safety is one of the most appealing uses of blockchain for UAVs. Unfortunately, highly centralized blockchains are inconvenient, even though UAVs can gather data from numerous sources. Which uses recognize fraudulent recommendations. Technology can identify fraudulent offers, and automated systems reject the request for an effective method of thwarting cyber-attack audibility centralized Domain Name System (DNS). Furthermore, there needs to be a key-entry point because of various centralization. Additionally, blockchain works best for organizations to stop DDoS attacks concealed in fake hardware. No viruses can enter the network thanks to hardware provenance on blockchain-based devices. A comprehensive review of blockchain-assisted UAV communication systems can cover several aspects listed below.

- *Confidentiality:* It entails preventing unauthorized users from accessing data. Like other network systems, UAV networks are vulnerable to confidentiality attacks such as data theft, sniffing, eavesdropping, and replay attacks. Several scenarios have been put forth in which a low-cost, tamper-proof blockchain-based system would protect the privacy of UAV networks [53]. Federal Aviation Administration (FAA) regulations use an ID management system [54] on drones to authenticate and authorize users. Furthermore, they take advantage of delta drone international limited (DLT) ability to keep the information about the drones' flight paths secret. The authors explained that blockchain employs asymmetric encryption and homomorphic obfuscation to raise the secrecy of the network. On the other hand, [55] utilize blockchain to preserve the confidentiality of the cached content by revealing only the essential vehicle substance for specific vehicles. A distributed crowd-monitoring system supported by drone swarms, this task aims to ensure that the supervision data is kept up-to-date, secure, and confidential [56].
- *Integrity:* The study in [57] proves the data's integrity while lowering the overall volume of direct requests made to multi-access edge computing (MEC) servers. A blockchain, in contrast, enhanced their performance and the accuracy of the data shared between drones in an internet of drones (IoD) environment. Their technology chooses the miner to swarm UAVs to protect plants smartly. They use the DLT to keep data safe; in addition, ensuring the availability of services for UAVs in the airspace is a significant concern. A blockchain is decentralized; an excellent blockchain network should resist malicious entity attacks.
- *Non-repudiation:* Non-repudiation is another critical criterion for UAV network cybersecurity. This phrase refers to the incapacity to deny or avoid responsibility for one's conduct using critical public infrastructure, such as when a UAV signs messages before sending them over the internet. As a condition for UAV networks, non-repudiation meets the requirement. Therefore, it suggests that a UAV may refuse to provide photographs of illegal content. In conclusion, A UAV system protects the

required IoD infrastructure, and the study of [54] argues for four blockchain-based concepts to improve drone security. These facets digital fingerprint, data structure, consensus process and access control, underpin consensus methods and aid in preventing security breaches by empowering network nodes to determine an invoice.

- *Availability:* All the blockchain-based solutions proposed for unmanned aircraft system traffic management (UTM) [58] architectures are fundamentally similar regarding a single point of failure. However, they are decentralized, requiring little or no centralization authority. For example, the authors [59] present a zone-based, decentralized system for registering and validating drones. They designate a reliable ground-based source in their architecture. The authentic is a drone control agent within a predetermined boundary. They maintain availability by allowing neighbours to participate in the authentication scheme. Drone controllers will stand in for failed ones at the UTM. In this context, the authors in [60] deny blockchain architecture's existence. According to them, their architecture eliminates latency between nodes by securing communication. In decentralized systems, it presents an advantage for sensitive applications. Additionally, smart contracts with transparency and immutability support the model. Thus, the task is accomplished using a decentralized method resistant to attacks on Ethereum and the interplanetary file system (IPFS).
- *Authenticity:* Finally, UAV networks must ensure the legitimacy of users and messages. Authentication is the capacity to detect real user identity authentication issues in UAV network attacks, such as cloaking. The UAV network also includes cryptographic data for authentication and privacy, as discusses in [61]. However, placement improves total spectral network efficiency a straightforward blockchain paradigm that is secure allows for anonymity and work accreditation [62]. They reject an adversary's request for a surveillance UAV, an attack model that permits altering a blockchain before verifying it. Users reject both the handoff problem and the malleability attack. Applying a unique blockchain architecture adds a delay every time a UAV moves between GCS.

A. BUILDING A SECURE UAV COMMUNICATION SYSTEM

A secure blockchain-assisted UAV communication system and it's technical considerations and best practices involve several technical aspects few of them listed below.

- *Blockchain Architecture Design:* The first step in building a blockchain-assisted UAV communication system is to design the blockchain architecture. This involves selecting the appropriate blockchain platform, such as Ethereum or Hyperledger, and determining the consensus mechanism, block size and transaction rate that best suits the system's requirements.
- *Smart Contract Development:* Smart contracts are self-executing programs that run on a blockchain network. They are used to automate certain functions in a blockchain-assisted UAV communication system, such as data authentication and access control. Developing smart contracts involves coding the contract logic in a programming language such as Solidity and testing the contracts using a development environment like Remix.
- *Network Infrastructure Setup:* Setting up the network infrastructure for a blockchain-assisted UAV communication system involves configuring the nodes that make up the blockchain network, including full and light nodes. It also involves setting up communication channels between the UAVs and the blockchain network, such as Wi-Fi, Bluetooth, or cellular networks.
- *Cryptography Implementation:* Cryptography plays a critical role in securing the data transmitted between the UAVs and the blockchain network. Implementing cryptography involves selecting appropriate cryptographic algorithms and protocols, such as Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA), which configure them in the system's software. Authors in [63] present a BETA-UAV blockchain-based efficient authentication for secure UAV communication that promises how BETA-UAV resists attacks. The objective is to enable mutual authentication and freshness identification so that the UAV networks can establish secure communication channels. Proof-of-freshness or authentication protocols allow UAVs to integrate with these systems with minimal hassle and maximum security.
- *User Interface Design:* The user interface is the front end of the blockchain-assisted UAV communication system that allows users to interact with the system. User interface design involves designing the screens, menus, and buttons that users will interact with, as well as designing the user experience to be intuitive and easy to use.
- *System Testing and Evaluation:* Once the system has been built, it needs to be thoroughly tested and evaluated to ensure that it works as intended. This involves conducting functional testing, performance testing, and security testing to identify any bugs, performance issues, or security vulnerabilities that need to be addressed.

Table 2 compares consensus algorithms and how blockchain interacts with other languages. Cyberattacks are less likely to occur on the UAV network after integrating blockchain. This also results in a fork resolved by creating the longest chain. Table 3 describes cybersecurity-related problems in UAV networks. To prevent further forking, the longest chain can be built; for example, [64] utilize blockchain technology to protect data with cryptography. Data is therefore verified and encrypted to stop unauthorized modification.

B. SOLUTION TAXONOMY: CHALLENGES AND CONSTRAINTS IN UAV NETWORKS

Due to the unique characteristics of the UAV network, such as fluid topology, node mobility, and finicky links, it faces

TABLE 2. Comparison Among Consensus Algorithms

Consensus Algorithms	Blockchain Platform	Markup language	Pro and Cons	Years
Proof-of-weight	File coin	Stark, Snarky	Improved security and safer / centralization energy-intensive.	2017
PoB	Slim coin	C++, Python, shell	Preservation of the network / need special equipment, not suitable for public data	2014
PoC	Burst coin	Java	Cheap, Efficient, Distributed / Favoring bigger fishes and the decentralization issue	2014
PoI	NEM	C++, XEM, Java	Democratic and Network resilience	2015
PoA	Decred	Go	Fairness, investment, verification / not suitable for public data networks.	2016
DAG	IOTA	Rust, Java Go,	Infinite transactions per second / Special equipment needed	2015
DBFT	NEO	Python, NET,c++, Go, REST	No energy expenditure is needed, no forks on the NEO blockchain. / Delegates need to operate	2016
SBFT	Chain	Java, Node, Ruby	Energy-efficiency, Transaction finality, Low reward variance / Sybil attacks, Scaling	2014
PBFT	Hyperledger Fabric	Java script REST and GO	Transaction finality, Low reward variance / Exponentially increasing message count	2015
PoET	Sawtooth	Java Javascript, REST and GO, C++	More efficient and cheap / Low participation	2018
LPoS	Waves	Scala	Fair usage lease coins and Not suitable for public network/ Decentralization Issue	2016
DPoS	Lisk	Java script	More scalable, energy-efficient and Decentralization, low participation	2016
PoS	NXT	Java	Efficient Lower barrier to entry, Accessibility Limitations The 50 Percent Attack	2013
PoW	Bitcoin	C++	Capable of supporting a network worth hundreds of billions of dollars	2009

unique communication challenges compared to other wireless networks. Therefore, we categorize them in three directions:

- *Security Constrain:* Some drones lack encryption on their onboard chips due to price or energy consumption considerations, leaving them vulnerable to attackers. This poses a threat to privacy, as attackers can easily access communication contents. Additionally, according to [9], drones without encryption can be easily hijacked, which is dangerous as it can lead to loss of control and heavy damage. Encryption, authentication is also crucial for UAV network communications. Without authentication, security threats such as tampering, replay attacks, spoofing, and impersonation can occur. For example, in the logistics industry, an attacker can impersonate a valid drone in the network and tamper with address information, resulting in cargo being sent to the wrong destination and causing property damage to the company and customers. Availability is also a significant concern, with DoS attacks being a common method that damages availability. During a DoS attack, the whole network could fail if the attacker goes after the GCS, which would be even worse.
- *Power Constraint:* The energy sources for drones in UAV networks are more expensive than those of vehicles in VANETs or mobile phones in MANETs. Moreover, drones' battery lives may need to be increased even for routine tasks, much less bolstering the safety of human-to-human communications. Consequently, schemes designed for UAV networks must be compact and have low power consumption.
- *Scalability Constrain:* Drones in a UAV network constitute a dynamic 3D topology in which the number of nodes, their positions, and their speeds constantly change. Consequently, links may form and disappear sporadically, and the network may frequently partition, resulting in unstable communications. Airborne jamming attacks exacerbate the situation. These communication stability issues may lead to drone collisions and task failure in self-organized UAV networks, which rely on cooperation to maintain performance.

