



Hafeez, Sana (2024) *Blockchain-based secure Unmanned Aerial Vehicles (UAV) in network design and optimization*. PhD thesis.

<https://theses.gla.ac.uk/84460/>

Copyright and moral rights for this work are retained by the author

A copy can be downloaded for personal non-commercial research or study, without prior permission or charge

This work cannot be reproduced or quoted extensively from without first obtaining permission from the author

The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the author

When referring to this work, full bibliographic details including the author, title, awarding institution and date of the thesis must be given

Enlighten: Theses

<https://theses.gla.ac.uk/>  
[research-enlighten@glasgow.ac.uk](mailto:research-enlighten@glasgow.ac.uk)

# **Blockchain-based Secure Unmanned Aerial Vehicles (UAV) in Network Design and Optimization**

Sana Hafeez

Submitted in fulfilment of the requirements for the  
Degree of Doctor of Philosophy

School of Engineering  
College of Science and Engineering  
University of Glasgow



University  
of Glasgow

April 2024

# Abstract

Unmanned Aerial Vehicles (UAVs) have emerged as transformative technologies with wide-ranging applications, including surveillance, mapping, remote sensing, search and rescue, and disaster management. As sophisticated Unmanned Aerial Vehicle (UAV) increasingly operate in collaborative swarms, joint optimization challenges arise, such as flight trajectories, scheduling, altitude, Aerial Base Stations (ABS), energy harvesting, power transfer, resource allocation, and power consumption. However, the widespread adoption of UAV networks has been hindered by challenges related to optimal Three-Dimensional (3D) deployment, trajectory optimization, wireless and computational resource allocation, and limited flight durations when operating as ABSs. Crucially, the broadcast nature of UAV-assisted wireless networks renders them susceptible to privacy and security threats such as Distributed Denial-of-Service (DDoS) replay, impersonation, message injection, spoofing, malware infection, eavesdropping, and line-of-interference attacks.

This study aims to address these privacy and security challenges by leveraging blockchain technology's potential to secure data and delivery in UAV communication networks. With amalgamation of blockchain, this study seeks to harness its inherent immutability and cryptographic properties to ensure secure and tamper-proof data transmission, promote trust and transparency among stakeholders, enable automated Smart Contract (SC) for secure delivery, and facilitate standardization and interoperability across platforms. Specifically, blockchain can secure UAV network privacy and security through data privacy and integrity, secure delivery and tracking, access control, identity management, and resilience against cyber-attacks.

Furthermore, this study explores the synergies among blockchain, UAV networks, and Federated Learning (FL) for privacy-preserving intelligent applications in healthcare and wireless networks. FL enables collaborative training of Machine Learning (ML) models without sharing raw data, ensuring data privacy. By integrating FL with blockchain-assisted UAV networks, this study aims to revolutionize future intelligent applications, particularly in time-sensitive and privacy-critical domains. Overall, this thesis contributes to the field by providing a comprehensive analysis of integrating blockchain, FL, and UAV networks, beyond Fifth-Generation (5G) communication networks. It addresses privacy and security concerns related to data and delivery, thereby enabling secure, reliable, and intelligent applications in various sectors.

**Keywords:** Blockchain, drone communication, authentication, federated learning, privacy, security, UAV networks, data integrity, secure delivery.

# Contents

<b>Abstract</b>	<b>i</b>
<b>List of Acronyms</b>	<b>ix</b>
<b>List of Publications</b>	<b>xiii</b>
<b>Acknowledgements</b>	<b>xv</b>
<b>Statement of Copyright</b>	<b>xvi</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Background . . . . .	1
1.2 Research Motivation . . . . .	2
1.3 Aims and Objectives . . . . .	3
1.3.1 Aims . . . . .	3
1.3.2 Objectives . . . . .	3
1.4 Outline of Thesis and Research Publications . . . . .	4
<b>2 Literature Review</b>	<b>9</b>
2.1 Blockchain-enabled UAV Networks:	
Preliminaries and Overview . . . . .	12
2.1.1 UAV Communication Systems . . . . .	12
2.1.2 Data Security and Privacy Specifications in UAV Network . . . . .	14
2.1.3 Fundamentals of Blockchain Technology . . . . .	18
2.2 Role of Blockchain in UAV Networks . . . . .	20
2.2.1 Comparison of Consensus Algorithms and Blockchain Interaction . . . . .	25
2.2.2 Solution Taxonomy: Challenges and Constraints in Networks . . . . .	25
2.2.3 A Systematic Review of Security Issues in Blockchain-Assisted Systems	26
2.2.4 Blockchain-assisted UAV Challenges and Deployment Scenarios . . . . .	26
2.3 Data Security Analysis in Blockchain-enabled UAV Network . . . . .	28
2.4 Challenges and Open Research Directions in UAV Communications . . . . .	33
2.4.1 Confidentiality and Data Security . . . . .	33

2.4.2	Variable Latency Constraints . . . . .	33
2.4.3	Data Integrity and Bogus Parameter Updates . . . . .	33
2.4.4	Obstruction Detection and Communication Delays . . . . .	33
2.4.5	Integration of UAV Traffic Management Devices . . . . .	34
2.5	Summary . . . . .	36
<b>3</b>	<b>Blockchain-based Efficient and Trusted Authentication</b>	<b>37</b>
3.1	Introduction . . . . .	38
3.1.1	Background and Motivation . . . . .	39
3.1.2	Contributions . . . . .	40
3.1.3	Chapter Organization . . . . .	41
3.2	Proposed BETA-UAV Scheme . . . . .	41
3.2.1	System Model . . . . .	42
3.2.2	BETA-UAV: The Proposed Blockchain-Based Efficient Authentication Scheme . . . . .	42
3.2.3	Algorithmic Description . . . . .	44
3.3	Security Analysis . . . . .	44
3.3.1	Message Authentication . . . . .	45
3.3.2	Security Protection against Active Attacks . . . . .	45
3.3.3	Threat Model . . . . .	47
3.4	Implementation and Performance Evaluation . . . . .	47
3.5	Deployment on Rinkeby Ethereum Test Network . . . . .	49
3.5.1	Setting up the Ethereum Environment . . . . .	49
3.5.2	Configuring Metamask Wallet . . . . .	49
3.5.3	Deploying the Smart Contract . . . . .	50
3.5.4	Overview of the Initial Authentication Step . . . . .	50
3.5.5	Comprehensive Protocol Overview . . . . .	51
3.5.6	Analysis of the Wallet Interface on the Rinkeby Test Network . . . . .	51
3.5.7	Analysis of an Ethereum Blockchain Transaction . . . . .	53
3.5.8	Computation Cost Comparison . . . . .	54
3.5.9	Estimating Gas Cost . . . . .	54
3.5.10	Communication Cost Comparison . . . . .	54
3.6	Summary . . . . .	56
<b>4</b>	<b>UAV Networks for Post-Disaster: A Flocking Approach</b>	<b>58</b>
4.1	Introduction . . . . .	59
4.1.1	Background . . . . .	59
4.1.2	Motivation . . . . .	60
4.1.3	Contributions and Organization . . . . .	61

4.2	Preliminary Study . . . . .	61
4.2.1	Blockchain-Enabled UAV Solutions for Disaster Response . . . . .	61
4.2.2	Consensus Protocols and Smart Contracts for UAV Blockchains . . . . .	62
4.3	System Architecture and Models . . . . .	64
4.3.1	Communication Model . . . . .	65
4.3.2	Consortium Blockchain Architecture . . . . .	66
4.3.3	Security Measurements . . . . .	66
4.4	Decentralized Flocking Model for UAV Disaster Response . . . . .	67
4.4.1	Concrete Examples of Flocking Algorithms for UAV Disaster Relief Functions . . . . .	67
4.4.2	Reynolds Flocking Rules and Their Application . . . . .	68
4.4.3	Dynamic State Propagation and Battery Model . . . . .	68
4.4.4	Significance of Flocking Algorithms in Multi-Agent Systems . . . . .	69
4.4.5	Alpha-Neighbors of Alpha-Agents: Proximity Net . . . . .	70
4.5	Enhanced DPoS-PBFT Consensus Mechanism for UAV Networks . . . . .	70
4.5.1	Mechanism Overview . . . . .	72
4.6	Simulations and Discussions . . . . .	74
4.6.1	Simulation Settings . . . . .	74
4.7	Novel DPoS-PBFT Consensus Results . . . . .	77
4.7.1	Simulations Results . . . . .	78
4.8	Conclusion . . . . .	83
<b>5</b>	<b>Blockchain-Empowered Delivery Service</b>	<b>85</b>
5.1	Introduction . . . . .	86
5.2	System Model and Problem Description . . . . .	88
5.2.1	UAV Network Model . . . . .	89
5.2.2	Communication Model . . . . .	89
5.2.3	Mobility Model . . . . .	90
5.3	Proposed BIRDS Scheme . . . . .	91
5.3.1	Authentication and Registration Phase of BIRDS . . . . .	91
5.3.2	Proof-of-Competence in BIRDS . . . . .	92
5.3.3	BIRDS Criteria for Miners . . . . .	92
5.3.4	Credibility of UAV Node Selection . . . . .	93
5.3.5	Energy Consumption in BIRDS . . . . .	93
5.3.6	UAV Reputation Score in BIRDS . . . . .	94
5.4	Results and Discussion . . . . .	95
5.5	Conclusions . . . . .	97

<b>6</b>	<b>Blockchain-enabled Federated Learning (BCS-FL)</b>	<b>100</b>
6.1	Introduction . . . . .	101
6.2	System Model for UAV Networks . . . . .	102
6.2.1	UAV Network Topology Model . . . . .	102
6.2.2	Communication Capabilities and Clustering in UAV Networks . . . . .	103
6.2.3	Clustering Architecture for UAV Networks . . . . .	103
6.2.4	Roles and Responsibilities of UAVs in the Collaborative Training Framework . . . . .	103
6.3	Blockchain-Based Federated Learning . . . . .	104
6.3.1	BCS-FL Overview . . . . .	104
6.3.2	Role of Smart Contracts in BCS-FL Framework . . . . .	106
6.3.3	Federated Learning Workflow in BCS-FL Framework . . . . .	107
6.3.4	Model Aggregation Strategies in BCS-FL Framework . . . . .	108
6.3.5	Strategies for Inter-cluster Aggregation . . . . .	108
6.3.6	Trade-offs in Aggregation Strategies within BCS-FL Framework . . . . .	110
6.4	Numerical Results and Discussions . . . . .	111
6.4.1	Simulation Settings . . . . .	111
6.4.2	Model Efficiency . . . . .	111
6.4.3	Communication Overhead . . . . .	112
6.5	Summary . . . . .	114
<b>7</b>	<b>Conclusions and Future Works</b>	<b>116</b>
7.1	Limitations and Challenges . . . . .	117
7.2	Future works . . . . .	118
7.2.1	AI-Driven Network Optimization and Automation . . . . .	118
7.2.2	FL and Privacy-Preserving UAV Networks . . . . .	118
7.2.3	Digital Twin Integration and Virtual Testing . . . . .	118
7.2.4	Cross-Domain Interoperability and Standardization . . . . .	119
7.2.5	Cyber-Physical Resilience, Security, and Robustness of UAV Networks . . . . .	119

# List of Tables

2.1	Comparisons of Existing Survey Papers 1: 5G-concentrated, 2: Blockchain-concentrated, 3: UAV-concentrated 4: Performance Comparisons with other Technologies. . . . .	10
2.2	Summary of Privacy and Security Attacks in Blockchain-Enabled UAV Networks	14
2.3	Comparison Among Consensus Algorithms. Acronyms: PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Proof of Stake), PoC (Proof of Capacity), PoB (Proof of Burn), PoI (Proof of Importance), PoA (Proof of Activity), DAG (Directed Acyclic Graph), DBFT (Delegated Byzantine Fault Tolerance), SBFT (Simplified Byzantine Fault Tolerance), PBFT (Practical Byzantine Fault Tolerance), PoET (Proof of Elapsed Time), LPoS (Leased Proof of Stake). . . . .	22
2.4	Cybersecurity-related Requirement in UAV Networks . . . . .	32
2.5	Comparison of Communication Perspective Challenges vs. Blockchain Perspective Challenges in UAV Networks . . . . .	34
3.1	List of Notations for the Proposed BETA-UAV Scheme . . . . .	43
3.2	Remix Settings . . . . .	48
3.3	Comparison of Actual vs Estimated Cost . . . . .	54
4.1	Comparison of Consensus Protocols . . . . .	72
4.2	Key Parameters and Values of the Hybrid DPoS-PBFT Blockchain Mechanism	76
4.3	UAV Simulation Parameters . . . . .	77
5.1	List of Notations . . . . .	89



# List of Figures

1.1	Thesis Structure. . . . .	6
1.2	Evolution of Drones. . . . .	7
1.3	Summarize the Thesis Structure, Highlighting Three Core Sections. . . . .	8
2.1	Key Aspects and Considerations of Research. . . . .	10
2.2	An Illustrative Overview of Structure and Reading Map. . . . .	11
2.3	Percentage of Different Attacks on UAV Network [1]. . . . .	16
2.4	Exploitable Security Gaps and Solutions. . . . .	17
2.5	Simplified Operation of Blockchain Technology. . . . .	19
2.6	Asymmetric Key Cryptography Secure Blockchain Transactions. . . . .	20
2.7	Different Blockchain Consensus Mechanisms. . . . .	21
2.8	Blockchain-assisted UAV Scenario. . . . .	27
2.9	Blockchain-enabled UAV Communication. . . . .	29
3.1	UAV Ad-hoc Network. . . . .	41
3.2	Network Deployment. . . . .	48
3.3	Comprehensive Overview of the Communication Protocol. . . . .	51
3.4	Rinkeby Test Network MetaMask. . . . .	52
3.5	Contract Deployment for BETA-UAV. . . . .	52
3.6	Computational Delay vs Number of Drones. . . . .	55
3.7	Comparison of Computational Cost. . . . .	55
4.1	The Architecture for Blockchain-Enabled UAV Coordination in Disaster Response. . . . .	64
4.2	The 2D spatial distribution of flocking UAVs engaged in post-disaster activities. More detailed description is provided in Section 4.4. . . . .	69
4.3	Detailed Working Mechanism of the DPoS-PBFT Consensus Protocol. . . . .	71
4.4	(a) Throughput, Latency over Time (b) Latency Distribution. . . . .	77
4.5	Latency Comparison of Consensus Protocols. . . . .	78
4.6	Resilience Comparison - Cyberattacks. . . . .	79
4.7	Throughput and Latency Over Time. . . . .	79

4.8	Resilience Against Cyberattacks. . . . .	80
4.9	UAV Positioning Simulation with ANOVA Results. . . . .	81
4.10	Distribution of Latency Across UAV Operations. . . . .	81
4.11	Within-Cluster Latency. . . . .	82
4.12	Accross-Cluster Latency. . . . .	83
5.1	Applications of UAV Delivery Services. . . . .	86
5.2	Blockchain-Assisted UAV Delivery Services. . . . .	88
5.3	BIRDS Framework. . . . .	91
5.4	Blockchain Transaction Time vs Number of UAVs. . . . .	95
5.5	Estimated and Actual Delivery Time for UAV Tasks. . . . .	96
5.6	Traditional Blockchain vs BIRDS. . . . .	96
5.7	Impact of the Number of UAVs on the Delay. . . . .	97
6.1	The BCS-FL Framework. . . . .	105
6.2	A Demonstration of the kHA Scheme. . . . .	110
6.3	Performance of (a) Accuracy and (b) Loss, CIFAR-10 Dataset. . . . .	112
6.4	The BCS-FL Performance of Accuracy. . . . .	112
6.5	Performance on BCS-FL (a) Accuracy and (b) Loss MNIST Dataset. . . . .	113
6.6	Influence of $k$ on BCS-FL (a) Accuracy and (b) Loss. . . . .	113
6.7	Impact of Inter-cluster Aggregation Scheme on Communication Overhead. . . . .	113

# List of Acronyms

**2D** Two-Dimensional

**3D** Three-Dimensional

**3GPP** 3rd Generation Partnership Project

**5G** Fifth-Generation

**6G** Sixth-Generation

**A2A** Aerial-to-Aerial

**A2G** Aerial-to-Ground

**ABS** Aerial Base Stations

**AI** Artificial Intelligence

**ANOVA** Analysis of Variance

**B5G** Beyond 5G

**BCS-FL** Blockchain-Enabled Clustered and Scalable Federated Learning

**BCSFL** Blockchain-Enabled Clustered and Scalable Federated Learning

**BETA** Blockchain-Based Efficient Authentication

**BETA-UAV** Blockchain-Based Efficient Authentication for Secure UAV Communication

**BIRDS** Blockchain Empowered Immutable and Reliable Delivery Service

**BS** Base Stations

**CH** Cluster Head

**CHs** Cluster Heads

**CNN** Convolutional Neural Network

**CPS** Cyber-Physical System

**DLT** Delta Drone International Limited

**D2C** Drone-to-Cellular Communication

**D2D** Drone-to-Drone Communication

**D2G** Drone-to-Ground Communication

**D2S** Drone-to-Satellite Communication

**DDoS** Distributed Denial-of-Service

**DApps** decentralized applications

**DoS** Denial-of-Service

**DPoS** Delegated Proof of Stake

**DPoS-PBFT** Delegated Proof of Stake Practical Byzantine Fault Tolerance

**DNS** Domain Name System

**ECC** Elliptic Curve Cryptosystem

**ECDSA** Elliptic Curve Digital Signature Algorithm

**EVM** Ethereum Virtual Machine

**FAA** Federal Aviation Administration

**FANET** Flying Ad-Hoc Network

**FCA** Fully Centralised Aggregation

**FedAvg** Federated Averaging

**FedBlock** Federated Blockchain

**FL** Federated Learning

**GCS** Ground Control System

**GPS** Global Positioning System

**ICMP** Internet Control Message Protocol

**ID** Identity

- IID** Independent and Identically Distributed
- IoD** Internet-of-Drones
- IoT** Internet-of-Things
- IPFS** Interplanetary File System
- ITS** Intelligent Transportation System
- IDE** Integrated Development Environment
- IRS** Intelligent Reflecting Surfaces
- kHA** k-Hop Aggregation
- LoS** Line-of-Sight
- MAC** Medium Access Control
- MANET** Mobile Ad Hoc Networks
- MEC** Multi-Access Edge Computing
- MITM** Man-in-the-Middle
- ML** Machine Learning
- MNIST** Modified National Institute of Standards and Technology Database
- MIRACL** Multi-Precision Integer and Rational Arithmetic Cryptographic Library
- Non-IID** Non-Independent and Non-Identically Distributed
- NSA** National Security Agency
- NTN** Non-Terrestrial Networks
- OSI** Open System Interconnection
- PBFT** Practical Byzantine Fault Tolerance
- PHY** Physical Layer
- PoA** Proof-of-Authority
- PoC** Proof-of-Competence
- PoF** Proof-of-Freshness

- PoI** Proof-of-Identification
- PoR** Proof-of-Resources
- PoW** Proof-of-Work
- ReLU** Rectified Linear Unit
- RRC** Remote and Real-Time Control
- RSU** Roadside Unit
- SGD** Stochastic Gradient Descent
- SHA** Secure Hash Algorithms
- SNR** Signal-to-Noise Ratio
- SINR** The signal-to-interference-plus-noise ratio
- SC** Smart Contract
- SPoF** Single Point of Failure
- TA** Trusted Authority
- TCP/IP** Transmission Control Protocol/Internet Protocol
- THz** Terahertz Communications
- TPS** Transaction Per Second
- U-PBFT** UAV Practical Byzantine Fault Tolerance
- UAV** Unmanned Aerial Vehicle
- UAVs** Unmanned Aerial Vehicles
- UTM** Unmanned Aircraft System Traffic Management
- V2X** Vehicle-to-Everything
- VANET** Vehicular Ad-hoc Networks
- uRLLC** Ultra-Reliable Low Latency
- ZKP** zero-knowledge proofs

# List of Publications

During my PhD studies, As a first author, I have all publications including conference papers, journal articles, and technical papers. Each of these works is directly linked to the research and findings of my thesis. Below, is a comprehensive list of the publications I have authored throughout my doctoral journey

## Articles

- S. Hafeez, Y. Sun, and M. A. Imran, "Drones to the Rescue: Envisioning the Future of Healthcare Delivery in Scotland Using Autonomous Air Transportation," Drafted for Nature Communications, 2024.
- S. Hafeez, R. Cheng, L. Mohjazi, Y. Sun, and M. A. Imran, "Blockchain-Enhanced UAV Flocking Networks for Post-Disaster Communication," in Digital Communications and Networks (DCN), 2024 (Under Review).

## Conference Papers

- S. Hafeez, R. Cheng, L. Mohjazi, M. A. Imran, and Y. Sun, "A Blockchain-Enabled Framework of UAV Coordination for Post-Disaster Networks," in Proc. IEEE 99th Vehicular Tech. Conf. (VTC Spring), Singapore, June 2024.
- S. Hafeez, H. U. Manzoor, L. Mohjazi, A. Zoha, M. A. Imran, and Y. Sun, "Blockchain-Empowered Immutable and Reliable Delivery Service (BIRDS) Using UAV Networks," in Proc. IEEE Int. Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), UK, 2023.
- S. Hafeez, L. Mohjazi, M. A. Imran, and Y. Sun, "Blockchain-enabled Clustered and Scalable Federated Learning (BCS-FL) Framework in UAV Networks," in Proc. IEEE Int. Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 6–20, 2023.
- S. Hafeez, M. A. Shawky, M. Al-Quraan, L. Mohjazi, M. A. Imran, and Y. Sun, "BETA-UAV: Blockchain-based Efficient and Trusted Authentication for UAV Communication," IEEE 22nd Int. Conf. on Communication Tech. (ICCT), Nanjing, China, Nov. 2022.

**Surveys**

- S. Hafeez, A. R. Khan, M. Al-Quraan, L. Mohjazi, A. Zoha, M. A. Imran, and Y. Sun, "Blockchain-assisted UAV Communication Systems: A Comprehensive Survey," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 558-580, 2023.



# Acknowledgements

First and foremost, I humbly express my profound gratitude to *Allah (SWT)*, for his immeasurable grace and mercy that have sustained me through this journey. I am eternally indebted to the teachings of *Prophet Muhammad (pbuh)*, whose wisdom and examples have been my guiding stars in this endeavor. Completing this thesis would not have been possible without the immense support and guidance from several exceptional individuals.

I would like to express my deepest gratitude to Professor. *Muhammad Ali Imran*, for his unwavering support and motivation as a mentor throughout my PhD journey. His visionary leadership and constant encouragement propelled me through the peaks and valleys of my PhD journey. This endeavor would have been impossible without his steadfast dedication and unwavering belief in my capabilities, even during the most challenging moments. I am privileged and deeply grateful for the opportunity to work under his esteemed guidance. I am extremely grateful to Dr. *Yao Sun* and Dr. *Lina Mohjazi* for their patient supervision and insightful feedback and for allowing me to grow as a researcher under their wings. Their dedication to research and academic excellence has served as a source of inspiration. I extend my sincere appreciation to *University of Glasgow* and *CSI* for their unwavering support during my hardships.

I am profoundly grateful to the former Prime Minister of Pakistan, Mr. *Imran Khan*, for the scholarship that enabled my PhD journey at a renowned global institution. Through his generous support, my longstanding dream has transformed into a tangible reality, profoundly shaping my career trajectory and elevating my ambitions to unprecedented levels. My journey would have been incomplete without heartfelt prayers and steadfast encouragement from *Brigadier Jamil Sarwar Malik* to elect me into his blind trust. His vision of empowering future female leaders and his conviction of my potential ignited a spark to aim higher and work harder.

I owe everything I am today, from my core values to my aspirations, to the upbringing gifted by my beloved parents. Their unconditional affection, life lessons, and prayers at night and day enabled me to expand my knowledge. Finally, words cannot fully capture my appreciation for my family, whose limitless love and selfless sacrifices have been the foundation of my resilience. My heart overflows with love and thankfulness to my partner, *Muhammad Taimoor*, and my beloved daughters *Anabiya Noor*, *Umamah Noor*, and *Inshal Zahrah* whose constant support has been my guiding light, inspiring me to persist against all odds.

# Statement of Copyright

The copyright of this thesis rests with the author. No quotation from it should be published without the author's prior written consent and information derived from it should be acknowledged.

**University of Glasgow**  
*College of Science & Engineering*  
**Statement of Originality**

**Name:** Sana Hafeez

**Registration Number:** xxxxxxxx

I certify that the thesis presented here for examination of a PhD degree at the University of Glasgow is solely my work, other than where I have indicated that it is the work of others (in which case the extent of any work carried out jointly by me and any other person is identified in it) and that the thesis has not been edited by a third party beyond what is permitted by the University's PGR Code of Practice.

The copyright of this thesis rests with the authors. No quotation from it was permitted without full acknowledgement.

I declare that the thesis does not include the work-forming part of a thesis presented successfully to another degree.

I declare that This thesis has been produced by the University of Glasgow's Code of Good Practice in Research.

I acknowledge that if any issues are raised regarding good research practice based on a review of the thesis, the examination may be postponed, pending the outcome of any investigation of the issues.

**Signature:**

**Date:** July 9, 2024

# Chapter 1

## Introduction

This chapter introduces the background and research motivation underlying this thesis, discusses its objectives and main contributions, outlines the thesis, and includes the relevant publications.

### 1.1 Background

The 5G of cellular networks, which began rolling out in the late 2010s, has marked a significant leap. 5G promises ultra-low latency, massive device connectivity, and multi-Gbps data rates, enabling a wide range of applications, including enhanced mobile broadband, massive machine-type communications, and Ultra-Reliable Low Latency (uRLLC). uRLLC is particularly crucial for applications such as UAV communication networks, where real-time data transmission and reliable connectivity are paramount. In the future, Sixth-Generation (6G) wireless networks are expected to emerge around 2030, promising even higher data rates, lower latency, and improved spectral and energy efficiencies [2]. 6G is anticipated to leverage advanced technologies such as Terahertz Communications (THz), Intelligent Reflecting Surfaces (IRS), and seamless integration of terrestrial and Non-Terrestrial Networks (NTN), including UAV-based communication systems.

