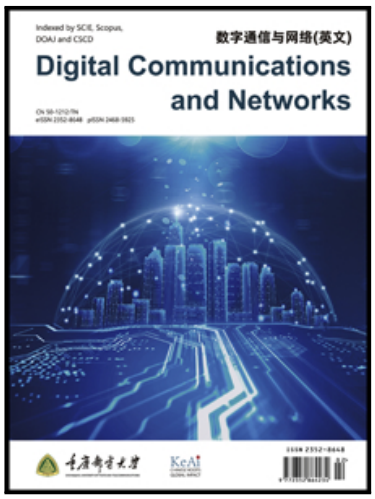
Journal Pre-proof



Blockchain-enhanced UAV networks for post-disaster communication: A decentralized flocking approach

Sana Hafeez, Runze Cheng, Lina Mohjazi, Yao Sun, Muhammad Ali Imran

PII: S2352-8648(26)00024-6
DOI: https://doi.org/10.1016/j.dcan.2026.03.006
Reference: DCAN 962

To appear in: *Digital Communications and Networks*

Received date: 10 October 2024
Revised date: 16 March 2026
Accepted date: 20 March 2026

Please cite this article as: Sana Hafeez, Runze Cheng, Lina Mohjazi, Yao Sun, Muhammad Ali Imran, Blockchain-enhanced UAV networks for post-disaster communication: A decentralized flocking approach, *Digital Communications and Networks* (2025), doi: https://doi.org/10.1016/j.dcan.2026.03.006

Journal Pre-proof
HOSTED BY
ELSEVIER
Available online at www.sciencedirect.com
ScienceDirect
journal homepage: www.elsevier.com/locate/dcan
DCN Digital Communications and Networks

Blockchain-enhanced UAV networks for post-disaster communication: A decentralized flocking approach

Sana Hafeez[a,1], Runze Cheng[a], Lina Mohjazi[a], Yao Sun[a,*], Muhammad Ali Imran[a]
[a]James Watt School of Engineering, University of Glasgow, Glasgow G12 8QQ, UK

Abstract

Unmanned Aerial Vehicles (UAVs) have significant potential for agile communication and relief coordination in post-disaster scenarios, especially when conventional ground infrastructure is compromised. However, effectively coordinating and securing swarms of heterogeneous UAVs from multiple service providers presents critical challenges related to privacy, scalability, lightweight consensus protocols, and cybersecurity resilience. This study proposes a blockchain-enabled UAV coordination framework that leverages consensus mechanisms, smart contracts, and cryptographic techniques to address these challenges. First, a consortium blockchain architecture is introduced, integrating Zero-Knowledge Proofs (ZKPs) to enable privacy-preserving, multi-agency coordination while ensuring access control and data security. Second, a hybrid Delegated Proof-of-Stake–Practical Byzantine Fault Tolerance (DPoS-PBFT) consensus protocol is developed to optimise security, efficiency, and resilience against node failures in resource-constrained UAV networks. Third, a decentralized flocking algorithm is proposed to enable adaptive and autonomous UAV cluster operations under dynamically changing connectivity conditions, ensuring seamless disaster relief functions. Comprehensive simulations show that the proposed system scales efficiently to 500 UAV nodes while maintaining high throughput and low latency, with only a 50-ms increase in latency from 10 to 500 nodes. The framework demonstrates strong cyber resilience, remaining robust under denial-of-service (DoS), spoofing, and tampering attacks. Furthermore, communication latencies remain under 10 milliseconds, with median values of approximately 2–3 ms, achieved through self-optimizing network intelligence. The results validate the proposed system as a secure, scalable, and high-performance solution for UAV-enabled disaster response, ensuring reliable emergency communication and efficient resource allocation in critical environments.

KEYWORDS: Blockchain, Unmanned aerial vehicles (UAVs), Emergency communications, Data privacy, Aerial communications, Secure wireless networks

1. Introduction

Natural disasters, such as hurricanes, floods, and earthquakes, can severely damage critical communication infrastructure, disrupting access to aid and relief coordination. In recent years, Unmanned Aerial Vehicles (UAVs) has emerged as a promising solution to rapidly restore connectivity in post-disaster scenarios. However, coordinating heterogeneous UAV flocks poses significant challenges in terms of security, privacy, and scalability [1]. This study proposes a novel framework using blockchain technology to address these limitations and improve UAV operations in disaster response situations.

1.1. Background and Motivation

Intelligent emergency communication systems ensure effective network connectivity during disaster-response scenarios. UAVs have proven to be effective in expanding wireless coverage for Internet Of Things (IoT) devices due to their ability to hover in diverse locations and establish reliable links [2]-[3]. However, the deployment of UAV fleets in disaster response faces several challenges, including limited flight endurance [4], restricted communication range [5], reliance on potentially damaged ground networks, and inadequate pre-planned routes [6]. Additionally, intermittent connectivity [7], lack of coordination between UAVs and human responders, security vulnerabilities arising from chaotic environments, and insufficient transparency mechanisms further complicate their effective utilization.

Recent research has explored decentralized blockchain approaches to help overcome some of these obstacles through inherent attributes such as distribution, security, transparency, automation, and resilience [8]. However, significant gaps remain before blockchain technology can be successfully incorporated into UAV networks for disaster response [9]. Blockchain integration introduces new challenges related to consensus mechanisms, interoperability, security, and smart contract design, specifically for decentralized disaster-resilient UAV fleet coordination [10].

*Corresponding author.
[1]This paper was submitted in part to IEEE VTC2024-Spring, Singapore.
[2]*E-mail addresses:*
S.Hafeez@ljmu.ac.uk (S. Hafeez)
Runze.Cheng@glasgow.ac.uk (R. Cheng)
Lina.Mohjazi@glasgow.ac.uk (L. Mohjazi)
Yao.Sun@glasgow.ac.uk (Y. Sun)
Muhammad.Imran@glasgow.ac.uk (M.A. Imran)

1.2. Related Work and Research Gaps

Existing work in blockchain-enabled UAV networks has primarily focused on addressing security issues in UAV swarms [11]. Researchers have explored building internal trust using blockchain [12], such as Universal Practical Byzantine Fault Tolerance (U-PBFT) for lightweight consensus and real-time trust evaluation [13]. However, the dynamic topology and limited resources of UAVs pose additional challenges [14], highlighting the need for secure, efficient, and intelligent blockchain coordination frameworks tailored for disaster-response UAVs. Despite these advancements, several research gaps persist in areas such as real-time data processing efficiency, scalability of blockchain solutions in large swarms, integration with existing air traffic control systems, and development of standardized interoperability protocols among diverse UAV systems. Furthermore, the potential environmental impact and ethical considerations related to surveillance and data privacy in blockchain-enabled UAV networks remain underexplored.

1.3. Proposed Framework and Contributions

To overcome these limitations, a comprehensive framework is introduced, integrating blockchain technology, advanced consensus protocols, and bio-inspired flocking algorithms to enhance UAV-based disaster response. Our approach aims to facilitate decentralized, efficient, and autonomous UAV-based operations even in challenging post-disaster environments, potentially improving the effectiveness of time-critical relief efforts [15]. The key contributions of this study are

1. We introduce a hybrid Delegated Proof Of Stake–Practical Byzantine Fault Tolerance (DPoS-PBFT) consensus approach that balances efficiency, security, and fault tolerance. This mechanism is specifically designed to address the constraints of UAV platforms and the volatility of aerial environments in disaster scenarios.

2. We incorporate bio-inspired flocking techniques based on Reynolds' rules to enable resilient coordination of UAV clusters under uncertain connectivity conditions during disaster relief operations.

3. We implement advanced privacy-preserving techniques, including ZKPs, to ensure secure and private data exchange among diverse stakeholders involved in disaster response efforts.

4. We present a holistic system architecture that addresses critical security and access control challenges in decentralized UAV fleets, enhancing overall disaster management capabilities.

5. Through extensive simulations, we demonstrate the efficiency and adaptability of our proposed blockchain-based coordination framework in dynamic environments with fluctuating resources, variable channel conditions, and diverse service requirements.

1.4. Paper Organization

The rest of this paper is organized as follows. Section 2 provides an overview of the relevant literature. Section 3 presents the architecture and the model of the proposed system. Section 4 details the decentralized flocking algorithm for UAV coordination. Section 5 describes a customized hybrid consensus protocol. Section 6 presents an analysis of the simulation setup and the results. Finally, Section 7 concludes the study and discusses future work.

2. Literature Review

This section presents a focused review of relevant literature on blockchain-enabled UAV solutions for disaster response, highlighting key advancements and persistent challenges in the field.

UAV ad hoc networks have gained significant attention due to their rapid deployment capabilities and resilience during disasters when ground infrastructure fails [22]-[23]. Blockchain technology has emerged as a promising approach to address security and coordination challenges in these networks, leveraging its inherent features of distributed trust and transparency [24].

Several studies have explored blockchain-based systems for UAV coordination in disaster response scenarios. Raja et al. [25] focused on secure information sharing, while Hafeez et al. [26] emphasized transparent data recording. Duan et al. [20] investigated accountability in relief distribution. However, these works primarily addressed specific aspects of UAV coordination, leaving gaps in comprehensive system design. Our study builds upon these foundations by proposing an integrated framework that combines secure information sharing, transparent data recording, and accountable resource distribution within a single, cohesive system. This holistic approach aims to address the limitations of previous works that focused on individual components in isolation.

The efficiency and fault tolerance of consensus protocols are critical factors in UAV networks, which typically involve resource-constrained nodes and intermittent connectivity. Sun et al. [27] highlighted the trade-offs between the Practical Byzantine Fault Tolerance (PBFT) and its high communication overhead. Wang et al. [28] proposed hybrid protocols combining PBFT and Proof-of-Authority (PoA) to balance efficiency and security. Building on these insights, our study introduces a novel DPoS-PBFT consensus approach. This mechanism is specifically designed to accommodate the unique constraints of UAV platforms and the volatility of aerial environments in disaster scenarios, addressing the limitations of existing consensus protocols in UAV networks.

Smart contracts have been explored to automate coordination and ensure transparency in disaster management scenarios. Afotanwo et al. [29] investigated applications including autonomous flight planning and decentralized information exchange. However, Paulin et al. [30] identified limitations in standard smart contract languages for handling spatial data required in UAV geo-coordination. Our work advances this field by developing geospatial smart contracts tailored for location-based UAV coordination. To enhance UAVdisaster response networks, extend smart contracts to improve spatial data storage and querying efficiency. A comprehensive analysis of the challenges in UAV networks for disaster response, along with blockchain-enabled solutions and existing research gaps, is presented in the Table. 1. This table highlights the key limitations of conventional UAVcommunication frameworks and demon-

Table 1: Comprehensive overview of challenges, blockchain-enabled solutions, and research gaps in UAV networks for disaster response

Category	Challenges and research gaps
Challenges in UAV-based disaster response [4],[16]	
Limited flight endurance	Battery dependence limits flight time and operational capability.
Restricted communication range	Requires multi-hop routing, which introduces delays.
Reliance on damaged infrastructure	Reduces navigation and control effectiveness.
Inadequate pre-planned trajectories	Dynamic environments need real-time path replanning.
Intermittent connectivity	Weather or mobility lead to disruptions.
Lack of coordination	Between UAVs, ground robots, and human responders.
Security vulnerabilities	Spoofing, tampering, hijacking due to chaos.
Communication and delivery	Low efficiency in communication and relief delivery.
Transparency and accountability	Lack of transparency in relief management.
Collaboration	Low collaboration due to different entity priorities.
Computing and energy	Centralised paradigms leading to failure points; energy constraints in UAV networks.
Communication channels	FL training issues due to UAV mobility and unreliable links.
Privacy and security	Data privacy concerns in UAV-based services.
Caching and delivery services	Challenges in content caching and UAV deployment.
Existing and proposed blockchain-enabled solutions [17],[1],[5],[18]	
Permissioned blockchains	For efficiency and privacy compared to public chains.
Lightweight consensus protocols	E.g., PBFT and PoA offer fault tolerance without mining.
Smart contracts	Automate coordination for flight plans and information sharing.
Tamper-proof data logging	Using blockchain to record UAV data.
Access control via smart contracts	Secure coordination by authentication.
Enhanced data integrity and security	Secure and immutable ledger for data integrity.
Improved resource allocation	Automated resource allocation via smart contracts.
Decentralised control	Reducing risks of central points of failure.
Transparent supply chain management	Real-time tracking and auditing of relief materials.
Identity management	Secure verification of individuals and organizations.
Real-time data sharing	Blockchain for efficient information exchange.
Supply chain automation	Blockchain for logistics and supply chain optimisation.
Tokenisation for incentivisation	Rewards for participation in disaster response.
Interoperability between systems	Seamless data exchange and coordination.
Open research challenges [10],[19],[20],[21],[22]	
Adaptive coordination algorithms	For dynamic environments and evolving needs.
Handling intermittent connectivity	In UAV blockchain networks.
UAV computational constraints	Limit complex chaincode and ledger size.
Geo-spatial smart contract support	Needed for location-based UAV coordination.
Security modelling and analysis	Against threats like DDoS and spoofing.
Privacy preservation	During UAV surveillance usage.
Multi-agency collaboration	For large-scale disaster response.
Optimisation of UAV payload and range	For efficient delivery and operation.
Robust systems for transparency	Ensuring accountability in relief operations.
Multi-stakeholder collaboration models	For effective information sharing.
Sustainable energy solutions	For UAV networks.
Enhanced privacy protection mechanisms	In UAV-based data gathering and AI model training.
Advanced algorithms for content caching	Efficient delivery services in UAV networks.
Effective tokenisation mechanisms	For incentivisation in disaster response efforts.
Standards and protocols for interoperability	Enhanced system integration in UAV networks.

strates how blockchain integration enhances security, scalability, and resilience in dynamic disaster scenarios.