C. A SYSTEMATIC REVIEW OF SECURITY ISSUES IN BLOCKCHAIN-ASSISTED SYSTEMS

A review of security issues in UAV-assisted systems is present in [20], where the authors employ blockchain technology to mitigate security threats. In a similar survey, the authors investigate blockchain applications in UAV communication, such as network security and decentralization [65]. Furthermore, the authors in [47] propose a comprehensive survey of blockchain-based communication systems for UAV networks. They introduce an IPFS for data storage to ensure user privacy and decrease transaction storage costs. The study in [66] also presents a systematic review of blockchain applications in UAV-assisted networks. The study summarizes how blockchain is used to ensure the security of UAV networks and divides UAV applications into several innovative categories. Blockchain technology offers a promising solution to data privacy concerns in UAV applications. As a distributed ledger, the blockchain securely records and tracks data without any centralized authority [67].

Blockchain technology ensures more reliability than other centralized systems. In particular, decentralization encrypts data to encode the information in the ledgers. Cryptography is a complex process for encrypting data as a barrier against malicious cyber-attacks [68]. In addition, this technology can identify fraudulent recommendations via an automated

TABLE 3. Cybersecurity-Related Requirement in UAV Networks

Authors	Application	Goals	Pros	Cons
[87]	Confidentiality	ID management system according to FAA requirements	Verify and authenticate drone operations using blockchain	Drones are vulnerable to 51% of attacks since they can flexibly join and leave, requiring storage and computational resources
[56]		Safeguard the confidentiality of conceivable cash content	No increase in a cache hit rate, and robustness	Considerable transmission overhead is also not possible
[57]		Crowd surveillance technology that is safe and respectful of privacy	PKI-based security protocol to authenticate UAVs, assign monitoring tasks, and allow secure data transmission	Significant time and computational costs
[88]		Maintain the anonymity of the UAV networks	Used PKI and OTP to secure the confidentiality of network communication channels	Considerable burden in terms of time and computational cost
[89]		Maintain the UAV's confidentiality	Comparatively, encryption, decryption, and essentials have low computational costs	Algorithms for computationally intensive cryptography
[90]	Integrity	Data integrity is checked before transfer to MEC servers	MEC servers store data on a blockchain. No UAV onboard story needed	It lacks scalability and UAV movement
[58]		Verify the integrity of the data between drones	Offer simulation and time analysis of suggested systems	Do not explicitly consider the UAV network
[69]		Secure power plants that detect touch are banned	User validation and tracking only a big deal of transactions reduces costs	There is no clear consensus method
[91]	Non-reproduction	Preventing dishonesty by UAV in a network	Highlights blocked UAV applications and features that improve drone security	No tactical solution or implementation issues are discussed
[92]		Improve UAV non-reputability	Secure critical infrastructure with an energy-efficient blockchain-based UAV system	Proof-of-work reduced system efficiency by trapping bad nodes
[61]	Availability	Increased node-to-node communication security support	UTM architecture fixes enterprise system latency a issues	There are no implementation results. The experiment uses one drone, and scalability is not studied
[60]		For UAV maintenance and authentication, a rusted ground-based drone controller was used	This enables peers to replace a family when maintaining availability requires communication	Overhead from responsible parties
[62]	Authenticity	Preventing attacks on the user's identity	Organizes the network in a way that relies on blocking-based software	UAV's mobile blockchain implementation with high data processing efficiency in real-time
[93]		Create an administration and authentication system for new drones	A blocked the best secure drone delegate transportation assistance by optimizing drone scalability	Scalability is not addressed

system and deny unauthorized requests. However, with the rising use of UAVs in various intelligent applications, collaborative intelligence, continuous learning, low latency, privacy, and massive connectivity are important. FANET dramatically improves the interoperability of UAVs and innovative solutions by providing a framework for AI to enhance its capabilities. As stated previously, traditional encryption techniques based on cryptography and trust are widely used in UAVs; however, this has changed with the advent of enabling technologies like AI, ML, FL etc.

1) *Blockchain Assisted UAV Solution:* Multiple applications recruit UAVs with wireless connectivity, including health care services, armed services, precision agriculture, urban planning, maritime communication, wildlife conservation, and rescue operations. As mentioned above, commercial and social gains result from effective UAVs in various intelligent applications. However, although 5G and beyond blockchain with the UAV network have many benefits, some problems still need to be solved.

- *Data Manipulation:* 6G communication technology operates in a frequency range of 95 GHz–3 THz, has a data rate of 1 Tbps (uplink and downlink), and a bandwidth of 1 THz, which is high. Faster than the current 5G, it generates massive data, requiring ML, deep learning, and Big Data analytic techniques to convert it into usable data [15].
- *Data Protection in UAV:* Data security is essential when D2D and D2G communication occurs. ML and physical layer security techniques can protect the UAV system from hackers. It is possible for cyberattacks like DoS, masquerades, and spoofing to happen. However, there is a prospect that the data will modify a lot due to quantum attacks, which might result in errors. Therefore, the blockchain-based system offered can address these data security issues. Nevertheless, its efficient real-time deployment is still in its infancy [65].
- *Standardization:* According to organizations, the IEEE and international telecommunications union

(ITU) have yet to finalize standards and regulations for blockchain technology. As a result, good rules, regulations, and advice for the real-time deployment of blockchain on the UAV network mean that standards and guidelines for using UAVs over the 6G communication channel must be simple and easy to follow. As a result, it is only elementary to implement blockchain in real-world 6G networks with standardization of the blockchain technology.

- *Vulnerability Assessment in Secure Systems:* Programming languages such as Solidity, Kotlin, and Java are designed for implementing smart contracts (SCs). For trusted members of the public, it builds trust agreements take place without any central authority. Therefore, it may be vulnerable to eavesdropping and MITM phishing attacks [69]. As a result, appropriate testing solutions require before deployment and verification of the security of SC vulnerabilities.
- *Energy-efficiency:* UAVs are battery-powered flying machines with limited processing power, storage capacity, and response times. Implementing smart contract and consensus mechanisms [70] on UAVs in a blockchain and 6G-based UAV network requires more processing power, leading to a computational power bottleneck. Therefore, optimizing the UAV network and operations is necessary to lessen bottleneck occurrences.
- *Handover Delays:* UAV communication data's safety and privacy are paramount. Centralized cloud and currently available fog systems offer some security, but there is only one point of failure. This survey also lists other gaps in the current state-of-the-art solutions researchers have proposed worldwide. Cyber-attacks, such as spoofing, eavesdropping, connecting, jamming, fabrication, and access control attacks, might compromise centralized solutions. Blockchain, a distributed ledger technology, may be a viable solution to the above problems. However, for applications where confidence assurance is necessary, it is essential to use it effectively. The hash of the previous block links the blocks. A block header contains hashes, headers, prior blocks, Merkle root nonces, and timestamps in a block's data structure.

Here are some practical examples of blockchain-assisted UAV communication that showcase the real-world applications of this research:

- *Drone Delivery Networks:* Blockchain can be used to create decentralized and secure drone delivery networks. Smart contracts on the blockchain can facilitate automated delivery operations, including order verification, payment processing, and tracking. This enables transparent and efficient delivery services while ensuring trust and accountability among the involved parties.
- *UAV Traffic Management:* Blockchain can play a vital role in managing and coordinating UAV traffic in urban airspace. By recording flight plans, permissions, and real-time flight data on the blockchain, multiple UAVs can securely and autonomously communicate and coordinate their movements. This improves airspace safety, minimizes collisions, and allows for more efficient use of limited airspace resources.
- *Emergency Disaster Response and Management:* During natural disasters or emergency situations, UAVs are often deployed for search and rescue missions, damage assessment, and communication support. Blockchain can enhance these operations by providing a decentralized communication network for UAVs, ensuring secure and reliable data transmission, and enabling coordination among multiple response teams in a transparent manner.
- *Environmental Monitoring:* UAVs equipped with sensors can collect valuable environmental data, such as air quality, temperature, or water pollution levels. By leveraging blockchain, this data can be securely stored and shared among stakeholders, including researchers, government agencies, and environmental organizations. Blockchain ensures data integrity, authenticity, and traceability, enabling more effective environmental monitoring and decision-making processes.
- *Precision Agriculture:* UAVs are increasingly used in precision agriculture for crop monitoring, pest detection, and irrigation management. Blockchain can enable secure and transparent data sharing among farmers, agronomists, and other stakeholders. Smart contracts can automate agreements for sharing agricultural data, ensuring fair compensation and fostering collaboration within the ecosystem.
- *UAV Swarm Coordination:* Blockchain technology can facilitate the coordination and synchronization of UAV swarms. By recording swarm parameters, mission objectives, and individual UAV behavior on the blockchain, swarm members can autonomously interact, exchange information, and collaboratively perform complex tasks. This enables efficient and robust swarm operations for applications such as surveillance, mapping, or infrastructure inspection. These practical examples highlight the diverse applications of blockchain-assisted UAV communication across various industries and domains. They demonstrate how blockchain technology can address critical challenges, enhance operational efficiency, and enable new possibilities in UAV-based services and applications.

