Received: 3 July 2020 | Revised: 21 September 2020 | Accepted: 6 October 2020

IET Communications

DOI: 10.1049/cmu2.12113

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH PAPER

Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges

Rajesh Gupta[1] | **Anuja Nair**[1] | **Sudeep Tanwar**[1] | **Neeraj Kumar** [2,3,4,5]

[1] Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India

[2] Department of Computer Science Engineering, Thapar Institute of Engineering and Technology, Deemed to be University, Patiala, Punjab, India

[3] Department of Computer Science and Information Engineering, Asia University, Taiwan

[4] King Abdul Aziz University, Jeddah, Saudi Arabia

[5] School of Computing, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India

Correspondence
Neeraj Kumar, Department of Computer Science Engineering, Thapar Institute of Engineering and Technology, Deemed to be University, Patiala, Punjab, India.
Sudeep Tanwar, Department of Computer and Science Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India.
Email: neeraj.kumar@thapar.edu, sudeep.tanwar@nirmauni.ac.in

Funding Information
This work is supported by Visvesvaraya Ph.D. Scheme for Electronics and IT by the Department of Electronics and Information Technology, Government of India under the unique awardee number MEITY-PHD-2828.

Abstract

From the past few years, Unmanned Aerial Vehicles (UAVs) has proved an immense potential in providing the cost and time-efficient solutions to the various societal applications such as healthcare, supply chain, and video & surveillance. It has many data security and privacy issues, and researchers across the globe have given many solutions to protect data from cyber-attacks. Many of them have suggested cryptographic-based solutions, which is very compute extensive. Very few researchers have suggested Blockchain (BC)-based solutions, but their solutions may suffer from high data storage cost as well as network latency, reliability, and bandwidth issues. To overcome the above-mentioned issues, this paper proposed an InterPlanetary File System and BC-based secure UAV communication scheme over the 6G network. This proposed scheme ensures data security and privacy, reduces data storage cost, and enhances network performance. Then, the research challenges and future directions for further improvement of the proposed system have been presented.

1 | INTRODUCTION

Unmanned Aerial Vehicle (UAV) or Uncrewed Aerial Vehicle is commonly known as a drone, which is a category of robotic vehicles that are either self-governed or remotely administered by means of remote control devices through wireless communication [1]. This ensures wireless connectivity, which is cost-effective for the devices not constituting infrastructure coverage. UAVs are mainly comprised of sensors to provide information about the state of the aerial vehicle and to detect targets in an efficient way. It also contains computing devices such as analogue controls and micro controllers, actuators, UAV software, and communication systems. In comparison to terrestrial communication systems, UAV wireless systems are on-demand and flying at low altitude is faster to deploy. It can be configured flexibly and seems to have well-worked communication channels attributable to Line-of-Sight (LOS) links that are short-ranged. UAVs were initially designed for military applications, but currently, it is adopted in a variety of civilian applications such as search & rescue operations, urban planning, weather monitoring, and precision agriculture. Apart from these, various other applications of UAVs are depicted in Figure 1.

Figure 2 estimation of the UAV market is projected to $108.7 billion in 2031 from $19.3 billion in 2019, which climbed to this significant level from $0.25 billion in 2013

FIGURE 1 Diversified applications of UAV network [2]

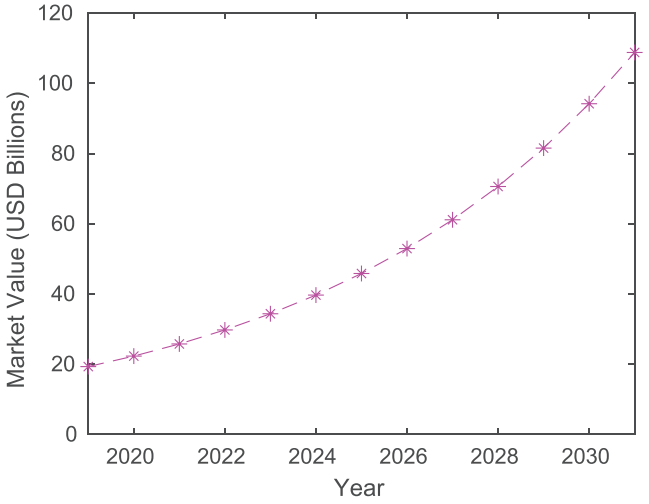

FIGURE 2 Growth of global UAV market [3]

[4]. According to the Federal Aviation Administration (FAA) [3], a total of 412,000 commercial drones are registered in the United States in 2019 and the drones are anticipated to be 2.4 million units in 2022. UAVs were initially employed by Japan-based Non-Governmental Organization (NGO) in order to scrutinize whaling that was unlicensed. Also, after the earthquake and tsunami in Japan that took place in 2011, many other UAVs were deployed to closely monitor the ground situation. The data collected from the employed UAVs were vital in the execution of emergency operations [5]. Such real-life examples have invigorated researchers to explore this domain actively and work on their strengths and weaknesses. Some of the monotonous applications like weather monitoring or agriculture and farming require a single UAV system, whereas others like nuclear plant surveillance that turns out to be too hazardous require a multi-UAV system. Even though single-UAV systems are being utilized since eras, but exploiting many small UAVs has its own advantages. As UAVs are circumscribed to confined topographical regions due to their LOS and energy constraint, single UAVs prove inefficient. They can communicate with only ground node and hence, communication will be only UAV-to-Infrastructure (U2I) one. A multi-UAV system (many small UAVs deployed in parallel) overcomes energy and coverage constraints and has the ability to observe data from diverse perspectives. Also, it intensifies the reliability of data and provides fault tolerance. The collective work of UAVs improves system performance and also reduces operational cost. Due to fault tolerance capability, the missions are completed in a quick and efficient manner.

For effective and productive mission completion, numerous UAVs can be used as a result of their abilities, flight time, and constrained payload. In order to efficiently organize multiple UAVs, proper cooperation is required by means of efficient communication and networking. Communication problems can be resolved by means of establishment of ad hoc networks amid multiple UAVs where all the UAVs formulate an ad hoc network, out of which roughly some UAVs are linked to the ground station. Ad hoc networks can be thought of as a distinct category of Vehicular Ad hoc Network (VANET) or Mobile Ad hoc Network (MANET) [6]. In such systems, also known as Flying Ad hoc Network (FANET), UAVs can communicate among each other and with the ground station as well. High mobility is one of the characteristics of UAV networks. In case of MANET and VANET, nodes are moving devices and cars, respectively, whereas, in the case of UAV networks, nodes fly. The network topology continuously changes due to this high mobility as compared to MANET and VANET. Similar to MANET and VANET, UAV networks establish Peer-to-Peer (P2P) communication to guarantee collaboration and coordination among UAVs. Data is generally collected by UAVs and passed to Ground Control Station (GCS) and thus ensuring U2I communication and UAV-to-UAV (U2U) communication.

Despite having high mobility and energy-constrained UAVs for wireless communications as promising benefits, various challenges [7] are also introduced by the UAV communication network. First, in order to support safety critical functions such as real-time control, crash, and collision avoidance, more rigid latency and security requirements are required in UAV systems as compared to normal communication links present in terrestrial communication systems. Secondly, due to high mobility in multi-UAV networks, effective UAV coordination is required. This maintains collaboration and communication among UAV nodes for proper information retrieval. Side by side, new communication protocols are need of the hour, taking into account intermittent and sparse network connectivity. Next, the size, power, and weight constraints of UAVs can limit their communication and computation capabilities. Also, due to high mobility, interference with neighbouring UAV enabled base stations is more likely to take place, requiring an effective interference management system. Due to these UAV challenges, studies and research are currently under progress for UAV communication systems.

The security vulnerabilities in the UAV communication network [8] are being explored by researchers as drones are connected directly to the Internet and communicate wirelessly, thus, causing a severe menace to the security of UAV networks. Drone hijacking programs such as Sky Jack are engineered to hack and take control of the drones wirelessly by an autonomous body,

converting them to zombie drones under attacker control. The cellular user equipment can suffer from interference owing to LOS links in case UAV is contrived by attackers. Hence, it is necessary to address the security of the UAV communication network. Security issues can be based on unprotected WiFi, manipulated settings of flight control, GPS attacks, and access to the configuration of drone. Such a Cyber-Physical System (CPS) attacks on UAVs can be mitigated by means of Blockchain (BC) technology [9, 10]. To make the UAVs safer with great accuracy and ease of control, BC technology is a path forward. Because of inter-coordination between multiple UAVs passing secure information between each other, UAV communication is a suitable candidate for BC implementation. BC technology consists of a chain of blocks containing transactions. Each block consists of a previous block's hash value in the BC and so forth. This feature of BC makes it highly difficult to tamper the data of the block as a minute alteration in data will alter the hash value of entire block. BC is a decentralized distributed ledger that is immutable, is accessed faster and is transparent to all the nodes (participants) of the BC network. Due to the distributed consensus mechanism, it is secure and reliable. Also, a Smart Contract (SC) [11, 12] uses the concept of BC. It is a digital document containing a set of rules self-enforced programmatically to be followed among numerous parties involved in a BC network. SC programs are generally written in Solidity or Go. SCs are tamper-proof, self-verifiable, and are self-executable.