Privacy and security concerns in blockchain-enabled UAV networks have been highlighted by several researchers. Nicolazzo et al. [31] explored privacy-preserving UAV coordination techniques, while Xing et al. [32] investigated geospatial smart contracts with privacy considerations. Building on these studies, our framework incorporates advanced privacy-preserving techniques, including ZKPs, to ensure secure and private data exchange among diverse stakeholders. This approach addresses the privacy concerns raised in previous works while maintaining the transparency benefits of blockchain technology.

In summary, while existing research has made significant strides in blockchain-enabled UAV networks for disaster response, challenges persist in scalability, lightweight consensus protocols, comprehensive privacy mechanisms, and effective utilization of smart contracts for spatial coordination. Our study aims to address these limitations by proposing an integrated framework that combines optimized consensus mechanisms, privacy-preserving techniques, and geospatial smart contracts tailored specifically for UAV-assisted disaster response scenarios.

While existing research has made significant strides in blockchain-enabled UAV networks for disaster response, sev-

eral critical gaps remain. These include the need for more scalable and energy-efficient consensus mechanisms tailored to UAV constraints, comprehensive privacy-preserving techniques for sensitive disaster data, and adaptive coordination algorithms for dynamic disaster environments. Our work addresses these gaps by introducing a novel framework that combines an optimized hybrid consensus protocol, advanced privacy-preserving methods including ZKPs, and bio-inspired flocking algorithms. This integrated approach aims to enhance the scalability, security, and adaptability of UAV networks in disaster scenarios, advancing beyond the limitations identified in current literature. The subsequent section presents the proposed system architecture and models, illustrating the approach taken to address these challenges.

The overall architecture of the proposed blockchain-enabled UAV coordination framework for disaster response is presented in Fig. 1. This architecture integrates a consortium blockchain, secure consensus mechanisms, and decentralized UAV coordination to enhance communication reliability, security, and scalability in post-disaster scenarios.

3. System Architecture and Models

This section describes the mathematical models used to characterize the architecture of UAV-based disaster response. Specifically, it includes models related to communication, mobility, flocking algorithms, reliability, and security. The communication model under discussion is primarily centered on the propagation characteristics of wireless links between UAVs in an aerial network. The *log-distance path-loss model* is a pivotal element of this model. This model is commonly used for modelling signal attenuation in Air-To-Air (A2A) channels, particularly in scenarios involving UAVs. The *log-distance path-loss model* is a fundamental concept in wireless communication. It is utilized to estimate the loss of signal strength, known as path loss [33], over distance. The model calculates this loss based on the logarithm of the distance between the transmitter and receiver. It considers the path loss exponent and the loss at a reference distance, making it particularly relevant in the context of UAV communications. This relevance stems from its utility in understanding and predicting signal strength variations over different distances in three-dimensional airspace. The mathematical symbols and variables used in the system model are detailed in the Table. 2, providing a concise reference for the notation used in our analytical framework.

3.1. Communication Model

The communication model defines the propagation characteristics of wireless links between UAVs to an aerial network A2A and between UAVs and ground users Air-To-Ground (A2G). To facilitate the derivations, a unified path loss model, Signal-To-Noise Ratio (SNR), and achievable data rate equations are introduced. Path loss quantifies signal attenuation influenced by distance and environmental conditions. A generalized path loss formulation is established for both A2A and A2G links as follows

$$\mathrm{PL}(d) = \mathrm{PL}_0 + 10n\log_{10}\left(\frac{d}{d_0}\right) + \chi \tag{1}$$

where $\mathrm{PL}(d)$ (dB) represents the total path loss at a separation distance d (m). The term χ is a log-normal fading variable, modeled as

$$\chi \sim \mathcal{N}(0, \sigma^2) \tag{2}$$

where σ (in dB) is the shadowing standard deviation, accounting for additional attenuation due to environmental obstructions. For A2G links, σ is typically higher (6–12 dB) due to terrain blockages, while for A2A links, shadowing is minimal (around 2–4 dB in open environments).

The received SNR for a link between a transmitting node i and receiving node j (which may be a UAV or ground user) is given by

$$\mathrm{SNR} = P_t + \mathcal{G}_i + \mathcal{G}_j - \mathrm{PL}(d) \tag{3}$$

where P_t is the transmit power, and $\mathcal{G}_i$ and $\mathcal{G}_j$ are the antenna gains of the transmitter and receiver, respectively. The maximum achievable data rate for a communication link is computed using Shannon's capacity formula

$$C = B\log_2(1 + \mathrm{SNR}) \tag{4}$$

where B is the channel bandwidth. For A2A communication, the reference distance d_0 is chosen based on free-space propagation conditions, while for A2G, the shadowing component χ captures terrain obstructions and urban effects. The models ensure a unified approach for evaluating both aerial and ground communication performance in disaster-response scenarios.

Table 2: Summary of Notations and Their Descriptions

Symbol	Description
$\mathrm{PL}(d_{ij})$	Path loss at distance d_{ij}.
PL_0	Path loss at reference distance d_0.
n	Path loss exponent.
d_0	Reference distance for path loss.
P_t	Transmit power of the UAV.
$\mathcal{G}_i, \mathcal{G}_j$	Antenna gains of UAVs i and j.
$\mathbf{P}_i, \mathbf{P}_j$	3D positions of UAVs i and j.
B	Channel bandwidth.
$T(N)$	Transaction throughput with N nodes.
$L(N)$	Communication latency with N nodes.
$D(t), S(t), T(t), M(t)$	Risk factors over time t.
$w_{\mathcal{D}}, w_{\mathcal{S}}, w_{\mathcal{T}}, w_{\mathcal{M}}$	Weights for risk factors.
$\lambda_{\mathcal{D}}, \lambda_{\mathcal{S}}, \lambda_{\mathcal{T}}, \lambda_{\mathcal{M}}$	Initial risk magnitudes.
$\mu_{\mathcal{D}}, \mu_{\mathcal{S}}, \mu_{\mathcal{T}}, \mu_{\mathcal{M}}$	Risk mitigation rates.
$\rho_i[\kappa], \Omega_i[\kappa]$	Position and velocity of UAV i at step κ.
$\Delta\tau$	Discrete time step size.
$\mathcal{A}$	Set of autonomous agents.
x_i, v_i	Position and velocity of agent i.
U_i	Control input for agent i.

3.2. Consortium Blockchain Architecture

This section outlines a consortium blockchain architecture tailored for decentralized coordination and access control in disaster response scenarios involving both service providers and UAV networks. Key parameters, such as the transaction throughput $T(N)$ and latency $L(N)$, are crucial for assessing the performance of the system and are analyzed using mathematical methods. The architecture is specifically designed to enhance communication, coordination, and data sharing among

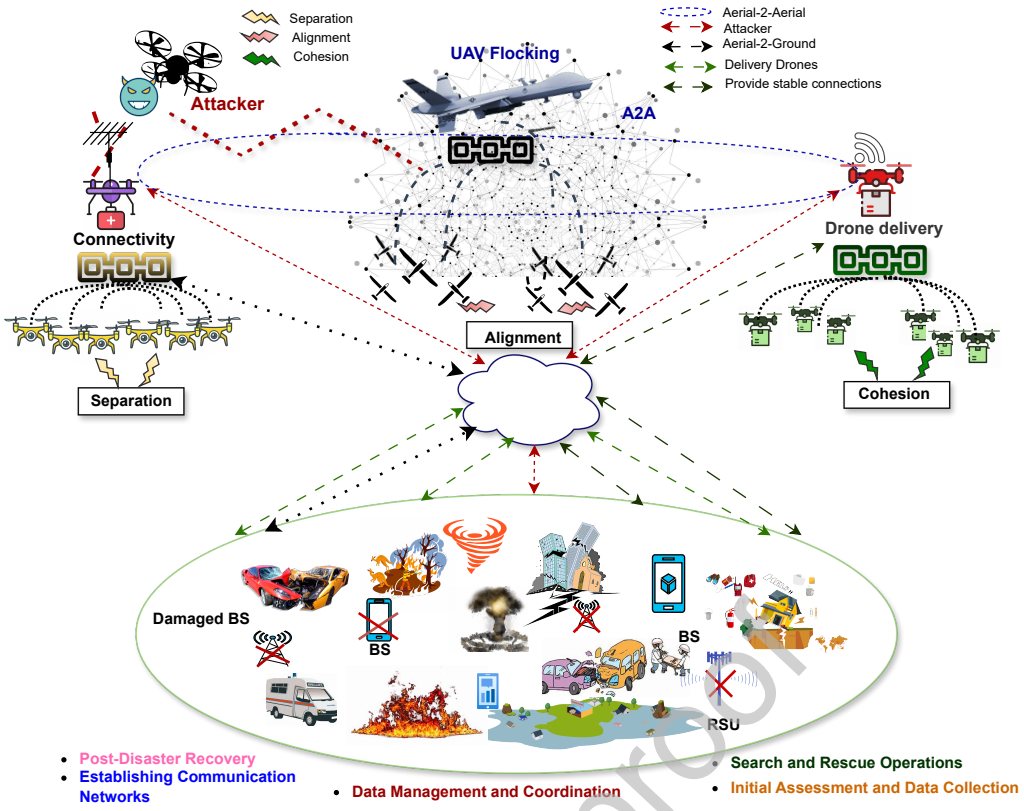


Fig. 1. The Architecture for Blockchain-Enabled UAV Coordination in Disaster Response.

the involved parties. Smart contracts establish robust access control policies. Each participating entity is assigned a specific permission $P(x)$ that dictates the level of access within the network. The function of a smart contract, denoted by $\mathrm{SC}_{\mathrm{ac}}(P(x), ac_i) \rightarrow \{\text{Allow, Deny}\}$, is to enforce these policies based on a set of predefined rules. ZKPs were employed to ensure privacy and security. ZKPs allow for the verification of transactions and data integrity without revealing the underlying information, thus preserving the confidentiality of sensitive data while maintaining trust and transparency in the network.

Performance metrics such as $T(N)$ and $L(N)$, where N represents the number of nodes in the network, were analyzed to understand their impact on the overall efficiency of the system. This analysis is particularly important because it provides insights into how the system's performance might vary with changes in scale and node density during disaster response operations. Moreover, the use of cryptographic methods, including ZKPs, has been highlighted to facilitate privacy-preserving coordination, particularly when handling sensitive information.

3.3. Challenges in Integrating Blockchain Techniques

Incorporating DPoS-PBFT consensus, geospatial smart contracts, and ZKP-based privacy mechanisms comes with several primary challenges: handling the scalability issues due to increased computational demands that impact transaction processing rates; achieving interoperability via standardized interfaces for smooth and reliable data transfer between diverse components; tackling resource limitations by developing lightweight blockchain protocols tailored for the constrained energy and processing capabilities of UAVs; modifying the consensus mechanism to suit the dynamic UAV networks marked by frequent changes in topology; achieving a balance between privacy and transparency through context-sensitive approaches to safeguard sensitive information; ensuring partition resilience to maintain operations during the frequent network disruptions seen in disaster scenarios; and adhering to regulatory standards that vary across jurisdictions. Tackling these intertwined challenges is essential to creating an effective and practical blockchain framework for UAV-enabled disaster response.