Blockchain-assisted UAV challenges and their deployment scenarios are highlighted in Fig. 7. The safety and privacy of UAV communication data are of paramount importance. Currently available centralized cloud and fog systems offer some level of security, but there is only one point of failure [72]. This survey also lists other gaps in the current state-of-the-art solutions researchers propose worldwide. Cyber-attacks, such as spoofing, eavesdropping, meaconing, connecting,

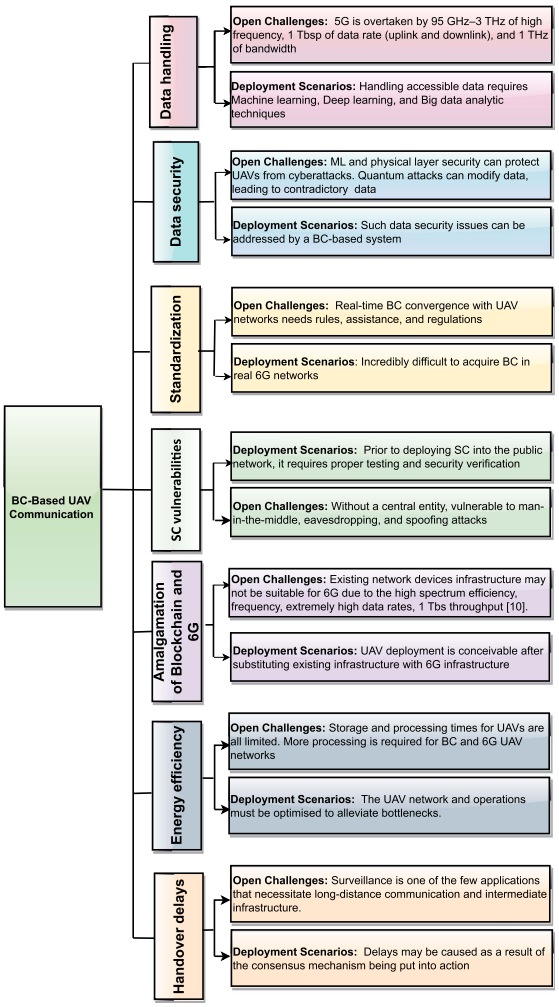

FIGURE 7. BC-assisted UAV scenario.

jamming, fabrication, and access control assaults, might compromise centralized solutions. Blockchain, a distributed ledger technology, may be a viable solution to the above problems. However, for applications where confidence assurance is necessary, it is essential to use it effectively. The hash of the previous block links the blocks. A block header is a piece of information such as hashes, headers, prior blocks, Merkle root nonce's, and timestamps in a block's data structure.

2) *Blockchain-Assited FL via UAV Network:* The use of UAVs and blockchain technology is in its infancy due to blockchain's immutable nature; UAV-assisted [71] communication enables shelter from cyber threats. Fig. 8 represents the blockchain layer, data sensing, application layer, or UAV application and control environment for blockchain-assisted UAV networks. The benefits of blockchain in UAV-assisted FL communication networks include scalability, privacy, security, immutability, transparency, and efficiency [73]. Combining FL and blockchain in UAV-assisted applications provides additional benefits [74]. In light of this, multiple kinds of research have recently been proposed to exploit the potential of UAVs and blockchain in distributed model training. For instance, the authors in [75] proposes a federated blockchain (FedBlock), which records and updates the local model parameter via a specific distributed ledger. This approach replaces the centralized FL server used for aggregation and operates a chain for consensus. The study in [76] introduces blockchain for the spectrum sharing of drones in the wireless network. The proposed architecture uses consortium blockchain technology to develop a secure spectrum-sharing mechanism in a UAV-assisted cellar network. The proposed architecture uses consortium blockchain technology to provide a safe spectrum-sharing means in a UAV-assisted cellar network. The authors in [77] propose a novel serverless architecture for FL enabled by blockchain and UAV technologies. The simulation outcomes affirm the advantages of blockchain by correlating the system's end-to-end efficiency in terms of latency and confidentiality.

IV. DATA SECURITY ANALYSIS IN BC-ENABLE UAV NETWORK

The use of blockchain in UAV communication has the potential to enhance data privacy and security in various ways.

- *Data Encryption:* Blockchain technology can encrypt the data being transmitted between UAVs to prevent unauthorized access or interception of the data.
- *Authentication:* Blockchain can help to verify the authenticity of the UAVs communicating with each other. By using public-key cryptography, each UAV can be assigned a unique digital identity, which can be verified by the blockchain network.
- *Immutable Record Keeping:* Blockchain can maintain an immutable record of all communication between UAVs, ensuring that any tampering or modification of the communication is easily detected.
- *Access Control:* Blockchain can implement access control mechanisms to prevent unauthorized access to UAV communication channels.
- *Smart Contracts:* Smart contracts can be used to automate certain security processes and ensure that certain conditions are met before communication is allowed between UAVs.
- *Consensus Mechanisms:* Blockchain can use consensus mechanisms to ensure that all nodes in the network agree on the state of the communication between UAVs.

Blockchain is transparent, meaning that all participants in the network have access to the same information, making it easier to identify and track any attempts to access or modify the data. In the context of drone communication, blockchain can provide data security by creating a tamper-proof ledger of all the data and transactions exchanged between drones and GCS. This includes flight data, sensor readings, and other mission-critical information. By using blockchain, the data is secured and cannot be modified or deleted, ensuring that the data remains accurate and trustworthy. Additionally,

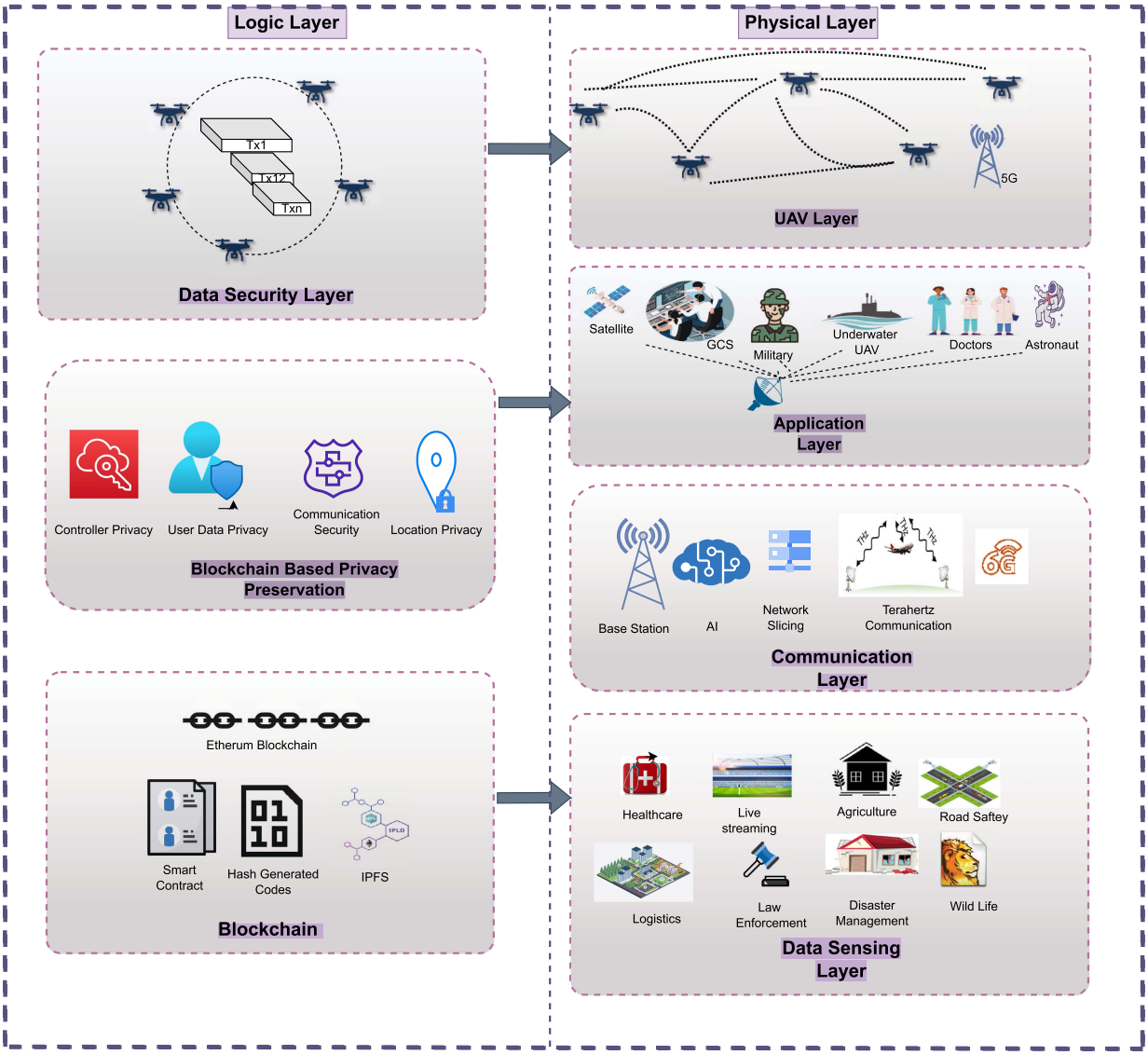

FIGURE 8. Blockchain-enabled UAV communication.