Let us consider an application of supply chain management. The data accumulated from UAVs carrying out various tasks such as inventory management can be transported to a CPS connected to a BC network. Every block of the BC can comprehend details of the data collected by UAV along with timestamp at which block was added and thus monitoring the flow of inventory data. UAVs are programmed to continuously perform scanning of inventory at regular intervals and thus automating the process. SC can be used to automate some processes happening at regular intervals, such as ordering of supplies when not in stock. As soon as the stock goes beyond a pre-defined limit, and conditions are met, SCs can be executed without any intervention of humans. Also, automated decision making can be performed by means of SCs on a multi-agent UAV system. For example, some amount of token, which is a digital currency, can be transferred from one agent (buyer) to another agent (seller) in a BC network for supply chain management, which transactions such as the ordering of supply is done and is successfully verified by the buyer. BC can be useful in many other applications such as decentralized storage in UAV networks, UAV networks for edge computing, co-ordinated UAV services, UAV surveillance application, etc. In most scenarios, BC enabled UAV applications require the establishment of private BC since secure communication between participating members is needed [13]. This ensures privacy between the participating members as well. Whereas in the case of public BC implemented on UAV networks, privacy is suffered as also researched in many literature surveys [14, 15].

Moreover, having security vulnerabilities as a weak point, reliability, low latency, high data rate, and fault tolerance are some strong points of the UAV communication network. These constraints can be resolved by means of Fifth-Generation (5G) [16] communication networks. Compared to the Fourth-Generation (4G) [17] communication 5G provides better Quality of Service (QoS) performance. Continual growth has been witnessed over the last decade in global mobile data traffic, with a data volume increase of 23 times in 2021 as compared to statistics in 2005. It is predicted by International Telecommunication Union (ITU) that this exponential growth will persist till 2030 and mobile data traffic will be reaching astoundingly five Zettabytes (ZB) per month as illustrated in Figure 3. Growth at an annual rate of 55% is predicted for overall mobile data traffic in 2020–2030, climbing to 607 Exabytes (EB) in 2025 and 5016 EB in 2030 [18]. 5G technology can meet the mobile communications requirement for up to 10 years but is expected to fade away well before 2030. Nonetheless, the exceeding growth of data-centric and automated systems may surpass the capabilities of 5G communication systems. Certain applications, such as AR & VR, require the devices to go up to a minimum of 10 Gbps data rate, which is far beyond the requirement of 5G technology. Hence, for overcoming these challenges, a Sixth-Generation (6G) [19] wireless system with the full support of Artificial Intelligence (AI), smart sensors, vehicle tracking, intelligent device computation, and three-dimensional printing is meticulously evolving. It will be like 5G but with higher speed, lesser latency, and much-improved bandwidth. 5G could not be more competent in smart intelligence and automation, which is easily overcome by the 6G network. It is predicted to have a transmission rate up to ∼ 1 Tbps, which is 1000 times faster than 5G. 6G will be experiencing ∼ 1 ms latency in order to ease the exhilarating AI feature.

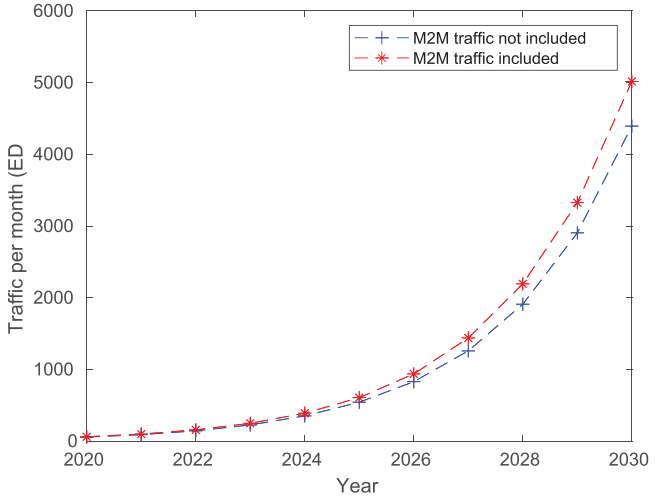

FIGURE 3 Global mobile data traffic forecasting [18]

To overcome the communication and security issues of the existing UAV solutions, this paper proposes a BC-assisted secure UAV communication in 6G environment. BC takes care of the security and privacy of UAV communication data, whereas 6G enhances the performance of network parameters. Storing data into the BC is very costly, which is ≈ $550 per 1 MB of data. The explanation for the Ethereum data storage cost is mentioned in Section 6.2. To overcome the storage cost issue,

we have used InterPlanetary File System (IPFS), which is distributed and immutable storage. It does not charge anything to store the data.

1.1 | Motivation of the review

In combination with BC technology, drones convey a tremendous potential in disrupting the way we populate. To enable UAVs to be fortified with cryptographically secure techniques in order to ensure secure and safe communication and to be useful in applications like financial and defense applications, BC technology should be implemented. BC is espoused by various application areas as it condenses the security concerns occurring in communication of UAVs. This leads to enhanced participation of UAV implementing BC technology, although present communication techniques battle because of lack of smart intelligence & automation and latency & scalability problems. So, the 6G as a communication method in UAV can accomplish a massive transmission rate of 1 Tbps and ultra-low latency (<1 ms) along with fully equipped AI features. The incorporation of 6G and BC technology has amazing potential in many sectors precisely in armed and commercial sectors. Also, military services must be fully tenable from all possible cyber-attacks as they contain mission-critical and confidential information. UAV communication becomes more secure, contrasting to vulnerabilities of the network due to the combination of BC and 6G for security and communication purposes, respectively. This paper reviews various concerns of the 6G-enabled UAV communication system and efforts to figure out better BC-based solutions as compared to traditional ones.

1.2 | Review contributions

In this paper, we highlighted the security issues of the existing UAV communication system and its consequences. The foremost focus of this paper is UAVs communication security. We also investigate the BC concepts, which can help to secure the UAV communication. Following are the crisp objectives of the paper:

- We present a systematic survey on security issues in the existing UAV network and highlight how BC technology helps to mitigate those.
- We proposed a BC-based secure UAV communication network in the 6G environment. We integrate IPFS with the BC network to minimize the BC data storage cost.
- Finally, we present various research challenges that the proposed system may face during its real-time deployment.

1.3 | Review organization

The structure of the survey is as shown in Figure 4. Table 1 lists all abbreviations used in the paper. The rest of the paper is organized as follows. Section 1 gives an introduction to UAV and its needs, the communication aspects of UAVs, i.e. 4G, 5G,

TABLE 1 Abbreviations

Abbreviation	Description
$\mathcal{D}_{S\mathcal{L}}$	Data Sensing Layer
S_n	Scenario
ξ	Hash Key
$\mathcal{H}_{\mathcal{D}}$	Data Hash
ζ_{IPFS}	IPFS Storage
$\mathcal{B}_{public}$	Public Blockchain
$\mathcal{A}$ & $\mathcal{C}_{Layer}$	Application and Control Layer
τ	Time
SC	Smart Contract
ℓ	Latency
$\mathcal{U}$	UAV
$\mathcal{GCS}$	Ground Control Station
UAV	Unmanned Aerial Vehicle
LOS	Line-of-sight
NGO	Non-Governmental Organization
FAA	Federal Aviation Administration
VANET	Vehicular Ad hoc Network
MANET	Mobile Ad hoc Network
FANET	Flying Ad hoc Network
P2P	Peer-to-peer
U2I	UAV-to-Infrastructure
U2U	UAV-to-UAV
CPS	Cyber Physical System
BC	Blockchain
5G	Fifth Generation
4G	Fourth generation
QoS	Quality of Service
ITU	International Telecommunication Union
ZB	Zettabytes
EB	Exabytes
6G	Sixth Generation
AI	Artificial Intelligence
UAS	Unmanned Aircraft System
DoD	Department of Defense
LAP	Low-Altitude Platform
HAP	High-Altitude Platform
IoT	Internet of Things
VAR	Virtual and Augmented Reality
mMTC	Massive machine type communication
eMBB	Enhanced mobile broadband
URLLC	Ultra-reliable low latency communication
SDN	Software-defined networking
NFV	Network function virtualization

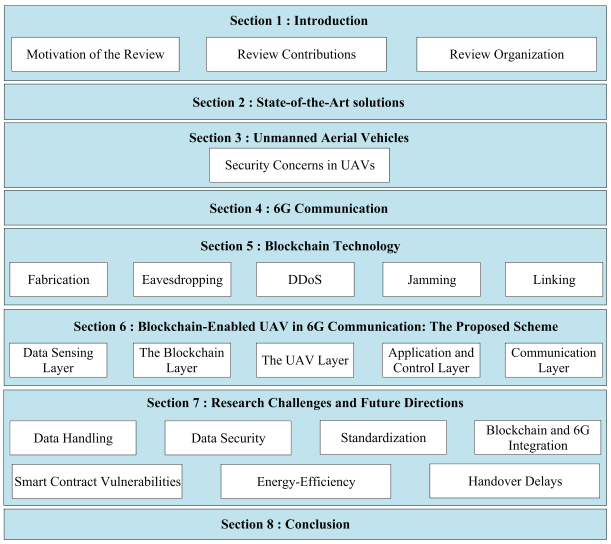

FIGURE 4 Organization of the paper

and 6G, various security issues in UAV communication and how BC can be plausible solution for the same. Section 2 represents the state-of-the-art solutions and their comparison with the proposed scheme. We give a brief overview of the fundamentals of UAV, BC technologies and 6G environment, and the scope of their integration which is the topic of this paper, in Sections 3, 4, and 5, respectively. In Section 6, we present the proposed BC-based secure UAV communication architecture in 6G environment. In Section 7, we discuss the research challenges and future directions of the proposed study. Finally, Section 8 concludes the paper.