3.4. Influence of UAV Diversity on System Architecture

Variations in UAV hardware capabilities, communication protocols, and energy constraints play a crucial role in shaping system architecture design. To effectively address this diversity, several key features are integrated

Adaptive Blockchain Consensus Mechanism: Given the differences in processing and energy among UAV, our DPoS-PBFT hybrid consensus method assigns validation duties to UAV with higher computational capacities, easing blockchain loads on those with limited energy.

Hierarchical Network Architecture: A multi-layered network design allows high-capacity UAV to function as leader nodes for blockchain transaction oversight, while energy-constrained UAV act as relay nodes to enhance coordination.

Energy-Aware Smart Contracts: To minimize energy consumption, lightweight smart contracts are deployed to dynamically adjust processing requirements based on UAV battery levels, allowing low-energy UAV to offload tasks to edge or cloud resources.

Interoperable Communication Protocols: Supporting various standards such as 5G, LoRa, and Wi-Fi, our system includes protocol translation layers to maintain seamless blockchain synchronization.

Security and Trust Management: The diversity among UAV

poses security challenges, as older models may be vulnerable. Trust-based authentication is implemented by assigning dynamic trust scores to UAV, which are determined based on their security level and transaction history.

Dynamic Flight Path Optimization: To accommodate varying UAV flight capabilities, our system dynamically adjusts load distribution, manipulating UAV clusters and data routes to reduce network congestion and maximize resource allocation. These measures ensure our UAV network, optimized for blockchain, functions efficiently despite hardware and communication protocol differences, supporting reliable disaster-response functions.

3.5. Security Measurements

This section presents a quantitative assessment of the overall risk $\mathcal{X}(t)$ and resilience $R(t)$ of a UAV network, considering multiple threat factors such as Denial Of Service (DoS) attacks, spoofing, tampering, and malware infections [34]. The analytical framework facilitates a systematic evaluation of the effectiveness of the implemented security mechanisms.

3.5.1. Overall Risk Calculation

The overall risk at time t, denoted by $\mathcal{X}(t)$, is computed using the weighted sum of the individual risk factors. The formula for the overall risk is given by

$$\mathcal{X}(t) = w_{\mathcal{D}}D(t) + w_{\mathcal{S}}S(t) + w_{\mathcal{T}}T(t) + w_{\mathcal{M}}M(t) \tag{5}$$

In this equation, $D(t)$, $S(t)$, $T(t)$, and $M(t)$ represent the risks of DoS attacks, spoofing, tampering, and malware infections, respectively. The weights $w_{\mathcal{D}}, w_{\mathcal{S}}, w_{\mathcal{T}}, w_{\mathcal{M}}$ reflect the relative importance of each risk factor.

3.5.2. Risk Factors Modeling

Each risk factor is modeled to capture its evolution over time, characterized by an initial risk magnitude and a mitigation rate. The meanings and modeling of these factors are detailed as follows

Denial of Service (DoS) Attack Risk, $D(t)$:. Represents the risk associated with DoS attacks, which aim to make the UAV network unavailable by overwhelming it with traffic.

$$D(t) = \lambda_{\mathcal{D}}e^{-\mu_{\mathcal{D}}t} \tag{6}$$

Where, $\lambda_{\mathcal{D}}$ is the initial magnitude of the DoS risk, and $\mu_{\mathcal{D}}$ is the mitigation rate, representing how quickly the network can reduce the risk over time.

Spoofing Risk, $S(t)$:. Represents the risk of spoofing attacks, where an attacker impersonates legitimate UAV or ground control stations to gain unauthorized access or disrupt operations.

$$S(t) = \lambda_{\mathcal{S}}(1 - e^{-\mu_{\mathcal{S}}t}) \tag{7}$$

In this model, $\lambda_{\mathcal{S}}$ is the initial magnitude of the spoofing risk, and $\mu_{\mathcal{S}}$ is the mitigation rate, indicating how effectively the network can counteract spoofing attempts over time.

Tampering Risk, $T(t)$:. Represents the risk of tampering attacks, where an attacker physically or remotely alters the UAVs hardware or software to disrupt its functionality.

$$T(t) = \lambda_{\mathcal{T}}te^{-\mu_{\mathcal{T}}t} \tag{8}$$

The parameter, $\lambda_{\mathcal{T}}$ is the initial magnitude of the tampering risk, and $\mu_{\mathcal{T}}$ is the mitigation rate, showing how the risk evolves and decreases over time.

Malware Infection Risk, $M(t)$:. Represents the risk of malware infections, where malicious software is introduced into the UAV network to steal information, disrupt operations, or cause damage.

$$M(t) = \lambda_{\mathcal{M}}(1 - e^{-\mu_{\mathcal{M}}t}) \tag{9}$$

Here, $\lambda_{\mathcal{M}}$ is the initial magnitude of the malware risk, and $\mu_{\mathcal{M}}$ is the mitigation rate, reflecting the network's ability to detect and remove malware over time. The 2D spatial distribution of flocking UAVs engaged in post-disaster activities is illustrated in Fig. 2. This Fig demonstrates the UAV swarm's adaptive behavior in dynamic environments, ensuring efficient coverage and coordination. A more detailed discussion of the UAV movement and clustering mechanisms is provided in Section 4.

3.6. Energy-Aware Resource Management

To mitigate the critical energy constraints of UAV in disaster response scenarios, an adaptive power management system is integrated within the blockchain framework. This system dynamically adjusts the UAV's transmission power P_{tx} based on the current network conditions and remaining battery life B_r

$$P_{\text{tx}} = P_{\min} + (P_{\max} - P_{\min}) \times \left(\frac{B_r}{B_{\text{total}}}\right) \times f(\text{SINR}) \tag{10}$$

where $P_{\min}$ and $P_{\max}$ are the minimum and maximum transmission powers, B_{total} is the total battery capacity, and $f(\text{SINR})$ is a function of the current Signal-to-Interference-plus-Noise Ratio. This approach ensures optimal energy utilization while maintaining necessary communication quality. An energy-aware task allocation mechanism is incorporated within the smart contracts to optimise resource distribution and prolong UAV network operation. The mechanism prioritizes tasks τ_i for each UAVu_j based on their energy cost $E(\tau_i)$ and remaining battery life $B_r(u_j)$

$$\text{Priority}(\tau_i, u_j) = w_1 \times \left(\frac{1}{E(\tau_i)}\right) + w_2 \times \left(\frac{B_r(u_j)}{B_{\text{total}}}\right) \tag{11}$$

where w_1 and w_2 are weighting factors. This prioritization ensures efficient use of available energy resources across the UAV network while maintaining critical disaster response capabilities.

4. Decentralized Flocking Model for UAV Disaster Response

This section presents a decentralized flocking model designed to enable resilient coordination among specialized UAV clusters conducting critical disaster-relief functions, even amidst disrupted connectivity.

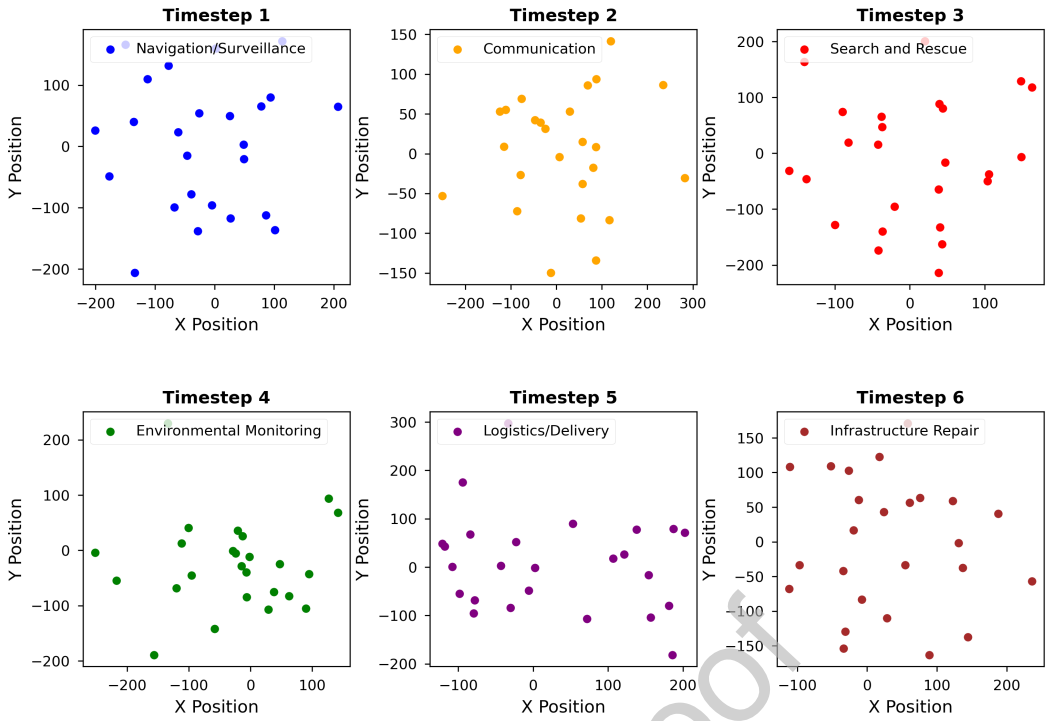


Fig. 2. The 2D Spatial Distribution of Flocking UAVs e Engaged in Post-disaster Activities. More detailed Description is Provided in Section 4.

4.1. Concrete Examples of Flocking Algorithms for UAV Disaster Relief Functions

The proposed UAV network is heterogeneous and comprises several specialized clusters: the delivery network S_λ, focused on transporting relief supplies; the survey network S_η, assigned to rapid damage assessment; and the connectivity network S_Ω, responsible for restoring communication links. A central UAV monitor, Υ_m, dynamically adjusts high-level coordination strategies based on evolving disaster-response priorities. The delivery flock $\mathcal{S}_\lambda$ plays a pivotal role in immediate relief efforts by transporting essential supplies to affected areas. Using flocking algorithms, these UAV maintain cohesion, alignment, and separation to ensure efficient and safe aid delivery. The survey flock $\mathcal{S}_\eta$ focuses on damage assessment and mapping. Employing flocking strategies, these UAV can systematically cover disaster areas, maintain communication, and avoid collisions. The connectivity flocks $\mathcal{S}_\Omega$ are aligned with 3rd Generation Partnership Project (3GPP) UAV standards to ensure efficient communication restoration in disaster-stricken areas. UAV use flocking rules to maintain optimal formation for wireless coverage and to navigate safely through the environment. The central monitor UAV, Υ_m, coordinates the activities of these flocks by utilizing a decentralized coordination algorithm based on Reynolds flocking rules. The control input φ_i for each UAVΥ_i comprises terms for separation, alignment, cohesion, and navigation, allowing for collision avoidance and coordinated trajectory planning. Additionally, a dynamic dissipating obstacle avoidance mechanism is incorporated, enabling UAV to effectively navigate around obstacles.

4.2. Risks and Mitigation Strategies for the Central UAV Monitor

The central UAV monitor plays a key role in collecting and disseminating network-wide information. However, its operation introduces potential risks that must be addressed

Privacy Leakage: The central monitor aggregates UAV data, making it a potential target for eavesdropping or unauthorized access. To address this challenge, homomorphic encryption is utilized for secure computations on encrypted data, while ZKPs are employed to verify UAV data authenticity without revealing sensitive information.

Communication Bottleneck: A single point of data collection may result in congestion, particularly in high-traffic scenarios. To mitigate network strain, a hierarchical UAV clustering model is utilized, where multiple local UAV leaders preprocess and aggregate data before transmitting it to the central monitor.

Failure Resilience: The failure of the central UAV monitor has the potential to disrupt system coordination. To mitigate this risk, a decentralized leader election mechanism based on Byzantine Fault Tolerant (BFT) consensus is implemented, allowing another UAV to dynamically assume monitoring functions in the event of a failure. These measures ensure the central UAV monitor operates securely, efficiently, and without introducing a single point of failure.

4.3. Integration with System Architecture

The decentralized flocking model operates within the UAV Communication Network component of our overall system architecture. It leverages the communication model described in Section 3.1 to facilitate information exchange between UAV, while the blockchain layer ensures secure and transparent coordination. This integration allows for robust and adaptive UAV formations that can respond effectively to dynamic disaster scenarios.

4.4. Specialized UAV Clusters for Disaster Response

Our model employs a heterogeneous UAV network comprising several specialized clusters, each designed to address specific aspects of disaster relief. The Delivery Network (S_λ) focuses on transporting essential relief supplies to affected areas.