blockchain's decentralized nature makes it more difficult for hackers or malicious actors to interfere with the communication between drones and GCS. Moreover, blockchain employs cryptographic techniques to secure the data. For instance, data is encrypted and stored in blocks, and each block is linked to the previous one using a cryptographic hash function, creating an immutable and tamper-proof chain. Furthermore, blockchain can provide secure authentication and identity management for UAVs. Each UAV can have a unique digital identity, and the blockchain can be used to verify the identity of each UAV and ensure that only authorized UAVs can access the network. While numerous initiatives have been taken to realize a blockchain-based communication network, the dynamic network characteristics and real-time data processing requirements of a V2X communication scenario render the straightforward adoption of existing blockchain technology inappropriate. Even though blockchain has much potential to improve security and network management, the technology has much latency. This means that new blockchain algorithms with exceptionally low latency must be made before they can be used in 6G-V2X. However, the current blockchain technology's limited throughput and scalability are also significant open issues that require extensive investigation. For example, the use of public blockchains can expose sensitive data to the public, and the integration of UAVs into blockchain networks can also introduce new vulnerabilities, such as rogue devices and DoS attacks. Therefore, further research is needed to address these concerns and develop effective solutions that can ensure the privacy and security of data in blockchain-enabled UAV communication.

The blockchain-based UAV on communication can help with supply chain management [78], disaster response [79], relief operations [80], product delivery [81], aerial photography [82], and surveillance [83]. According to surveys, they

have developed blockchain technology as one of the security solutions for UAV communications and outlined research challenges on blockchain-enabled UAV network security. This section discusses the functionalities and constraints of blockchain-enabled UAV communication and provides a comparative data security analysis. In contemporary computing systems, the decentralization of DNS using blockchain technology has emerged as a promising alternative to mitigate software attacks. By distributing content across multiple sites and enabling users to regulate the space between them, blockchain-based DNS [84] makes it impractical for malevolent actors to launch software attacks. Additionally, this approach confers legal ownership of the associated assets to authorized users, thereby preventing unauthorized access or alterations. Consequently, to ensure data privacy and security and the risk of unauthorized manipulation of the information is minimized. A hierarchical intrusion detection and reaction scheme to enhance the security of UAV networks against debilitating cyberattacks such as false information diffusion, GPS spoofing, jamming, and black hole and grey hole attacks [85]. The security of blockchain technology is heavily dependent on the cost required to breach the system and alter newly generated data, as this is essential for maintaining the integrity of the blockchain-enabled UAV between the security of blockchain products. Therefore, brand identity is crucial, particularly in situations where a single excavator (or pool) holds the majority of computational power, leading to a 51% attack on the current blockchain history. Furthermore, such an attack may result in undesirable consequences, such as the manipulation of transactions, double-spending, and other forms of cyber-attacks. This occurs because the dominant excavator gains more power in the administration process and generates more results in work verification than any other excavator on the blockchain network [86].

V. CHALLENGES AND OPEN RESEARCH DIRECTIONS

The field of UAV communication presents both challenges and opportunities through the integration of key technical drivers. This article focuses on the holistic integration of several critical technical drivers, including confidentiality, variable latency constraints, bogus parameter updates, obstruction detection, communication delay, and encouraging the edge, safety, and integrity of UAV traffic management devices to participate in the mining process.

Maintaining the confidentiality of sensitive information while allowing for effective communication and collaboration among UAV data security is a primary challenge associated with this integration. Additionally, variable latency constraints pose a significant challenge, requiring the development of sophisticated algorithms and communication protocols to ensure UAVs can operate safely and efficiently despite unpredictable delays. Bogus parameter updates and obstruction detection also present significant challenges, as they can compromise the safety and reliability of UAV operations. Communication delays are another critical challenge, leading to miscommunication and coordination errors between UAVs and traffic management devices.

Despite these challenges, integrating key technical drivers presents significant opportunities for improving UAV communication's safety, efficiency, and effectiveness. Encouraging the edge, security, and integrity of UAV traffic management devices to participate in the mining process can improve the accuracy and reliability of traffic management data in UAV delivery services while providing valuable insights into the behaviour of UAVs in different operational contexts. Effective solutions will require innovative approaches and collaboration among various stakeholders, including UAV manufacturers, UAV delivery service providers, and researchers. The use of blockchain technology can increase the reliability and efficiency of data transfer and storage by employing protocols and guidelines to prevent unauthorized access.

Apart from trust issues, the UAV industry is grappling with several challenges, including the need for effective air traffic management and the trustworthiness of operations in crowded areas. Strict safety protocols and regulations must be implemented to address these concerns, including robust encryption mechanisms and strict access control policies to ensure confidentiality. Ensuring compliance with flight regulations is also critical to maintaining public trust and safety.

In the realm of UAV communication systems, several attributes are deemed advantageous, including low cost, high adaptability and agility, and the ability to cover a larger area than terrestrial systems, resolve traffic issues promptly, and deploy easily. However, challenges persist, such as dynamic channel conditions and difficulties integrating UAVs into established networks due to limited battery capacity and load. In exceptional cases, such as in highland areas with limited communication resources, cellular networks present the most promising option in terms of range and scalability. Nevertheless, several issues must still be addressed, including connection reliability, network availability, energy efficiency, and security concerns in real-world situations.

A. COMMUNICATION PERSPECTIVE CHALLANGES

UAVs are envisioned as a vital part of future 6G mobile networks. The demanding prerequisites of these applications require the guidance of advances like reconfigurable intelligence surfaces (RIS), terahertz (THz) communication, AI, and small cell systems. Remote and real-time control (RRC), high-precision positioning and seamless coverage, and multimedia transmission UAV lightweight authentication schemes include industrial IoT, UAV, healthcare IoT, satellite IoT, and self-driving vehicles [94]. UAVs' major principles are deployment flexibility, LoS connectivity, and controlled mobility [95]. In addition, the UAV-to-everything (U2X) networks are being grown alongside 6G and IoE [96]. Furthermore, for self-driving UAVs to work efficiently beyond the visual line of sight, a solid UTM system is required [97]. UTMs need efficiency, security, and hazard communication to manage their movement in urban airspace. Consequently, 6G established

a UTM ecosystem centred on terrestrial and non-terrestrial capabilities that enable mobile, aerial, and satellite communication. Embracing UAVs as ABS raises ground station reach, resulting in better coverage and cell-free communications. 6G heterogeneous network integration requires a coherent framework composed of key enabling technologies such as artificial intelligence (AI), blockchain, visible light communication (VLC), quantum communications, and THz communications [98].

