Arabian Journal for Science and Engineering (2023) 48:1053–1074
https://doi.org/10.1007/s13369-022-07380-6

REVIEW ARTICLE-COMPUTER ENGINEERING AND COMPUTER SCIENCE

A Systematic Literature Review of Blockchain Technology for Internet of Drones Security

Yasmine Harbi[1] · Khedidja Medani[2] · Chirihane Gherbi[1] · Oussama Senouci[3] · Zibouda Aliouat[1] · Saad Harous[4]

Received: 28 April 2022 / Accepted: 3 October 2022 / Published online: 31 October 2022

Abstract

Internet of Drones (IoD) plays a crucial role in the future Internet of Things due to its important features such as low cost, high flexibility, and mobility. The number of IoD applications is drastically increasing from military to civilian fields. Nevertheless, drones are resource-constrained and highly vulnerable to several security threats and attacks. The use of blockchain technology for securing IoD networks has gained growing attention. To this end, this paper presents a systematic literature review to analyze the current research area regarding the security of IoD environments using the emerging blockchain technology. Forty relevant studies were selected from 129 published articles to answer the identified research questions. The selected studies were classified into three main classes based on blockchain type. Furthermore, a comparison of the reviewed articles in terms of different factors is provided. The research findings show that the blockchain can guarantee fundamental security requirements such as authentication, privacy-preserving, confidentiality, integrity, and access control. Finally, open issues and challenges related to the combination of blockchain and IoD technologies are discussed.

Keywords Internet of Things · Unmanned aerial vehicle · IoD · UAV · FANET · SLR

1 Introduction

The recent advancement in robotics and wireless communication has led to the emergence of Unmanned Aerial Vehicle (UAV) technology. A UAV, commonly known as *drone*, is an aircraft without a human pilot controlled by a remote user or control station [1]. Mostly, drones have been used for military applications where they are deployed for tracking insurgents, surveilling terrorists, or rescuing injured fighters [2].

Recently, the Federal Aviation Administration (FAA) of the United States of America (USA) has defined new regulations allowing the usage of UAVs for civilian and commercial purposes. As a result, the FAA expects that 7 million drones are currently flying in the USA [3].

Typically, drones are equipped with a Global Position System (GPS) and sensors for data collection and have limited storage and battery capacities [4]. The communication between drones and other entities such as the remote user or control station is based on wireless channels resulting in the Internet of Drones network.

Internet of Drones (IoD) is a class of Internet of Things (IoT) that enables communication and coordination of drones. Hence, it inherits the security weaknesses of IoT networks. Malicious adversaries can easily access the drone

✉ Saad Harous
harous@sharjah.ac.ae

Yasmine Harbi
yasmine.harbi@univ-setif.dz

Khedidja Medani
k.medani@univ-setif2.dz

Chirihane Gherbi
chirihane.gherbi@univ-setif.dz

Oussama Senouci
oussama.senouci@univ-bba.dz

Zibouda Aliouat
zaliouat@univ-setif.dz

1 LRSD Laboratory, Ferhat Abbas University of Setif1, Sétif, Algeria

2 Faculty of Literature and Languages, Mouhamed Lamine Debaghine University of Setif2, Sétif, Algeria

3 Computer Science Department, Mohamed El-Bachir El-Ibrahimi University, El Anceur, BBA, Algeria

4 College of Computing and Informatics, University of Sharjah, Sharjah, UAE

memory to get the stored data, compromise the physical components, or exploit the attacked drone for criminal uses. Therefore, it is highly required to explore the issues and vulnerabilities that affect the security of IoD environments [5,6].

According to [7], several emerging technologies and techniques can be adopted to enhance IoT security. Specifically, blockchain technology can mitigate potential security threats (*e.g.,* tampering and eavesdropping) due to its significant characteristics such as decentralization, immutability, and transparency.

1.1 Related Reviews

Many recent review studies addressed the security issues and challenges that face IoD networks. Wazid et al. [8] focused on authentication protocols for IoD environments. They discussed security requirements and challenges that need to be addressed to secure IoD communications. They provided a network model for remote user authentication where drones are deployed in different zones. Mutual authentication is needed between the remote user and the drone in order to access the real-time data of drones. The authors also presented two threat models that can be considered in IoD environments and introduced four authentication schemes [9–12]. They provided a comparison of these schemes in terms of communication overhead, computation overhead, and security features. However, they emphasized security solutions related to authentication and did not consider other fundamental security requirements.

Sun et al. [13] discussed the physical layer security of UAV systems, and they classified the security attacks into two classes, namely, passive eavesdropping and active eavesdropping. Subsequently, they introduced several techniques, including joint design, resource allocation, trajectory design, and artificial noise to resist eavesdropping attacks. They also presented emerging 5G technologies such as non-orthogonal multiple access (NOMA), 2D/3D beamforming, and millimeter-wave (mmWave) [14] to enhance UAV systems security. However, the authors did not provide a comparison of the presented techniques to highlight their benefits and limitations.

Alladi et al. [15] addressed the role of blockchain in UAV networks in various fields including the security of such systems. They focused on detecting and mitigating known attacks such as jamming, hijacking, and data tampering. In addition, they discussed the application of blockchain to secure UAV communications and data dissemination due to the hash function and public-key cryptography provided by the distributed ledger. The authors also presented major challenges that need to be addressed for efficiently securing UAV networks. However, few studies were introduced to show the role of blockchain in improving IoD security.

Yahuza et al. [16] explored the security issues of IoD networks. They reviewed existing architectures of IoD and proposed a secure architecture based on mobile edge computing (MEC) to provide efficient drone communications. They also suggested a classification of drones and highlighted the security vulnerabilities of each class. Moreover, they introduced a taxonomy of attacks, discussed the required countermeasures, and proposed solutions to mitigate the identified threats. However, they did not present security solutions based on blockchain technology.

Hassija et al. [17] analyzed the security issues including major attacks. They also presented the security vulnerabilities of different drone applications. In addition, the authors discussed the use of four emerging technologies, namely, blockchain, software-defined networking (SDN), machine learning, and fog computing to enhance the security of drone communications. However, they did not provide a comparison of the studied security solutions.

Table 1 illustrates a summary of related review studies on IoD security. The work presented in [8] and [13] identified the security attacks, requirements, and solutions for IoD environments. However, they did not investigate the use of blockchain technology. Other studies [15–17] introduced blockchain-based solutions to improve IoD security. However, they did not use the SLR methodology [18,19] to analyze the proposed solutions. Hence, the paper selection method is not clear. This work systematically explores the existing security solutions based on blockchain technology for IoD environments. It provides an in-depth analysis and systematic overview of blockchain-based IoD security.

1.2 Motivations and Contributions

None of the previous studies [8,13,15–17] used the SLR methodology to address the security of IoD. The SLR aims to formally and comprehensively identify, classify, and compare existing studies in this field. Therefore, this work intends to systematically analyze the application of blockchain technology for securing IoD networks. Forty relevant research articles published recently were selected using the SLR methodology, classified, and compared in terms of different parameters.

The main contributions of this work are the following:

- Proposing taxonomy of blockchain-based solutions for IoD security.
- Providing a comparison of the studied blockchain-based schemes.
- Highlighting open issues and challenges related to the integration of blockchain in IoD.

Table 1 Comparison of related work

Reference	Publication year	Main contributions	Systematic review	Blockchain	Taxonomy and comparison
Wazid et al. [8]	2018	Security requirements and challenges in IoD Authentication schemes for IoD environments	No	No	Yes
Sun et al. [13]	2019	Security attacks of UAV systems Security solutions for studied attacks	No	No	No
Alladi et al. [15]	2020	Applications of blockchain in UAV networks Security threats Challenges involved in each application	No	Yes	Yes
Yahuza et al. [16]	2021	Secure architecture for IoD networks Classification of drones Security attacks and mitigation techniques	No	Yes	Yes
Hassija et al. [17]	2021	Security vulnerabilities in drone applications Analysis of emerging technologies for security	No	Yes	No

1.3 Organization of the Paper

Figure 1 shows the organization of the present work. In Sect. 2, we briefly introduce IoD, blockchain technology, and IoD security. Section 3 defines the review steps using the SLR methodology. The selected articles are classified, analyzed, and compared in Sect. 4. The study results and open issues and challenges are discussed in Sect. 5. Finally, we conclude our study in Sect. 6.

2 Background

2.1 Internet of Drones

The IoD paradigm has recently attracted significant attention from both research and industry communities. It can be widely applied in different applications ranging from military to civilian and commercial domains; mostly owing to the advantages anticipated from the exploitation of the UAV's flexibility, mobility, and low-cost deployment [20].

The UAVs can fly over a large area in order to cooperatively gather data of interest or to accomplish different tasks. These UAVs are able to communicate with one another via temporary UAV-to-UAV links creating a flying ad hoc network (FANET) [21]. Furthermore, the UAVs communicate with control ground stations (CGS) using up/down links in order to send collected data or receive control information. The CGS is responsible for controlling the airspace and providing services to users remotely connected to dedicated servers [22].

Along with the integration of the UAVs/drones and the Internet of things (IoT), the IoD is described as a network architecture that enables communications between UAVs and a variety of entities deployed on the ground [22,23].

UAVs in IoD pave a way for diversified and increased applications, such as smart cities, industry, agriculture, healthcare, emergency situations, and environment surveillance.