The Survey Network (S_η) is assigned to rapid damage assessment and mapping of disaster-stricken regions. The Connectivity Network (S_Ω) is responsible for restoring communication links in areas where infrastructure has been compromised. A central UAV monitor, Υ_m, dynamically adjusts high-level coordination strategies based on evolving disaster-response priorities.

4.5. Reynolds Flocking Rules Adapted for Disaster Scenarios

The classic Reynolds flocking rules are adapted to facilitate the decentralized coordination of UAV in disaster response scenarios. The control input φ_i for each UAV Υ_i consists of four key components: separation (φ_i^s), ensuring that UAV maintain safe distances from one another particularly crucial in cluttered post-disaster environments; alignment (φ_i^a), enabling UAV to match velocity and direction, thereby improving coordinated movement during search and rescue operations; cohesion (φ_i^c), maintaining flock integrity to ensure stable communication links and collective efficiency; and navigation (φ_i^n), directing UAV towards specific disaster-related objectives or away from hazardous areas. The combined control input is expressed as

$$\varphi_i = w_s\varphi_i^s + w_a\varphi_i^a + w_c\varphi_i^c + w_n\varphi_i^n \tag{12}$$

where w_s, w_a, w_c, and w_n are weighting factors that can be dynamically adjusted based on the specific disaster response task and environmental conditions.

4.6. Obstacle Avoidance in Disaster Environments

A dynamic obstacle avoidance mechanism is integrated to enable effective navigation around common post-disaster obstacles, such as debris and damaged structures. This is mathematically represented as

$$\langle \mathbf{v}_\gamma, \bar{\mathbf{v}} \rangle \geq \cos(\vartheta_m)|\bar{\mathbf{v}}|^2 \tag{13}$$

where ϑ_m denotes the maximum allowable misalignment angle between the UAV velocity vector $\mathbf{v}_\gamma$ and desired direction $\bar{\mathbf{v}}$.

4.7. Application to Specific Disaster Response Functions

The Delivery Flock (S_λ) utilizes flocking algorithms to maintain cohesion and alignment while transporting supplies. It employs obstacle avoidance to navigate through potentially hazardous environments and coordinates with the survey flock to identify optimal delivery routes and drop points. The Survey Flock (S_η) applies flocking strategies to systematically cover disaster areas for damage assessment. It uses alignment rules to ensure efficient area coverage and avoid redundant scanning, integrating with the blockchain layer to securely store and share real-time survey data. The Connectivity Flock (S_Ω) aligns with 3GPP `https://www.3gpp.org/` UAV standards to restore communication in affected areas. It uses flocking rules to maintain optimal formation for wireless coverage and dynamically adjusts positions based on evolving connectivity needs and terrain challenges. Due to their high maneuverability, UAVs are well suited for providing coverage in disaster scenarios. However, several limitations including battery dependence, mobility constraints, and hovering impacts can lead to deviations between simulated performance and actual real-world behavior [35]. The central monitoring UAV, Υ_m, coordinates these specialized flocks using a decentralized algorithm based on the adapted Reynolds rules. This allows for flexible and resilient disaster response operations that can adapt to changing conditions and priorities on the ground.

4.8. Dynamic State Propagation and Battery Model

The state of each UAV evolves, according to

$$\rho_i[\kappa+1] = \rho_i[\kappa] + \Delta\tau \cdot \Omega_i[\kappa] \tag{14}$$

$$\Omega_i[\kappa+1] = \Omega_i[\kappa] + \Delta\tau \cdot (\varphi_i^s + \varphi_i^a + \varphi_i^c + \varphi_i^n) \tag{15}$$

Here, $\Delta\tau$ represents the discrete time step. The battery dynamics of the UAV are modelled to account for power. This Fig. 2 presents the Two-Dimensional (2D) spatial distribution of flocking UAVs engaged in post-disaster activities, including Navigation/Surveillance, Communication, Search and Rescue, Environmental Monitoring, Logistics/Delivery, and Infrastructure Repair, across consecutive time steps labelled 1 through 6. Each scatter plot represents a specific time step, with the x and y axes indicating the geographical coordinates within a 2D plane. The scattered dots within each plot represent individual UAVs, with their positions depicting the flocking patterns, deployment areas, and coverage for the corresponding post-disaster activity during that particular time interval.

4.9. Significance of Flocking Algorithms in Multi-Agent Systems

Consider a group of autonomous agents $\mathcal{A} = \{A_1, A_2, \ldots, A_N\}$, where each agent A_i has a state $(x_i, v_i) \in \mathbb{R}^n \times \mathbb{R}^n$ representing its position and velocity vectors, respectively. The control input U_i for each agent A_i comprises three terms

$$U_i = \hat{U}_i^{\text{coh}} + \bar{U}_i^{\text{damp}} + \check{U}_i^{\text{nav}} \tag{16}$$

where $\hat{U}_i^{\text{coh}}$ enables cohesion towards the flock center, $\bar{U}_i^{\text{damp}}$ achieves velocity consensus through damping force, and $\check{U}_i^{\text{nav}}$ drives navigation towards the group objective. Two flocking algorithms are introduced, each based on distinct interaction rules, to enhance the adaptability and coordination of UAV swarms in dynamic environments. These algorithms enable autonomous UAV clusters to maintain efficient formation and perform cooperative tasks while responding to real-time changes in connectivity and operational constraints.

$$U_i = U_i^\alpha \tag{17}$$

where,

$$U_i^\alpha = \underbrace{\sum_{A_j \in \mathcal{N}_i} \phi_b(\|x_j - x_i\|_\sigma)\mathbf{n}_{ij}}_{\text{Cohesion Term}} + \underbrace{\sum_{A_j \in \mathcal{N}_i} a_{ij}(x)(v_j - v_i)}_{\text{Damping Term}} \tag{18}$$

where ϕ_b is used for the Reynolds flocking rule terms, and $\mathcal{N}_i$ are the neighbour sets for agent i.

4.10. Alpha-Neighbors of Alpha-Agents: Proximity Net

Let $\mathcal{V}_\alpha = \{1, 2, \ldots, n_\alpha\}$ and $\mathcal{V}_\beta = \{1, 2, \ldots, n_\beta\}$ denote the sets of alpha and beta agents, respectively. An obstacle $\beta_k \in \mathcal{V}_\beta$ is a neighbour of alpha-agent $i \in \mathcal{V}_\alpha$ if

$$\mathcal{B}(q_i, r_\beta) \cap O_k \neq \emptyset \tag{19}$$

where $\mathcal{B}(q_i, r_\beta)$ is a ball centered at q_i with radius r_β, and O_k is the obstacle region. The alpha and beta neighbour sets are defined as

$$\mathcal{N}_{\alpha i} = \{j \in \mathcal{V}_\alpha : \|q_j - q_i\| < r_\alpha\} \tag{20}$$

$$\mathcal{N}_{\beta i} = \{k \in \mathcal{V}_\beta : \mathcal{B}(q_i, r_\beta) \cap O_k \neq \emptyset\} \tag{21}$$

where q_i and v_i are the position and velocity of the agent i in the obstacle boundary dynamics, respectively. This induces a bipartite proximity graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ between the alpha and beta agents, where $\mathcal{V} = \mathcal{V}_\alpha \cup \mathcal{V}_\beta$ and $\mathcal{E} \subseteq \mathcal{V}_\alpha \times \mathcal{V}_\beta$. Here, r_α and r_β are the radii for proximity in the alpha and beta neighbour sets, respectively.

4.11. Dynamic State Propagation and Battery Model

The state of each UAV evolves, according to

$$\rho_i[\kappa + 1] = \rho_i[\kappa] + \Delta\tau \cdot \Omega_i[\kappa] \tag{22}$$

$$\Omega_i[\kappa + 1] = \Omega_i[\kappa] + \Delta\tau \cdot (\varphi_i^s + \varphi_i^a + \varphi_i^c + \varphi_i^n) \tag{23}$$

Here, $\Delta\tau$ represents the discrete time step. The battery dynamics of the UAVs were modelled to account for power.

4.12. Significance of Flocking Algorithms in Multi-Agent Systems

Consider a group of autonomous agents $\mathcal{A} = \{A_1, A_2, \ldots, A_N\}$, where each agent A_i has a state $(x_i, v_i) \in \mathbb{R}^n \times \mathbb{R}^n$ that represents its position and velocity vectors, respectively. The control input U_i for each agent A_i comprises three terms

$$U_i = \hat{U}_i^{\text{coh}} + \bar{U}_i^{\text{damp}} + \check{U}_i^{\text{nav}} \tag{24}$$

where $\hat{U}_i^{\text{coh}}$ enables cohesion towards the flock center, $\bar{U}_i^{\text{damp}}$ achieves velocity consensus through damping force, and $\check{U}_i^{\text{nav}}$ drives navigation towards the group objective. Two flocking algorithms are introduced, each based on distinct interaction rules, to enhance UAV coordination in dynamic environments. The first algorithm leverages localised communication and decentralised decision-making, enabling UAV to adapt to changing network conditions without relying on a central authority. The second algorithm incorporates hierarchical control mechanisms, optimising formation stability and energy efficiency while maintaining robust swarm coordination. Both approaches are designed to facilitate seamless UAV operations, ensuring reliable communication, efficient task execution, and enhanced resilience in challenging disaster response scenarios.

$$U_i = U_i^\alpha \tag{25}$$

where,

$$U_i^\alpha = \underbrace{\sum_{A_j \in \mathcal{N}_i} \phi_b(\|x_j - x_i\|_\sigma)\mathbf{n}_{ij}}_{\text{Cohesion Term}} + \underbrace{\sum_{A_j \in \mathcal{N}_i} a_{ij}(x)(v_j - v_i)}_{\text{Damping Term}} \tag{26}$$

where ϕ_b is used for the Reynolds flocking rule terms and $\mathcal{N}_i$ are the neighbour sets for agent i.

4.13. Alpha-Neighbors of Alpha-Agents: Proximity Net

Let $\mathcal{V}_\alpha = \{1, 2, \ldots, n_\alpha\}$ and $\mathcal{V}_\beta = \{1, 2, \ldots, n_\beta\}$ denote sets of alpha and beta agents, respectively. An obstacle $\beta_k \in \mathcal{V}_\beta$ is a neighbor of alpha-agent $i \in \mathcal{V}_\alpha$ if

$$\mathcal{B}(q_i, r_\beta) \cap O_k \neq \emptyset \tag{27}$$

where $\mathcal{B}(q_i, r_\beta)$ is a ball centered at q_i with radius r_β and O_k is the obstacle region. The alpha and beta neighbour sets are defined as

$$\mathcal{N}_{\alpha i} = \{j \in \mathcal{V}_\alpha : \|q_j - q_i\| < r_\alpha\} \tag{28}$$

$$\mathcal{N}_{\beta i} = \{k \in \mathcal{V}_\beta : \mathcal{B}(q_i, r_\beta) \cap O_k \neq \emptyset\} \tag{29}$$

where q_i and v_i are the position and velocity of the agent i, respectively, in the obstacle boundary dynamics. This induces a bipartite proximity graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ between the alpha and beta agents, where $\mathcal{V} = \mathcal{V}_\alpha \cup \mathcal{V}_\beta$ and $\mathcal{E} \subseteq \mathcal{V}_\alpha \times \mathcal{V}_\beta$. Here, r_α and r_β are the radii of proximity in the alpha and beta neighbour sets, respectively.

4.14. Considerations for Privacy in Blockchain-Integrated UAV Networks

Ensuring privacy is critical in our blockchain-integrated UAV network to protect sensitive disaster-response data. The primary privacy challenges are addressed through the following strategies:

Data Confidentiality: Utilization of end-to-end encryption (ECC) along with ZKPs secures UAV data transmission, maintaining confidentiality without revealing raw data.

Access Control: Attribute-Based Encryption (ABE) implements access limitations, allowing data decryption solely by authorized participants.

Anonymity and Pseudonymization: To prevent tracking, UAV identities are concealed with the use of dynamic pseudonyms and ring signatures.

Privacy-Preserving Smart Contracts: Deployment of zk-SNARKs facilitates contract execution while safeguarding transaction details from exposure.

Decentralized Identity Management: Self-sovereign identity (SSI) frameworks enable secure and trust-independent UAV authentication.

Secure Consensus Participation: In the DPoS-PBFT consensus approach, homomorphic encryption safeguards UAV voting activities to inhibit vote tracking.

Resistance to Traffic Analysis: Use of mix networks alongside dummy transactions conceals UAV communication flows. These privacy strategies are crucial for ensuring secure and effective UAV coordination in disaster-response operations.

