IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 3, 2022, accepted January 17, 2022, date of publication January 20, 2022, date of current version February 9, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3145199

Blockchain Interoperability in Unmanned Aerial Vehicles Networks: State-of-the-Art and Open Issues

RUBA ALKADI, NOURA ALNUAIMI, CHAN YEOB YEUN, (Senior Member, IEEE), AND ABDULHADI SHOUFAN
Center for Cyber-Physical Systems, Khalifa University, Abu Dhabi, United Arab Emirates

Corresponding author: Ruba Alkadi (ruba.alkadi@ku.ac.ae)

This work was supported by the Centre for Cyber-Physical Systems, Khalifa University.

ABSTRACT The breakthrough of blockchain technology has facilitated the emergence and deployment of a wide range of unmanned aerial vehicles (UAV) networks-based applications. Yet, the full utilization of these applications is still limited due to the fact that each application is operating on an isolated blockchain. Thus, it is inevitable to orchestrate these blockchain fragments by introducing a cross-blockchain platform that governs the inter-communication and transfer of assets in the UAV networks context. In this paper, we survey the literature on the state-of-the-art cross blockchain frameworks to highlight the latest advances in the field. We also provide an up-to-date review of blockchain-based UAV networks applications. Based on the outcomes of our survey, we introduce a spectrum of scenarios related to UAV networks that may leverage the potentials of the currently available cross-blockchain solutions. Finally, we identify open issues and potential challenges associated with the application of a cross-blockchain scheme for UAV networks that will hopefully guide future research directions.

INDEX TERMS Blockchain, unmanned aerial vehicles, interoperability, cybersecurity, survey.

I. INTRODUCTION

Recently, unmanned aerial vehicles (UAVs) have emerged as a game changing tech across many commercial industries. This fact is emphasized by the exponential increase in the UAV global market which is predicted to reach $22.55 billion by the end of 2026 [1]. Numerous UAV-based applications have been already developed by the research community [2]. The full deployment of UAVs' activities is, however, associated with safety, security, and reliability issues. These issues are fueling a surge of research activities to provide an optimum way to manage the airspace traffic flawlessly. Particularly, the Internet of Drones (IoD) concept has been resonating recently [3]. It basically fosters the idea of borrowing concepts from currently deployed networks (i.e. cellular networks, air traffic management (ATM), and the Internet). Nonetheless, adopting concepts from these networks to the unmanned air traffic is not straightforward due to the heterogeneous nature of the latter. The UAVs' ability to move in three dimensions at high speeds makes the problem even harder.

The blockchain technology, as a form of the distributed ledger technology (DLT), has proved effective in a multitude of security applications. Fundamentally, it is an immutable temper-proof distributed ledger that offers vital features such as treacability, transparency, and auditability. Together with its cryptographic algorithms, DLT serves as a secure repository of data and events. The blockchain works by first initiating a transaction where a set of nodes can verify or reject this transaction. The data in the blockchain is stored in blocks with specific sizes. Once a block reaches its maximum storage, it is linked to the block before it which will create a chain, hence the name blockchain. Due to its decentralized form, the blockchain offers traceability of the transactions. Blockchains can either be built permissioned or permissionless [4]. A permissioned blockchain requires the authentication of the nodes before processing any transactions. Nodes require authorization to be able to read and write data. A permissionless blockchain is, on the other hand, considered as a public blockchain where no authorization is

The associate editor coordinating the review of this manuscript and approving it for publication was Yang Tang.

required to read and write data. A blockchain can also be private or public, where a private blockchain can belong to a single company and all the nodes are controlled by that company while a public blockchain allows the public to join the network.

The advantages of DLT were quickly recognized and thus applied in many fields to tackle various emerging problems. In this regard, it has been articulated that employing blockchain technology in the UAV networks context will mitigate security and safety risks and improve reliability. This resulted in a large number of fragmented blockchains. Recently, it has been realized that these isolated chains need to communicate and inter-operate to exploit their full potential. The notion of cross-blockchain was proposed to address the portability and scalability of the blockchain technology. Portability refers to the ability of transferring assets and data between blockchains in a trustless way, while scalability refers to the ability to offload data to other blockchains. Several approaches to achieve interoperability between blockchains have fairly matured and successfully deployed for cryptocurrency exchanges. Besides, a multitude of applications have benefited from its potentials including healthcare data sharing [5], cyber-security [6], video games [7], and many others.

Although the unmanned air traffic management industry could remarkably profit from the advances in cross-blockchain technology, none of the proposed blockchain-based UAV networks highlighted this potential. Notably, there is a lack of research that reviews current literature in these two contexts and sheds the lights on possible future directions in unifying and inter-operating fragmented blockchains to serve the UAV networks industry. To the best of our knowledge, this work is the first to explore potential opportunities and use cases of cross-blockchain technology in the IoD context. Particularly, we are motivated by the enormous applications of the blockchain technology in the UAV networks and we believe that addressing the problem of interoperability of parallel blockchains is crucial to enabling efficient deployment of a decentralized immutable IoD *environment*.

A. OBJECTIVES

We, therefore, dedicate this paper to bridge the gap between the advances in blockchain interoperability and the various blockchain-based UAV networks by providing a brief, yet, comprehensive review of each topic. Our main objective is to scrutinize and exploit the state-of-the-art cross-blockchain models to enable an efficient integration and synchronization of blockchain-based UAV networks.

B. CONTRIBUTION

In brief, our contribution is distinguished by the following aspects:

- Providing a brief review and comparison between the most popular blockchain interoperability frameworks.
- Providing an up-to-date review of the recent blockchain-based applications in an IoD environment.
- Introducing possible scenarios where cross-blockchain is applicable in an IoD context.
- Identifying open issues and challenges in the current landscape and guiding future research.

C. SIGNIFICANCE OF CONTRIBUTION

The outcomes of this review will pave the way for new research questions and contributions related to the practical implementation of blockchain-based UAV networks applications in a more scalable and portable manner. Essentially, the problem of blockchain interoperability is more challenging in the UAV networks context since it intersects with other existing challenges such as processing and energy limitations.

D. PAPER ORGANIZATION

In this work, we perform a systematic review on the applicability of cross-blockchain frameworks in the context of UAV networks. We highlight the limitation of the literature in Section II. We, then, survey the literature on the current landscape of cross blockchain interoperability (Section III) and the latest blockchain-based UAV networks (section IV). In light of our review, we discuss possible use cases of the cross-blockchain framework in Section V. In Section VI, we emphasize the lessons learned, discuss the open issues and challenges, and envisage future directions. Finally, we conclude the paper in Section VII. A detailed paper organization diagram is provided in Figure 1 to assist the reader navigating through the paper.

II. RELATED WORK

Alladi *et al.* [8] and Mehta *et al.* [9] have reviewed the literature on the deployment of blockchain for serving several UAV networks. In the former, the authors focused on categorizing related literature according to the various applications of UAV networks. On contrary, Mehta *et al.* [9] considered the security triad (confidentiality, integrity, and availability) besides reliability and energy efficiency as the main themes for their review. Recently, Alvares *et al.* [10] published a survey on UAV-assisted internet of vehicles. Their review briefly highlighted some use cases of the blockchain in the UAV networks context. On the other hand, Belchoir *et al.* [11] reviewed the state-of-the-art in blockchain interoperability frameworks. None of the available reviews have focused on both: applications and security of blockchain-based UAV networks. Further, these surveys did not explore the potential of blockchain interoperability platforms in the UAV networks context. Table 1 compares between the related surveys.

III. CURRENT LANDSCAPE OF BLOCKCHAIN INTEROPERABILITY

Fueled by the unprecedented success of blockchain technology in enabling a decentralized cryptocurrency market, many industries have shown great interest (real and hype) in

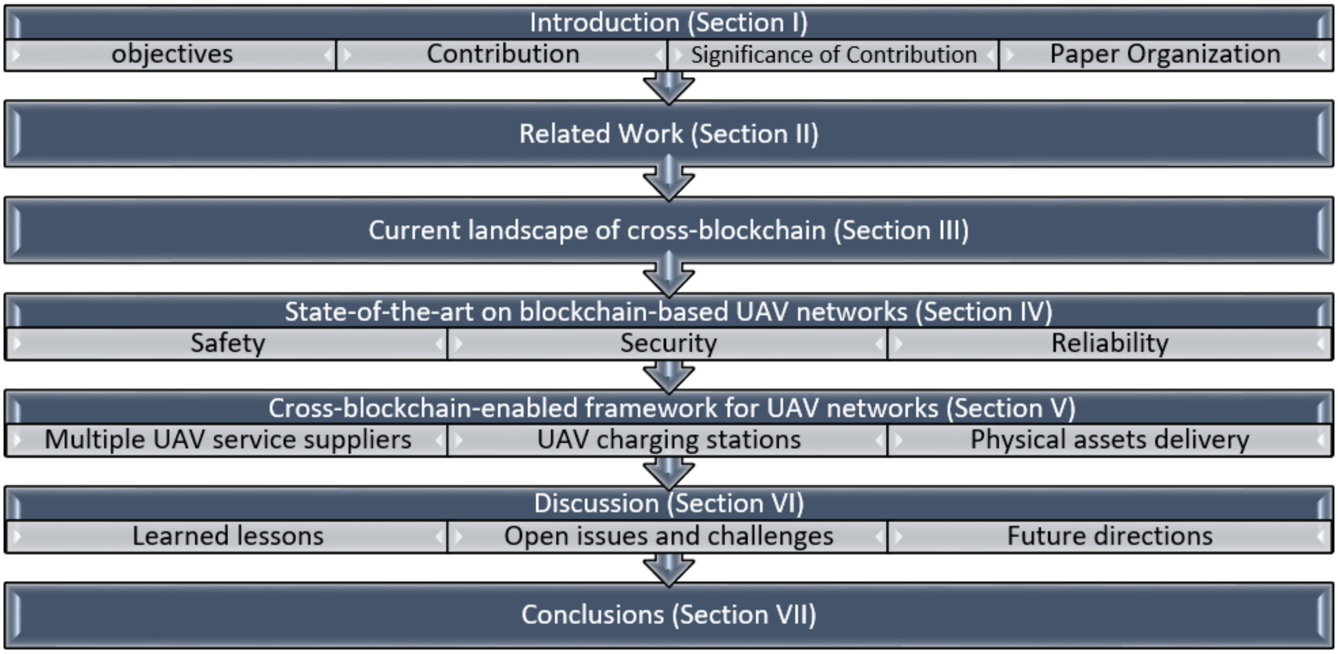
Introduction (Section I)
objectives
Contribution
Significance of Contribution
Paper Organization
Related Work (Section II)
Current landscape of cross-blockchain (Section III)
State-of-the-art on blockchain-based UAV networks (Section IV)
Safety
Security
Reliability
Cross-blockchain-enabled framework for UAV networks (Section V)
Multiple UAV service suppliers
UAV charging stations
Physical assets delivery
Discussion (Section VI)
Learned lessons
Open issues and challenges
Future directions
Conclusions (Section VII)

FIGURE 1. Paper organization diagram.

