BRL Working Paper Series No. 32

Blockchain and Unmanned Aerial Vehicles: A Bibliometric Analysis and Research Agenda

Fred Steinmetz [1, *], Friedrich-Philipp Wazinski [1], Lennart Ante [1,2]

1) Blockchain Research Lab, Weidestraße 120b, 22083 Hamburg, Germany
2) Constructor University, School of Business, Social & Decision Sciences, Germany

* Correspondence: steinmetz@blockchainresearchlab.org

Abstract: The convergence of blockchain technology and unmanned aerial vehicles (UAVs) has garnered significant attention due to its potential to enhance security, automation, and data management in UAV ecosystems. However, the ongoing growth of research in this domain necessitates a systematic analysis to delineate its intellectual structure and development trajectories. This study employs bibliometric techniques, specifically co-citation analysis and exploratory factor analysis (EFA), to identify and analyze key research streams at the intersection of blockchain and UAV technologies. Based on a dataset of 340 peer-reviewed publications retrieved from Web of Science, the analysis reveals six distinct research streams: (I) privacy and security in the Internet of Drones (IoD), (II) implications of combining emerging technologies, (III) federated learning, (IV) resource and data management in IoT, (V) optimization, security, and applications in UAV-enabled mobile edge computing (MEC) systems, and (VI) blockchain-enabled data sharing and automation in the IoD. These findings highlight blockchain's role in securing UAV communication, optimizing resource management, and enabling decentralized automation. Despite these advancements, challenges related to scalability, computational efficiency, and interoperability persist, with limited empirical validation of proposed frameworks. This study provides a structured overview of the evolving research landscape, offering insights for future investigations and interdisciplinary collaborations aimed at addressing these challenges. Building on the identified research streams, this study proposes a research agenda that highlights unresolved challenges and critical gaps—such as lightweight consensus protocols, privacy-preserving federated learning, efficient resource allocation, and integration with emerging technologies—thereby advancing the secure and efficient integration of blockchain and UAV technologies across diverse applications.

Keywords: Blockchain; UAVs; drones; distributed ledger; bibliometrics; review;

1 Introduction

Integrating blockchain technology with unmanned aerial vehicle (UAV) systems, commonly referred to as drones, has emerged as a frontier of innovation in academic research and practical applications in recent years. Blockchain technology, renowned for its robust security features, decentralized infrastructure, and immutability, offers significant enhancements in the operation and management of UAVs. These enhancements include improved data security, process automation via smart contracts, and transparent maintenance logs critical in delivery services, surveillance, and agriculture. This enables blockchain-specific use cases such as traffic monitoring (Allouch et al. 2021), the management of drone swarms (Xu et al. 2021), decentralized data storage in UAVs (Alladi et al. 2020), or the implementation of drone-based federated learning systems (Alsamhi et al. 2022; Wang et al. 2021). While these applications demonstrate the promise of blockchain in UAV systems, the field remains fragmented, with several crucial research challenges yet to be systematically addressed.

The rapidly expanding corpus of literature on the intersection of blockchain and UAVs reflects its growing technological and societal implications. However, the sheer volume and diversity of research make it challenging to discern the development trajectories and thematic pillars that define this interdisciplinary field. This necessitates a structured examination to navigate the complexities and uncover the core themes shaping this area of study. Only a few studies employ a systematic review or survey approach to investigate this convergence. Harbi et al. (2023a) focus on security schemes within the framework of the Internet of Drones (IoD), with a specific emphasis on the utilization of blockchain technology, and Mehta et al. (2020) present a taxonomy that aims to classify and organize the various security concerns that arise in the realm of blockchain-based UAV networks. Finally, Alladi et al. (2020) provide a thorough analysis of the application areas in which blockchain technology is implemented within networks of UAVs, and Billah et al. (2022a) present a holistic viewpoint on blockchain-based federated learning frameworks in the context of the Internet of Vehicles (IoV), thereby not explicitly focusing on UAVs. In addition to consolidating past contributions, it is equally important to chart directions for future inquiry, particularly in areas where current approaches remain conceptual, resource-intensive, or technically constrained.

Despite these foundational contributions, the existing literature has not adequately explored the underlying intellectual structure of the convergence between UAVs and blockchain technology. The need to systematically identify and analyze the principal research streams and themes within the field is critical for developing a cohesive understanding that can inform future academic inquiries and practical implementations. This paper addresses this gap by employing bibliometric techniques—specifically co-citation analysis and exploratory factor analysis (EFA)—to dissect and delineate the intellectual contours of the nexus between blockchain and UAVs. Beyond mapping the key scholarly networks, influential works, and thematic clusters, the study contributes a forward-looking research agenda that highlights underexplored areas crucial for advancing the field. These include blockchain-enabled security and privacy frameworks, blockchain-integrated federated learning, efficient resource and computing management, and the integration of blockchain with emerging technologies such as AI, IoT, and next-generation networks to support autonomous UAV operations.

Our bibliometric approach is structured as follows: Initially, we extract 340 peer-reviewed articles on blockchain and UAVs using Web of Science as a data basis. Relying on this primary literature dataset, we generate a secondary dataset based on co-citations, which forms the base for our empirical analysis. We then apply EFA to group-related research based on co-citation patterns, thus identifying the main intellectual currents within the field. Network and density analysis are employed to unveil the relationships and influence among these identified research clusters. The results from our analyses aim to provide a detailed map of the intellectual landscape, highlighting how blockchain technologies are being integrated with UAV systems in various domains.

Ultimately, our approach not only enriches understanding of the current research dynamics but also identifies under-researched domains that form the basis for the proposed research agenda. By articulating key directions for future inquiry, this study aims to catalyze further research and collaboration, thereby advancing both the theoretical and practical aspects of blockchain–UAV integration. This is essential for stakeholders in academia, industry, and policy-making to harness the

full potential of these technologies, ensuring that their convergence leads to innovative, secure, and efficient UAV applications.

2 Data and methods

2.1 Primary dataset

For this study, the literature data was sourced from Web of Science, an extensively utilized, comprehensive database that supports the systematic identification and extraction of scholarly articles. This database offers the systematic querying of specific search terms and more complex search strings focusing on peer-reviewed publications. Web of Science further provides useful metadata, such as the references cited in each article, which lays the foundation for advanced bibliometric analysis. A limitation is the potential of missing recent and non-peer-reviewed contributions that could be relevant to the specific search but have not been peer-reviewed or indexed already.

In February 2023, we identified 340 peer-reviewed publications. The search terms used were *TS=((blockchain* OR "distributed ledger*" OR "smart contract*") AND (drone* OR "unmanned aerial vehicle*"))*, where the asterisk (*) denotes a wildcard character, capturing variations of the root word (e.g., drones, droning). The terms "blockchain" represent the technological aspect, while "UAV" and "drone" pertain to the application in unmanned aerial systems. While the Web of Science database does not encompass every publication on the intersection of blockchain technology and UAVs, the dataset obtained is presumed to contain a sufficiently large and representative sample for effective bibliometric and co-citation analysis. It is important to note that bibliometric data are often skewed, with a small number of highly cited publications disproportionately influencing the field. This skewness, recognized in the laws of information science by scholars such as Lotka (1926), Bradford (1985), and Zipf (1949) underscores that our analysis, focused on underlying references within the selected publications, captures the most significant contributions to the scholarly discourse on this topic.

2.2 Secondary dataset and co-citation analysis

Co-citation analysis is instrumental in understanding the relationships and thematic overlaps between publications by examining how frequently two articles are cited together. This approach posits that a high frequency of co-citations between two documents indicates their importance and relevance to a specific scientific discourse, as they often form the foundation upon which subsequent authors build their scholarly arguments (Small, 1973). Analyzing clustered co-citation data allows for the exploration of the intellectual structure of a field, revealing core themes and influential research (White and Griffith, 1981).

The primary dataset from the Web of Science database collectively references 28,417 unique citations. Of these, 3,120 citations appeared more than once across different articles, making them suitable candidates for co-citation analysis. To manage the complexity (Zupic and Čater, 2015) and skewness of data (Chen and Leimkuhler, 1986), we applied a threshold value of three to identify significant co-citations. This threshold was established based on an 'elbow criterion' derived from the distribution of co-citation frequencies, a method consistent with standard bibliometric practices (Small, 2006). The point where the curve begins to flatten (the elbow) was identified by examining the frequency distribution curve, and a threshold of five co-citations was set. This resulted in a refined set of 272 highly co-cited references.

These 272 references were then used to construct a symmetric co-citation matrix, which includes one row and one column for each of the 272 publications. Each cell in this matrix represents the frequency of co-citation between the pair of articles denoted by the respective row and column. This matrix serves as the foundation for our subsequent factor analysis (White and McCain, 1998), facilitating a deeper understanding of the interconnectedness and thematic clustering within the literature on blockchain and UAV integration.

2.3 Exploratory factor analysis for co-citation analysis

EFA is a statistical method used to reduce the dimensionality of large datasets by identifying latent variables, or factors, that explain patterns of correlations within a set of observed variables. In the context of our bibliometric study, this technique is applied to the symmetric co-citation matrix to group articles into distinct factors that represent underlying research streams within blockchain and UAV technologies.

Using EFA, articles are clustered based on their co-citation relationships, suggesting that they address similar themes or belong to the same conceptual framework. The primary outputs from this analysis are factor loadings and factor scores. Factor loadings are correlation coefficients that measure how strongly each article (variable) is associated with each factor (research stream). These loadings range from -1 to 1 and undergo a Varimax rotation to maximize the variance of squared loadings, which aids in clearer interpretation (Gorsuch, 1988). A common threshold in bibliometric studies is a factor loading of 0.4, indicating that an article significantly contributes to a research stream. Articles with loadings above 0.7 are considered highly representative of their respective streams (McCain, 1990).

Factor scores, on the other hand, provide a metric to assess the relative importance of each article within a particular factor. These scores are calculated via regression analysis and help rank the articles regarding their contribution to the identified research streams. It is important to note that a high factor score does not necessarily mean a substantial contribution to the stream's literature volume; for instance, review articles may score highly due to their comprehensive coverage but may not contribute new research or insights.

To ensure the relevance and cohesion of the factors, articles with low communalities (below 0.5), indicating weak associations with any factor, are progressively removed from the analysis. This pruning process is crucial to maintain the integrity and interpretability of the resulting research streams. Following this methodology, the EFA yielded 258 articles that effectively represent the intellectual structure of blockchain applications in UAV technology. The identified factors—or research streams—are subsequently named based on a qualitative review of the content of the core articles within each stream. While somewhat subjective, this naming process is informed by an in-depth examination of the themes and focus areas of the articles that compose each factor, ensuring that the labels accurately reflect the underlying scholarly discourse.

3 Findings on the Discourse and Individual Research Streams

Based on the aforementioned methodology and data, six research streams have been identified, explaining a combined 49.6% of the variance. Table 1 provides the interpretation of the results of the exploratory factor analysis based on co-citation data. Each stream represents a factor with an Eigenvalue >1. To be part of a factor, articles required a factor loading (FL) of 0.4 or higher, whereas a FL of 0.7 or higher indicates the highest (intellectual) fit. The variance indicates the degree to which a specific research stream contributes to the broader field of blockchain and UAVs. The identified research streams are ordered according to their share of the explained variance and thus indicate their different weights of importance for the academic discourse on the intersection of blockchain technology and UAVs.

The primary subjects of research structured in the identified streams comprise IoD-centric topics such as privacy and security prerequisites and issues (Stream I, V and VI), harnessing novel technology to improve existing areas of practice beyond UAV systems (Stream II), federated learning (Stream III) as well as optimization in restricted resource allocation scenarios (Stream IV and V) and data management (Stream V).

There a several ways the topics of the regarded research streams can be categorized on a higher level: Some streams exhibit a strong focus on drones and UAV systems, whereas others do not. While, for example, federated learning (Stream III) is a concept not solely applicable in the context of UAV communication and coordination, other streams' tenor is about the explicit advancement of current UAV systems, e.g., security and confidentiality aspects (Stream I) or optimizations in resource-

constrained UAV use cases (Stream V). Another way to categorize the identified streams is according to the relevance of blockchain technology. The majority of the identified streams exhibit a strong blockchain focus, where the overarching topic discusses, conceptualizes or tests blockchain technology implementations and scenarios (Stream I, II, III, IV, VI). In contrast, solely Stream V focuses on fundamental issues of mobile edge computing in UAV systems, where blockchain technology is not considered.