- *Smart cities* the application scenarios of UAVs in smart cities aim to enhance the quality of human life in different fields, including road traffic and smart transportation systems [24], healthcare monitoring [25], smart home [26] and others.
- *Industry and agriculture* industry and agriculture use cases benefit from IoD innovation in real-time monitoring in order to provide automated water intervention [27], crop quality and quantity improvement [28], and efficient energy deployment in industrial smart grid [29]; while palliating the negative impacts on the environment and improving cost-effectiveness.
- *Emergency* one of the most relevant applications of UAVs involves natural disaster monitoring, such as forest-fire management [30], rescue missions [31], and finding missing persons [32]. In such emergency situations, IoD aims to provide efficient coverage in order to connect victims and injured people and to aid in the rapid solicitation of rescue teams.
- *Product delivery* owed to the high mobility of UAVs, the IoD boosts product delivery services for commercial and non-commercial uses with the benefits of reducing costs and delays [33].
- *Intelligent environment surveillance and monitoring* to support the activities of human operators, intelligent surveillance for real-time information acquisition from inaccessible areas via video streaming and images is exploited [34]. For instance, wildfire detection and pollution mitigation applications scenarios are involved

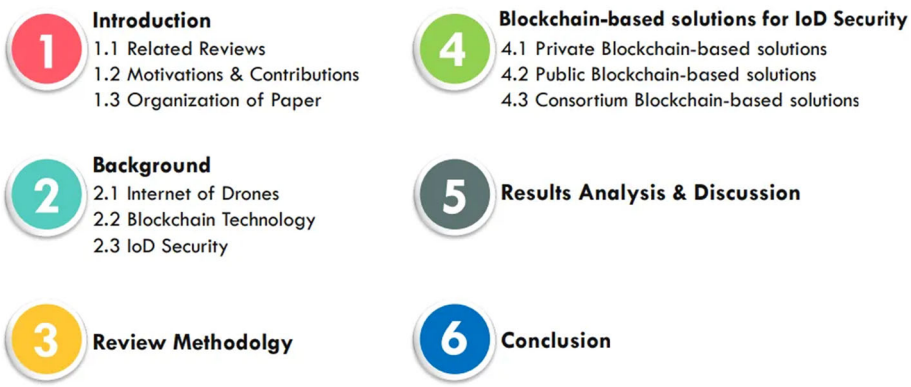

Fig. 1 Organization of the paper

in this context. In addition, several works investigate indoor/outdoor environment inspection which aims to track multiple static or mobile targets [35]. Recently, UAVs were included into wireless sensor networks (WSNs) to provide sensor nodes clustering and act as mobile base stations for data gathering. As consequence, the congestion problem in WSNs can be handled due to the flexibility of flying UAVs in the sensing areas [36].

However, due to the mobility and energy constraints of UAVs, the application scenarios design faces many challenges in terms of deployment, energy consumption, data transmission (communication), and security and privacy [5,20,37].

- *Deployment-related challenges* take into account the number of UAVs that should be deployed in order to cover the target area or to accomplish the planned task. Furthermore, UAVs' placement and mobility/trajectory motion have to be considered to mitigate interference and collision issues.
- *Energy-related challenges* energy consumption optimization remains one of the most interesting IoD challenges which is vital for data processing, storage, and transmission.
- *Communication-related challenges* due to UAVs' sparse density, data communication and routing solutions aim to increase the throughput and reduce latency and delays. This provides a high data rate related to large covered areas.
- *Security and privacy-related challenges* regarding the broadcast nature of the wireless medium, UAVs are vulnerable to various threats. The IoD solutions should ensure data security and privacy in different communication layers (i.e., physical, transportation, and application layers).

2.2 Blockchain Technology

Blockchain is a combination of technologies that have been around for a long time. It can be called a decentralized ledger to store transaction records on a network. Blocks are data structures that store lists of transactions. Peers create these transactions and exchange them in the blockchain network, causing the blockchain to change state [38]. In a distributed network, where no trust between peers exists, consensus protocols are established to agree on a single copy of the ledger.

Consensus is the process of agreeing on the final state of the data by untrusted nodes. To achieve consensus, different algorithms can be used. It is simple to provide a protocol between two nodes (for example, in a client–server system). However, reaching consensus becomes very difficult when multiple nodes participate in a distributed system and must agree on a value [39]. Some of the most frequently used consensus algorithms in the blockchain ledger are described next.

- Proof of work (PoW) is the most popular consensus mechanism used by common crypto-currency networks such as Bitcoin and Litecoin. The participants are required to demonstrate the work that they perform and submit qualifies for the right to add new transactions to the blockchain. PoW is the most mature and proven method; it has high cost and low transaction speed. It also prevents network participants from investing resources in alternative channels [38].
- Proof of stake (PoS) is a crypto-currency consensus mechanism used to process transactions and create new blocks in the blockchain. A consensus mechanism is a method of validating and securing database entries in a distributed system. In the case of crypto-currencies, the database is called the blockchain, so the consensus mechanism protects the blockchain. Using the PoS mechanism, crypto-currency owners validate transactions on the blockchain based on the number of coins staked by validators. The PoS was created as an alternative to the

PoW, and it is considered more secure against cyberattacks [38].

- Practical Byzantine Fault Tolerance (PBFT) is a consensus algorithm designed to work efficiently in asynchronous systems. It is optimized to achieve low execution time. It is intended to solve many of the problems associated with already available Byzantine fault-tolerant solutions (i.e., protection against Byzantine failures). It has been implemented in several modern distributed computing systems, including some blockchain platforms. These blockchains often use a combination of PBFT and other consensus mechanisms [38].
  Unlike the PoW mechanism, the PBFT can achieve network consensus without the need for energy-intensive computation. Some PBFT systems use PoW to prevent Sybil attacks, but only after a defined number of blocks, not for every block. The PBFT requires collective decision-making by voting on records by signing messages. As a result, every node in the PBFT system will be incentivized.
- There are other consensus algorithms such as Delegated Proof of Stake (DPoS), Directed Acyclic Graph (DAG), Delegated Byzantine Fault Tolerance (DBFT), and so on, that can be used by blockchain networks. The reader can refer to [40] for more details.

All types of blockchains can be described as permissionless, permissioned, or both. Any user can join a network with permissionless blockchain. Conversely, permissioned blockchains restrict the network access to specific nodes and potentially the authority of those nodes over the network. There are three types of blockchain structures:

- A public blockchain is inherently permissionless, allowing anyone to join, and is completely decentralized. All nodes in public blockchains have equal access to the ledger, the ability to create new transactions and validate the blocks. Public blockchains have been used primarily for trading and mining crypto-currencies.
- Private blockchain, also known as trust blockchain, is an authorized blockchain controlled by a single organization. A central authority decides whether nodes become participants in a private blockchain. The central authority does not necessarily give every node the same rights to perform the functions. Because public access to private blockchains is restricted, they are partially decentralized.
- A consortium blockchain is an authorized blockchain managed by a group of organizations, not a single entity like a private blockchain. As a result, consortium blockchains enjoy a higher degree of decentralization than private blockchains, leading to a higher level of security. However, building blockchains is a complex process since it requires collaboration between different organizations, which poses trust challenges and security concerns.

2.3 IoD Security

The drone industry is growing rapidly, and the number of UAV-based applications is increasing. This growth is faced by several security attacks and requirements that need to be addressed to provide secure and safe drone applications. Because of their characteristics and deployment nature, drones are vulnerable to various types of attacks [41]. These attacks can be classified into three main classes: device-based attacks, network-based attacks, and software-based attacks [42].

- *Device-based attacks* aim to gain physical access to drone components such as memory to obtain confidential data or take control of the drone.
- *Network-based attacks* include man-in-the-middle, replay, eavesdropping, and modification attacks where an adversary can intercept and alter the transmitted data.
- *Software-based attacks* aim to exploit software vulnerabilities by injecting malicious data into drones and ground stations. They can be used to launch other attacks such as denial of service/distributed denial of service (DoS/DDoS) attacks.

To overcome the aforementioned attacks, it is required to ensure main security attributes, namely, confidentiality, integrity, availability, authentication, and privacy-preserving [43].

- *Confidentiality* protects communication from unauthorized access and prevents the risk of data leakage.
- *Integrity* guarantees the detection of modification or tampering of data during transmission.
- *Availability* maintains the access to resources or services provided to authorized drones/users.
- *Authentication* involves the verification of identity before data access or exchange.
- *Privacy-preserving* prevents malicious attackers from disclosing personal data without permission.

3 Review Methodology

This study investigates the use of blockchain technology to address the security of IoD networks by applying the SLR methodology. Figure 2 summarizes the present work steps. Our review methodology consists of five steps including review questions, data searching, initial selection, data filtering, and final selection.

First, we defined the following review questions (RQ):

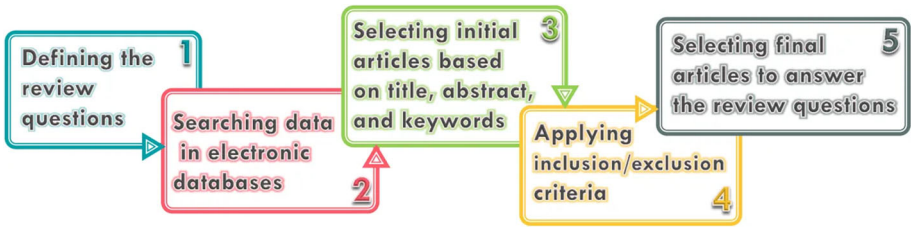

Fig. 2 Flowchart of the review methodology

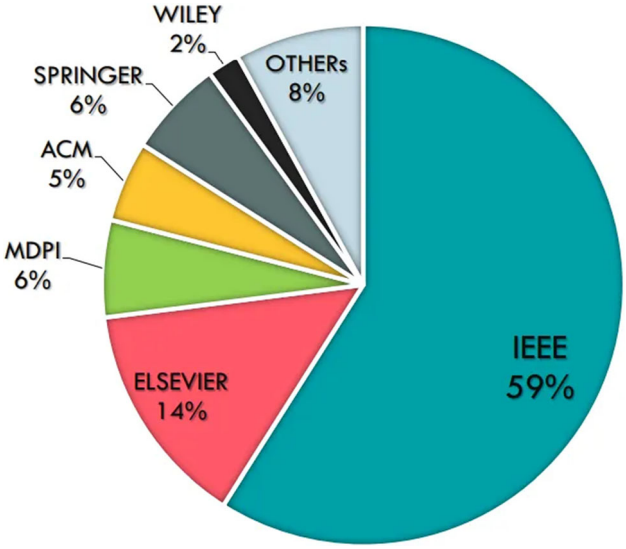

Fig. 3 Percentage of research studies by publisher

- *RQ1* Why is blockchain used in IoD?
- *RQ2* How can blockchain enhance the IoD security?
- *RQ3* What are the data contained in the blockchain?
- *RQ4* What are the strengths and weaknesses of using blockchain in IoD?
- *RQ5* What are the open issues related to the integration of blockchain and IoD?