2 | STATE-OF-THE-ART SOLUTIONS

A significant number of the survey papers are published till present by various researchers on the different security and communication facets of the UAV communication network. Almost all the reviews and research have fixated on either 5G or lesser communication networks, and very few have focused on the 6G network for the UAV communication network. The contextual information of BC technology, 6G network, UAV communication, and why the aforementioned three needs to be integrated is covered in the proposed survey. Na et al. [20] represented UAV along with the C-NOMA system using 6G-enabled Internet of Things (IoT) where the issue of non-convexity was resolved by means of an iterative algorithm providing a good convergence. Zhang et al. [19] demonstrated a way so that UAVs can adjust their communication modes as per the needs of sensing applications. This resulted in an improvement of QoS performance of transmission along with sensory performance. The only drawback both of them suffered was trust among the stakeholders was not established as security factor was not addressed at all. Nguyen et al. [21] addressed various challenges and opportunities related to the usage of BC in 6G but failed to focus on the UAV communication network.

Some literature is available that has not conversed about the combination of BC technology and 6G network, even though BC-enabled UAV networks were discussed in the same. García-Magariño et al. [10] discussed about maintaining security in UAV networks keeping surveillance as a context using BC technology. Implementation of BC helps in detecting compromised UAVs on the basis of trust policies. The paper was lacking in representing communication networks such as 5G, 6G, etc. for UAV communication. Jensen et al. [22] discussed how BC could be applied so that various cyber-attacks for UAV swarm networks can be defended, although, Hyperledger Fabric as the only framework was explored for UAV swarm. Rana et al. [23] represented ways to improve the security of drones and UAVs using BC technology, focusing on increasing the connectivity by means of a generic access control system. Mozaffari et al. [24] explored applications, challenges, and open issues of UAVs for wireless networks and also represented tools for addressing unique UAV issues. Koubaa et al. [25] integrated cloud computing paradigm with UAV for addressing cost and latency issues. Security and privacy issues were not addressed in [24, 25]. Public BCs when used, always create issues in privacy, whereas private BCs always ensure privacy. Islam and Shin [14] made use of private BC for data acquisition using UAV swarm wherein security, performance, connectivity, and energy consumption issues were taken into consideration leaving privacy as a concern unaddressed. The same author also created another data acquisition scheme using a UAV network but, instead of using a multi-UAV network, has explored the usage of only a single UAV network in [26].

Many of the literature have not explored the role of 6G networks in UAV along with BC usage. Chamola et al. [27] presented an extensive review of the main facets allied with the COVID-19 pandemic in which UAV and BC were one of the factors, but failed to address 6G as a communication network and has discussed only the role of 5G. Hentati and Fourati [28] and Alladi et al. [29] provided an extensive survey on UAV communication network and BC-enabled UAV network, respectively, but failed to address the role of 6G in UAV communication network. Mehta et al. [30] have represented the integration of 5G-enabled UAV network with BC along with representing the taxonomy of security concerns in UAV network. Ferrag et al. [15] developed a BC-based healthcare system with UAV assistance in IoT, focusing on improving the performance and security of the proposed healthcare scheme as well as the body sensors. Whereas, privacy issue was not addressed by the same. A summary of the aforementioned surveys in comparison to the proposed survey is represented in Table 2.

3 | UNMANNED AERIAL VEHICLES

The term drone came into picture in the early 1920s, referring to target aircraft that is remotely flown used in practice firing. These drones were not sophisticated and were just radio-controlled aircraft being controlled by a human pilot at all times. Later, the term got replaced by the Unmanned Aircraft System (UAS) espoused by the Department of Defense (DoD) of the United States and the FAA United States in 2005. UAS shows its complexity as it comprises of a drone, GCS, and communication network in order to make information exchange [31].

TABLE 2 Comparative analysis of pre-existing surveys on UAVs security with the proposed survey

Related works	Year	Key contributions	Merits	Demerits
[10]	2019	To maintain security in UAV networks keeping in account surveillance as a context using BC	BC is implemented in order to detect compromised UAVs on the basis on trust policies	Communication networks like 5G, 6G, etc. are not explored
[22]	2019	To discover the application of BC in order to defend various cyber-attacks	Development of BC for UAV swarm networks	Only Hyperledger Fabric framework is explored for UAV swarm
[23]	2019	To improve security of drones and UAVs using BC technology	Focuses on increasing the connectivity by means of generic access control system	Comparison with other existing solutions is not mentioned
[24]	2019	To explore applications, challenges and open issues of UAVs for wireless networks	Tools for addressing unique UAV issues are presented	Security and privacy issues are not addressed
[25]	2019	To integrate cloud computing paradigm with UAV for addressing cost and latency issues	An architecture is presented for integration of cloud with UAV	Integration of BC technology for security purpose is not addressed
[14]	2019	To present BC enabled scheme for acquisition of data using UAV swarm	Security, performance, connectivity, and energy consumption issues are taken into consideration	Privacy issue is not addressed as public BC is not implemented here
[26]	2019	To present BC enabled scheme for acquisition of data from IoT devices using UAV	Security, pseudonymity, and integrity of data is addressed here	It supports only single UAV in acquisition of data rather than multi-UAV
[27]	2020	To present detailed review on major aspects associated with COVID-19 pandemic	Role of UAV and BC is discussed	Only 5G is addressed here
[20]	2020	To represent UAV along with C-NOMA system for 6G enabled IoT	Non-convexity issue is solved by means of iterative algorithm giving a good convergence	Trust among the stakeholders and transparency issue is not addressed
[30]	2020	To represent integration of 5G-enabled UAV network with BC	A taxonomy of security issues in UAV network is presented. Also, latency, reliability, and energy efficiency issues are addressed	No framework is presented here
[19]	2020	To provide UAVs to adjust their communication modes as per the needs of sensing applications	Improvement in QoS performance of transmission	Security factor is not addressed
[28]	2020	To survey UAVs communication networks	Presented a deep review on communication protocols of UAV and BC as a research challenge is discussed	6G as a communication network is not discussed
[29]	2020	To survey BC enabled UAV networks	Application-specific examples with respect to BC features that overcomes cons of UAV is discussed	Role of 6G is not addressed
[21]	2020	To survey challenges and opportunities related to usage of BC in 6G	Mitigation of security threats in 6G by means of BC is discussed	Does not focus on UAV
[15]	2020	To develop BC-based healthcare system with UAV assistance in IoT	Focused on improving the performance and security of healthcare scheme and body sensors	Privacy issue, satellite communications for remote areas, and incentives to reward the validators is not addressed
Proposed Survey	2020	To integrate BC in 6G-enabled UAV network with purpose of resolving privacy, security, and communication issues	Presents a taxonomy of BC enabled UAV in 6G	-

UAVs are just aircraft that are autonomous either fully or partially by means of pre-programmed flight plans and is remotely controlled by pilots at GCS by means of remote control devices. UAV mainly is comprised of sensors for providing information about the state of the aircraft and to detect targets in an efficient way, computing devices such as analogue controls and micro controllers, actuators, UAV software, and communication systems.

Based on the number of UAVs exploited, it can be classified into two types. *Single UAV systems* are utilized in unknown geographical locations for navigation and control in order to monitor distant targets. Such UAV systems require each UAV node to behave like an isolated node where it communicates directly with GCS sending collected data [32]. This type of communication system falls under the category of the U2I communication system. Single UAV systems produce low latency and high data

rate when they are close to the ground station but also suffers from a failure of completion of tasks and survivability. *Multi-UAV systems* are used in most of the public and civil applications. UAVs here are smaller in size, are less expensive, and work in a coordinated way. The major design challenge in multi-UAV systems is efficient communication between coordinating UAVs as there is no GCS control. Such type of communication systems is categorized into U2U communication system [28]. Multi-UAV system possesses advantages like missions are completed at a lower cost as compared to single UAV system, scalability and coverage can be improved due to collaborative work on multiple UAVs covering the wide geographical area, survivability is increased because if one UAV fails, the operation can be survived by other UAVs in the vicinity, missions are completed in a quick and efficient manner as compared to single UAV system. The ultimate goal of these systems are high throughput, low latency, and wide coverage and due to their requirements, 6G can be considered as an integral part of UAVs.

On the basis of flying mechanism, UAVs can be classified into three types [33]: (a) *Multi-rotor drones* can fly over a specific location to provide continuous cellular coverage and thus making it less mobile and consuming significant power due to their tolerance against gravity continuously. (b) *Fixed-wing drones* are more energy-efficient and are able to carry a heavy payload. They can glide over the air, which helps them to travel at a faster speed. They cannot fly over a fixed location and do not possess the ability of vertical take-off and landing, as was in the case of multi-rotor drones. (c) *Hybrid wing drones* are a combination of multi-rotor and fixed-wing, taking the qualities from both. The UAVs that can fly over a specific location function properly in multi-UAV systems and are used mostly in surveillance applications. Such UAV systems are best suitable for integrating BC technology to ensure trust among UAVs and to communicate securely.

Depending upon the weight, UAV can be categorized into micro (less than 100 g), very small (between 100 g and 2 kg), small (between 2 and 25 kg), medium (between 25 and 150 kg), and large (more than 150 kg) UAVs. Out of which, large UAVs are used in mission-critical or defense applications, whereas small UAVs are used for performing regular tasks as in case of civilian applications. Inter-drone communications are best supported by cellular networks increasing the efficiency and safety of drone operations. 6G communication network provides better reliability and connectivity for UAV operations beyond LOS. 6G supports more dense IoT deployment and hence, offering IoT deployment in blind zone communication as well. Low latency, high throughput, and reliability features required by UAV are all provided by 6G communication in an efficient manner. 6G networks provide around 10-fold [34], i.e. 10 million devices per square km more than 5G network and thus giving large coverage area to UAV networks.