TABLE 1. Comparison between related surveys.

Survey	Year	Scope	Popularity	UAV-Networks Taxonomy			Cross blockchain
				Security vulnerabilities	Applications	Safety	
Alladi et al. [8]	2020	Surveys the various applications of BC in the UAV networks context	medium		✓		
Mehta et al. [9]	2020	Surveys the security vulnerabilities of UAV networks and how BC is adopted to address these vulnerabilities	high	✓	✓		
Alvares et al. [10]	2021	UAV-assisted internet of vehicles and blockchain solutions for smart cities.	low		✓		
Belchoir et al. [11]	2021	Explore the current landscape concerning blockchain interoperability, both in industry and academia.	high				✓
This survey	2022	Surveys the literature of UAV networks that employed BC to improve the safety, security, and reliability of various applications.	-	✓	✓	✓	✓

this technology. In the UAV networks context, researchers, as well as manufacturers, have called for a reimplementation of current UAV networks-based functions to exploit the security advantages of the blockchain and smart contracts (SC). Nonetheless, the omnipresence of these blockchain-based functions has led to fragmentation, redundancies, and fraudulent activities. Particularly, the implementation of such functions usually takes place on private and thus isolated blockchains.

Therefore, the interoperability of these isolated blockchains and their associated functions is crucial for enabling a fully connected Internet of blockchains that reduce the overall friction between participating businesses and achieves portability, scalability, and privacy. Moreover, cross-blockchain interoperability is envisioned to reduce redundant transactions and the associated cost. This is especially fundamental for UAV networks which are known to be limited in terms of energy, processing power, and memory [12]. A multitude of frameworks has been proposed to achieve blockchain interoperability. Table 2 provides a summary of the most common ones.

Originally proposed by Back *et al.* [31], sidechains are secondary blockchains connected to other blockchains via a two-way peg protocol [32]. This protocol requires locking the transferred funds on the mainchain until they are created in the sidechain. Then, these locked funds may be destroyed. Both, the sidechain and the mainchain may not have the same features or consensus mechanism. However, creating and maintaining sidechains is a complex task because sidechains are designed to interconnect two chains only. Connecting N blockchains requires creating N-1 sidechains, which limits the scalability of this solution.

TABLE 2. Blockchain interoperability approaches.

Interoperability approach	Description	Weaknesses	Examples
Sidechains	A blockchain connected to the mainchain via CCC protocol.	-Require TTP -Complex to build and not scalable	Solana [13], polkadot [14], loom [15], RSK [16], Horizon [17]
Notary schemes	Centralized or decentralized exchanges that make changes to the blockchains on behalf of users. They are faster and easier to use.	-Mainly for asset transfers -Most are centralized	Binance [18], coinbase [19], kraken [20]
Hashed time-lock contracts	Asset transfer mechanism without a TTP. It locks the fund on one blockchain for a specific time. Fund is unlocked again using a shared secret between the sender and receiver.	-Sender and receiver need to be online. -Only supports asset transfer. -A secret needs to be created for each use	Uniswap [21], lightning network [22], onechain [23], fusion [24]
Blockchain of blockchains	Use case specific blockchains that interact with each other	-Interoperability between blockchains of the same architectures -other architectures are not supported	-Ethereum 2.0 [25], Cardano [26], Polkadot [14], cosmos [27]
Trusted relays	Relay transactions from source blockchain to destination blockchain	-Private blockchains only	Hyberledger cactus [28]
Blockchain agnostic protocol	Translator between blockchains	-Private and public -Some lack enforcing smart contracts and non-fungible tokens -Rely on TTP	Quant [29], hyberledger Quilt [28], interledger [30]

Notary schemes are usually centralized exchanges that transfer assets between multiple blockchains. Sometimes, a group of exchanges performs the asset transfer task which is referred to as decentralized notary [33]. Although this approach is the easiest and most convenient, it is prone to centralization-related security risks as well as single-point of failures.

Hashed time-lock contracts are used for atomic swaps and off-chain transactions between trustless parties. The tokens are locked for a specific time on one blockchain. The receiver can unlock the tokens using by revealing a secret which is shared with him by the sender [34]. It, thus, requires sharing a secret between the sender and receiver which may be associated with security risks. Also, it requires the sender and receiver to be online during the transfer time. This is somehow similar to the one-time password (OTP). For this reason, it cannot be considered as a robust interoperability solution in the long run.

Blockchain of blockchains is a framework that connects multiple blockchains in a way similar to sidechains called bridges. Each blockchain is connected to other blockchains in the network either directly or via hubs. The current implementation requires interconnected blockchains to have the same architecture. In addition, this interoperability framework requires additional transaction fees which may prevent scalability on the global level [11].

Trusted relay is a decentralized approach that allows validators from source and target chains to validate, sign and deliver transactions between two blockchains. Sometimes, a TTP is employed to perform the tasks of the decentralized verifiers. For instance, Cactus implements multiple TTPs to issue transactions in several blockchains [35].

Ideologically, blockchain agnostic protocol is an abstraction layer that allows one to build an application that is operable on multiple blockchains in a seamless manner. Unlike other solutions which depend on constructing bridges between different blockchains, agnostic protocols must be able to function on a higher level layer abstracting from chain-specific protocols. Yet, this solution did not mature to achieve fully interoperable blockchains and is still under development. Although several approaches are proposed [36], a consensus on a fully agnostic protocol is yet to be unveiled.

A stimulating analogy between the Internet and the blockchain has been discussed in [37]. The authors highlighted the importance of understanding the aspects of the Internet that have made it scalable, resilient, sustainable, and commercially viable. They emphasized blockchain interoperability as a crucial requirement for managing and maintaining current and future blockchains. It is argued that the interoperability of the Internet is what made it scalable to the global level. Compared to the Internet, blockchains are viewed as Autonomous Systems (AS) that have predefined physical perimeters and are operated by an ISP.

IV. STATE-OF-THE-ART ON BLOCKCHAIN-BASED UAV NETWORKS

The realm of blockchain technology has sufficiently matured to solve emerging issues related to UAV traffic networks.

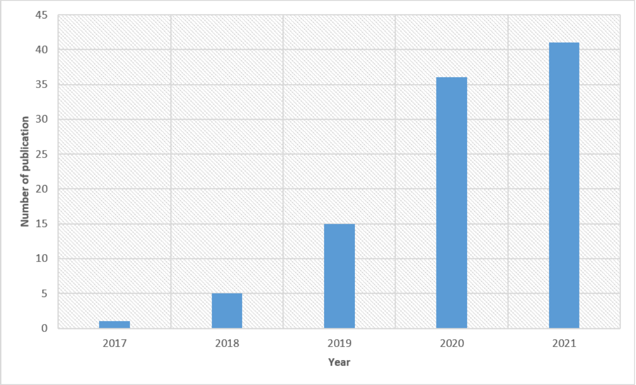

FIGURE 2. Breakdown of articles resulted in the preliminary search according to the year of publication.

In this section, we systematically review the state-of-the-art in UAV networks that deploy different versions of blockchain to exploit multiple advantages such as immutability, transparency, traceability, and auditability. To conduct our systematic review, we searched Google Scholar for full-text publications. Google Scholar is believed to be the world's largest academic search engine [38]. Already in 2014, Khabsa and Giles estimated that Google Scholar covers 80 to 90% of all articles published in English [39]. We used the advanced search tool to search for articles that contain the keyword *blockchain* in the title and at least one of the following words in the title as well: *UAV*, *UAS*, *drones*, *unmanned aerial vehicles*, or *unmanned aerial systems*. This resulted in 98 publications which are classified according to the year of publication as shown in Figure 2. Patents and gray literature papers were excluded. Articles published before 2018 are also excluded. The set of remaining articles was briefly screened for relevance. Some articles were excluded because their scope was not directly related to the application of blockchain on the UAV networks context. The set was thus reduced to 35 articles, three of which are review articles that were discussed previously in this paper (see section II).

Unlike other application-oriented reviews [8], our review spins three axes based on the ultimate motivation of each work, namely: safety, security, and reliability. We dedicate one subsection for each category to highlight the recent major contributions (from 2018 to 2021). Our review hierarchy is illustrated in Figure 3. Besides, the focus of the reviewed papers is summarized in Table 3. In this table, we compare between articles based on the stated objectives, the claimed advantages of the proposed solution, and the weaknesses or limitations identified by ourselves.

A. SAFETY

Safety refers to maintaining a good physical condition of a cyber-physical system while in operation. Not only the physical condition of the participating drones shall be preserved, but also the safety of the public residing under the national airspace. This is one of the ultimate goals of a UAV traffic management system that is achieved using different techniques such as route de-confliction, collision Avoidance, and geofencing.