The significant concerns are listed below:

1) *The Aerial Nature of Drones:* Presents a significant challenge in cellular communication. Most existing cellular antennas are designed to point downward, complicating drone communication in several ways. Firstly, drones have a weaker signal to work with, making it difficult to maintain a stable connection. Secondly, drones may need to switch between multiple BS, resulting in frequent handoff discussions.
2) *Security Scrutinize:* Recently, the use of UAVs has become increasingly popular among criminals and youth due to their small size and ease of use. This has raised concerns, as terrorists have also begun using UAVs for their operations, taking advantage of their affordability and accessibility. UAVs can be used to transport weapons, hazardous chemicals, and even explosives that can cause damage to buildings and structures.
   Furthermore, military analysts are worried about the potential of UAVs being used for espionage, surveillance, and gathering political and military intelligence. While research has focused on addressing security concerns for nations and organizations, the security and structure of UAVs remain critical areas of study.
3) *Safety Concerns:* Ensuring drone flight safety is crucial for conducting drone operations in specific circumstances while maintaining an acceptable level of protection. Therefore, the drone industry offers a four-phase model for developing drones.
4) *Assessment of Risk of UAVs:* This critical approach determines the acceptable solution in correspondence with the effort required. In any organization, usability is essential, as it establishes a framework for securing and maintaining reliable operations through permission and insurance. Additionally, the documented procedures must provide constant safety assurance, as the results determine the overall threat to unmanned aircraft systems (UAS) safety.
5) The combination of two technologies presents several challenges that must be addressed. Implementing 5G requires a thorough examination of various structural and technical aspects. Clear regulatory frameworks should be developed and identified to facilitate the implementation of smart contracts. The scalability of blockchain technology should also be improved to accommodate numerous devices, each requiring a unique address. The presence of rogue devices may lead to network instability, making it difficult to inter-operate blockchain platforms and hindering the addition of new information.
6) *Scalability of Drone-chain Networks:* Combining multiple drones to accomplish various tasks can create a drone network, which helps reduce the possibility of counterfeit drones and other security risks [99]. 5G is a significant leap in wireless communication technology, and it can achieve all the objectives using existing technology. A flying base station serves as both a user device and a relay, and each 5G use case has its unique requirements. Utilizing drones for communication during disasters is a creative and intelligent idea that can enable first responders and remote cities in attack zones to share orders and coordinate forces in war zones effectively. However, novel techniques and standards must be established before UAVs become more prevalent in UAV-assisted 5G communications.
   Integrating the three emerging technologies of blockchain, UAVs, and AI (FL, ML) can lead to revolutionary applications characterized by security, intelligence, and support for mission-critical scenarios. However, this integration presents several challenges that require further research to be useful [100]. Unfortunately, few studies have considered this research direction, and there is still ample room for contribution and improvement. Regarding latency, UAV networks require significant resources and extremely low latency when communicating with GCS to support real-time surveillance. In addition, adding blockchain to the UAV network architecture can induce further delay; for instance, transactions can take seconds or minutes to include in a block, and multiple blocks can exacerbate this delay. Furthermore, using FL algorithms can aggravate the latency problem due to the need to train models and transfer model updates between clients and a third-party server [101]. Thus, more research is necessary to accurately predict the system's latency and address this issue.
   Another promising research direction is to consider power consumption accompanying various processes such as communication, sensing, training, and mining. Given that UAVs are resource-limited devices, designing a low-power scheme of lightweight blockchain and ML models can reduce the computational complexity of the integrated system, help scale the operations of UAVs, and generate a cost-effective and reliable network. Furthermore, UAVs will primarily be involved in many applications that require information exchange over wireless links. Therefore, designing a scheme that can classify operations based on their importance and prioritize transmission resources would also be an exciting research direction.

B. BLOCKCHAIN PERSPECTIVE CHALLENGES

The 5G network is a decentralized system that eliminates the need for trusted external authority. The decentralization

method also eliminates bottlenecks, resulting in more effective service delivery. Furthermore, the blockchain-enabled verification approach can improve quality of service (QoS), i.e., low latency and high throughput, but requires robust confidentiality security with the abolition of malicious BSs [102]. Recently, communication networks for UAVs can reimburse for insufficient wireless network coverage [103]. All whilst UAVs can deliver products [104] and collect real-time traffic flow data [105]. According to new findings, UAVs can support content-centric networking and mobile edge computing [106]. However, ensuring trustworthiness and restricting disobedient UAVs in decentralized, untrusted UAV networks is tricky. The convergence of blockchain technology into UAV networks can ensure UAVs' confidence. In addition, International Business Machines Corporation (IBM) resubmitted a patent application to create a blockchain-based system to safeguard the privacy and security of UAV data [107]. To be precise, blocks in blockchains store information about UAVs, such as product lines, manufacturers, and adjacency to a specified territory. And inappropriate UAV behaviour can be recognized and identified regularly.

There are several security challenges associated with blockchain-assisted UAV communication, including:

- *Private Key Management:* Private keys are used to sign transactions and secure the blockchain network. If a private key is lost or stolen, it can lead to unauthorized access and transactions. In a UAV network, private key management becomes more challenging due to the dynamic and distributed nature of the network.
- *Malware and Cyber Attacks:* UAVs are vulnerable to malware and cyber attacks, which can compromise the security and integrity of the blockchain network. Attackers can use malware to take control of UAVs or exploit vulnerabilities in the blockchain network to steal data or disrupt operations.
- *Network Congestion:* UAVs generate a large volume of data that needs to be processed and stored on the blockchain network. This can lead to network congestion and slow down the transaction processing time. As a result, the UAV network may become less efficient, and data may become more vulnerable to attacks.
- *Scalability:* Blockchain networks are not inherently scalable, and the addition of UAVs can exacerbate this problem. As the number of UAVs in the network increases, the amount of data generated also increases, which can lead to scalability issues.
- *Interoperability:* UAV networks that rely on different blockchain platforms may not be interoperable, making it difficult to share data between different networks. This can lead to data silos, which can reduce the efficiency and effectiveness of the UAV network.
- *Regulatory Compliance:* Blockchain-assisted UAV networks may be subject to regulatory compliance requirements, such as data privacy and security regulations. Compliance with these regulations can be challenging, especially if the UAV network operates across different jurisdictions.

Blockchain technology has the potential to revolutionize wireless communication networks by providing enhanced security, trust, and decentralized operations. Here are some notable use cases where blockchain can be applied to improve wireless communication networks:

1) *Secure and Trustworthy Communication:* Blockchain can ensure secure and tamper-proof communication between devices in wireless networks. By recording communication transactions on the blockchain, it becomes challenging for malicious actors to alter or manipulate the data. This enables secure and trustworthy communication, especially in critical applications such as UAV communications.
2) *Spectrum Management:* Blockchain can help optimize spectrum allocation and management in wireless networks. With blockchain, different entities can register their spectrum usage and negotiate access rights through smart contracts. This decentralized approach enables efficient spectrum sharing, reduces interference, and improves overall network performance.
3) *Identity and Access Management:* Blockchain can provide a decentralized identity management system for wireless communication devices. Each device can have a unique identity stored on the blockchain, enabling secure and verified access to network resources. This eliminates the need for centralized authentication authorities and enhances privacy while ensuring authorized access to the network.
4) *Resource Sharing and Trading:* Blockchain-based smart contracts can facilitate peer-to-peer resource sharing and trading in wireless communication networks. For example, UAVs can autonomously negotiate and share resources like computing power or network bandwidth using smart contracts. This decentralized resource management improves efficiency, reduces costs, and enables dynamic resource allocation.
5) *Billing and Micropayments:* Blockchain can streamline billing and payment processes in wireless networks, particularly for microtransactions. Smart contracts on the blockchain can automatically execute payments between devices or service providers based on predefined rules. This enables efficient and transparent payment mechanisms, supporting new business models and incentivizing participation in the network.
6) *Network Monitoring and Management:* Blockchain can provide a distributed and transparent network monitoring and management system. By recording network statistics, performance metrics, and events on the blockchain, network administrators and stakeholders can have real-time visibility into the network's health and performance. This promotes proactive network management and troubleshooting.

Overall, blockchain-assisted UAV communication offers several benefits, but it also presents several security challenges

that need to be addressed to ensure the security and integrity of the network. Here are some potential research directions for blockchain-assisted UAV communication:

- *Scalability:* Developing methods to scale blockchain technology to handle the large amounts of data generated by UAV communication systems.
- *Security:* Exploring new cryptographic techniques and other security mechanisms to enhance the security of UAV communication systems.
- *Privacy:* Investigating ways to ensure the privacy of data transmitted between UAVs, such as using zero-knowledge proofs or homomorphic encryption.
- *Energy Efficiency:* Developing techniques to reduce the energy consumption of blockchain-based UAV communication systems, such as using more efficient consensus mechanisms or optimizing smart contract execution.
- *Consensus Mechanisms:* Investigating new consensus mechanisms that can provide better scalability, latency, and energy efficiency for UAV communication systems.
- *Standardization:* Developing standards for blockchain-based UAV communication systems to ensure interoperability and facilitate the adoption of the technology.
- *Integration with other technologies:* Exploring ways to integrate blockchain technology with other emerging technologies, such as AI, IoT, and edge computing, to create more advanced and efficient UAV communication systems.
- *Real-world Testing:* Conducting real-world testing of blockchain-assisted UAV communication systems to evaluate their effectiveness and identify potential challenges and limitations.

VI. CONCLUSION

Blockchain technology seems to have promising features for a wide range of applications. However, deploying these advanced technologies faces numerous challenges, including scalability and portability. Cost, computational and storage resources, and the compatibility of different blockchain ledgers are all barriers. This article highlights the blockchain-enabled UAV communication environment. There are several security concerns about UAV communications and the integration of blockchain and FL to enhance UAV wireless communications. One major dilemma is privacy and security challenges, which are discussed in depth, and blockchain offers a promising solution. Subsequently, our survey potentials and future trends are thoroughly discussed. Finally, we provide a thorough explanation of certain challenges and future research directions that require the attention of blockchain enable UAV communication technology researchers.

REFERENCES

[1] H. Kang, J. Joung, J. Kim, J. Kang, and Y. S. Cho, "Protect your sky: A survey of counter unmanned aerial vehicle systems," *IEEE Access*, vol. 8, pp. 168671–168710, 2020.