Table 1. *Overview of research streams on the intersection of blockchain technology and UAVs.*

Research Stream	Variance explained	# articles	% articles	FL > 0.4	FL > 0.7	Summary
Stream I: Privacy and Security in IoD	15.7%	65	22%	15.6%	9.9%	Blockchain and encryption enabled drone authentication and communication
Stream II: Implications of combining emerging technologies	11.7%	46	16%	9.2%	6.5%	Leveraging emerging technologies for enhanced security, privacy, and efficiency in multiple sectors
Stream III: Federated Learning	8.8%	37	13%	6.8%	5.8%	Synergies of blockchain technology and federated learning Fundamentals of federated learning
Stream IV: Resource and Data Management in IoT	5.3%	31	11%	7.8%	2.7%	Resource and data management in IoT Blockchain usage for energy and CPU optimization and data management
Stream V: Optimization, Security and Applications in UAV-Enabled Mobile Edge Computing Systems	4.9%	25	9%	5.4%	3.1%	UAV-enabled mobile edge system optimization Computation offloading in MEC systems
Stream VI: Blockchain-enabled data sharing and automation on the Internet of Drones	3.2%	15	5%	3.1%	2.0%	IoD-centric data sharing, authentication and automation using blockchain technology

The temporal development of the research relevant to the intersection of blockchain and UAVs by each stream, visualized in Figure 1, exhibits a significant uptrend in the number of published articles over the past years. Particularly interesting is the surge in articles from 2018 to 2019, with a remarkable increase in volume across all streams. The largest increase in absolute terms between 2018 and 2019 can be found in research covering the implications of combining novel technologies (Stream II) from four articles in 2018 to 18 articles in 2019. The absolute numbers of the articles in each stream and in total, however, underscore that the scientific exploration of the intersection between blockchain technology and UAVs as a whole is still a niche, albeit its apparent growth. In 2020, the total number of articles retained at a high level above 60, before declining to 37 in 2021.

On a relative base, Figure 2 showcases that the streams with growth momentum leading into 2022 span the issues of privacy and security in IoD (Stream I) and blockchain-enabled data sharing and automation on the IoD (Stream VI). In contrast, the topic of federated learning (Stream III) stagnates and the other streams appear to lose relevance over time. Particularly interesting is the loss of relevancy for Stream V about optimizations in MEC environments, which has represented 35% of articles in the research area and has faded almost into irrelevance by 2021. Similarly, research exploring and identifying the potential of new technologies (Stream II) has been important at the time the technology was actually emerging, and many researchers explored blockchain implementations across sectors and in combination with other technologies. Meanwhile, such explorative research has lost significant relevance to the literature on the topic of blockchain and UAVs, indicating that the potential of the technologies' combination has been wholly explored and understood.

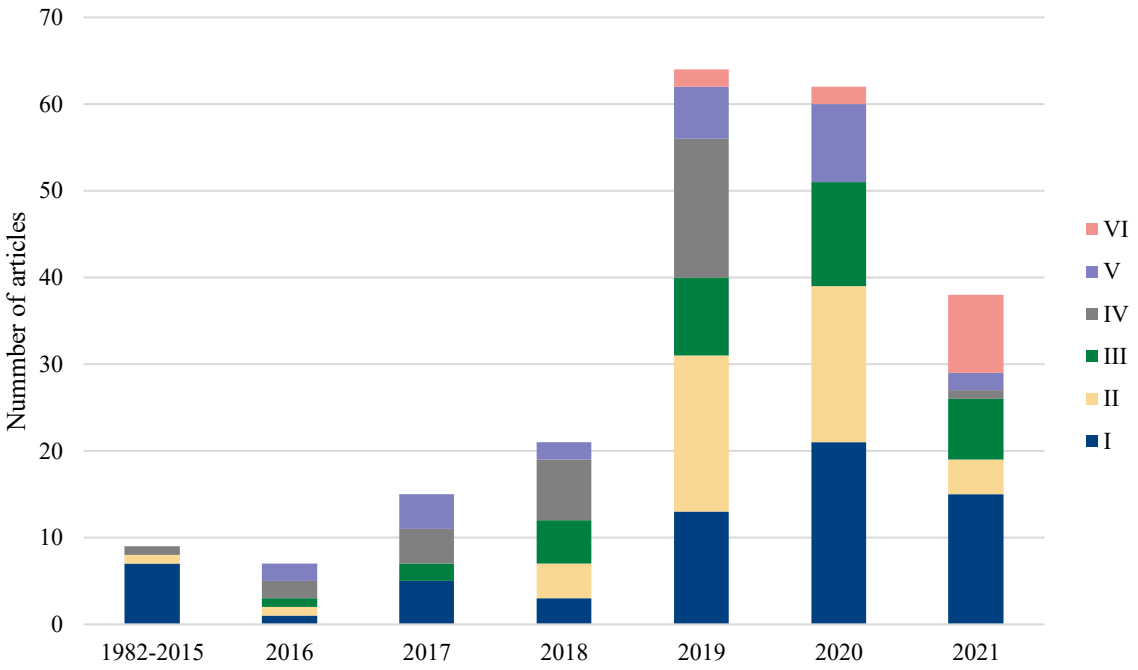

Figure 1. *Temporal development of the scientific literature on blockchain and UAVs in absolutes by research stream from pre-2016 to 2021.*

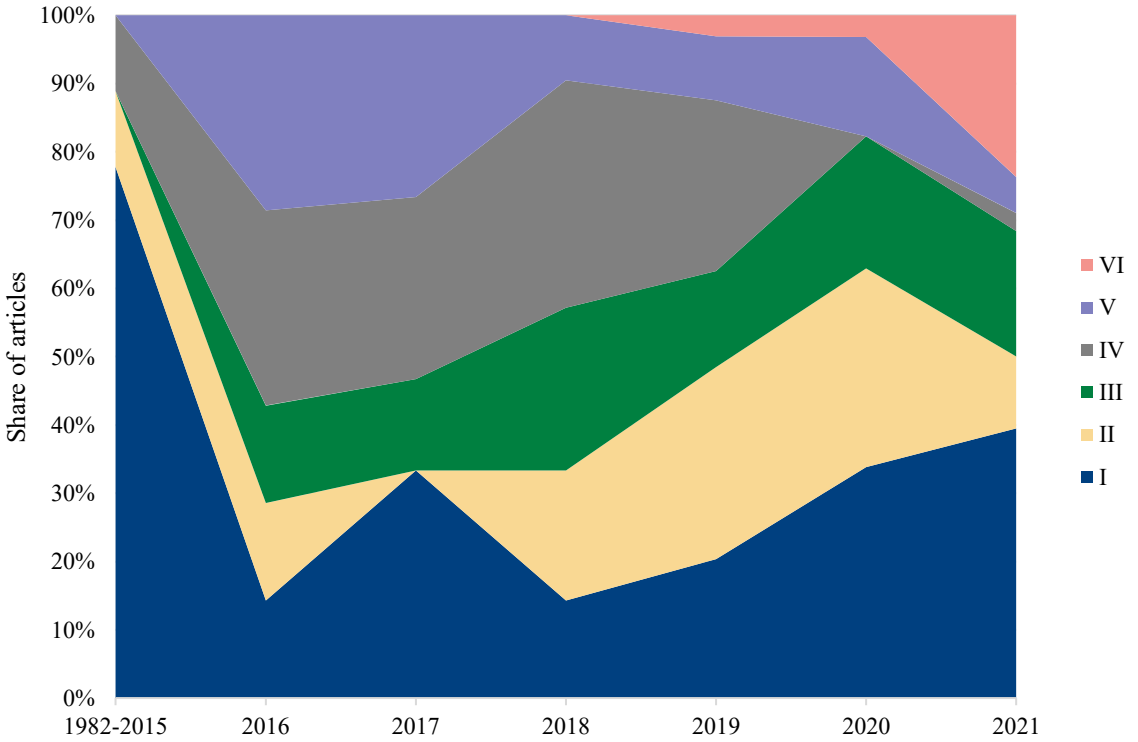

Figure 2. *Temporal development of the scientific literature on blockchain and UAVs in relation to research stream from pre-2016 to 2021.*

3.1 Research Stream I: Privacy and Security in Internet of Drones

Research Stream I comprises 71 publications, making up 24% of the dataset's total. Among these, 30 papers exhibit a factor loading above 0.7. Table 2 displays the 15 articles with the highest factor loadings and two further high-impact articles that exhibit high factor scores albeit lower factor loadings. In its entirety, research stream I constitutes 15.7% of the explained variance—arguably representing a major subject in the topical discourse.

Publications assigned to Stream I deal with the development of privacy and security frameworks in the context of the IoD. These frameworks address the securitization of communication and data transmission between UAVs, among UAVs and terrestrial vehicles, and among UAVs and ground-based server stations (GSS). Prominent issues addressed include vulnerabilities in relation to authentication, position and trajectory data disclosure, drone hijacking, and identity breaches. In accordance, Stream I is entitled *Privacy and Security in the Internet of Drones.*

Table 2. Key publications in Stream I.

Publication	Factor loading	Factor score
Ever (2020)	0.94	4.13
Hussain et al. (2021)	0.92	2.29
Zhang et al. (2020)	0.91	3.79
Nikooghadam et al. (2021)	0.91	2.67
Pu and Li (2020)	0.90	2.19
Gope and Sikdar (2020)	0.88	2.18
Boccadoro et al. (2021)	0.86	2.73
Yahuza et al. (2021)	0.86	1.97
Bera et al. (2021)	0.86	2.96
Wazid et al. (2019)	0.85	2.68
Bera et al. (2020)	0.85	4.42
Tian et al. (2019)	0.85	4.38
Bera et al. (2020)	0.84	4.01
Srinivas et al. (2019)	0.84	3.63
Ali et al. (2020)	0.83	2.12
…	…	…
Gharibi et al. (2016)	0.79	3.85
Alsamhi et al. (2019)	0.65	2.67
Other: 15 publications with FL > 0.7		

The study employed principal component analysis (PCA) and Varimax rotation technique, incorporating Kaiser normalization (KMO). KMO value indicated: 0.606; Bartlett test yielded a p-value less than .001.

The research stream under consideration is profoundly influenced by Bera et al.'s (2020) publication, as evidenced by the significant factor score of 4.42. The study introduced an access control framework that leverages blockchain technology for enhanced security. The proposed scheme enables peer-to-peer access control within a cloud server network for inter-drone and drone-to-GSS communication. The framework incorporates the Ripple Protocol Consensus Algorithm (RPCA) to prevent a range of security threats, such as replay attacks, man-in-the-middle attacks, mutual authentication, key agreement, and drone impersonation attacks.

Besides authoring the most influential publication for the stream, the factor scores of Bera et al. (2020) and Bera et al. (2021) indicate the author's weight in this stream. Bera et al. (2020) introduced the BS2D2C-IoD scheme, leveraging blockchain technology to secure data exchange in IoD environments, facilitated by 5G technology. The scheme conceptualizes secure transactions between drones and GSS as well as control rooms. Bera et al. (2021) present the ACSUD-IoD framework, an access control scheme aimed at detecting and mitigating unauthorized UAV activities in an IoD setting. Similar to

Bera et al. (2020), this framework integrates blockchain technology and employs a Byzantine fault tolerance consensus algorithm.

The tenor of this stream's publications focuses on the topic of authentication schemes for UAVs and the preservation of confidential information in authentication processes. Ever (2020) stands as a pivotal publication for the research stream with the highest factor loading of 0.94. It introduced a lightweight authentication protocol using elliptic curve cryptography (ECC) and a hierarchical architecture for use in scenarios where UAVs serve as mobile sinks within wireless sensor networks (WSNs). Tian et al. (2019), with a factor score of 4.38, proposed an authentication framework that prioritizes privacy preservation in edge-assisted IoD applications. The architecture proposed employs lightweight online/offline signature design, a buffer pseudonym, and a public key update strategy, ensuring UAV anonymity and secure anticipatory authentication. Similarly, Hussain et al. (2021) and Nikooghadam et al. (2021) put forth ECC-based schemes for secure UAV authorization in smart city environments. Yahuza et al. (2021) addressed the balance between security and lightweight design by using the Brainpoolp256r1-elliptic curve in their secure lightweight authentication key agreement scheme, SLAPAKA. The mutual authentication protocol (PCAP) of Pu and Li (2020) employs challenge-response pairs of physical unclonable functions (PUF), serving as a secure communication protocol between UAVs and ground stations. Likewise, Gope and Sikdar (2020) proposed an authentication key agreement scheme that combines double-PUF and hash function-based techniques for edge-assisted UAV environments. The authentication and key agreement scheme proposed by Wazid et al. (2019) employs hash functions, one-way cryptographic hash functions, XOR operations, fuzzy extractor method, and biometrics to establish a secure communication channel between users and drones.