In principle, *route de-confliction* refers to the mutual planning of flight paths of UAVs in space and time to ensure minimum or no conflicts. Scarlato *et al.* [40] proposed the design of a permissioned blockchain for the collision avoidance and recovery of UAVs. They envisioned a cooperative environment where participating UAVs communicate obstacle coordinates and collisions continuously. Moreover, Rahman *et al.* [41] proposed a UAV network to ensure a collision-free environment. Routes are planned in a way to avoid restricted areas such as private properties. Also, the flight altitude is specified to reduce the collision risk by minimizing the number of drones flying at the same height. To ensure that the drone is following the coordinates of the specified route, the authors use a smart contract to log drone movement and location information during the entire mission. If any of those attributes violates the specified flight route, a negative point is added to the drone's reputation.

On the other hand, Kuzmin and Znak [42] proposed a route-sharing scheme where cooperative drones deconflict their routes autonomously using the route information on a blockchain. They emphasized the usefulness of this approach especially when a manually operated drone loses connection with its base station. Motivated by a similar application, Allouch *et al.* [43] proposed, implemented, and evaluated a permissioned blockchain to perform secure path planning and data sharing among participating drones. To deal with the limited computation power and storage resources of the UAVs, they offload the computations to a cloud server while employing a decentralized off-chain storage system, namely OrbitDB. Moreover, they exclude the participating UAVs from the peer-to-peer network and only consider ground control stations as peers that store a copy of the ledger. To evaluate their architecture, they implemented the solution on the Hyper-ledger Fabric platform. Finally, they estimated the delay and resource consumption of one transaction. The average latency of an invoke transaction on a network of 50 users was 454 ms. Despite being relatively high compared to existing networks delays, this work has shown promise of the application of blockchain-based UAV networks in the real-time.

In contrast, *dynamic geofencing* refers to the virtual geographical fences usually imposed, maintained, and updated by an airspace authority. Dasu *et al.* [44] presented a hybrid method where parts of the airspace traffic is controlled by a central authority while others are decentralized with the help of blockchain principles. They separate the two parts using dynamic geofencing. In the decentralized zones, participating drones reserve a volume of air to conduct their missions. The reservation is logged in a transaction on a public ledger and is approved if the requested volume is idle at the time of the mission. To achieve this, they employ the double-spending avoidance concept originally deployed in cryptocurrencies. The authors also suggest that, depending on the congestion

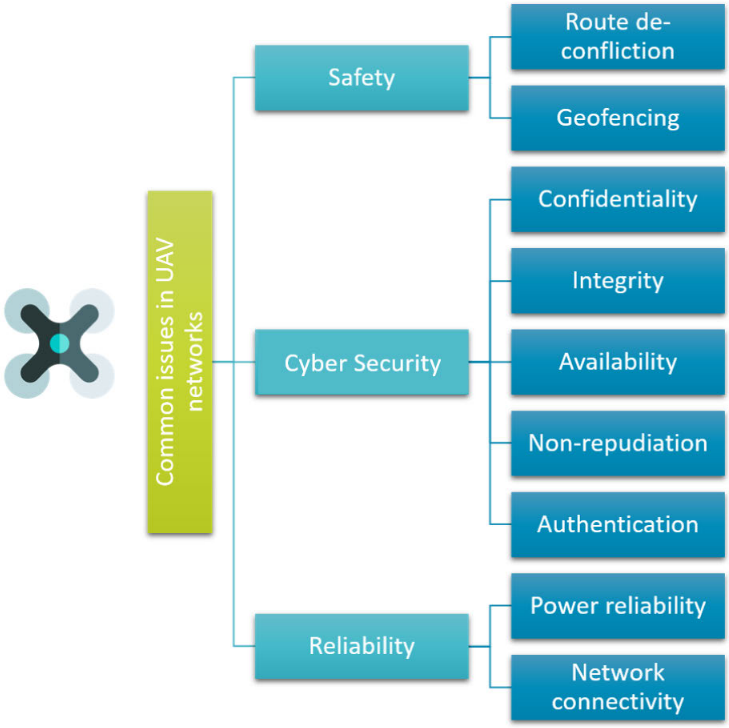

FIGURE 3. Emerging issues in UAV networks that are addressed using blockchain.

of the required airspace, authorities may charge users for airspace allocation. This approach guarantees a fair share of the airspace while reducing the congestion in peak-hours and urban areas. It also improves the public safety by avoiding collisions and dynamically prohibiting missions over people crowds.

1) INSIGHTS

Route deconfliction and planning is a common application of blockchain in the UAV networks. This is due to the various advantages of blockchain in maintaining an immutable and traceable record of data without a need for a managing trusted third party such as the USS. The work of Allouch *et al.* [43] has shown that real-time implementation of such blockchain-based application is possible with a reasonable delay. On the other hand, the work on the geofencing application is still limited in the literature. Although such application would be a good candidate for the blockchain technology. This is achievable by introducing a blockchain that connects airspace authorities with UAVs and operators.

B. CYBERSECURITY

Cybersecurity serves as an overarching goal for the employment of blockchain technology in the UAV networks context. Essentially, the immutability feature of this technology makes it a perfect candidate for ensuring accountability of end-users. Most of the papers that proposed a blockchain-based solution for UAV traffic are motivated by cybersecurity-related requirements, including confidentiality, integrity, availability, non-repudiation, and authentication. We briefly review how each aspect is addressed in the literature. Although, most of the proposed solutions simultaneously address the five security aspects, we tend to group them based on the most dominant one. For a more detailed review of earlier works, the reader is referred to [9].

Confidentiality refers to protecting information from being accessed by unauthorized users. Like other networks, UAV networks are prone to confidentiality attacks such as data sniffing, eavesdropping, and replay attacks. Wu *et al.* [45] have recently outlined multiple scenarios at which blockchain can be employed to preserve the privacy of UAV networks. They suggested a cost-effective, tamper-proof blockchain-based ID management system to authenticate and authorize drones as per the Federal Aviation Authority (FAA) requirements. Besides, they leveraged the potentials of the DLT to preserve the privacy of the trajectory information of the drones. The authors argued that asymmetric encryption and homomorphic obfuscations schemes inherited in blockchain can be utilized to improve the confidentiality of the network.

On the other hand, Qian *et al.* [46] employed blockchain to protect the privacy of cached content by sharing only necessary content with selected vehicles. Similarly, Xiao *et al.* [47] proposed a drone-swarm-aided distributed crowd monitoring system that features efficient identity authentication, secure communication, and distributed data management. The goal of the work is to ensure that the monitoring data are kept confidential and secure. They outline a public key infrastructure (PKI)-based security protocol to authenticate participating

TABLE 3. Latest proposals on blockchain-enabled UAV networks.

Authors	Field of contribution	Blockchain Application	Objectives	Advantages	Weaknesses
Scarlato *et al.* [40]	Safety	Collision avoidance	Avoid UAV crashes and enable recovery after collisions	Blockchain is adapted to log the GPS coordinates every 3 seconds. In case of a collision, SCs are used to recover the drone by the help of rescuers and repairers. An award system is introduced to incentivize the recovery mechanism.	No simulation or implementation is presented. Scalability issues may arise. Requires high transaction rate to log the GPS coordinate.
Rahman *et al.* [41]	Safety	Collision avoidance	Plan routes ahead of time to avoid collisions.	Employs a SC to log the the UAV's location and altitude and compare it with the planned route. A penalty system is proposed to ensure that the drones follow the planned route	The proposed scheme requires on-board processing power and high throughput communication channel . Limited scalability.
Kuzmin *et al.* [42]	Safety	Route deconfliction	Decentralized route planning mechanism	No trusted third party is needed to perform route planning. Useful when a manually operated drone losses connection with its base-station.	The work lacks mathematical modeling and verification of the applicability of the proposed proof-of-graph consensus mechanism.
Allouch *et al.* [43]	Safety	Route deconfliction	Secure path planning and data sharing	Power efficient solution by utilizing cloud servers and off-chain storage. The P2P is run on the base-station.	Communication overhead to the base station.
Dasu *et al.* [44]	Safety	geofencing	Acheiving dynamic geofencing and congestion management	Introducing a hybrid method (centralized and decentralized). Introducing a dynamic pricing model	No implementation or simulation.
Wu *et al.* [45]	Cybersecurity	Confidentiality	ID management system as per the FAA requirements	Authenticate and authorize drones while preserving the privacy of their missions using blockchain	Prone to 51% attacks as drones can freely join and leave, requires excessive storage and computational resources.
Qian *et al.* [46]	Cybersecurity	Confidentiality	Preserve the privacy of cached content	Higher cache hit rate and robustness	Scalablity not possible. Significant communication overhead.
Xiao *et al.* [47]	Cybersecurity	Confidentiality	Secure and privacy-aware crowd monitoring system	PKI-based security protocol to authenticate participating UAVs, assign the monitoring task to UAVs, and allow secure access for the monitoring data.	Time overhead for key generation.
Ghribi *et al.* [48]	Cybersecurity	Confidentiality	Preserve he confidentiality of UAV networks	Employs PKI and OTP to ensure the confidentiality of the network communication channels	significant time overhead and computational cost
Lv *et al.* [49]	Cybersecurity	Confidentiality	Preserve he confidentiality of UAV networks	Low computing cost for encryption, decryption and key generation compared to current data sharing models	Computationally expensive cryptographic algorithms.
Islam *et al.* [50]	Cybersecurity	Integrity	Ensure the integrity of the data before being transmitted to MEC servers.	The data is securely kept in a blockchain at MEC servers. No extra storage required on-board the UAV	Limited scalability, does not consider UAV mobility.