UAV networks can also be classified into *Low-Altitude Platforms (LAPs)* and *High-Altitude Platforms (HAPs)* [28] depending on altitude. LAPs are effective in terms of cost and are deployed faster, thus making it suitable for cellular communications. Also, they provide short-range LOS links enhancing communication performance. HAPs, on the other hand, provide wide coverage and can survive for more time in the air. They are complex and are not suitable for cellular communications as they cause network outage because of tremendous inter-cell interference. HAPs are mostly used by Internet companies.

3.1 | Security concerns in UAVs

Security is a significant concern when dealing with any digital system. Because of remote wireless communication and the unmanned nature of the UAV communication system, security is, even more, a serious concern. The concerned UEs are more likely to lose communication if the flying cellular BS is taken control by the attackers. Also, they might suffer from strong interference issues by means of LOS links. Therefore, for cellular communications, it is necessary to ensure the security of UAV systems. Majorly, UAV networks are prone to cyber-attacks targeting integrity and privacy of infrastructure, network, and information present in UAV. Attacks such as eavesdropping and keylogging [35] threaten the interception of the data between UAS and GCS, making the privacy of the information to suffer. Such attacks take place due to a lack of strong communication and encryption standards and lead to unauthorized access to private information. Keyloggers are used to track information entered by the keyboard. Originally used for parental control of activities of children, to track sensitive information being entered by employees, to track criminals, etc. Keyloggers are now used for the purpose of stealing information. Either in the case of ATMs, where pin is recovered by keyboard sniffers or in case of UAVs where privacy of information passed between multiple UAVs is compromised. Keyloggers cannot be detected by antivirus software and can remotely access your data over the Internet. Eavesdropping, as the name suggests, is the process of unauthorized listening of transmissions and can manipulate communications between multiple UAVs.

Attacks such as deauthentication, GPS spoofing, and message injections [36, 37] threaten the modification of exchanged data taking control over the UAS and its communication mechanism, thus causing causalities. GPS navigation system based on satellites delivers information to the users about the positioning and location of the traffic. In GPS spoofing, false GPS signals are sent by high power systems, which results in nodes accepting false GPS signals rather than legitimate signals. It is dangerous because it can make UAV nodes to capture, crash, or collide with other UAVs. Message injections are the process of injecting pseudo-legitimate messages having an exactly similar structure as that of a legitimate message. These messages mislead the aircraft or the ground station machine for making an appearance of fake aircraft. Message deletion and message modification also work with fake messages making it appear to be legitimate messages. In order to authenticate UAS and GCS and start a communication channel between them, management packets are used. These packets are compromised by means of sending deauthentication frames to both of them in order to disconnect their communication and thus attacker taking control of either UAV or GCS.

Attacks such as jamming are categorized under the denial of service (DoS) [33] preventing communication between multiple UAVs in the network. Jamming is performed by means of

TABLE 3 Interesting characteristics of 6G in comparison to 5G [39–41]

Characteristics	5G	6G
Bandwidth	1–2 GHz	1 THz
Data rate	20/10 Gbps	1 Tbps
Spectrum efficiency	120 bps/Hz	5–10 times that of 5G
Multiplexing	NOMA, Edge Computing	OAM
Localization Precision	10 cm on 2D	1 cm on 3D
Mobility	500 Kmph	>1000 Kmph
Connection density	1,000,000 per squareKm	10,000,000 per squareKm
End-to-End Delay	<5 ms	<1 ms
Radio-only Delay	100 ns	10 ns
Technique	m-MIMO	SM-MIMO, UM-MIMO
Throughput	10 Gbps	1 Tbps
Frequency	3–300 GHz	95 GHz–3 THz
Traffic capacity	10 Mbps/m^2	1–10 Gbps/m^2
Reliability	10^{-5}	10^{-9}

deliberately sending fake signals to the receiver and thus making it inefficient to receive legitimate signals. The network is jammed and thus denying legitimate services.

4 | 6G COMMUNICATION

Although 5G is on the verge of its deployment phase, it talks about 6G is catching up the momentum. Even though it is an early stage to speculate about 6G, but there is no doubt that 6G is going to take its shape in the near future. 5G communication network fails to meet requirements by 2030 with massive usage of the IoT and data-intensive applications. Hence, the emergence of 6G technology is the need of the hour for holographic projections, gaming, and remote surgery based on AR & VR, as 5G will not be able to support such a demand. Table 3 shows an exhaustive comparison between 5G and 6G communication networks. 6G with its various capabilities and characteristics such as 100 Gbps individual data rate, >1 Tbps data link data rate, <1 ms latency, up to 1000 km/h mobility and up to 1 THz of operating frequency is going to be a milestone in the field of mobile communications [38]. 6G has its promising feature of being AI-empowered from the physical layer to the service layer. 6G encompasses being useful in applications such as haptic communication in Virtual and Augmented Reality (VAR), IoT integrated smart city, which includes smart homes, connected vehicles, and autonomous driving and smart healthcare, automation and manufacturing, etc. One of the important elements of 6G communications will be UAV or drones. The aforementioned characteristics of 6G will prove to maximum beneficial for high data rate wireless connectivity required by the UAV communication network. 6G technology having key factors as Massive Machine Type Communication (mMTC), Enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communication (URLLC) will serve the purpose for UAVs. Also, with billions of user equipment and

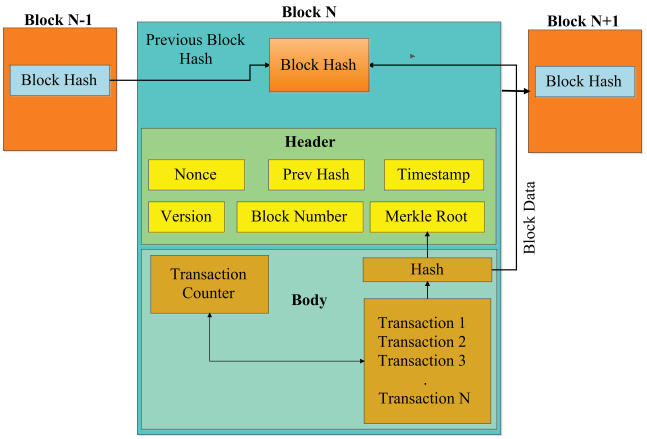

FIGURE 5 Structure of a blockchain block

IoT devices connected throughout in a UAV network, securing of sheer volumes of data collected from various platforms to fulfill the privacy and security requirements will require an all-rounded approach in 6G. BC technology is likely to play a major role in fulfilling these requirements and secure the communication system in UAV with 6G.

5 | Blockchain Technology

The key concern in UAV communication is its data security and privacy. Existing cloud and fog-based centralized solutions provide security to an extent but having a single point of failure. Likewise, other lacunas in the existing state-of-the-art solutions given by the researchers across the globe are mentioned in Table 2. The centralized solutions are also susceptible to various cyber-attacks such as masquerade, eavesdropping, linking, jamming, fabrication, and access control attacks. The plausible solution to the aforementioned issues is the BC, which is a distributed ledger technology coined by the anonymous researcher Satoshi Nakamoto in 2008. It has the potential to execute the applications, where trust assurance is required between the different stakeholders. It is a group of blocks that are chained together with the hash of the previous block [42]. A block is a data structure, which keeps the information like block hash, block header, previous block hash, Merkle root, nonce, timestamp, version, and block number. Figure 5 shows the detailed structure of a block.

BC is a chain of blocks in which the stored transactions are immutable and secure with cryptographic hashing techniques. It prevents transactions from cyber frauds and security risks. It is a distributed ledger technology, the peer nodes are responsible for the validation of transaction before added into the block of a BC using public–private key pairs. The peer nodes validate the transaction by using their private keys. A blockchain can also be viewed as a hash chain, where the transactions are stored as a hash $\mathcal{H}$ value (calculated using the hash of the previous block and the data stored) to prevent it from modification [43]. The hashing algorithm should be strong enough, which does not allow its reverse hash calculation. BC has the concept of an

SC, which is a programming code and can be self-executed on the encounter of the specific condition. It overruled the requirement of trusted centralized (third party) systems to maintain the trust between the peer nodes of the BC.

BC is of three different types, such as public (fully decentralized), private (centralized), and federated BCs (hybrid). A *public BC* is absolutely distributed and permissionless, which allows any entity (UAVs and GCS) can enter the BC network at any time. It needs some fixed processing charges in order to store data into the BC network. A *private BC* is partially distributed and completely permissioned BC, operated by a single organization, where each peer member is well known to the organization. Compared to the public BC, the private BCdoes not impose any transaction processing fee. Here, only those UAVs which are known to the organization can join the blockchain network. Finally, the *federated BC* is the hybrid of public and private BCs, where the control is not in the hands of a single organization (administer by group [44]). It is likely to have the same benefits as private BC. In this, UAVs from the different organization can communicate in a privatized way. Table 2 shows the characteristics of BC and its potential in UAV communication. Integration of BC in UAV network helps to prevent various cyber-attacks as follows.

5.1 | Fabrication

It is a kind of counterfeiting where any malicious user can access or append the new information by mimicking the original information. It can be a message forgery or a UAV spoofing attack. The immutability property and consensus mechanisms of BC prevent the data fabrication attack.

5.2 | Linking attack

In this kind of attack, a malicious UAV tries to link multiple transactions of different UAVs with the same key to know the IDs of the neighbouring UAVs.

5.3 | Eavesdropping attack

In this attack, a malicious UAV listens to the secret communication between the peer UAVs with the intention not to harm the network transmission. The BC technology offers transaction and identity security with cryptographic measures and digital signature algorithms.