In summary, Research Stream I publications primarily address privacy and security issues in the context of IoD, focusing on secure communication, authentication, and key agreement. These studies propose a variety of schemes that aim to balance security with lightweight characteristics, employing technologies such as blockchain, ECC, and PUF.

3.2 Research Stream II: Implications of combining emerging technologies

The second research stream encompasses 47 publications, representing 15.9% of the dataset. Table 3 presents a record of 15 publications that demonstrate the greatest factor loading, along with two other publications that exhibit high factor scores. The research stream under consideration displays the second-highest explained variance among the research streams, with an explained variance of 11.73%. Thematically, the discussion in Stream II revolves around cutting-edge technologies such as artificial intelligence (AI), blockchain, tactile internet, and smart vehicle networks. Specifically, the discourse places an emphasis on security and privacy-related issues with reference to the integration of novel technologies. Thus, the stream can be referred to as *Implications of combining emerging technologies*.

The most important publication in this stream is Gupta et al.'s (2020a) "Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools, Techniques and Challenges". Exhibiting the highest factor score and factor loading in Stream II suggests a strong relationship between the publication and the research stream, while also providing the best thematic fit. In the context of blockchain technology's potential for integration into cyber-physical systems, the authors conduct a thorough investigation into the privacy and security vulnerabilities that are inherent in smart contract code. Specifically, their study focuses on logical vulnerabilities, structural vulnerabilities, and testing procedures. The scientific endeavor of the study pertains to the meticulous examination of AI integration techniques that ensure privacy preservation, with a primary objective of enhancing privacy and security in smart contracts. The study stands exemplary for the studies in this stream, focusing on the combination of recent advancements and novel technologies, e.g., combining Cyber-physical systems, blockchain technology, and AI.

Sheth et al. (2020) explore the potential uses of artificial intelligence in various areas such as object localization, UAV communication, surveillance, security, and privacy protection in communication technologies enabled by sixth-generation (6G) networks. The authors propose a multilayered architecture for 6G that incorporates AI capabilities. Tanwar et al. (2019) present a taxonomy that centers on four dimensions pertaining to the incorporation of machine learning in blockchain-based

smart applications. This research offers a comparative evaluation of machine learning techniques in the context of blockchain technology, with a particular focus on their efficacy in achieving specific objectives, enabling intelligent applications, facilitating layer-based operations, and implementing countermeasures. Similarly, Bhattacharya et al. (2021) and Hathaliya et al. (2019) research incorporates blockchain and machine learning into healthcare. Hathaliya et al. (2019) propose a decentralized AI-powered permissioned blockchain architecture for remote patient monitoring. In contrast, Bhattacharya et al. (2021) introduce a framework that utilizes blockchain and deep learning technologies to facilitate the sharing of electronic health records. The utilization of blockchain technology fosters trust among healthcare stakeholders while also enhancing privacy and security measures by thwarting collusion and quantum attacks through the implementation of lattice-based key and signature verification schemes. The incorporation of machine learning techniques facilitates the development of prognostic models that can be utilized to detect forthcoming diseases by analyzing available medical records.

Table 3. *Key publications in Stream II.*

Publication	Factor loading	Factor score
Gupta et al. (2020a)	0.94	4.02
Gupta et al. (2019a)	0.90	3.24
Gupta et al. (2019b)	0.89	2.81
Tanwar et al. (2018)	0.89	3.43
Gupta et al. (2020b)	0.87	3.56
Bhattacharya et al. (2021)	0.87	2.51
Gupta et al. (2019c)	0.86	3.78
Sheth et al. (2020)	0.84	2.21
Hathaliya et al. (2019)	0.84	2.24
Rana et al. (2019)	0.78	2.88
Bodkhe et al. (2020)	0.78	1.60
Tanwar et al. (2019)	0.77	2.04
Gupta et al. (2020c)	0.77	3.73
García-Magariño et al. (2019)	0.76	3.87
Tanwar et al. (2020)	0.75	2.81
…	…	…
Alladi et al. (2020)	0.50	3.12
Gupta et al. (2016)	0.54	2.72
Other: 4 publications with FL > 0.7		

Subsequent publications within this stream examine security issues in vehicular networks, as well as the use of blockchain technology, and the fundamental principles of blockchain in the context of smart vehicle networks to address security concerns such as lack of reliability and trust, and data security. For instance, Tanwar et al. (2018) present a taxonomy for classifying attacks and countermeasures in the setting of ad hoc and vehicular networks. Similarly, Gupta et al.'s (2020b) systematic review provides a comprehensive classification of attacks associated with autonomous vehicles, along with conventional strategies to mitigate them. The authors proceed to analyze an autonomous vehicle framework that utilizes blockchain technology and compare its security resilience with traditional countermeasures. Moreover, Alladi et al. (2020) present an in-depth review of the potential applications and roles of blockchain technology in the automation of supply chain management, UAVs, security of UAV networks, utilization of UAV networks for edge computing, surveillance based on swarm technology, and decentralized storage. The authors posit that the implementation of blockchain technology has the potential to effectively address issues pertaining to data protection, as well as those related to the coordination, security, and decision-making processes of UAVs. Rana et al. (2019) offer a blockchain-

based safety mechanism that makes use of hashing and digital signature techniques to encrypt gathered data. García-Magariño et al. (2019) present a security technique that leverages blockchain principles to augment the monitoring of UAVs. The technology employed utilizes asymmetric encryption to identify compromised UAVs within vehicle networks in accordance with established trust policies. Further, Gupta et al. (2020c) propose a Smart-contract-based approach to ensure the security, trustworthiness, and confidentiality in drone-based medical delivery.

The studies by Gupta et al. (2019a) and Gupta et al. (2019b) examine the challenges and applications of tactile internet within the context of 5G technology. Gupta et al.'s (2019a) survey classifies the obstacles in designing and implementing tactile internet for various ultra-low latency applications, whereas Gupta et al.'s (2019b) study focuses on the system architecture and challenges associated with tactile internet-based telesurgery systems. The authors outline five areas of difficulties, namely: achieving ultra-low latency, ensuring ultra-high reliability, addressing security and privacy concerns, managing high communication costs, and mitigating latency in multi-user haptic communications.

In summary, Stream II deals with the combination of recent technologies and the implications and challenges that arise from their integration. The studies do generally not focus on contexts relevant to UAVs, e.g., AI-assisted smart contract vulnerability detection by Gupta et al. (2020c). However, the application of blockchain technology for securing and managing health care records (e.g., Hathaliya et al., 2019) may yield important findings for its integration in a UAV context, e.g., managing and securing access control and authentication. In that sense, security and privacy implications of the regarded technologies and their combinations with other technologies, as well as how a technology's particular features can be used to improve another, are central to Stream II, which is in differentiation to Stream I, which focused on inter-drone and drone-to-GSS communication.

3.3 Research Stream III: Federated Learning

The third research stream includes a total of 42 publications, which account for 14.29% of all publications included in the dataset. Fifteen of the 42 publications possess a factor loading of 0.7 or higher (35.71%). However, these publications additionally exhibit a negative factor score, indicating negative thematic relevance, notwithstanding their high thematic fit owing to the high factor loading. Table 4 presents a summary of 15 publications with a factor loading exceeding 0.7 and their corresponding factor scores. Additionally, the table includes two other publications that exhibit high factor scores. In its entirety, Stream III accounts for 8.82% of the variance in the co-citations, making it the research stream with the third-highest explained variance. Stream III's academic work is bifurcated into two thematically related parts, both of which pertain to federated learning. The first group of research papers focuses on examining fundamental principles, techniques, obstacles, and domains of implementation associated with federated learning. The second cohort investigates the conceptualization and synergies of federated learning systems based on blockchain technology across diverse Internet of Things (IoT) settings, including but not limited to IoD, Industrial Internet of Things (IIoT), and smart home applications. The thematic discourse surrounding federated learning is shared by both identified groups, thus justifying the designation of Stream III as *Federated Learning*.

With a factor score of 3.5, the scientific article with the greatest impact on the research stream is the publication by McMahan et al. (2017). The authors propose federated learning as a privacy-preserving training method that allows mobile devices to retain their sensitive data while sharing the aggregated model without central storage. Other publications important to Stream III include Lim et al. (2020) with a factor score of 3.21, Lu et al. (2020; 3.19), and Brik et al. (2020; 3.15). Lim et al. (2020) investigate the implementation of federated learning in mobile edge computing and the application fields of federated learning in wireless communication, including edge computing, caching, autonomous driving, spectrum management, coexistence of heterogeneous systems, and 5G core networks. Lu et al. (2020) employ federated learning on a permissioned blockchain to establish a secure and privacy-preserving data sharing mechanism for multiple dispersed parties in IIoT. The authors' approach reduces data leakage risk and enables secure connectivity between IoT devices, whereas the blockchain governs data access and retrieval. Brik et al. (2020) introduce federated learning in UAV-enabled wireless networks and discuss its application and challenges in various domains, including 5G cellular networks for UAVs, IoT, and edge computing. The most influential works for this stream concern both

topics – federated learning facilitation under specific conditions (e.g., wireless networks) and the integration of blockchain in federated learning systems.

Table 4. *Key publications in Stream III.*

Publication	Factor loading	Factor score
Zhao et al. (2021)	0.88	2.75
Yang et al. (2019)	0.82	2.90
Liu et al. (2019)	0.82	1.99
Kim et al. (2020)	0.81	2.80
Lu et al. (2020)	0.81	3.19
Bonawitz et al. (2019)	0.80	2.82
Lim et al. (2020)	0.80	3.21
Wang et al. (2019)	0.79	2.36
Zhou et al. (2018)	0.78	2.13
Niknam et al. (2020)	0.77	2.95
Wang et al. (2021)	0.76	2.95
McMahan et al. (2017)	0.75	3.50
Pokhrel (2020)	0.75	2.04
Brik et al. (2020)	0.72	3.15
Mollah et al. (2021)	0.71	1.72
…	…	…
Zeng et al. (2020)	0.70	3.09

Several other publications with a factor loading >0.7 address the convergence of blockchain and federated learning. Zhao et al. (2021) propose a federated learning framework that leverages blockchain technology and incorporates a reputation mechanism, specifically tailored for IoT device manufacturers. The proposed system utilizes blockchain technology to validate the authenticity of customer-trained and signed models, prevent malicious activities by both customers and manufacturers, and guarantee transparency and traceability in the process. The study conducted by Kim et al. (2020) introduces a federated learning framework that utilizes blockchain technology to facilitate on-device machine learning. This approach eliminates the need for centralized coordination and data storage. The suggested design relies on a Proof-of-Work (PoW) consensus mechanism. Upon successful execution, the authenticated locally produced model is modified and securely registered on the blockchain. Along with the on-device architecture proposed by Kim et al. (2020), Liu et al. (2019) propose blockchain-based federated learning frameworks as a means of ensuring secure data sharing in the context of IIoT. Liu et al. (2019) put forward an Ethereum-based deep reinforcement learning framework for data collection and sharing. The framework seeks to enhance mobile terminal data collection efficiency while reducing energy usage. Further, the framework utilizes the Ethereum blockchain to enhance secure data sharing among mobile terminals and increase resistance to attacks such as denial-of-service (DOS) and distributed denial-of-service (DDoS). Alsamhi et al. (2022) highlight the potential synergies between blockchain technology and federated learning in the context of drone-enabled edge intelligence for the purpose of establishing smart green environments. The study's primary focus is on exploring synergies between blockchain and federated learning in various domains, including data collection, security and privacy, energy consumption, connectivity, and quality of service.

Additional notable publications in this field of study investigate the amalgamation of blockchain and federated learning within the context of the IoD. For instance, Wang et al. (2021) introduce a collaborative learning framework for drone-assisted mobile crowdsensing that employs a consortium blockchain to enable secure exchange of local model updates and validation of contributions without a centralized entity. Further, the design includes an integrated two-tier reinforcement learning incentive

mechanism that encourages more accurate model sharing among UAVs. Pokhrel (2020) proposes a mobile federated learning blockchain system for emergency and disaster scenarios in a 6G edge environment. The system utilizes UAVs as mobile miners using PoW, while base stations and access points are defined as communication nodes. The prescribed network structure facilitates concurrent sharing, updating, and verification of local vehicle model updates during a disaster scenario.