TABLE 3. ***(Continued.)*** **Latest proposals on blockchain-enabled UAV networks.**

Authors	Field of contribution	Blockchain Application	Objectives	Advantages	Weaknesses
Singh *et al*. [51]	Cybersecurity	Integrity	Improve the integrity of data transferred between drones	Intelligently detect anomalies in the BC-based blockchain. Provides simulation and time analysis of the proposed system.	Does not explicitly consider UAV networks.
Kanade *et al*. [52]	Cybersecurity	Integrity	Secure power plants sensing data	A BC-based UAV swarm to log sensed data. Reduce cost by introducing human validators and logging only important transactions.	Requires human interaction. No clear consensus mechanism.
Yazdinejad *et al*. [53]	Cybersecurity	Availability	Maintain the availability of UAV networks and provide an authentication scheme for participating drones.	Introduce trusted ground-based drone controller to manage the authentication. Allow neighbor drone controllers to substitute for a failing one to maintain the availability.	Requires trusted parties. Communication overhead.
Kapitonov *et al*. [54]	Cybersecurity	Availability	Improve security between communicating nodes	Supports the UTM architecture. Solves the latency issue that is found in decentralized systems	No results of the implementation are reported (time overhead, computational overhead, etc). Only one drone is used in the experiments, scalability is not studied or discussed.
Barka *et al*. [55]	Cybersecurity	Non-repudiation	Improve the non-repudiation feature of UAV applications	Introduces a trusted blockchain-based UAV system to protect critical infrastructure. Efficient energy consumption solution. High accuracy in detecting malicious nodes	The use of proof-of-work consensus degraded the system's efficiency.
Almotary *et al*. [56]	Cybersecurity	Non-repudiation	Preventing dishonesty by UAV in a network	Highlights the features of blockchain that enhances drone security. Presents statistics of blockchain-based UAV applications.	No technical solution is proposed. Implementation challenges are not considered.
Kumari *et al*. [57]	Cybersecurity	Authentication	Preventing authentication attacks	Presenting a blockchain-based softwarization of the UAV network management scheme.	High data processing latency. Real-time deployment of blockchain on the movable UAVs.
Cheema *et al*. [58]	Cybersecurity	Authentication	Develop a registration and authentication scheme fore drones in the IoV environment	A blockchain-based secure intelligent transportation system is proposed for the drone-enabled wireless technology. Addresses the communication overhead by optimizing the positioning of drones. Optimizes the power allocation of drones to serve for longer time.	Scalability is not addressed.
Andola *et al*. [59]	Cybersecurity	Authentication	Address the malleability attack and drone handoff latency issues.	Describes detailed blockchain-based authentication scheme following four approaches. Full security analysis is provided for all approaches	Time and computational overhead are not optimized or considered in the design.

TABLE 3. ***(Continued.)*** **Latest proposals on blockchain-enabled UAV networks.**

Authors	Field of contribution	Blockchain Application	Objectives	Advantages	Weaknesses
Hassija *et al* [60]	Reliability	Power reliability: recharging/ refueling	Manage power-charging/refueling between UAVs and charging stations	Propose a power trading model between UAVs and charging stations using a game-theoretic approach. Increase the operational time of UAV swarms.	Transaction validation is acyclic. Suffers from centralization issues.
Jiang *et al* [61]	Reliability	Power reliability	Manage wireless power trading	Contract theory-based resource cooperation scheme to motivate UAVs and validators to participate in wireless power transfer	Transaction validation is acyclic. Suffers from centralization issues.
Qiu *et al* [62]	Reliability	Power reliability	Introduce a spectrum trading platform for UAV-assisted cellular networks	Offloads processing to MEC devices and introduce a reputation algorithm. Stackelberg game-based business model. Outperforms three benchmarks	Slow convergence of deep reinforcement learning algorithm which increases the time overhead of the mechanism.
Pathak *et al* [63]	Reliability	Power reliability	Enable UAV as a service scheme by connecting UAV owners, end users, and UAV-service providers	Allows for an efficient utilization of resources by renting UAVs	Limited scalability and low security due to the use of private blockchain. UAVs are assumed to be connected to the Internet to transmit data in real-time.
Gai *et al* [64]	Reliability	Power reliability	Facilitate secure and reliable group communication between UAVs.	Introduce voters and attributes to validate identities. Incentivization model.	Latency and cost of blockchain transactions are not addressed.
Wu *et al*. [65]	Reliability	Power reliability	Ensure security and scalability of IoT.	Integrates blockchain and edge computing to maintain secure and scalable IoT infrastructure. Identifies challenges with the adoption of blockchain.	Does not provide solutions to common blockchain challenges such as scalability and latency.
Hassija *et al* [66]	Reliability	Network connectivity	Enable drones-mounted small cell base stations with high reliability and security.	Implements a smart contract based on the game theory to dynamically allocate bandwidth to users based on cost and availability	Does not consider computational and time overhead.
Feng *et al.* [67]	Reliability	Network connectivity	Introduce secure and reliable data sharing scheme for 5G flying drone.	Blockchain and attribute-based encryption are proposed. Energy and computational overhead are reduced by parallel outsourced computation.	-
Sharma *et al*. [68]	Reliability	Network coverage	Provide ultra-reliable flattened 5G network service	Presented a neural-blockchain-based scheme for MEC caching. Improved connectivity, reduced energy consumption.	Maximum failure rate is increased by 13%
Aloqaily *et al*. [69]	Reliability	Network connectivity	To enable an on-demand mobile access points by the use of UAVs	Public and private blockchains deployed on UAVs, supported by fog and cloud computing servers. Increased total number of delivered packets.	If data generation rate exceeds the blockchain throughput (mining process), the system fails. Scalability is an issue. Cost is not considered.
Singh *et al*. [70]	Reliability	Network connectivity	Improve the security and reliability of UAV networks	Proposed a one-drone one-block architecture. Vulnarability analysis of several common attacks shows robustness of the solution. Adopts a novel consensus mechanism	Consensus is based on the position of the drone which is not a reliable feature.

UAVs, assign the monitoring task to participating UAVs, and allow secure access for the monitoring data by the management.

They propose the use of a private blockchain with smart contracts to log the events and actions throughout the task. In terms of results, their simulation revealed that the time overhead of the security protocol increases as the size of the swarm increase, whereas the key creation stage is responsible for the largest delay among other operations.

In the same context, Ghribi *et al.* [48] targeted the confidentiality aspect of UAV networks by implementing a private blockchain with encrypted transactions. The popular public key cryptography with the Elliptic Curve Diffie-Hellman (ECDH) model was used along with a one-time password (OTP). A communication between the sender and the receiver UAVs is done by a nominated endorsement UAV which generates a 128-bit key by using the ECDH. After that, an OTP key is generated by hashing the ECDH key. Finally, the generated key is sent to the sender UAV and the rest of the endorsement UAVs for approval. On the contrary, Lv *et al.* [49] addressed the confidentiality of blockchain aided UAV-networks data sharing scheme by means of the number theory research unit cryptosystem. They argue that their scheme requires low computing cost for encryption, decryption and key generation compared to current data sharing models.

Data *integrity* is also important to ensure that transmitted data is not altered or modified by an intruder. Islam and Shin [50] proposed an architecture to preserve the integrity of the data transmitted between IoT devices and Mobile Edge Computing (MEC) devices and servers. They used UAVs as trusted relays to ensure the integrity of the data before being transmitted to MEC servers. The data is securely kept in a blockchain at MEC servers. The proposed mechanism which includes an encryption scheme improves the overall integrity of the transferred data and reduces the number of direct requests to MEC servers. In contrast, Singh *et al.* [51] employed a blockchain to improve the integrity of data transferred between drones in an IoD environment. Their mechanism intelligently selects the miner node using a deep Boltzmann machine. Power plants surveillance is another application that requires high data integrity. Kanade [52] proposed a secure surveillance system for power plants using UAV swarms. They employ the DLT to preserve the integrity of the plant data sensed by the UAVs. To reduce the computational cost, transactions are only issued for high risk signals. Further, block validation task is assigned to human workers to reduce the computational cost.

Moreover, maintaining the *availability* of services for UAVs in the airspace is a vital concern. By design, blockchain is a decentralized technology which is immune to single-point-of-failure [71]. All proposed blockchain-based UAV traffic management (UTM) architectures are essentially decentralized and require limited or no central authority. Yazdinejad *et al.* [53] proposed a decentralized zone-based system for registering and authenticating drones. In their architecture, they assign a trusted ground-based drone-controller agent to manage the authentication within a predefined perimeter. They maintain the availability of the authentication scheme by allowing neighbor drone-controllers to substitute for a failing one. In the UTM context, the authors of [54] defined a blockchain architecture for UTM in which they implemented a so called Robonomic protocol to provide security between communicating nodes. They argue that their architecture solves the latency issue that is found in decentralized systems, which is essentially beneficial for critical applications. The model is supported by smart contracts that provide transparency and immutability. Thus, the work is implemented by means of the decentralized Ethereum and InterPlanetary File System.

Another crucial requirement for the cybersecurity of UAV networks is *non-repudiation*. This term is defined as the inability to deny or refuse responsibilities of actions. This can be achieved using public key infrastructure, where a UAV signs messages using its private key before sending it via the network. In [55], Barka *et al.* highlighted the importance of non-repudiation as a requirement for UAV networks. They argued that a UAV might deny sending images of restricted areas. Thus, the authors proposed a trusted blockchain-based UAV system to protect critical infrastructure. Similarly, the authors of [56] defined four blockchain concepts that can enhance the drone security. These elements comprise: digital fingerprint, data structure, consensus mechanism, and access control. They emphasize the role of the consensus mechanism in preventing dishonesty by allowing nodes in the network to agree on a transaction.

Finally, ensuring *authenticity* of users and messages is a key requirement for UAV networks. In principle, authentication is defined as the ability to recognize the real identity of a user. UAV networks may suffer from authentication attacks such as masquerading attack. Kumari *et al.* [57] addressed such threats in UAV networks by presenting a blockchain-based softwarization of the UAV network management scheme. They argue that the UAV network should be provisioned with cryptographic data to ensure authentication and confidentiality. Similarly, Cheema *et al.* [58] employed blockchain technology to develop a registration and authentication scheme for drones in a smart vehicular network context. They also addressed the issue of optimal drone positioning to enhance the overall spectral efficiency in the network. Under the same consideration, Andola *et al.* [59] proposed a lightweight blockchain model that provides authentication and anonymity. Their work provides security preferences for a surveillance UAV. They defined an adversary model in which an attacker can modify the transactions of a blockchain during the communication before they are verified. This kind of attack is called a malleability attack. They also defined an issue during the handoff process when a UAV moves from one Ground Control station (GCS) to another, where latency might occur. They solve this issue by implementing a novel blockchain architecture which they called SpyChain. They have described a detailed authentication scheme of their work following four approaches.