5. Enhanced DPoS-PBFT Consensus Mechanism for UAV Networks

The decentralized flocking model and the enhanced DPoS-PBFT consensus mechanism are integral, interoperating components of our blockchain-enabled UAV network for disaster response. While the flocking model governs the physical coordination and movement of UAV, the consensus mechanism ensures secure and efficient information sharing and decision-making within the network. The flocking algorithm relies on frequent, reliable communication between UAV s to maintain formation and adapt to changing conditions. This communication is facilitated by the blockchain network, with transactions validated through the consensus mechanism. Conversely, the consensus mechanism benefits from the spatial distribution and mobility patterns determined by the flocking model, as these influence network topology and, consequently, the efficiency of the consensus process. For instance, the selection of validator nodes in the Delegated Proof Of Stake (DPoS) component considers the spatial distribution of UAV s to ensure a balanced and responsive network. Furthermore, the PBFT component's performance is optimized by leveraging the natural clustering that emerges from the flocking behavior. This synergy between the flocking model and the consensus mechanism enables our system to maintain robust, decentralized coordination even in the

challenging, dynamic environments typical of disaster scenarios.

UAVs play a crucial role in disaster management by enabling rapid response and recovery. An enhanced consensus mechanism is introduced, integrating the DPoS-PBFT to optimise security, efficiency, and fault tolerance. This design leverages DPoS for efficient block validation and PBFT for heightened security, and optimizes UAV network performance in adverse disaster conditions. Fig. 3 demonstrates the detailed sequence of steps in the proposed hybrid DPoS-PBFT consensus protocol for efficient and secure block validation among the UAVs.

5.1. Mechanism Overview

The mechanism is initiated by the stake-based selection of the block proposer. The UAV generates a block and circulates it among the selected validators through the DPoS framework. Validators $\mathcal{V}$ that are assigned based on their UAV-specific metrics authenticate the block. Approval by a two-thirds majority confirms the block, whereas PBFT intervenes in cases of disagreement or malicious activity to ensure consensus and network integrity.

Notation: Let $\mathcal{V}$ represent a subset of UAVs serving as validators. Validator selection considers factors such as the stakes, fuel, sensing capabilities, and historical performance. Each UAVi is assigned a validator score V_i calculated as

$$V_i = w_1 S_i + w_2 F_i + w_3 C_i + w_4 H_i \tag{30}$$

where S_i denotes the stake, F_i denotes the remaining fuel, C_i denotes the sensing capability, and H_i denotes historical utility. The weights w_1, w_2, w_3, w_4 quantify the importance of these parameters. The top n UAVs form validator set $\mathcal{V}$. The block proposer probability p_i for UAVi is given by

$$p_i = \frac{S_i}{\sum_{j \in \mathcal{V}} S_j} \tag{31}$$

Process Flow: A `PRE-PREPARE` message, containing the new block, is broadcast by a validator to the other validators. The validators validate the block and broadcast a `PREPARE` message if it is valid. A `COMMIT` state is reached, and the corresponding message is broadcast when more than $\frac{2}{3}$ `PREPARE` messages are received. A block was added to the blockchain upon receiving a matching set of $\frac{2}{3}$ `COMMIT` messages. If consensus is not reached, a new view is initiated, potentially altering the block proposer. Following the explanation of the consensus protocol, the simulation setup used to assess the performance of the proposed approach is presented. Table 3 compares the different consensus protocol options and their attributes relevant to the UAV networks. Our consensus protocol combines DPoS-PBFT to address the unique challenges in UAV networks during disaster response. This novel approach enhances communication efficiency while maintaining robust security, advancing UAV applications in emergency management. As outlined in Algorithm 1, the DPoS phase involves selecting validators based on UAV stakes. An elected proposer creates a block, which is verified by the validators. In the PBFT phase, validators vote on the block. If insufficient votes are received, a view change occurs. Consensus through a supermajority adds the block to the blockchain, ensuring secure and efficient network operations. Specifically, the Algorithm 2 combines DPoS and PBFT to achieve efficient decentralized consensus in UAV networks for disaster response scenarios. The DPoS phase selects validators and a leader node based on delegated stakes to propose a block. If faults exceed a threshold, PBFT is triggered for additional consensus through preparatory and commit phases before finalizing consensus on adding the approved block. The hybrid mechanism balances efficiency, security, and fault tolerance for reliable coordination between resource-constrained UAVs with intermittent aerial connections. The key parameters and their corresponding values for the proposed hybrid DPoS-PBFT blockchain mechanism are detailed in Table. 4. These parameters are carefully selected to optimize security, efficiency, and resilience in UAVnetworks, ensuring robust consensus and minimal latency in disaster response scenarios.

Table 3: Comparison of consensus protocols

Metric	PBFT	DPoS	Hybrid
Speed	Low	High	Moderate
Throughput	Low	High	Moderate
Fault tolerance	High	Low	Moderate
Permissioning	Private	Public	Configurable

Algorithm 1 Blockchain-based UAV Coordination

```
Initialize: UAV u ∈ U has blockchain.
for all u ∈ U do
    u has blockchain height B.
end for
Propose Block: Rotating schedule.
Select UAV P ∈ V.
P gathers transactions, creates & broadcasts block B + 1.
Verify Block:
for all v ∈ V do
    if v verifies B + 1 valid then
        v signs & broadcasts approval.
    end if
end for
if approvals > (2/3)N then
    Add block B + 1 to blockchain.
end if
```

5.2. Geospatial Smart Contract Integration

The proposed architecture runs on a permissioned quorum chain, supporting privacy-preserving transactions between approved disaster response agencies using ZKPs. Each agency operates a local quorum node maintaining a ledger copy. Inter-agency consensus utilizes the hybrid DPoS-PBFT protocol. Within agencies, lightweight UAV blockchain nodes connect to the quorum node to submit transactions and access chain data when required. On-chain access control is enforced via smart contracts, with agencies managing permissions for their UAV fleets. Resilience is enhanced through the geographic distribution of nodes in regional clusters. Integrating location-based coordination requires supporting geospatial data like GPS coordinates alongside transactions. To address the inefficiency of JSON [36] formats in storing spatial data,A compressed binary encoding of GeoJSON is implemented, achieving a reduction in storage requirements of up to 60%. This enables efficient representation of Three-Dimensional (3D) positions, boundaries, and disaster zones of UAVs as programmable contract objects. The geospatial capabilities are further enhanced through the implementation of a quadtree spatial index structure within smart contracts, optimizing spatial queries and reducing complexity from $O(n)$ to $O(\log n)$ for most operations. A ray-casting

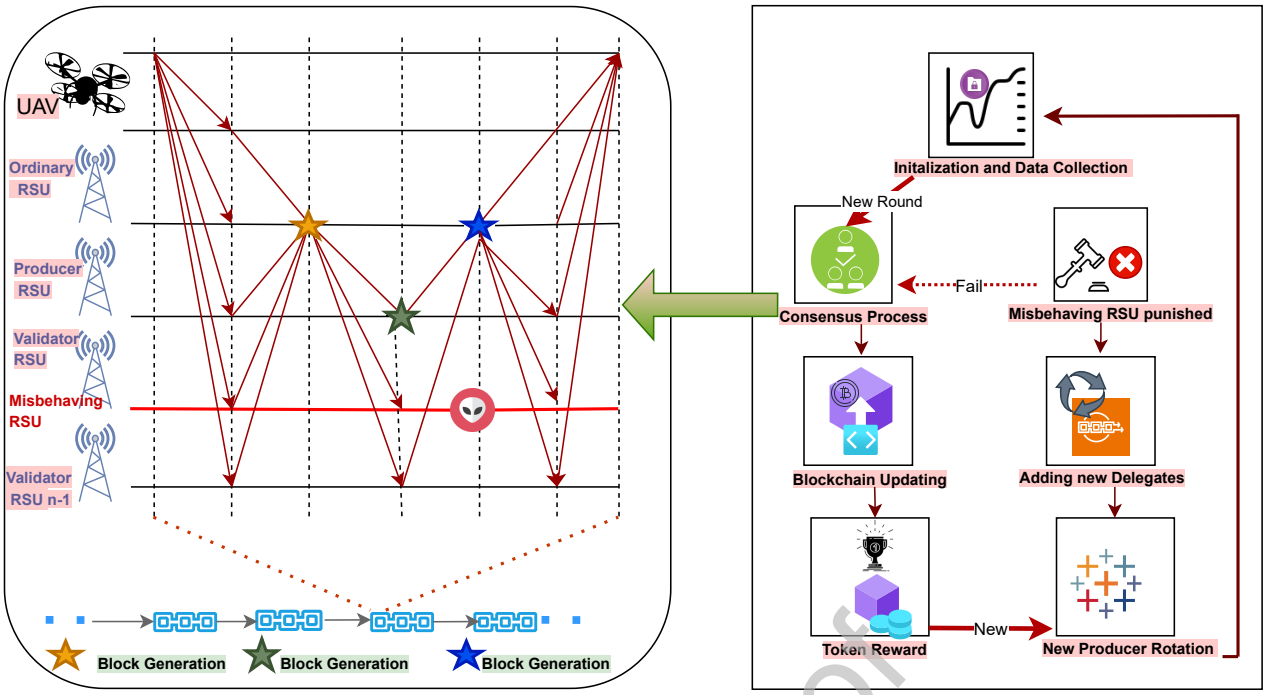


Fig. 3. Detailed Working Mechanism of the DPoS-PBFT Consensus Protocol.

method is employed for efficient point-in-polygon tests in geo-fencing applications, while a modified A* algorithm with a custom heuristic function facilitates 3D UAV path planning. The hybrid consensus protocol is extended to include spatial validation rules, ensuring the integrity of location-based data. Additionally, efficient on-chain spatial operators for intersection, distance calculation, and nearest neighbour queries are provided, maintaining a maximum complexity of $O(\log n)$ for large point sets.

These technical implementations collectively enable sophisticated geospatial operations within the blockchain framework, significantly enhancing the capabilities of UAV based disaster response coordination. The integration of geospatial smart contracts allows for precise and secure management of UAV operations in dynamic disaster scenarios, improving the overall effectiveness of the response efforts. These enhancements enable efficient spatial queries for proximity alerts, geo-fencing, and coordinated navigation. To trigger location-aware executions, oracles provide disaster scenario and situational data feeds. The resulting system balances on-chain security with off-chain computational efficiency, ensuring all critical decision-making logic is executed on the blockchain while maintaining responsive and precise location-based coordination of UAV fleets in disaster scenarios. These enhancements enable efficient spatial queries for proximity alerts, geo-fencing, and coordinated navigation. To trigger location-aware executions, oracles provide disaster scenario and situational data feeds. The resulting system balances on-chain security with off-chain computational efficiency, ensuring all critical decision-making logic is executed on the blockchain while maintaining responsive and precise location-based coordination of UAV fleets in disaster scenarios. The FOAM protocol [37] enables vector data storage. The 3D positions, boundaries, and disaster zones of UAVs can be encoded in GeoJSON, representing them as programmable contract objects. This allows spatial queries for proximity alerts, geo-fencing, and coordinated navigation. To trigger location-aware executions, oracles provide disaster scenario and situational data feeds. Algorithm 3 presents a sample Solidity code for a smart contract that coordinates UAVs for search and rescue operations in a disaster response scenario. It defines key parameters, such as the center of the disaster zone and search radius. Functions are included to assign search grid areas to UAVs, report the findings of trapped people or hazards, and update the UAV status. The comments explain each function's purpose. This implements location-aware coordination logic to automate UAV search and rescue tasks via smart contracts executed based on location data and events.

Algorithm 2 DPoS-PBFT Consensus

Require: Set $\mathcal{U}$ of N UAV nodes
Ensure: Consensus on block B
Initialize DPoS
  Delegate stakes and select leader l
  l validates and proposes block B
DPoS Execution
if $\geq \frac{2N}{3}$ validators approve B **then**
  Add B to blockchain
else if faults $> \vartheta$ **then**
  Trigger PBFT consensus
end if
Initialize PBFT
  l broadcasts B; nodes validate and broadcast prepares
PBFT Execution
if $\geq \frac{2N}{3}$ prepares **then**
  Nodes broadcast commit
end if
if $\geq \frac{2N}{3}$ commits **then**
  Nodes add B
end if
Finalize Consensus
  Update permissions, remove faulty nodes
  Add B if approved

Table 4: Key Parameters and Values of the Hybrid DPoS–PBFT Blockchain Mechanism

Parameter	Example Value/Type
Network Latency	100–500 ms.
DPoS Parameters	Number of delegates: 20; block time: 5 seconds; voting margin: 66%.
Node Distribution	DPoS nodes: global; PBFT nodes: regional.
Finality	DPoS: probabilistic; PBFT: instant.
Energy Use	Prioritise DPoS; invoke PBFT for finality as required.
Throughput	Target: 100 transactions per second (TPS); fallback: 10 TPS.
Security Thresholds	DPoS: $\geq$ 15 delegates; PBFT: $\geq$ 5 nodes.
PBFT Parameters	Normal mode quorum: 4; degraded mode quorum: 3.