Second, we selected the appropriate keywords for data searching through Google Scholar which is the most popular electronic database based on known scientific publishers such as IEEE, Elsevier, ACM, Springer, etc. We used the Boolean operation $< AND >$ to select the main searched keywords, including "Internet of Drones," "security," "blockchain," and "solution." We used the Boolean operation $< OR >$ to select synonyms and alternative spellings of the main keywords, such as: "IoD," "UAV," "scheme," "framework," or "approach."

We initially selected 129 research papers published during the last five years (from 2017 to 2021). Figure 3 shows the percentage of research studies by each considered publisher. It is observed that most of the research articles are published in three leading databases, namely IEEE, Elsevier, and Springer, with 59%, 14%, and 6%, respectively.

Table 2 Inclusion and exclusion criteria of our work

Inclusion criteria	Exclusion criteria
Articles published between 2017 and 2021	Articles not written in English
Articles published in journals/conference	Duplicated and non-available articles
Articles that address IoD security requirements	Articles not peer-reviewed
Articles that present UAV in the context of IoT	Articles that do not use the blockchain for IoD security

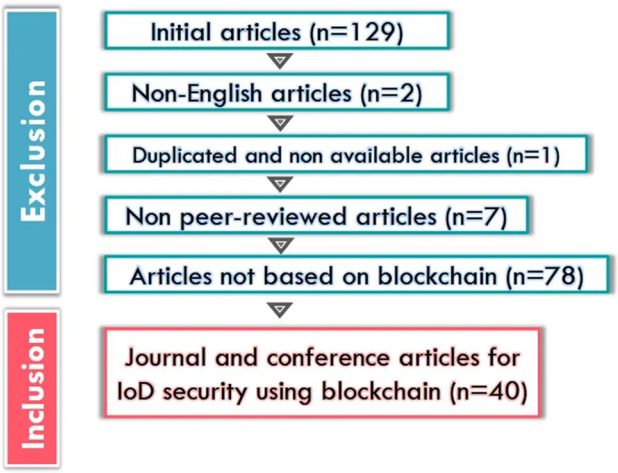

Fig. 4 Selection of final articles

After the initial selection of several published papers by analyzing the title, abstract, and keywords of each article, we applied the inclusion and exclusion criteria defined in Table 2. Figure 4 shows the selection of final studies based on the inclusion and exclusion principles. We initially selected 129 articles, then we exclude non-English, duplicated, non-peer-reviewed, and articles that investigate the security of IoD but are not based on blockchain.

Finally, 40 research articles were selected to answer the identified analytical questions of the systematic review.

4 Blockchain-Based Solutions for IoD Security

This section presents a description of the final selected articles according to the SLR methodology. We provide a

taxonomy of blockchain-based solutions that includes three classes: private blockchain solutions, public blockchain solutions, and consortium blockchain solutions. We note that papers that did not mention the type of the used blockchain are considered public blockchain solutions. Furthermore, the reviewed studies are compared in terms of different parameters including the system model, attack model, security model, consensus algorithm, targeted application, and advantages and limitations.

4.1 Private Blockchain-Based Solutions

Li et al. [44] defined a blockchain-based group key distribution solution for UAV networks. The UAVs are authenticated by the ground station (GS) to join or leave the network. The GS creates a private blockchain, generates the genesis block, and distributes the group keys. The blockchain contains join or leave transactions, group keys, and key recovery messages. Therefore, each UAV node can recover the group key from the distributed database.

Islam et al. [45] proposed a blockchain-protected data collection scheme. It uses a cluster of UAVs where data are collected from IoT devices and then transmitted to the server. Before the data collection process, the UAV swarm shares a public key with the IoT devices to maintain communication. However, before transmitting the data to the drone swarm, the IoT device encrypts them. Once the drone swarm receives the data, it uses a Bloom hash filter and a digital signature algorithm for two-step verifications to verify the sender. In addition, it encrypts the data before sending them to the nearest server. However, all validators must agree before data can be added to the blockchain. Finally, the usefulness of the proposed scheme is demonstrated by implementation and simulation. The security and performance findings reveal that UAVs help IoT devices in terms of connectivity and energy usage, as well as providing security against various attacks.

Singh et al. [46] investigated the use of blockchain technology to secure communication in drone-based delivery systems. The proposed system model includes different entities where the delivery transaction is executed based on a smart contract and stored in the blockchain. After the validation of the smart contract, a drone is used for the delivery of goods. The evaluation results demonstrated that the proposed scheme is effective in terms of gas consumption, transaction time, and mining time.

Bera et al. [47] introduced a novel blockchain-based secure system for data management among IoD communication entities. The introduced approach has the ability to tackle several known potential attacks. In order to validate the proposed scheme, a detailed comparative analysis is done in terms of security and functionality requirements. The proposed scheme provides better performance in terms of communication and computation overheads as compared to other related schemes.

In [48], the authors proposed a blockchain-based access control scheme for IoT-enabled IoD environments. A registration phase of UAVs and their associated ground station servers is enrolled by the central authority (CA). The CA ensures the authentication of the communicating entities. Two kinds of access control mechanisms for messages exchange using secret keys were provided; access control between drones and access control between drones and the ground station. In addition, a ripple protocol consensus algorithm (RPCA) is implemented by the GSS in order to add the transactions into blocks which are later added to the blockchain in the cloud server.

Hassija et al. [49] proposed a blockchain-based security framework for drones to set up base stations in a tactile Internet environment. These aerial base stations can be used in different situations catastrophic, public events, rural areas, etc. The proposed scheme dynamically allocates bandwidth to different users based on bandwidth availability and cost. The use of the blockchain provides a layer of security in internal communication between drones with limited resources. A basic smart contract was also deployed to make automatic network charging decisions and strategies.

The authors in [50] provided a secure communication framework based on blockchain for drone-assisted healthcare environments. The authors considered a private blockchain due to healthcare data sensitivity and confidentiality. They also adopted machine learning (ML) techniques for big data analytics. The combination of blockchain and ML allows powerful resistance against various types of attacks. A blockchain-based simulation is performed on the proposed framework to measure its impact on various performance parameters.

Ge et al. [51] proposed a distributed scheme using blockchain technology for securing UAV systems. They introduced a new secure, private, and lightweight blockchain architecture that reduces computation and storage costs while achieving privacy and security advantages. They also presented a new reputation-based consensus protocol to efficiently add blocks to the chain. The performance and security evaluations show that the blockchain-based distributed system is secure and efficient.

The authors in [52] proposed a new solution based on blockchain technology to deal with security issues in IoD. They adopted a lightweight architecture in order to reduce the computational, communication, and storage requirements of blockchain for the IoD ecosystem. The auto-shrinking mechanism was implemented to allow UAVs to hold only the hash of previously executed transactions. However, the ground station or aviation authority holds the complete ledger.

Gai et al. [53] designed a blockchain-enabled approach to secure data transmission in UAVs network (i.e., UAV-

to-UAV communication and UAV-to-Controller communication). They proposed an attribute-based algorithm to achieve authentication between UAVs. The transmitted data are validated based on attributes of the UAV and added to the blockchain.

Su et al. [54] designed a novel aerial-ground collaborative network architecture assisted by drones and blockchain in disaster areas. Moreover, they developed a credit-based consensus algorithm to track the behavior of nodes and record data transactions safely and consistently. A node does not have explicit knowledge of the entire network. However, reinforcement learning-based algorithms were used to optimize the planning of price and quality data sharing strategies for data providers and consumers. Simulation results prove that the proposed scheme effectively improves the security of the consensus phase.

In [55], a new blockchain-based security mechanism for cyber-physical systems was developed to enable secure data transfer between drones. The main contributions of this research are divided into three parts. First, a cyber-physical model for the IoD environment was presented, allowing for secure data transfer between drones via drone-to-drone (D2D) and D2X modes. Second, a blockchain-based security system was proposed, which includes registration, verification, and transaction phases. Finally, a deep learning-based technique was used for miner node selection.

Xu et al. [56] investigated the security and energy efficiency in blockchain-enabled data collection for UAV-assisted IoT systems. In this work, UAVs act as edge data collection nodes to provide long-term network access for IoT devices through regular cruises with recharging. The more the UAV forwards data and records transactions, the more it gets charging coins as rewards. Thus, malicious UAVs run out of their energy so soon. To resist the joining of malicious nodes, the UAVs exchange the charging time and establish the distributed ledger. An adaptive linear prediction algorithm implements an upload prediction model instead of original data to greatly reduce in-network transmissions. In addition, charging stations are deployed in the network to supply energy for the UAV.

Feng et al. [57] proposed an efficient and secure blockchain-enabled data sharing model for 5 G flying drones. To ensure the security of data sharing, blockchain and attribute-based encryption (ABE) were used. A smart contract is adopted for authentication and access control, public-key cryptography is applied to provide accounts and ensure account security, and a distributed ledger is used for audit security. In addition, an ABE model with parallel outsourced computing (ABEM-POC) is built to speed up outsourced computations and reduce electricity consumption. According to the findings of the experiments, parallel processing considerably enhances the speed of outsourced encryption and decryption when compared to serial computation.

Wazid et al. [58] proposed a robust blockchain-based scheme to secure communications in IoD environments. Their network layered architecture contains smart devices, drones, ground vehicles, cloud servers, a big data center, and users. These entities are initially registered to a trusted registration authority (RA). Each drone is attached to a ground vehicle and acts as an edge device that forwards data from smart devices. The ground vehicle receives the data from drones and creates a partial block. The consensus algorithm is performed by cloud servers to add a full block to the chain.