5.4 | Distributed DoS attack

In this attack, malicious UAV sends junk or falsified data requests to the other UAVs with the intention to increase the network traffic and block the communication. BC is a full decentralized and distributes the same content to a large number of nodes, which makes it difficult for malicious UAVs to execute the attack.

5.5 | Jamming attack

It is an attack that generates a radio signal with the motive to disrupt the communication between the UAVs by increasing channel interference and noise. The SC concept in BC helps to prevent such attacks by allowing only relevant data entered into the BC network.

6 | BLOCKCHAIN-ENABLED UAV IN 6G COMMUNICATION: THE PROPOSED SCHEME

Figure 6 presents the proposed BC-based secure UAV network in the 6G environment underlying various applications such as surveillance, precision agriculture, law enforcement, live streaming, search and rescue, traffic monitoring, and many more. It delivers intelligence, flexibility, security, privacy, reliability, and efficiency to the UAV network communication, i.e. U2U, UAV-to-everything, and UAV-to-ground station. The proposed scheme is visionary and logically bifurcated into five divergent layers, such as (i) data sensing layer, (ii) communication layer, (iii) UAV layer, (iv) BC layer, and (v) application and control layer. All layers function jointly in order to achieve the security and privacy of UAV network communication. The detail description of each layer is as follows.

6.1 | Data sensing layer

In this layer, the physical entities or scenarios $\{S_1, \ldots S_n, \ldots S_N\} \in \mathcal{D}_{\mathcal{SL}}$ generates a huge amount of real-time heterogeneous data. The physical scenarios would be smart city (S_1), urban planning (S_2), road traffic (S_3), on-field gaming (S_4), agriculture (S_5), wildlife conservation (S_5), law enforcement (S_6), healthcare (S_6), satellite communication (S_7), and underwater communication (S_8). The data generated by (S_n) is in raw form and there is a need for secure and efficient processing in order to make real-time decisions. For example, S_1 generates real-time surveillance data, that helps to take quick action in case of any mishappening. A S_3 scenario generates traffic monitoring data to take preventive measures before get stuck into the traffic jam (helps to save time and cost). In S_6 scenario, wearable devices generates a person's health-related data, which helps to save them from any healthcare emergency. Likewise, other scenarios also generate real-time data for their respective applications. Table 5 shows the scenario wise type of data generated along with their purpose. This layer is passive, which only deals with the generation of an ample amount of data. The generated data is then stored into the IPFS off-chain distributed and immutable storage system and get a key (ξ) as an acknowledgement. A ξ allows access to the data from IPFS at any time. Then, the hash ($\mathcal{H}_D$) of data

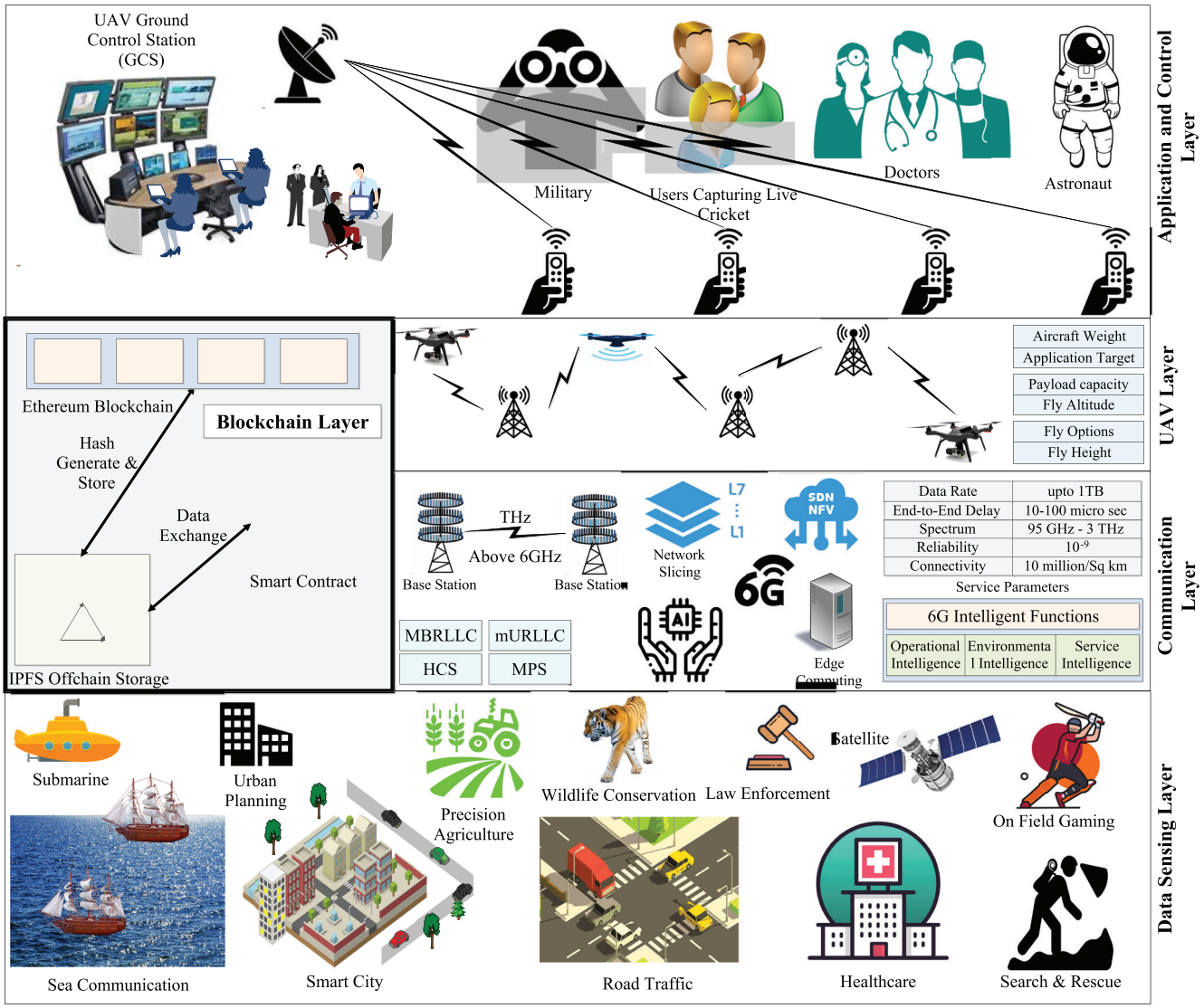

FIGURE 6 Blockchain-enabled secure UAV architecture in 6G environment [39, 40]

is calculated and stored into the BC $\mathcal{B}_{public}$. UAVs can access the data from BC for further processing and decisions taking. Figure shows the characteristics of the communication medium, i.e. 6G between the IPFS and the data sensing layer.

$$n, N > 0, \quad n < N, \tag{1}$$

$$S_n \neq NULL \ \& \ S_n \in \mathcal{D}_{S\mathcal{L}}, \tag{2}$$

$$\mathcal{H}_D \leftarrow hash\_function(\xi, data), \tag{3}$$

$$\zeta_{IPFS} \xrightarrow{Generates} \mathcal{H}_D \xrightarrow{Stores} \mathcal{B}_{public}, \tag{4}$$

where Equation (2) depicts that there exists at least one scenario that can generate the data and Equation (4) shows the IPFS generates the hash of data and stored it into the BC.

6.2 | The blockchain layer

It is a BC layer, which is cryptographically secure and shared ledger [45]. It stores the data captured from $\mathcal{D}_{S\mathcal{L}}$, U2U communication data, and $\mathcal{A}$ & $\mathcal{C}_{Layer}$ commands as a transaction into the chain of blocks. It is immutable and transparent in nature, which provides security to the data stored in the BC. It has the concept of the smart contract (SC) to maintain the trust and integrity between the participants across the BC. SC's are self-executable and self-enforceable, which eliminates the need for trusted third-party systems. Here, we consider the public BC ($\mathcal{B}_{public}$), i.e. Ethereum, where the ultimate goal is to create the world perfectly decentralized and the digital assets should be completely transferable and protected all times. It also has the concept of consensus mechanisms such as proof-of-work, proof-of-stake, delegated proof-of-stake, and proof-of-capacity where the participating

TABLE 4 Characteristics of BC and their potential in UAV communication

BC characteristics	Description	Potential applications in UAV communication
Decentralization	It is a decentralized ledger that is shared among all peers of the Ethereum BC network.	It overcomes the need of third-party systems to maintain trust in the UAV communication network and the cryptographic primitives are used to secure the UAV data in communication. It also solves the issue of single point failure, which ensures the availability of UAV communication network working in any application scenario.
Immutability	Immutability does not allow any kind of change in the transactional data once written in the chain of block.	In UAV communication, immutability restricts the participants or peers to modify the recorded critical data.
Transparency	The BC data is publicly available to all its peer nodes in order to maintain the integrity of data.	The UAV communication the data must be visible to all peers such as UAVs, ground station, and users, so that they can make real-time decisions appropriately.
Security and Privacy	BC stores the encrypted data, which is cryptographically secure and also uses access control mechanisms to provide data security and privacy.	BC ensures high security to the UAV communication network by distributing the same data in encrypted form among all the peers, so it would be difficult for a malevolent user to modify all such instances of the encrypted data.
Trust	The trust among the peer nodes in a BC network can be achieved using smart contracts and consensus mechanisms.	BC ensures the trust among the peer nodes for the data being captured from sensing layers.
Traceability	BC keeps the complete information about the transaction, which is unmodifiable. This helps to trace the transactions occurred before.	In UAV communication, the traceability is utmost important in identifying the malevolent nodes in the BC network

TABLE 5 Various UAV application scenarios with their purpose

Scenario	Type of data generated	Purpose
Smart City	City surveillance	To protect city from any kind of theft or mishappening
Road traffic	Traffic monitoring	To monitor and analyse the traffic conditions like traffic jam and accident
Precision agriculture	Crop and environmental monitoring	To monitor the crops and agricultural conditions for precision irrigation
Law enforcement	Criminal monitoring	To monitor and resist the criminals, weaponed, and unauthorized persons to perform malicious activity
Search and rescue	Searching and monitoring	To search the objects or people from unreachable extreme locations and helps to rescue it
Wildlife conservation	Wildlife animals and forest monitoring	Protection of wild animal species as per the Endangered Species Act
On-Field gaming	Streaming	Live streaming of sports to the remote locations
Healthcare	Health parameters monitoring	Monitor the healthcare parameters and send alert to nearby hospital to save human lives
Urban planning	Monitoring building structural information	Monitoring the construction sites and building structures for proper urban development and planning
Underwater communication	Monitors underwater activities	To monitor the under water acoustic communication, which helps Navy as a shark eye.

members are synchronized and agree upon the transaction as legitimate before stored into the BC (by matching the hash values of all the distributed copies of the data). The new block is added to the $\mathcal{B}_{public}$ only after the consensus mechanism is successfully executed.