1) INSIGHTS

Most of the proposed DLT-based UAV networks aim at upgrading the security features of their traditional centralized counterparts. Confidentiality is improved by the inherited cryptographic features of the blockchain. Decentralized storage systems can also be utilized to serve the confidentiality of data shared by UAVs such as video streaming. Similarly, the asymmetric encryption of the blockchain technology is employed to improve the integrity and non-repudiation of the UAV networks data. Further, availability of the UAV network is maintained by deploying a blockchain framework which requires no central authority and is resilient to single-point-of-failures scenarios. Authentication of nodes in the UAV networks is also widely addressed in the literature of blockchain. Most of the studies have already analyzed the time and processing overhead of implementing blockchain to enhance the security of UAV networks. It is concluded that the time overhead increases as the size of the UAV network increases, thus limiting the scalability of the blockchain-based solution.

C. RELIABILITY

Improving the reliability of UAV traffic management is a crucial prerequisite to attracting large-scale commercial applications such as package delivery, transportation, and network coverage. This is achieved by optimizing power reliability and network connectivity while minimizing the cost. A surge of research activities have been identified in this direction.

Hassija *et al.* [60] presented a blockchain-based architecture to manage power-charging/refueling between UAVs and charging stations. Their proposed model allows UAVs to buy power using digital tokens. Wireless power trading in UAV networks based on blockchain principles is also proposed in [61]. The same idea was also proposed earlier in [62] where a consortium blockchain was exploited to introduce a spectrum trading platform for UAV-assisted cellular networks. In this work, MEC devices were employed to reduce the computation overhead of the verification process. To select the block miner, they implemented a reputation algorithm for the MEC devices. Further, the business model is incentivised by a Stackelberg game to maximize the profit of the cellular network operators and the UAV operators. They claim that the proposed framework enables a secure, efficient, and decentralized spectrum trading between both trading parties. Another UAV-based business model is proposed by Pathak *et al.* [63] where a blockchain-based UAV virtualization is introduced to provide UAV as a service. The envisioned platform aims at connecting UAV owners, end users, and UAV-service providers via a permissioned distributed network, enabling UAV owners to rent their vehicles to end users which in turns allows for a more efficient utilization of resources. Their architecture is similar to the previously proposed sensor virtualization [72].

The concept of blockchain is employed to ensure efficient resource utilization, security, and market competition. Comparably, Gai *et al.* [64] incentivised miners to validate authentication and authorization certificates. The presented approach aims at facilitating secure and reliable group communication between UAVs. Particularly, blockchain was employed to record and validate actions. On the other hand, an attribute-based voting mechanism is introduced by means of smart contracts. Real-time experiments were carried out to verify and assess the model performance. On the other hand, Wu *et al.* [65] proposed a layered IoT architecture that supports offloading computationally-intensive mining processes to edge servers. This, in turn, reduces power consumption on UAVs and base stations.

To improve the 5G network coverage, the authors of [66] proposed another blockchain-based model for using drones as dynamic base-stations. Their model integrates a game-theoretic smart contract that ensures fair and efficient allocation of bandwidth between users. Likewise, the authors of [67] proposed a blockchain enabled 5G drones network to address the identity authentication and secure data sharing of drones. In their work, they implement three core services utilizing blockchain technology, namely: identity authentication, operation management, and security auditing. Moreover, they employ a multi-signature smart contract managed by a central authority for registering and authenticating drones. To incentivise miners, peers request a certain amount of coins to verify that the requesting drone is already in the registered drones list. Besides, secure data sharing is enabled by uploading encrypted data to the cloud. Similarly, the uploading process is mainly managed by a smart contract deployed on the blockchain. On the contrary, Sharma *et al.* [68] presented a neural-blockchain-based scheme for MEC caching. In their model, they used drones as base stations to provide ultra-reliable flattened 5G network service. The proposed model was evaluated in terms of flyby time and area spectral efficiency. Similarly, Aloqaily *et al.* [69] envisioned a blockchain assisted 5G network which improves the quality of service by deploying public and private ledgers supported by fog and cloud data centers. They showed that their framework improves packet delivery success rate compared to traditional networks without blockchain. Additionally, Singh *et al.* [70] addressed the problem of reliability in UAV-networks by introducing a light-weight permissioned blockchain solution that in which each drone in the network would access its own block rather than all the blocks in the ledger. They argue that this architecture solves the issue of large ledger that would be produced each time more data and blocks are added. A shrinking mechanism has also been implemented to provide a fast lightweight blockchain.

1) INSIGHTS

Blockchain was widely adopted to manage UAV networks on the application layer. Most papers employed a blockchain framework to facilitate a supply chain application on UAV networks. Others focused on providing a fair and secure

5G network sharing scheme. To tackle the limited resources on-board the UAV, modification of the blockchain architecture was adopted in some proposals. It is important to note that these applications are usually required to run in parallel which necessitates the development of a suitable mechanism that integrates multiple blockchain architectures in the same framework.

V. CROSS-BLOCKCHAIN-ENABLED FRAMEWORK FOR UAV NETWORKS

Despite the remarkable advances in blockchain-aided UAV networks, the exploitation of cross-blockchain communication framework is still limited. The main purpose of the cross-blockchain technology is to connect the *independent* blockchain networks. A variety of solutions have been introduced to cope with the interoperability limitation. Qasse *et al.* categorized cross blockchain solutions into four groups: sidechains [73], trusted third party [14], blockchain routers [74], [75], and smart contracts [76]. Alternatively, Belchoir *et al.* [11] categorized the proposed approaches into three categories, comprising: public connectors [77], [78], hybrid connectors [79], [80], and blockchain of blockchains [27], [81]. As discussed in the previous section, blockchain is playing an important role in building UAV networks. Basically, UAV networks have a variety of functionalities, yet each paper discussed focuses on either a single or double functionalities. Eventually, a sophisticated network must combine all of the functionalities to build a secure and safe UAV environment. One could take lessons from previously implemented cross-blockchain models in other fields such as asset transfer [82], [83] and health records [84]. Fueled by the enormous applications that may potentially benefit from the cross-blockchain concept, software development environment were also introduced to enable easier deployment of cross-blockchain models [85], as well as the associated smart contracts [86]. In this section, we highlight opportunities and discuss multiple proposals to employ interoperable blockchains in the IoD environment including: multiple UAV Service Suppliers (USS), UAV charging stations, and UAV delivery application (supply chain).

A. MULTIPLE UAV SERVICE SUPPLIERS

The USS is an entity that provides services to subscribed UAS operators to help them meet the operational requirements specified by the national aviation authority. Operation planning, strategic and tactical de-confliction, Remote ID (RID), and airspace authorization are examples of the services provided by a USS. A UAV operator may subscribe to one or more USSs to avail multiple services. Upon subscription to a USS, the UAV is given a unique ID and automatically registered on a public blockchain which is accessible by other USSs and aviation authorities. In parallel, the USS deliver digital assets/data to the UAV using another blockchain that is only visible to the UAVs in a certain zone and this particular USS. The USS needs to interface the two ledgers to synchronize the process of serving new subscribers while keeping record of their IDs in a public blockchain.

Another scenario could happen when a USS user migrates to another USS. In this case, he might request the old USS to migrate his data and reputation/awards to the new USS to make use of them. Recall that keeping all assets (i.e. registration, payment, reputation, IDs, location-based services, etc.) in one ledger is inefficient, especially when the chain becomes too long. Moreover, some of these information shall not be shared with some parties while other should be public. Thus, adopting specialized ledgers and allowing communication between them improves scalability and confidentiality.

On the other hand, UAV networks could also make use of the decentralized identifiers (DID) scheme to enable the minimum disclosure of users' information on a need-to-know basis. Many DID frameworks are built on top of a blockchain [87]. Indeed, DID preserves users' privacy while promoting a universally unique identity that can be used across multiple blockchains [88]. Currently, the DID framework is being considered for universal standardization by the World Wide Web Consortium (W3C) [89] which implies the importance of integrating it with the current blockchain-based UAV networks. Amiri *et al.* [90] proposed a decentralized cross-domain blockchain that interfaces multiple applications via a DID system. Ideologically, UAV networks could make use of such solutions after carefully tailoring them for the UAV environment.

B. UAV CHARGING STATIONS

As discussed earlier, Hassija *et al.* [60] envisioned a UAV charging-refueling scheme built on top of the blockchain. They assumed that UAVs can buy power/fuel from ground stations using tokens or cryptocurrencies. However, every fuel supplier might restrict transactions on its blockchain using a particular cryptocurrencies. What if the UAV does not hold coins of the same cryptocurrency in its wallet? A straightforward solution would be to implement cross-blockchain solutions to exchange coins to the desired cryptocurrency.

C. PHYSICAL ASSETS DELIVERY

The need to incorporate cross-blockchain technology in UAV networks becomes evident in the physical-assets delivery scenario. That is, a delivery UAV needs to operate on at least two blockchains: one related to the supply-chain, and another related to the airspace traffic network. In some cases, the supply-chain ledger might request traffic and location-related information from the air traffic ledger to track the shipment. Possibly, this use case could be addressed using the CAPER framework [91], where confidentiality and interoperability are jointly provided. In other cases, the two ledgers may need to exchange coins to pay for USS services and refueling. Figure 4 illustrates a potential scenario at which blockchain interoperability is required for a delivery drone.