Apart from articles that focus on the intersections between blockchain and federated learning, several of Stream III's articles belong to the group that focuses on investigating fundamental principles, techniques, challenges, and implementation issues associated with federated learning. For example, Bonawitz et al. (2019) put forward a distributed machine learning method for mobile devices that utilizes TensorFlow to train models on decentralized data. Wang et al. (2019) publication discusses a learning approach that encompasses a broad range of gradient-descent-based machine learning models across numerous edge nodes.

In summary, Stream III concerns the underlying principles and practical applications of federated learning in various domains and explores the possible benefits of combining decentralized learning with blockchain technology. The amalgamation of federated learning and blockchain technology is an intriguing technological combination that possesses the ability to facilitate the transmission of data among mobile entities in IoT while adhering to security and privacy preservation and obviating the presence of a central authority (Liu et al. 2019; Lu et al. 2020).

3.4 Research Stream IV: Resource and Data Management in IoT

Research Stream IV comprises 38 publications, which account for 12.93% of the publications present in the dataset. Furthermore, the stream exhibits an explained variance of 5.3%. Table 5 indicates that eight publications in the stream demonstrate a factor loading exceeding 0.7. Moreover, the data table depicts an additional set of three publications that possess a substantial factor score, signifying a strong thematic coherence within the corresponding research domain. The publications under consideration explore diverse themes related to resource and data management in IoT environments, thereby warranting the categorization of Stream IV as *Resource and data management in IoT*.

Table 5. *Key publications in Stream IV.*

Publication	Factor loading	Factor score
Shen et al. (2019)	0.85	2.64
Esposito et al. (2018)	0.80	2.15
Mozaffari et al. (2017)	0.79	2.41
Zhu et al. (2019)	0.79	2.68
Novo (2018)	0.77	2.32
Xiong et al. (2019)	0.72	2.15
Xiong et al. (2018)	0.72	2.36
Dorri et al. (2017)	0.70	2.24
…	…	…
Hayat et al. (2016)	0.49	3.06
Ferrer (2018)	0.44	2.83
Gupta et al. (2016)	0.41	2.82

In the identified cohort, Hayat et al.'s (2016) publication, titled "Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint", received the highest factor score of 3.06, indicating the best thematic fit. The survey's authors acknowledge that the four designated applications for UAVs - search and rescue, coverage, construction, and delivery of goods - have varying qualitative and quantitative resource needs. Specifically, they highlight the significance of communication and minimum data requirements, including delay tolerance, real-time communication,

low and high capacity, as well as short- and long-range communication requirements within UAV networks (Hayat et al. 2016). Furthermore, several publications in this research stream suggest employing blockchain technology as a method of managing data and resources. For instance, Xiong et al. (2018) introduce an architectural framework for mobile blockchain edge computing that considers the constraints of IoT devices with limited energy and CPU resources. The proposed architecture employs a Stackelberg game to optimize the utilization of CPU and energy resources by delegating IoT mining tasks from resource-restricted mobile devices to mobile edge servers. Similarly, Xiong et al. (2019) introduce a two-stage Stackelberg game-based resource management system for proof-of-work blockchain networks. The system aims to optimize resource allocation by offloading computational tasks from resource-limited devices to fog or cloud providers (Xiong et al. 2019). Besides the optimization of energy and CPU resources proposed by Xiong et al. (2018) and Xiong et al. (2019), Novo (2018) proposes an Ethereum-based access management system that connects resource-limited IoT devices to the Ethereum blockchain via the management of so-called hub nodes. Novo (2018) indicates that this architecture can improve the efficiency of device management by eliminating the need for a central access point, particularly in scenarios in which frequent access management is required. Furthermore, Shen et al. (2019) and Zhu et al. (2019) put forth the proposition of utilizing blockchain technology for the purpose of managing data systems. Shen et al. (2019) present a blockchain-based platform that facilitates secure data exchange among IoT data providers. The platform incorporates a privacy-compliant support vector machine training scheme for encrypted IoT data. Similarly, Zhu et al. (2019) put forward a model for blockchain-based data management, which can be deployed in cloud environments and is designed to enhance control through the implementation of designated trust nodes. Mozaffari et al. (2017) suggest an approach to enhance the energy efficiency of uplink data collection from UAVs in IoT networks. This method involves optimizing UAV locations, trajectories, IoT device allocation, and uplink power control for UAV movements in IoT data collection scenarios.

The research stream focuses on the integration of UAV networks with blockchain and edge computing technologies to address the communication and resource management challenges in civil applications such as search and rescue, delivery, and construction. It highlights the diverse requirements of UAV operations, such as real-time communication and energy efficiency, while proposing innovative solutions like decentralized architectures and resource optimization strategies. Blockchain emerges as a key enabler for secure and efficient data exchange, decentralized access management, and resource allocation, particularly for IoT-integrated UAV systems. Overall, Stream IV underscores the potential of combining UAVs with cutting-edge technologies to enhance operational efficiency and scalability in diverse application domains.

3.5 Research Stream V: Optimization, Security, and Applications in UAV-Enabled Mobile Edge Computing Systems

The fifth research stream encompasses a total of 25 publications, representing approximately 8.50% of the dataset and demonstrating an explained variance of 4.87%. Table 6 shows a collection of nine publications that have significantly influenced the ongoing research trajectory, with each of these publications exhibiting notable factor loadings (≥0.7), indicating their strong association with the underlying factor. Additionally, the table includes two other publications that have obtained a high factor score, highlighting their significance in the research domain. The articles showcased in Stream V primarily focus on the application of UAVs in conjunction with mobile edge computing (MEC) or edge cloud computing. The research conducted in this specific field encompasses a diverse array of subjects, such as task offloading, computational efficiency and trajectory optimization, and the assessment of security performance. It is thus conceivable to classify this specific research stream as *Optimization, Security, and Applications in UAV-Enabled Mobile Edge Computing Systems.*

The study that exhibits the highest thematic alignment, as indicated by a factor score of 4.68, is the research conducted by Zhou et al. (2020) entitled "Secure Communications for UAV-Enabled Mobile Edge Computing Systems". The study provides an MEC framework that leverages UAVs to enable the efficient offloading of computationally intensive tasks from ground users to UAVs in close proximity. The authors of this publication have developed a low-complexity algorithm with the aim of optimizing

the maximum secrecy capacity of UAVs. The primary objective of this study is to investigate the joint optimization of multiple parameters, encompassing the strategic placement of corresponding UAVs, the transmit power allocation for users, the offload ratio, the computing capacity, and the interference power of UAVs. The authors identify the fundamental performance trade-off between security and latency of UAV-enabled MEC systems.

Table 6. *Key publications in Stream V.*

Publication	Factor loading	Factor score
Zhou et al. (2018)	0.87	4.47
Liu et al. (2020)	0.87	4.21
Guo and Liu (2020)	0.85	3.25
Zhou et al. (2020)	0.83	4.68
Shahmoradi et al. (2020)	0.80	2.68
Yu et al. (2020)	0.80	3.08
Motlagh et al. (2017)	0.79	3.43
Mach and Becvar (2017)	0.72	2.65
Chen et al. (2019)	0.70	3.22
…	…	…
Xu et al. (2021)	0.69	2.96
Chen et al. (2017)	0.59	2.92

In addition to Zhou's security-focused work, other authors have also explored UAV-enabled MEC systems, with strong but not limiting reference to joint offloading, computation rate maximization, and trajectory optimization. For instance, Zhou et al. (2018) propose a two-stage algorithm for partial computation offloading and a three-stage algorithm for binary computation offloading in UAV-enabled MEC systems. The study's objective is to optimize the weighted sum computation bits, taking into account CPU frequencies, offloading times, and transmission powers in order to optimize resource allocations. Similarly, Liu et al. (2020) propose a UAV-enabled MEC system in which UAV energy resources are optimized by jointly optimizing UAV trajectories and CPU frequencies, as well as transmitting power and the offloading of computations. Similar to Zhou et al. (2018), the authors also propose two algorithms, namely a successive convex approximation-based algorithm (SCA) and a decomposition and iteration-based algorithm (DAI). Guo and Liu (2020) propose an approach that involves computation offloading, trajectory optimization, and bit allocation in both uplink and downlink to reduce energy consumption in UAV-based mobile edge environments. The authors put forward a technique for optimizing resource efficiency in UAV-based MEC systems by formulating the problem as a mixed-integer nonconvex optimization. Further, they present a block coordinate descent and successive convex approximation-based algorithm to solve the problem. Further, Yu et al. (2020) put forward a system that employs UAVs and edge clouds to provide MEC services, specifically collaborative UAV-edge clouds offloading for IoT devices in areas with terrestrial signal blockage or shadowing. The authors suggest an algorithm based on SCA to jointly solve and optimize UAV energy consumption, minimize the service delay of IoT devices, make task-sharing decisions, and offload resources. Chen et al. (2019) study proposes a hybrid computing model for UAV edge clouds to enhance the quality of service and resource management in UAV swarms. The authors rely on the Markov approximation algorithm as a solution for the routing problem of UAVs with critical latency.

Besides the presented studies that target specific optimizations in MEC environments, other studies in this research stream focus on surveying and categorizing research on computation offloading in general, as well as data and computation offloading in specific application scenarios. For instance, Mach and Becvar's (2017) survey presents particular MEC application scenarios and categorizes computation offloading research into three categories: decision on computation offloading, resource allocation, and

mobility management. Motlagh et al.'s (2017) study exemplifies the utilization of video data offloading to MEC nodes in crowd surveillance, resulting in enhanced data analysis efficiency and energy conservation.

In summary, Stream V focuses on UAV-enabled MEC systems, emphasizing secure and efficient task offloading, resource optimization, and energy efficiency. Central to this stream is Zhou et al.'s (2020) work, which investigates the trade-offs between security and latency in MEC systems while optimizing UAV placement, power allocation, and computing capacity. Complementary studies explore trajectory optimization, collaborative UAV-edge cloud offloading, and hybrid computing models for UAV swarms, using advanced algorithms to enhance energy efficiency and resource management. Broader surveys categorize computation offloading research and highlight application-specific scenarios, such as video data offloading for crowd surveillance, demonstrating the transformative potential of MEC systems in diverse environments.

3.6 Research Stream VI: Blockchain-enabled data sharing and automation on the Internet of Drones

A total of 28 publications can be assigned to Stream VI, which corresponds to 9.52% of the publications in the dataset. Additionally, the present research stream exhibits an explained variance of 3.2%. Table 7 illustrates six publications that showcase a factor loading that is greater than 0.7, alongside five other influential publications that exhibit a high factor score. The articles published within that specific domain demonstrate thematic coherence in their examination of the prospective uses of blockchain technology within IoD ecosystems. In particular, the subject of these articles concerns the utilization of blockchain technology to enable safe data transfer, execute automated processes through smart contracts, and verify the identity of drones within drone networks, thereby addressing major security and privacy concerns. Stream VI can be designated as *Blockchain-enabled data sharing and automation on the Internet of Drones*.

Table 7. *Key publications in Stream VI.*

Publication	Factor loading	Factor score
Cheema et al. (2021)	0.83	3.08
Hassija et al. (2020)	0.80	3.11
Khan et al. (2021)	0.77	2.13
Feng et al. (2021)	0.75	3.74
Gai et al. (2021)	0.75	3.49
Allouch et al. (2021)	0.71	3.29
…	…	…
Yazdinejad et al. (2021)	0.55	4.11
Singh et al. (2021)	0.60	3.56
Su et al. (2022)	0.60	3.34
Singh et al. (2020)	0.57	3.22
Xiao et al. (2021)	0.68	3.12

Yazdinejad et al. (2021) attained the highest factor score (4.11) in Stream VI, indicating the best thematic alignment. The authors introduce an approach for creating a secure and efficient drone network in smart city contexts. The evaluated system employs a network architecture based on zones and incorporates blockchain technology, which employs a decentralized consensus mechanism named "drone-based delegated proof of stake". The consensus mechanism provides an authentication process without requiring re-authentication and facilitates the authentication of all network transactions. As per the authors' assertion, this technique guarantees secure communication and data transmission across diverse zones, concurrently optimizing the authentication procedure to augment efficiency (Yazdinejad et al. 2021).

Several publications are incorporating artificial intelligence in conjunction with blockchain technology. Khan et al. (2021) propose a blockchain-based decentralized machine learning system to enhance security in IoD environments by detecting intrusions through predictive analytics. While Singh et al. (2020) put forward a framework that utilizes deep Boltzmann machine and blockchain technology to facilitate secure data transfer and information sharing in cyber-physical systems, specifically in IoD environments. The framework has the specific objective of preventing unapproved drone access to the network. Feng et al. (2021) also establish a blockchain-based data sharing and authentication design, which, in contrast to Singh et al. (2020), relies on smart contracts for automated identification as well as attribute-based encryption.