In [59], the authors proposed a new access control scheme to detect and mitigate unauthorized drones in IoD environments. Authentication of UAVs is performed by the ground station server (GSS). Then, the authenticated transaction data are stored in the private blockchain. Formal security analysis using the Real-Or-Random (ROR) model and Automated Validation of Internet Security Protocols and automatic application (AVISPA) tool was provided. The proposed scheme is robust against many potential attacks required in the IoD environment. A practical demonstration based on blockchain shows the effectiveness of the proposed scheme.

Irshad et al. [60] proposed an enhanced blockchain-enabled authenticated and key agreement scheme to authenticate UAVs. The proposed technique establishes a reliable access control system between UAVs and the ground station. It also ensures that all entities in the IoD environment can exchange transactions safely.

Perumalla et al. [61] designed a new technique for securing transmission in IoD environments using blockchain. Pre-deployment, registration, authentication, and access control are the four main processes. Besides, they developed an intrusion detection system for IoD using a deep neuro-fuzzy network.

Xiao et al. [62] introduced a novel blockchain-based secure crowd monitoring system using a UAV swarm. An encryption mechanism was applied to ensure and improve the security of each stage of the system. Furthermore, a drone swarm collaboration was provided to reliably complete monitoring tasks. A blockchain network was introduced to achieve tamper-proof of log recording and facilitate collective decision-making for monitoring transactions.

Kang et al. [63] proposed a decentralized data management system based on permissioned blockchain technology. The latter is deployed mainly in pre-selected ground base stations to ensure secure and efficient peer-to-peer data sharing in 5 G and beyond (B5G) drone environments. However, the ground base stations that serve as miners could be hacked, resulting in deliberately modified block verification. As a result, the authors developed a secure credit-based miner selection mechanism based on a four-weight subjective logic model. In comparison with previous schemes, performance findings reveal that the proposed scheme is more effective for

securing data exchange in permissioned blockchain-based B5G drone networks.

Table 3 presents a comprehensive comparison of private blockchain-based solutions that enhance the security of IoD networks.

4.2 Public Blockchain-Based Solutions

Aggarwal et al. [66] designed an efficient system to satisfy secure data dissemination in IoD using blockchain technology. In the proposed system, two types of nodes are distinguished: forger and normal nodes. The forger node is responsible for block creation, whereas normal nodes are used for verifying and validating the blockchain without any external authorities. A forger node selection algorithm that selects the forger node based on game theory is proposed. The validation results reveal that the blockchain security model has a high performance in terms of communication latency and cost.

Patel et al. [67] employed UAVs to enhance real-time user authentication and identity management. The user registers with one or more UAVs using biometric data then the user registration information is added to the blockchain. After the registration phase, each user should be authenticated based on a smart contract. The authentication transactions are also stored in the blockchain. The proposed framework has reduced latency compared to centralized systems, and it is robust against several attacks.

Masuduzzaman et al. [68] addressed the protection of data in UAV-assisted military applications. UAVs capture images from the battlefield then send them to the near edge server. The collected data are encrypted using symmetric cryptography before transmission. The edge server decrypts the received data, processes the captured image, and stores the data in the blockchain to ensure integrity and immutability.

Ch et al. [69] proposed a blockchain-based solution to monitor, manage, and control sensitive data captured by UAVs. Information about the authentication, integrity, and device reactions are stored in a cloud server. The authors used elliptic curve cryptography (ECC) and hash function to ensure privacy in data storage. To allow seamless transactions, the data are later stored in an Ethereum blockchain. The proposed solution provides data protection against stalkers, plaintext, and ciphertext attacks. The performance analysis showed reduced attack rates compared to existing non-blockchain approaches.

Li et al. [70] proposed a joint optimization framework to enhance both data computation cost and throughput of the blockchain system. UAVs can operate as flying mobile terminals and act as relay nodes in out-of-coverage areas. Mobile edge computing (MEC) servers were used to execute complicated computation tasks. Additionally, the authors adopted a dueling deep Q-network (DQN) to achieve maximum system rewards and increase the trustworthiness of the blockchain-based system.

Gupta et al. [71] presented a blockchain-based outdoor delivery scheme using UAVs for healthcare services, called VAHAK. In a decentralized way, the VAHAK allows reliable communication between UAVs and other healthcare entities. It guarantees that critical patients get the medical supplies they need. The Ethereum smart contract (ESC) has been used to overcome security, privacy, and reliability concerns in VAHAK, while the InterPlanetary File System (IPFS) protocol has been used to solve storage cost issues. The open-source tool MyThril was used to test the VAHAK's security vulnerabilities. The performance evaluation shows that the VAHAK solution outperforms the existing schemes in terms of scalability, latency, and network bandwidth.

Tan et al. [72] proposed a distributed key management scheme for heterogeneous drones using blockchain. They also suggested an efficient miner election method to enhance the time of mining process. To reduce the energy consumption of drones, the network architecture is organized into clusters. The head drone has high computation capabilities and is responsible for distributing the cluster key and generation of new blocks in the chain. It performs the mining process and maintains a copy of the blockchain. The member drone can update its asymmetric key pair in case of joining or leaving its cluster. The proposed consensus algorithm requires less time compared to PoW and PoS algorithms.

Cheema et al. [73] proposed a secure authentication scheme for drone-enabled smart vehicular networks. The proposed scheme involves the registration of smart vehicles, roadside units (RSUs), and drones using a smart contract. These entities are authenticated based on the registered information recorded on the blockchain. After successful authentication, the association of RSUs with drones is performed to provide energy-efficient communications.

Yazdinejad et al. [74] introduced a low-latency security authentication model for drones in smart cities. The authors applied a regional architecture to the drone network and used a custom decentralized consensus called DDPOS (Drone-based Delegated Proof of Stake). The proposed architecture is designed to have a positive impact on IoD security and reduce latency. They conducted an empirical analysis of the proposed architecture compared to other previously proposed peer-to-peer IoD models. The experimental results clearly show that compared to the peer-to-peer model, the proposed architecture not only has a low packet loss rate, high throughput, and low end-to-end delay but also can detect a high percentage of malicious attacks.

Lv et al. [75] adopted blockchain technology to guarantee the privacy of data generated by UAVs. The proposed scheme is based on a number theory research unit algorithm which includes key generation, encryption, and decryption processes.

Table 3 Comparison of private blockchain-based solutions

Reference	Publication year	System model	Threat model	Security model	Consensus algorithm	Blockchain data	Targeted application	Pros(+) and Cons(−)
[44]	2019	UAVs and GS	Eavesdropping, tampering, replay, and impersonation attacks	Authentication	Proposed consensus	Group key	Multi-fields	(+)Suitable for UAV dynamic topology (−)Storage cost is not considered
[45]	2019	UAVs and IoT devices	Not mentioned	Authentication, integrity, and privacy-preserving	Proof of authority (PoA)	Collected data	Disaster rescue	(+)Reducing energy consumption of IoT devices (−)Does not provide incentive for validator
[46]	2020	Buyer, seller, drones, cloud, and warehouse	Not mentioned	Integrity and authenticity	Not mentioned	Shipping details	Healthcare	(+)Ensures privacy of users (−)Does not support scalability
[47]	2020	Drones, GSS, RA, and control room	DY model [64] and CK model [65]	Authentication and integrity	PBFT	Shared data among drones	Multi-fields	(+)Acceptable level of security (−)Does not achieve anonymity and untraceability
[48]	2020	UAVs, GSS, CA, and cloud server	DY model and CK model	Authentication, confidentiality, and integrity	RPCA	Collected data	IoT applications	(+)Supports dynamic drone addition (−)Does not achieve drone anonymity
[49]	2020	Drones, users, and BS	Not mentioned	Authentication and availability	PoW	Network information	Tactile internet environments	(+)Secures inner-communications (−)Requires large amount of energy

Table 3 continued

Reference	Publication year	System model	Threat model	Security model	Consensus algorithm	Blockchain data	Targeted application	Pros(+) and Cons(−)
[50]	2020	Drones, patients, healthcare staffs, and GSS	DY model	Authentication, and privacy-preserving	PBFT	Exchanged messages	Healthcare	(+)Resists potential attacks (−)Does not support drone addition
[51]	2020	UAVs, GCS, and cloud server	GPS spoofing, sybil and DoS attacks	Confidentiality and availability	Proposed consensus	Exchanged messages	Multi-fields	(+)Lightweight consensus algorithm (−)Storage cost is not considered
[52]	2020	Drones, GS, and CA	Various types of IoD attacks	Confidentiality integrity, and authenticity	Proposed consensus	Drone information	Delivery service	(+)Robustness against known attacks (−)Storage cost is not considered
[53]	2021	UAVs, controller, and server	Compromised node attack	Authentication	Proposed consensus	Data transfer	Monitoring	(+)Effective for real-world applications (−)Distribution of private keys is not described
[54]	2020	UAVs, vehicles, and GS	Not mentioned	Privacy-preserving and availability	DPoS	Misbehavior of UAV	Disaster rescue	(+)Improving consensus efficiency (−)Does not secure data acquisition
[55]	2020	Physical, network, and computing plane	Not mentioned	Privacy-preserving and integrity	Proposed consensus	Drone information	Multi-fields	(+)Efficient miner selection (−)Storage cost is not considered

Table 3 continued

Reference	Publication year	System model	Threat model	Security model	Consensus algorithm	Blockchain data	Targeted application	Pros(+) and Cons(−)
[56]	2020	UAVs, IoT devices, and charging stations	Not mentioned	Confidentiality and integrity	Not mentioned	Tasks of drones	Data collection	(+)Low energy consumption (−)Key management is not investigated
[57]	2021	Drones, CA, user, and cloud server	Not mentioned	Authentication, and confidentiality	Not mentioned	Shared data	5G flying drones	(+)Provides parallel outsourced computations (−)Location privacy is not considered
[58]	2021	End, middle, and cloud layer	Eavesdropping, replay, modification, and session key attacks	Key management and authentication	PBFT	IoD data	Multi-fields	(+)Robustness against major attacks (−)Storage cost is not considered
[59]	2021	Drones, GS, and CA	DY model and CK model	Authentication and confidentiality	PBFT	Normal and abnormal data	Multi-fields	(+)Provides mutual authentication (−)Does not achieve anonymity and untraceability
[60]	2021	Drones, GS, and CA	DY model and CK model	Authentication and anonymity	PBFT	Collected data	Multi-fields	(+)Dynamic addition of drones (−)Storage cost is not considered
[61]	2021	Drones, GSS, CR, and cloud server	Neptune and smurf attacks	Access control and intrusion detection	Not mentioned	Not mentioned	Multi-fields	(+)Achieves low end-to-end delay (−)Energy consumption is not considered

Table 3 continued

Reference	Publication year	System model	Threat model	Security model	Consensus algorithm	Blockchain data	Targeted application	Pros(+) and Cons(−)
[62]	2021	Data, blockchain, and decision making layer	Double spend and fake chain attacks	Access control and availability	PBFT	Monitoring data	Crowd monitoring	(+)Supports group decision-making (−)Location privacy is not considered
[63]	2021	Drones and GSs	Block verification collusion attack	Integrity	PBFT or Raft	Shared data	B5G drone networks	(+)Provides secure miner selection (−)Computational cost is not considered

Khan et al. [76] presented intelligent processing of captured data by UAVs using blockchain and machine learning (ML) techniques. The proposed approach allows sharing of machine learning models through UAV participating nodes to improve the accuracy and precision of intelligent data analysis and preserve data privacy. Each UAV chooses its ML method, processes the dataset, and sends the results to the blockchain to achieve data integrity.