[2] J. Li et al., "Joint optimization on trajectory, altitude, velocity, and link scheduling for minimum mission time in UAV-Aided data collection," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1464–1475, Feb. 2020.

[3] Z. Ullah, F. Al-Turjman, U. Moatasim, L. Mostarda, and R. Gagliardi, "UAVs joint optimization problems and machine learning to improve the 5G and beyond communication," *Comput. Netw.*, vol. 182, 2020, Art. no. 107478.

[4] M. Soni and D. K. Singh, "Blockchain-based group authentication scheme for 6G communication network," *Phys. Commun.*, vol. 57, 2023, Art. no. 102005.

[5] R. Majeed, N. A. Abdullah, M. F. Mushtaq, and R. Kazmi, "Drone security: Issues and challenges," *Parameters*, vol. 2, 2021, Art. no. 5GHz.

[6] G. K. Pandey, D. S. Gurjar, H. H. Nguyen, and S. Yadav, "Security threats and mitigation techniques in UAV communications: A comprehensive survey," *IEEE Access*, vol. 10, pp. 112858–112897, 2022.

[7] A. Afaq, Z. Ahmed, N. Haider, and M. Imran, "Blockchain-based collaborated federated learning for improved security, privacy and reliability," 2022, *arXiv:2201.08551*.

[8] F. Ayaz, Z. Sheng, D. Tian, and Y. L. Guan, "A blockchain based federated learning for message dissemination in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 1927–1940, Feb. 2022.

[9] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and privacy issues of UAV: A survey," *Mobile Netw. Appl.*, vol. 25, no. 1, pp. 95–101, 2020.

[10] H. Sachdeva, S. Gupta, A. Misra, K. Chauhan, and M. Dave, "Improving privacy and security in unmanned aerial vehicles network using blockchain," 2022, *arXiv:2201.06100*.

[11] S. Aggarwal, N. Kumar, and S. Tanwar, "Blockchain-envisioned UAV communication using 6G networks: Open issues, use cases, and future directions," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5416–5441, Apr. 2021.

[12] B. Li, Z. Fei, Y. Zhang, and M. Guizani, "Secure UAV communication networks over 5G," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 114–120, Oct. 2019.

[13] Y. Zeng, Q. Wu, and R. Zhang, "Accessing from the sky: A. tutorial on UAV communications for 5G and beyond," *Proc. IEEE*, vol. 107, no. 12, pp. 2327–2375, Dec. 2019.

[14] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain envisioned UAV networks: Challenges, solutions, and comparisons," *Comput. Commun.*, vol. 151, pp. 518–538, 2020.

[15] R. Gupta, A. Nair, S. Tanwar, and N. Kumar, "Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges," *IET Commun.*, vol. 15, no. 10, pp. 1352–1367, 2021.

[16] D. Saraswat 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.

[17] V. Hassija et al., "Fast, reliable, and secure drone communication: A comprehensive survey," *IEEE Commun. Surv. Tut.*, vol. 23, no. 4, pp. 2802–2832, Fourthquarter 2021.

[18] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6G: Challenges, opportunities and research directions," in *Proc. IEEE 2nd 6G Wireless Summit*, 2020, pp. 1–5.

[19] A. Sanober and S. Anwar, "Blockchain for content protection in E-healthcare: A case study for COVID-19," in *Proc. IEEE 8th Int. Conf. Adv. Comput. Commun. Syst.*, 2022, pp. 661–666.

[20] M. Ghamari, P. Rangel, M. Mehrubeoglu, G. S. Tewolde, and R. S. Sherratt, "Unmanned aerial vehicle communications for civil applications: A review," *IEEE Access*, vol. 10, pp. 102492–102531, 2022.

[21] E. M. Ghourab, W. Jaafar, L. Bariah, S. Muhaidat, and H. Yanikomeroglu, "Interplay between physical layer security and blockchain technology for 5G and beyond: A comprehensive survey," to be published.

[22] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for UAV communications and flying Ad-Hoc networks," *Ad Hoc Netw.*, vol. 133, 2022, Art. no. 102894.

[23] M. Hooper et al., "Securing commercial WiFi-based UAVs from common security attacks," in *Proc. IEEE MILCOM Mil. Commun. Conf.*, 2016, pp. 1213–1218.

[24] D. He, S. Chan, and M. Guizani, "Drone-assisted public safety networks: The security aspect," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 218–223, Aug. 2017.

[25] J.-A. Maxa, M.-S. B. Mahmoud, and N. Larrieu, "Survey on UAANET routing protocols and network security challenges," *Ad Hoc Sensor Wireless Netw.*, p. 40, 2017.

[26] F.-H. Tseng, L.-D. Chou, and H.-C. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," *Hum.-Centric Comput. Inf. Sci.*, vol. 1, no. 1, pp. 1–16, 2011.

[27] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, and R. Brooks, "The sleep deprivation attack in sensor networks: Analysis and methods of defense," *Int. J. Distrib. Sensor Netw.*, vol. 2, no. 3, pp. 267–287, 2006.

[28] J. R. Douceur, "The sybil attack," in *Proc. Peer-Peer Syst.: 1st Int. Workshop*, 2002, pp. 251–260.

[29] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 370–380, Feb. 2006.

[30] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "Mitigating byzantine attacks in ad hoc wireless networks," *Dept. Comput. Sci., Johns Hopkins Univ., Baltimore, MD, USA*, Tech. Rep. Version1, Mar. 2004.

[31] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proc. 2nd ACM Workshop Wireless Secur.*, 2003, pp. 30–40.

[32] A. Koubâa, A. Allouch, M. Alajlan, Y. Javed, A. Belghith, and M. Khalgui, "l: A survey," *IEEE Access*, vol. 7, pp. 87658–87680, 2019.

[33] V. Kriz and P. Gabrlik, "Uranuslink-communication protocol for UAV with small overhead and encryption ability," *IFAC-PapersOnLine*, vol. 48, no. 4, pp. 474–479, 2015.

[34] N. A. Khan, N. Z. Jhanjhi, S. N. Brohi, and A. Nayyar, "Emerging use of UAVs: Secure communication protocol issues and challenges," in *Drones in Smart-Cities*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 37–55.

[35] J. A. Saputro, E. E. Hartadi, and M. Syahral, "Implementation of GPS attacks on DJI phantom 3 standard drone as a security vulnerability test," in *Proc. IEEE 1st Int. Conf. Inf. Technol., Adv. Mech. Elect. Eng.*, 2020, pp. 95–100.

[36] E. Deligne, "ARDrone corruption," *J. Comput. Virol.*, vol. 8, pp. 15–27, 2012.

[37] K. Wesson and T. Humphreys, "Hacking drones," *Sci. Amer.*, vol. 309, no. 5, pp. 54–59, 2013.

[38] S.-H. Seo, B.-H. Lee, S.-H. Im, and G.-I. Jee, "Effect of spoofing on UAV using counterfeited GPS signal," *J. Positioning, Navigation, Timing*, vol. 4, no. 2, pp. 57–65, 2015.

[39] J. Crook, "Infamous hacker creates SkyJack to hunt, hack, and control other drones," *TechCrunch*, 2013.

[40] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, "A survey on ransomware: Evolution, taxonomy, and defense solutions," *ACM Comput. Surv.*, vol. 54, no. 11s, pp. 1–37, 2022.

[41] M. Fyrbiak et al., "Hardware reverse engineering: Overview and open challenges," in *Proc. IEEE 2nd Int. Verification Secur. Workshop*, 2017, pp. 88–94.

[42] N. Krishnan et al., "Establishment of FANETs using IoT-based UAV and its issues related to mobility and authentication," in *Modelling and Simulation of Fast-Moving Ad-Hoc Networks (FANETs and VANETs)*, IGI Global, Hershey, PA, USA, 2023, pp. 74–93.

[43] S. Hashemi, S. A. Hashemi, R. M. Botez, and G. Ghazi, "A novel air traffic management and control methodology using fault-tolerant autoencoder and P2P blockchain application on the UAS-S4 ehécatl," in *Proc. AIAA SCITECH Forum*, 2023, Art. no. 2190.

[44] V. Mohindru, Y. Singh, and R. Bhatt, "Hybrid cryptography algorithm for securing wireless sensor networks from node clone attack," *Recent Adv. Elect. Electron. Eng. (Formerly Recent Patents Elect. Electron. Eng.)*, vol. 13, no. 2, pp. 251–259, 2020.

[45] P. Zheng et al., "Aeolus: Distributed execution of permissioned blockchain transactions via state sharding," *IEEE Trans. Ind. Inform.*, vol. 18, no. 12, pp. 9227–9238, Dec. 2022.

[46] S. Tanwar, "Basics of cryptographic primitives for blockchain development," in *Blockchain Technology: From Theory to Practice*. Berlin, Germany: Springer, 2022, pp. 83–111.

[47] R. Gupta, A. Kumari, and S. Tanwar, "Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 1, 2021, Art. no. e4176.