Furthermore, numerous research endeavours have integrated blockchain technology into a variety of other applications. Hassija et al. (2020) suggest a blockchain-based security design for drone-mounted base stations that can be used in rural areas, specific emergency cases, and disaster areas. In this concept, blockchain facilitates the technical infrastructure for a smart contract-based game-theoretic model for dynamic bandwidth allocation. Cheema et al. (2021) present a framework that incorporates blockchain technology to enable secure authentication and optimal placement of drones in smart vehicular networks, focusing on optimization of constraints such as bandwidth, links a drone can support, and backhaul limitations. Allouch et al. (2021) conceptualize a traffic monitoring system for low-altitude drones that is based on a permissioned Hyperledger fabric blockchain. Lastly, Xiao et al. (2021) design a swarm monitoring system of drones that utilizes a private blockchain network for drone identification, data transaction monitoring, and collective decision making.

In sum, Research Stream VI explores the application of blockchain technology to address critical issues related to secure communication, identity verification, and automated operations within drone networks. This stream demonstrates a strong thematic focus on leveraging blockchain to enable secure data transfer, smart contract execution, and privacy preservation, thereby addressing inherent challenges in IoD ecosystems. Key contributions include decentralized authentication mechanisms, such as drone-based delegated proof of stake, predictive analytics for intrusion detection, and smart contract-enabled automated identification and encryption. The research also encompasses diverse applications, including swarm and traffic monitoring systems, blockchain-supported drone-mounted base stations for disaster relief, and frameworks for optimizing drone placement in smart vehicular networks. Collectively, these studies underscore the potential of blockchain in enhancing the security, efficiency, and scalability of IoD systems within diverse operational contexts.

4 Discussion

4.1 Reflections on main results

The six research streams identified through this bibliometric analysis underscore blockchain's growing role in securing, managing, and automating UAV ecosystems. Taken together, they reveal both a strong concentration of work on privacy and authentication in the IoD and a diversification into federated learning, resource management, MEC, and automation. However, these findings must be understood not as isolated silos, but as contributions to broader discourses on blockchain in the IoV and related domains, where UAVs are increasingly deployed as mobile relays, data collectors, and autonomous agents.

The predominance of security- and privacy-oriented studies (Streams I and II) reflects the vulnerabilities of open UAV communication channels and confirms earlier survey results (e.g., Harbi et al., 2023; Tychola et al., 2024). Across both UAV and IoV contexts, blockchain is positioned as a decentralized trust mechanism that strengthens authentication frameworks and protects data integrity. For example, Khan et al. (2022) introduced a permissioned Hyperledger-based system that secures UAV-assisted vehicle communication while reducing network load. Similarly, Kumar et al. (2024) and Alagha et al. (2025) demonstrated how lightweight blockchain protocols, combined with edge computing and reinforcement learning, can improve coverage, connectivity, and transparency in UAV-assisted IoV. These works resonate with our findings on the dominance of authentication and

communication security, but they also highlight a gap in standardization: most solutions remain domain-specific, raising questions about interoperability across UAV–IoV ecosystems.

Streams III and IV, focused on federated learning and resource management, reveal how UAV research is beginning to incorporate decentralized intelligence and efficient computation. Here, blockchain serves as both a ledger for secure aggregation and an incentive mechanism to encourage participation. These results extend the insights of Billah et al. (2022), who surveyed blockchain-based federated learning in the IoV but left UAV-specific challenges largely unaddressed. In UAV networks, mobility, limited energy supply, and unstable connectivity exacerbate the computational challenges of federated learning (Alsamhi et al., 2022; Wang et al., 2021). Recent proposals in adjacent domains, such as Tang et al. (2022), show how proof-of-stake consensus and reinforcement learning can reduce overhead while maintaining incentives for secure data collection in UAV–IoT systems. This suggests that integrating blockchain with federated learning for UAVs is promising but will require lighter consensus and UAV-tailored optimization strategies before it can scale.

Our analysis also shows growing scholarly attention to MEC-enabled UAV systems (Stream V). While many studies in this stream are not primarily blockchain-focused, they emphasize task offloading and computational efficiency—issues that directly intersect with blockchain overhead. Aloqaily et al. (2021) provided early design guidelines for blockchain-assisted 5G–UAV networks, highlighting the importance of decentralized service delivery and data availability. More recent frameworks (Alagha et al., 2025; Kumar et al., 2024) confirm that combining edge computing with lightweight blockchain protocols can significantly improve network efficiency. The challenge, as our bibliometric evidence also suggests, lies in reconciling blockchain's latency and computational costs with UAVs' strict performance requirements.

Finally, Stream VI on automation and data sharing highlights blockchain's potential for enabling UAV autonomy, swarm coordination, and disaster-response operations through smart contracts and decentralized verification. This aligns with recent arguments by Tychola et al. (2024), who stressed that blockchain can enhance IoD reliability and connectivity but warned that scalability and resource constraints remain unresolved. Our findings reinforce this view: consensus mechanisms designed for static or resource-rich blockchain environments do not translate easily into dynamic UAV networks.

Synthesizing across the six streams and the wider IoV–UAV literature, several cross-cutting insights emerge. First, blockchain is consistently recognized as a solution to security and trust concerns, but efficiency and scalability trade-offs remain central. Second, the literature often blurs distinctions between public, consortium, and private blockchain models, complicating evaluations of feasibility in UAV contexts. Third, many proposed frameworks remain conceptual: as both our analysis and recent works (e.g., Alagha et al., 2025; Kumar et al., 2024) show, empirical validation in real-world UAV deployments is scarce. These gaps suggest that the field has reached a stage where proof-of-concept studies must evolve into experimental deployments.

Together, these reflections indicate that blockchain–UAV integration has matured enough to provide a rich conceptual foundation but remains fragmented, domain-specific, and under-validated in practice. Addressing these shortcomings requires cross-disciplinary approaches, drawing lessons from IoV, IoT, and 5G/6G research while tailoring solutions to the unique constraints of UAV networks. These insights directly motivate the research agenda outlined in Section 4.2, which reframes the persistent gaps into priority areas for future investigation.

4.2 Research Agenda

The convergence of blockchain technology and UAVs has given rise to a dynamic and multi-faceted research field. Despite significant advancements, several crucial aspects remain underexplored. The present research agenda outlines key areas where further investigation is essential to advance the integration of blockchain in UAV systems. By addressing these gaps, future studies can enhance the practical application, security, and efficiency of blockchain-enabled UAV operations. The following sections outline four primary areas where more focused research is needed.

There is a need for more research on blockchain-enabled security and privacy in UAV networks.

UAV networks are highly susceptible to cyber threats due to their wireless connectivity and the open nature of their communication channels (Harbi et al., 2023; Mehta et al., 2020). These vulnerabilities include privacy breaches, various forms of cyberattacks, and data integrity issues. Ensuring secure data transmission and effective authentication mechanisms is crucial. Blockchain technology, with its decentralized and immutable nature, can offer a safe framework. However, existing blockchain consensus methods often introduce delays that are incompatible with the real-time demands of UAV operations (Alladi et al., 2020). As a result, developing customized, lightweight consensus protocols tailored to UAV contexts is a priority. Future studies should also investigate integrating blockchain with identity management and access control, specifically for UAV systems.

Blockchain can enhance accountability and reduce the risk of single points of failure by distributing trust across multiple stakeholders, such as operators, service providers, and regulatory bodies. Nevertheless, this decentralization also brings challenges in ensuring data privacy and security (Bera et al., 2020; Bera et al., 2021). Research should focus on designing authentication schemes that balance robust security with low computational overhead. Moreover, exploring the suitability of permissioned versus public blockchain models for UAV operations could yield insights into their practical deployment. Developing security frameworks that are optimized for IoD applications, followed by empirical testing in realistic environments, is essential.

There is a need for more research on blockchain-enabled federated learning for UAV networks.

Integrating federated learning with blockchain is a promising direction for UAV networks, as it allows collaborative model training while preserving data privacy (Alsamhi et al., 2022; Wang et al., 2021). Blockchain can provide a secure ledger for recording and aggregating model updates without sharing raw data. However, the practical implementation of blockchain-integrated federated learning in UAV systems is still limited. Many existing approaches remain conceptual, lacking experimental validation. Research should develop frameworks that can handle the challenges of drone mobility and inconsistent connectivity. Additionally, lightweight consensus mechanisms that maintain efficiency without compromising privacy would be beneficial.

Even though federated learning does not involve sharing raw data, model updates can still reveal sensitive information (Kim et al., 2020; Liu et al., 2019). Therefore, enhancing privacy-preserving techniques in blockchain-based federated learning is crucial. Another challenge lies in decentralizing the aggregation process itself, as current federated learning approaches often rely on a central server. Blockchain could offer a decentralized alternative, but practical implementations are scarce. Further research is needed to develop decentralized federated learning models specifically for UAV networks, addressing challenges like computational efficiency and data integrity.

There is a need for more research on efficient resource and computing management in blockchain-integrated UAV networks.

The integration of blockchain technology into UAV systems can put a strain on their limited resources, including battery life, processing power, and storage capacity (Shen et al., 2019; Xiong et al., 2019). One way to alleviate this burden is through MEC, which enables the offloading of computational tasks. However, managing resource allocation in a blockchain context remains challenging. Coordination between UAVs and edge servers needs to be optimized, especially when blockchain transactions are involved. Developing adaptive resource management algorithms that consider blockchain overhead is a promising research direction.

Latency and computational delays caused by blockchain consensus mechanisms can compromise UAV performance (Mach and Becvar, 2017; Mozaffari et al., 2017). Exploring lightweight consensus models and off-chain data handling can reduce these delays. Additionally, blockchain scalability issues can arise when dealing with high-frequency data streams from multiple UAVs. Investigating hybrid on-chain/off-chain approaches or the use of sharding to maintain throughput without overloading the system could significantly improve efficiency.

There is a need for more research on integrating multiple emerging technologies with blockchain to enable autonomous UAV operations.

UAVs are increasingly being integrated with technologies like AI, IoT, and next-generation networks (5G/6G), but how blockchain fits into this technological ecosystem requires deeper exploration (Gupta et al., 2020; Sheth et al., 2020). Combining blockchain with AI could lead to more secure and autonomous UAV applications, as blockchain can ensure data integrity while AI enhances decision-making processes. Research should focus on how to develop lightweight AI models and edge computing solutions that are compatible with blockchain-enabled UAV networks.

Smart contracts can facilitate autonomous operations by encoding predefined rules that execute without human intervention. This can be particularly useful in applications such as traffic management or coordinated swarm operations. However, the design of reliable and adaptable smart contracts for dynamic environments remains a challenge (Tanwar et al., 2019). Developing frameworks that ensure smart contract security, scalability, and compliance with aviation regulations would support the practical deployment of blockchain-driven autonomous UAV systems.

5 Conclusion

The findings of this bibliometric analysis provide a comprehensive overview of the evolving research landscape at the intersection of blockchain technology and UAV applications. Through the identification of six distinct research streams, this study highlights the breadth and depth of academic discourse surrounding the integration of blockchain within UAV ecosystems. The analysis reveals that privacy and security concerns in the IoD represent the most extensively studied topic, with Research Stream I encompassing the highest number of publications and explaining the largest proportion of variance. This prominence underscores the critical importance of secure authentication, privacy preservation, and decentralized trust mechanisms in ensuring the integrity and reliability of UAV communication networks. The prevalence of cryptographic authentication schemes and decentralized trust mechanisms demonstrates the critical importance of securing UAV communications. Yet, the absence of standardized frameworks poses a challenge for large-scale interoperability.

Beyond security-centric investigations, the broader implications of integrating blockchain with other emerging technologies are highly relevant to the discourse. Research Stream II, which accounts for the second-highest explained variance, underscores the interdisciplinary nature of this domain, where blockchain intersects with artificial intelligence, tactile internet, and smart vehicle networks. This cross-domain relevance offers valuable opportunities for knowledge transfer and methodological adaptation. However, the unique constraints associated with UAV operations, such as energy efficiency and real-time data processing, necessitate tailored solutions.