The design and optimization of UAV communication networks are inherently linked to the development of cellular generation. UAVs, also known as drones, have emerged as versatile platforms for various applications, including surveillance, remote sensing, and emergency response. Effective communication between the UAV and Ground Control System (GCS) is critical for real-time data exchange, command and control, and situational awareness. Optimizing UAV communication networks involves addressing several key challenges such as path planning, resource allocation, interference management, and energy efficiency [3]. Mathematical optimization techniques including convex optimization, game theory, and ML play pivotal roles in the development of efficient algorithms for network design and resource allocation.

Privacy and security are paramount concerns in UAV communication networks, particularly in sensitive applications such as military operations or critical infrastructure monitoring. Secure

communication protocols, encryption techniques, and access control mechanisms are essential for protecting against unauthorized access, eavesdropping, and cyber-attacks [4]. In addition, the integration of blockchain technology into UAV communication networks has been proposed to enhance the security, transparency, and decentralized control. Blockchain's distributed ledger and consensus mechanisms can facilitate secure data exchange, access control, and trustless coordination among UAVs and ground stations. Looking ahead, the continued convergence of 5G, 6G, and UAV technologies, blockchains, and advanced optimization techniques will shape the future of UAV communication networks. Ongoing research efforts are focused on developing intelligent, self-organizing, and resilient networks that can adapt to dynamic environments, ensuring reliable, secure, and efficient communication for a wide range of applications.

## 1.2 Research Motivation

The motivation for this study stems from the growing demand for secure and resilient UAV communication networks that can withstand cyber threats, ensure data integrity, and maintain privacy. Blockchain technology, with its inherent characteristics of decentralization, transparency, and immutability, is a promising approach for addressing these challenges. Benefiting from the power of distributed ledgers and consensus mechanisms, blockchains can establish secure and tamper-proof infrastructure for UAV communication, thereby enhancing trust, accountability, and resilience [5]. The growing use of UAVs in various sectors such as monitoring, remote sensing, and emergency services has heightened the demand for durable and dependable communication systems. Traditional centralized systems are vulnerable to Single Point of Failure (SPoF) and susceptible to cyber-attacks, compromising the confidentiality and integrity of sensitive data [6]. However, owing to its distributed and decentralized nature, blockchain technology offers a resilient alternative by eliminating central authority and enabling secure peer-to-peer transactions.

Moreover, the immutability of blockchain records ensures that data transmitted within UAV networks remain tamper-proof and auditable while safeguarding against malicious modifications or unauthorized access. This property is particularly crucial in scenarios where UAVs operate in hostile environments or handle sensitive information such as military operations or critical infrastructure monitoring. Privacy concerns also arise when UAVs collect and transmit data that can potentially capture personal information and sensitive details. The integration of blockchain with privacy-preserving techniques, such as zero-knowledge proofs (ZKP) and homomorphic encryption, can enable secure data sharing and processing while maintaining the confidentiality of sensitive information [7].

Furthermore, blockchain-enabled UAV networks can facilitate trustless coordination and collaboration among multiple UAVs, thereby enabling decentralized decision making and efficient resource allocation. This capability is particularly valuable in scenarios where centralized con-

trol is impractical or unreliable, such as post-disaster situations or remote areas that lack traditional communication infrastructure. To address these pressing challenges, this study aims to unlock the full potential of UAV communication networks, thereby enabling secure, resilient, and private-preserving operations. The integration of blockchain technology with UAV networks not only enhances security and privacy, but also fosters trust, accountability, and transparency, paving the way for the widespread adoption and utilization of these aerial systems across various critical applications.

## 1.3 Aims and Objectives

This section summarizes the aims, and objectives of the study.

### 1.3.1 Aims

The main goal of this dissertation is to develop a comprehensive blockchain architecture that tackles the challenges of security, privacy, resilience, and intelligence in UAV communication networks. By incorporating cryptographic and consensus methodologies, this thesis aims to provide a robust and all-encompassing framework that leverages blockchain's distinctive features to maintain security, privacy, resilience, and intelligence in UAV communication networks. This research establishes a solid foundation for the extensive application and integration of UAVs in crucial sectors, ensuring dependable and trustworthy operations in complex and demanding environments.

### 1.3.2 Objectives

The primary research objectives are as follows. This thesis aims to develop innovative blockchain-based solutions to address critical challenges in UAV networks with a strong emphasis on security, resilience, and decentralization. The specific research objectives were as follows:

- *Objective 1:* To come up with a robust blockchain model for enabling resilient and self-organizing UAV swarms in post-disaster scenarios, capable of sustaining communication channels independent of central infrastructure. This model leverages the inherent properties of blockchain technology to foster trust and coordination among UAVs, without relying on a SPoF.
- *Objective 2:* To formulate a secure and transparent blockchain-driven framework for UAV-involved logistics and supply chain operations. This framework ensures the integrity and traceability of delivery records while optimizing route planning and transportation through SCs and consensus mechanisms, thereby enhancing operational efficiency and accountability.

- *Objective 3:* To introduce an innovative clustered and scalable FL approach for decentralized UAV networks, seamlessly integrating blockchain technology with privacy-preserving ML techniques. This approach enables collaborative model training and knowledge sharing among UAVs without compromising data privacy and promoting intelligent decision-making and adaptive behaviour.
- *Objective 4:* To investigate potential challenges, limitations, and future research avenues in the seamless integration of blockchain technology with UAV communication networks. This exploration will lay the groundwork for ongoing progress and innovation in this field by addressing the emerging requirements and real-world deployment scenarios.
- *Objective 5:* To conduct precise theoretical analyses and simulation-based performance evaluations to assess the effectiveness, security, and scalability of the proposed blockchain solutions in UAV networks. Comprehensive comparative studies will be carried out against existing state-of-the-art methods to quantify the improvements in efficiency, security, latency, and overhead achieved by the proposed solutions.
- *Objective 6:* Rigorous security analysis is conducted to ensure the resilience of the proposed methodologies against various types of attacks. Formal verification techniques such as logic-based analysis were employed to assess the security guarantees provided by the proposed authentication schemes.

## 1.4 Outline of Thesis and Research Publications

This thesis presents a comprehensive investigation of the application of blockchain technology to address the privacy and security challenges in UAV communication networks. This thesis is structured across multiple chapters, 1–6, each building in the previous chapter as shown in Fig. 1.1, to construct a cohesive and robust solution. Chapter 1 introduces the background and research motivation underlying this thesis, discusses the objectives and main contributions, outlines the structure of the thesis, and includes the publications. Chapter 2 establishes the foundation by providing a comprehensive survey of existing literature on blockchain-assisted UAV communication systems. This chapter analyzes the state-of-the-art in this domain and identifies the key challenges, limitations, and opportunities for further research. The insights derived from this survey inform the subsequent chapters and serve as a springboard for the proposed solutions.

Building on the literature review, Chapter 3 demonstrate Blockchain-Based Efficient Authentication for Secure UAV Communication (BETA-UAV), a novel framework that employs blockchain technology to enable efficient and trusted authentication of UAV communication networks. This framework addresses the critical issue of secure and reliable authentication, a prerequisite for maintaining the integrity and confidentiality of data exchanged within UAV

networks. BETA-UAV leverages cryptographic primitives and decentralized consensus mechanisms to establish a robust and resilient authentication infrastructure.

While BETA-UAV focuses on authentication, Chapter 4 extends the application of blockchain technology to address the challenges of post-disaster communication using UAV flocking networks. The traditional communication infrastructure is often compromised due to natural disasters, necessitating the deployment of resilient and adaptable solutions. This section proposes a blockchain-enhanced UAV flocking network that enables secure and reliable communication in such scenarios. The proposed solution, which merges intelligent swarming algorithms with blockchain-based consensus protocols, guarantees the integrity and accessibility of communication channels while sustaining performance even in the absence of a centralized infrastructure.

Chapter 5 explores the potential of blockchain technology and UAV networks in revolutionizing logistics and supply chain domains. It introduces Blockchain Empowered Immutable and Reliable Delivery Service (BIRDS), a framework that leverages the strengths of these two technologies to enable secure, transparent, and efficient delivery services. Utilizing the immutability and transparency inherent in blockchain technology, BIRDS ensures the integrity and traceability of the delivery records. Concurrently, the agility and efficiency of UAV networks enhance the navigation and transportation of goods across complex terrain. This synergy optimizes the reliability and effectiveness of the delivery process.

Finally, Chapter 6 introduces a novel framework for enabling clustered and scalable FL in UAV networks, termed Blockchain-Enabled Clustered and Scalable Federated Learning (BCS-FL). This framework addresses the challenges of distributing ML models and training data across decentralized UAV networks, while preserving privacy and scalability. Integrating blockchain technology with FL principles, BCS-FL enables collaborative model training, where UAV contribute their data and computational resources while maintaining data privacy. This approach facilitates the development of intelligent and adaptive UAV networks capable of tackling complex challenges and optimizing their performance in dynamic environments. Chapter 7 concludes the findings of this thesis and offers future insights into further enhancing the security, privacy, and intelligence of UAV network research questions and answers. In summary, this thesis presents a cohesive and comprehensive research endeavor that builds progressively upon the foundations established in each chapter. It begins with a literature review, followed by the development of a secure authentication framework BETA-UAV, blockchain-enhanced solution for post-disaster communication (UAV flocking networks), secure and transparent delivery service BIRDS, and culminating blockchain-enabled FL framework BCS-FL to enable intelligent and adaptive UAV networks. The ultimate objective of this endeavor is to effortlessly incorporate blockchain technology in order to resolve the privacy and security issues inherent in UAV communication networks. This would allow these aerial systems to function securely, robustly, and with heightened collective intelligence, without any compromise on their performance.

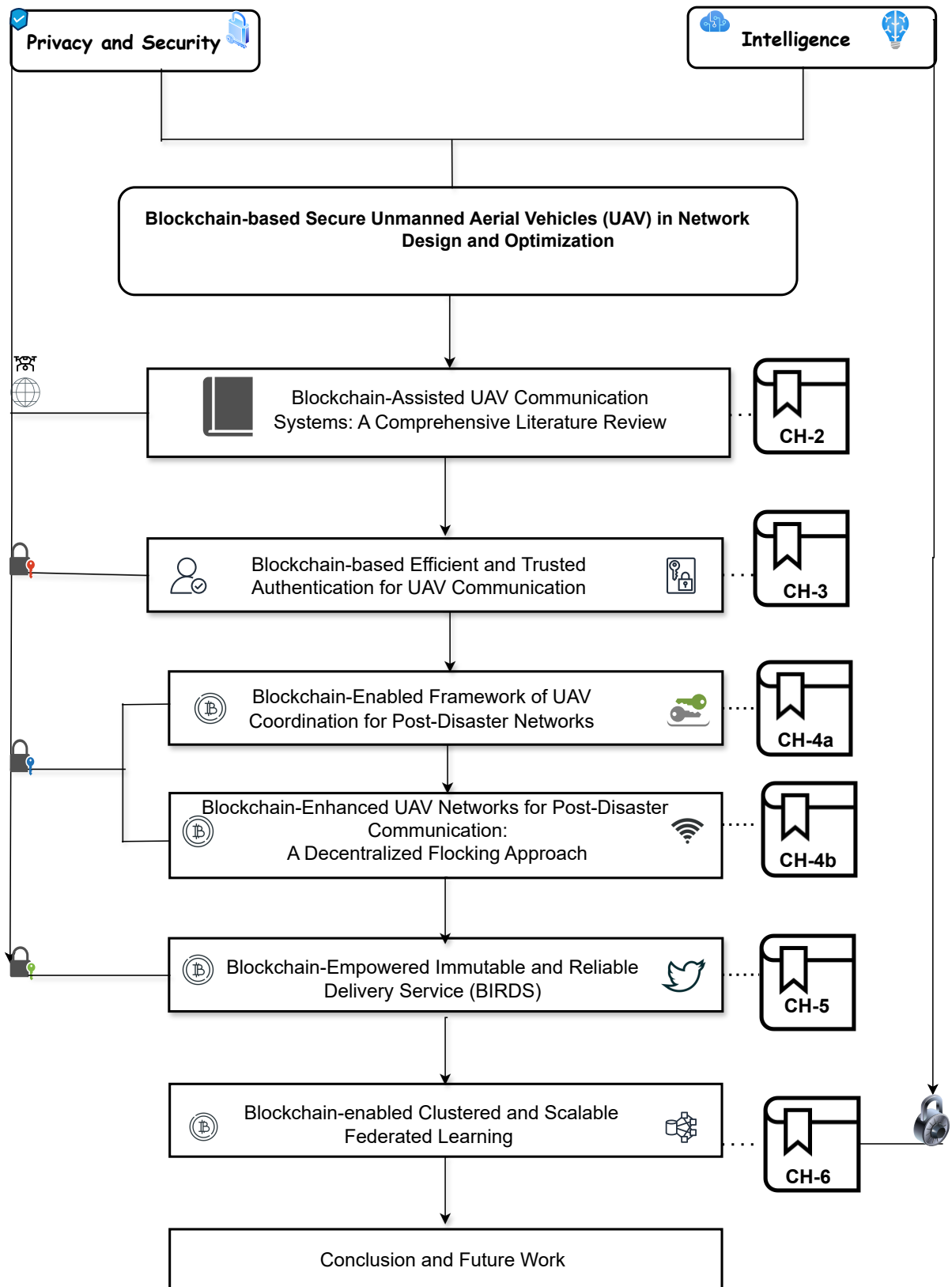


Figure 1.1: Thesis Structure.



The use of UAV has gained significant attention owing to its high mobility, affordability, and ease of use. UAV are considered valuable service enablers for innovative city applications, healthcare domains, real-time surveillance and monitoring, disaster management, and wireless communication and military as presented in Fig. 1.2. Approximately 102.4 billion dollars will be spent annually on UAV by 2030, a compound annual growth rate of 19.6%, surpassing 19.78 billion dollars in 2020 [8]. Solely devoted UAVs can be deployed as ABSs, or relays to assist terrestrial wireless communications from the sky, resulting in an innovative approach known as UAV-assisted communications. This approach has several advantages, including potential on-demand deployment, high network reconfiguration flexibility, and high probability of Line-of-Sight (LoS) communication links. UAV have the potential to meet these requirements concerning user mobility, random channel fluctuations, and blocking effects. UAV can broaden the coverage area, decrease the blind spots of terrestrial Base Stations (BS), and increase the probability of a direct LoS. The environmental challenges UAV face cannot be solved using conventional optimization techniques.

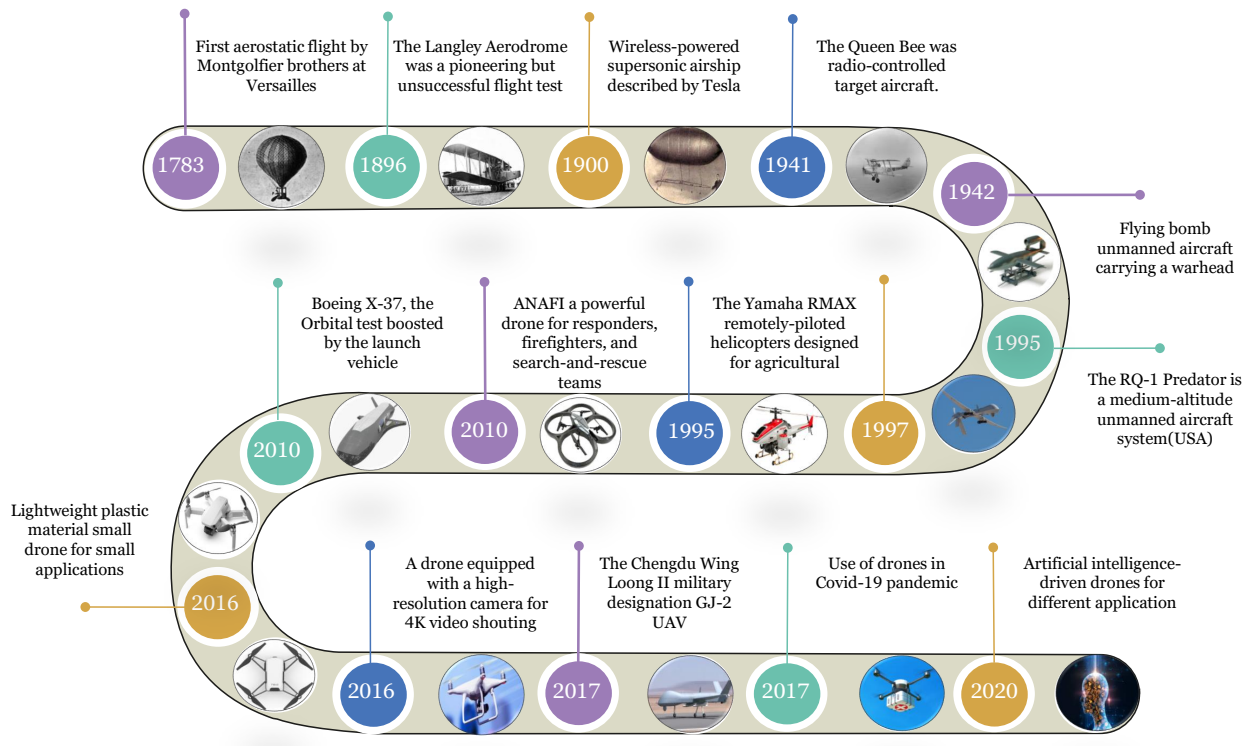


Figure 1.2: Evolution of Drones.

This thesis consists of three key sections, as presented in Fig. 1.3, which focus on different yet interconnected aspects of blockchain-enhanced UAV network design and optimization

- 1. UAV Communication Systems:** This part is discussed in Section 2.1.1 and explores the traditional communication challenges within UAV networks, such as topology control, and the diverse applications of these networks in fields like delivery services, post-disaster management, and healthcare.

2. **Intelligence in UAV Networks:** Here, in Section 2.2.4, the focus shifts to the integration of ML, particularly FL, into UAV networks. This integration is pivotal for enhancing the intelligence and efficiency of these systems, particularly in healthcare and wireless-network applications.
3. **Data Security and User Privacy in UAV Networks:** The final part, Sections 2.1.2 and 2.1.3-2.2, is the core of the thesis—the application of blockchain technology in fortifying data security and user privacy within UAV networks.

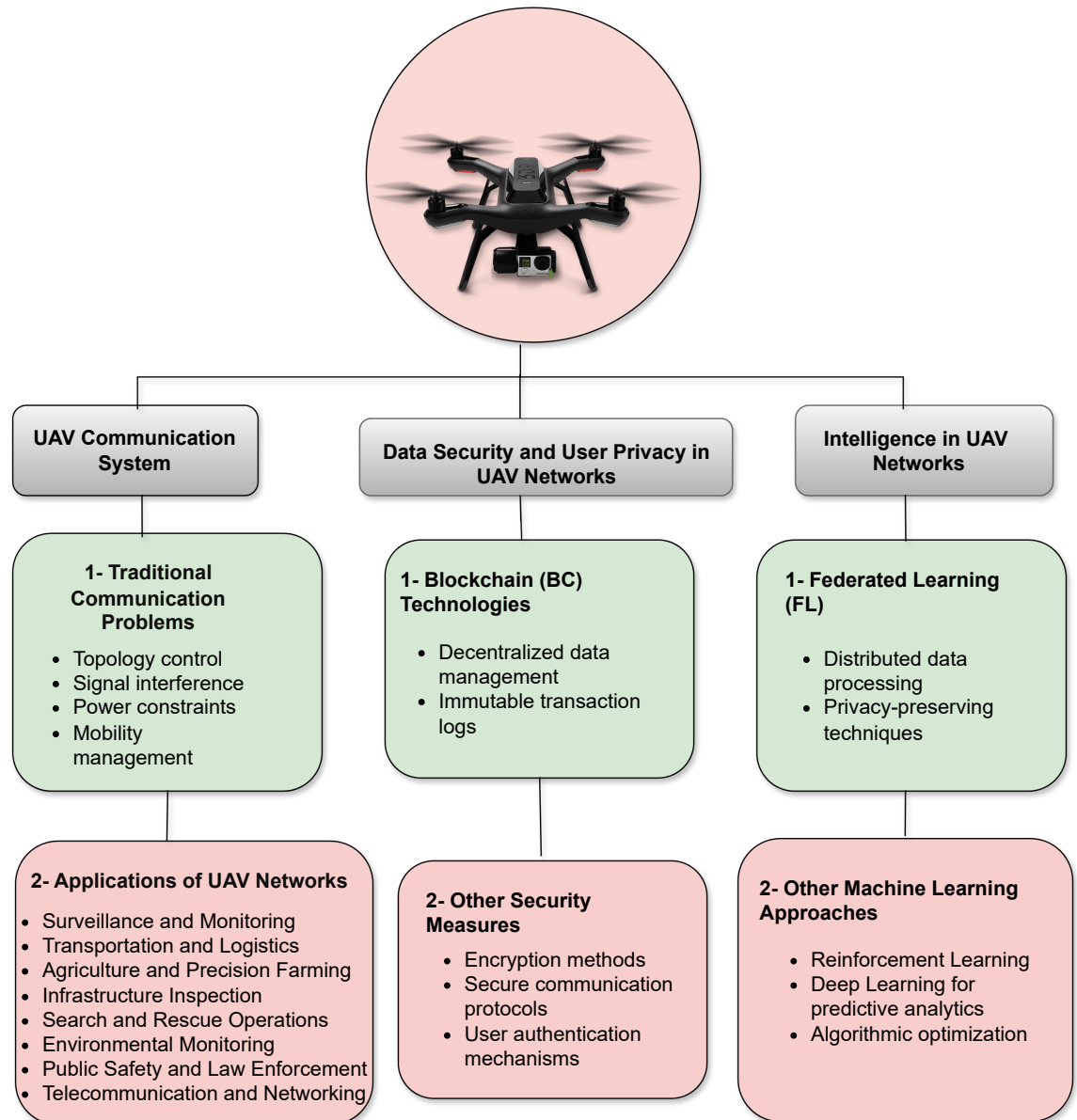


Figure 1.3: Summarize the Thesis Structure, Highlighting Three Core Sections.

# Chapter 2

## Literature Review

Recently, some surveys in the literature have dealt with UAV-assisted communication enabled by blockchains. The comparisons of the existing surveys are presented in Table 2.1. In the literature, a detailed survey [9] provides comprehensive information on 6G network-based blockchain-envisoned UAV communication. In addition, this study covers the architecture, specifications, and use cases of 6G technology, while also discussing the security and communication aspects of the technology. Finally, it identifies potential privacy challenges that blockchain can solve. Similarly, another survey [10] introduced Physical Layer (PHY) layer security in UAV communication networks to address the problem of information leakage caused by potential eavesdropping. A UAV network of this type aims to achieve information exchange confidentiality. In [11], UAV energy constraints, high altitude, and 3D mobility were presented, followed by a literature review on Global Positioning System (GPS) communication. Subsequent studies [12] have focused on UAV networks and blockchain technology, including their security problems, limitations, and solutions. Moving on to general blockchain surveys, a thorough survey [13] covered the integration of GPS and 6G with blockchains in UAV communications. Maintaining the present trend, this chapter [14] provides a comprehensive overview of recent developments in blockchain-based FL. According to previous studies, blockchain has been widely used to address the challenges of drone networks. The UAV layer connects drones for specific tasks such as blockchain mining. On the other hand, the resource layer involves setting up a blockchain and allocating resources. A service provider at the network edge sets up a management layer to manage resources and make decisions such as sending work to drones to perform computations. Although research on blockchain-assisted UAV communication systems has emerged, several gaps and limitations must be addressed. This Chapter presents a comprehensive review of several aspects, including the potential factors shown in Fig. 2.1. Recent studies have focused on improving the privacy and security of UAV communication networks using blockchain technology. However, more research is needed on combining technologies, such as blockchain, UAVs, FL, and Beyond 5G (B5G) communication. This gap has motivated us to investigate the potential benefits of these technologies when combined.

Table 2.1: Comparisons of Existing Survey Papers 1: 5G-concentrated, 2: Blockchain-concentrated, 3: UAV-concentrated 4: Performance Comparisons with other Technologies.

Ref.	Year	Goals	1	2	3	4
[10]	2019	Presented PHY-layer Security for UAVCommunication Networks	✓	X	✓	X
[11]	2019	Concentrated on UAV Energy Constraints, High Altitude, and 3-D Mobility	✓	X	✓	✓
[9]	2020	Blockchain-envisioned UAVcommunication using 6G Networks	X	✓	✓	X
[12]	2020	Discusses the Blockchain Technology in GPS-enabled Networks	X	✓	✓	✓
[13]	2021	UAV Security and 6G/BC Integration are Explained	✓	✓	✓	X
[15]	2021	Overview of Secure Drone Communication	✓	X	✓	X
[14]	2022	Blockchain-based FL in UAVs Beyond GPS Networks	✓	✓	✓	X
Our Work	2023	Blockchain-Assisted UAVCommunication Systems	✓	✓	✓	✓

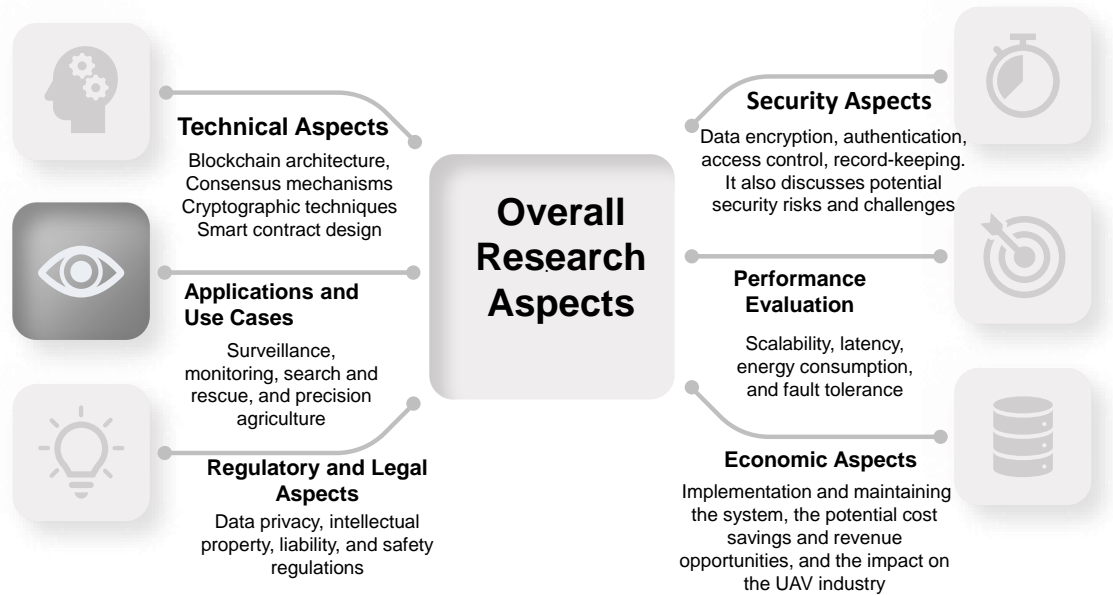


Figure 2.1: Key Aspects and Considerations of Research.