Allouch et al. [77] introduced a lightweight blockchain-based security solution. It is called Unmanned Traffic Management Chain (UTM-Chain) and uses hyperledger fabric for UTM of low-altitude UAVs. The UTM-Chain approach is suitable for UAVs that have limitations in terms of computational and storage resources. Furthermore, it ensures that the data traffic between UAVs and their ground control stations (GCSs) is secure and trustworthy. To validate the performance of the suggested approach in terms of transaction latency and resource use, the authors used the cAdvisor tool. Based on the examination of security factors, the proposed UTM-Chain is practical and expandable for the secure sharing of UTM.

Andola et al. [78] investigated the use of blockchain technology to handle security issues, namely authentication, in surveillance applications maintained by UAV networks. The proposed model considers a scenario where multiple tasks can be assigned to UAVs of different networks. The tasks' assignment will take place anonymously via an entity called an agency. The validation of transactions will be performed by ground control stations. The proposed model consists of four approaches to guarantee mutual authentication of a drone when it needs to cross the coverage area of flying zones. The first approach aims to provide perfect unlinkability between public keys of users in order to preserve node anonymity. The second approach aims to detect any adversary that attempts to modify a transaction or discard the modified transaction. The third approach allows tracking of the sender's identity by the receiver. In the fourth approach, a UAV can delegate its task of tracking transactions to the GS. The security of the proposed techniques is analyzed using the theorem-proof method.

Mitra et al. [79] proposed an access control scheme based on blockchain to secure wildlife monitoring systems. Drones are deployed in different flying zones to collect data of wild animals and send it to their associated GSS. The drones also are connected to IoT smart devices that are attached to animals to collect real-time data. The GSS receives the sensed data, creates the transactions, and constructs the blocks using the PBFT consensus algorithm. The authors evaluated the proposed scheme in terms of computation time for adding transactions into the block and adding blocks into the chain. Their scheme has an acceptable computational cost.

Table 4 presents a comprehensive comparison of public blockchain-based solutions that enhance the security of IoD networks.

4.3 Consortium Blockchain-Based Solutions

Islam et al. [80] proposed an approach to secure health data (HD) transmission using UAVs. The HD are collected from the wearable sensors of users and transmitted to the nearest MEC server. The user encrypts the HD before sending them to MEC to provide privacy preservation. The HD are diagnosed at MEC, and the MEC server notifies the user and the nearby hospitals if any anomalies are discovered in the user's health data. The HD are stored in blockchain with the permission of validators once the data processing is completed.

The authors in [81] introduced a new blockchain-based secure healthcare scheme in which HD are collected from users via UAVs. In the presented scheme, the UAV shares a generated key with body sensor hives (BSHs) to provide low-power secure communication. The UAV decrypts the encrypted HD using the shared key and performs a new two-phase authentication method. The HD are sent by the UAV to the nearest server, which securely stores tha data in the blockchain. To demonstrate the feasibility of the suggested secure healthcare scheme, a security study was performed. Implementation and simulation were used to validate the proposed scheme's performance. According to the security and performance analysis results, the proposed approach provides an improved cost for BSHs networks while retaining security.

Liao et al. [82] focused on securing the collaboration of multiple drones in smart city applications. They integrated blockchain and software-defined networking (SDN) technologies to ensure an efficient architecture. The proposed architecture consists of the application, control, and data plane where two types of drones, namely task drone and controller drone, were employed. The controller drones provide instructions to task drones and cooperate using smart contracts. The authors proposed a new consensus algorithm called proof-of-security-guarantee (PoSG) and a new cryptocurrency named Cooperation Coin to secure and motivate the collaboration of controller drones. The PoSG algorithm outperforms the traditional PoW algorithm in terms of security and performance.

In [83], the authors presented a blockchain-based pandemic surveillance scheme. It consists of a large number of drones that can autonomously monitor epidemics, thus, limiting human involvement as low as possible. The authors considered the STRIDE attack model (i.e., spoofing, tampering, repudiation, information disclosure, DoS, and elevation of privilege). A use case based on the current pandemic (i.e., COVID-19) was discussed. They used two types of drone swarms to manage multiple tasks. In addition, two-level lightweight security mechanisms were presented. The experimental results show the feasibility of the proposed scheme.

Feng et al. [84] proposed a decentralized framework based on blockchain technology and federated learning (FL) for 5 G-enabled UAVs. The FL is used to protect the privacy of datasets collected by drones. The drones are registered in the consortium blockchain and authenticated through the smart contract before participating in FL. In addition, the authors adopted homomorphic encryption to prevent data leakage and inference attacks. The proposed scheme avoids the single point of failure and guarantees data security and privacy.

Liu et al. [85] investigated the cross-domain authentication among drones. They proposed a decentralized approach based on consortium blockchain to provide secure and effective cooperation of drones from different domains. A mobile edge computing server (MEC) is deployed in each domain to maintain the consortium blockchain. Drones are registered and authenticated using a smart contract (SC). The authors also employed a key generation center (KGC) to achieve intra-domain authentication of drones. The performance of the proposed scheme is evaluated in terms of computational and communication overheads. The evaluation results showed the efficiency of the proposed scheme.

Table 5 presents a comprehensive comparison of consortium blockchain-based solutions that enhance the security of IoD networks.

5 Results Analysis and Discussion

In this section, we statistically analyze the results of SLR of using blockchain technology to enhance the security of IoD. Moreover, we respond to the analytical questions RQ1, RQ2, RQ3, RQ4, and RQ5.

- *RQ1* Why is blockchain used in IoD?
  The IoD paradigm is progressively used in diverse domains such as healthcare, industry 4.0, smart city, etc. This increasing number of UAV-based applications faces serious problems related to security issues and concerns. The recent emerging blockchain technology can be used to efficiently secure the IoD environments due to its prominent features and cryptographic properties. Figure 5 depicts the distribution per year of the reviewed studies that incorporate blockchain in IoD networks. It is obvious that the use of the distributed ledger increased in 2021 which means that blockchain-based IoD is attracting considerable interest and becoming a major research topic.
- *RQ2* How can blockchain enhance the IoD security?
  The characteristics of blockchain such as decentralization, immutability, and transparency make it a suitable solution to provide fundamental security require-

Table 4 Comparison of public blockchain-based solutions

Reference	Publication year	System model	Threat model	Security model	Consensus algorithm	Blockchain data	Targeted application	Pros(+) and Cons(−)
[66]	2019	IoD, infrastructure, and user layer	Spoofing, DoS, eavesdropping, man-in-the-middle, and tampering attacks	Authentication, authorization, accountability, anonymity, and integrity	PoS	Collected data	Data dissemination	(+)Removing central authority (−)Storage cost is not considered
[67]	2020	UAVs, GSS, and users	Impersonation, password guessing and DoS attacks	Authentication	Not mentioned	Users information	Digital identification	(+)Resilience against attacks (−)Storage cost is not considered
[68]	2020	UAVs, base station, edge and cloud servers	Not mentioned	Confidentiality and access control	PBFT	Image data	Military application	(+)Low delay and high precision (−)Key distribution is not described
[69]	2020	UAVs and cloud server	Stalkers, plaintext, and ciphertext attacks	Authentication, confidentiality, and integrity	PoW	Collected data	Vehicle monitoring	(+)Low latency and attack rate (−)High data response time
[70]	2020	Drones, BS, and IoT devices	Not mentioned	Integrity	PBFT	Collected data	M2M communications	(+)Enhances computation cost and throughput (−)Mutli-hop relay is not considered
[71]	2020	UAVs, hospital, warehouse, and patients	Not mentioned	Integrity	PoW	Delivery information	Healthcare	(+)Improves latency, scalability, and bandwidth (−)Does not support UAV location privacy

Table 4 continued

Reference	Publication year	System model	Threat model	Security model	Consensus algorithm	Blockchain data	Targeted application	Pros(+) and Cons(−)
[72]	2021	Members and head UAVs	Eavesdropping, tampering, replay, impersonation, and cloning attacks	Confidentiality	Proposed consensus	UAVs public keys and cluster ID	Industrial IoD	(+)Lightweight mining process (−)Detection of malicious UAV head
[73]	2021	Smart vehicles, drones, RSUs, and ground core network	Unauthorized access, malicious users, and DoS attack	Authentication	Not mentioned	System entities information	Smart transportation	(+)Avoiding single point of failure (−)Increasing blockchain size
[74]	2021	Drone-controllers and drones	Not mentioned	Authentication	DDPoS	Drone data	Smart city	(+)Low packet loss and high throughput (−)Drone speed is not considered
[75]	2021	User, data, and cloud layers	Tampering attack	Privacy-preserving	Not mentioned	Cloud operations	Multi-fields	(+)Privacy protection of drones data (−)Does not support user fault tolerance
[76]	2021	Monitor node and miner nodes	DoS and probing attacks	Privacy-preserving and integrity	Ranking algorithm	Detection model results	Decision-making system	(+)Decentralized attack detection (−)Authentication of UAVs is not considered
[77]	2021	Drones, GS, users, and cloud server	Physical and cyber attacks	Privacy-preserving, availability, and integrity	Not mentioned	Drone data	Traffic management	(+)Resilience against attacks (−)High storage cost for drones