BC technology scale-up the security and privacy of UAV communication, i.e. UAV-to-everything due to their fundamental characteristics such as decentralization, data immutability, data reliability, transparency, security, trust, and traceability. Table 4 shows the description of each characteristic and their realization in the UAV communication network. The data is stored into the $\mathcal{B}_{public}$ only if it satisfies all the conditions mentioned in the SC, otherwise discarded. Algorithm 1 shows the detailed procedure to whether the data to be stored or read from the BC or denied by the SC. Figure 7 depicts the sample SC, which is a set of software codes written in specified languages such as Java, C++, Kotlin, and Solidity. To store data in an Ethereum blockchain is quite costly and the storage cost calculation is shown in the box below.

Algorithm 1 BC Data Access Procedure by Different Entities

Input: $\mathcal{U}_k, \mathcal{D}_{\mathcal{SL}}, \mathcal{GCS}, \mathcal{B}_{public}$

Output: Data stored or accessed from $\mathcal{B}_{public}$ or denied.

procedure Data_Srore$\mathcal{U}_k, \mathcal{D}_{\mathcal{SL}}, \mathcal{GCS}$
  while (TRUE) **do**
    $\vartheta \leftarrow$ Data_Generated($\mathcal{D}_{\mathcal{SL}}$) ▷ ϑ is data generated at $\mathcal{D}_{\mathcal{SL}}$.
    if ($\vartheta \neq NULL$) **then**
      if (ϑ satisfies SC) **then**
        $\zeta_{IPFS} \leftarrow \vartheta$ ▷ Store generated data into IPFS.
        ζ_{IPFS} returns data access ξ.
        $\varsigma \leftarrow hash\_function(\xi, \vartheta)$ ▷ ς is the calculated hash value.
        $\mathcal{B}_{public} \leftarrow \varsigma$
      else
        SC denies the data entry.
      end if
    else
      No entry stored into the $\mathcal{B}_{public}$.
      Go To Line number 3
    end if
    if ($\mathcal{U}_k \in \mathcal{B}_{public}$) **then** ▷ $\mathcal{U}_k$ is the participating member of $\mathcal{B}_{public}$.
      $\mathcal{U}_k \leftarrow$ Read_Store_Data ($\mathcal{B}_{public}, \mathcal{D}_{\mathcal{SL}}$)
      $\mathcal{COM}_j \leftarrow$ Pass_Command ($\mathcal{GCS}, \mathcal{B}_{public}$)
      if ($\mathcal{COM}_j \neq NULL$) **then**
        Store $\mathcal{H}_D$ into $\mathcal{B}_{public}$.
      end if
    else
      SC denies the data entry.
    end if
  end while
end procedure

In Ethereum, 1 single word comprises of 256 bits and gas required to write it in Ethereum's SSTORE is 20K Gas, i.e. $\mathcal{G} = 20K$ [46].

$$1\ word = 20,000\ Gas. \tag{5}$$

To store 1 KB of data, the gas required is

$$1\ KB = \frac{2^{10}}{256} \times 20,000\ Gas \tag{6}$$

$$= \frac{2^{10}}{2^5} \times 20,000\ Gas \tag{7}$$

$$= 2^5 \times 20,000\ Gas. \tag{8}$$

The current gas price ($\mathcal{G}_{\text{price}}$) and the Ethereum prices ($\mathcal{E}_{\text{price}}$) are *23.186 gwei* [47] and *$232.96*, respectively. So, the cost to store η-words in Ethereum is as follows:

$$1\ ETH = 10^9\ gwei \tag{9}$$

$$ETH_{\eta-words} = \frac{\eta \times \mathcal{G}}{10^9}. \tag{10}$$

So, the cost to store η-words in USD is

$$USD_{\eta-words} = (\mathcal{G}_{price} \times ETH_{\eta-words}) \times \mathcal{E}_{price}. \tag{11}$$

```
pragma experimental ABIEncoderV2;
pragma solidity >=0.4.22 <0.6.0;

contract UAV_Communication {

Entity UAV, SensingDevices;

string public Data;

function UAV_Data_Exchange (string Data) {
        Statement1;
        Statement2;
        Statement3;
                .
                .
                .
        StatementN
}
}
```

FIGURE 7 Sample smart contract for UAV communication

To overcome such a high storage cost issue in Ethereum, an IPFS protocol is used in the proposed scheme, which is immutable, distributed, and free of cost data storage. It accelerates the data downloading speed with the hosting of data parts to other peers by exploiting minimum network bandwidth [48]. The data is stored into the IPFS and the $\mathcal{H}_D$ is generated, which then stored into the $\mathcal{B}_{public}$. The size of $\mathcal{H}_D$ is quite small than the actual data, so we can accommodate more number of transactions in Ethereum BC. For the same transaction, the IPFS generates the same hash value, which avoids the data redundancy issues. IPFS keeps the data in fixed block sizes, which are associated as generalized Merkle Tree.

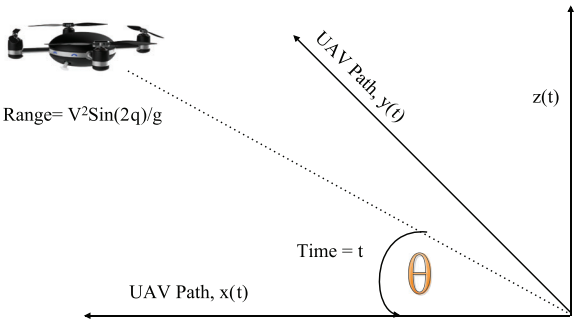

FIGURE 8 Projectile of UAV communication

6.3 | The UAV layer

In this layer, the physical UAVs are flying to sense the data from the $\mathcal{D}_{\mathcal{SL}}$. Data sensing is based on the application/scenario, i.e. $\{S_1, \ldots S_n, \ldots S_N\}$ for which UAV is deployed. Different sizes of UAVs are there for different application scenarios having different weights, payload capacity, fly altitude, and fly options. We are assuming that the UAVs are flying in a three-dimensional space having coordinates at time τ can be $[x(\tau), y(\tau), z(\tau)]$, where $x(\tau)$ and $y(\tau)$ are the coordinates parallel to ground and $z(\tau)$ is along the vertical height that UAV can fly [49, 50]. If the UAV is projected at angle θ from the ground with the initial speed of $\mathcal{V}$ at time τ is given by equations as follows and also shown in Figure 8:

$$x(\tau) \leftarrow \mathcal{V}(\tau)\text{Cos}(\theta(\tau)), \tag{12}$$

$$y(\tau) \leftarrow \mathcal{V}(\tau)\ \text{Sin}(\theta(\tau)), \tag{13}$$

$$z(\tau) \leftarrow \mathcal{U}(\tau) - gt^2/2. \tag{14}$$

The range $\mathcal{R}$ of UAV that it covers is specified as

$$\mathcal{R} = \frac{\mathcal{V}^2\text{Sin}(2\theta)}{g}, \tag{15}$$

where $\mathcal{R}$ is one of the factors in deciding UAV deployment in particular scenario. For example, in case of military application, the $\mathcal{R}$ should be high. UAVs can communicate and share data among other UAVs at the UAV layer over the $\mathcal{B}_{public}$ network, to make communication secure and reliable. A UAV can store data into the $\mathcal{B}_{public}$ only if it satisfies the SC rules and conditions. On the other hand, UAVs can sense the data from $\mathcal{D}_{\mathcal{SL}}$ also via $\mathcal{B}_{public}$ network to ensure data security and privacy. Each UAV has the copy of shared ledger as shown in Figure 9, which reduces the latency in accessing information stored in the ledger. UAV communicates with other UAVs and ground station over the 6G communication channel in order to reduce latency and increase reliability of the system.

6.4 | Application and control layer

It is the layer, where the organizations initiates the UAVs and operate it using the remote control. Organizations are application-specific such as military surveillance, healthcare monitoring, broadcast live streaming, and space data capturing. There is one ground station, which controls all UAVs by receiving commands from the respective organizations. All control commands are stored into the ζ_{IPFS} storage which in turn connected to the $\mathcal{B}_{public}$. Here, the role of $\mathcal{B}_{public}$ is to secure as well as track the UAV operation commands, so that organization cannot refuse it later in case of any mishappening.