The key contributions of this study are as follows:

1. This chapter provides a comprehensive exploration of the integration of multiple technologies such as UAVs, blockchain, next-generation wireless communication, and FL for future intelligent applications presented in Fig. 2.2.

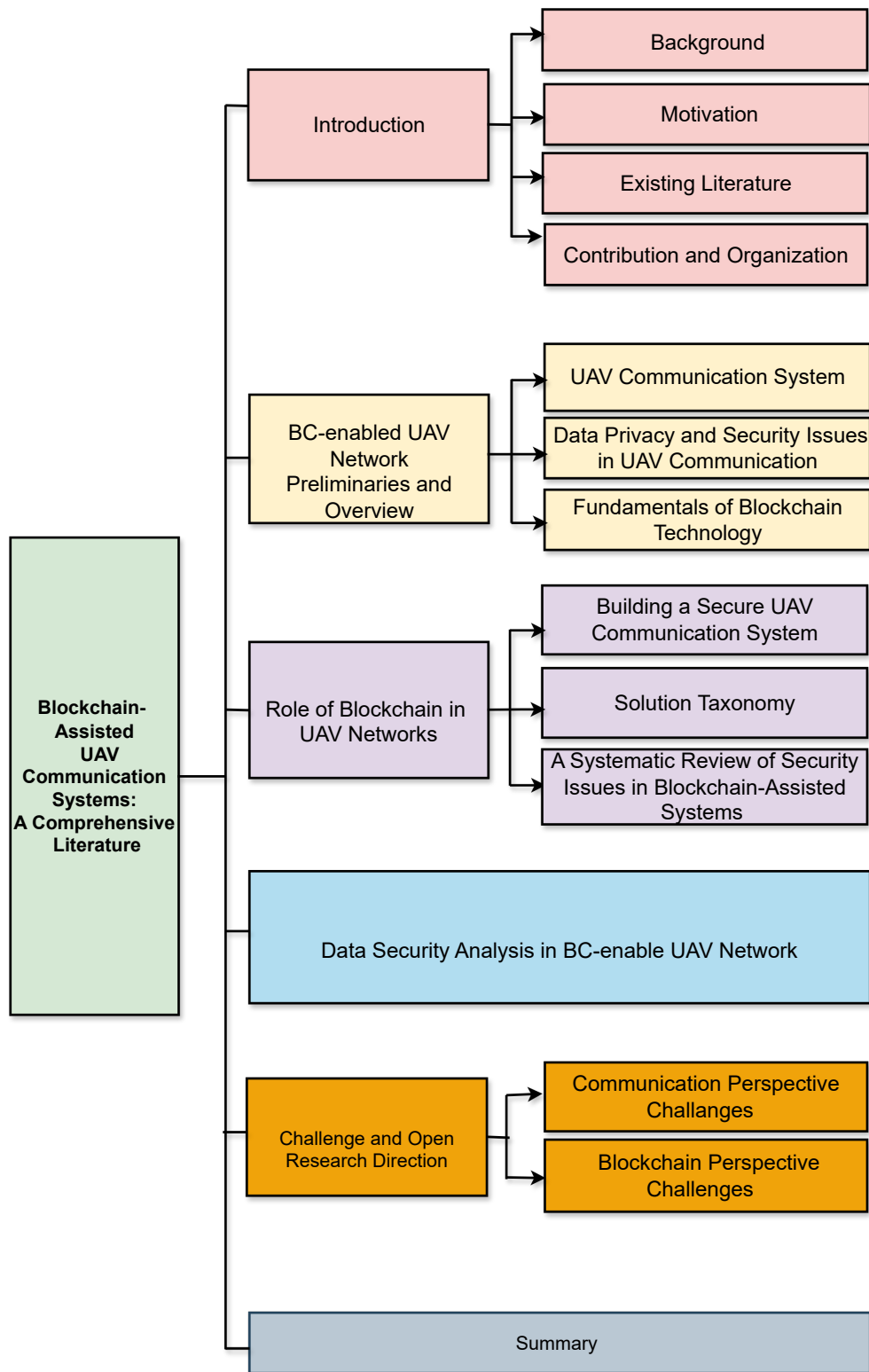


Figure 2.2: An Illustrative Overview of Structure and Reading Map.

2. We also cover the necessary enabling technologies for a reliable UAV network, such as B5G communication for massive connectivity, uRLLC, and higher data rates. In addition, blockchain is used for security and privacy, whereas FL is used for distributed learning

and collaborative intelligence.

3. We thoroughly discuss privacy and security of data in UAV communication, as blockchain technology has the potential to enhance the privacy and security of drone communication by providing a decentralized and tamper-proof system for data storage and transmission.
4. Furthermore, this study covers various aspects and provides a holistic view of the technology, its benefits, and potential challenges of more secure and privacy-aware systems capable of integrating distributed learning.

## **2.1 Blockchain-enabled UAV Networks: Preliminaries and Overview**

This section presents a summary of the blockchain-enabled UAV network and the preliminary information. It briefly discusses the evolution of UAV technology, related applications, conceptual communication frameworks, and challenges that arise. Furthermore, a primer on the fundamentals of blockchain technology is explained.

### **2.1.1 UAV Communication Systems**

The UAV or drones are operated remotely by GCS, also known as ground cockpits, either by human pilots or autonomous systems, such as autopilots, which require no human intervention. Initially, the UAV was designed for military and surveillance applications. However, rapid research and development have significantly reduced the cost of UAV manufacturing. Consequently, UAV technology has been adopted in many commercial and non-military applications, such as intelligent city surveillance, delivery services, agriculture, search and rescue, weather monitoring, filmmaking [16], photography, and innovative healthcare [17]. The communication system is vital to UAV applications because it connects the flying node, GCS, stationary nodes, and the infrastructure. Therefore, the communication capacities of the entire system are Drone-to-Ground Communication (D2G), Drone-to-Drone Communication (D2D), Drone-to-Satellite Communication (D2S), and Drone-to-Cellular Communication (D2C).

- D2G: In D2G communication, the ground station controller monitors the UAV's flight path. Then, on-duty technicians or field staff start flight control, upload the path to the flight control, and set up parameters for automatic takeoff and landing, such as closing speed, lift angle, climb height, and end altitude. D2G communication ensures the smooth operation of the tasks assigned to UAV. Moreover, GCS collects data captured by the UAVs and sends control commands based on the adherence. Therefore, a secure connection between UAV and GCS is required.

- **D2D:** In most existing applications, multi-UAV systems and ad hoc networks are used, where two or more UAVs participate in completing the task. The fundamental design challenge for a multi-UAV system [18] is communication and coordination between multiple devices. UAV serve as Mobile Ad Hoc Networks (MANET) for communication while in flight. Consequently, in an MANET environment, each UAV is considered a mobile node. An Open System Interconnection (OSI) framework is commonly used, including the OSI model's data link, network, transport, and application stages, which include the physical layer security, data link, network transport, and application stages. Communication between each UAV and the ground station limits system capabilities when there are multiple UAVs.
- **D2S:** UAV satellite communication is predominantly used beyond LoS communications. Because of Earth's rotation, standard LoS data links are rendered unusable over long distances. Moreover, drones can fly beyond terrestrial networks including GPS and other cellular services. Instead, a satellite can relay and amplify radio or microwave frequency signals between a vehicle and its BS. In regions without a wireless communication infrastructure, military-based applications use D2S [19]. GPS devices ensure real-time location tracking for drones and facilitate drone communication via satellite links. However, this setup can also be useful in exceptional emergencies such as earthquakes and floods.
- **D2C:** Communication between aircraft, or Aerial-to-Aerial (A2A) communications, occurs during missions involving multiple UAV. In these cases, the UAV works together and coordinates using low-power wireless technologies (such as Bluetooth and Zigbee) to send and receive data either directly or via a series of intermediate nodes [20]. A single UAV operates within a network of UAV, where they all share information and complete the flight mission. However, the throughput and transmission bandwidth of D2D communications are extremely low.

The remainder of this chapter is organized as follows. Section 2.1 presents an overview of preliminary topics, such as blockchain technologies, data security, privacy concerns in communication systems, and UAV communication systems. Section 2.2 explores the role of blockchains in UAV networks, and Section 2.3 analyzes the data privacy and security concerns in blockchain-enabled UAV security solutions. Section 2.4 discusses the challenges and open research directions. Finally, Section 2.5 provides concluding remarks.

Table 2.2: Summary of Privacy and Security Attacks in Blockchain-Enabled UAV Networks

<b>Attack Level</b>	<b>Attack Type</b>	<b>Description</b>	<b>Ref.</b>
<b>Communication-Level Attacks</b>			
Physical & MAC Layer	Zero-day Attacks	Attacks on commercial Wi-Fi-based UAVs, compromising D2G communication.	[21]
Network Layer	Eavesdropping, DoS, MITM, Replay, Forgery, FANETs Routing, Jamming	Various attacks targeting UAV communication integrity and availability, including eavesdropping, denial of service, and man-in-the-middle attacks.	[22]
Transport Layer	ICMP Flooding, Packet Injection	Attacks exploiting vulnerabilities in MAVLink protocol, compromising data transmission.	[23], [24]
<b>Sensor-Level Attacks</b>			
GPS Data	Jamming	Disruption of GPS signals leading to loss of UAV control.	[25]
Sensor Data	False Data Injection	Injecting false data into UAV sensors, leading to navigation system malfunction.	[26], [24], [27]
<b>Software-Level Attacks</b>			
Software Vulnerabilities	Zero-day, Malicious Software	Exploiting software vulnerabilities in UAV systems, leading to data loss and control issues.	[24], [28]
<b>Hardware-Level Attacks</b>			
Hardware Components	Hijacking, Supply Chain, Battery, RF Module Attacks	Attacks targeting physical components of UAVs, compromising security and operation.	[29]

### 2.1.2 Data Security and Privacy Specifications in UAV Network

UAVs have recently demonstrated their capability to provide cost-effective and credible solutions for various real-world scenarios. UAV offers an immense range of services due to their autonomy, mobility, adaptability, and communication interoperability. Despite the extensive



use of UAV to support ground communications, data exchanges in these networks are susceptible to security threats because most communication occurs through radio or Wi-Fi signals, which are easy to hack. Several techniques exist to protect against cyberattack. The recently emerging blockchain technology is a promising way to enhance data security and user privacy in peer-to-peer UAV networks. Utilizing the advantages of blockchain, multiple entities can communicate securely, decentralize, and equitably. This chapter comprehensively overviews the privacy and security integration in blockchain-assisted UAV communication. To achieve this goal, we present a set of fundamental analyses and critical requirements that can help build privacy and security models for blockchains and aid in managing and supporting decentralized data storage systems. The security requirements and objectives of the UAV communication system, including availability, authentication, authorization, confidentiality, integrity, privacy, and non-repudiation, were thoroughly examined to provide deeper insights, as presented in Table 2.2. We conclude with a discussion of the open research challenges, constraints of current UAV standards, and potential future research directions. Internet-connected UAVs are prone to cyberattacks, posing profound uncertainty to the security and privacy of their users. Such attacks fall into five broad categories: confidentiality, integrity, availability, authenticity and privacy. Fig. 2.3 presents the percentage of attacks compiled in recent surveys [30]. The following section describes the specifications of each intrusion. The risk of passive and active attacks is heightened by the lack of security measures for UAVs operating in the national airspace. In this study, we categorized the potential vulnerabilities of UAVs into four groups: sensor, hardware, software, and communication. In Fig. 2.4, we provide a detailed breakdown of the threats and vulnerabilities that UAVs face based on their functional level. We then review various attacks and their corresponding countermeasures currently available in the literature.<sup>1 2</sup>

1. **Communication-level Attacks:** UAV flight control and data transmission require effective communication protocols. Typically, the UAV communicates wirelessly with the GCS. This section examines the vulnerabilities, threats, and attacks that can compromise the confidentiality, integrity, authenticity, and accessibility of UAV communications. Communication-level vulnerabilities and threats can be categorized based on the following communication layers.

2. **Physical & MAC Layer Vulnerabilities and Attacks:**

The security of UAV communication networks is compromised owing to vulnerabilities in different layers of the communication protocol. In this regard, physical and Medium Access Control (MAC) layer vulnerabilities and attacks have been identified in the complex D2G wireless communication network. A recent study [31] reported three zero-day

---

<sup>1</sup>Active attacks: Malicious actions that directly attempt to alter system resources or affect their operation, often involve modification of data or system behavior.

<sup>2</sup>Passive attacks: Attempts to gain unauthorized access to information without altering system resources, typically involving eavesdropping or monitoring of network traffic.

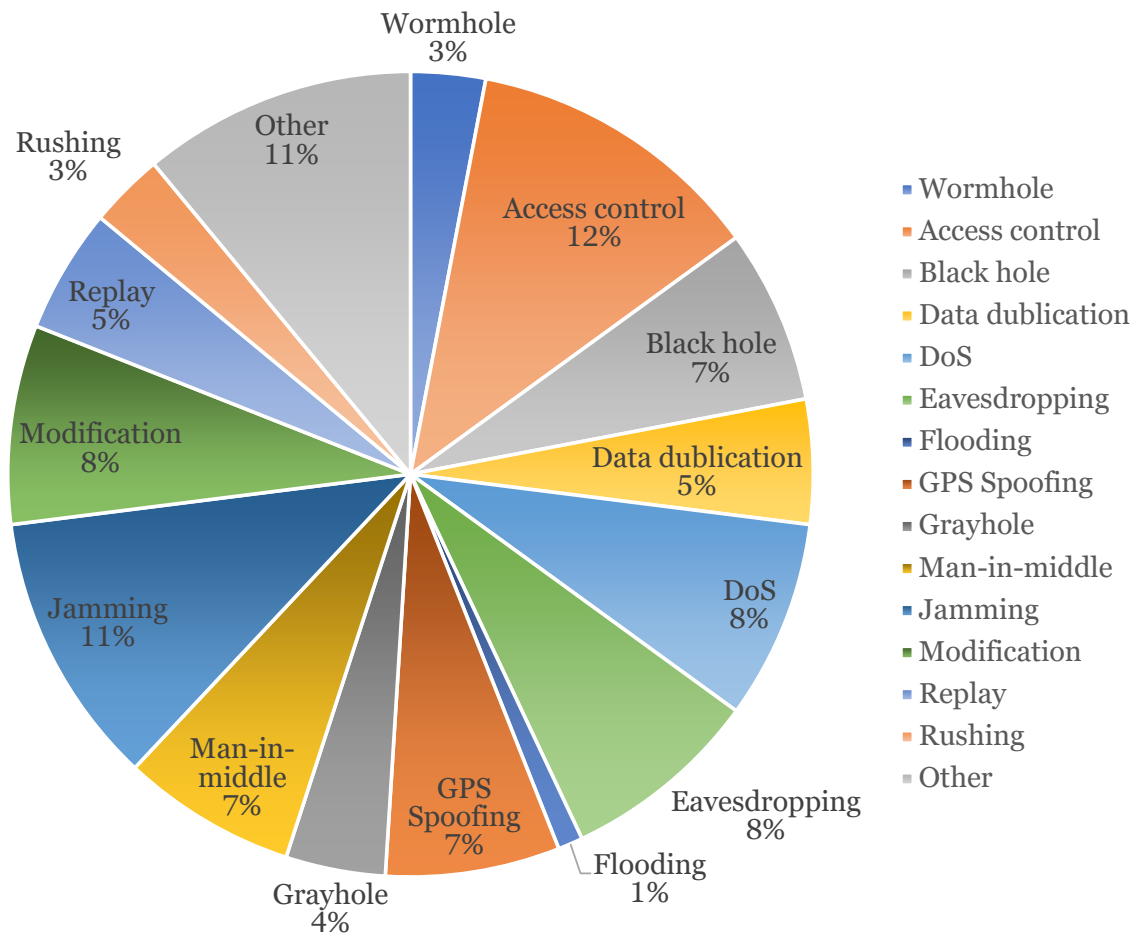


Figure 2.3: Percentage of Different Attacks on UAV Network [1].

attacks on commercial WI-Fi-based UAVs, including the Parrot Bebop UAV.

### 3. Network Layer Vulnerabilities and Attacks:

In addition, the ad hoc mode of UAV networks, known as Flying Ad-Hoc Network (FANET), poses serious threats owing to its dynamic topology. A previous study [32] highlighted the security risks of a UAV public safety network. UAV routing protocols are particularly vulnerable due to the limited resources and lack of wireless encryption in these networks, as discussed in [11].

### 4. Eavesdropping Attacks:

Sniffing or snooping attacks are a form of eavesdropping on confidentiality, integrity, authenticity, and availability of communication to access information. This phenomenon is known as information theft. When the UAV sends or receives data, these attacks are typically undetectable.

### 5. Denial of Service (DoS) Attacks:

In Denial-of-Service (DoS) attacks, the communication protocol layers and services are

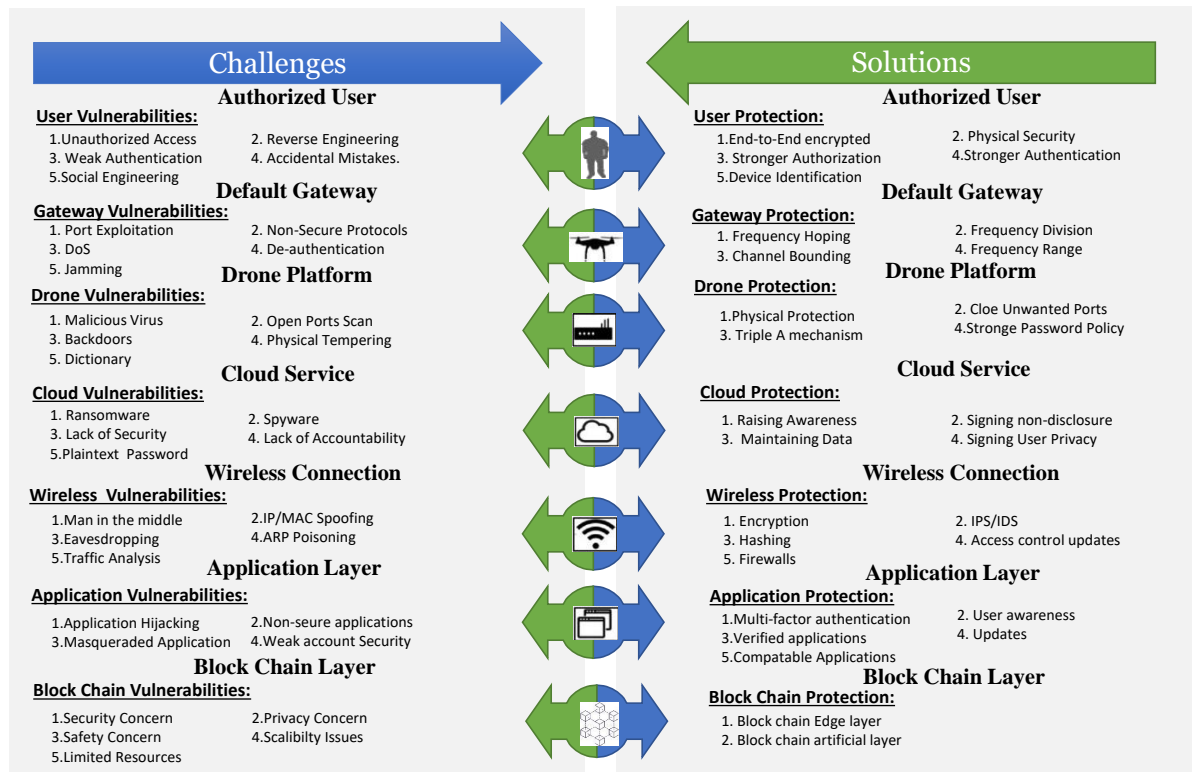


Figure 2.4: Exploitable Security Gaps and Solutions.

targeted, resulting in degradation of the system performance. Techniques to deal with DoS attacks include network firewalls and intrusion-detection systems.

#### 6. Man-in-the-Middle (MITM) Attacks:

Man-in-the-Middle (MITM) attacks involve interfering with user-to-UAV communication. The attacker has complete control over the interaction, misleading both the user and the UAV into believing that they are communicating with each other.

#### 7. Replay Attacks:

Eavesdropping is a potential attack in UAV networks, where an adversary intercepts and replays legitimate data with UAV. Without replay protection, an UAV may be unable to distinguish between genuine and malicious requests.

#### 8. Forgery Attacks:

An adversary can compromise UAV by sending spoof requests, disrupting D2G communication, and creating malicious requests that appear legitimate.

#### 9. FANETs Routing Attacks:

MANET routing protocols are vulnerable to attacks such as blackhole, sleep deprivation, sybil attacks, and wormhole attacks. These attacks target the routing functionality in FANETs, thereby affecting the path discovery, route maintenance, and data forwarding.

#### 10. Jamming Attacks:

UAV networks built with epidemic routing are vulnerable to jamming attacks, which can cause UAV to enter autopilot flight mode and lose contact with the control station. Attackers use jamming to gain control of the UAV and manipulate GPS signals.

#### 11. Transport Layer Vulnerabilities and Attacks:

UAV communication protocols such as MAVLink are vulnerable to attacks like Internet Control Message Protocol (ICMP) flooding and packet injection. Implementing secure transport layer protocols is critical for protecting UAV communication.

#### 12. Sensor-level Attacks:

Attacks at the sensor level include GPS data jamming, false sensor data injection, and sensor-channel attacks.

### 2.1.3 Fundamentals of Blockchain Technology

Blockchain technology is a decentralized and distributed ledger that enables the secure and transparent tracking of transactions for both physical and intangible assets, such as vehicles and intellectual property. It consists of core components such as distributed ledgers, immutable records, and SC, which ensure data security and eliminate the need for third-party involvement. Additionally, the decentralized nature of blockchain technology promotes democratization and allows any node to participate in decision making. The fundamentals of blockchain technology include six distinct zones: Transmission Control Protocol/Internet Protocol (TCP/IP), [33], cryptographic algorithms [34], execution, transactions, and SC. The simplest architecture of blockchain technology consists of digital signatures, hash functions, and applications with cryptographic hashing and digital signatures used for data security.

- **Hash Functions:** The cryptographic hashing process generates a unique fixed-length digital fingerprint or hash value from an input of any length. These hash functions are designed to be collision-resistant (different inputs produce different hashes), hiding the original input (concealing property), and efficient in solving cryptographic puzzles. The National Security Agency (NSA) developed popular hash algorithms like Secure Hash Algorithms (SHA)-256, SHA-512, and message digest algorithms (MD2, MD3, MD6) exhibiting these properties, making them suitable for various cryptographic applications [35].
- **A Digitized Ledger:** Satoshi Nakamoto introduced a digitized ledger system in 2008 [36]. This system facilitates the replication of transactions between computers, and is linked to prevent record tampering. An immutable record-keeping system eliminates the need for third parties. Chaining together the hashes of previous blocks creates a chain of blocks.

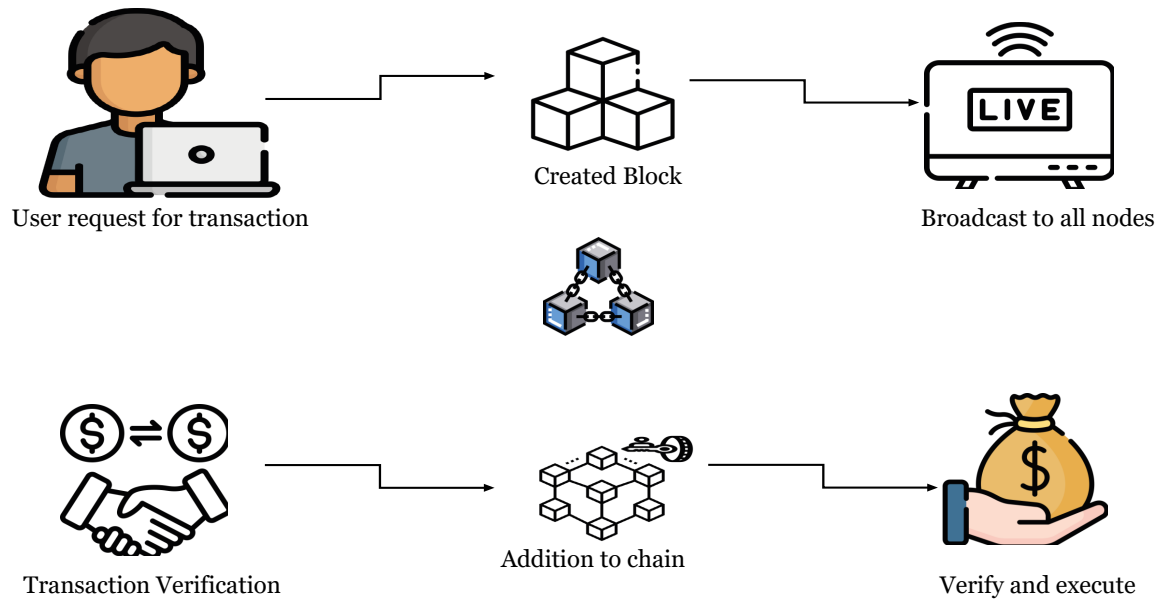


Figure 2.5: Simplified Operation of Blockchain Technology.

A single block stores nonces, previous block hashes, Merkle roots of timestamps, block numbers and hashes. Private blockchains fall into two categories: public [37] and consortia. Fig. 2.5 illustrates a simplified model of how a blockchain system operates. Integrating drone and blockchain technologies is a practical possibility, with both technologies being investigated and refined simultaneously across many industrial applications. The blockchain technology for drones has the potential to increase operational effectiveness and circumvent many of the current potential barriers to drone attacks, as outlined in this chapter.