[48] C. Feng, B. Liu, K. Yu, S. K. Goudos, and S. Wan, "Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3582–3592, May 2022.

[49] Y. Tan, J. Liu, and N. Kato, "Blockchain-based key management for heterogeneous flying ad hoc network," *IEEE Trans. Ind. Inform.*, vol. 17, no. 11, pp. 7629–7638, Nov. 2021.

[50] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, "Elliptic curve cryptography; applications, challenges, recent advances, and future trends: A. comprehensive survey," *Comput. Sci. Rev.*, vol. 47, 2023, Art. no. 100530.

[51] U. S. Aditya, R. Singh, P. K. Singh, and A. Kalla, "A survey on blockchain in robotics: Issues, opportunities, challenges and future directions," *J. Netw. Comput. Appl.*, vol. 196, 2021, Art. no. 103245.

[52] S. Hafeez, H. Manzoor, R. Cheng, L. Mohjazi, M. A. Imran, and Y. Sun, "BIRDS: Blockchain-empowered immutable and reliable delivery service using UAV network," to be published.

[53] Y. Wu, P. Song, and F. Wang, "Hybrid consensus algorithm optimization: A mathematical method based on POS and PBFT and its application in blockchain," *Math. Problems Eng.*, vol. 2020, p. 13, 2020.

[54] R. Alkadi, N. Alnuaimi, C. Y. Yeun, and A. Shoufan, "Blockchain interoperability in unmanned aerial vehicles networks: State-of-the-art and open issues," *IEEE Access*, vol. 10, pp. 14463–14479, 2022.

[55] Y. Qian, Y. Jiang, L. Hu, M. S. Hossain, M. Alrashoud, and M. Al-Hammadi, "Blockchain-based privacy-aware content caching in cognitive internet of vehicles," *IEEE Netw.*, vol. 34, no. 2, pp. 46–51, Mar./Apr. 2020.

[56] W. Xiao, M. Li, B. Alzahrani, R. Alotaibi, A. Barnawi, and Q. Ai, "A blockchain-based secure crowd monitoring system using UAV swarm," *IEEE Netw.*, vol. 35, no. 1, pp. 108–115, Jan./Feb. 2021.

[57] M. Singh, G. S. Aujla, and R. S. Bali, "ODOB: One drone one block-based lightweight blockchain architecture for Internet of Drones," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops*, 2020, pp. 249–254.

[58] S. R. Nagrare, L. A. Tony, A. Ratnoo, and D. Ghose, "Multi-lane UAV traffic management with path and intersection planning," in *Proc. AIAA Scitech Forum*, 2022, Art. no. 1505.

[59] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling drones in the Internet of Things with decentralized blockchain-based security," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6406–6415, Apr. 2021.

[60] A. Kapitonov, I. Berman, V. Manaenko, V. Rzhevskiy, V. Bulatov, and A. Zenkin, "Robonomics as a blockchain-based platform for unmanned traffic management of mobile vehicles," in *Proc. IEEE Workshop Res., Educ. Develop. Unmanned Aerial Syst.*, 2019, pp. 9–17.

[61] M. S. Kumar, S. Vimal, N. Jhanjhi, S. S. Dhanabalan, and H. A. Alhumyani, "Blockchain based peer to peer communication in autonomous drone operation," *Energy Rep.*, vol. 7, pp. 7925–7939, 2021.

[62] N. Andola et al., *Wireless Pers. Commun.*, vol. 119, no. 1, pp. 343–362, 2021.

[63] S. Hafeez, M. A. Shawky, M. Al-Quraan, L. Mohjazi, M. A. Imran, and Y. Sun, "BETA-UAV: Blockchain-based efficient and trusted authentication for UAV communication," in *Proc. IEEE 22nd Int. Conf. Commun. Technol.*, 2022, pp. 613–617.

[64] I. J. Jensen, D. F. Selvaraj, and P. Ranganathan, "Blockchain technology for networked swarms of unmanned aerial vehicles (UAVs)," in *Proc. IEEE 20th Int. Symp. A World Wireless, Mobile Multimedia Netw.*, 2019, pp. 1–7.

[65] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," *Veh. Commun.*, vol. 23, 2020, Art. no. 100249.

[66] S. H. Alsamhi et al., "Drones' edge intelligence over smart environments in B5G: Blockchain and federated learning synergy," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 1, pp. 295–312, Mar. 2022.

[67] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," *Procedia Comput. Sci.*, vol. 132, pp. 1815–1823, 2018.

[68] V. A. Kanade, "Securing drone-based ad hoc network using blockchain," in *Proc. IEEE Int. Conf. Artif. Intell. Smart Syst.*, 2021, pp. 1314–1318.

[69] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet Things*, vol. 11, 2020, Art. no. 100218.

[70] M. Mukhandi, F. Damião, J. Granjal, and J. P. Vilela, "Blockchain-based device identity management with consensus authentication for IoT devices," in *Proc. IEEE 19th Annu. Consum. Commun. Netw. Conf.*, 2022, pp. 433–436.

[71] S. Hafeez, L. Mohjazi, M. A. Imran, and Y. Sun, "BCSFL: Blockchain-enabled clustered and scalable federated learning (BCS-FL) in UAV swarms," to be published.

[72] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. Leung, "Blockchain and machine learning for communications and networking systems," *IEEE Commun. Surv. Tut.*, vol. 22, no. 2, pp. 1392–1431, Secondquarter 2020.

[73] S. H. Alsamhi et al., "Drones' edge intelligence over smart environments in B5G: Blockchain and federated learning synergy," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 1, pp. 295–312, Mar. 2022.

[74] D. Hamouda, M. A. Ferrag, N. Benhamida, and H. Seridi, "PPSS: A privacy-preserving secure framework using blockchain-enabled federated deep learning for industrial IoTs," *Pervasive Mobile Comput.*, vol. 88, 2022, Art. no. 101738.

[75] F. Zhou, R. Q. Hu, Z. Li, and Y. Wang, "Mobile edge computing in unmanned aerial vehicle networks," *IEEE Wireless Commun.*, vol. 27, no. 1, pp. 140–146, Feb. 2020.

[76] D. Li, Z. Luo, and B. Cao, "Blockchain-based federated learning methodologies in smart environments," *Cluster Comput.*, vol. 25, no. 4, pp. 2585–2599, 2022.

[77] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 451–466, Jan. 2020.

[78] M. Al-Bkree, "Managing the cyber-physical security for unmanned aerial vehicles used in perimeter surveillance," *Int. J. Innov. Res. Sci. Stud.*, vol. 6, no. 1, pp. 164–173, 2023.

[79] A. A. Hughes, "Unmanned aerial vehicle use in humanitarian activities," *Lynchburg J. Med. Sci.*, vol. 5, no. 1, 2023, Art. no. 137.

[80] M. A. Farzaneh, S. Rezapour, A. Baghaian, and M. H. Amini, "An integrative framework for coordination of damage assessment, road restoration, and relief distribution in disasters," *Omega*, vol. 115, 2023, Art. no. 102748.

[81] O. Ozkan, "Multi-objective optimization of transporting blood products by routing UAVs: The case of istanbul," *Int. Trans. Oper. Res.*, vol. 30, no. 1, pp. 302–327, 2023.

[82] Y. Li et al., "Unmanned aerial vehicle remote sensing for antarctic research: A review of progress, current applications, and future use cases," *IEEE Geosci. Remote Sens. Mag.*, vol. 11, no. 1, pp. 73–93, Mar. 2023.

[83] S. M. Teutsch, L. Lee, S. Teutsch, S. Thacker, and M. St Louise, "Considerations in planning a surveillance system," *Princ. Pract. Public Health Surveill.*, vol. 18, no. 10, 2010, Art. no. 1093.

[84] H. Wang, H. Li, A. Smahi, Y. Yao, and S.-Y. R. Li, "MIS: A multi-identifier management and resolution system based on consortium blockchain in metaverse," 2023, *arXiv:2301.03529*.

[85] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 9, pp. 1594–1606, Sep. 2018.

[86] A. Kumar, Y. Singh, and N. Kumar, "Secure Unmanned Aerial Vehicle (UAV) Communication Using Blockchain Technology," in *Recent Innovations in Computing: Proceedings of ICRIC 2021*, 2022, pp. 201–211.

[87] Q. Wu, L. Liu, and R. Zhang, "Fundamental trade-offs in communication and trajectory design for UAV-enabled wireless network," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 36–44, Feb. 2019.

[88] E. Ghribi, T. T. Khoei, H. T. Gorji, P. Ranganathan, and N. Kaabouch, "A secure blockchain-based communication approach for UAV networks," in *Proc. IEEE Int. Conf. Electro Inf. Technol.*, 2020, pp. 411–415.

[89] Z. Lv, L. Qiao, M. S. Hossain, and B. J. Choi, "Analysis of using blockchain to protect the privacy of drone Big Data," *IEEE Netw.*, vol. 35, no. 1, pp. 44–49, Jan./Feb. 2021.

[90] A. Islam and S. Y. Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things," *Comput. Elect. Eng.*, vol. 84, 2020, Art. no. 106627.