6.5 | The communication layer

The communication system used to exchange the information between the UAVs, ground station, BC layer, and the $\mathcal{D}_{\mathcal{SL}}$ layer is 6G that offers an extremely wide spectrum and is perfectly suitable for latency-aware applications. Few of the characteristics of 6G communication channel are ultra-reliability (10^{-9}), massive ultra-low latency (<100 μs), high data rate (>1 TB), high spectrum efficiency (3–10× over 5G), and high connection density, that is, $10^7/\text{km}^2$. Table 3 shows the exhaustive list of 6G features in comparison to 5G. 6G allows softwarization, virtualization, and slicing of networks using software-defined networking (SDN) and network function virtualization (NFV). SDN is a softwarization technique that separates the data plane from the control plane to make the UAV network management easy and efficient. NFV logically virtualizes the network infrastructure such as computing, storage, and network hardware devices to make the UAV network cost-effective, efficient, and resilient.

As few UAV applications are critical application, where even a millisecond of delay is not tolerable. such applications would be military and healthcare applications. Higher the network latency, more chances of the unsuccessful operation. So, latency (ℓ) is a key parameter in UAV communication.

$$\ell = Time_{RT}(\mathcal{C}_{Wireless}). \tag{16}$$

Value of ℓ (*end-to-end delay*) varies from channel to channel, i.e. from LTE-A to 6G as specified below.

$$\ell_{LTE-A} \leq 20 \text{ ms}$$

$$\ell_{5G} \leq 5 \text{ ms}$$

$$\ell_{Beyond-5G} \leq 1 \text{ ms}$$

$$\ell_{6G} \leq 0.1 \text{ ms}.$$

7 | RESEARCH CHALLENGES AND FUTURE DIRECTIONS

UAVs with 6G are continuously evolving and deploying in the diversified application areas such as healthcare, military, precision agriculture, urban planning, sea communication, wildlife conservation, and search & rescue. The expeditious usage of UAVs in various smart applications, as mentioned above, leads to commercial and societal benefits. Although

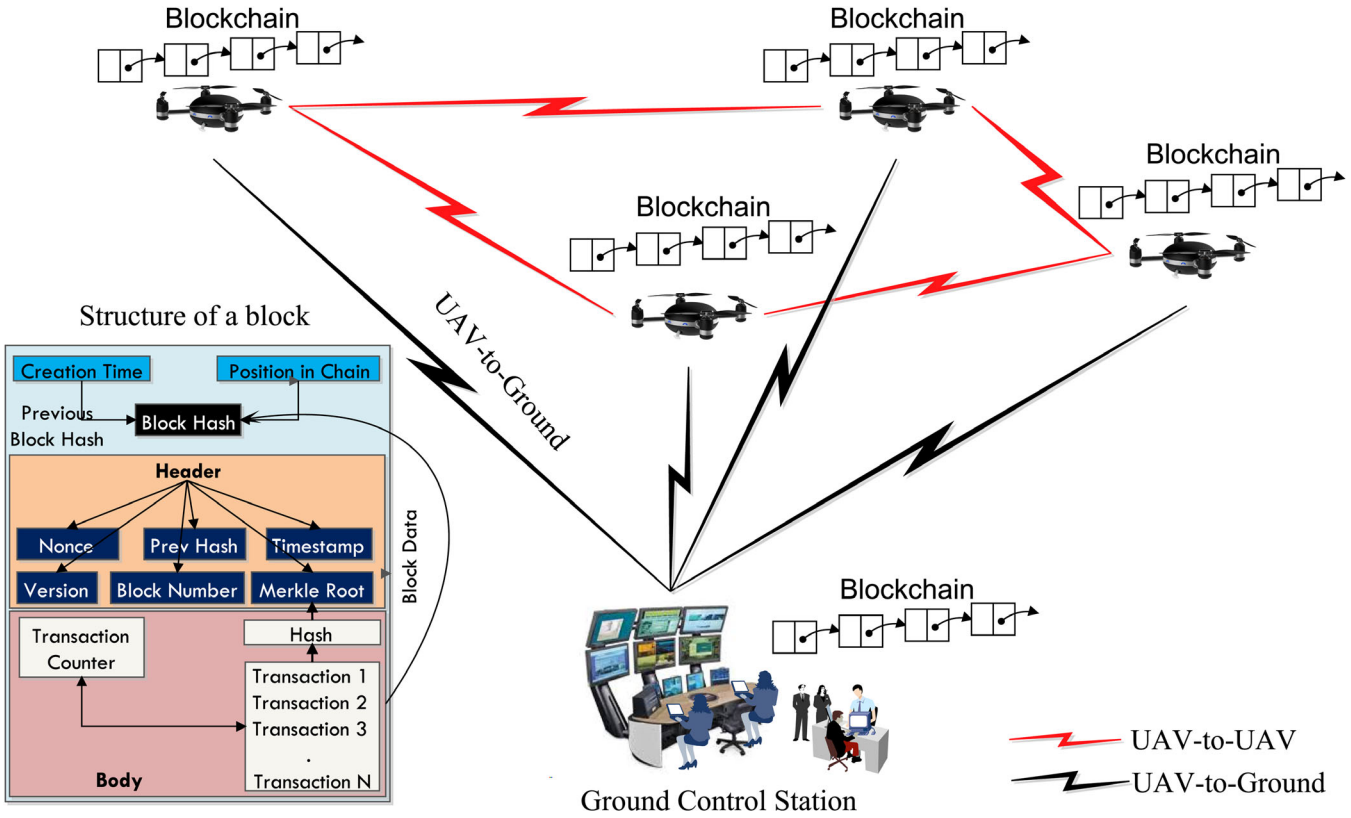

FIGURE 9 BC-based UAV communication scenario

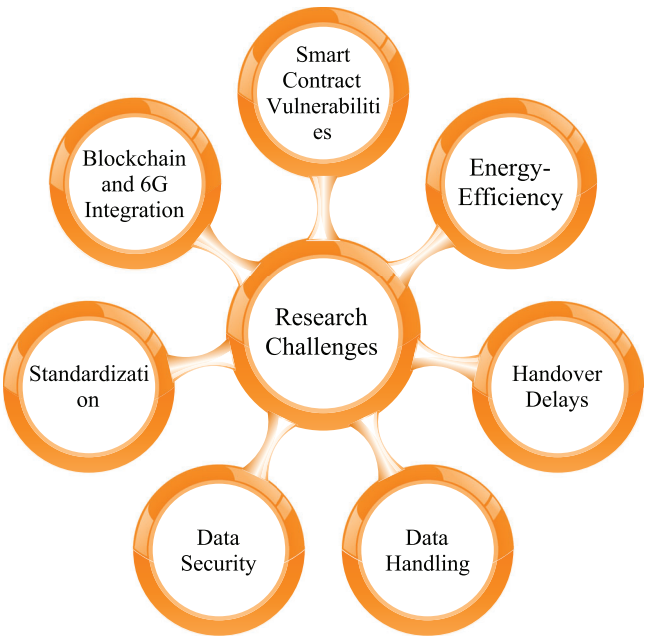

FIGURE 10 Research challenges in BC-based UAV communication

numerous benefits are there with the integration of 6G and BC with the UAV network, there still exists some challenges. Figure 10 shows the key research challenges of the proposed scheme and the description of these are as follows.

7.1 | Data handling

6G communication technology works with a high frequency of *95 GHz–3 THz*, the data rate of 1 Tbps (both uplink and downlink), and the bandwidth of 1 THz, which is quite faster compared to the existing 5G communication technology. This would generate a gigantic amount of data, which requires machine learning, deep learning, and big data analytics techniques to process it into usable information [51].

7.2 | Data security

The key concern in U2U and UAV-to-Ground communication is its data security. Machine learning and physical layer security techniques can be used to secure the UAV system from various cyber-attacks such as DoS, masquerade, spoofing, and eavesdropping attacks. But still, the data can be modifiable (using quantum attacks), which can lead to incorrect results. So, the proposed BC-based system can resolve such data security issues, but its real-time efficient deployment is still infancy [29].

7.3 | Standardization

The standardization and regulation of BC technology has not been completed yet by the renowned organizations such as IEEE and ITU. Thus, the integration of BC with the UAV network needs proper rules, guidance, and regulations in its

real-time deployment. So, this arises the need to frame technical standards with proper guidelines that make its deployment in UAV over 6G communication channel simple and efficient. Without the BC technology standardization, it is quite challenging to acquire BC in real-world 6G networks.

7.4 | Blockchain and 6G integration

The integration of BC, UAV, and 6G can face UAV deployment issues due to the lack of 6G communication infrastructure [52]. The existing network devices and BC infrastructure may not be suitable for 6G communication systems due to high spectrum efficiency, frequency, extremely high data rates, the throughput of 1 Tbps, and so on. First, complete existing infrastructure needs to be replaced with the 6G supporting infrastructure, then, the UAV deployment is feasible. This would be a great challenge in terms of capital and operational expenditures.

7.5 | SC vulnerabilities

SC's are the software codes written in specific programming languages such as solidity, kotlin, and java. It is used to create trust among the participating members of the $\mathcal{B}_{public}$ for trusted agreements without any involvement of any central entity, that may be susceptible to man-in-the-middle, eavesdropping, and spoofing attacks. So, there is a need for proper testing solutions and security verification of SC vulnerabilities before deploying it into the $\mathcal{B}_{public}$ network.

7.6 | Energy efficiency

UAVs are power constrained flying devices with limited processing capabilities, storage capacity, and processing times. BC and 6G-based UAV network requires more processing capabilities to execute SC and consensus mechanisms on UAVs, which can create a bottleneck in computation power. So, there is a need for optimization of the UAV network and operations to reduce the bottleneck condition.