- **Digital Signatures:** Similar to hash functions, digital signatures are underlying cryptographic building blocks. As with a digital signature, the key difference is that unlike a traditional signature, this signature cannot be copied and pasted from one manuscript to another. Instead, they must be signed only once, and interpreted by a third party.
- **Decentralization:** The decentralized nature of blockchains is a distinct advantage leveraged in blockchain-related applications. In [38], the authors proposed a blockchain-based key management scheme for heterogeneous FANET, in which all drones collectively maintain public key information through the blockchain in a decentralized and distributed manner without any participation from a third party, thus avoiding a SPoF. If each drone stores the details of the flight paths of other drones in the blockchain, the effects of jamming attacks can be reduced, because collisions can be avoided.
- **Asymmetric-Key Cryptography:** The Elliptic Curve Digital Signature Algorithm (ECDSA) [39] garners and affirms digital signatures to use public-private key pairs. Specific domain

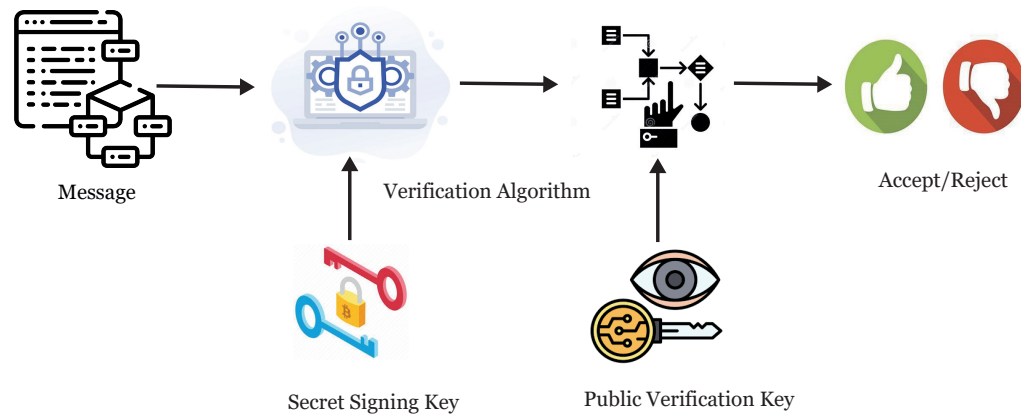


Figure 2.6: Asymmetric Key Cryptography Secure Blockchain Transactions.

parameters specified for a particular period were validated. The measures of advertised blockchain transactions are shown in Fig. 2.6.

- **Consensus Mechanisms:** The next block of acknowledgement is one of the most important aspects of blockchain technology. This problem could be addressed by incorporating a consensus model. The different blockchain consensus mechanisms and their operations are shown in Fig. 2.7. The basic structure of a blockchain network must acknowledge that it should start with a public-genesis block, making it the only preconfigured block. This is required for participation, and the primary objective of the consensus mechanism is to produce an acceptable outcome, such as preventing double spending, aligning economic incentives, and objecting to fair, equitable, and fault tolerances [40]. Consensus algorithms are used in blockchain networks to facilitate agreement among numerous distributed nodes. Blockchain is crucial as it maintains a distributed ledger that records all module activities and supplies necessary information for in-depth analysis using Artificial Intelligence (AI). Additionally, adversaries can exploit SC codes that incorporate AI to discover potential contract limitations. However, this risk can be minimized by employing AI to enhance the adaptability and intelligence of SC. Furthermore, SC and consumption optimization can reduce transaction authentication times by half, making them more sustainable and accessible to additional participants. Moreover, benefits include superior energy efficiency, increased reliability, and quicker decision-making.

## 2.2 Role of Blockchain in UAV Networks

The use of blockchain technology in UAV networks can significantly enhance data security and privacy by providing immutability, decentralization, encryption, SC, and auditability. The technology seamlessly integrates to store decentralized data, while ensuring data integrity, immutability, and transparency.

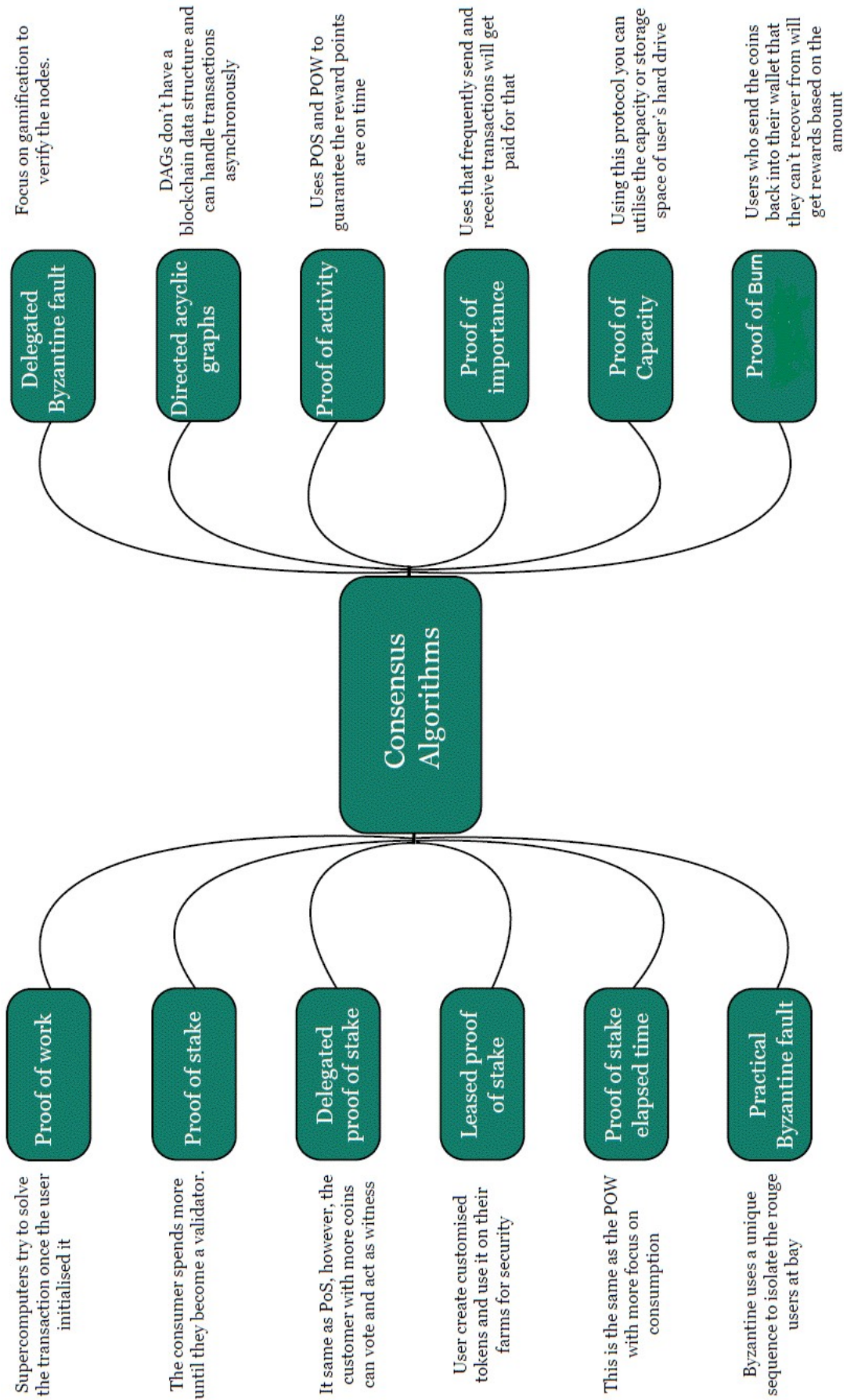


Figure 2.7: Different Blockchain Consensus Mechanisms.

Table 2.3: Comparison Among Consensus Algorithms. Acronyms: PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Proof of Stake), PoC (Proof of Capacity), PoB (Proof of Burn), PoI (Proof of Importance), PoA (Proof of Activity), DAG (Directed Acyclic Graph), DBFT (Delegated Byzantine Fault Tolerance), SBFT (Simplified Byzantine Fault Tolerance), PBFT (Practical Byzantine Fault Tolerance), PoET (Proof of Elapsed Time), LPoS (Leased Proof of Stake).

<b>Algos</b>	<b>Blockchain Platform</b>	<b>Markup language</b>	<b>Pro and Cons</b>	<b>Years</b>
PoW	Bitcoin	C++	Capable of supporting a network worth hundreds of billions of dollars / Energy-intensive	2009
PoS	NXT	Java	Efficient, Lower barrier to entry, Accessibility Limitations, The 50 Percent Attack	2013
DPoS	Lisk	JavaScript	More scalable, energy-efficient, Decentralization / Low participation	2016
PoC	Burstcoin	Java	Cheap, Efficient, Distributed / Favoring bigger participants and decentralization issues	2014
PoB	Slimcoin	C++, Python, Shell	Preservation of the network / Need special equipment, not suitable for public data	2014
PoI	NEM	C++, XEM, Java	Democratic and Network resilience	2015
PoA	Decred	Go	Fairness, investment, verification / Not suitable for public data networks	2016
DAG	IOTA	Rust, Java, Go	Infinite transactions per second / Special equipment needed	2015
DBFT	NEO	Python, .NET, C++, Go, REST	No energy expenditure required; no forks on the NEO blockchain / Delegates need to operate	2016
SBFT	Chain	Java, Node, Ruby	Energy-efficiency, Transaction finality, Low reward variance / Sybil attacks, Scaling	2014
PBFT	Hyperledger Fabric	JavaScript, REST, Go	Transaction finality, Low reward variance / Exponentially increasing message count	2015
PoET	Sawtooth	Java, JavaScript, REST, Go, C++	More efficient and cheap / Low participation	2018
LPoS	Waves	Scala	Fair usage, lease coins / Not suitable for public network, Decentralization issues	2016

However, a central server is sometimes required to ensure the smooth operation of the blockchain framework. The decentralization of private and Federated Blockchain (FedBlock) is partial. Compared with other centralized platforms, blockchain offers improved security.



Cryptography is also required to protect the sensitive data in ledger systems. Cryptography is a complex process that encrypts data as a barrier to malicious cyberattacks [41]. Security is one of the most appealing use cases of blockchain for UAVs. Although highly centralized blockchains are inconvenient, UAV can gather data from numerous sources. The technology can identify fraudulent offers and automated systems reject requests, providing an effective method for thwarting cyber-attacks. Furthermore, because of the audibility of centralized Domain Name System (DNS), there must be a key entry point because of various centralizations.

In addition, blockchain works best for organizations to stop DDoS attacks concealed by fake hardware. No viruses can enter the network owing to hardware provenance on blockchain-based devices. A comprehensive review of blockchain-assisted UAV communication systems covers the following aspects:

- Confidentiality

This entails preventing unauthorized users from accessing data. Similar to other network systems, UAV networks are vulnerable to confidentiality attacks such as data theft, sniffing, eavesdropping, and replay. Several scenarios have been proposed in which a low-cost tamper-proof blockchain-based system can protect the privacy of UAV networks [42].

The Federal Aviation Administration (FAA) regulations use an Identity (ID) management system [43] for drones to authenticate and authorize users. Furthermore, they leverage Delta Drone International Limited (DLT)'s ability to keep information about the drone's flight paths confidential. The authors explained that the blockchain employs asymmetric encryption and homomorphic obfuscation to enhance network confidentiality. In contrast, [44] utilized a blockchain to preserve the confidentiality of cached content by revealing only the essential vehicle information for specific vehicles. A distributed crowd-monitoring system supported by drone swarms aims to ensure that surveillance data are kept up-to-date, secure, and confidential.

- Integrity

A study by [45] demonstrated the integrity of data while reducing the overall volume of direct requests made to Multi-Access Edge Computing (MEC) servers. By contrast, a blockchain enhances the performance and accuracy of the data shared between drones in an Internet-of-Drones (IoD) environment. Their technology selects miners to swarm UAVs for intelligent plant protection. They utilize DLT to secure data, and ensuring the availability of services for UAV in the airspace is a significant concern. As a decentralized system, a robust blockchain network must resist attack by malicious entities.

- Non-repudiation

Non-repudiation is another critical criterion for UAV network cybersecurity. This term refers to the inability to deny or avoid responsibility for one's actions using critical public

infrastructure, such as when a UAV signs messages before sending them over the internet. Non-repudiation is required for UAV networks. This suggests that a UAV may refuse to provide photographs of illegal content.

In conclusion, an UAV system protects the required IoD infrastructure, and a study by [46] argues for four blockchain-based concepts to improve drone security. These aspects – digital fingerprints, data structure, consensus process, and access control – underpin consensus methods and aid in preventing security breaches by empowering network nodes to validate transactions.

- Availability

All blockchain-based solutions proposed for UAV Unmanned Aircraft System Traffic Management (UTM) [47] architectures are fundamentally similar, in terms of a SPoF. However, they are decentralized and require little or no centralized authority. For example, [48] presented a zone-based decentralized system for registering and validating drones.

They designated a reliable ground-based source within a predetermined boundary as an authority. They maintain their availability by allowing neighbours to participate in the authentication scheme. Drone controllers are used for the failed controllers at UTM. In this context, the authors of [49] explain the existence of blockchain architecture.

Their architecture eliminates the latency between nodes by securing communication. This presents an advantage for sensitive applications in decentralized systems. In addition, SC with transparency and immutability support this model. Thus, this task is accomplished by using a decentralized method that is resistant to attacks on Ethereum and Interplanetary File System (IPFS).

- Authenticity

Finally, UAV networks must ensure the legitimacy of the users and messages, authentication is the ability to verify a user's identity. Authentication issues in UAV networks include attacks, such as spoofing. The UAV network includes cryptographic data for authentication and privacy [50]. However, this placement improved the overall spectral efficiency of the network. A straightforward blockchain paradigm is secure and allows for anonymity and work authorization [51].

They reject an adversary's request for surveillance UAV, an attack model that permits alteration of a blockchain before verifying it. Users reject both handoff and traceable attacks. Applying a unique blockchain architecture adds a delay each time a UAV moves between GCS.

### 2.2.1 Comparison of Consensus Algorithms and Blockchain Interaction

Table 2.3 compares the consensus algorithms and how the blockchain interacts with other technologies. Cyberattacks are less likely to occur in a UAV network after integrating the blockchain. This resulted in a fork that was resolved by the creation of the longest chain. Table 2.4 describes cybersecurity-related problems in UAV networks. The longest chain is constructed to prevent further forking. For example, [52] used blockchain technology to protect data through cryptography. Therefore, the data were verified and encrypted to prevent unauthorized modifications.

### 2.2.2 Solution Taxonomy: Challenges and Constraints in Networks

Owing to the unique characteristics of the network, such as fluid topology, node mobility, and intermittent links, it faces unique communication challenges compared with other wireless networks. Therefore, we categorized them into three categories

- **Security Constraint**

Some drones lack encryption on their onboard chips owing to cost or energy consumption considerations, leaving them vulnerable to attackers. This poses a threat to privacy because attackers can easily access communication content. Additionally, according to [53], drones without encryption can be easily hijacked, which is dangerous because it can lead to loss of control and severe damage. Encryption and authentication are crucial for network communication. Without authentication, security threats, such as tampering, replay attacks, spoofing, and impersonation, can occur. For example, in the logistics industry, an attacker can impersonate a valid drone in the network and tamper with address information, resulting in cargo being sent to the wrong destination, causing property damage to the company and customers.

Availability is also a significant concern, with DoS attacks being a common method that damages the availability. During a DoS attack, the entire network can fail if the attacker targets GCS, which would be even worse.

- **Power Constraint**

The energy sources for drones in networks are more constrained than those for vehicles in Vehicular Ad-hoc Networks (VANET) or mobile phones in MANET. Moreover, the battery life of drones may need to be extended, even for routine tasks, to bolster the security of human-to-human communication. Consequently, schemes designed for networks must be compact and have a low power consumption.

- **Scalability Constraint**

Drones in a network constitute a dynamic 3D topology, in which the number of nodes, their positions, and their speeds constantly change. Consequently, links may form and

disappear sporadically and the network may frequently partition, resulting in unstable communication. Airborne jamming attacks can exacerbate this situation. These communication stability issues may lead to drone collisions and task failures in self-organized networks, which rely on cooperation to maintain performance.

### **2.2.3 A Systematic Review of Security Issues in Blockchain-Assisted Systems**

A review of security issues in UAV-assisted systems was presented in [54], where blockchain technology was employed to mitigate security threats. In a similar survey, the authors investigated blockchain applications in communication such as network security and decentralization. Furthermore, [55] proposed a comprehensive survey of blockchain-based communication systems in the networks. They introduced IPFS for data storage to ensure user privacy and to decrease transaction storage costs. The study by [56] also presented a systematic review of blockchain applications in UAV-assisted networks. This study summarizes how blockchain is used to ensure network security, and divides applications into several innovative categories. Blockchain technology offers a promising solution to data privacy concerns in applications. As a distributed ledger, blockchain securely records and tracks data without any centralized authority [57]. Blockchain technology ensures higher reliability than other centralized systems. Decentralization encrypts data to encode information in ledgers. Cryptography is a complex process that encrypts data as a barrier to malicious cyberattacks [58]. Additionally, this technology can identify fraudulent recommendations via an automated system and deny unauthorized requests. However, with the increasing use of UAV in various intelligent applications, collaborative intelligence, continuous learning, low latency, privacy, and massive connectivity are important. FANET dramatically improves the interoperability of UAVs and innovative solutions by providing a framework for AI to enhance its capabilities. As stated previously, traditional encryption techniques based on cryptography and trust are widely used in UAV; however, this has changed with the advent of enabling technologies such as AI, ML, and FL.

### **2.2.4 Blockchain-assisted UAV Challenges and Deployment Scenarios**

The blockchain-assisted UAV challenges and their deployment scenarios are shown in Fig. 2.8. The safety and privacy of UAV communication data is of paramount importance. Currently, available centralized cloud and fog systems offer some level of security; however, there is only one point of failure. This survey also lists other gaps in the current state-of-the-art solutions proposed by researchers worldwide. Cyber attacks, such as spoofing, eavesdropping, man-in-the-middle, jamming, fabrication, and access control attacks, may compromise centralized solutions. Blockchain, a distributed ledger technology, may be a viable solution for these problems. However, for applications in which confidence assurance is necessary, effective use is essential. The

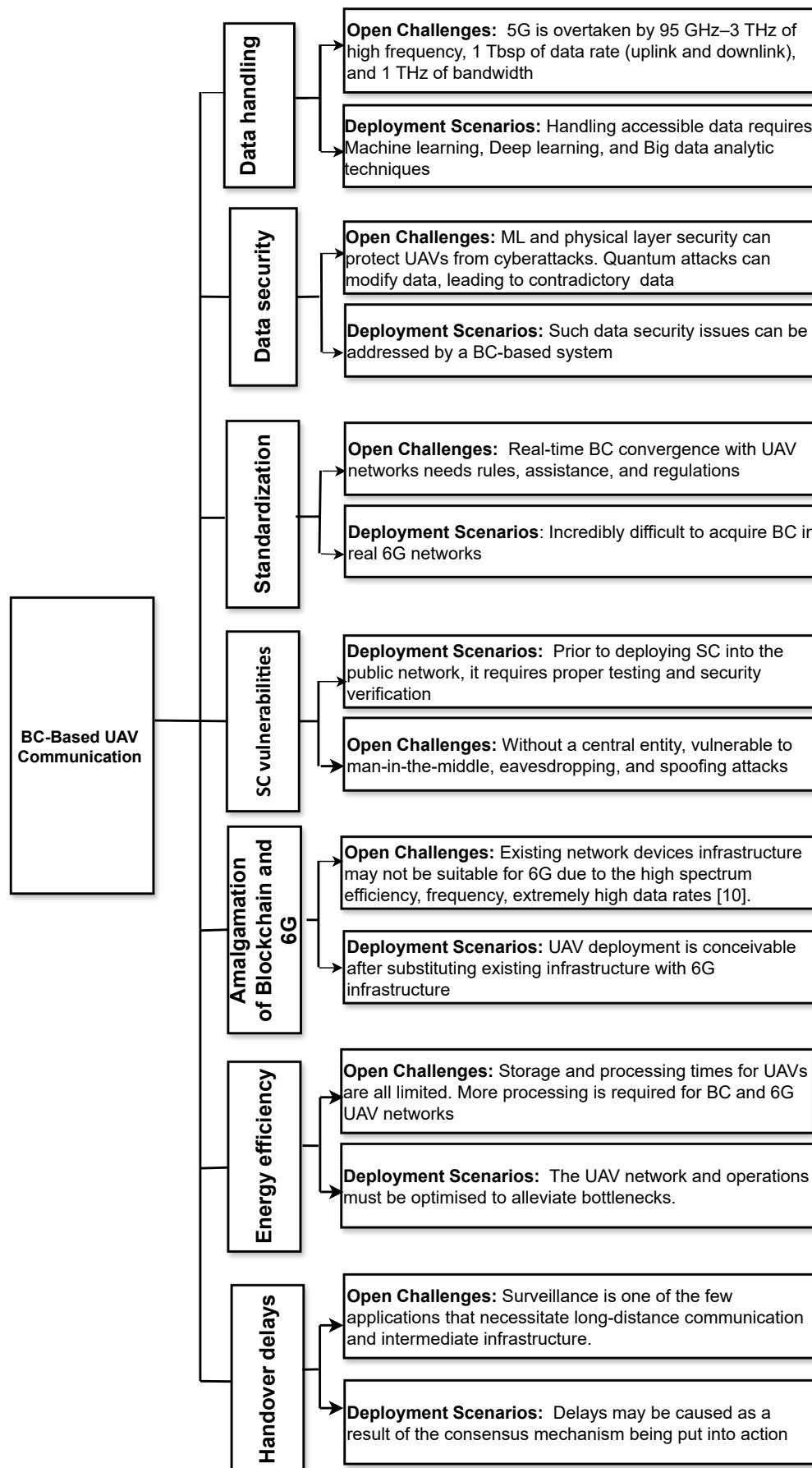


Figure 2.8: Blockchain-assisted UAV Scenario.

hash of the previous block links blocks. A block header contains information such as hashes, headers, prior blocks, Merkle root nonces, and timestamps in its data structure.

- **Blockchain-Assisted FL via UAV Network:** The use of UAV and blockchain technologies is still in its infancy. Owing to the immutable nature of blockchains, UAV-assisted communication provides protection from cyber threats [59]. Fig. 2.9 represents the blockchain layer, data detection, application layer, or UAV application and control environment for blockchain-assisted UAV networks. The benefits of blockchain technology in UAV-assisted FL communication networks include scalability, privacy, security, immutability, transparency, and efficiency [60]. Combining FL and blockchain in UAV-assisted applications provides additional benefits [61]. In light of this, multiple types of research have recently been proposed to exploit the potential of UAV and blockchains in distributed model training. For instance, [62] proposed an FedBlock that records and updates local model parameters via a specific distributed ledger. This approach replaces the centralized FL server used for aggregation, and operates a consensus chain. The study in [63] introduced a blockchain for the spectrum sharing of drones in a wireless network. The proposed architecture uses consortium blockchain technology to develop a secure spectrum-sharing mechanism in a UAV-assisted cellular network. The authors of [62] proposed a novel serverless architecture for FL, enabled by blockchain and UAV technologies. The simulation outcomes affirm the advantages of the blockchain by correlating the end-to-end efficiency of the system in terms of latency and confidentiality.

## 2.3 Data Security Analysis in Blockchain-enabled UAV Network

The use of blockchains in UAV communication can enhance data privacy and security in several ways.

- **Data Encryption:** Blockchain technology can encrypt the data being transmitted between UAVs to prevent unauthorized access or interception of the data.
- **Authentication:** Blockchain can help to verify the authenticity of the UAVs communicating with each other. Using public-key cryptography, each UAV can be assigned a unique digital identity, which can be verified using a blockchain network.
- **Immutable Record Keeping:** Blockchain can maintain an immutable record of all communication between UAVs, ensuring that any tampering or modification of the communication is easily detected.

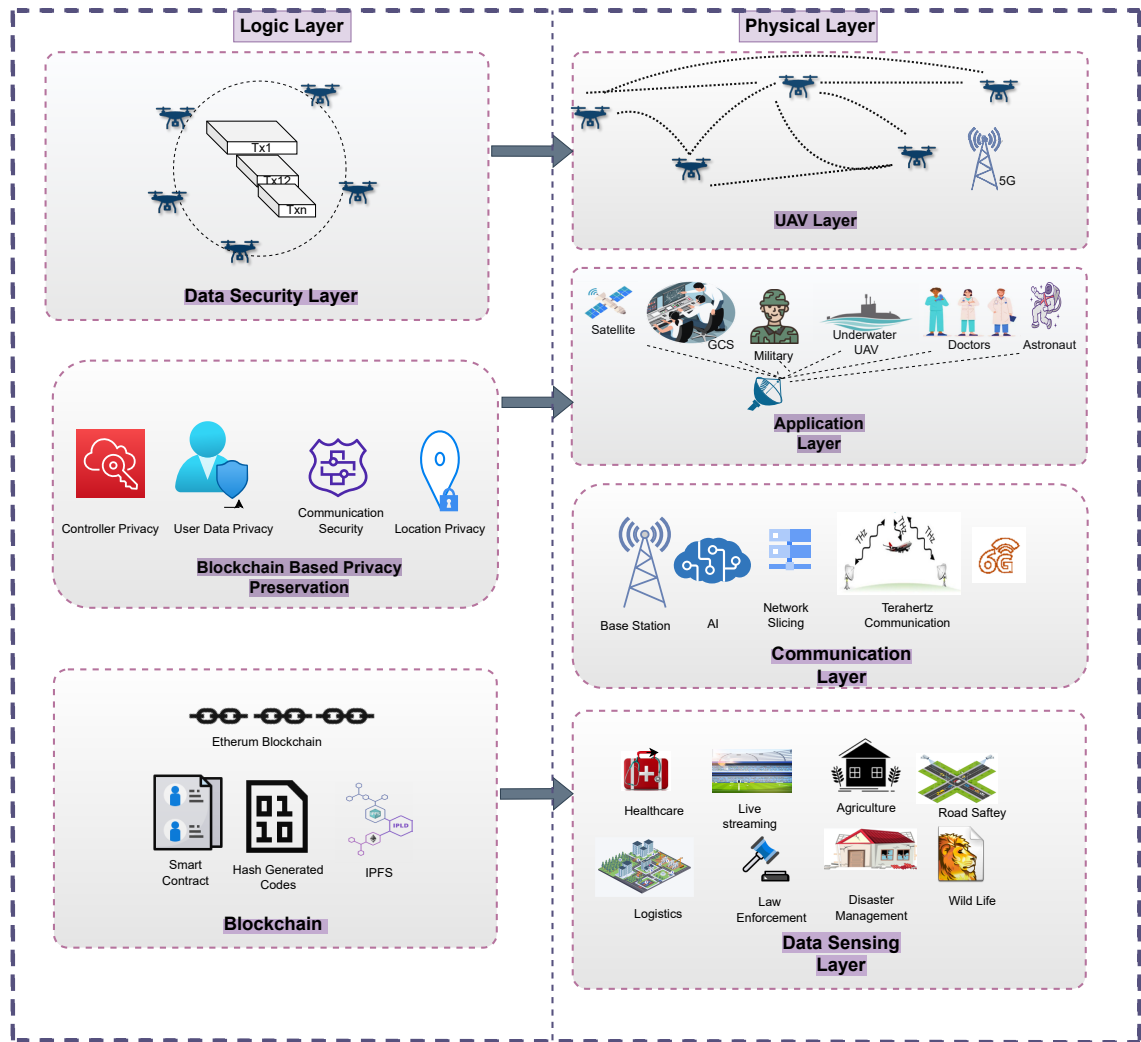


Figure 2.9: Blockchain-enabled UAV Communication.