In this scenario, four blockchains need to interoperate to accomplish a simple delivery mission. In the first blockchain,

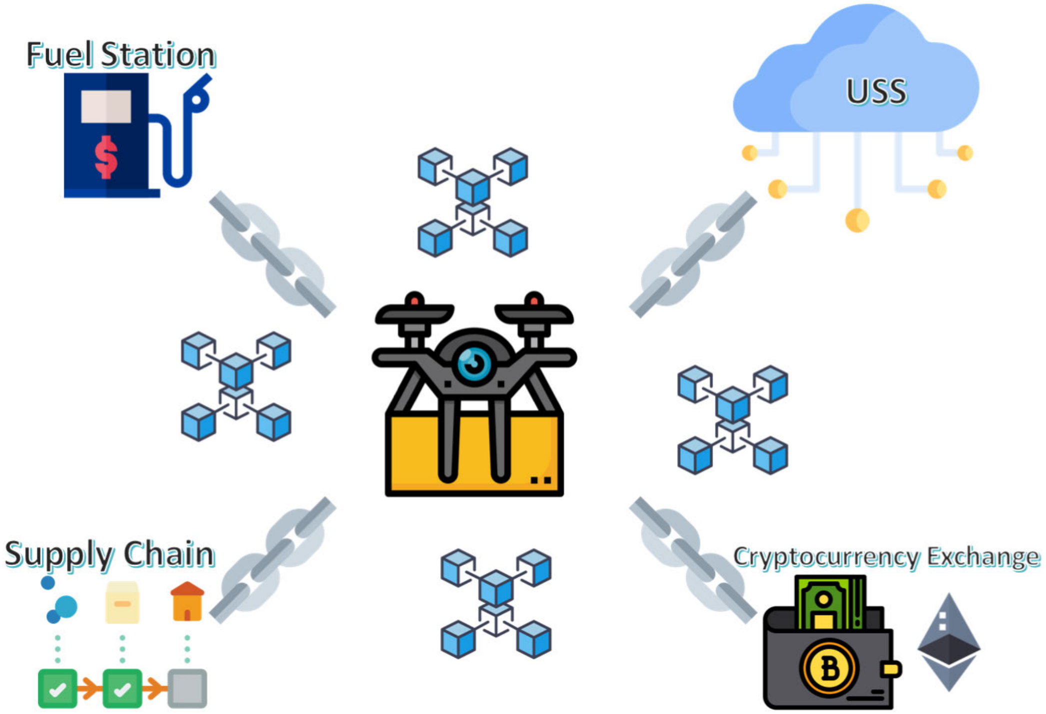

FIGURE 4. Potential cross-blockchain scenario at which a delivery drone is operating on four ledgers simultaneously.

the drone subscribes to a USS smart contract at which it gets flight-related services such as dynamic geofencing and route de-confliction. To subscribe to this USS, a specific cryptocurrency wallet is required, which lives in another ledger. Further, the UAV needs to connect to a private supply chain related ledger, where the supplier and costumer can track the shipment location. Another possible use of blockchain is for fueling or charging the drone using a re-charging station. Essentially, the drone needs to exchange information securely between these ledgers without compromising data integrity or security. A cross-blockchain solution is indispensable in such cases.

VI. DISCUSSION

In this section, we provide insights about the current status of the research in the area. We, first, list the lessons learned. Then, we highlight the open issues and challenges. Finally, we introduce future directions of the research in this field.

A. LEARNED LESSONS

Following are the main take-home highlights of our survey:

- A multitude of blockchain applications have been proposed for the UAV networks context in the last four years.
- Mainly, these proposals aim to enable a safe, secure and reliable operation of UAV networks.
- Most of the reviewed papers focus on improving the security features of the UAV networks by deploying a customized blockchain. Only few papers addressed the safety and reliability issues of the UAV networks by envisioning a blockchain solution.
- Most authors highlighted the challenges of implementing a blockchain on-board the UAV such as limited resources, power, and storage. The most common approach of addressing these challenges is offloading the storage and validation process to other devices connected to the UAV network such as ground controllers and cloud servers.
- Blockchain interoperability is crucial to reduce redundant costs and friction between businesses, thus enabling a universal blockchain environment that serves multiple applications.
- None of the works have identified or addressed the challenge of interoperability of multiple blockchain based UAV applications.

B. OPEN ISSUES AND CHALLENGES

Both, blockchain interoperability and UAV networks are still in the research and development phase. Thus, the integration of both technologies is faced with many practical problems. We devote this section to discuss challenges and possible research opportunities that may guide the future work in this topic.

a: SELECTION OF CROSS-BLOCKCHAIN TECHNOLOGY

Despite the substantial efforts dedicated to develop efficient and secure cross-blockchain interfaces [11], the selection of the most appropriate one for managing the different applications in the UAV networks is a critical design challenge. All currently available cross-blockchain platforms still suffer from either security, reliability, or efficiency issues. Consequently, it is inevitable to choose the optimum platform that minimizes the risks while maintaining satisfactory performance.

b: ABSENCE OF A MANAGING THIRD PARTY

Although the decentralized nature of peer-to-peer (P2P) networks provides enormous advantages and mitigates substantial security risks, it is, yet, vulnerable to 51% attacks [92]. This is especially intimidating in the case of UAV networks, where UAVs can join and leave freely [45]. Also, the wide availability of relatively cheap UAVs may facilitate such attacks. To tackle this issue, Dasu *et al.* [44] presented a hybrid traffic management model where parts of the airspace are managed by a centralized authority, while others are left to blockchain-based decentralized management. Further, the authors presented a novel approach to prevent denial-of-airspace attack by charging airspace users some fees based on the local demand. This will also limit 51% attacks as it makes it more expensive for malicious users to join the UAV network with many drones at a time. Another way to improve the security feature of the cross-blockchain scheme was introduced by Kim [93]–[95] where the blockchain governance game was proposed to deal with attackers who try to gain control over the blockchain by adding more illegitimate nodes.

c: LIMITED POWER

Optimizing the power consumption of UAVs is a prerequisite to enabling a variety of UAV-based applications. The vast majority of currently available drones are limited in terms of energy resources, and hence not able to satisfy the processing required by blockchain-based applications. Further, UAV can only carry limited amount of fuel or small-sized batteries which in turns limits their fly-time and computational power. On the other hand, blockchain consensus mechanisms such as the proof-of-work (PoW) drain a large amount of energy. Some studies have already addressed this issue by using the proof-of-authority or proof-of-stake mechanisms [40]. Besides, the problem of limited power was addressed by proposing an optimized UAV charging framework [96]. Others suggested an energy harvesting scheme that enables drones to extract energy from ambient resources such as radio frequency and solar energy [97]. Moreover, the issue of power efficiency might be addressed by reducing the weight of the UAV frame which is proposed in [98]. Nonetheless, more power optimization research is required to allow blockchain-based UAV applications to be practically feasible.

d: COST EFFECTIVENESS

Proposing any cross-blockchain solution in the UAV network management context shall be cost effective. That is, most of the civilian UAV-based applications are commercial and thus the successful deployment of any solution in the drone market is significantly dependent on the associated costs.

e: SIMULATION TOOLS

We emphasize the importance of developing effective simulation tools for blockchain-based UAV applications, where the computational costs, memory size, message overhead, and UAV dynamics are taken into consideration. The availability of such tools will definitely drive the development of efficient cross-blockchain solutions tailored for the unique dynamic nature of the IoD environment. Moreover, Mehta *et al.* [9] highlighted the impact of the lack of proper programming practices on the efficiency of the blockchain implementations.

f: LIMITED COMPUTATIONAL AND STORAGE RESOURCES

This is the major barrier in the application of blockchain in the UAV networks. This fact is emphasized in [8], [9], [45]. Particularly, most current consensus mechanisms are, by design, power-consuming. Also, keeping a copy of the blockchain on the UAV board requires a large memory. In fact, increasing the capacity and computational power of UAVs while minimizing power consumption is one of the most active research topics. Yet, a game-changing solution is far from being deployed. Thus, it will be helpful to implement lightweight consensus mechanism such as the one presented in [99]. Relying on edge serves for computational-intensive tasks and storage is also proposed [65]. Nonetheless, one should pay attention to the associated communication overheads and trust issues.

g: COMPATIBILITY OF BLOCKCHAIN LEDGERS

By reviewing the related literature, it had come to our notice that each research uses a different type of blockchain. The work done by [41] focused on the permissioned blockchain to ensure the authorization of blockchain miners. Yet, security vulnerabilities may arise if other blockchain ledgers in the cross-blockchain platform employ the permissionless architecture. This might lead to reducing the security level that was granted by the permissioned blockchain. In other words, certain blockchains might be implemented either as public or private, permissioned or permissionless. If combined together, the security level of the entire system will be determined by the least-secure component. Another issue that requires further research is whether or not combining different blockchain ledgers will introduce new vulnerabilities to a system.

C. FUTURE DIRECTIONS

Based on the learned lessons and open issues identified above, we present the following future directions:

- In light of the scenarios proposed in section V, future work on blockchain-based UAV networks must consider the portability of the solution and interoperability with other applications.

- To facilitate the practical implementation of these applications, optimizing a blockchain interoperability solution for UAV networks is inevitable.
- Trusted relays are one option to achieve interoperability in UAV networks if the same group of validators of the participating blockchains are involved in the relaying process.
- Blockchain of blockchains could be another option to interconnect blockchains applications that exhibit the same architecture.
- Introducing a standardized architecture for blockchain-based UAV networks may help integrating the different solutions in one interoperability framework.
- Designing a simulation tool for UAV networks is inevitable to induce more homogeneous solutions that can be integrated and inter-operated easily. Simulation tools are especially essential in the UAV context due to the many restrictions and challenges associated with performing real experimentation.