The third research stream, dedicated to federated learning, highlights an emerging area of interest wherein blockchain serves as a trust-enabling mechanism for decentralized learning in UAV networks. The observed bifurcation within this stream—between studies focusing on fundamental federated learning principles and those investigating its integration with blockchain in IoD and other IoT settings—reflects the growing recognition of federated learning's potential to enable secure, distributed intelligence in UAV applications. However, the computational demands of federated learning, coupled with UAVs' inherent resource constraints, present significant challenges that must be addressed through optimization strategies and blockchain-based incentive mechanisms.

With an emphasis on secure data exchange, decentralized access control, and resource allocation in IoT-integrated UAV systems, Research Stream IV underscores blockchain's role in enhancing the operational efficiency of UAV networks. Nevertheless, while blockchain's transparency and immutability contribute to improved data security, concerns regarding latency and computational overhead must be mitigated through hybrid approaches that incorporate edge computing and off-chain storage solutions.

Research Stream V exhibits a notable non-blockchain focus. The discourse in this stream surrounds UAV-enabled MEC systems, optimizing UAV task execution, computational offloading, and security

performance. The studies within this stream predominantly explore how UAVs, when integrated with edge cloud computing infrastructures, can improve computational efficiency while ensuring data integrity and minimizing security risks.

Finally, Research Stream VI highlights blockchain's role in enabling secure data sharing and automation within IoD environments. This stream encompasses investigations into decentralized authentication mechanisms, smart contract-enabled UAV automation, and blockchain-backed frameworks for UAV swarm coordination and disaster response. The thematic coherence observed in this stream underscores blockchain's capacity to support autonomous UAV operations while addressing persistent security concerns. However, as UAV networks scale and operate in increasingly dynamic environments, the limitations of existing blockchain consensus mechanisms, particularly in high-traffic scenarios, necessitate continued exploration of alternative protocols that enhance scalability without compromising security. Building on these insights, this study advances a research agenda that synthesizes unresolved challenges into four priority areas for future inquiry.

Taken together, the insights derived from this bibliometric analysis emphasize both the progress made and the challenges that remain in harnessing blockchain technology for UAV applications. While blockchain offers substantial promise in enhancing security, data management, and automation within UAV networks, its implementation is not without constraints. Computational efficiency, scalability, and interoperability remain pivotal concerns that future research must address. Moreover, despite the extensive theoretical discourse surrounding blockchain's integration with UAVs, empirical validation through real-world testing remains limited. Bridging this gap between conceptual advancements and practical implementation will be critical in realizing the full potential of blockchain-enabled UAV ecosystems. By addressing these challenges within the framework of the proposed research agenda—covering blockchain-enabled security and privacy, blockchain-integrated federated learning, efficient resource and computing management, and the integration of emerging technologies—future investigations can further refine blockchain's role in UAV applications, ultimately contributing to the development of more secure, efficient, and autonomous drone networks.

Acknowledgement

The study was conducted as part of the research project AVIK (acronym; engl.: automated ground-air intercommunication in mobility for enhancing interaction and collaboration) which focuses on automating and enhancing the interconnectedness of different vehicles and mobility actors (e.g. UAVs and cars) in the context of data transmission, harmonization, aggregation and monetization. The project is funded by Germany's Federal Ministry for Digital and Transport (BMDV) under the conditions of the mFUND program (FKZ: 19F2227A). Consortium partners of AVIK comprise ASINCO GmbH (Consortium leader), Technische Hochschule Wildau, Werner Turck GmbH & Co. KG, and Blockchain Research Lab gGmbH.

References

Alagha, A., Kadadha, M., Mizouni, R., Singh, S., Bentahar, J., and Otrok, H. 2025a. "UAV-Assisted Internet of Vehicles: A Framework Empowered by Reinforcement Learning and Blockchain," *Vehicular Communications* (52), p. 100874. (https://doi.org/10.1016/j.vehcom.2025.100874).

Alagha, A., Kadadha, M., Mizouni, R., Singh, S., Bentahar, J., and Otrok, H. 2025b. "UAV-Assisted Internet of Vehicles: A Framework Empowered by Reinforcement Learning and Blockchain," *Vehicular Communications* (52), p. 100874. (https://doi.org/10.1016/j.vehcom.2025.100874).

Ali, Z., Chaudhry, S. A., Ramzan, M. S., and Al-Turjman, F. 2020. "Securing Smart City Surveillance: A Lightweight Authentication Mechanism for Unmanned Vehicles," *IEEE Access* (8), Institute of Electrical and Electronics Engineers Inc., pp. 43711–43724. (https://doi.org/10.1109/ACCESS.2020.2977817).

Alladi, T., Chamola, V., Sahu, N., and Guizani, M. 2020. "Applications of Blockchain in Unmanned Aerial Vehicles: A Review," *Vehicular Communications* (23), Elsevier Inc. (https://doi.org/10.1016/J.VEHCOM.2020.100249).

Allouch, A., Cheikhrouhou, O., Koubâa, A., Toumi, K., Khalgui, M., and Nguyen Gia, T. 2021. *UTM-Chain: Blockchain-Based Secure Unmanned Traffic Management for Internet of Drones*. (https://doi.org/10.3390/s21093049).

Aloqaily, M., Bouachir, O., Boukerche, A., and Ridhawi, I. Al. 2021. "Design Guidelines for Blockchain-Assisted 5G-UAV Networks," *IEEE Network* (35:1), pp. 64–71. (https://doi.org/10.1109/MNET.011.2000170).

Alsamhi, S. H., Almalki, F. A., Afghah, F., Hawbani, A., Shvetsov, A. V., Lee, B., and Song, H. 2022. "Drones' Edge Intelligence over Smart Environments in B5G: Blockchain and Federated Learning Synergy," *IEEE Transactions on Green Communications and Networking* (6:1), Institute of Electrical and Electronics Engineers Inc., pp. 295–312. (https://doi.org/10.1109/TGCN.2021.3132561).

Alsamhi, S. H., Ma, O., Ansari, M. S., and Almalki, F. A. 2019. "Survey on Collaborative Smart Drones and Internet of Things for Improving Smartness of Smart Cities," *IEEE Access* (7), Institute of Electrical and Electronics Engineers Inc., pp. 128125–128152. (https://doi.org/10.1109/ACCESS.2019.2934998).

Bera, B., Chattaraj, D., and Das, A. K. 2020. "Designing Secure Blockchain-Based Access Control Scheme in IoT-Enabled Internet of Drones Deployment," *Computer Communications* (153), Elsevier B.V., pp. 229–249. (https://doi.org/10.1016/J.COMCOM.2020.02.011).

Bera, B., Das, A. K., and Kumar Sutrala, A. 2021. "Private Blockchain-Based Access Control Mechanism for Unauthorized UAV Detection and Mitigation in Internet of Drones Environment," *Computer Communications* (166), pp. 91–109. (https://doi.org/10.1016/j.comcom.2020.12.005).

Bera, B., Saha, S., Das, A. K., Kumar, N., Lorenz, P., and Alazab, M. 2020. "Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment," *IEEE Transactions on Vehicular Technology* (69:8), Institute of Electrical and Electronics Engineers Inc., pp. 9097–9111. (https://doi.org/10.1109/TVT.2020.3000576).

Bhattacharya, P., Tanwar, S., Bodkhe, U., Tyagi, S., Member, S., and Kumar, N. 2021. *BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications; BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications*. (https://doi.org/10.1109/TNSE.2019.2961932).

Billah, M., Mehedi, Sk. T., Anwar, A., Rahman, Z., and Islam, R. 2022a. *A Systematic Literature Review on Blockchain Enabled Federated Learning Framework for Internet of Vehicles*.

Billah, M., Mehedi, Sk. T., Anwar, A., Rahman, Z., and Islam, R. 2022b. *A Systematic Literature Review on Blockchain Enabled Federated Learning Framework for Internet of Vehicles*.

Boccadoro, P., Striccoli, D., and Grieco, L. A. 2021. "An Extensive Survey on the Internet of Drones," *Ad Hoc Networks* (122), Elsevier B.V. (https://doi.org/10.1016/J.ADHOC.2021.102600).

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., and Alazab, M. 2020. "Blockchain for Industry 4.0: A Comprehensive Review," *IEEE Access* (8), pp. 79764–79800. (https://doi.org/10.1109/ACCESS.2020.2988579).

Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., Kiddon, C., Konečn´y, J. K., Mazzocchi, S., Mcmahan, H. B., Overveldt, T. Van, Petrou, D., Ramage, D., and Roselander, J. 2019. *TOWARDS FEDERATED LEARNING AT SCALE: SYSTEM DESIGN*.

Bradford, S. 1985. "Sources of Information on Specific Subjects 1934," *Journal of Information Science* (10:4), SAGE Publications Ltd, pp. 176–180. (https://doi.org/10.1177/016555158501000407).

Brendan McMahan Eider Moore Daniel Ramage Seth Hampson Blaise AgüeraAg, H., and Arcas, A. 2017. *Communication-Efficient Learning of Deep Networks from Decentralized Data*.

Brik, B., Ksentini, A., and Bouaziz, M. 2020. *Federated Learning for UAVs-Enabled Wireless Networks: Use Cases, Challenges, and Open Problems*. (https://doi.org/10.1109/ACCESS.2020.2981430).

Cheema, M. A., Shehzad, M. K., Qureshi, H. K., Hassan, S. A., and Jung, H. 2021. "A Drone-Aided Blockchain-Based Smart Vehicular Network," *IEEE Transactions on Intelligent Transportation Systems* (22:7), pp. 4160–4170. (https://doi.org/10.1109/TITS.2020.3019246).

Chen, M., Member, Student, Mozaffari, M., Saad, Walid, Member, Senior, Yin, C., Debbah, M., Seon Hong, C., and Saad, W. 2017. "Caching in the Sky: Proactive Deployment of Cache-Enabled Unmanned Aerial Vehicles for Optimized Quality-of-Experience," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS* (35:5). (https://doi.org/10.1109/JSAC.2017.2680898).

Chen, W., Liu, B., Huang, H., Guo, S., and Zheng, Z. 2019. *When UAV Swarm Meets Edge-Cloud Computing: The QoS Perspective; When UAV Swarm Meets Edge-Cloud Computing: The QoS Perspective*. (https://doi.org/10.1109/MNET.2019.1800222).

Chen, Y.-S., and Leimkuhler, F. F. 1986. "A Relationship between Lotka's Law, Bradford's Law, and Zipf's Law," *Journal of the American Society for Information Science* (37:5), pp. 307–314. (https://doi.org/10.1002/(SICI)1097-4571(198609)37:5<307::AID-ASI5>3.0.CO;2-8).

Dorri, A., Kanhere, S. S., Jurdak, R., and Gauravaram, P. 2017. *Blockchain for IoT Security and Privacy: The Case Study of a Smart Home*. (https://doi.org/10.1109/PERCOMW.2017.7917634).

Esposito, C., De Santis, A., Tortora, G., Chang, H., and Choo, K.-K. R. 2018. "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," *IEEE Cloud Computing* (5:1), pp. 31–37. (https://doi.org/10.1109/MCC.2018.011791712).

Ever, K. Y. 2020. "A Secure Authentication Scheme Framework for Mobile-Sinks Used in the Internet of Drones Applications," *Computer Communications* (155), Elsevier, pp. 143–149. (https://doi.org/10.1016/J.COMCOM.2020.03.009).

Feng, C., Yu, K., Bashir, A. K., Al-Otaibi, Y. D., Lu, Y., Chen, S., and Zhang, D. 2021. "Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach," *IEEE Network* (35:1), Institute of Electrical and Electronics Engineers Inc., pp. 130–137. (https://doi.org/10.1109/MNET.011.2000223).

Ferrer, E. C. 2018. "The Blockchain: A New Framework for Robotic Swarm Systems," *Proceedings of the Future Technologies Conference*. (http://bitcoin.org/bitcoin.pdf).

Gai, K., Member, S., Wu, Y., Zhu, L., Raymond Choo, K.-K., and Xiao, B. 2021. "Blockchain-Enabled Trustworthy Group Communications in UAV Networks," *IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS* (22:7). (https://doi.org/10.1109/TITS.2020.3015862).

García-Magariño, I., Lacuesta, R., Rajarajan, M., and Lloret, J. 2019. "Security in Networks of Unmanned Aerial Vehicles for Surveillance with an Agent-Based Approach Inspired by the Principles of Blockchain," *Ad Hoc Networks* (86), Elsevier B.V., pp. 72–82. (https://doi.org/10.1016/J.ADHOC.2018.11.010).