Algorithm 3 SearchAndRescue Contract

```
struct UAV
    id
    location
    battery
    status
Address owner
Location disasterZoneCenter
Radius searchRadius
UAV Location[] availableUAVs
function AssignSearchGrid(UAV drone) ▷ Divide disaster zone into grids ▷ Assign grid to UAV for search & rescue
end function
function ReportFindings(Location location, FindingType type) ▷ Log findings (people, hazards) ▷ Notify authorities or UAVs
end function
function UpdateUAVStatus(UAV drone, Status status) ▷ Update UAV status (battery, ops)
end function
```

5.3. Trade-offs and Limitations

While our hybrid DPoS-PBFT approach offers significant advantages, it's important to consider potential trade-offs and limitations. The integration of two consensus mechanisms increases system complexity, potentially leading to higher implementation and maintenance costs. PBFT can be resource-intensive, especially in terms of communication overhead, which may strain the limited resources of UAVs, particularly in prolonged disaster response scenarios. As the number of validators increases, the communication overhead of PBFT grows quadratically, which could limit the scalability of the network. The DPoS component may lead to a concentration of power among high-stake validators, potentially compromising decentralization. In disaster scenarios with frequent network partitions, the PBFT component may struggle to reach consensus, potentially causing temporary system halts. The increased computational and communication requirements may lead to higher energy consumption, reducing UAV flight times and operational efficiency. Additionally, the additional PBFT round may increase the time to achieve block finality, which could be critical in time-sensitive disaster response situations.

5.4. Mitigation Strategies

To overcome these limitations, several mitigation strategies are introduced. An adaptive consensus mechanism is implemented to dynamically adjust the consensus process based on network conditions, minimising complexity and optimising resource utilisation when feasible. Introducing a sharding mechanism could improve scalability by allowing subsets of validators to reach consensus on different parts of the network. To promote a more decentralized validator set, rules should be implemented to prevent excessive stake concentration. Developing a lightweight fallback consensus mechanism for scenarios with severe network partitions could help maintain network functionality in challenging conditions. Incorporating energy levels into the validator selection process could help balance consensus participation and operational longevity. Finally, implementing efficient communication protocols could reduce overhead and improve latency in the PBFT phase. Applying these strategies enhances the robustness and effectiveness of our hybrid DPoS-PBFT consensus mechanism for UAV networks in disaster response scenarios.

6. Simulations and Discussions

6.1. Clarification on Simulation Parameter Selection

The selection of simulation parameters is based on standardized UAV network configurations, real-world disaster response constraints, and validated references from existing literature. *Network Topology and UAV Deployment:* The number of UAV and network dimensions were chosen based on disaster-response scenarios, considering area coverage, energy limitations, and connectivity demands. The UAV mobility model follows the 3GPP TR 36.777 standard, ensuring realistic aerial trajectories. *Channel and Propagation Model:* Path loss and SNR models for A2A and A2G communication were selected based on both free-space and urban environments, incorporating empirical data from existing studies. Transmission power, antenna gains, and noise levels were chosen to match commercially available UAV communication systems. *Performance Metrics Justification:* Throughput, latency, and resilience were prioritized as essential performance indicators. Latency was evaluated based on real-time situational awareness needs, while resilience was tested under simulated network disruptions, including UAV failures and link degradation. *Computational and Blockchain Parameters:* The blockchain consensus mechanism was evaluated across different transaction loads to measure its impact on UAV resource consumption and transaction finalization time. These parameters were calibrated based on benchmarks from lightweight blockchain implementations designed for UAV networks.

The UAV simulation parameters used to evaluate the proposed framework are summarized in Table. 5. These parameters define the operational conditions, network configurations, and environmental factors considered in the simulations, ensuring a realistic assessment of UAV performance in disaster response scenarios.

6.2. Simulation Settings

Our disaster response simulation is set within a 25 km × 25 km urban area severely impacted by a natural disaster. This environment includes a primary Base Station (BS), a compromised BS in a power outage zone, an adversarial-controlled region, a disaster relief coordination hub, refugee camps, and critical medical facilities requiring prioritized aid. The simulation involves a heterogeneous swarm of 200 UAV, each powered by lithium-ion batteries and operating autonomously. UAV have unique identifiers and energy profiles and are equipped with navigation, networking sensors, and processors supporting both A2A and A2G communication. They form a multi-tier mesh network at an altitude of 500 m, adhering to aviation safety protocols, including collision avoidance mechanisms. Key performance metrics evaluated include network throughput, latency, resilience against cyberattacks and malicious nodes, mobility, and coordination of UAV flocks, packet delivery rate, and overall network reliability.

Table 5: UAV Simulation Parameters

Parameter	Value
Total Number of UAVs	200.
Flock 1 (Delivery Services)	90 UAVs.
Flock 2 (Connectivity Support)	25 UAVs.
Flock 3 (Monitoring)	85 UAVs.
Disaster Region Size	25 km × 25 km.
Total UAV Network Coverage Radius	5.5 km.
UAV Flight Altitude	30 m.
UAV Transmit Power	2 mW.
Network Latency	30–100 ms.
Supported Data Rate	15 Mbps.

6.3. Blockchain-Enabled UAV Coordination

The blockchain-enabled UAV coordination framework within this simulation achieved a throughput of 100 Transactions Per Second (TPS) with an average latency of 26 ms, and a packet delivery rate of 99.7%. The framework employs a hybrid DPoS-PBFT consensus mechanism, balancing resilience and computational efficiency. DPoS is utilized for standard transactions, with 20 elected delegates managing consensus. PBFT is activated for transactions requiring immediate finality, supported by five regional servers. This hybrid configuration ensures efficient transaction validation while minimizing UAV energy consumption.

6.4. 3GPP-Standardized Realism in Simulation

To ensure realism and industry alignment, our simulation adheres to 3GPP standards

- 3GPP TR 36.777 for UAV mobility modeling `https://www.3gpp.org/ftp/Specs/archive/36_series/36.777/`.
- 3GPP TR 36.842 for BS deployment, `https://www.3gpp.org/ftp/Specs/archive/36_series/36.842/` 3GPP TR 36.842 BS Deployment.
- 3GPP-compliant communication models for A2G and A2A links.

The A2G model accounts for probabilistic propagation and environmental attenuation, while the A2A model considers free-space path loss.

6.5. Resilience Against Cyberattacks

Resilience to cyberattacks was validated through simulations of various security threats *Distributed Denial of Service:* Evaluated under high-traffic malicious flooding conditions. *Spoofing Attacks:* Simulated adversarial nodes attempting to impersonate UAV. *Message Tampering:* Assessed the blockchain's immutability in preventing unauthorized data alterations. The system maintained stability, ensuring continued mission execution despite these adversarial conditions.

6.6. Real-World Applicability and Testing

This comprehensive simulation validates the practical applicability of the proposed system for disaster response, particularly when ground infrastructure is compromised. The effectiveness of the architecture was further tested in a controlled UAV testbed, verifying real-world feasibility.

6.7. Simulations Results

The simulation results demonstrated the effectiveness of the system in terms of security, efficiency, scalability, and resilience. Security measures include AES-256 encryption, ECDSA signatures, SHA-256 hashes, and hybrid blockchain consensus, which provide a robust defence against Byzantine failures. The system's performance targets a throughput of 100 TPS with less than two seconds of latency and 99% reliability for UAV packet delivery. Scalability tests involved increasing the UAV network size and load, demonstrating the capability of the system to handle high traffic volumes seamlessly. As seen in Fig. 4 summarize the network throughput and latency metrics as the number of UAV nodes scales up to 500 on the private blockchain network. Throughput is measured in TPS processed across the flocking network, with a millisecond latency for transaction finality. The latency increased marginally from 50ms at 10 nodes to 68ms at 500 nodes. The blockchain-enabled network sustains transaction-processing speeds exceeding 100 TPS with reasonable finality times below 70ms, even at scale. The key insight is that leveraging blockchain and decentralization principles can enable scalable flock coordination among hundreds of UAVs, which is necessary for wide-area post-disaster surveying. Linear throughput scaling to 500 nodes shows that UAVs can independently coordinate paths and targets through fast and trustless transactions. Stable sub-100ms latency despite scaling offers viability for real-time decision-making. Fig. 5 visualises the network throughput and latency as the number of UAV nodes increases from 10 to 100. The throughput scales linearly up to 100 TPS with 60 nodes, and then saturates. The latency remained below 50 ms, despite higher loads. Max transaction volumes occur at saturation with 100 nodes, without increased latency. This demonstrates the linear throughput scalability to a saturation point without latency impacts as the UAV network expands. Testing beyond 100 nodes revealed the upper scalability limits. Peak transactions during saturation did not affect the latency. The results validate the system's ability to deliver real-time coordination for sizable UAV fleets via a decentralized blockchain backbone with excellent throughput scalability to a saturation threshold without latency degradation. As shown in Fig. 6, the system main-

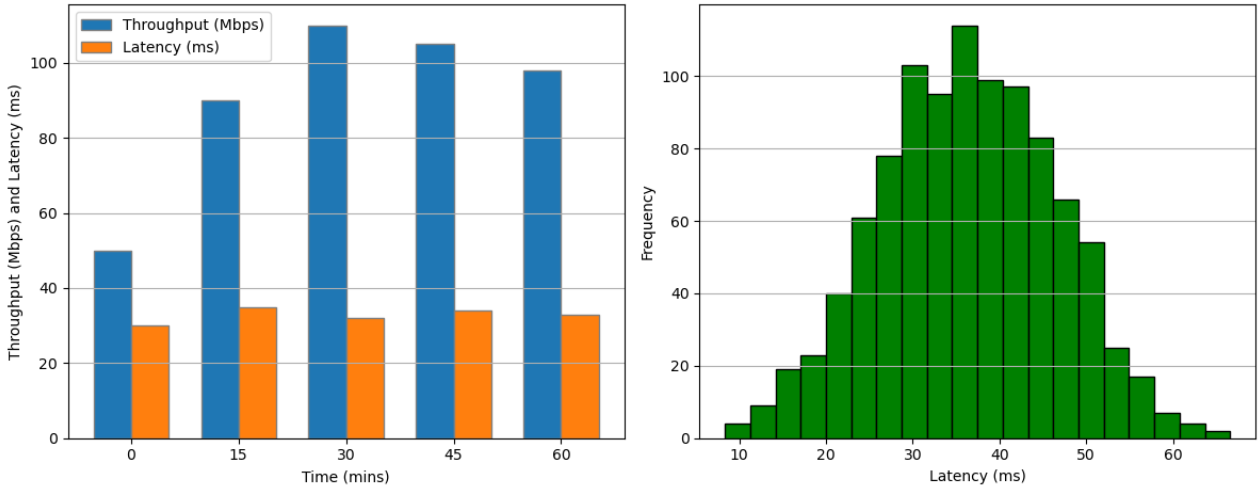


Fig. 4. Scalability and Performance Analysis of Blockchain-Enabled UAV Communication.

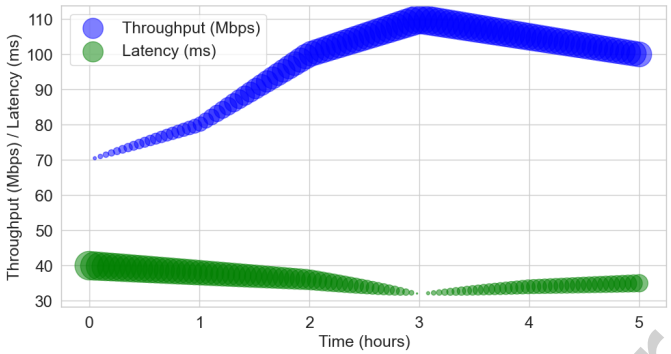


Fig. 5. Throughput and Latency Over Time.