VII. CONCLUSION

The blockchain technology sees to offer promising features in many applications. In this paper we discussed different employments of the blockchain to advance the safety, cybersecurity, and reliability of UAV networks. We identified different properties that has been addressed and exploited in recent literature and concluded that the deployment of this technology is faced with many barriers such as scalability and portability. A range of cross-blockchain interoperability solutions has been proposed to improve scalability while maintaining transparency, immutability, and decentralization. Motivated by the advances in cross-blockchain solutions, we outlined multiple scenarios at which current blockchain-based UAV networks may potentially profit from the deployment of blockchain inter-operation protocols. This includes a scenario in which the functionalities of four different blockchain ledgers are combined to fulfill the purpose of a single UAV system operating under the concept of cross-blockchain. We then, highlighted the challenges associated with implementing a network of blockchains to concurrently enable multiple functionalities of UAV networks. Some of these challenges include cost, computational and storage resources, and the compatibility of different blockchain ledgers. We finally suggested possible research directions that will form the basis for future proposals to integrate cross-blockchain solutions in the IoD environment.

REFERENCES

[1] Fortune Business Insights. (Feb. 21, 2020). *Small Drones Market*. [Online]. Available: https://www.fortunebusinessinsights.com/press-release/small-drones-market-9611

[2] B. Alzahrani, O. S. Oubbati, A. Barnawi, M. Atiquzzaman, and D. Alghazzawi, "UAV assistance paradigm: State-of-the-art in applications and challenges," *J. Netw. Comput. Appl.*, vol. 166, Sep. 2020, Art. no. 102706.

[3] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of drones," *IEEE Access*, vol. 4, pp. 1148–1162, 2016.

[4] M. Y. Khan, M. F. Zuhairi, T. Ali, T. Alghamdi, and J. A. Marmolejo-Saucedo, "An extended access control model for permissioned blockchain frameworks," *Wireless Netw.*, vol. 26, no. 7, pp. 1–12, 2019.

[5] S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere, and S. P. Mohanty, "Interoperability and synchronization management of blockchain-based decentralized e-Health systems," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1363–1376, Nov. 2020.

[6] R. Neisse, J. L. Hernandez-Ramos, S. N. Matheu-Garcia, G. Baldini, A. Skarmeta, V. Siris, D. Lagutin, and P. Nikander, "An interledger blockchain platform for cross-border management of cybersecurity information," *IEEE Internet Comput.*, vol. 24, no. 3, pp. 19–29, May 2020.

[7] L. Besancon, C. F. D. Silva, and P. Ghodous, "Towards blockchain interoperability: Improving video games data exchange," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 81–85.

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

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

[10] P. Álvares, L. Silva, and N. Magaia, "Blockchain-based solutions for UAV-assisted connected vehicle networks in smart cities: A review, open issues, and future perspectives," in *Telecom*, vol. 2, no. 1. Basel, Switzerland: MDPI, Mar. 2021, pp. 108–140.

[11] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," 2020, *arXiv:2005.14282*.

[12] A. Lipton and T. Hardjono, "Blockchain intra-and interoperability," *Innov. Technol. Interface Finance Oper.*, 2021.

[13] A. Yakovenko, "Solana: A new architecture for a high performance blockchain v0.8.13," White Paper, 2018.

[14] G. Wood, "PolkaDot: Vision for a heterogeneous multi-chain framework," Parity.io, White Paper, 2016, vol. 21.

[15] *Intro to Loom Network: Loom SDK*. Accessed: Dec. 13, 2021. [Online]. Available: https://loomx.io/developers/en/intro-to-loom.html

[16] S. D. Lerner, "RSK," RootStock Core Team, White Paper, 2015.

[17] *Horizon Blockchain Games*. Accessed: Jul. 11, 2021. [Online]. Available: https://horizon.io/

[18] *Binance*. Accessed: Jul. 11, 2021. [Online]. Available: https://www.binance.com/en

[19] J. Crabb, "Interview: Coinbase legal team talk crypto," *Int. Financial Law Rev.*, Apr. 2021.

[20] *Kraken Exchange*. Accessed: Jul. 11, 2021. [Online]. Available: https://www.kraken.com/

[21] *Uniswap*. Accessed: Jul. 11, 2021. [Online]. Available: https://uniswap.org/

[22] *Lightning Network*. Accessed: Jul. 11, 2021. [Online]. Available: https://lightning.network/

[23] *Onechain*. Accessed: Jul. 11, 2021. [Online]. Available: http://www.onechain.one/index_en.html

[24] Fusion. *A Connected Ecosystem for Financial Transactions*. Accessed: Jul. 11, 2021. [Online]. Available: https://fusion.org/en

[25] *Ethereum 2.0*. Accessed: Jul. 11, 2021. [Online]. Available: https://ethereum.org/en/

[26] *Cardano*. Accessed: Jul. 11, 2021. [Online]. Available: http://www.cardano.org/

[27] J. Kwon and E. Buchman, "Cosmos whitepaper," White Paper, 2019. [Online]. Available: https://cosmos.network/resources/whitepaper

[28] (Oct. 2021). *Hyperledger: Open Source Blockchain Technologies*. [Online]. Available: https://www.hyperledger.org/

[29] *Quant*. Accessed: Jul. 11, 2021. [Online]. Available: https://www.quant.network/

[30] *Interledger*. Accessed: Dec. 13, 2021. [Online]. Available: https://interledger.org/news/attention-creatives-grant-for-the-webs-call-for-proposals-is-now-open/

[31] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille. *Enabling Blockchain Innovations With Pegged Sidechains*. vol. 72. 2014. [Online]. Available: http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains

[32] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K.-K.-R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102471.

[33] S. Schulte, M. Sigwart, P. Frauenthaler, and M. Borkowski, "Towards blockchain interoperability," in *Proc. Int. Conf. Bus. Process Manage.* Vienna, Austria: Springer, 2019, pp. 3–10.

[34] C. Decker and R. Wattenhofer, "A fast and scalable payment network with bitcoin duplex micropayment channels," in *Proc. Symp. Self-Stabilizing Syst.* Edmonton, AB, Canada: Springer, 2015, pp. 3–18.

[35] T. Hegnauer, "Design and development of a blockchain interoperability API," Ph.D. dissertation, CSG@IFI, Univ. Zurich, Zurich, Switzerland, 2019.

[36] A. Pupyshev, D. Gubanov, E. Dzhafarov, I. Sapranidi, I. Kardanov, V. Zhuravlev, S. Khalilov, M. Jansen, S. Laureyssens, I. Pavlov, and S. Ivanov, "Gravity: A blockchain-agnostic cross-chain communication and data oracles protocol," 2020, *arXiv:2007.00966*.

[37] T. Hardjono, A. Lipton, and A. Pentland, "Toward an interoperability architecture for blockchain autonomous systems," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1298–1309, Nov. 2020.

[38] M. Gusenbauer, "Google Scholar to overshadow them all? Comparing the sizes of 12 academic search engines and bibliographic databases," *Scientometrics*, vol. 118, no. 1, pp. 177–214, Nov. 2018.

[39] M. Khabsa and C. L. Giles, "The number of scholarly documents on the public web," *PLoS ONE*, vol. 9, no. 5, May 2014, Art. no. e93949.

[40] M. Scarlato, C. Perra, M. Y. Jabarulla, G. Jung, and H. N. Lee, "A blockchain for the collision avoidance and the recovery of crashed UAVs," *Korean Soc. Electron. Eng.*, pp. 463–467, 2019.

[41] M. S. Rahman, I. Khalil, and M. Atiquzzaman, "Blockchain-powered policy enforcement for ensuring flight compliance in drone-based service systems," *IEEE Netw.*, vol. 35, no. 1, pp. 116–123, Jan. 2021.

[42] A. Kuzmin and E. Znak, "Blockchain-base structures for a secure and operate network of semi-autonomous unmanned aerial vehicles," in *Proc. IEEE Int. Conf. Service Oper. Logistics, Informat. (SOLI)*, Jul. 2018, pp. 32–37.

[43] A. Allouch, O. Cheikhrouhou, A. Koubâa, K. Toumi, M. Khalgui, and T. N. Gia, "UTM-chain: Blockchain-based secure unmanned traffic management for Internet of Drones," *Sensors*, vol. 21, no. 9, p. 3049, Apr. 2021.

[44] T. Dasu, Y. Kanza, and D. Srivastava, "Geofences in the sky: Herding drones with blockchains and 5G," in *Proc. 26th ACM SIGSPATIAL Int. Conf. Adv. Geogr. Inf. Syst.*, Nov. 2018, pp. 73–76.

[45] Y. Wu, H.-N. Dai, H. Wang, and K.-K. R. Choo, "Blockchain-based privacy preservation for 5G-enabled drone communications," 2020, *arXiv:2009.03164*.

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

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

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

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

[50] A. Islam and S. Y. Shin, "BUAV: A blockchain based secure UAV-assisted data acquisition scheme in Internet of Things," *J. Commun. Netw.*, vol. 21, no. 5, pp. 491–502, Oct. 2019.

[51] M. Singh, G. S. Aujla, and R. S. Bali, "A deep learning-based blockchain mechanism for secure Internet of Drones environment," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4404–4413, Jul. 2021.

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

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

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

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

[56] A. Ossamah, "Blockchain as a solution to drone cybersecurity," in *Proc. IEEE 6th World Forum Internet Things (WF-IoT)*, Jun. 2020, pp. 1–9.

[57] A. Kumari, R. Gupta, S. Tanwar, and N. Kumar, "A taxonomy of blockchain-enabled softwarization for secure UAV network," *Comput. Commun.*, vol. 161, pp. 304–323, Sep. 2020.

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

[59] N. Andola, V. K. Yadav, S. Venkatesan, and S. Verma, "SpyChain: A lightweight blockchain for authentication and anonymous authorization in IoD," *Wireless Pers. Commun.*, vol. 119, pp. 1–20, Feb. 2021.

[60] V. Hassija, V. Chamola, D. N. G. Krishna, and M. Guizani, "A distributed framework for energy trading between UAVs and charging stations for critical applications," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5391–5402, May 2020.

[61] L. Jiang, B. Chen, S. Xie, S. Maharjan, and Y. Zhang, "Incentivizing resource cooperation for blockchain empowered wireless power transfer in UAV networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15828–15841, Dec. 2020.