[91] A. Ossamah, "Blockchain as a solution to drone cybersecurity," in *Proc. IEEE 6th World Forum Internet Things*, 2020, pp. 1–9.

[92] E. Barka, C. A. Kerrache, H. Benkraouda, K. Shuaib, F. Ahmad, and F. Kurugollu, "Towards a trusted unmanned aerial system using blockchain for the protection of critical infrastructure," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 8, 2019, Art. no. e3706.

[93] M. A. Cheema, M. K. Shehzad, H. K. Qureshi, S. A. Hassan, and H. Jung, "A drone-aided blockchain-based smart vehicular network," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4160–4170, Jul. 2021.

[94] A. S. Khan et al., "A survey on 6G enabled light weight authentication protocol for UAVs, security, open research issues and future directions," *Appl. Sci.*, vol. 13, no. 1, 2023, Art. no. 277.

[95] Q.-V. Pham et al., "Aerial computing: A. new computing paradigm, applications, and challenges," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8339–8363, Jun. 2022.

[96] S. Zhang, H. Zhang, and L. Song, "Beyond D2D: Full dimension UAV-to-Everything communications in 6G," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6592–6602, Jun. 2020.

[97] R. Shrestha, R. Bajracharya, and S. Kim, "6G enabled unmanned aerial vehicle traffic management: A. perspective," *IEEE Access*, vol. 9, pp. 91119–91136, 2021.

[98] A. Kalla, C. De Alwis, P. Porambage, G. Gür, and M. Liyanage, "A survey on the use of blockchain for future 6G: Technical aspects, use cases, challenges and research directions," *J. Ind. Inf. Integration*, vol. 30, 2022, Art. no. 100404.

[99] Y. Wu, H.-N. Dai, H. Wang, and K.-K. R. Choo, "Blockchain-based privacy preservation for 5G-Enabled drone communications," *IEEE Netw.*, vol. 35, no. 1, pp. 50–56, Jan./Feb. 2021.

[100] J. Zhu, J. Cao, D. Saxena, S. Jiang, and H. Ferradi, "Blockchain-empowered federated learning: Challenges, solutions, and future directions," *ACM Comput. Surv.*, vol. 55, no. 11, pp. 1–31, 2023.

[101] E. T. Michailidis, K. Maliatsos, D. N. Skoutas, D. Vouyioukas, and C. Skianis, "SecureUAV-Aided mobile edge computing for IoT: A. review," *IEEE Access*, vol. 10, pp. 86353–86383, 2022.

[102] J. Wang, Y. Liu, S. Niu, H. Song, W. Jing, and J. Yuan, "Blockchain enabled verification for cellular-connected unmanned aircraft system networking," *Future Gener. Comput. Syst.*, vol. 123, pp. 233–244, 2021.

[103] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

[104] G. Kimchi et al., "Unmanned aerial vehicle delivery system," US Patent 9,573,684, Feb. 21, 2017.

[105] L. Wang, F. Chen, and H. Yin, "Detecting and tracking vehicles in traffic by unmanned aerial vehicles," *Automat. Construction*, vol. 72, pp. 294–308, 2016.

[106] N. Cheng et al., "Air-ground integrated mobile edge networks: Architecture, challenges, and opportunities," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 26–32, Aug. 2018.

[107] A. Kumar, A. Kundu, C. A. Pickover, and K. Weldemariam, "Unmanned aerial vehicle data management," US Patent 10,611,474, Apr. 7 2020.

SANA HAFEEZ (Student Member, IEEE) received the B.S. degree in software engineering from the Mirpur University of Science and Technology, Mirpur, and the M.S. degree in computer science from COMSATS University Islamabad, Islamabad, Pakistan, in 2020. She is currently working toward the Ph.D. degree in electrical and electronic engineering in autonomous systems and connectivity with the University of Glasgow, Glasgow, U.K. She was an Investigator Supervisor with the Cybercrimes Division of the Law Enforcement Agencies in Islamabad and the Azad Jammu and Kashmir Police. Her research interests include artificial intelligence, unmanned aerial vehicles, blockchain, vehicular networks, and intelligent wireless networking. She is also the Member of the Equality, Diversity, and Inclusion Group (EDIG), University of Glasgow, WIE, WIDS, and IEEE young professionals.

AHSAN RAZA KHAN received the B.S. degree in electrical engineering from Comsats University Islamabad, Islamabad, Pakistan, in 2015 and the M.S. degree in electrical engineering from the Mirpur University of Science and Technology, Mirpur, Pakistan, in 2019. He is currently working toward the Ph.D. degree in electronic and electrical engineering with the James Watt School of Engineering, University of Glasgow, Glasgow, U.K. His research interests includes distributed learning for next-generation intelligent applications, mobile edge computing, wireless sensing, and non-orthogonal multiple access.

MOHAMMAD M. AL-QURAAN (Student Member, IEEE) received the B.Sc. (Hons.) degree in telecommunications engineering and the M.Sc. (Excellence) degree in wireless telecommunications engineering from Yarmouk University, Irbid, Jordan, in 2011 and 2019, respectively. He is currently working toward the Ph.D. degree in electronics and electrical engineering with the University of Glasgow, Glasgow, U.K. From 2012 to 2018, he was a senior network and telecommunications Engineer with the Jordan University of Science and Technology (JUST), Al Ramtha, Jordan. Till 2020, he was the Head of the Network and Telecommunications Department, JUST. His research interests include machine learning, computer vision, cognitive radio, and beyond 5G wireless technologies.

LINA MOHJAZI (Senior Member, IEEE) received the B.Sc. (Hons.) degree in electrical and electronic engineering from the United Arab Emirates University, Al Ain, UAE, in 2008, the M.Sc. degree with distinction in electrical and electronic engineering from Khalifa University, Abu Dhabi, UAE, in 2012, and the Ph.D. degree in electrical and electronic engineering from the Institute for Communication Systems, University of Surrey, Guildford, U.K., in 2018. She is currently an Assistant Professor (Lecturer) with the James Watt School of Engineering, University of Glasgow, Glasgow, U.K. Her research interests include beyond 5G wireless technologies, physical-layer optimization and performance analysis, wireless power transfer, machine learning for future wireless systems, and reconfigurable intelligent surfaces. She is an Associate Editor for IEEE COMMUNICATIONS LETTERS and IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY. She is an Affiliate Member of the Mohammed bin Rashid Academy of Scientists, UAE and a Fellow of the Women's Engineering Society.

AHMED ZOHA (Senior Member, IEEE) received the Ph.D. degree from the esteemed 6G/5GIC Centre, University of Surrey, Guildford, U.K., in 2014. He is currently an Associate Professor with the James Watt School of Engineering, University of Glasgow, Glasgow, U.K. He has more than 15 years of experience. His research interests include AI, machine learning, and advanced signal processing. His research has been cited by national and international bodies. His contributions in designing intelligent applications and algorithms for 5G and beyond, connected healthcare, and smart energy monitoring have gained local and international recognition. He was the recipient of three prestigious IEEE best paper awards and endorsed as a UK exceptional talent by the Royal Academy of Engineering awarded to early-career world-leading innovators and scientist. He actively contributes to organizing IEEE and EAI conferences, serving in various leadership roles.

MUHAMMAD ALI IMRAN (Fellow, IEEE) received the M.Sc. (with Hons.) and Ph.D. degrees from Imperial College London, U.K., in 2002 and 2007, respectively. He is currently the Dean of Graduate Studies in the College of Science & Engineering. He is also Head of Autonomous Systems and Connectivity Division and a Professor of communication systems with the James Watt School of Engineering, University of Glasgow, Glasgow, U.K. He has authored/co-authored more than 500 journals and conference publications, and has supervised more than 50 successful Ph.D. graduates. He has over 20 years of experience with several leading roles in multi-million pound-funded projects, working primarily in the areas of cellular communication systems. He has been awarded ten patents. He is the Specialty Chief Editor for the IoT section of *Frontiers in Communications and Networks* and an Associate Editor for IEEE TRANSACTIONS ON COMMUNICATIONS and previously servied in editorial roles for the IEEE COMMUNICATIONS LETTERS, IEEE ACCESS, and *IET Communications*.

YAO SUN (Senior Member, IEEE) received the B.S. degree in mathematical sciences and the Ph.D. degree in communication and information system from the University of Electronic Science and Technology of China, Chengdu, China, in 2014 and 2019, respectively. He is currently a Lecturer with the James Watt School of Engineering, University of Glasgow, Glasgow, U.K. He has extensive research experience in wireless communication area. His research interests include intelligent wireless networking, network slicing, blockchain system, Internet of Things, and resource management in mobile networks. Dr. Sun was the recipient of the IEEE IoT Journal Best Paper Award 2022, IEEE Communication Society of TAOS Best Paper Award in 2019 ICC, and Best Paper Award in 22nd ICCT. He was the Guest Editor for special issues of several international journals. He was the TPC Chair for UCET 2021, and a TPC Member for a number of international flagship conferences, including ICC 2022, VTC spring 2022, GLOBECOM 2020, WCNC 2019, and ICCT 2019.