- **Access Control:** Blockchain can implement access control mechanisms to prevent unauthorized access to UAV communication channels.
- **Smart Contracts:** SC can be used to automate certain security processes and ensure that certain conditions are met before communication is allowed between UAVs.
- **Consensus Mechanisms:** Blockchain can use consensus mechanisms to ensure that all nodes in the network agree on the state of the communication between UAVs.
- **Authentication:** Blockchain can help to verify the authenticity of the UAVs communicating with each other. Using public-key cryptography, each UAV can be assigned a unique digital identity that can be verified using the blockchain network.
- **Immutable Record-Keeping :** Blockchain can maintain an immutable record of all communication between UAVs, ensuring that any tampering or modification of the communication is easily detected.
- **Access Control:** Blockchain can implement access control mechanisms to prevent unauthorized access to UAV communication channels.
- **Smart Contracts:** SC can be used to automate certain security processes and ensure that certain conditions are met before communication is allowed between UAVs.
- **Consensus Mechanisms:** Blockchain can use consensus mechanisms to ensure that all nodes in the network agree on the state of the communication between UAVs.

Blockchain is transparent, meaning that all participants in the network have access to the same information, making it easier to identify and track any attempt to access or modify the data. In the context of drone communication, blockchain can provide data security by creating a tamper-proof ledger of all data and transactions exchanged between drones and GCS. These include flight data, sensor readings, and other critical mission data. Using blockchain, data are secured and cannot be modified or deleted, thereby ensuring that they remain accurate and trustworthy. Additionally, the decentralized nature of blockchain makes it more difficult for hackers or malicious actors to interfere with communication between drones and GCS. Moreover, blockchain employs cryptographic techniques to secure data. For example, data are encrypted and stored in blocks, and each block is linked to the previous block using a cryptographic hash function, thereby creating an immutable and tamper-proof chain.

Furthermore, the blockchain can provide secure authentication and identity management for UAVs. Each UAV has a unique digital identity, and the blockchain can be used to verify the identity of each UAV and to ensure that only an authorized UAV can access the network. Although numerous initiatives have been undertaken to realize a blockchain-based communication network, the dynamic network characteristics and real-time data processing requirements of



an Vehicle-to-Everything (V2X) communication scenario render the straightforward adoption of the existing blockchain technology inappropriate. Although blockchain has great potential for improving security and network management, it also has considerable latency. This implies that new blockchain algorithms with exceptionally low latencies must be developed before they can be used in 6G–V2X. However, the limited throughput and scalability of the current blockchain technology are also significant open issues that require extensive investigation. For example, the use of public blockchains can expose sensitive data to the public, and the integration of UAV into blockchain networks can introduce new vulnerabilities such as rogue devices and DoS attacks. Therefore, further research is required to address these concerns and develop effective solutions to ensure the privacy and security of data in blockchain-enabled UAV communications. Blockchain-based UAV in communication can help with supply chain management [64], disaster response [65], relief operations, product delivery [66], aerial photography [9], and surveillance [57]. According to surveys, blockchain technology has been developed as a security solution for UAV communications, and outlined research challenges on blockchain-enabled UAV network security. This section discusses the functionalities and constraints of blockchain-enabled UAV communication, and provides a comparative data security analysis.

In contemporary computing systems, decentralization of DNS using blockchain technology has emerged as a promising alternative for mitigating software attacks. Distributing content across multiple sites and enabling users to regulate the space between them, blockchain-based DNS [66] is impractical for malevolent actors to launch software attacks. Additionally, this approach confers legal ownership of associated assets to authorized users, thereby preventing unauthorized access or alterations. Consequently, to ensure data privacy and security, the risk of the unauthorized manipulation of information is minimized. A hierarchical intrusion detection and reaction scheme to enhance the security of UAV networks against debilitating cyberattacks, such as false information diffusion, GPS spoofing, jamming, and black- and gray-hole attacks [67]. The security of blockchain technology is heavily dependent on the cost required to breach the system and alter newly generated data, which is essential for maintaining the integrity of blockchain-enabled UAV between the security of blockchain products. Therefore, brand identity is crucial, particularly in situations in which a single miner (or pool) holds the majority of computational power, leading to a 51% attack on the current blockchain history. Such an attack may result in undesirable consequences such as the manipulation of transactions, double spending, and other forms of cyberattacks. This is because the dominant miner gains more power in the administration process and generates more results in work verification than any other miner in a blockchain network [68].

Table 2.4: Cybersecurity-related Requirement in UAV Networks

Ref	Application	Goals	Pros	Cons
[69]	Confidentiality	ID management system according to FAA requirements	Verify and authenticate drone operations using blockchain	Drones are vulnerable to 51% of attacks, requiring storage and computational resources
[70]		Safeguard confidentiality of cash content	No increase in cache hit rate, robustness	Considerable transmission overhead
[71]		Safe and privacy-respecting crowd surveillance technology	PKI-based security protocol for UAVs	Significant time and computational costs
[72]		Maintain anonymity of UAV networks	PKI and OTP to secure communication channels	Time and computational cost burdens
[73]		Maintain UAV's confidentiality	Low computational costs for encryption/decryption	Intensive cryptography algorithms
[74]	Integrity	Data integrity checked before transfer to MEC servers	MEC servers store data on blockchain	Lacks scalability and UAV movement considerations
[75]		Verify data integrity between drones	Simulation and time analysis of systems	UAV network not explicitly considered
[76]		Secure power plants, detect touch bans	User validation and transaction tracking	No clear consensus method
[77]	Non-repudiation	Prevent dishonesty in UAV network	Highlights UAV security enhancements	No tactical solution or implementation discussion
[43]		Improve UAV non-reputability	Secure infrastructure with energy-efficient blockchain system	Proof-of-work reduces system efficiency
[78]	Availability	Increased node-to-node communication security	UTM architecture fixes system latency issues	No implementation results, scalability untested
[79]		UAV maintenance and authentication	Replaces faulty units to maintain availability	Overhead from responsible parties
[80]	Authenticity	Prevent identity attacks	Network organization relies on blockchain-based software	High data processing efficiency challenges
[81]		Administration and authentication system for drones	Secure drone transportation assistance	Scalability not addressed

## **2.4 Challenges and Open Research Directions in UAV Communications**

The integration of UAV into future communication networks presents multifaceted challenges and opportunities. This section highlights critical issues and potential research directions in UAV communications from a holistic perspective, encompassing aspects such as confidentiality, latency constraints, data integrity, obstruction detection, communication delays, and integration of UAV traffic management devices.

### **2.4.1 Confidentiality and Data Security**

Maintaining confidentiality and ensuring data security are paramount concerns when integrating UAV into communication networks [82]. Sensitive information transmitted between UAV and ground stations must be protected from unauthorized access and potential cyber threats. This challenge requires the development of robust encryption mechanisms and strict access control policies to safeguard the confidentiality of mission-critical data.

### **2.4.2 Variable Latency Constraints**

UAV operations are subject to stringent latency constraints, necessitating the development of sophisticated algorithms and communication protocols [83]. These protocols must account for variable latency conditions while ensuring the safe and efficient operation of UAVs. Remote and Real-Time Control (RRC), high-precision positioning, and seamless coverage are critical requirements that must be addressed to enable reliable UAV communication systems.

### **2.4.3 Data Integrity and Bogus Parameter Updates**

Ensuring data integrity is crucial for maintaining the reliability and trustworthiness of UAV operations [84]. Bogus parameter updates, whether intentional or unintentional, can compromise the safety of UAV flights and potentially lead to catastrophic consequences. Robust mechanisms for validating the data integrity and detecting anomalies in parameter updates are essential for mitigating these risks.

### **2.4.4 Obstruction Detection and Communication Delays**

UAVs operating in urban environments face challenges related to obstruction detection and communication delays [85]. Obstacles, such as buildings and infrastructure, can disrupt LoS communication links, leading to intermittent connectivity and potential safety hazards. Furthermore, communication delays can result in miscommunication and coordination errors between

the UAV and traffic-management devices, necessitating the development of delay-tolerant communication protocols.

### 2.4.5 Integration of UAV Traffic Management Devices

The integration of UAV traffic management devices into communication networks presents challenges and opportunities. Encouraging the participation of these devices in mining processes can improve the accuracy and reliability of traffic management data, and enhance the safety and efficiency of UAV delivery services [82]. However, addressing concerns related to security, integrity, and privacy is crucial to ensuring the trustworthiness of these devices and the data they generate. Overall, blockchain-assisted UAV communication offers several benefits, but also

Table 2.5: Comparison of Communication Perspective Challenges vs. Blockchain Perspective Challenges in UAV Networks

<b>Communication Perspective Challenges</b>	<b>Blockchain Perspective Challenges</b>
<b>Aerial Nature of UAVs:</b> Challenges in cellular communication due to weaker signal strength and frequent base station switching.	<b>Private Key Management:</b> Difficulties in securing blockchain networks owing to the dynamic nature of UAV networks.
<b>Security Scrutiny:</b> Increased use by criminal groups and concerns for espionage, surveillance, and public safety.	<b>Malware and Cyber Attacks</b> UAVs vulnerable to attacks that compromise the integrity of the blockchain network.
<b>Safety Concerns:</b> Need for continuous improvement in safety protocols, risk assessment, and incident management.	<b>Network Congestion:</b> A large volume of data leads to transaction processing delays and reduces the network efficiency.
<b>Assessment of Risk of UAVs:</b> Essential to determine acceptable solutions and maintain reliable operations through permission and insurance.	<b>Scalability:</b> Challenges in scalability owing to increasing number of UAVs and data generation.
<b>Challenges in Implementing 5G:</b> Requires examination of structural and technical aspects and clear regulatory frameworks for SC.	<b>Interoperability:</b> Difficulty in sharing data between networks that rely on different blockchain platforms.
<b>Scalability of Drone-chain Networks:</b> Need for novel techniques and standards to manage multiple drones and support 5G communications.	<b>Regulatory Compliance:</b> Challenges in complying with regulatory requirements, especially across different jurisdictions.

presents several security challenges that must be addressed to ensure the security and integrity of the network. Some potential research directions for blockchain-assisted UAV communication are as follows.

- **Scalability:** Developing methods to scale blockchain technology to handle the large amounts of data generated by UAV communication systems.

- **Security:** Exploring new cryptographic techniques and other security mechanisms to enhance the security of UAV communication systems.
- **Privacy:** Investigating ways to ensure the privacy of data transmitted between UAVs, such as using durables or homomorphic encryption.
- **Energy Efficiency:** Developing techniques to reduce the energy consumption of blockchain-based UAV communication systems, such as using more efficient consensus mechanisms or optimizing SC execution.
- **Consensus Mechanisms:** Investigating new consensus mechanisms that can provide better scalability, latency, and energy efficiency for UAV communication systems.
- **Standardization:** Developing standards for blockchain-based UAV communication systems to ensure interoperability and facilitate the adoption of the technology.
- **Integration with other Technologies:** Exploring ways to integrate blockchain technology with other emerging technologies, such as AI, Internet-of-Things (IoT), and edge computing, to create more advanced and efficient UAV communication systems.
- **Real-world Testing:** Conducting real-world testing of blockchain-assisted UAV communication systems to evaluate their effectiveness and identify potential challenges and limitations.

The challenges and open research directions highlighted in Section 2.4 directly inform and motivate the contributions presented in this study. Our comprehensive exploration of integrating UAVs, blockchain, next-generation wireless communication, and FL (contribution 1) addresses the multifaceted challenges of confidentiality, data security, and variable latency constraints. The focus on enabling technologies like B5G communication (contribution 2) directly tackles the issues of massive connectivity and uRLLC. Our thorough discussion of privacy and security in UAV communication using blockchain technology (contribution 3) responds to the critical challenges of data integrity, bogus parameter updates, and the need for robust encryption mechanisms. Finally, our holistic approach to integrating distributed learning with secure and privacy-aware systems (contribution 4) aligns with the open research directions of developing sophisticated algorithms and communication protocols to ensure safe and efficient UAV operations. Addressing these challenges and research directions, our study provides a comprehensive framework for advancing UAV communications in the context of emerging technologies and security requirements.

## 2.5 Summary

This comprehensive study explores the integration of blockchain technology with UAV communication networks to enhance security, privacy, and trust. The authors emphasized the growing importance of UAVs in various applications such as surveillance, mapping, search, and rescue, as well as the associated challenges in ensuring secure and reliable communication. This chapter presents a systematic review of existing blockchain consensus mechanisms, cryptographic techniques, and SC architectures that can be leveraged to address security vulnerabilities and communication challenges faced by UAV networks. These include threats, such as GPS spoofing, jamming, eavesdropping, and DDoS attacks, which can compromise the confidentiality, integrity, and availability of UAV communication. This justifies the inherent properties of blockchains, such as decentralization, immutability, and cryptographic security, which can mitigate these threats and provide a robust framework for secure UAV communication. Specifically, blockchain can enable secure authentication, access control, data encryption, and tamper-proof record-keeping, thereby enhancing the privacy and trustworthiness of UAV networks.

This chapter also explores the potential of integrating blockchain with other emerging technologies such as FL and B5G communication networks. This convergence can facilitate distributed learning, collaborative intelligence, and massive connectivity, enabling a wide range of intelligent applications including healthcare, precision agriculture, and disaster response. However, the authors identified several challenges and open research directions that must be addressed for a successful blockchain-assisted UAV network deployment. These include scalability, latency, energy efficiency and regulatory compliance. In addition, the integration of blockchain with AI, FL, and B5G networks presents challenges related to security, privacy, and interoperability. This chapter highlights the potential of blockchain technology to enhance the security, privacy, and trust of UAV communication networks. Addressing the identified challenges and leveraging synergies with emerging technologies, blockchain-assisted UAV networks can pave the way for secure and reliable UAV operations, enabling a wide range of innovative applications in various domains.

## Chapter 3

# Blockchain-based Efficient and Trusted Authentication

This chapter proposes a blockchain-based efficient authentication scheme called BETA-UAV for secure communication in UAV-assisted networks. This scheme aims to exploit the inherent properties of blockchain technology, such as immutability and transparency, to record communication sessions through transactions using SC. The BETA-UAV scheme comprises of three phases: system initialization, registration, signature generation, and verification. In the system initialization phase, an Trusted Authority (TA) initializes the system parameters and deploys an SC in the blockchain network. In the registration phase, the TA registers all GCS and UAVs by issuing long-term digital certificates.

The signature generation and verification phase facilitates mutual authentication and freshness identification between UAVs to establish a secure communication channel. This phase involves the exchange of signed messages, verification of signatures, and triggering of SC functions to record transactions IDs in the blockchain for subsequent transmission. A security analysis was conducted to evaluate the resistance of the proposed scheme to various active attacks, such as modification, replaying, impersonation, man-in-the-middle attacks, and birthday collisions. They also implemented the BETA-UAV scheme on the Ethereum public blockchain and analyzed its performance in terms of the computational and communication costs.

The results show that the proposed BETA-UAV scheme outperforms the existing traditional and blockchain-based authentication schemes in terms of computational and communication efficiency. We plan to develop that the BETA-UAV scheme is a promising solution for securing UAV communication in UAV-assisted networks. We plan to extend their work by implementing the scheme in practical scenarios and comparing it with other encryption algorithms.<sup>1</sup>

---

<sup>1</sup>Birthday collision attacks specifically refer to cryptographic attacks that exploit the mathematics behind the birthday paradox to find collisions in hash functions more efficiently than brute force methods. In the blockchain and cryptographic systems context, a birthday collision attack attempts to find two different inputs that produce the same hash output, potentially compromising the system's integrity or security.

### 3.1 Introduction

UAV technology significantly enhances the reliability and efficiency of transportation systems, especially in scenarios involving heterogeneous and non-stationary data traffic. However, the sharing of diverse data types introduces considerable security and privacy concerns, presenting challenges for future integration of UAVs in Intelligent Transportation System (ITS) [86]. The increasing importance of connectivity in multi-UAV systems poses unique communication challenges, owing to factors such as high node mobility, dynamic network topology, long distances between nodes leading to intermittent connections, and limited power availability. The extensive adoption of UAV technology has been attributed to its capability for wide-area coverage, exploration, and enhanced intelligence. The rising interest in UAV is evident from their deployment across various global applications, such as aerial photography, agriculture, and film production. Ensuring secure communication channels is vital for dependable UAV operation. The protection of both external communication links (between UAVs and infrastructure) and internal communication within UAVs is crucial. Moreover, it is imperative that UAVs grant access to their resources only to authorized entities, and authenticate all internal modules to maintain device security [87]. Given the autonomous operation of UAVs, robust device-to-device authentication is essential to ensure secure access to GCS.

Blockchain technology can be used to create a distributed system in which entities can enter and verify blocks, thereby ensuring the system integrity. However, because users can request data for flying drones directly from UAVs instead of servers, drones continue to lose or leak data during the transmission. This situation determines the complexity of a scheme. Consequently, the transmitted data may be subjected to extensive computation, thereby increasing the possibility of privacy leakage. Furthermore, revealing privileged information can result in a transmission security breach. Therefore, a lightweight BETA-UAV scheme is proposed for secure UAV communication. The objective is to enable mutual authentication and freshness identification such that the UAV can establish secure communication channels. Proof-of-Freshness (PoF) or authentication protocols allow UAVs to integrate into these systems quickly and securely.

In this study, we propose to accomplish the aforementioned goals by conceiving new strategies by combining Elliptic Curve Cryptosystem (ECC) and a trusted authentication scheme. We present an BETA-UAV blockchain-based efficient and trusted authentication for secure UAV communication that promises that BETA-UAV can resist attacks. The objective is to enable mutual authentication and freshness identification such that the UAV network can establish secure communication channels. PoF or authentication protocols allow UAVs to integrate into these systems with minimal hassle and maximum security.



## Research Objectives

1. Design and develop a secure and efficient blockchain-based authentication scheme BETA-UAV for UAV communication in UAV-assisted networks.
2. Evaluate the performance of the proposed BETA-UAV scheme in terms of computational complexity, communication overhead, and resistance to various security attacks.
3. Implement and deploy the BETA-UAV scheme on a public blockchain platform, such as Ethereum, and analyze its practical feasibility and associated costs.
4. Conduct a comparative analysis of the BETA-UAV scheme with existing traditional and blockchain-based authentication mechanisms in UAV communication, evaluating aspects of security, efficiency, and scalability.
5. Optimize the BETA-UAV scheme for diverse UAV-assisted network scenarios, including urban air mobility, precision agriculture, and disaster management, while accounting for the specific requirements and constraints inherent in each application.

This section presents a novel blockchain-based efficient and trusted authentication scheme for secure UAV communication, called BETA-UAV. The proposed scheme leverages the intrinsic properties of blockchain technology, such as immutability and decentralization, to establish trust and allow secure message exchange among UAV operating in ad hoc networks. The integration of UAV into ITS has garnered significant attention owing to its potential to improve the operational efficiency and reliability. However, the dynamic nature of UAV networks, coupled with untethered wireless communication channels, presents critical security and privacy challenges. Ensuring the authenticity, integrity, and confidentiality of the transmitted data is paramount for the successful adoption of UAV-enabled ITS.

Traditional authentication mechanisms often fail to address the unique requirements of UAV networks, such as limited computational resources, intermittent connectivity, and absence of centralized authority. BETA-UAV addresses these challenges by offloading the authentication process to a blockchain-based SC, thereby reducing the computational burden on UAVs while maintaining a decentralized and trustless environment.

### 3.1.1 Background and Motivation

#### **Importance of UAV Technology in Intelligent Transportation Systems ITS.**

UAVs, also known as drones, have gained significant attention in recent years due to their potential for enhancing operational efficiency and reliability in various domains, including ITS. The integration of UAV into ITS offers numerous advantages such as real-time monitoring of traffic conditions, efficient delivery of goods and services, and rapid response to emergencies.

## Security and Privacy Challenges in UAV Communication

However, the widespread adoption of UAV technology in ITS has been hindered by critical security and privacy challenges. UAV networks operate in dynamic and untethered wireless environments, exposing them to potential threats such as eavesdropping, message tampering, and unauthorized access. Ensuring the authenticity, integrity, and confidentiality of the transmitted data is paramount for the successful deployment of UAV-enabled ITS.

## Limitations of Traditional Authentication Mechanisms

Traditional authentication mechanisms often fail to address the unique requirements of UAV networks, such as limited computational resources, intermittent connectivity, and absence of a centralized authority. Conventional cryptographic algorithms and authentication protocols may impose substantial computational overheads, rendering them impractical for resource-constrained UAV systems.

### 3.1.2 Contributions

The following summarizes the contributions of this chapter, which are published in [25], fulfilling the outlined thesis objectives (1, 2, 5) detailed in Section 3.2

1. Introduction of the BETA-UAV scheme, which comprises three phases: system initialization, registration, and signature generation and verification.
2. Utilization of ECC for efficient key management and authentication, utilizing its lightweight nature and reduced computational complexity compared to traditional cryptographic algorithms.
3. Integration of a SC deployed on the Ethereum blockchain, enabling secure and transparent recording of authentication sessions and facilitating the verification of message freshness.
4. Comprehensive security analysis, demonstrating BETA-UAV's resilience against various active attacks, including replay, modification, impersonation, and MITM attacks.
5. Implementation and performance evaluation of BETA-UAV on the Rinkeby Ethereum test network, showcasing its computational and communication efficiency advantages over existing schemes.

Addressing the critical security challenges in UAV communication, BETA-UAV paves the way for the seamless integration of UAVs into ITS, enabling a wide range of applications while ensuring privacy and integrity of the transmitted data.

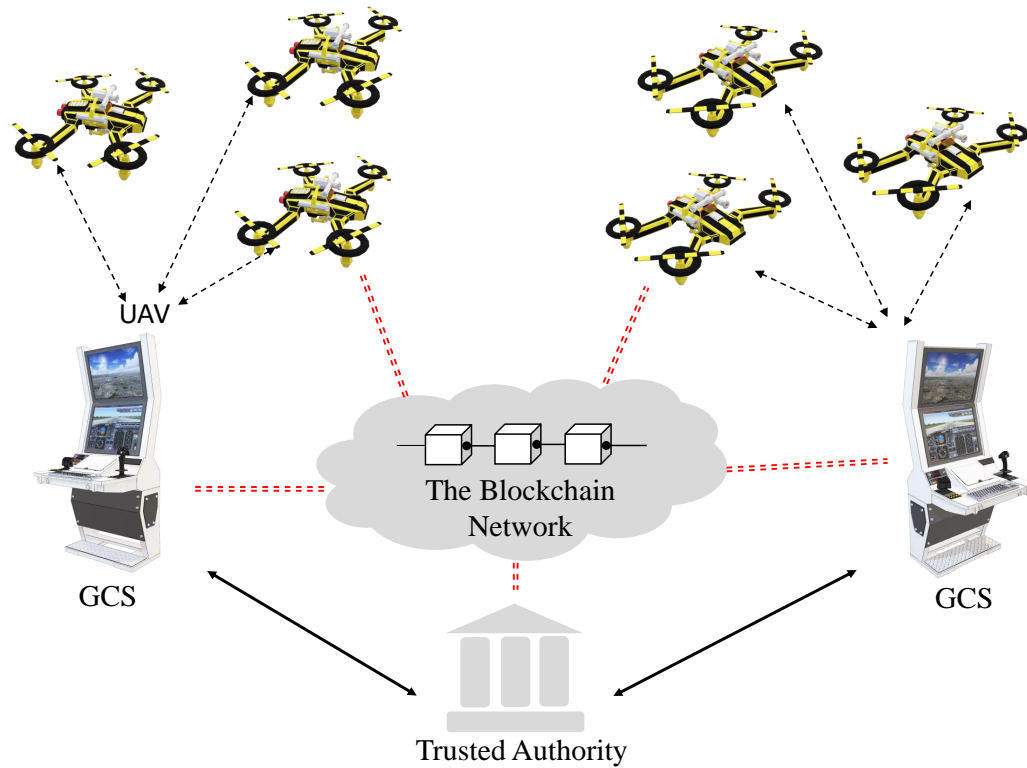


Figure 3.1: UAV Ad-hoc Network.

### 3.1.3 Chapter Organization

The structure of this chapter is as follows. Section 3.2 analyzes details of the proposed BETA-UAV scheme, including the system model, scheme phases, and algorithmic aspects. Section 3.3 explores the security analysis, focusing on message authentication and defence against active attacks. Section 3.4 discusses the implementation and performance assessment of BETA-UAV, compares the computational and communication costs, and discusses gas costs and initial authentication. Section 3.5 introduces a timestamp-based authentication protocol using blockchain, and analyzes the wallet interface and Ethereum transactions. The chapter concludes with Section 3.6, summarizing key points and suggesting future research directions.

## 3.2 Proposed BETA-UAV Scheme

This section examines the layout of the BETA-UAV scheme depicted in Fig. 3.1. As shown in Table 3.1, BETA-UAV requires a lower computational cost on the user side than related existing schemes [88]– [89]. The computational cost on the GCS side in the proposed BETA-UAV is approximately 19.28 ms, whereas [88]– [89] require approximately 0.848 ms, 2.084 ms, 3.058 ms, and 2.138 ms, respectively. Therefore, BETA-UAV had a lower computational cost than the schemes listed in Table 3.1. In contrast to the other schemes, the computational cost of the drone (Dx) or sensor node in the proposed BETA-UAV is approximately 19.28 ms, whereas [88]– [89]

requires approximately 14.38 ms, 16.32 ms, and 22.804 ms, respectively.