Table 4 continued

Reference	Publication year	System model	Threat model	Security model	Consensus algorithm	Blockchain data	Targeted application	Pros(+) and Cons(−)
[78]	2021	UAVs, agency, and GCS	Malleability and DoS attacks	Unlinkability in ciphertext and unforgeability of signature	Proof of authorization	Tasks of drones	Surveillance system	(+)Provides drone identity privacy
								(−)Computation cost is not considered
[79]	2021	Drones, RA, GSS, and IoT devices	DY, CK models and power analysis attack	Access control and confidentiality	PBFT	UAVs information	Wildlife monitoring	(+)Effective computational time
								(−)Does not achieve anonymity

ments for IoD. Figure 6 shows the security requirements (i.e., authentication, privacy-preserving, confidentiality, integrity, and access control) that are achieved by the studied blockchain-based schemes. Authentication is the most investigated requirement with 19 articles. Seven of research papers focus on applying blockchain to achieve privacy-preserving/confidentiality. Integrity and access control are considered by four articles and five articles, respectively. According to Fig. 7, we observed that 50% of research papers used the private blockchain. Public blockchain and consortium blockchain are applied by 35% and 15% of the reviewed studies, respectively. Most of the schemes adopted the private blockchain network, where the consensus mechanism is performed by pre-selected nodes and the transactions are private. In contrast, all nodes can participate to reach a consensus and be rewarded in the public blockchain. Nevertheless, it is less efficient in terms of processing time due to the increased number of handling nodes in the network. Compared to both private and public blockchain networks, the nodes in the consortium blockchain decide who acts as miners and which transactions are public.

- *RQ3* What are the data contained in the blockchain?
  According to Tables 3, 4, and 5, most of the reviewed studies [46,52,55,71,74,77,79] store the drone data such as location, speed, zone, and amount of power as records in the involved blockchain. Other studies [45,48,60,62,66,69,70] add the collected data by drones in the distributed ledger, while in [54,58,59], the big data analytic is required to classify the collected data before the creation of the block. Some research articles [68,80,81,83] store personal data such as health and biometric data in the public/consortium blockchain. On the other hand, the exchanged and shared messages among drones and other entities in [47,50,51,53,57,63] are recorded in the decentralized blockchain. However, adding a large number of transactions on the blockchain is extremely costly and reduces the system efficiency. In addition, storing sensitive information and private data in the public ledger requires encryption/decryption mechanisms to provide data privacy protection. Therefore, there are several challenges with conventional blockchain that need to be addressed to make it suitable for IoD environments.
- *RQ4* What are the strengths and weaknesses of using blockchain in IoD?
  The blockchain is a promising technology that can potentially enhance IoD security. It can be effectively applied in various UAV-based applications by offering the following advantages: (a) it overcomes the single point of failure due to its decentralization property, (b) it provides security to the drone communication, (c) it allows the drone data to be transparently recorded and cannot be modified or changed, (d) it provides accountability and traceabil-

Table 5 Comparison of consortium blockchain-based solutions

Reference	Publication year	System model	Threat model	Security model	Consensus algorithm	Blockchain data	Targeted application	Pros(+) and Cons(−)
[80]	2019	UAVs, users, and MEC servers	Not mentioned	Confidentiality and integrity	Not mentioned	Health data	Healthcare	(+)Provides secure health data transmission (−)Increasing energy consumption of UAV
[81]	2020	UAVs, users, GCS, MEC and cloud servers	Man-in-the-middle, unauthorized access, tampering, and replay attacks	Authentication, confidentiality, and integrity	PoA	Health data	Healthcare	(+)Resilience against known attacks (−)Health data privacy is not considered
[82]	2021	Data, control, and application planes	Not mentioned	Privacy-preserving	Proposed consensus	Not mentioned	Smart city	(+)Efficient consensus and incentive mechanisms (−)High communication cost
[83]	2021	Drones and servers	STRIDE	Authentication	PoW	Biometric data and entity ID	Healthcare	(+)Lightweight authentication mechanism (−)Personal data privacy is not considered
[84]	2021	P2P, blockchain, and application layers	Not mentioned	Privacy-preserving, and authentication	PBFT	FL model updates and entities information	Industry 4.0	(+)Avoiding single point of failure (−)Storage cost is not considered
[85]	2021	Drones, KGC, and MEC server	Not mentioned	Authentication	Raft algorithm	System parameters	5G-enabled UAVs	(+)Dynamic identity management (−)Provides high latency

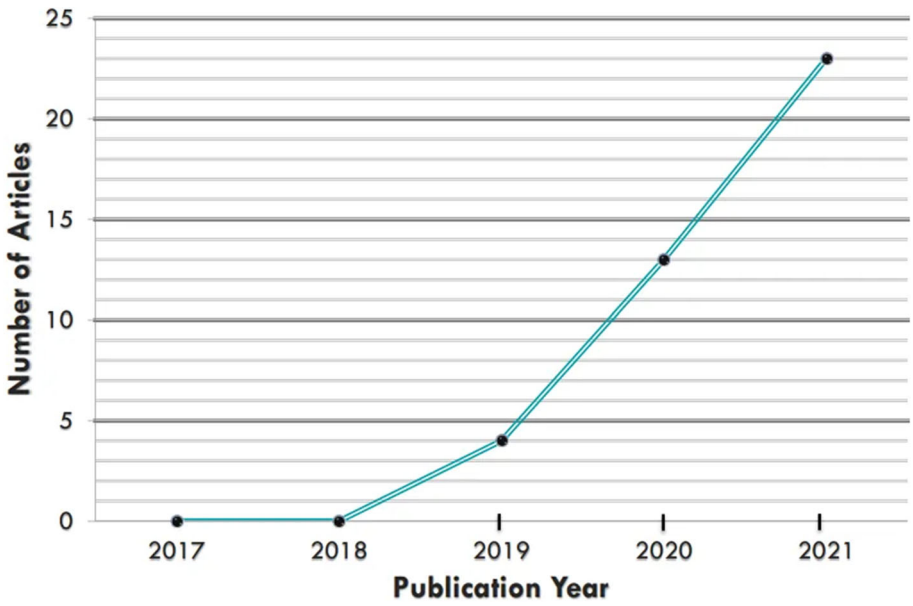

Fig. 5 Investigation of blockchain-based IoD per year

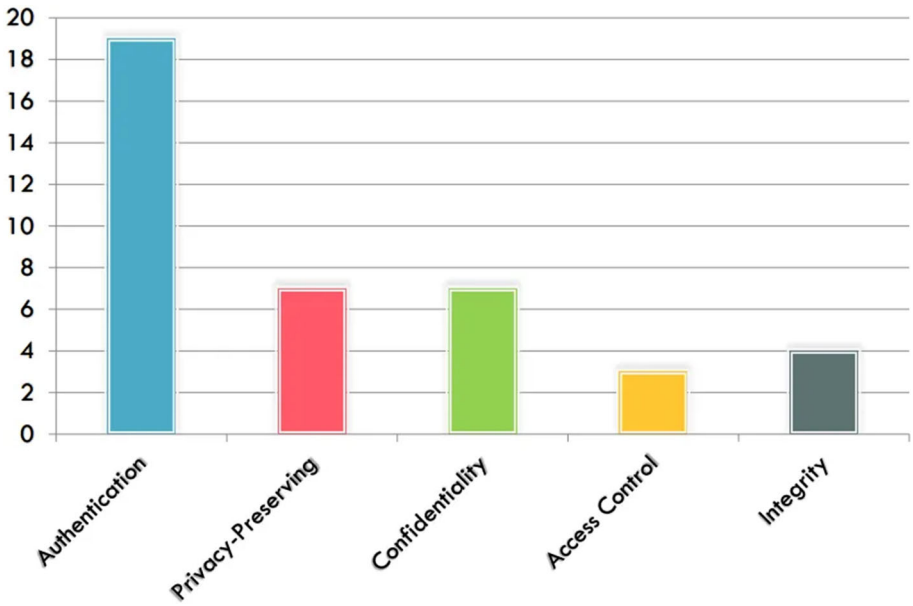

Fig. 6 Percentage of security requirements

ity. In addition, the blockchain can perfectly be combined with other common technologies such as edge computing, SDN, and machine learning. However, several weaknesses remain in the feasibility of blockchain-based IoD systems. Specifically, the blockchain is based on the distributed consensus mechanism which is vulnerable to 51% attack. This occurs when a single miner gains control of 50% of the blockchain computing power. An attacker can exploit this vulnerability to launch other attacks such as double-spending attack [39].

- *RQ5* What are the open issues related to the integration of blockchain and IoD?

Several issues and challenges arise to the combination of blockchain and IoD technologies due to the low cost and mobility of drones. PoW, PoS, and PBFT are the most common consensus algorithm used in the blockchain. However, these mechanisms do not take into consideration the resource limitations of UAVs such as storage and computing capacities. Therefore, the development of efficient consensus algorithms is one of the major challenges in blockchain-based IoD. In addition, drones are not able to store the blockchain that grows because of the large-scale IoD networks. Hence, the design of blockchain-specific infrastructures that store only recent transactions is suggested.