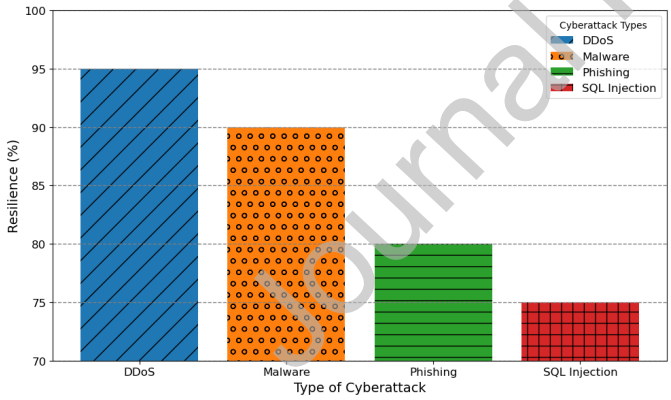


Fig. 6. Cyberattack Resilience of UAV Blockchain Network: Defense Against Malicious Threats.

tains high throughput and low latency despite spoofing, DDoS, and tampering attacks. This validates the strong resilience capabilities. The system architecture demonstrated good overall cyber resilience across the four attack types: DDoS, malware, phishing, and SQL injection. Resilience exceeded 70%, even for the most successful attack (SQL injection of 75 %). DDoS attacks were most effectively mitigated at 95%. The system also showed strong resilience to malware 90% and phishing (80 %). The results indicate acceptable cyber resilience for safe UAV fleet operations across attack types, especially against network-level attacks such as DDoS. Risks remain from application-layer attacks, such as SQL injection, requiring further database server hardening. Insufficient end-user device protection is likely to explain the higher phishing and malware effectiveness. Fig. 7 highlights the distribution of communi-

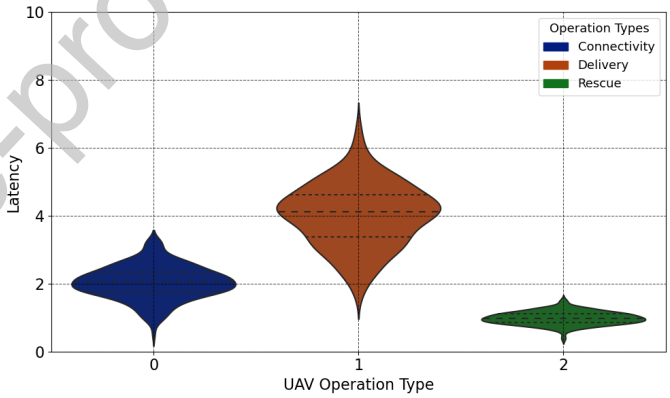


Fig. 7. Mission-Specific Latency Profiling for UAV Operation.

cation latency across UAV operational scenarios using violin plots. The latency remained under 10 ms in all cases, with median values of approximately 2–3 ms. However, distinct distribution shapes were observed. The surveillance exhibited a normal-like profile centered at 3 ms. The assessment followed a right-skewed shape, peaking at approximately 1 ms. The delivery showed multimodal performance. The tracking displayed a left-skewed distribution with the highest density below 2 ms. The differential latency characteristics demonstrate the adaptability to meet specialized requirements. For instance, a sub-2 ms latency enables rapid location updates for tracking. Minimal latency facilitates quick assessment. Network intelligence allows self-optimization of the demands of each context. In summary, the tuned latency distributions maintained medians under 5 ms for diverse UAV applications. Optimized profile shapes provide differentiated capabilities, allowing the network to conform to the specific demands of post-disaster use cases through intelligent resource allocation. Fig. 8 compares within-cluster and across-cluster coordination communication latency. Within the 50-drone clusters, latency ranges from 1 to 50 ms (median 25 ms), enabling rapid in-group synchronization. In Fig. 9, across-cluster latency is higher at 50–100 ms between distant leaders, allowing necessary deconfliction. The bifur-

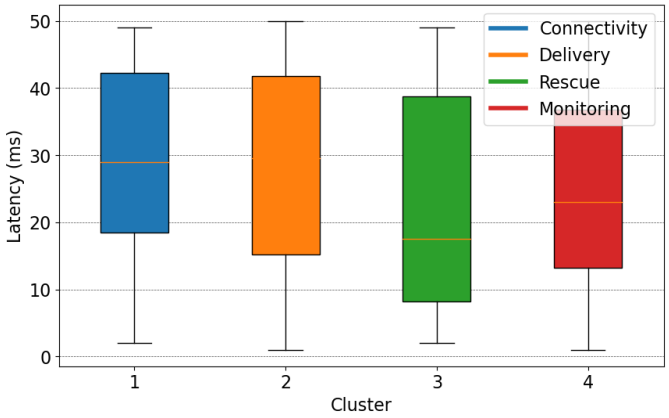


Fig. 8. Latency Variations Within UAV Clusters for Decentralized Coordination.

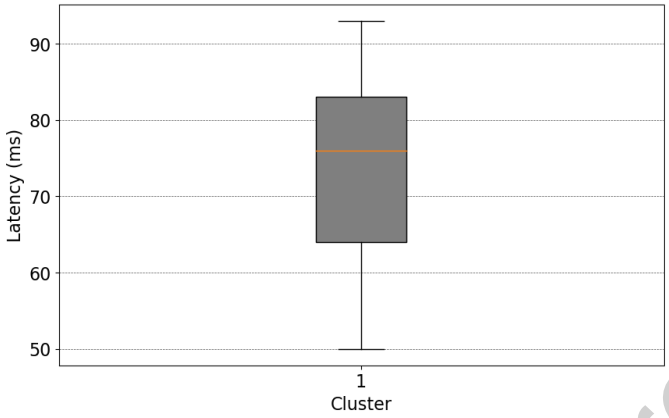


Fig. 9. Accross-Cluster Latency.

cated profile validates efficient localized coordination within clusters while sustaining fleet visibility via across-cluster transactions. This hierarchy supports tight drone flocking and high-level swarm oversight. In summary, the latency dichotomy exhibited provides rapid decentralized responses within clusters along with sufficient global communication quality across the architecture by partitioning the blockchain ledger. The key insight is how the communication locality enabled by blockchain transactions results in bifurcated latency that delivers both localized control and fleet coordination, which is crucial for decentralized multi-UAV flocking at scale.

7. Conclusion

This paper has introduced a comprehensive blockchain-enabled framework for secure, resilient, and autonomous UAV-based disaster response. Through the combined use of distributed ledger technology, bio-inspired flocking, and an energy-aware DPoS-PBFT consensus protocol, the system resolves long-standing issues in trust management, decentralised control, and coordinated decision-making across multi-UAV networks. The consortium blockchain removes single points of failure while enabling auditable and tamper-resistant information exchange across agencies. In parallel, bio-inspired swarm dynamics enhance robustness under intermittent connectivity and adversarial manipulation. Extensive simulations demonstrate measurable improvements in throughput, latency, energy efficiency, and cyber-resilience, underscoring the suitability of the architecture for mission-critical emergency operations.

7.1. Potential for Real-World Implementation and Collaboration

Deployment of this architecture in operational disaster-response settings will require multidisciplinary collaboration. Partnerships with emergency management agencies will support integration with existing command-and-control processes and enable structured field evaluations. Engagement with UAV manufacturers will facilitate hardware-level optimisation, ensuring compatibility with heterogeneous platforms and addressing constraints related to power, compute capability, and communication standards. Joint field trials will generate empirical datasets essential for refining performance thresholds, validating regulatory compliance, and accelerating the practical adoption of blockchain-enabled UAV coordination for high-stakes missions.

7.2. Future Directions

Future research will extend this framework across several technically demanding directions. A fundamental next step involves developing real-world prototypes and field trials to assess system performance under practical environmental variability, including weather-induced channel impairments, electromagnetic interference, and complex obstacle-dense terrains. Adaptive channel modelling, learning-driven interference prediction, and dynamic spectrum allocation will be explored to maintain robust UAV communication in such conditions.

Regulatory compliance will become increasingly critical as autonomous flight and data governance frameworks evolve. To address this, decentralised identity management, verifiable access control, and blockchain-anchored audit logs will be enhanced to satisfy emerging aviation, safety, and privacy regulations. Hardware and energy constraints remain an important challenge; future work will therefore focus on lightweight edge-computing pipelines, computation–communication co-optimisation, and energy-aware consensus strategies to ensure sustained UAV operation during prolonged missions.

Algorithmically, integrating advanced artificial intelligence such as deep reinforcement learning, graph neural networks, federated multi-agent optimisation, and risk-aware trajectory planning will further improve decision-making in dynamic and uncertain environments. Enhancements to geospatial smart contracts will enable dynamic, context-aware task allocation and fine-grained multi-agency coordination, supporting heterogeneous UAV fleets operating autonomously in complex disaster zones.

Privacy-preserving analytics will be reinforced using homomorphic encryption, secure multi-party computation, and zero-knowledge proofs to allow sensitive situational data to be used securely across stakeholders. Cross-chain interoperability mechanisms will be investigated to enable seamless integration with external blockchain and data systems relevant to logistics, healthcare, and emergency coordination. Complementary advances in energy-aware routing and consensus design will prolong UAV operational lifetimes and enhance mission continuity.

Finally, future work will include the development of intuitive human–UAV interaction interfaces to support supervisory control and situational awareness during time-critical operations. These interfaces will provide semantically rich summaries, risk

projections, and interpretability for AI-based decisions, improving operator confidence and effectiveness. Collectively, these efforts will increase the robustness, scalability, and real-world applicability of blockchain-enabled UAV networks for modern disaster response.

7.2.1. Long-Term Vision for 2030–2050

Beyond near-term enhancements, the framework holds potential to evolve into a quantum-resilient, semantically informed, and AI-native coordination fabric for next-generation disaster response (2030–2050). At the cryptographic layer, transitioning from classical public-key cryptography to post-quantum primitives particularly lattice-based key encapsulation and digital signatures will safeguard inter-agency authentication and blockchain integrity against quantum-capable adversaries.

A key architectural extension is the development of a continuously synchronised digital twin encompassing the disaster environment, the UAV swarm, and the blockchain state. Deployed across edge–cloud federations, this digital twin would simulate UAV trajectories, consensus dynamics, geospatial smart contract execution, and risk propagation in real time. Quantum-inspired and hybrid quantum–classical optimisation algorithms could explore immense coordination spaces, enabling predictive analysis, stress testing, and "safe-to-fail" policy validation before live deployment in multi-hazard scenarios.

At the communication layer, the shift to semantic and intent-driven communication protocols will reduce raw data transmission and instead exchange task-level meaning representations. These semantic artefacts, anchored on-chain, will support low-overhead, intent-aware coordination of heterogeneous UAV fleets operating across multiple jurisdictions. Coupled with geospatial smart contracts, semantics will enable greater precision and autonomy in mission planning and execution.

Generative and foundation-model-based artificial intelligence will further transform the framework. Multi-modal generative models trained on historical disaster datasets, simulation trajectories, and digital-twin feedback will propose optimal swarm formations, validator rotations, and energy-aware routing strategies under varying mission states. Human operators will interact with an AI-assisted "coordination co-pilot" capable of generating candidate policies, forecasting operational trade-offs, and executing validated strategies through on-chain governance mechanisms.

Overall, these long-term research directions position the system as a foundational infrastructure for quantum-secure, AI-driven, and semantically intelligent UAV coordination, supporting the increasing complexity and scale of global disaster-response missions from 2030 to 2050 and beyond.

8. Conflict of Interest Declaration

To: The Editorial Office
Digital Communications and Networks (DCN)
Subject: Conflict of Interest Declaration for Manuscript Submission
Dear Editorial Team,

I, Dr Sana Hafeez, and Dr Yao Sun the corresponding author of the manuscript titled "Blockchain-Enhanced UAV Networks for Post-Disaster Communication: A Decentralized Flocking Approach", hereby declare that there are no conflicts of interest that could have influenced the work presented in the manuscript. Specifically:

- I do not have any financial interests, relationships, or agreements that may have impacted the content, analysis, or interpretation of this manuscript.
- I do not have any personal relationships with individuals, organizations, or entities that could be perceived as influencing the research or the review process.
- I do not hold any professional affiliations or roles that may compromise my impartiality in submitting this manuscript for consideration.

I affirm that this manuscript is a result of independent research and that any potential conflicts of interest, financial or otherwise, have been disclosed in accordance with the guidelines set by Digital Communications and Networks (DCN).
Should any conflicts arise during the course of the manuscript review process, I will immediately notify the editorial office.
Thank you for your consideration.
Sincerely,
Dr Sana Hafeez
University of Glasgow

9. Acknowledgments

We are grateful for the EPSRC UK funding for the future telecom hub – CHEDDAR EP/X040518/1 and CHEDDAR Uplift EP/Y037421/1.