### 3.2.1 System Model

#### Trusted Authority (TA)

The TA is a trusted third party for the key distribution. TA provides secret keys (SK) for identity-based encryption schemes. The approved node responsible for monitoring the behavior or cooperation pattern of other nodes is known as an TA node, which validates the identification of a UAV that intends to send messages or produce a new identity, and verifies that another UAV possesses the specified identity.

#### Smart Contract Deployer

Evidence has also shown that SC must establish a user account in a consortium blockchain. Therefore, to eliminate the trust barriers between domains, a  $(t, n)$  threshold multisignature SC is created. Let  $n$  be the number of participants and  $t$  be the threshold. The number of elements contained in the Merkle tree is a combinatorial number,  $C(n, t)$ . The space complexity of this tree,  $O\left(n^{\binom{n-t}{t}}\right)$ , is exponential on the threshold and the complexity is  $O(\log(C(n, t))) < O(\log(n^t)) = O(t \cdot \log(n))$ .

#### Ground Control Station GCS

GCS receives UAV data, processes it, and converts and transfers it to other communication protocols to link clients on the same network for decisive piloting and communication between a UAV and its network. In addition, GCS typically allows UAV autopilots, live videos, and data streaming. Ground stations for UAV are essential for a new era of long-range aerial data collection. In recent years, reliable and secure communications have become scarce. A link between GCS and UAV was observed, which was also a significant concern in our study.

2

### 3.2.2 BETA-UAV: The Proposed Blockchain-Based Efficient Authentication Scheme

BETA-UAV comprises three phases that can be described as follows.

---

<sup>2</sup>Gas cost/fee in Ethereum is a pricing mechanism that determines the computational cost of executing transactions or smart contracts on the Ethereum network. It's calculated as the product of gas used (computational steps) and gas price (in Ether per unit of gas, set by the user). This system compensates miners/validators for their resources and helps prevent network spam, with prices fluctuating based on network demand.

### System Initialization Phase

TA initializes the system parameters as follows: TA initializes the elliptic curve  $E : y^2 = x^3 + ax + b \pmod p$  such that  $a, b \in \mathbb{Z}_q^*$ ,  $\Delta = 4a^3 + 27b^2 \neq 0$  [90], and  $p, q$  are 160-bit prime numbers with 80-bit security. Based on generator  $g$ , TA creates a cyclic group  $\mathbb{G}$  that includes the points of  $E$  in addition to the point of infinity  $\mathcal{O}$ . TA selects the secret parameter of the system  $Sk_{TA} \in \mathbb{Z}_q^*$ , then calculates its associated public parameter  $Pk_{TA} = Sk_{TA} \cdot g$ . Secure hash function  $H_1$ ; for example, SHA-256. TA deploys the  $SC$  through transaction  $Tx$  and retrieves the  $SC$ 's address  $SCID$ . Finally, the public parameters of the scheme are  $PPs = \langle a, b, p, q, g, SCID, H_1, Pk_{TA} \rangle$ .

### Registration Phase

For all terminals in the network, TA is responsible for registering all GCS and UAVs before being part of the network, as follows. For each  $GCS_j$ , TA creates a long-term digital certificate  $Cert_{GCS_j}$  by selecting  $Sk_{GCS_j} \in \mathbb{Z}_q^*$ , calculating  $Pk_{GCS_j} = Sk_{GCS_j} \cdot g$ , and signing it to generate  $\sigma_{TA} = Sign_{Sk_{TA}}(Pk_{GCS_j} || T_R)$ , where  $T_R$  is the expiration date.

Finally,  $Cert_{GCS_j} = \langle Pk_{GCS_j}, T_R, \sigma_{TA} \rangle$ , For each  $UAV_i$ , TA creates a long-term digital certificate,  $Cert_{UAV_i} = \langle Pk_{UAV_i}, T_R, \sigma_{TA} \rangle$ .

### Signature Generation and Verification Phase

Considering  $UAV_1$  in the communication range of  $UAV_2$ , the authentication process is divided into authentication for the first and subsequent transmission slots as follows.

Table 3.1: List of Notations for the Proposed BETA-UAV Scheme

Symbol	Definition	Symbol	Definition
TA	Trusted Authority	GCS	Ground Control Station
UAV	Unmanned Aerial Vehicle	Sk	Secret Key
Pk	Public Key	Cert	Certificate
CRL	Certificate Revocation List	$T_R$	Expiration Date
$T_1, T_2, T_3$	Timestamps	$T_S$	Session Time Interval
$\sigma_1, \sigma_2, \sigma_3$	Digital Signatures	TxID	Transaction ID
SC	SC	SCID	Smart Contract Address
E	Elliptic Curve	G	Cyclic Group
$H_1$	Secure Hash Function	A	Adversary
a, b	Elliptic Curve Parameters	p, q	Prime Numbers
g	Generator of Cyclic Group G	$\Delta$	Elliptic Curve Discriminant
$Sk_{TA}$	Secret Key of Trusted Authority	$Pk_{TA}$	Public Key of Trusted Authority
$Sk_{GCS_j}$	Secret Key of $GCS_j$	$Pk_{GCS_j}$	Public Key of $GCS_j$
$Sk_{UAV_i}$	Secret Key of $UAV_i$	$Pk_{UAV_i}$	Public Key of $UAV_i$
n	Number of Participants	t	Threshold

For the first transmission slot,

$UAV_1$  sends  $UAV_2$  a communication request in the form of a tuple  $\langle Cert_{UAV_1}, T_1, T_S, \sigma_1 \rangle$ , where  $\sigma_1 = Sign_{Sk_{UAV_1}}(Cert_{UAV_1} || T_1 || T_S)$  is signed at  $T_1$  and  $T_S$  is the entire session time interval (e.g., [00:10:00]).

$UAV_2$  in turn, checks  $T_1$ 's freshness, verifies  $\sigma_1$  as  $Verf_{Pk_{UAV_1}}(\sigma_1)$ , and then triggers the  $Issue-UAV_2(Pk_{UAV_1}, Pk_{UAV_2}, T_1)$  function in the SC using  $SCID$  and retrieves  $TxID_2$ .  $UAV_1$  stores  $\langle Pk_{UAV_1}, T_S, TxID_2 \rangle$ .

Similarly,  $UAV_2$  sends  $UAV_1$  a reply in the form of a tuple  $\langle Cert_{UAV_2}, T_2, T_S, \sigma_2 \rangle$ , where  $\sigma_2 = Sign_{Sk_{UAV_2}}(Cert_{UAV_2} || T_2 || T_S)$  is signed at  $T_2$  timestamp.

$UAV_1$  in turn, checks  $T_2$ 's freshness, verifies  $\sigma_2$  as  $Verf_{Pk_{UAV_2}}(\sigma_2)$ , and then triggers the  $Issue-UAV_1(Pk_{UAV_2}, Pk_{UAV_1}, T_2)$  function in the SC using  $SCID$  and retrieves  $TxID_1$ . At last,  $UAV_2$  stores  $\langle Pk_{UAV_2}, T_S, TxID_1 \rangle$ .

### 3.2.3 Algorithmic Description

#### UAV1 - UAV2 Freshness-Identification Algorithm

The proposed algorithm 3.1, titled "UAV1 - UAV2 Freshness-Identification," is a crucial component of the BETA-UAV scheme, which aims to facilitate secure communication and freshness identification between two UAVs (UAV1 and UAV2) in a decentralized environment governed by a trusted authority TA. The algorithm uses the Solidity programming language and SC functionality on the Ethereum blockchain to establish a robust framework for key exchange and timestamp verification between the UAVs. It commences by defining the necessary data structures, such as the D2D structure, which encapsulates the public keys (PK1 and PK2) and timestamps (T1 and T2) of the respective UAVs. The deployer function initializes the TA's address, granting it the authority to oversee and validate the freshness-identification process. Subsequent functions, namely, IssueUAV1 and IssueUAV2, allow UAV1 and UAV2 to securely submit their public keys and timestamps, which are stored in the corresponding D2D structure on the blockchain. The owner modifier ensures that only the designated TA can initiate and manage these functions, thereby safeguarding process integrity. Ultimately, the output of the algorithm consists of exchanged public keys and timestamps, enabling the UAV to establish secure communication channels and verify the freshness of the received data, thereby mitigating potential replay attacks and ensuring the trustworthiness of the overall system.

### 3.3 Security Analysis

The GCS and drone have certificates for registration from the TA. Both parties exchange credentials and check the authenticity of the certificates as  $Cert_{UAV_i} = \langle Pk_{UAV_i}, T_R, \sigma_{TA} \rangle$  during the

**Algorithm 1** UAV1 - UAV2 Freshness-Identification

---

```

1: Given: Function name, Set Parameter
2: Require: Functions write up
3: struct D2D {
4:   uint Pk1;
5:   uint PK2;
6:   uint T1;
7:   uint T2;
8: }
9: // Parameters Descriptions
10: address TA= 0xB84697ae058709060b2ACE092876ea09E65254b9;
11: mapping (uint -> uint256) public;
12: function Deployer() public {
13:   TA = msg.sender;
14: }
15: // Define the deployer as the TA
16: modifier onlyOwner {
17:   require(msg.sender == TA);
18:   _;
19: }
20: // D2D Freshness-Identification
21: D2D Freshness-Identification;
22: function IssueUAV1(uint _PK1, uint _PK2, uint _T1) public returns (uint, uint, uint) {
23:   Freshness-Identification1.PK1 = _PK1;
24:   Freshness-Identification1.PK2 = _PK2;
25:   Freshness-Identification1.T1 = _T1;
26:   return (Freshness-Identification1.PK1, Freshness-Identification1.PK2, Freshness-Identification1.T1);
27: }
28: // D2D Freshness-Identification for UAV2
29: function IssueUAV2(uint _PK2, uint _PK1, uint _T2) public returns (uint, uint, uint) {
30:   Freshness-Identification2.PK1 = _PK1;
31:   Freshness-Identification2.PK2 = _PK2;
32:   Freshness-Identification2.T2 = _T2;
33:   return (Freshness-Identification2.PK2, Freshness-Identification2.PK1, Freshness-Identification2.T2);
34: }

```

---

agreement. Consequently, if the drone and the ground station have valid certificates, they can authenticate each other.

### 3.3.1 Message Authentication

$UAV_1$  sends  $UAV_2$  a communication request in the form of tuple  $\langle Cert_{UAV_1}, T_1, T_S, \sigma_1 \rangle$ , where  $\sigma_1 = Sign_{Sk_{UAV_1}}(Cert_{UAV_1} || T_1 || T_S)$  is signed at  $T_1$  and  $T_S$ . The intended recipient and receiver UAV share symmetric key  $S_K$  to determine the authentication process.

### 3.3.2 Security Protection against Active Attacks

Attacker A can quickly monitor and eavesdrop on communication messages on a public channel if every message refreshes every session, such as  $\sigma_2$  and  $Verf_{Pk_{UAV_2}}(\sigma_2)$ , rendering it impractical for an attacker to extract all the pertinent information. The Blockchain-Based Efficient Authen-

tication (BETA) sends no parameters twice. Therefore, the proposed model resists both tracking and eavesdropping.

### Resilience to Modification

Resilience is a fundamental requirement for multi-UAV operation. Because these systems operate in dynamic and open environments, they are susceptible to various interruptions. For each message  $m$ ,  $UAV_1$  signs  $m$  at  $T_3$  timestamp to get  $\sigma_3 = \text{Sign}_{SK_{UAV_1}}(m || T_3 || Pk_{UAV_1})$  and sends  $\langle m, T_3, Pk_{UAV_1}, \sigma_3 \rangle$  to  $UAV_2$ . A multi-UAV system is robust if it can accomplish the original mission at an acceptable level of performance despite diversion. The UAV assigns public key  $pk$  and secret keys  $sk$  for each authentication. Information from the blockchain checks the session continuity by determining whether  $T_3 - T_1 \leq T_S$  holds. If this fits,  $m$  is accepted. Otherwise, the sample was discarded.

### Resilience to Impersonation

When an adversary  $\mathbb{A}$  attempts to impersonate an unauthorized drone (e.g., Alice), he must compute a valid signature for a coherent topic using Alice's credentials. Nonetheless, it is difficult for an  $T_S$  opponent owing to the message authentication characteristic, namely, the  $T_2$ 's freshness, to authenticate  $\sigma_2$  as  $\text{Verf}_{Pk_{UAV_2}}(\sigma_2)$ , and then trigger the  $(Pk_{UAV_2}, Pk_{UAV_1}, T_2)$  function in the SC using  $SCID$  and retrieve  $TxID_1$ . Finally,  $UAV_2$  stores  $\langle Pk_{UAV_2}, T_S, TxID_1 \rangle$ .

### Resilience to Man-in-the-Middle (MITM) Attack

According to the schema, an adversary can capture and compromise all the messages sent and received  $w$ . The message exposure during the freshness identification process is  $\langle Cert_{UAV_1}, T_1, T_S, \sigma_1 \rangle, \langle Cert_{UAV_1}, T_2, T_S, \sigma_2 \rangle$ . If  $\mathbb{A}$  attempts to reconstruct the UAV certification, the content of  $UAV_1$  and  $UAV_2$  must be modified. Moreover, for  $\mathbb{A}$  to reconstruct UAVs,  $pk$  and  $Sk$  must be known for  $pk$  and  $Sk$  are the parameters required for message regeneration. Hence, without requisite secret credentials, it is impractical for  $\mathbb{A}$  to reissue a valid message. Therefore, BETA-UAV is resistant to MITM attacks.

### Resilience to Birthday Collision

The proposed method encounters this property if the endorsed blockchain is susceptible to birthday collisions. For our design, we employed developed blockchain systems such as Ethereum that support SC. This distributed ledger system uses secure hash functions such as SHA-256 [91]. Therefore, computing a block hash can eliminate the two-birthday collisions.



### 3.3.3 Threat Model

The BETA-UAV scheme operates under the following threat model assumptions.

1. **Trusted Authority (TA):** The TA is considered a fully trusted entity responsible for initializing the system parameters, registering UAVs and GCS, and issuing digital certificates. TA is assumed to be honest and follow the prescribed protocols.
2. **UAVs and GCS:** The UAVs and GCSs are considered semi-trusted entities. They are assumed to follow the protocols correctly, but may be compromised by an adversary or behave maliciously.
3. **Communication Channels:** The communication channels between UAVs, and between UAVs and GCSs, are assumed to be insecure and susceptible to eavesdropping, message tampering, and replay attacks.
4. **Blockchain Network:** The underlying blockchain network, in this case, the Ethereum network, is assumed to be secure and resistant to 51% of the attacks. Blockchain's consensus mechanism ensures the immutability and integrity of recorded transactions.
5. **Adversary Model:** The adversary is assumed to have the following capabilities.
  - a) Can eavesdrop on all communication channels and intercept transmitted messages.
  - b) Can modify, delete, or inject false messages into the communication channels.
  - c) Can compromise a subset of UAVs or GCS and gain control over their operations.
  - d) Cannot compromise the TA or the blockchain network.
  - e) Has limited computational resources and cannot break the underlying cryptographic primitives (e.g., ECC, SHA-256) within a reasonable time frame.

Under this threat model, the BETA-UAV scheme aims to provide secure communication between UAV, ensuring message authentication, integrity, and freshness while preventing various active attacks, such as replay, modification, impersonation, and MITM attacks.

## 3.4 Implementation and Performance Evaluation

Our BETA-UAV protocol demonstrates its prototype blockchain implementation in Ethereum test networks, its demonstrated efficiency in drone authentication, and a simulated UAV ad-hoc network scenario. Performance is then considered in the context of implementation outcomes. First, we deployed our smart design contract on an online public Ethereum test network (the

Overview	State
Transaction Hash:	0x28ef49323cafc471a9a7d5c481f1bdf4b37f5294958149a67ad02add5795d24f
Status:	Success
Block:	11247190 4 Block Confirmations
Timestamp:	1 min ago (Aug-22-2022 01:07:16 PM +UTC)
From:	0xb84697ae058709060b2ace092876ea09e65254b9
To:	[Contract 0x96767cb104ae41f3344b569c70aedfb25b42d8d7 Created]
Value:	0 Ether (\$0.00)
Transaction Fee:	0.000554832957785824 Ether (\$0.00)
Gas Price:	0.000000002566484836 Ether (2.566484836 Gwei)
Gas Limit & Usage by Txn:	216,184   216,184 (100%)
Gas Fees:	Base: 0.066484836 Gwei   Max: 2.64217227 Gwei   Max Priority: 2.5 Gwei

Figure 3.2: Network Deployment.  
Table 3.2: Remix Settings

Parameter	Value
Compiler	0.8.7.commit.228d28d7
Language	Solidity
EVM version	Compiler default
Deployment Environment	JavaScript Virtual Machine
Featured Plugins	Solidity Compiler, Deploy and Run Transactions Solidity Static Analysis, and Solidity Unit Testing

Rinkeby Test Network). Rinkeby offers a comprehensive development environment ID for proficient compilation and deployment of SC. This expedites the prototyping process of blockchain-enabled systems. Specifically, we employed the following Remix settings compiler (0.8.7. commit.228d28d7). Our gas cost analysis shown in 3.2 begins by compiling our solidity SC code, which is subsequently deployed in the configuration described above using Remix. The first is the gas price of Eth, which reflects the cost of maintaining an Ethereum blockchain [92]. We simulated cryptographic primitives in the desktop and Raspberry PI environments with different configurations. Linux Ubuntu 18.04 LTS, Intel Core CPU @ 3.60 GHz, 8 GB RAM, and Raspberry PI 4 B, Quad-core ARM Cortex-A72 @ 1.5 GHz, 16GB RAM [93].

## 3.5 Deployment on Rinkeby Ethereum Test Network

The authors deployed BETA-UAV SC on the Rinkeby Ethereum Test Network to evaluate its feasibility and performance. The Rinkeby Test Network is a popular and widely used Ethereum test environment that simulates the behaviour of the main Ethereum network, allowing developers to test and experiment with their decentralized applications (DApps) and SC before deploying them in the main network.

### 3.5.1 Setting up the Ethereum Environment

Before deploying the BETA-UAV SC, we set up the necessary Ethereum environment. This involves the installation and configuration of the following components.

1. **Ethereum Client:** An Ethereum client, such as Geth or Parity, is required to interact with the Ethereum network. The authors likely used Geth, which is the official Go implementation of the Ethereum Protocol.
2. **Solidity Compiler:** The BETA-UAV SC is written in Solidity, which is the primary programming language used for developing Ethereum SC. The authors utilized the Solidity compiler version 0.8.7 (commit.228d28d7) to compile their SC.
3. **Remix IDE:** Remix is a popular Integrated Development Environment (IDE) for Solidity SC development. This provides a user-friendly interface for writing, testing, and deploying an SC. The authors used Remix to compile and deploy BETA-UAV SC on a Rinkeby Test Network.

### 3.5.2 Configuring Metamask Wallet

Metamask is a popular Ethereum wallet that allows users to interact with DApps and SC directly from their web browsers. We follow these steps to deploy and interact with the BETA-UAV SC.

1. Install the Metamask browser extension on their preferred web browser.
2. Create a new Ethereum account or import an existing one into Metamask.
3. Configure Metamask to connect to the Rinkeby Test Network by selecting the appropriate network from the network dropdown menu.
4. Obtain some test Ether (the cryptocurrency used on the Ethereum network) from a Rinkeby Test Network faucet to fund their Metamask account.

### 3.5.3 Deploying the Smart Contract

With the Ethereum environment setup and Metamask configured, the authors could deploy their BETA-UAV SC using Remix IDE.

1. Open the Remix IDE in their web browser.
2. Create a new Solidity file or copy-paste the BETA-UAV SC code into the Remix editor.
3. Compile the SC by clicking the "Compile" button in Remix.
4. Connect Remix to their Metamask wallet by clicking the "Deploy & Run Transactions" button and selecting the "Injected Web3" environment.
5. Deploy the SC by selecting the appropriate contract from the compiled contracts list and clicking the "Deploy" button.
6. Confirm the deployment transaction in Metamask by approving the gas fee and waiting for the transaction to be mined on the Rinkeby Test Network.

After the deployment transaction is mined, the deployed SC address can be obtained from the Remix IDE or Metamask. This address is essential for interacting with BETA-UAV SC and invoking its functions.

### 3.5.4 Overview of the Initial Authentication Step

TA generates the public parameters of the system using the following processes:

- Choosing two large prime numbers  $p$  and  $q$ , and 160-bits elliptic curve  $E$  for 80-bits security defined by  $y^2 = x^3 + ax + b \pmod p$  over a prime field  $F_p$  for  $a, b \in F_p$ , where  $\Delta = 4a^3 + 27b^2 \neq 0$ .
- Construction of the cyclic additive group  $\mathbb{G}$  of order  $q$  based on the generator  $P$ , so that  $\mathbb{G}$  consists of all the points on  $E$  and the infinity point  $\mathcal{O}$ .
- Randomly choosing the system master key  $\beta \in Z_q^*$ .
- Selecting the hash function  $H$ .

Fig. 3.3 presents a detailed step-by-step description of the communication protocol for a blockchain-based UAV system. It outlines various phases such as system initialization, user registration, SC deployment, and multiple stages of authentication and verification. Each step in these phases is meticulously described, highlighting key actions such as cryptographic operations, certificate issuance, SC updates, timestamp generation, and mutual authentication processes between UAVs. This structured presentation effectively illustrates the complexity and thoroughness of communication protocols within the system.

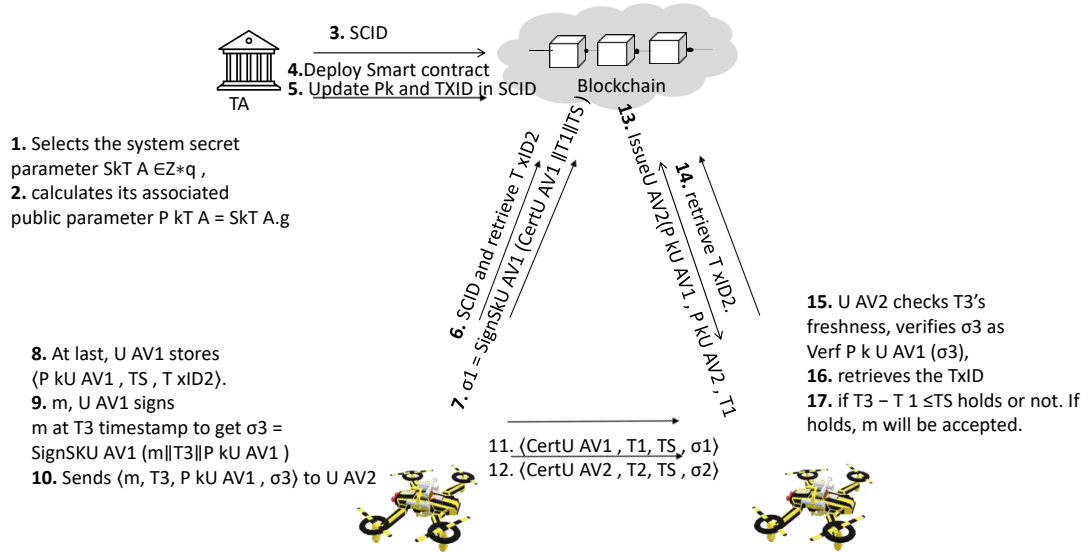


Figure 3.3: Comprehensive Overview of the Communication Protocol.

### 3.5.5 Comprehensive Protocol Overview

In the technical analysis of blockchain transaction data, In Figs. 3.4 - 3.5, we observe a confirmed contract deployment on the Ethereum Rinkeby test network. The transaction is uniquely identified by its hash  $0x28ef49323\dots d5795d24f$  and was included in block number 11247190, which has accrued four confirmations, thereby ensuring its finality on the network. The transaction was timestamped on August 22, 2022, at 01:07:16 UTC, denoting the exact moment of its successful inclusion in a block.

It was initiated from the Ethereum address  $0xb84697ae\dots e65254b9$  and directed towards a new contract address  $0x96767cb1\dots b25b42d8d7$ , indicating that the transaction's purpose was to create and deploy an SC rather than the transfer of Ether, as evidenced by the zero Ether value of the transaction. The transaction incurred a total fee of  $0.000554832957785824$  Ether, reflecting the network's processing cost at the time. The specified gas price for this transaction was  $2.566484836$  Gwei, with a gas limit and actual gas price of 216,184 units, suggesting that the transaction consumed the entire gas limit. The base fee, which is the minimum per-unit gas cost necessary for inclusion in the blockchain, is  $0.066484836$  Gwei. Meanwhile, the maximum gas price set by the initiator was  $2.64217227$  Gwei, with an additional specified maximum priority fee of 2.5 Gwei to incentivize faster processing by miners, although the total gas cost remained within the limits of the Rinkeby test network.

### 3.5.6 Analysis of the Wallet Interface on the Rinkeby Test Network

**Network Connection:** The wallet interface explicitly indicates a connection to the Rinkeby test network, as shown in Fig. 3.4. Rinkeby is one of the several Ethereum blockchain test environments. These test networks are integral to developers, facilitating the trial of new blockchain

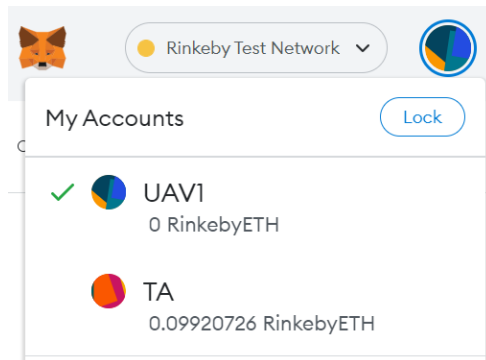


Figure 3.4: Rinkeby Test Network MetaMask.

## Contract Deployment ✕



<b>Status</b>	<a href="#">View on block explorer</a>
<b>Confirmed</b>	<a href="#">Copy Transaction ID</a>
<b>From</b>	<b>To</b>
 0xB84...54b9	 New Contract
<b>Transaction</b>	
Nonce	0
Amount	<b>-0 RinkebyETH</b>
Gas Limit (Units)	216184
Gas Used (Units)	216184
Base Fee (GWEI)	0.066484836
Priority Fee (GWEI)	2.5
Total Gas Fee	0.000555 RinkebyETH
Max Fee Per Gas	0.000000003 RinkebyETH
<b>Total</b>	<b>0.00055483 RinkebyETH</b>

Figure 3.5: Contract Deployment for BETA-UAV.

applications without expending the native cryptocurrencies of Ether Ethereum. The primary advantage of such networks lies in the use of valueless ethers, which enables cost-free experimentation and development.