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

[63] N. Pathak, A. Mukherjee, and S. Misra, "AerialBlocks: Blockchain-enabled UAV virtualization for industrial IoT," *IEEE Internet Things Mag.*, vol. 4, no. 1, pp. 72–77, Mar. 2021.

[64] K. Gai, Y. Wu, L. Zhu, K.-K.-R. Choo, and B. Xiao, "Blockchain-enabled trustworthy group communications in UAV networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4118–4130, Jul. 2021.

[65] Y. Wu, H.-N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2300–2317, Feb. 2021.

[66] V. Hassija, V. Saxena, and V. Chamola, "A blockchain-based framework for drone-mounted base stations in tactile Internet environment," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 261–266.

[67] C. Feng, K. Yu, A. K. Bashir, Y. D. Al-Otaibi, Y. Lu, S. Chen, and D. Zhang, "Efficient and secure data sharing for 5G flying drones: A blockchain-enabled approach," *IEEE Netw.*, vol. 35, no. 1, pp. 130–137, Jan. 2021.

[68] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K.-K.-R. Choo, "Neural-blockchain-based ultrareliable caching for edge-enabled UAV networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5723–5736, Oct. 2019.

[69] M. Aloqaily, O. Bouachir, A. Boukerche, and I. Al Ridhawi, "Design guidelines for blockchain-assisted 5G-UAV networks," 2020, *arXiv:2007.15286*.

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

[71] R. Agrawal, P. Verma, R. Sonanis, U. Goel, A. De, S. A. Kondaveeti, and S. Shekhar, "Continuous security in IoT using blockchain," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2018, pp. 6423–6427.

[72] S. Misra and A. Chakraborty, "QoS-aware dispersed dynamic mapping of virtual sensors in sensor-cloud," *IEEE Trans. Services Comput.*, vol. 14, no. 6, pp. 1970–1980, Nov. 2021.

[73] J. Poon and V. Buterin, "Plasma: Scalable autonomous smart contracts," Plasma.io, White Paper, 2017, pp. 1–47.

[74] D. Ding, T. Duan, L. Jia, K. Li, Z. Li, and Y. Sun, "Interchain: A framework to support blockchain interoperability," in *Proc. 2nd Asia–Pacific Work. Netw.*, 2018, pp. 1–2.

[75] L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, L. C. Gao, and H. Kai, "A multiple blockchains architecture on inter-blockchain communication," in *Proc. IEEE Int. Conf. Softw. Qual., Rel. Secur. Companion (QRS-C)*, Jul. 2018, pp. 139–145.

[76] P. Bennink, L. V. Gijtenbeek, O. V. Deventer, and M. Everts, "An analysis of atomic swaps on and between ethereum blockchains using smart contracts," OS3, Tech. Rep., 2018.

[77] H. Wang, D. He, X. Wang, C. Xu, W. Qiu, Y. Yao, and Q. Wang, "An electricity cross-chain platform based on sidechain relay," *J. Phys., Conf. Ser.*, vol. 1631, no. 1. Bristol, U.K.: IOP Publishing, Sep. 2020, Art. no. 012189.

[78] J. Rueegger and G. S. Machado, "Rational exchange: Incentives in atomic cross chain swaps," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2020, pp. 1–3.

[79] E. Abebe, D. Behl, C. Govindarajan, Y. Hu, D. Karunamoorthy, P. Novotny, V. Pandit, V. Ramakrishna, and C. Vecchiola, "Enabling enterprise blockchain interoperability with trusted data transfer (industry track)," in *Proc. 20th Int. Middleware Conf. Ind. Track*, Dec. 2019, pp. 29–35.

[80] E. Fynn, A. Bessani, and F. Pedone, "Smart contracts on the move," in *Proc. 50th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2020, pp. 233–244.

[81] M. Spoke, "AION: Enabling the decentralized internet," AION, Nuco, Amazon AWS, Seattle, WA, USA, White Paper, Jul. 2017.

[82] M. Sigwart, P. Frauenthaler, C. Spanring, M. Sober, and S. Schulte, "Decentralized cross-blockchain asset transfers," 2020, *arXiv:2004.10488*.

[83] M. Borkowski, C. Ritzer, D. McDonald, and S. Schulte, "Caught in chains: Claim-first transactions for cross-blockchain asset transfers," Technische Universität Wien, Vienna, Austria, Tech. Rep., 2018.

[84] S. Cao, J. Wang, X. Du, X. Zhang, and X. Qin, "CEPS: A cross-blockchain based electronic health records privacy-preserving scheme," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.

[85] H. Qiu, X. Wu, S. Zhang, V. C. M. Leung, and W. Cai, "ChainIDE: A cloud-based integrated development environment for cross-blockchain smart contracts," in *Proc. IEEE Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, Dec. 2019, pp. 317–319.

[86] M. Nissl, E. Sallinger, S. Schulte, and M. Borkowski, "Towards cross-blockchain smart contracts," 2020, *arXiv:2010.07352*.

[87] *Decentralized Identifiers (DIDS) V1.0*. [Online]. Available: https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers

[88] B. G. Kim, Y.-S. Cho, S.-H. Kim, H. Kim, and S. S. Woo, "A security analysis of blockchain-based did services," *IEEE Access*, vol. 9, pp. 22894–22913, 2021.

[89] B. Alzahrani, "An information-centric networking based registry for decentralized identifiers and verifiable credentials," *IEEE Access*, vol. 8, pp. 137198–137208, 2020.

[90] R. Chen, F. Shu, S. Huang, L. Huang, H. Liu, J. Liu, and K. Lei, "BIdM: A blockchain-enabled cross-domain identity management system," *J. Commun. Inf. Netw.*, vol. 6, no. 1, pp. 44–58, 2021.

[91] M. J. Amiri, D. Agrawal, and A. El Abbadi, "CAPER: A cross-application permissioned blockchain," *Proc. VLDB Endowment*, vol. 12, no. 11, pp. 1385–1398, 2019.

[92] M. Saad, J. Spaulding, L. Njilla, C. A. Kamhoua, D. Nyang, and A. Mohaisen, "Overview of attack surfaces in blockchain," in *Blockchain for Distributed Systems Security*. Hoboken, NJ, USA: Wiley, 2019, pp. 51–66.

[93] S.-K. Kim, "The trailer of strategic alliance for blockchain governance game," 2019, *arXiv:1903.11172*.

[94] S.-K. Kim, "Enhanced IoV security network by using blockchain governance game," *Mathematics*, vol. 9, no. 2, p. 109, Jan. 2021.

[95] S.-K. Kim, C. Y. Yeun, E. Damiani, Y. Al-Hammadi, and N.-W. Lo, "New blockchain adoptation for automotive security by using systematic innovation," in *Proc. IEEE Transp. Electrific. Conf. Expo, Asia–Pacific (ITEC Asia–Pacific)*, May 2019, pp. 1–4.

[96] V. Hassija, V. Saxena, and V. Chamola, "Scheduling drone charging for multi-drone network based on consensus time-stamp and game theory," *Comput. Commun.*, vol. 149, pp. 51–61, Jan. 2020.

[97] T. Quyen, C. Nguyen, A. Le, and M. Nguyen, "Optimizing hybrid energy harvesting mechanisms for UAVs," *EAI Endorsed Trans. Energy Web*, vol. 7, no. 30, 2020, Art. no. 164629.

[98] N. Sagar, B. Esakki, C. Udayagiri, and K. Vepa, "Multistage mass optimization of a quadcopter frame," in *Innovative Design, Analysis and Development Practices in Aerospace and Automotive Engineering*. Singapore: Springer, 2021, pp. 181–188.

[99] Z. Su, Y. Wang, Q. Xu, and N. Zhang, "LVBS: Lightweight vehicular blockchain for secure data sharing in disaster rescue," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 1, pp. 19–32, Jan./Feb. 2020.

RUBA ALKADI received the B.Sc. degree in electrical engineering from the American Univesrity of Sharjah, Sharjah, UAE, in 2016, and the M.Sc. (by research) degree in engineering from Khalifa University, Abu Dhabi, UAE, in 2018. She is currently a Research Associate with the Center of Cyber-Physical Systems, Khalifa Univesrsity. Her research interests include unmanned aerial vehicles traffic management, machine learning, blockchain, and image processing.

NOURA ALNUAIMI received the B.Sc. degree in computer engineering from the Khalifa University of Science and Technology, Abu Dhabi, where she is currently pursuing the M.Sc. degree in cybersecurity. She is also working as a Research/Teaching Assistant with Khalifa University. Her research interests include blockchain technology and artificial intelligence (AI) techniques for cybersecurity.

CHAN YEOB YEUN (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in information security from Royal Holloway and the University of London, in 1996 and 2000, respectively. After his Ph.D. degree, he joined Toshiba TRL, Bristol, U.K., and later became the Vice President of LG Electronics, Mobile Handset Research and Development Center, Seoul, South Korea, in 2005, where he was responsible for developing mobile TV technologies and related security. He left LG Electronics in 2007 and joined KAIST, South Korea, until August 2008 and then the Khalifa University of Science and Technology, in September 2008. He is currently a researcher in cybersecurity including the IoT/USN security, cyber-physical system security, cloud/fog security, and cryptographic techniques as an Associate Professor with the Department of Electrical Engineering and Computer Science and an active Cybersecurity Leader of Center for Cyber-Physical Systems (C2PS). He also enjoys lecturing M.Sc. information security and Ph.D. engineering courses at Khalifa University. He has published more than 140 journal articles and conference papers, nine book chapters, and ten international patent applications. He also serves on the editorial board of multiple international journals and on the steering committee of international conferences.

ABDULHADI SHOUFAN received the Dr.-Ing. degree from Technische Universität Darmstadt, Germany, in 2007. He is currently an Associate Professor in information security and electrical and computer engineering and a member of the Center of Cyber-Physical Systems, Khalifa University, Abu Dhabi. His research interests include drones' security and safe operation, embedded security, learning analytics, and engineering education.