In 5 G-enabled UAV applications, the privacy of drone data can be threatened by malicious adversaries. Several cryp-

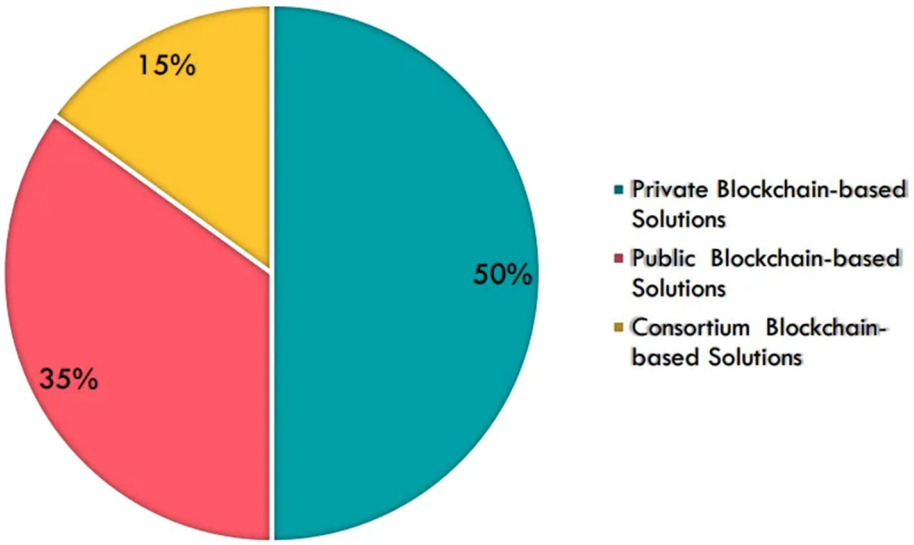

Fig. 7 Percentage of blockchain type

tographic techniques based on anonymization are proposed to carefully provide privacy-preserving for IoD applications. Some researchers tackle the physical layer security of drones to protect real-time data [40]. However, achieving a trade-off of efficiency and privacy is still a significant challenge in blockchain-based IoD.

6 Conclusion

This study presented a systematic literature review of security schemes in IoD environments using blockchain technology. Forty research articles were selected based on inclusion and exclusion criteria. The selected studies were classified into three classes: private blockchain-based schemes, public blockchain-based schemes, and consortium blockchain-based schemes. Additionally, a comprehensive comparison in terms of the system model, threat model, security model, consensus algorithm, targeted application, and advantages and limitations was provided. Finally, the study discussed open issues and challenges related to the incorporation of blockchain technology for securing the IoD networks.

This paper can help interested researchers to have an up-to-date review of the application of blockchain for IoD security and investigate the highlighted issues and challenges.

References

1. Kang, J.H.; Park, K.J.; Kim, H.: in: 2015 International conference on information and communication technology convergence (ICTC) (IEEE, 2015), pp. 533–538
2. Cook, K.L.: in: 2007 IEEE aerospace conference, (IEEE, 2007), pp. 1–7
3. Atherton, K.D.: The FAA says there will be 7 million drones flying over America by 2020. Pop. Sci. (2016)
4. Mitka, E.; Mouroutsos, S.G.: Classification of drones. Amer. J. Eng. Res **6**, 36–41 (2017)
5. Abdelmaboud, A.: The Internet of Drones: requirements, taxonomy, recent advances, and challenges of research trends. Sensors **21**(17), 5718 (2021)
6. Nguyen, H.P.D.; Nguyen, D.D.: Drone application in smart cities: the general overview of security vulnerabilities and countermeasures for data communication. Dev. Fut. Internet Drones (IoD): Insights, Trends Road Ahead, pp. 185–210 (2021)
7. Harbi, Y.; Aliouat, Z.; Refoufi, A.; Harous, S.: Recent security trends in Internet of Things: a comprehensive survey. IEEE Access (2021)
8. Wazid, M.; Das, A.K.; Lee, J.H.: Authentication protocols for the Internet of Drones: taxonomy, analysis and future directions. J. Ambient Intell. Humaniz. Comput, pp. 1–10 (2018)
9. Turkanović, M.; Brumen, B.; Hölbl, M.: A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. Ad Hoc Netw. **20**, 96–112 (2014)
10. Farash, M.S.; Turkanović, M.; Kumari, S.; Hölbl, M.: An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment. Ad Hoc Netw. **36**, 152–176 (2016)
11. Challa, S.; Wazid, M.; Das, A.K.; Kumar, N.; Reddy, A.G.; Yoon, E.J.; Yoo, K.Y.: Secure signature-based authenticated key establishment scheme for future IoT applications. IEEE Access **5**, 3028–3043 (2017)
12. Won, J.; Seo, S.H.; Bertino, E.: Certificateless cryptographic protocols for efficient drone-based smart city applications. IEEE Access **5**, 3721–3749 (2017)
13. Sun, X.; Ng, D.W.K.; Ding, Z.; Xu, Y.; Zhong, Z.: Physical layer security in UAV systems: challenges and opportunities. IEEE Wirel. Commun. **26**(5), 40–47 (2019)
14. Wong, V.W.; Schober, R.; Ng, D.W.K.; Wang, L.C.: Key Technologies for 5G Wireless Systems. Cambridge University Press (2017)
15. Alladi, T.; Chamola, V.; Sahu, N.; Guizani, M.: Applications of blockchain in unmanned aerial vehicles: a review. Veh. Commun. **23**, 100,249 (2020)
16. Yahuza, M.; Idris, M.Y.I.; Ahmedy, I.B.; Wahab, A.W.A.; Nandy, T.; Noor, N.M.; Bala, A.: Internet of drones security and privacy

issues: taxonomy and open challenges. IEEE Access **9**, 57243–57270 (2021)
17. Hassija, V.; Chamola, V.; Agrawal, A.; Goyal, A.; Luong, N.C.; Niyato, D.; Yu, F.R.; Guizani, M.: Fast, reliable, and secure drone communication: a comprehensive survey. IEEE Commun. Surv. Tutor. **23**(4), 2802–2832 (2021)
18. Kitchenham, B.: Procedures for performing systematic reviews. Keele, UK, Keele Univ. **33**(2004), 1–26 (2004)
19. Kitchenham, B.; Brereton, O.P.; Budgen, D.; Turner, M.; Bailey, J.; Linkman, S.: Systematic literature reviews in software engineering-a systematic literature review. Inf. Softw. Technol. **51**(1), 7–15 (2009)
20. Alzahrani, B.; Oubbati, O.S.; Barnawi, A.; Atiquzzaman, M.; Alghazzawi, D.: UAV assistance paradigm: state-of-the-art in applications and challenges. J. Netw. Comput. Appl. **166**, 102,706 (2020)
21. Chriki, A.; Touati, H.; Snoussi, H.; Kamoun, F.: Fanet: communication, mobility models and security issues. Comput. Netw. **163**, 106,877 (2019)
22. Boccadoro, P.; Striccoli, D.; Grieco, L.A.: An extensive survey on the Internet of Drones. Ad Hoc Netw. **122**, 102,600 (2021)
23. Gharibi, M.; Boutaba, R.; Waslander, S.L.: Internet of Drones. IEEE Access **4**, 1148–1162 (2016)
24. Outay, F.; Mengash, H.A.; Adnan, M.: Applications of unmanned aerial vehicle (UAV) in road safety, traffic and highway infrastructure management: recent advances and challenges. Transp. Res. Part A: Policy Pract. **141**, 116–129 (2020)
25. Ullah, S.; Kim, K.I.; Kim, K.H.; Imran, M.; Khan, P.; Tovar, E.; Ali, F.: UAV-enabled healthcare architecture: issues and challenges. Fut. Gener. Comput. Syst. **97**, 425–432 (2019)
26. Alsamhi, S.H.; Ma, O.; Ansari, M.S.; Almalki, F.A.: Survey on collaborative smart drones and Internet of Things for improving smartness of smart cities. IEEE Access **7**, 128125–128152 (2019)
27. Rahman, M.F.F.; Fan, S.; Zhang, Y.; Chen, L.: A comparative study on application of unmanned aerial vehicle systems in agriculture. Agriculture **11**(1), 22 (2021)
28. Anghelache, D.; Persu, C.; Dumitru, D.; Bălțatu, C.; et al.: Intelligent monitoring of diseased plants using drones. Ann. Univ. Craiova-Agric. Montanol. Cadastr. Ser. **51**(2), 146–151 (2021)
29. Zhou, Z.; Zhang, C.; Xu, C.; Xiong, F.; Zhang, Y.; Umer, T.: Energy-efficient industrial internet of UAVs for power line inspection in smart grid. IEEE Trans. Ind. Inform. **14**(6), 2705–2714 (2018)
30. Zhang, H.; Dou, L.; Xin, B.; Chen, J.; Gan, M.; Ding, Y.: Data collection task planning of a fixed-wing unmanned aerial vehicle in forest fire monitoring. IEEE Access **9**, 109847–109864 (2021)
31. Dong, J.; Ota, K.; Dong, M.: UAV-based real-time survivor detection system in post-disaster search and rescue operations. IEEE J. Miniat. Air Space Syst. **2**(4), 209–219 (2021)
32. Sambolek, S.; Ivasic-Kos, M.: Automatic person detection in search and rescue operations using deep CNN detectors. IEEE Access **9**, 37905–37922 (2021)
33. Ozkan, O.: Multi-objective optimization of transporting blood products by routing UAVs: the case of Istanbul. Int. Trans. Op. Res. pp. 302–327 (2022)
34. Li, X.; Savkin, A.V.: Networked unmanned aerial vehicles for surveillance and monitoring: a survey. Fut. Internet **13**(7), 174 (2021)
35. Zhang, J.; Huang, H.: Occlusion-aware UAV path planning for reconnaissance and surveillance. Drones **5**(3), 98 (2021)
36. Sharma, B.; Srivastava, G.; Lin, J.C.W.: A bidirectional congestion control transport protocol for the Internet of Drones. Comput. Commun. **153**, 102–116 (2020)
37. Zaidi, S.; Atiquzzaman, M.; Calafate, C.T.: Internet of flying things (IoFT): a survey. Comput. Commun. **165**, 53–74 (2021)
38. Herbadji, A.; Goumidi, H.; Harbi, Y.; Medani, K.; Aliouat, Z.: Blockchain for internet of vehicles security. Blockchain Cybersecur. Priv.: Archit. Chall. Appl. **1**, 159–197 (2020)
39. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H.: Blockchain technologies for the Internet of Things: research issues and challenges. IEEE Internet Things J. **6**(2), 2188–2204 (2018)
40. Ferrag, M.A.; Shu, L.: The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: a tutorial. IEEE Internet Things J. **8**(24), 17236–17260 (2021)
41. Yaacoub, J.P.; Noura, H.; Salman, O.; Chehab, A.: Security analysis of drones systems: attacks, limitations, and recommendations. Internet Things **11**, 100,218 (2020)
42. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N.: Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. IEEE Commun. Surv. Tutor. **21**(3), 2702–2733 (2019)
43. Harbi, Y.; Aliouat, Z.; Harous, S.; Bentaleb, A.; Refoufi, A.: A review of security in Internet of Things. Wirel. Pers. Commun. **108**(1), 325–344 (2019)
44. Li, X.; Wang, Y.; Vijayakumar, P.; He, D.; Kumar, N.; Ma, J.: Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network. IEEE Trans. Veh. Technol. **68**(11), 11309–11322 (2019)
45. 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**, 103,231-103,249 (2019)
46. Singh, M.; Aujla, G.S.; Bali, R.S.; Vashisht, S.; Singh, A.; Jindal, A.: in: Proceedings of the 2nd ACM MobiCom workshop on drone assisted wireless communications for 5G and beyond (2020), pp. 25–30
47. Bera, B.; Saha, S.; Das, A.K.; Kumar, N.; Lorenz, P.; Alazab, M.: Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled internet of drones environment. IEEE Trans. Veh. Technol. **69**(8), 9097–9111 (2020)
48. Bera, B.; Chattaraj, D.; Das, A.K.: Designing secure blockchain-based access control scheme in IoT-enabled internet of drones deployment. Comput. Commun. **153**, 229–249 (2020)
49. Hassija, V.; Saxena, V.; Chamola, V.: in: IEEE INFOCOM 2020-IEEE conference on computer communications workshops (INFOCOM WKSHPS) (IEEE, 2020), pp. 261–266
50. Wazid, M.; Bera, B.; Mitra, A.; Das, A.K.; Ali, R.: in: Proceedings of the 2nd ACM MobiCom workshop on drone assisted wireless communications for 5G and beyond (2020), pp. 37–42
51. Ge, C.; Ma, X.; Liu, Z.: A semi-autonomous distributed blockchain-based framework for UAVs system. J. Syst. Archit. **107**, 101,728 (2020)
52. Singh, M.; Aujla, G.S.; Bali, R.S.: in: IEEE INFOCOM 2020-IEEE conference on computer communications workshops (INFOCOM WKSHPS) (IEEE, 2020), pp. 249–254
53. Gai, K.; Wu, Y.; Zhu, L.; Choo, K.K.R.; Xiao, B.: Blockchain-enabled trustworthy group communications in UAV networks. IEEE Trans. Intell. Transp. Syst. **22**(7), 4118–4130 (2021)
54. Su, Z.; Wang, Y.; Xu, Q.; Zhang, N.: Lvbs: Lightweight vehicular blockchain for secure data sharing in disaster rescue. IEEE Trans. Depend. Secure Comput. **19** (1), 19–32 (2021)
55. Singh, M.; Aujla, G.S.; Bali, R.S.: A deep learning-based blockchain mechanism for secure Internet of Drones environment. IEEE Trans. Intell. Transp. Syst. **22**(7), 4404–4413 (2021)
56. Xu, X.; Zhao, H.; Yao, H.; Wang, S.: A blockchain-enabled energy-efficient data collection system for UAV-assisted IoT. IEEE Internet Things J. **8**(4), 2431–2443 (2021)
57. Feng, C.; Yu, K.; Bashir, A.K.; Al-Otaibi, Y.D.; Lu, Y.; Chen, S.; Zhang, D.: Efficient and secure data sharing for 5G flying drones: a blockchain-enabled approach. IEEE Netw. **35**(1), 130–137 (2021)