Authors Biography

Sana Hafeez (SMIEEE, MIET, MACM, WiCyS) is a Royal Academy of Engineering Global Talent Fellow and an emerging researcher in intelligent wireless systems, secure autonomous networks, and next-generation digital technologies. She is currently a Research Associate in Digital Technologies at Liverpool John Moores University and a Research Consultant on the national Cybersecurity Pioneer Grant – Quantum-Resistant Cryptography for Drones, funded through Saudi Arabia's RDI Programme.

She holds a Ph.D. in Electronic and Electrical Engineering from the University of Glasgow and an M.S. in Computer Science from COMSATS University Islamabad. She has previously worked at the University of Glasgow and Queen Mary University of London, contributing to UKRI and EPSRC projects and the CHEDDAR Hub, SecureSense, and 6G-FINESSE programmes in secure communications and autonomous systems. Her research covers 6G security, JCAS/ISAC, non-terrestrial networks, UAV and SATCOM systems, quantum-resilient cryptography, privacy-preserving AI, and formal verification. Internationally, she collaborates with academic and industry partners across the UK, Canada, Saudi Arabia, and China to advance resilient and sustainable next-generation communication architectures.

Runze Cheng is a Research Associate in Autonomous Systems and Connectivity at the James Watt School of Engineering, University of Glasgow, U.K. He received his M.Sc. from the University of Nottingham in 2020 and his Ph.D. from the

University of Glasgow in 2023. His research interests include wireless resource management, semantic communication, distributed machine learning, blockchain systems, and space–air–ground integrated networks.

Lina Mohjazi is a Senior Lecturer in Autonomous Systems and Connectivity at the James Watt School of Engineering, University of Glasgow, United Kingdom. She received her B.Sc. degree from the United Arab Emirates University, her M.Sc. degree (with Distinction) from Khalifa University, and her Ph.D. degree from the 5G/6G Innovation center, University of Surrey. Her research interests include sustainable wireless communication systems, the Internet of Things, machine learning for network intelligence, and beyond-5G/6G technologies. She is a Senior Member of the IEEE, a Fellow of the Women's Engineering Society, and an Associate Editor of IEEE Communications Letters. She has received multiple recognitions, including the IEEE Women in Engineering U.K. and Ireland Excellence in Engineering Award and selection among the "100 Brilliant and Inspiring Women in 6G."

Yao Sun is a Senior Lecturer in Autonomous Systems and Connectivity at the University of Glasgow, U.K. He holds a Ph.D. in Electronic and Electrical Engineering from the same institution. His research interests include wireless communications, IoT, blockchain-enabled networking, and distributed intelligence. He has received several best paper awards including the IEEE ComSoc TAOS Award (ICC 2019) and the IEEE IoT Journal Best Paper Award (2022). He is a Senior Member of IEEE and serves on multiple TPCs and editorial boards.

Muhammad Ali Imran is Professor of Communication Systems and Dean of Transnational Engineering Education at the University of Glasgow, United Kingdom. He received his M.Sc. degree (with Distinction) and his Ph.D. degree in communication systems from Imperial College London. He has led numerous multimillion-dollar international research programs in wireless communication, sensing, and 5G/6G innovation. He has authored or co-authored more than 1,000 peer-reviewed papers and has supervised over 60 Ph.D. graduates. He has served in leadership roles for several flagship IEEE conferences and is Editor-in-Chief for the IoT and Sensors area of Frontiers in Communications and Networks. His awards include the IEEE Communications Society Fred Ellersick Prize and the Research Culture Award. He is a Fellow of the Royal Society of Edinburgh, the IEEE, and the IET.

References

[1] S. Hafeez, R. Cheng, L. Mohjazi, M. A. Imran, Y. Sun, A blockchain-enabled framework of UAV coordination for post-disaster networks, in: 2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring), 2024, pp. 1–5. doi:10.1109/VTC2024-Spring62846.2024.10683259.

[2] S. Hafeez, Blockchain-based secure unmanned aerial vehicles (uav) in network design and optimization, Ph.D. thesis, University of Glasgow (2024).

[3] A. Derhab, O. Cheikhrouhou, A. Allouch, A. Koubaa, B. Qureshi, M. A. Ferrag, L. Maglaras, F. A. Khan, Internet of drones security: taxonomies, open issues, and future directions, Vehicular Communications 39 (2023) 100552.

[4] E. A. Keller, D. E. DeVecchio, Natural hazards: earth's processes as hazards, disasters, and catastrophes, Routledge, 2019.

[5] S. Hafeez, L. Mohjazi, M. A. Imran, Y. Sun, Blockchain-enabled clustered and scalable federated learning (BCS-FL) framework in UAV networks, in: 2023 IEEE 28th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2023, pp. 68–73. doi:10.1109/CAMAD59638.2023.10478423.

[6] Y. Wang, Z. Su, Q. Xu, R. Li, T. H. Luan, P. Wang, A secure and intelligent data sharing scheme for UAV-assisted disaster rescue, IEEE/ACM Transactions on Networking.

[7] X. Zheng, G. Sun, J. Li, J. Wang, Q. Wu, D. Niyato, A. Jamalipour, UAV swarm-enabled collaborative post-disaster communications in low altitude economy via a two-stage optimization approach, arXiv preprint arXiv:2501.05742.

[8] J. Cui, Y. Zhu, H. Zhong, Q. Zhang, C. Gu, D. He, Efficient blockchain-based mutual authentication and session key agreement for cross-domain IIoT, IEEE Internet of Things Journal.

[9] A. Ahad, Z. Jiangbina, M. Tahir, I. Shayea, M. A. Sheikh, F. Rasheed, 6G and intelligent healthcare: taxonomy, technologies, open issues and future research directions, Internet of Things (2024) 101068.

[10] T. Li, T. Meng, G. Meng, C. Wang, B. Wang, M. Zhou, X. Han, Formation optimization of airborne radar coordinated detection system using an improved artificial fish swarm algorithm, Scientific Reports 14 (1) (2024) 248.

[11] J. Yang, X. Liu, X. Jiang, Y. Zhang, S. Chen, H. He, Toward trusted unmanned aerial vehicle swarm networks: a blockchain-based approach, IEEE Vehicular Technology Magazine 18 (2) (2023) 98–108. doi:10.1109/MVT.2023.3242834.

[12] A. Aldaej, T. A. Ahanger, I. Ullah, Blockchain-enabled M2M communications for UAV-assisted data transmission, Mathematics 11 (10). doi:10.3390/math11102262.
URL https://www.mdpi.com/2227-7390/11/10/2262

[13] Y. Zhang, X. Lin, J. Wu, B. Pei, Y. Han, Blockchain-assisted UAV data free-boundary spatial querying and authenticated sharing, in: 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD), IEEE, 2023, pp. 565–570.

[14] T. Liu, G. Bai, J. Tao, Y.-A. Zhang, Y. Fang, A multistate network approach for resilience analysis of UAV swarm considering information exchange capacity, Reliability Engineering & System Safety 241 (2024) 109606.

[15] X. Wang, Y. Guo, Y. Gao, Unmanned autonomous intelligent system in 6G non-terrestrial network, Information 15 (1) (2024) 38.

[16] S. Hafeez, G. E. M. Abro, S. A. Memon, T. A. Khan, I. Memon, H. Nasir, Quantum-secured routing in drone communication for 6g-enabled smart mobility, Scientific Reports 16 (1) (2026) 8626. doi:10.1038/s41598-026-36297-5.
URL https://doi.org/10.1038/s41598-026-36297-5

[17] S. Hafeez, A. R. Khan, M. M. Al-Quraan, L. Mohjazi, A. Zoha, M. A. Imran, Y. Sun, Blockchain-assisted UAV communication systems: a comprehensive survey, IEEE Open Journal of Vehicular Technology 4 (2023) 558–580. doi:10.1109/OJVT.2023.3295208.

[18] G. J. Mendis, Y. Wu, J. Wei, M. Sabounchi, R. Roche, A blockchain-powered decentralized and secure computing paradigm, IEEE Transactions on Emerging Topics in Computing 9 (4) (2020) 2201–2222.

[19] Y. Wang, H. Peng, Z. Su, T. H. Luan, A. Benslimane, Y. Wu, A platform-free proof of federated learning consensus mechanism for sustainable blockchains, IEEE Journal on Selected Areas in Communications 40 (12) (2022) 3305–3324.

[20] X. Duan, Y. Guo, Y. Guo, Design of anonymous authentication scheme for vehicle fog services using blockchain, Wireless Networks 30 (1) (2024) 193–207.

[21] Z. Kaleem, F. A. Orakzai, W. Ishaq, K. Latif, J. Zhao, A. Jamalipour, Emerging trends in UAVs: from placement, semantic communications to generative AI for mission-critical networks, IEEE Transactions on Consumer Electronics.

[22] Z. Kaleem, M. Yousaf, A. Qamar, A. Ahmad, T. Q. Duong, W. Choi, A. Jamalipour, UAV-empowered disaster-resilient edge architecture for delay-sensitive communication, IEEE Network 33 (6) (2019) 124–132.

[23] S. Hafeez, G. E. M. Abro, H. Mustafa, Quantum-resilient threat modelling for secure ris-assisted isac in 6g uav corridors (2025). arXiv:2510.25411.
URL https://arxiv.org/abs/2510.25411

[24] O. Chughtai, N. Nawaz, Z. Kaleem, C. Yuen, Drone-assisted cooperative routing scheme for seamless connectivity in V2X communication, IEEE Access.

[25] G. Raja, A. Manoharan, H. Siljak, UGEN: UAV and GAN-aided ensemble network for post-disaster survivor detection through ORAN, IEEE Transactions on Vehicular Technology.

[26] S. Hafeez, H. U. Manzoor, L. Mohjazi, A. Zoha, M. A. Imran, Y. Sun, Blockchain-empowered immutable and reliable delivery service (BIRDS) using UAV networks, in: 2023 IEEE 28th International Workshop on

Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2023, pp. 7–12. doi:10.1109/CAMAD59638.2023.10478401.

[27] G. Sun, L. He, Z. Sun, Q. Wu, S. Liang, J. Li, D. Niyato, V. C. M. Leung, Joint task offloading and resource allocation in aerial-terrestrial UAV networks with edge and fog computing for post-disaster rescue, IEEE Transactions on Mobile Computing.

[28] Z. Wang, J. Li, J. Li, C. Liu, A decentralized decision-making algorithm of UAV swarm with information fusion strategy, Expert Systems with Applications 237 (2024) 121444.

[29] A. Afotanwo, Exploring blockchain-based smart contracts and privacy-preserving cryptocurrencies, FUPRE Journal of Scientific and Industrial Research (FJSIR) 8 (2) (2024) 55–68.

[30] G. Paulin, S. Sambolek, M. Ivasic-Kos, Application of raycast method for person geolocalization and distance determination using UAV images in real-world land search and rescue scenarios, Expert Systems with Applications 237 (2024) 121495.

[31] S. Nicolazzo, M. Arazzi, A. Nocera, M. Conti, et al., Privacy-preserving in blockchain-based federated learning systems, arXiv preprint arXiv:2401.03552.

[32] R. Xing, Z. Su, T. H. Luan, Q. Xu, Y. Wang, R. Li, UAVs-aided delay-tolerant blockchain secure offline transactions in post-disaster vehicular networks, IEEE Transactions on Vehicular Technology 71 (11) (2022) 12030–12043.

[33] N. Cherif, M. Alzenad, H. Yanikomeroglu, A. Yongacoglu, Downlink coverage and rate analysis of an aerial user in vertical heterogeneous networks (VHetNets), IEEE Transactions on Wireless Communications 20 (3) (2020) 1501–1516.

[34] S. Hafeez, M. A. Shawky, M. Al-Quraan, L. Mohjazi, M. A. Imran, Y. Sun, BETA-UAV: blockchain-based efficient and trusted authentication for UAV communication, in: 2022 IEEE 22nd International Conference on Communication Technology (ICCT), IEEE, 2022, pp. 613–617.

[35] Y. Qin, M. A. Kishk, M.-S. Alouini, Performance evaluation of UAV-enabled cellular networks with battery-limited drones, IEEE Communications Letters 24 (12) (2020) 2664–2668.

[36] A. Burger, C. Cichiwskyj, S. Schmeißer, G. Schiele, The elastic internet of things: a platform for self-integrating and self-adaptive IoT-systems with support for embedded adaptive hardware, Future Generation Computer Systems 113 (2020) 607–619.

[37] Q. Qu, I. Nurgaliev, M. Muzammal, C. S. Jensen, J. Fan, On spatio-temporal blockchain query processing, Future Generation Computer Systems 98 (2019) 208–218.