7.7 | Handover delays

Few applications such as surveillance need long-range communication and need connectivity with intermediate infrastructure, which requires handover techniques. In the BC-based proposed system, all communication is through $\mathcal{B}_{public}$, which can be little-bit delayed due to the execution of consensus mechanism [28].

8 | CONCLUSION

UAVs play a protuberant role in commercial usage, complicated safety-critical missions along with many other diverse ranges of applications. UAV should be able to provide wide coverage and connectivity to the inaccessible areas under all circumstances. It possesses many characteristics with the integration of 6G technology such as high data rate, low latency, and wide range of coverage. Also, BC technology can secure confidential information gathered by the UAVs to prevent unauthorized access from attackers. This paper presented a discussion and comparison of state-of-the-art solutions. Various security concerns in UAV and their integration with 6G and BC are discussed. This paper presented a BC-based secure UAV network in a 6G environment. BC data storage cost is minimized by means of integration of IPFS with the BC network. Also, we have listed various research challenges that the proposed scheme may face during its real-time deployment. In the future, a game-theoretic approach can be used to manage the resources efficiently without any biases.

ACKNOWLEDGEMENT

This publication is an outcome of the R & D work supported by Visvesvaraya PhD Scheme of Ministry of Electronics & Information Technology (MeitY), Govt. of India, being implemented by Digital India Corporation <MEITY-PHD-2828>.

ORCID

Sudeep Tanwar https://orcid.org/0000-0002-1776-4651
Neeraj Kumar https://orcid.org/0000-0002-3020-3947

REFERENCES

1. Zeng, Y., Zhang, R., Lim, T.J.: Wireless communications with unmanned aerial vehicles: Opportunities and challenges. IEEE Commun. Mag. 54(5), 36–42 (2016)
2. U.V. University: Applications of UAVs. https://www.uxvuniversity.com/wp-content/uploads/2014/05/comads.png (2014)
3. Price, H.: Federal Aviation Administration (FAA) forecast fiscal years 2017–2038. https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=22594. Accessed 25 Oct 2019
4. MarketsandMarkets: Unmanned aerial vehicle (UAV) market. https://www.marketsandmarkets.com/Market-Reports/unmanned-aerial-vehicles-uav-market-662.html (2020)
5. Schiffman, R.: Drones flying high as new tool for field biologists. Science 344(6183), 459–459 (2014)
6. Gupta, L., Jain, R., Vaszkun, G.: Survey of important issues in UAV communication networks. IEEE Commun. Surv. Tutorials 18(2), 1123–1152 (2016)
7. Shakhatreh, H., et al.: Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges. IEEE Access 7, 48572–48634 (2019)
8. Dey, V., et al.: Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study. In: 31st International Conference on VLSI Design and 17th International Conference on Embedded Systems (VLSID), pp. 398–403 (2018)
9. Ferrer, E.C.: The blockchain: A new framework for robotic swarm systems. CoRR abs/1608.00695 (2016)
10. García-Magariño, I., et al.: Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain. Ad Hoc Networks 86, 72–82 (2019)
11. Zhang, Y., et al.: Smart contract-based access control for the internet of things. IEEE Internet Things J. 6(2), 1594–1605 (2019)
12. Gupta, R., et al.: Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges. IEEE Access 8, 24746–24772 (2020)
13. Gupta, R., Kumari, A., Tanwar, S.: A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles. Trans. Emerging Telecommun. Technol. e4009 (2020)

14. Islam, A., Shin, S.Y.: BUS: A blockchain-enabled data acquisition scheme with the assistance of UAV swarm in internet of things. IEEE Access 7, 103231–103249 (2019)
15. Ferrag, M.A., et al.: A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in internet of things. Comput. Electr. Eng. 84, 106627 (2020)
16. Andrews, J.G., et al.: What will 5G be? IEEE J. Sel. Areas Commun. 32(6), 1065–1082 (2014)
17. Khan, F.: LTE for 4G Mobile Broadband: Air Interface Technologies and Performance. Cambridge University Press, Cambridge, UK (2009)
18. International Telecommunications Union (ITU): IMT traffic estimates for the years 2020 to 2030. https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2370-2015-PDF-E.pdf (2015)
19. Zhang, S., Zhang, H., Song, L.: Beyond D2D: Full dimension UAV-to-Everything communications in 6G. IEEE Trans. Veh. Technol. 69(6), 6592–6602 (2020)
20. Na, Z., et al.: UAV-supported clustered NOMA for 6G-enabled internet of things: Trajectory planning and resource allocation. IEEE Internet Things J. 1–1 (2020)
21. Nguyen, T., et al.: Privacy-aware blockchain innovation for 6G: Challenges and opportunities. In: 2nd 6G Wireless Summit (6G SUMMIT), pp. 1–5 (2020)
22. Jensen, I.J., Selvaraj, D.F., Ranganathan, P.: Blockchain technology for networked swarms of unmanned aerial vehicles (UAVs). In: IEEE 20th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1–7 (2019)
23. Rana, T., et al.: An intelligent approach for UAV and drone privacy security using blockchain methodology. In: 9th International Conference on Cloud Computing, Data Science Engineering (Confluence), pp. 162–167 (2019)
24. Mozaffari, M., et al.: A tutorial on UAVs for wireless networks: Applications, challenges, and open problems. IEEE Commun. Surv. Tutorials 21(3), 2334–2360 (2019)
25. Koubâa, A., et al.: Dronemap planner: A service-oriented cloud-based management system for the internet-of-drones. Ad Hoc Networks 86, 46–62 (2019)
26. Islam, A., Shin, S.Y.: BUAV: A blockchain based secure UAV-assisted data acquisition scheme in internet of things. J. Commun. Networks 21(5), 491–502 (2019)
27. Chamola, V., et al.: A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact. IEEE Access 8, 90225–90265 (2020)
28. Hentati, A.I., Fourati, L.C.: Comprehensive survey of UAVs communication networks. Comput. Stand. Interfaces 72, 103451 (2020)
29. Alladi, T., et al.: Applications of blockchain in unmanned aerial vehicles: A review. Veh. Commun. 23, 100249 (2020)
30. Mehta, P., Gupta, R., Tanwar, S.: Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. Comput. Commun. 151, 518–538 (2020)
31. Gupta, R., et al.: Blockchain-envisioned softwarized multi-swarming UAVs to tackle COVID-19 situations. IEEE Network 1–8 (2020)
32. Gupta, R., et al.: VAHAK: A blockchain-based outdoor delivery scheme using UAV for Healthcare 4.0 services. In: IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 255–260 (2020)
33. Fotouhi, A., et al.: Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. IEEE Commun. Surv. Tutorials 21(4), 3417–3442 (2019)
34. Tariq Faisal, et al.: A Speculative Study on 6G. IEEE Wireless Communications 27, (4), 118–125 (2020). http://doi.org/10.1109/mwc.001.1900488
35. Manesh, M.R., Kaabouch, N.: Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. Comput. Secur. 85, 386–401 (2019)
36. Krishna, C.G.L., Murphy, R.R.: A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In: IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), pp. 194–199 (2017)
37. Madan, B.B., Banik, M., Bein, D.: Securing unmanned autonomous systems from cyber threats. J. Def. Model. Simul. 16(2), 119–136 (2019)
38. Sheth, K., et al.: A taxonomy of ai techniques for 6G communication networks. Comput. Commun. 161, 279–303 (2020)
39. 5G vs 6G | Difference between 5G and 6G. https://www.rfwireless-world.com/Terminology/Difference-between-5G-and-6G.html (2020)
40. Saad, W., Bennis, M., Chen, M.: A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. IEEE Network 34(3), 134–142 (2020)
41. Gupta, R., et al.: Tactile internet and its applications in 5G era: A comprehensive review. Int. J. Commun. Syst. 32(14), e3981 (2019)
42. Gupta, R., et al.: Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. Comput. Electr. Eng. 86, 106717 (2020)
43. Kumari, A., et al.: A taxonomy of blockchain-enabled softwarization for secure UAV network. Comput. Commun. 161, 304–323 (2020)
44. Kumari, A., et al.: When blockchain meets smart grid: Secure energy trading in demand response management. IEEE Network 1–7 (2020)
45. Kasireddy, P.: How does Ethereum work, anyway? https://www.preethikasireddy.com/post/how-does-ethereum-work-anyway (2017)
46. Wood, G.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper 151, 1–32 (2014)
47. Ethereum Statistics: https://ethstats.net/ (2020)
48. Rajalakshmi, A., et al.: A blockchain and IPFS based framework for secure research record keeping. Int. J. Pure Appl. Math. 119, 1437–1442 (2018)
49. Savkin, A.V., Huang, H., Ni, W.: Securing UAV communication in the presence of stationary or mobile eavesdroppers via online 3D trajectory planning. IEEE Wireless Commun. Lett. 9(8), 1211–1215 (2020)
50. Projectiles: https://colalg.math.csusb.edu/⟨devel/IT/main/m10_parametric/src/s03_projectile.html (2017)
51. Christensen, G.: What is sixth generation wireless? https://www.isemag.com/2019/09/telecom-6g-network-deployment-operations/#prettyPhoto (2019)
52. Nguyen, D.C., et al.: Blockchain for 5G and beyond networks: A state of the art survey. J. Netw. Comput. Appl. 166, 102693 (2020)

How to cite this article: Gupta R, Nair A, Tanwar S, Kumar N. Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges. *IET Commun.* 2021;1–16. https://doi.org/10.1049/cmu2.12113