### Account Overview:

- **UAV1 Account:** Exhibits a balance of 0 Rinkeby ETH, the designated cryptocurrency of the Rinkeby network. A green checkmark adjacent to this account may signify the current activation status or the form of verification.
- **TA Account:** Shows a balance of approximately 0.09920726 Rinkeby ETH, indicating prior transactional activities on this network. The presence of this balance, though minimal, suggests an engagement with network-specific operations.

**Security Feature:** A notable lock icon positioned in the upper-right corner of the interface indicates the security mechanism. This feature likely enables the wallet to be locked, thereby requiring a password for the subsequent access and transaction execution.

**Visual Account Identification:** Each account is accompanied by a unique, automatically generated icon. These icons, which vary in color and design, serve as visual aids for users to easily distinguish between multiple accounts.

**Account Labeling:** The accounts are labelled as "UAV1" and "TA" names presumably assigned by the user for identification convenience. These labels could correspond to specific roles or functionalities within the user's blockchain development activities, such as TA.

**Functional Capabilities:** The wallet interface is designed for multifaceted account management, enabling users to toggle different Ethereum networks and execute various transactions. These include the transfer of ether and interaction with SC. The display of the Rinkeby Test Network confirms the wallet's utilization in blockchain development and testing scenarios.

### 3.5.7 Analysis of an Ethereum Blockchain Transaction

In this section, we scrutinize a transaction processed in the Ethereum blockchain and examine its components and their significance within the network protocol. The transaction is identified by a unique 256-bit alphanumeric hash that ensures immutability and nonrepudiation within the blockchain ledger. This was confirmed and validated by the network's consensus mechanism, Irreversible recorded on the blockchain in block number 11247190, with four confirmations at the time of the snapshot, indicating the depth achieved in the network. The transaction was confirmed on August 22, 2022, at 13:07:16 UTC, providing a chronological context. The originating address is a 42-character hexadecimal Ethereum address, pseudonymous yet allowing for the traceability of funds. Simultaneously, the destination is a verified SC, suggesting that the purpose is to invoke a function, rather than a simple transfer of ether. The transaction value is stated as 0 Ether, indicative of a non-value transfer event, possibly an SC execution that alters the state or triggers an event within the Ethereum Virtual Machine (EVM). The minimal transaction fee, denominated in Ether and adhering to the network's dynamic fee structure (EIP-1559), underscores the nonfinancial nature of the transaction. Gas price details, including the base fee per gas and the priority fee (tip), aim to regulate network congestion and transaction throughput. The gas limit set and gas used are both enumerated, demonstrating the transaction's resource consumption as processed by EVM, with full utilization of the allocated gas, implying adequate provisioning without an out-of-gas exception. The gas fee breakdown provides insight into the economic considerations of executing transactions, with the base fee being burnt (removed from circulation) and the maximum priority fee awarded to the miner, thus incentivizing

prompt transaction processing.

### 3.5.8 Computation Cost Comparison

Compared with previous schemes proposed by the authors [8]–[11], the BETA-UAV performance IoD was determined based on their computational and communication costs. We implemented Multi-Precision Integer and Rational Arithmetic Cryptographic Library (MIRACL) for an experimental examination of various cryptographic primitives. Therefore, using the MIRACL library, we simulated and evaluated the execution times of cryptographic primitives [7]. In this section, the computational costs of the proposed and the associated schemes are determined.

### 3.5.9 Estimating Gas Cost

Ethereum performs simple computations that coincide with a swarm of computers, called nodes. An elite group of nodes is defined as the miners who work the hardest. Miners protect the network from intrusion and prioritize computations. Therefore, the miners must pace a stream of requests. Without this, the network may become overloaded because of heavy usage, or spammers picking up what is done. First, miners rely on the gas price and the gas limit of the last unit measures; however, it has no monetary value. Miners pay tiny amount of the ETH called Gwei. In this study, we deployed an SC in Rinke by testing the network. We then connected and deployed it to a meta-mask. Once the transaction is confirmed and mined, we proceed to the Blockchain Explorer page to determine the number of gas units used for this transaction. For the transaction hash: `0x28ef49323cafc471a9a7d5...` Gas prices are listed in Table. 3.3 is 0.000000002566484836 Ether (2.566484836 Gwei).

Table 3.3: Comparison of Actual vs Estimated Cost

Function	Estimated	Actual
Deployer	0.0005499 ETH	0.000555 ETH
Issue UAV1	0.00023767 ETH	0.000238 ETH

In Fig .3.6 BETA-UAV system demonstrates the most feasible and efficient computational delay performance in this graph, with low baseline delay that scales gradually and predictably with several nodes. This makes it the most promising system based on the visualized results.

### 3.5.10 Communication Cost Comparison

We evaluated the communication costs of our scheme in comparison to those of the existing algorithms discussed above. The identity, hash function, random number, SHA-256, timestamp, and modular exponentiation are respectively 32 bits, 256 bits, 160 bits, and 128 bits. We obtain the communication cost of the proposed scheme for each message as follows: 2240, 3360,



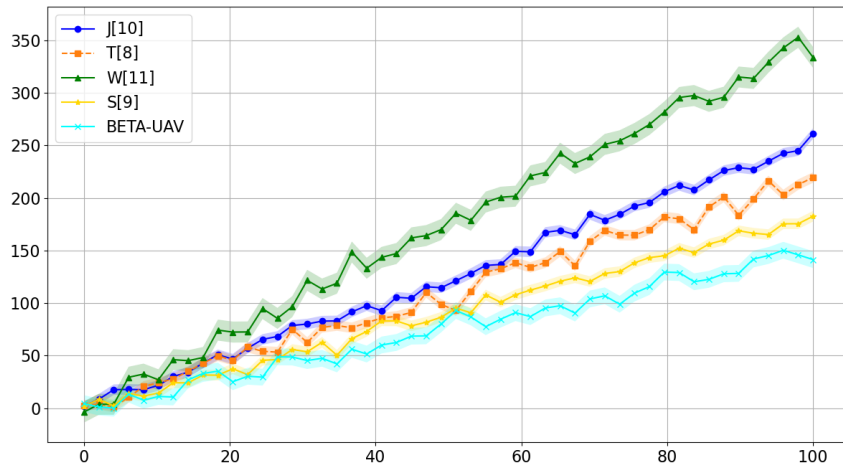


Figure 3.6: Computational Delay vs Number of Drones.

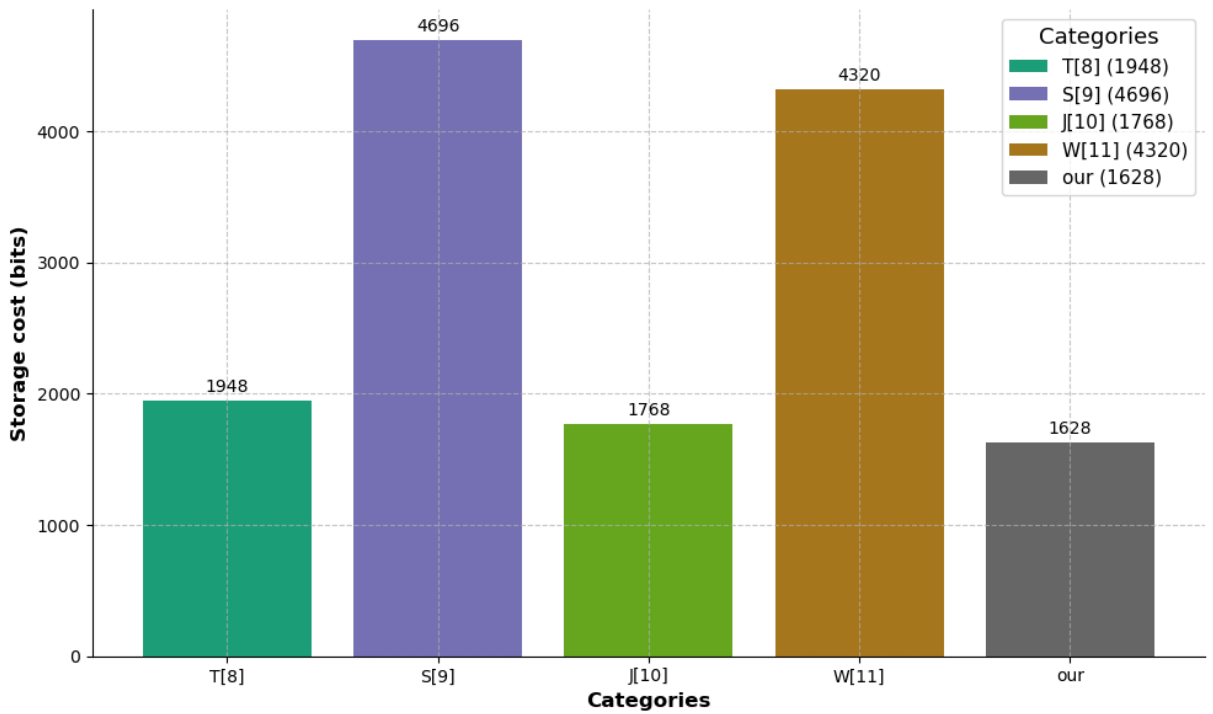


Figure 3.7: Comparison of Computational Cost.

2656, and 3200 bits by applying these notations. Therefore, the proposed scheme had a total communication cost of  $160 + 256 + 40 + 100 \approx 556$  bits.

In this section, we compare the communication costs of the proposed protocol with those of the related schemes [92]– [89]. The results indicate that the proposed method has lower communication costs than existing solutions. The bar chart Fig. 3.7 compares the storage costs in bits for different works. The costs range from 1628 bits for our own data to 4696 bits for category S[9]. The legend shows the exact storage cost for each category. Overall, the graph illustrates the relative storage requirements for the data categories, with [91] being the most expensive, and our data being the most efficient. This comparison highlights the storage optimization achieved

using the proposed method.

In the context of the BETA-UAV system, the following is a detailed tabular representation that can be included in the thesis chapter for the analysis of computational costs and the comparison of actual and estimated costs. The BETA-UAV system exhibited a lower computational cost (19.28 ms) than other strategies, thereby highlighting its efficiency. This analysis is crucial for the technical assessment of the proposed system in terms of its computational demands and performance relative to the existing solutions.

### 3.6 Summary

In this chapter, we propose BETA-UAV, a blockchain-based efficient authentication scheme for secure UAV communication. The scheme inherits the properties of blockchain technology, such as immutability and decentralization, to establish trust and enable secure message exchange among UAV operating in ad hoc networks. The BETA-UAV scheme is divided into three phases: system initialization, registration, signature generation, and verification. During the system initialization phase, the trusted authority TA initializes the system parameters, including the elliptic curve parameters, secure hash function, and SC deployment on the Ethereum blockchain.

In the registration phase, the TA is responsible for registering all GCS and UAV before they can participate in the network. This process involves issuing long-term digital certificates to each entity to ensure authentication and authorization. The signature generation and verification phases govern the authentication process between UAVs. For the first transmission slot, UAV exchange certificates, timestamps, and digital signatures are used. Subsequently, they trigger SC functions to record the authentication session on the blockchain and retrieve transaction identifiers (TxIDs) as proof of freshness and trustworthiness for subsequent transmissions. For subsequent transmission slots, the UAVs sign messages with their private keys include relevant TxIDs from the blockchain. The receiving UAV verifies message freshness, sender signature, and session continuity by checking the blockchain for the corresponding TxID and timestamp information.

BETA-UAV demonstrates resilience against various active attacks, such as replay, modification, impersonation, and MITM attacks, through its robust authentication mechanisms and the inherent properties of the blockchain. The performance evaluation of the BETA-UAV implemented on the Rinkeby Ethereum test network demonstrated its computational and communication efficiency advantages over the existing schemes. The scheme exhibited lower computational costs on both the user and central server sides, as well as reduced communication overhead, making it well suited for resource-constrained UAV environments. In conclusion, BETA-UAV presents a novel and efficient approach for securing UAV communication, addressing critical security challenges, and paving the way for the seamless integration of UAVs into ITS while ensuring the privacy and integrity of the transmitted data. Chapter 4 also sets the stage for fu-

ture research in areas such as testbed validation, integration with edge computing, 5G networks, and privately preserving data sharing. These advancements and potential research directions highlight the evolution of foundational blockchain applications in UAV communication (Chapter 3) to complex, scalable, and efficient solutions for critical scenarios such as disaster response (Chapter 4).

# Chapter 4

## UAV Networks for Post-Disaster: A Flocking Approach

This chapter presents a robust blockchain-enabled framework for secure and efficient coordination of UAV fleets in post-disaster communication scenarios. The proposed architecture exploits blockchain technology to overcome the challenges related to decentralization, security, privacy, and scalability in UAV network coordination during disasters. The key contributions include a consortium blockchain architecture that enables secure and private multi-agency coordination through access control and privacy mechanisms; an optimized hybrid consensus protocol combining Delegated Proof of Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT) to balance efficiency, security, and resilience; and decentralized flocking algorithms for adaptable and autonomous swarm operations between specialized UAV clusters performing critical disaster relief functions.

This chapter presents mathematical models for communication, mobility, reliability, and security and describes the integration of Reynolds flocking rules for decentralized UAV coordination. The Delegated Proof of Stake Practical Byzantine Fault Tolerance (DPoS-PBFT) consensus mechanism is introduced, along with its implementation details and performance analysis. Comprehensive simulations demonstrated the framework's ability to enhance transparency, automation, scalability, and cyber-attack resilience for reliable and secure UAV swarm communication in post-disaster scenarios. The results demonstrate the system's effectiveness in achieving security, efficiency, scalability, and resilience objectives, outperforming the existing approaches. The chapter concludes by highlighting the potential for further research in areas such as tested validation, deep reinforcement learning, geospatial SC, and privacy-preserving data sharing, to advance the capabilities of the proposed framework and its real-world applicability. The following research questions and objectives were formulated for this thesis on UAV-assisted network design and optimization.

UAVs have significant potential for agile communication and relief coordination in post-disaster scenarios, particularly when ground infrastructure is compromised. However, effi-

ciently coordinating and securing flocks of heterogeneous UAV from different service providers poses significant challenges related to privacy, scalability, lightweight consensus protocols, and comprehensive cybersecurity mechanisms. This study introduced a robust blockchain-enabled framework designed to tackle these technical challenges through a combination of consensus protocols, SC, and cryptographic techniques. First, we propose a consortium blockchain architecture that ensures secure and private multiagency coordination by controlling access and safeguarding the privacy of sensitive data. Second, we develop an optimized hybrid consensus protocol that merges DPoS-PBFT to achieve an effective balance between efficiency, security, and resilience against node failures. Finally, we introduce decentralized flocking algorithms that facilitate adaptable and autonomous operations among specialized UAV clusters, thereby ensuring critical disaster relief functions under conditions of uncertain connectivity. Comprehensive simulations demonstrated that the system achieved linear throughput scaling up to 500 UAV nodes, with only a 50ms increase in latency from 10 to 500 nodes. The framework maintained high throughput and low latency despite spoofing, DoS, and tampering attacks, thus exhibiting strong cyber-resilience. Communication latencies were kept under 10ms for diverse UAV operations through self-optimizing network intelligence, with median values of approximately 2-3ms.

## **4.1 Introduction**

Natural disasters such as hurricanes, floods, and earthquakes can severely damage critical communication infrastructure, disrupting access to aid and relief coordination. UAVs offer the potential for rapidly restoring connectivity, but coordinating heterogeneous UAV flocks poses challenges in security, privacy, and scalability [5]. This motivated the design of innovative blockchain-enabled UAV flocking networks to address these limitations. This chapter proposes a novel framework using blockchain technology to improve UAV operations in post-disaster scenarios.

### **4.1.1 Background**

Intelligent emergency communication systems are vital for ensuring effective network connectivity during disaster-response scenarios. UAVs have proven effective at expanding wireless coverage for IoT devices due to their ability to hover in diverse locations and establish reliable links [59]. However, coordinating heterogeneous UAV fleets presents several challenges, such as limited flight endurance [94], restricted communication range [5], reliance on damaged ground networks and inadequate pre-planned routes [95], intermittent connectivity [96], lack of coordination between UAVs and human responders, security vulnerabilities caused by chaos, and insufficient transparency mechanisms. Recent research has explored decentralized blockchain approaches to help overcome some obstacles through inherent attributes, such as distribution,

security, transparency, automation, and resilience [82]. However, significant gaps remain before blockchain technology can be successfully incorporated into UAV networks for disaster response [97], despite the analytical frameworks that optimize UAV deployment. Blockchain integration introduces new consensus, interoperability, security, and SC design challenges, specifically for decentralized disaster-resilient UAV fleet coordination [98]. Although blockchain-enabled UAV networks have been studied to address security issues in UAV swarms [99], research gaps remain 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. Further research is needed on the potential environmental impact and ethical considerations related to surveillance and data privacy. Existing studies have focused on building internal trust using blockchains [100], such as UAV Practical Byzantine Fault Tolerance (U-PBFT), for lightweight consensus and real-time trust evaluation [101]. However, dynamic topology and limited UAV resources pose challenges [102], highlighting the need for secure, efficient, and intelligent blockchain coordination frameworks tailored for disaster response UAVs to fully realize their decentralized collaborative autonomy potential. This has motivated the design of a blockchain framework to realize the potential of UAVs for revolutionizing disaster response, addressing the identified gaps through innovations in consensus protocols [103], interoperability, security mechanisms, and SC architectures specialized for resource-constrained UAV disaster-response coordination.

### 4.1.2 Motivation

This study proposes several innovative solutions to address the identified limitations related to optimized blockchain consensus protocols, heterogeneous network interoperability, security against threats, and adaptive SC for evolving disaster coordination needs. The thorough motivation is to transform disaster response strategies by unlocking the full potential of UAV networks through blockchain integration. Specifically, the aim is to facilitate decentralized, efficient, and autonomous UAV-based operations even in challenging post-disaster environments. This has the potential to significantly improve the effectiveness of the time-critical relief [104]. A hybrid DPoS-PBFT consensus approach that balances efficiency, security, and fault tolerance is promising for accommodating the constraints of the UAV platform and the volatility of the aerial environment. In addition, bio-inspired flocking techniques based on Reynolds rules [105] can enable the resilient coordination of UAV clusters under uncertain connectivity during disaster relief. However, decentralized flocking alone cannot address critical security and access control challenges. Therefore, this study holistically tackles these motivations by developing an advanced decentralized ecosystem for secure, reliable, and optimized coordination among UAV fleets to enhance disaster management. The specific technical details that underpin the system design of the proposed framework are discussed in Sections 4.3–4.5.

### 4.1.3 Contributions and Organization

In this study, we introduce a novel framework aimed at enhancing operations in wireless networks. Specifically, we propose strategies to optimize network performance within our framework while also suggesting additional enhancements. Through simulations, we demonstrated the efficiency and adaptability of our proposed blockchain-based coordination framework, particularly in dynamic environments with fluctuating resources, variable channel conditions, and diverse service requirements. The key contributions of this study are the pioneering advancements in system architecture, consensus protocols, and coordination algorithms to address existing limitations. The main contributions are as follows:

- We propose a blockchain architecture enabling decentralized coordination across UAV networks, with a focus on preserving privacy and access control - crucial for efficient and secure disaster response.
- We design an optimized DPoS-PBFT consensus protocol for resource-constrained UAVs, balancing efficiency, security, fault tolerance and achieving lightweight processing, high throughput, low latency, and robustness.
- We present decentralized Reynolds flocking techniques enabling adaptable coordination of UAV swarms under uncertain connectivity.
- We demonstrate through comprehensive simulations that our proposed framework overcomes limitations in existing UAV network coordination. Specifically, we achieve excellent scalability, cyber resilience, and optimized latency profiles that unlock the potential of decentralized and intelligent UAVs for disaster response.

The remainder of this chapter is organized as follows. Section 4.2 provides an overview of the relevant literature. Section 4.3 presents the architecture and the model of the proposed system. Section 4.4 details the decentralized flocking algorithm for UAV coordination. Section 4.5 describes a customized hybrid consensus protocol. Section 4.6 presents an analysis of the simulation setup, and Section 4.7. Finally, Section 4.8 concludes the study and discusses future work.

## 4.2 Preliminary Study

### 4.2.1 Blockchain-Enabled UAV Solutions for Disaster Response

UAV ad hoc networks have gained significant attention for their rapid deployment capabilities and resilience during disaster scenarios when ground infrastructure fails [42]. However, ensuring secure decentralized coordination within these dynamic networks poses several challenges.

Blockchain technology offers a promising approach for addressing these challenges owing to its inherent features of distributed trust, transparency, and consensus mechanisms [56]. Nevertheless, consensus algorithms optimized for intermittent aerial links and resource-constrained UAV platforms are essential for an effective implementation.

Existing blockchain solutions developed for vehicular networks have limited applicability when applied to the volatile and dynamic nature of UAV swarms [56, 106]. Numerous studies have explored blockchain-based systems for UAV coordination in disaster response scenarios, with emphasis on secure information sharing [107], transparent data recording [24], and accountability in relief distribution [108]. However, challenges related to scalability, lightweight optimized consensus protocols for resource-constrained UAV, and comprehensive privacy mechanisms remain largely unaddressed [107]. The existing works in [109] utilized SC solely for agency authentication and access control, relying on centralized network components that limit robustness and resilience.

#### 4.2.2 Consensus Protocols and Smart Contracts for UAV Blockchains

The efficiency and fault tolerance of consensus protocols are critical factors for UAV networks, and typically involve resource-constrained nodes and intermittent connectivity. While the PBFT protocol provides resilience against Byzantine failures, it suffers from high communication overhead [110]. However, the Proof-of-Authority (PoA) consensus mechanism reduces overhead by involving fewer validators but introduces centralization issues. To address the trade-offs between efficiency and security, recent studies proposed hybrid protocols that combine PBFT and PoA [111]. These hybrid approaches also incorporate techniques such as sharding and utilizing UAV mobility patterns to further improve throughput and reduce latency. Such optimized consensus protocols aim to achieve an effective balance between efficiency, security, and fault tolerance, making them suitable for time-sensitive UAV disaster-response operations while maintaining the necessary security guarantees [112].

In the context of disaster management, SC have been explored to automate coordination and ensure transparency by encoding rules executed based on predefined conditions. The proposed applications of SC in UAV disaster networks include autonomous flight planning, decentralized information exchange between responders, and the transparent tracking of aid distributions [113]. However, standard SC languages and data formats lack native support for the spatial data required for the geo-coordination of UAVs [114]. Novel geospatial SC tailored for location-based UAV coordination show promise but require further research and development to address challenges such as efficient storage and querying of spatial data on the blockchain. Recent advancements in areas such as geospatial SC, disaster-resilient communication protocols [115], and privacy-preserving UAV coordination techniques [116] show promise for overcoming these limitations. This motivated the design of a comprehensive framework that emphasizes decentralization, efficiency, privacy, and resilience, tailored specifically for secure blockchain-enabled



coordination in real-world UAV-assisted disaster response scenarios. In summary, UAV ad hoc networks are increasingly being recognized for their rapid deployment capabilities and resilience when ground infrastructure is compromised [117]. However, securing decentralized coordination within these dynamic networks remains a significant challenge. Although blockchain technology offers distributed trust and consensus mechanisms to address these challenges, algorithms specifically tailored for intermittent aerial communication links and resource-constrained UAV platforms are essential [109]– [117]. The existing blockchain solutions for vehicular networks have limited applicability to the volatile nature of UAV swarms [118]. Although UAV consensus protocols have been proposed, they often lack consideration of fluctuating nodes, link conditions, and the unique constraints of UAV platforms. Numerous studies have focused on blockchain systems for disaster response UAV coordination, secure information sharing, transparent data recording, and accountability in relief distribution [119]. However, issues remain with scalability, lightweight consensus protocols for resource-constrained UAV, comprehensive privacy mechanisms, and effective utilization of SC for the spatial coordination of UAV fleets. Recent advancements in areas such as geospatial SC, resilient communication protocols, and privacy-preserving coordination techniques have shown promise in addressing these limitations [120]. This study aims to advance secure, blockchain-enabled coordination specifically tailored for real-world disaster response UAVs, focusing on decentralization, efficiency, privacy, resilience, and effective utilization of SC for the spatial coordination of heterogeneous UAV fleets.

This Fig. 4.1 illustrates the deployment and coordination of UAVs in a post-disaster scenario. It showcases various UAV operations and activities aimed at facilitating an effective disaster response and recovery. The figure shows UAV flocks engaged in different tasks such as search and rescue operations, initial assessment and data collection, data management and coordination, and post-disaster recovery efforts. The UAVs are organized into flocks and exhibit flocking behaviour characterized by separation, cohesion, and alignment, which enables coordinated movement and efficient coverage of the affected areas. The figure also highlights the establishment of communication networks, including A2A and Aerial-to-Ground (A2G) links, to provide stable connectivity and enable drone-delivery services. These communication networks are crucial for maintaining reliable communication channels, coordinating UAV operations and facilitating the delivery of essential supplies to affected regions.