58. Wazid, M.; Bera, B.; Das, A.K.; Garg, S.; Niyato, D.; Hossain, M.S.: Secure communication framework for blockchain-based internet of drones-enabled aerial computing deployment. IEEE Internet Things Mag. **4**(3), 120–126 (2021)
59. Bera, B.; Das, A.K.; Sutrala, A.K.: Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in internet of drones environment. Comput. Commun. **166**, 91–109 (2021)
60. Irshad, A.; Chaudhry, S.A.; Ghani, A.; Bilal, M.: A secure blockchain-oriented data delivery and collection scheme for 5G-enabled IoD environment. Comput. Netw. **195**, 108,219 (2021)
61. Perumalla, S.; Chatterjee, S.; Kumar, A.S.: in: 2021 6th international conference on communication and electronics systems (ICCES) (IEEE, 2021), pp. 511–518
62. Xiao, W.; Li, M.; Alzahrani, B.; Alotaibi, R.; Barnawi, A.; Ai, Q.: A blockchain-based secure crowd monitoring system using UAV swarm. IEEE Netw. **35**(1), 108–115 (2021)
63. Kang, J.; Xiong, Z.; Niyato, D.; Xie, S.; Kim, D.I.: Securing data sharing from the sky: integrating blockchains into drones in 5G and beyond. IEEE Netw. **35**(1), 78–85 (2021)
64. Dolev, D.; Yao, A.: On the security of public key protocols. IEEE Trans. Inf. Theory **29**(2), 198–208 (1983)
65. Canetti, R.; Krawczyk, H.: in: International conference on the theory and applications of cryptographic techniques (Springer, 2002), pp. 337–351
66. Aggarwal, S.; Shojafar, M.; Kumar, N.; Conti, M.: in: ICC 2019-2019 IEEE international conference on communications (ICC) (IEEE, 2019), pp. 1–6
67. Patel, S.B.; Kheruwala, H.A.; Alazab, M.; Patel, N.; Damani, R.; Bhattacharya, P.; Tanwar, S.; Kumar, N.: in: Proceedings of the 2nd ACM MobiCom workshop on drone assisted wireless communications for 5G and beyond (2020), pp. 43–48
68. Masuduzzaman, M.; Islam, A.; Rahim, T.; Shin, S.Y.: in 2020 International conference on information and communication technology convergence (ICTC) (IEEE, 2020), pp. 412–416
69. Ch, R.; Srivastava, G.; Gadekallu, T.R.; Maddikunta, P.K.R.; Bhattacharya, S.: Security and privacy of UAV data using blockchain technology. J. Inf. Secur. Appl. **55**, 102,670 (2020)
70. Li, M.; Yu, F.R.; Si, P.; Yang, R.; Wang, Z.; Zhang, Y.: UAV-assisted data transmission in blockchain-enabled m2m communications with mobile edge computing. IEEE Netw. **34**(6), 242–249 (2020)
71. Gupta, R.; Shukla, A.; Mehta, P.; Bhattacharya, P.; Tanwar, S.; Tyagi, S.; Kumar, N.: in: IEEE INFOCOM 2020-IEEE conference on computer communications workshops (INFOCOM WKSHPS) (IEEE, 2020), pp. 255–260
72. Tan, Y.; Liu, J.; Kato, N.: Blockchain-based key management for heterogeneous flying ad hoc network. IEEE Tran. Ind. Inform. **17**(11), 7629–7638 (2021)
73. Cheema, M.A.; Shehzad, M.K.; Qureshi, H.K.; Hassan, S.A.; Jung, H.: A drone-aided blockchain-based smart vehicular network. IEEE Trans. Intell. Transp. Syst. **22**(7), 4160–4170 (2021)
74. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H.; Srivastava, G.; Aledhari, M.: Enabling drones in the Internet of Things with decentralized blockchain-based security. IEEE Internet Things J. **8**(8), 6406–6415 (2021)
75. Lv, Z.; Qiao, L.; Hossain, M.S.; Choi, B.J.: Analysis of using blockchain to protect the privacy of drone big data. IEEE Netw. **35**(1), 44–49 (2021)
76. Khan, A.A.; Khan, M.M.; Khan, K.M.; Arshad, J.; Ahmad, F.: A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs. Comput. Netw. **196**, 108,217 (2021)
77. Allouch, A.; Cheikhrouhou, O.; Koubâa, A.; Toumi, K.; Khalgui, M.; Nguyen Gia, T.: UTM-chain: blockchain-based secure unmanned traffic management for internet of drones. Sensors **21**(9), 3049 (2021)
78. Andola, N.; Yadav, V.K.; Venkatesan, S.; Verma, S.; et al.: Spychain: a lightweight blockchain for authentication and anonymous authorization in IoD. Wirel. Pers. Commun. **119**(1), 343–362 (2021)
79. Mitra, A.; Bera, B.; Das, A.K.: in: IEEE INFOCOM 2021-IEEE conference on computer communications workshops (INFOCOM WKSHPS) (IEEE, 2021), pp. 1–6
80. Islam, A.; Shin, S.Y.: in: 2019 7th international conference on information and communication technology (ICoICT) (IEEE, 2019), pp. 1–6
81. Islam, A.; Shin, S.Y.: A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things. Comput. Electr. Eng. **84**, 106,627 (2020)
82. Liao, S.; Wu, J.; Li, J.; Bashir, A.K.; Yang, W.: Securing collaborative environment monitoring in smart cities using blockchain enabled software-defined internet of drones. IEEE Internet Things Mag. **4**(1), 12–18 (2021)
83. Islam, A.; Rahim, T.; Masuduzzaman, M.; Shin, S.Y.: A blockchain-based artificial intelligence-empowered contagious pandemic situation supervision scheme using Internet of Drone things. IEEE Wirel. Commun. **28**(4), 166–173 (2021)
84. Feng, C.; Liu, B.; Yu, K.; Goudos, S.K.; Wan, S.: Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs. IEEE Trans. Ind. Inform. **18**(5), 3582–3592 (2021)
85. Liu, B.; Yu, K.; Feng, C.; Choo, K.K.R.: in: Proceedings of the 4th ACM MobiCom workshop on drone assisted wireless communications for 5G and beyond (2021), pp. 25–30