Gharibi, M., Boutaba, R., and Waslander, S. L. 2016. "Internet of Drones," *IEEE Access* (4), Institute of Electrical and Electronics Engineers Inc., pp. 1148–1162. (https://doi.org/10.1109/ACCESS.2016.2537208).

Gope, P., and Sikdar, B. 2020. "An Efficient Privacy-Preserving Authenticated Key Agreement Scheme for Edge-Assisted Internet of Drones," *IEEE Transactions on Vehicular Technology* (69:11), Institute of Electrical and Electronics Engineers Inc., pp. 13621–13630. (https://doi.org/10.1109/TVT.2020.3018778).

Gorsuch, R. L. 1988. "Exploratory Factor Analysis," in *Handbook of Multivariate Experimental Psychology*, Boston, MA: Springer US, pp. 231–258. (https://doi.org/10.1007/978-1-4613-0893-5_6).

Guo, H., and Liu, J. 2020. "UAV-Enhanced Intelligent Offloading for Internet of Things at the Edge," *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS* (16:4). (https://doi.org/10.1109/TII.2019.2954944).

Gupta, L, Jain, R., and Vaszkun, G. 2016. "Survey of Important Issues in UAV Communication Networks," *IEEE Communications Surveys & Tutorials* (18:2), pp. 1123–1152. (https://doi.org/10.1109/COMST.2015.2495297).

Gupta, Lav, Jain, R., and Vaszkun, G. 2016. "Survey of Important Issues in UAV Communication Networks," *IEEE COMMUNICATIONS SURVEYS & TUTORIALS* (18:2), p. 1123. (https://doi.org/10.1109/COMST.2015.2495297).

Gupta, R., Shukla, A., Mehta, P., Bhattacharya, P., Tanwar, S., Tyagi, S., and Kumar, N. 2020a. "VAHAK: A Blockchain-Based Outdoor Delivery Scheme Using UAV for Healthcare 4.0 Services," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, July, pp. 255–260. (https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162738).

Gupta, R., Shukla, A., Mehta, P., Bhattacharya, P., Tanwar, S., Tyagi, S., and Kumar, N. 2020b. *VAHAK: A Blockchain-Based Outdoor Delivery Scheme Using UAV for Healthcare 4.0 Services; VAHAK: A Blockchain-Based Outdoor Delivery Scheme Using UAV for Healthcare 4.0 Services*.

Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., and Nauman, A. 2020a. *Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools,Techniques and Challenges*. (https://doi.org/10.1109/ACCESS.2020.2970576).

Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., and Kim, S. W. 2020b. "Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools, Techniques and Challenges," *IEEE Access* (8), pp. 24746–24772. (https://doi.org/10.1109/ACCESS.2020.2970576).

Gupta, R., Tanwar, S., Kumar, N., and Tyagi, S. 2020a. "Blockchain-Based Security Attack Resilience Schemes for Autonomous Vehicles in Industry 4.0: A Systematic Review," *Computers & Electrical Engineering* (86), p. 106717. (https://doi.org/10.1016/j.compeleceng.2020.106717).

Gupta, R., Tanwar, S., Kumar, N., and Tyagi, S. 2020b. "Blockchain-Based Security Attack Resilience Schemes for Autonomous Vehicles in Industry 4.0: A Systematic Review R," *Computers and Electrical Engineering* (86), p. 106717. (https://doi.org/10.1016/j.compeleceng.2020.106717).

Gupta, R., Tanwar, S., Kumar, N., and Tyagi, S. 2020c. "Blockchain-Based Security Attack Resilience Schemes for Autonomous Vehicles in Industry 4.0: A Systematic Review," *Computers & Electrical Engineering* (86), p. 106717. (https://doi.org/10.1016/j.compeleceng.2020.106717).

Gupta, R., Tanwar, S., Tyagi, S., and Kumar, N. 2019a. "Tactile Internet and Its Applications in 5G Era: A Comprehensive Review," *International Journal of Communication Systems* (32:14), John Wiley and Sons Ltd. (https://doi.org/10.1002/DAC.3981).

Gupta, R., Tanwar, S., Tyagi, S., and Kumar, N. 2019b. "Tactile-Internet-Based Telesurgery System for Healthcare 4.0: An Architecture, Research Challenges, and Future Directions," *IEEE Network* (33:6), Institute of Electrical and Electronics Engineers Inc., pp. 22–29. (https://doi.org/10.1109/MNET.001.1900063).

Gupta, R., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., and Sadoun, B. 2019. "HaBiTs: Blockchain-Based Telesurgery Framework for Healthcare 4.0," in *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, IEEE, August, pp. 1–5. (https://doi.org/10.1109/CITS.2019.8862127).

Harbi, Y., Medani, K., Gherbi, C., Senouci, O., Aliouat, Z., and Harous, S. 2023a. "A Systematic Literature Review of Blockchain Technology for Internet of Drones Security," *Arabian Journal for Science and Engineering* (48:2), pp. 1053–1074. (https://doi.org/10.1007/s13369-022-07380-6).

Harbi, Y., Medani, K., Gherbi, C., Senouci, O., Aliouat, Z., and Harous, S. 2023b. "A Systematic Literature Review of Blockchain Technology for Internet of Drones Security," *Arabian Journal for Science and Engineering* (48:2), pp. 1053–1074. (https://doi.org/10.1007/s13369-022-07380-6).

Hassija, V., Saxena, V., and Chamola, V. 2020. "A Blockchain-Based Framework for Drone-Mounted Base Stations in Tactile Internet Environment; A Blockchain-Based Framework for Drone-Mounted Base Stations in Tactile Internet Environment," *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*.

Hathaliya, J., Sharma, P., Tanwar, S., and Gupta, R. 2019. *Blockchain-Based Remote Patient Monitoring in Healthcare 4.0*.

Hayat, S., Yanmaz, E., and Muzaffar, R. 2016. "Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint; Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint," *IEEE Communications Surveys & Tutorials* (18:4). (https://doi.org/10.1109/COMST.2016.2560343).

Hussain, S., Chaudhry, A., Alomari, A., Alsharif, M. H., Khurram Khan, M., and Kumar, N. 2021. "Amassing the Security: An ECC-Based Authentication Scheme for Internet of Drones; Amassing the Security: An ECC-Based Authentication Scheme for Internet of Drones," *IEEE Systems Journal* (15:3). (https://doi.org/10.1109/JSYST.2021.3057047).

Khan, A. A., Khan, M. M., Khan, K. M., Arshad, J., and Ahmad, F. 2021. "A Blockchain-Based Decentralized Machine Learning Framework for Collaborative Intrusion Detection within UAVs," *Computer Networks* (196), Elsevier B.V. (https://doi.org/10.1016/J.COMNET.2021.108217).

Khan, A. A., Laghari, A. A., Shafiq, M., Awan, S. A., and Gu, Z. 2022. "Vehicle to Everything (V2X) and Edge Computing: A Secure Lifecycle for UAV-Assisted Vehicle Network and Offloading with Blockchain," *Drones* (6:12), p. 377. (https://doi.org/10.3390/drones6120377).

Kim, H., Park, J., Bennis, M., and Kim, S.-L. 2020. "Blockchained On-Device Federated Learning; Blockchained On-Device Federated Learning," *IEEE Communications Letters* (24:6), p. 1279. (https://doi.org/10.1109/LCOMM.2019.2921755).

Kumar, V., Ali, R., and Sharma, P. K. 2024a. "IoV-6G+: A Secure Blockchain-Based Data Collection and Sharing Framework for Internet of Vehicles in 6G-Assisted Environment," *Vehicular Communications* (47), p. 100783. (https://doi.org/10.1016/j.vehcom.2024.100783).

Kumar, V., Ali, R., and Sharma, P. K. 2024b. "IoV-6G+: A Secure Blockchain-Based Data Collection and Sharing Framework for Internet of Vehicles in 6G-Assisted Environment," *Vehicular Communications* (47), p. 100783. (https://doi.org/10.1016/j.vehcom.2024.100783).

Lim, Luong, Hoang, Jiao, Liang, Yang, Niyato, and Miao. 2020. "Federated Learning in Mobile Edge Networks: A Comprehensive Survey; Federated Learning in Mobile Edge Networks: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials* (22:3). (https://doi.org/10.1109/COMST.2020.2986024).

Liu, C. H., Lin, Q., and Wen, S. 2019. "Blockchain-Enabled Data Collection and Sharing for Industrial IoT With Deep Reinforcement Learning," *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS* (15:6). (https://doi.org/10.1109/TII.2018.2890203).

Liu, Y., Xiong, K., Ni, Q., Member, S., Fan, P., and Ben Letaief, K. 2020. "UAV-Assisted Wireless Powered Cooperative Mobile Edge Computing: Joint Offloading, CPU Control, and Trajectory Optimization; UAV-Assisted Wireless Powered Cooperative Mobile Edge Computing: Joint Offloading, CPU Control, and Trajectory Optimization," *IEEE Internet of Things Journal* (7:4). (https://doi.org/10.1109/JIOT.2019.2958975).

Lotka, A. J. 1926. “The Frequency Distribution of Scientific Productivity,” *Journal of the Washington Academy of Sciences* (16:12), Washington Academy of Sciences, pp. 317–323. (http://www.jstor.org/stable/24529203).

Lu, Y., Huang, X., Dai, Y., Maharjan, S., and Zhang, Y. 2020. “Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT,” *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS* (16:6), p. 4177. (https://doi.org/10.1109/TII.2019.2942190).

Mach, P., and Becvar, Z. 2017. “Mobile Edge Computing: A Survey on Architecture and Computation Offloading,” *IEEE Communications Surveys and Tutorials* (19:3), Institute of Electrical and Electronics Engineers Inc., pp. 1628–1656. (https://doi.org/10.1109/COMST.2017.2682318).

McCain, K. W. 1990. “Mapping Authors in Intellectual Space: A Technical Overview,” *Journal of the American Society for Information Science* (41:6), pp. 433–443. (https://doi.org/10.1002/(SICI)1097-4571(199009)41:6<433::AID-ASI11>3.0.CO;2-Q).

Mehta, P., Gupta, R., and Tanwar, S. 2020. “Blockchain Envisioned UAV Networks: Challenges, Solutions, and Comparisons,” *Computer Communications* (151), pp. 518–538. (https://doi.org/10.1016/j.comcom.2020.01.023).

Mollah, M. B., Zhao, J., Niyato, D., Guan, Y. L., Yuen, C., Sun, S., Lam, K.-Y., and Koh, L. H. 2021. “Blockchain for the Internet of Vehicles Towards Intelligent Transportation Systems: A Survey,” *IEEE Internet of Things Journal* (8:6), pp. 4157–4185. (https://doi.org/10.1109/JIOT.2020.3028368).

Motlagh, N. H., Bagaa, M., and Taleb, T. 2017. “UAV-Based IoT Platform: A Crowd Surveillance Use Case,” *IEEE Communications Magazine* (55:2), Institute of Electrical and Electronics Engineers Inc., pp. 128–134. (https://doi.org/10.1109/MCOM.2017.1600587CM).

Mozaffari, M., Member, Student, Saad, Walid, Member, Senior, Bennis, M., Debbah, M., Mozaffari Mozaffari, M. M., and Saad, W. 2017. “Mobile Unmanned Aerial Vehicles (UAVs) for Energy-Efficient Internet of Things Communications,” *IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS* (16:11). (https://doi.org/10.1109/TWC.2017.2751045).

Niknam, S., Dhillon, H. S., and Reed, J. H. 2020. “Federated Learning for Wireless Communications: Motivation, Opportunities, and Challenges; Federated Learning for Wireless Communications: Motivation, Opportunities, and Challenges,” *IEEE Communications Magazine* (58). (https://doi.org/10.1109/MCOM.001.1900461).

Nikooghadam, M., Amintoosi, H., Islam, S. H., and Moghadam, M. F. 2021. “A Provably Secure and Lightweight Authentication Scheme for Internet of Drones for Smart City Surveillance,” *Journal of Systems Architecture* (115), North-Holland, p. 101955. (https://doi.org/10.1016/J.SYSARC.2020.101955).

Novo, O. 2018. “Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT; Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT,” *IEEE INTERNET OF THINGS JOURNAL* (5:2). (https://doi.org/10.1109/JIOT.2018.2812239).

Pokhrel, S. R. 2020. “Federated Learning Meets Blockchain at 6G Edge: A Drone-Assisted Networking for Disaster Response,” *DroneCom 2020 - Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond*, Association for Computing Machinery, Inc, pp. 49–54. (https://doi.org/10.1145/3414045.3415949).

Pu, C., and Li, Y. 2020. “Lightweight Authentication Protocol for Unmanned Aerial Vehicles Using Physical Unclonable Function and Chaotic System,” *IEEE Workshop on Local and Metropolitan Area Networks* (2020-July), IEEE Computer Society. (https://doi.org/10.1109/LANMAN49260.2020.9153239).

Rana, T., Shankar, A., Kamran Sultan, M., Patan, R., and Balusamy, B. 2019. *An Intelligent Approach for UAV and Drone Privacy Security Using Blockchain Methodology; An Intelligent Approach for UAV and Drone Privacy Security Using Blockchain Methodology*.

Shahmoradi, J., Talebi, E., Roghanchi, P., and Hassanalian, M. 2020. “A Comprehensive Review of Applications of Drone Technology in the Mining Industry,” *Drones* (4:3), p. 34. (https://doi.org/10.3390/drones4030034).

Shen, M., Tang, X., Zhu, L., and Guizani, M. 2019. “Privacy-Preserving Support Vector Machine Training Over Blockchain-Based Encrypted IoT Data in Smart Cities,” *IEEE INTERNET OF THINGS JOURNAL* (6:5). (https://doi.org/10.1109/JIOT.2019.2901840).

Sheth, K., Patel, K., Shah, H., Tanwar, S., Gupta, R., and Kumar, N. 2020. “A Taxonomy of AI Techniques for 6G Communication Networks,” *Computer Communications* (161), Elsevier B.V., pp. 279–303. (https://doi.org/10.1016/J.COMCOM.2020.07.035).

Singh, M., Singh Aujla, G., and Singh Bali, R. 2020. *ODOB: One Drone One Block-Based Lightweight Blockchain Architecture for Internet of Drones; ODOB: One Drone One Block-Based Lightweight Blockchain Architecture for Internet of Drones*.

Singh, M., Singh Aujla, G., and Singh Bali, R. 2021. “A Deep Learning-Based Blockchain Mechanism for Secure Internet of Drones Environment,” *IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS* (22:7). (https://doi.org/10.1109/TITS.2020.2997469).

Small, H. 1973. “Co-citation in the Scientific Literature: A New Measure of the Relationship between Two Documents,” *Journal of the American Society for Information Science* (24:4), pp. 265–269. (https://doi.org/10.1002/asi.4630240406).

Small, H. 2006. “Tracking and Predicting Growth Areas in Science,” *Scientometrics* (68:3), pp. 595–610. (https://doi.org/10.1007/s11192-006-0132-y).

Srinivas, J., Das, A. K., Kumar, N., and Rodrigues, J. J. P. C. 2019. "TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment," *IEEE Transactions on Vehicular Technology* (68:7), Institute of Electrical and Electronics Engineers Inc., pp. 6903–6916. (https://doi.org/10.1109/TVT.2019.2911672).

Su, Z., Wang, Y., Xu, Q., and Zhang, N. 2022. "LVBS: Lightweight Vehicular Blockchain for Secure Data Sharing in Disaster Rescue," *IEEE Transactions on Dependable and Secure Computing* (19:1), Institute of Electrical and Electronics Engineers Inc., pp. 19–32. (https://doi.org/10.1109/TDSC.2020.2980255).

Tang, X., Lan, X., Li, L., Zhang, Y., and Han, Z. 2022. "Incentivizing Proof-of-Stake Blockchain for Secured Data Collection in UAV-Assisted IoT: A Multi-Agent Reinforcement Learning Approach," *IEEE Journal on Selected Areas in Communications* (40:12), pp. 3470–3484. (https://doi.org/10.1109/JSAC.2022.3213360).

Tanwar, S., Bhatia, Q., Patel, P., Kumari, A., Kumar Singh, P., and Hong, W.-C. 2019. *Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward*. (https://doi.org/10.1109/ACCESS.2019.2961372).

Tanwar, S., Parekh, K., and Evans, R. 2020. "Blockchain-Based Electronic Healthcare Record System for Healthcare 4.0 Applications," *Journal of Information Security and Applications* (50), Elsevier Ltd. (https://doi.org/10.1016/J.JISA.2019.102407).

Tanwar, S., Vora, J., Tyagi, S., Kumar, N., and Obaidat, M. S. 2018. "A Systematic Review on Security Issues in Vehicular Ad Hoc Network," *Security and Privacy* (1:5), Wiley, p. e39. (https://doi.org/10.1002/SPY2.39).

Tian, Y., Yuan, J., and Song, H. 2019. "Efficient Privacy-Preserving Authentication Framework for Edge-Assisted Internet of Drones," *Journal of Information Security and Applications* (48), Elsevier Ltd. (https://doi.org/10.1016/J.JISA.2019.06.010).

Tychola, K. A., Voulgaridis, K., and Lagkas, T. 2024a. "Beyond Flight: Enhancing the Internet of Drones with Blockchain Technologies," *Drones* (8:6), p. 219. (https://doi.org/10.3390/drones8060219).

Tychola, K. A., Voulgaridis, K., and Lagkas, T. 2024b. "Beyond Flight: Enhancing the Internet of Drones with Blockchain Technologies," *Drones* (8:6), p. 219. (https://doi.org/10.3390/drones8060219).

Wang, S., Tuor, T., Salonidis, T., Leung, K. K., Makaya, C., and Chan, K. 2019. "Adaptive Federated Learning in Resource Constrained Edge Computing Systems," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS* (37:6), p. 1205. (https://doi.org/10.1109/JSAC.2019.2904348).

Wang, Y., Su, Z., Zhang, N., and Benslimane, A. 2021. "Learning in the Air: Secure Federated Learning for UAV-Assisted Crowdsensing," *IEEE Transactions on Network Science and Engineering*. (https://doi.org/10.1109/TNSE.2020.3014385).

Wazid, M., Das, A. K., Kumar, N., Vasilakos, A. V., and Rodrigues, J. J. P. C. 2019. "Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment," *IEEE Internet of Things Journal* (6:2), Institute of Electrical and Electronics Engineers Inc., pp. 3572–3584. (https://doi.org/10.1109/JIOT.2018.2888821).

White, H. D., and Griffith, B. C. 1981. "Author Cocitation: A Literature Measure of Intellectual Structure," *Journal of the American Society for Information Science* (32:3), pp. 163–171. (https://doi.org/10.1002/asi.4630320302).

White, H. D., and McCain, K. W. 1998. "Visualizing a Discipline: An Author Co-Citation Analysis of Information Science, 1972–1995," *Journal of the American Society for Information Science* (49:4), pp. 327–355. (https://doi.org/10.1002/(SICI)1097-4571(19980401)49:4<327::AID-ASI4>3.0.CO;2-4).

Xiao, W., Li, M., Alzahrani, B., Alotaibi, R., Barnawi, A., and Ai, Q. 2021. "A Blockchain-Based Secure Crowd Monitoring System Using UAV Swarm," *IEEE Network* (35:1), Institute of Electrical and Electronics Engineers Inc., pp. 108–115. (https://doi.org/10.1109/MNET.011.2000210).

Xiong, Z., Member, Student, Feng, Shaohan, Wang, Wenbo, Niyato, Dusit, Wang, P., Member, Senior, Han, Z., Wang Xiong, P. Z., Feng, S, Wang, W, and Niyato, D. 2019. "Cloud/Fog Computing Resource Management and Pricing for Blockchain Networks; Cloud/Fog Computing Resource Management and Pricing for Blockchain Networks," *IEEE Internet of Things Journal* (6:3). (https://doi.org/10.1109/JIOT.2018.2871706).

Xiong, Z., Zhang, Y., Niyato, D., Wang, P., and Han, Z. 2018. "When Mobile Blockchain Meets Edge Computing; When Mobile Blockchain Meets Edge Computing," *IEEE Communications Magazine* (56). (https://doi.org/10.1109/MCOM.2018.1701095).

Xu, H., Huang, W., Zhou, Y., Yang, D., Li, M., and Han, Z. 2021. "Edge Computing Resource Allocation for Unmanned Aerial Vehicle Assisted Mobile Network With Blockchain Applications," *IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS* (20:5), p. 3107. (https://doi.org/10.1109/TWC.2020.3047496).

Xu, X., Zhao, H., Yao, H., and Wang, S. 2021. "A Blockchain-Enabled Energy-Efficient Data Collection System for UAV-Assisted IoT," *IEEE INTERNET OF THINGS JOURNAL* (8:4). (https://doi.org/10.1109/JIOT.2020.3030080).

Yahuza, M., Idris, M. Y. I., Wahab, A. W. A., Nandy, T., Ahmedy, I. Bin, and Ramli, R. 2021. "An Edge Assisted Secure Lightweight Authentication Technique for Safe Communication on the Internet of Drones Network," *IEEE Access* (9), Institute of Electrical and Electronics Engineers Inc., pp. 31420–31440. (https://doi.org/10.1109/ACCESS.2021.3060420).

Yang, Q., Liu, Y., Chen, T., and Tong, Y. 2019. "Federated Machine Learning: Concept and Applications," *ACM Transactions on Intelligent Systems and Technology (TIST)* (10:2), ACM PUB27 New York, NY, USA . (https://doi.org/10.1145/3298981).

Yazdinejad, A., Parizi, R. M., Dehghantanha, A., Srivastava, G., and Aledhari, M. 2021. "Enabling Drones in the Internet of Things With Decentralized Blockchain-Based Security," *IEEE INTERNET OF THINGS JOURNAL* (8:8). (https://doi.org/10.1109/JIOT.2020.3015382).

Yu, Z., Gong, Y., Gong, S., and Guo, Y. 2020. "Joint Task Offloading and Resource Allocation in UAV-Enabled Mobile Edge Computing," *IEEE Internet of Things Journal* (7:4), pp. 3147–3159. (https://doi.org/10.1109/JIOT.2020.2965898).

Zeng, T., Semiari, O., Mozaffari, M., Chen, M., Saad, W., and Bennis, M. 2020. "Federated Learning in the Sky: Joint Power Allocation and Scheduling with UAV Swarms," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, IEEE, June, pp. 1–6. (https://doi.org/10.1109/ICC40277.2020.9148776).

Zhang, Y., He, D., Li, L., and Chen, B. 2020. "A Lightweight Authentication and Key Agreement Scheme for Internet of Drones," *Computer Communications* (154), Elsevier B.V., pp. 455–464. (https://doi.org/10.1016/J.COMCOM.2020.02.067).

Zhao, Y., Student Member, G., Zhao, J., Jiang, L., Tan, R., Member, S., Niyato, D., Li, Z., Lyu, L., Liu, Y., and Zhao Yang Zhao, J. 2021. "Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices; Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices," *IEEE Internet of Things Journal* (8:3). (https://doi.org/10.1109/JIOT.2020.3017377).

Zhou, F., Wu, Y., Member, S., Qingyang Hu, R., and Qian, Y. 2018. "Computation Rate Maximization in UAV-Enabled Wireless-Powered Mobile-Edge Computing Systems," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS* (36:9). (https://doi.org/10.1109/JSAC.2018.2864426).

Zhou, Y., Pan, C., Yeoh, L., Wang, K., Elkashlan, M., Vucetic, B., and Li, Y. 2020. "Secure Communications for UAV-Enabled Mobile Edge Computing Systems," *IEEE TRANSACTIONS ON COMMUNICATIONS* (68:1). (https://doi.org/10.1109/TCOMM.2019.2947921).

Zhou, Z., Member, S., Feng, Junhao, Gu, B., Ai, B., Mumtaz, Shahid, Rodriguez, J., Guizani, M., Guizani Zhou, M. Z., Feng, J, and Mumtaz, S. 2018. "When Mobile Crowd Sensing Meets UAV: Energy-Efficient Task Assignment and Route Planning," *IEEE TRANSACTIONS ON COMMUNICATIONS* (66:11). (https://doi.org/10.1109/TCOMM.2018.2857461).

Zhu, L., Wu, Y., Gai, K., and Choo, K. K. R. 2019. "Controllable and Trustworthy Blockchain-Based Cloud Data Management," *Future Generation Computer Systems* (91), Elsevier B.V., pp. 527–535. (https://doi.org/10.1016/J.FUTURE.2018.09.019).

Zipf, G. K. 1949. “Human Behavior and the Principle of Least Effort.,” *Human Behavior and the Principle of Least Effort.*, Oxford, England: Addison-Wesley Press.

Zupic, I., and Čater, T. 2015. “Bibliometric Methods in Management and Organization,” *Organizational Research Methods* (18:3), pp. 429–472. (https://doi.org/10.1177/1094428114562629).