Additionally, this diagram illustrates an attacker's presence, indicating potential security threats and the need for robust cybersecurity measures to protect UAV networks and their operations from malicious attacks. The diagram also shows damaged BS and Roadside Unit (RSU), representing the disruption of the ground infrastructure commonly experienced in disaster scenarios. This emphasizes the importance of UAVs in providing alternative means of communication and support when the traditional infrastructure is compromised. Overall, this main scenario illustrates the various components and activities involved in a coordinated UAV-based disas-

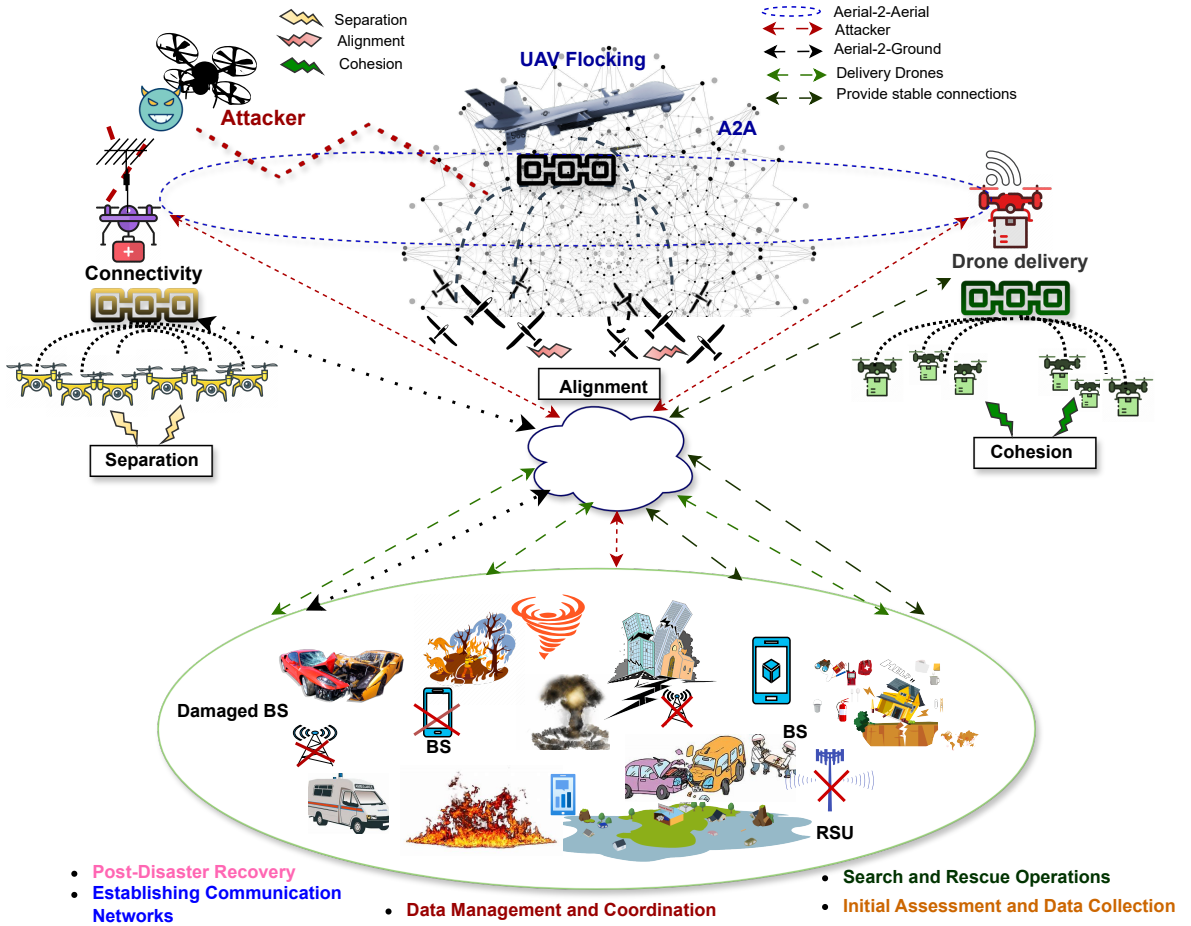


Figure 4.1: The Architecture for Blockchain-Enabled UAV Coordination in Disaster Response.

ter response effort, highlighting the importance of communication networks, flocking behavior, drone delivery services, and the need for security measures to ensure effective and resilient operation in challenging post-disaster environments.

### 4.3 System Architecture and Models

This section describes the mathematical models used to characterize the architecture of UAV-based disaster response. Specifically, they include 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 UAV in an aerial network. This model is commonly used for modeling signal attenuation in A2A channels, particularly in scenarios involving UAVs. The *log-distance path-loss model* is a fundamental concept in wireless communication. It is used to estimate the loss of signal strength, known as path loss, over a 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 loss at a reference

distance, making it particularly relevant in the context of UAV communication. This relevance stems from its utility in understanding and predicting signal-strength variations over different distances in the 3D airspace. Resource Allocation Assumption – No Interference Resource allocation in UAV networks typically involves distributing available communication resources (like bandwidth, power, and channels) among the UAVs to optimize performance metrics such as throughput, latency, and reliability. No interference implies that the model assumes ideal conditions where there is no external or internal interference affecting the communication links between UAVs. This means no overlapping frequency usage, no signal degradation due to noise, and no jamming or other forms of interference.

### 4.3.1 Communication Model

The communication model defines the propagation characteristics of wireless links between UAVs in an aerial network. A2A propagation relies on the log-distance path-loss model, which is commonly used for modeling signal attenuation in A2A channels. The path loss  $PL(d_{ij})$  depends on the distance  $d_{ij}$  between the transmitting UAV  $i$  and receiving UAV  $j$ . This describes how the signal strength decays with the distance as it propagates through the medium. The path loss is calculated as

$$PL(d_{ij}) = PL_0 + 10n \log_{10} \left( \frac{d_{ij}}{d_0} \right). \quad (4.1)$$

where  $n$  is the path loss exponent,  $d_0$  is the reference distance, and  $PL_0$  is the path loss at reference distance  $d_0$ . The path-loss exponent  $n$  depends on the specific environment. Using this path loss model, the received Signal-to-Noise Ratio (SNR) between UAVs  $i$  and  $j$  can be computed as

$$SNR_{ij} = P_t + \mathcal{G}_i + \mathcal{G}_j - PL(d_{ij}), \quad (4.2)$$

where  $P_t$  is the transmit power of UAV  $i$  and  $\mathcal{G}_i$  and  $\mathcal{G}_j$  are the antenna gains of UAVs  $i$  and  $j$ , respectively. The 3D positions  $\mathbf{P}_i$  and  $\mathbf{P}_j$  determine the separation distance  $d_{ij}$ , which directly affects path loss. The maximum achievable data rate  $R_{ij}$  for the A2A link is calculated using Shannon's capacity formula

$$R_{ij} = B \log_2(1 + SNR_{ij}). \quad (4.3)$$

where  $B$  denotes the channel bandwidth, and sustaining adequately high mesh link data rates is crucial for reliable UAV coordination and message exchange control. To model mobility, 3rd Generation Partnership Project (3GPP) TR 36.777 was referenced, which provides standard statistical 3D trajectory models.<sup>1</sup> This allows the capture of realistic fluctuations in UAV trajectories.

<sup>1</sup>[https://www.3gpp.org/ftp/Specs/archive/36\\_series/36.777/](https://www.3gpp.org/ftp/Specs/archive/36_series/36.777/)

### 4.3.2 Consortium Blockchain Architecture

This section outlines the consortium blockchain architecture tailored for decentralized coordination and access control in disaster response scenarios involving both service providers and UAV networks. We focus on key parameters, such as transaction throughput  $T(N)$  and latency  $L(N)$ , which 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 the involved parties. SC establish robust access control policies. Each participating entity is assigned a specific permission  $P(x)$  which dictates the level of access within the network. The function of a SC, denoted by  $SC_{ac}(P(x), ac_i) \rightarrow \{\text{Allow, Deny}\}$ , is to enforce the policies based on a set of predefined rules.

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 performance might vary with changes in scale and node density during disaster response operations. Moreover, cryptographic methods, including durables, have been highlighted as a means of facilitating privacy-preserving coordination, particularly when handling sensitive information.

### 4.3.3 Security Measurements

Analytical models are used to quantify the overall risk  $\mathcal{X}(t)$  and resilience  $R(t)$  based on various threat factors including denial-of-service, spoofing, and tampering. This enables the evaluation of security mechanisms. We modelled the security risks faced by UAV networks such as denial-of-service attacks, spoofing, tampering, and malware infections. The overall risk  $\mathcal{X}(t)$  at time  $t$  is given by

$$\mathcal{X}(t) = w_{\mathcal{D}}D(t) + w_{\mathcal{S}}S(t) + w_{\mathcal{T}}T(t) + w_{\mathcal{M}}M(t), \quad (4.4)$$

where  $D(t)$ ,  $S(t)$ ,  $T(t)$ , and  $M(t)$  represent the individual risk factors and  $w_{\mathcal{D}}$ ,  $w_{\mathcal{S}}$ ,  $w_{\mathcal{T}}$ , and  $w_{\mathcal{M}}$  are the weights for tuning their relative importance. The individual risk factors are modelled as follows

$$D(t) = \lambda_{\mathcal{D}}e^{-\mu_{\mathcal{D}}t}, \quad (4.5)$$

$$S(t) = \lambda_{\mathcal{S}}(1 - e^{-\mu_{\mathcal{S}}t}), \quad (4.6)$$

$$T(t) = \lambda_{\mathcal{T}}te^{-\mu_{\mathcal{T}}t}, \quad (4.7)$$

$$M(t) = \lambda_{\mathcal{M}}(1 - e^{-\mu_{\mathcal{M}}t}). \quad (4.8)$$

Here,  $\lambda$  denotes the initial risk magnitude and  $\mu$  represents the mitigation rate for each threat. This allows for analytical quantification of the evolution of risk. The resilience  $R(t)$  is measured

as

$$R(t) = 1 - \frac{\mathcal{X}(t)}{\mathcal{X}(0)}, \quad (4.9)$$

where  $\mathcal{X}(0)$  denotes initial risk. The simulations assessed  $R(t)$  for different attack scenarios and intensities. The results demonstrate that the system maintains resilience with  $R(t) > 80\%$  under realistic threat levels, owing to the implemented security mechanisms. The quantitative evaluation of resilience through analytical modeling ensures the robustness of the system against evolving attacks.

## 4.4 Decentralized Flocking Model for UAV Disaster Response

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

### 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  $S_\lambda$ , focused on transporting relief supplies; the survey network  $S_\eta$ , assigned to rapid damage assessment; and the connectivity network  $S_\Omega$ , which is responsible for restoring communication links. A central UAV monitor,  $\Upsilon_m$ , 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 UAVs maintain cohesion, alignment, and separation to ensure the efficient and safe delivery of aid. Survey flock  $\mathcal{S}_\eta$  focuses on damage assessment and mapping. By employing flocking strategies, these UAV can systematically cover disaster areas, maintain communication, and avoid collisions. The connectivity flocks  $\mathcal{S}_\Omega$  were aligned with 3GPP UAV standards to ensure efficient communication restoration in disaster-stricken areas. UAVs use flocking rules to maintain optimal formation for wireless coverage and to navigate safely through the environment.

The central monitor UAV,  $\Upsilon_m$ , coordinates the activities of these flocks by utilizing a decentralized coordination algorithm based on the Reynolds flocking rules. The control input  $\varphi_i$  for each UAV  $\Upsilon_i$  comprises terms for separation, alignment, cohesion, and navigation, allowing collision avoidance and coordinated trajectory planning. In addition, a dynamic dissipating obstacle avoidance mechanism was incorporated, enabling UAV to effectively navigate around obstacles.

### 4.4.2 Reynolds Flocking Rules and Their Application

The Reynolds flocking rules guide the decentralized coordination of UAV in the proposed model. These rules are comprised of four key components: separation ( $\varphi_i^s$ ), alignment ( $\varphi_i^a$ ), cohesion ( $\varphi_i^c$ ), and navigation ( $\varphi_i^n$ ). Each UAV  $\Upsilon_i$  receives a control input  $\varphi_i$ , which is a combination of these components that facilitates coordinated movement while avoiding collisions.

**Obstacle Avoidance Dynamics:** To successfully navigate around obstacles, UAVs utilize adaptive techniques for obstacle avoidance. The mathematical representation of this dynamic process is as follows

$$\langle \mathbf{v}_\gamma, \bar{\mathbf{v}} \rangle \geq \cos(\vartheta_m) |\bar{\mathbf{v}}|^2. \quad (4.10)$$

Here,  $\vartheta_m$  denotes the maximum allowable misalignment angle between the UAV's velocity vector  $\mathbf{v}_\gamma$  and the desired direction  $\bar{\mathbf{v}}$ . In our model, each UAV is considered as an autonomous agent with a state comprising its position and velocity vectors, denoted by  $(x_i, v_i)$  for UAV  $i$ . The control protocol for obstacle avoidance, which is essential in cluttered post-disaster environments, is the sum of three terms:  $u_i = u_i^\alpha + u_i^\beta + u_i^\gamma$ , where each term represents a specific control aspect for the UAV. Our approach emphasizes a peer-to-peer control mechanism that avoids a centralized command structure. This design enhances the resilience and adaptability of the system. A central monitoring UAV,  $\Upsilon_m$ , orchestrates the overall flocking behaviour and adapts to the dynamic disaster response needs. The primary objective of this decentralized flocking system is to enable robust and autonomous coordination among UAV flocks, thereby facilitating key disaster-response tasks. Each UAV's state is defined by its position  $\rho_i$ , velocity  $\Omega_i$ , and designated flock type  $\zeta_i$ , ensuring that every UAV contributes optimally to the overall mission.

### 4.4.3 Dynamic State Propagation and Battery Model

The state of each UAV evolves according to

$$\rho_i[\kappa + 1] = \rho_i[\kappa] + \Delta\tau \cdot \Omega_i[\kappa], \quad (4.11)$$

$$\Omega_i[\kappa + 1] = \Omega_i[\kappa] + \Delta\tau \cdot (\varphi_i^s + \varphi_i^a + \varphi_i^c + \varphi_i^n). \quad (4.12)$$

Here,  $\Delta\tau$  represents the discrete time step. The battery dynamics of the UAVs were modelled to account for the power. This Fig. 4.2 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 1-6. Each scatter plot represents a specific time step, with the x- and y-axes indicating geographical coordinates within the 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.

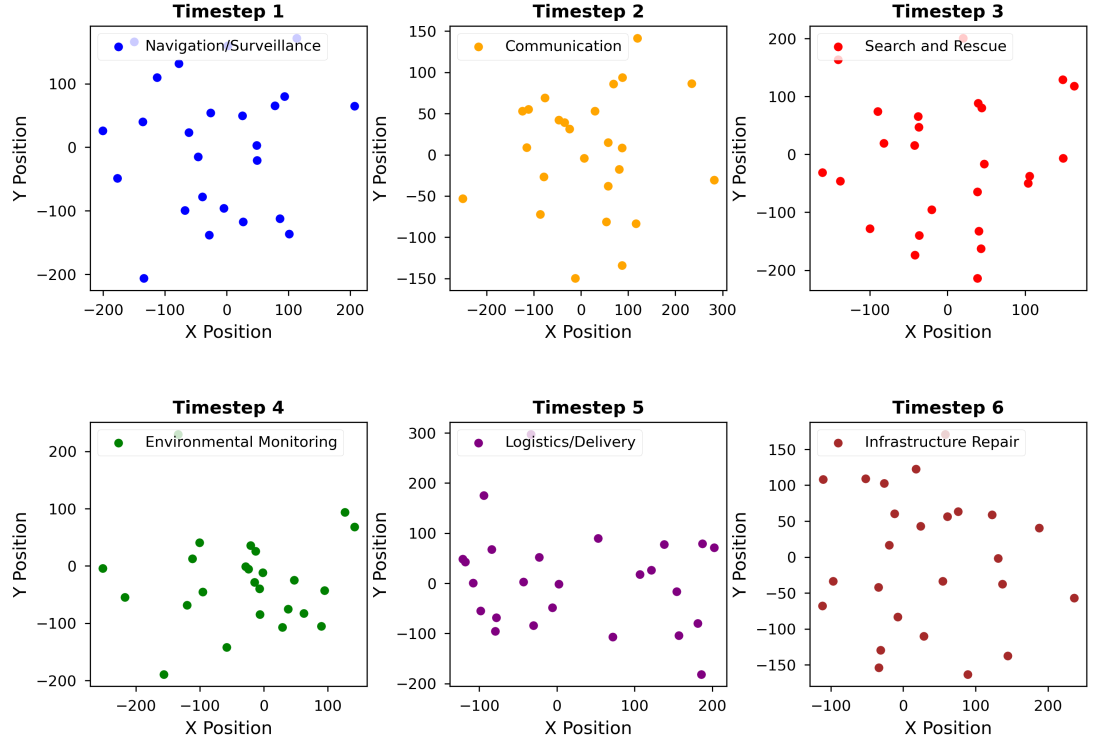


Figure 4.2: The 2D spatial distribution of flocking UAVs engaged in post-disaster activities. More detailed description is provided in Section 4.4.

#### 4.4.4 Significance of Flocking Algorithms in Multi-Agent Systems

Consider a group of autonomous agents  $\mathcal{A} = \{A_1, A_2, \dots, A_N\}$ , where each agent  $A_i$  has 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

$$U_i = \hat{U}_i^{\text{coh}} + \bar{U}_i^{\text{damp}} + \check{U}_i^{\text{nav}}, \quad (4.13)$$

where  $\hat{U}_i^{\text{coh}}$  enables cohesion towards the flock centre,  $\bar{U}_i^{\text{damp}}$  achieves velocity consensus through damping force, and  $\check{U}_i^{\text{nav}}$  drives navigation towards the group objective. We propose two flocking algorithms based on different interaction rules

$$U_i = U_i^\alpha, \quad (4.14)$$

where,

$$U_i^\alpha = \underbrace{\sum_{A_j \in \mathcal{N}_i} \phi_b(\|x_j - x_i\|_\sigma) \mathbf{n}_{ij}}_{\text{Cohesion Term}} + \underbrace{\sum_{A_j \in \mathcal{N}_i} a_{ij}(x)(v_j - v_i)}_{\text{Damping Term}}, \quad (4.15)$$

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

#### 4.4.5 Alpha-Neighbors of Alpha-Agents: Proximity Net

Let  $\mathcal{V}_\alpha = \{1, 2, \dots, n_\alpha\}$  and  $\mathcal{V}_\beta = \{1, 2, \dots, n_\beta\}$  denote 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

$$\mathcal{B}(q_i, r_\beta) \cap O_k \neq \emptyset, \quad (4.16)$$

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

$$\mathcal{N}_{\alpha i} = \{j \in \mathcal{V}_\alpha : \|q_j - q_i\| < r_\alpha\}, \quad (4.17)$$

$$\mathcal{N}_{\beta i} = \{k \in \mathcal{V}_\beta : \mathcal{B}(q_i, r_\beta) \cap O_k \neq \emptyset\}. \quad (4.18)$$

where  $q_i$  and  $v_i$  are the position and velocity of agent  $i$ , respectively, in 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,  $r_\alpha$  and  $r_\beta$  are the radii of proximity in the alpha and beta neighbor sets, respectively.

### 4.5 Enhanced DPoS-PBFT Consensus Mechanism for UAV Networks

UAVs are pivotal in disaster management for rapid response and recovery. We propose an enhanced consensus mechanism that integrates DPoS-PBFT. This design uses DPoS for efficient block validation and PBFT for heightened security, thereby optimizing UAV network performance in adverse disaster conditions. There are several key justifications for combining DPoS and PBFT in the proposed consensus mechanism for UAV networks.

- **Balancing efficiency and security:** DPoS offers high efficiency and throughput, while PBFT provides stronger security and fault tolerance. Combining them allows the system to leverage the strengths of both.
- **Resource constraints:** UAVs have limited computational resources. The hybrid approach allows using the lightweight DPoS for most operations, while reserving PBFT for situations requiring higher security.
- **Adaptability:** The hybrid mechanism can adapt to different network conditions and security requirements in volatile disaster scenarios.
- **Scalability:** DPoS enables better scalability for large UAV swarms, while PBFT provides robust consensus for critical operations.



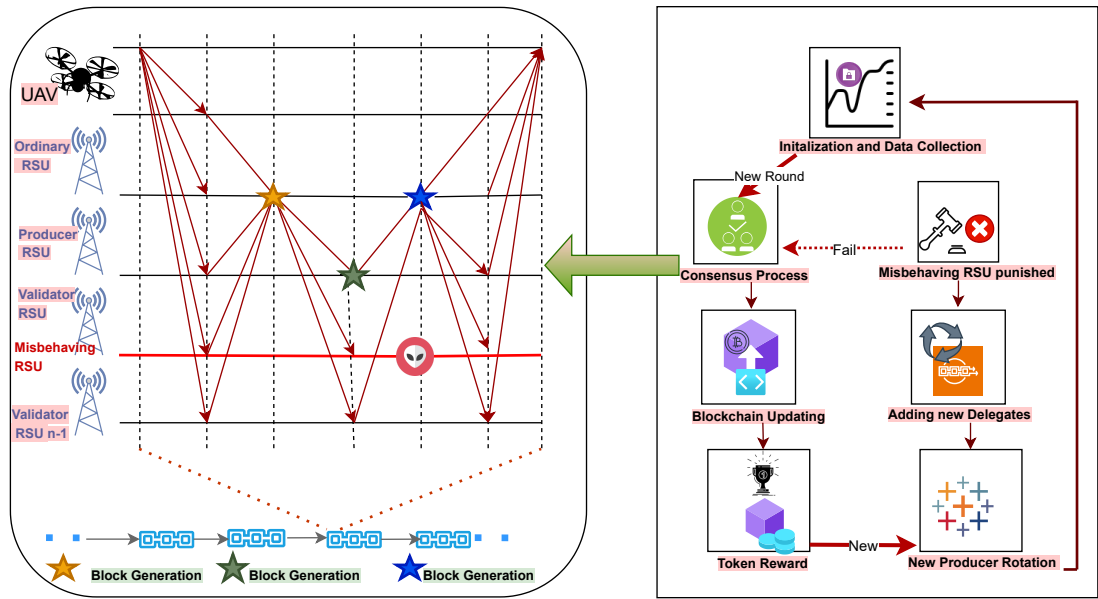


Figure 4.3: Detailed Working Mechanism of the DPoS-PBFT Consensus Protocol.

Regarding the safety and reliability of the DPoS-PBFT protocol:

- **Safety:** The PBFT component ensures safety as long as less than  $\frac{1}{3}$  of the nodes are Byzantine (malicious or faulty). So if there are  $n$  total nodes, the system can tolerate up to  $f$  Byzantine nodes where:

$$f < \frac{n}{3}$$

- **Reliability:** The DPoS component improves reliability through its delegate selection process. The paper does not specify exact numbers, but typically DPoS can maintain consensus as long as most honest delegates are online and functioning.

PBFT is designed to work in asynchronous networks for link failures and can tolerate network partitions. The number of link failures tolerated would depend on the specific implementation and network topology. The chapter states that the hybrid configuration uses 20 DPoS delegates and five regional PBFT servers ensuring efficient and robust transaction processing. This suggests the system could tolerate

- Up to 6 Byzantine nodes in the DPoS layer (less than  $\frac{1}{3}$  of 20)
- 1 Byzantine node in the PBFT layer (less than  $\frac{1}{3}$  of 5)

Fig. 4.3 demonstrates the detailed sequence of steps in the proposed hybrid DPoS-PBFT consensus protocol for efficient and secure block validation among the UAVs.

### 4.5.1 Mechanism Overview

The mechanism is initiated by stake-based selection of the block proposer. The UAV generates a block and circulates it between the selected validators using the DPoS framework. Validators  $\mathcal{V}$ , which are assigned based on their UAV-specific metrics, authenticate a block. Approval by two-thirds of the 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 UAV  $i$  is assigned a validator score  $V_i$  calculated as

$$V_i = w_1 S_i + w_2 F_i + w_3 C_i + w_4 H_i, \quad (4.19)$$

where  $S_i$  represents the stake,  $F_i$  denotes the remaining fuel,  $C_i$  signifies 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 UAV  $i$  is given by

$$p_i = \frac{S_i}{\sum_{j \in \mathcal{V}} S_j}, \quad (4.20)$$

**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 no consensus was reached, a new view was initiated, potentially changing the proposed block. After detailing the consensus protocol, we describe the simulation setup used to evaluate the performance of our proposed approach. Table 4.1 compares the different consensus protocol options and their attributes relevant to UAV networks.

Table 4.1: Comparison of Consensus Protocols

Metrics	PBFT	DPoS	Hybrid
Speed	Low	High	Moderate
Throughput	Low	High	Moderate
Fault Tolerance	High	Low	Moderate
Permissioning	Private	Public	Configurable

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 and advancing UAV applications in emergency management. As outlined in Algorithm 2, the DPoS phase involves selecting validators based on the UAV stakes. An elected proposer creates a block that is verified by the validators. In the PBFT phase, valida-

**Algorithm 2** Blockchain-based UAV Coordination

---

```

1: Initialize: UAV  $u \in U$  has blockchain
2: for all  $u \in U$  do
3:    $u$  has blockchain height  $B$ 
4: end for
5: Propose Block: Rotating schedule
6: Select UAV  $P \in V$ 
7:  $P$  gathers transactions, creates & broadcasts block  $B + 1$ 
8: Verify Block:
9: for all  $v \in V$  do
10:  if  $v$  verifies  $B + 1$  valid then
11:     $v$  signs & broadcasts approval
12:  end if
13: end for
14: if approvals  $> (2/3)N$  then
15:   Add block  $B + 1$  to blockchain
16: end if

```

---

tors vote on the block. If insufficient votes are received, there is a change in view. Consensus through supermajority results in the addition of a block to the blockchain, thereby ensuring secure and efficient network operations. Specifically, Algorithm 3 combines DPoS and PBFT to achieve efficient decentralized consensus in UAV networks for disaster response scenarios. The DPoS phase selects validators and leader nodes based on delegated stakes to propose a block. If the faults exceed a certain threshold, PBFT is triggered for additional consensus through the preparatory and commit phases before finalizing the consensus on adding the approved block. The hybrid mechanism aims to balance efficiency, security, and fault tolerance for reliable coordination between resource-constrained UAV with intermittent aerial connections. The proposed architecture runs on a permissioned quorum chain, supporting privacy-preserving transactions between approved disaster response agencies by using durables. Each agency operates a local quorum node to maintain ledger copy. The interagency consensus uses a hybrid protocol. Among these 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 SC 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 such as GPS coordinates, along with transactions. Because JSON [121] formats used in SC languages inefficiently store spatial data, we incorporate geospatial Ethereum extensions, such as the FOAM protocol [122] to enable vector data storage. The 3D positions, boundaries, and disaster zones of the UAV can be encoded in GeoJSON to represent them as programmable objects. This allows for spatial queries for proximity alerts, geofencing, and coordinated navigation. To trigger location-aware executions, oracles provide disaster scenarios and situational data feed. Algorithm 4 presents a sample Solidity code for a SC that coordinates UAVs for search and rescue operations in a disaster-response scenario. It defines key parameters, such as the center of the

**Algorithm 3** DPoS-PBFT Consensus

---

**Require:** Set  $\mathcal{U}$  of  $N$  UAV nodes  
**Ensure:** Consensus on block  $B$

- 1: **Initialize DPoS**
- 2:   Delegate stakes and select leader  $l$
- 3:    $l$  validates and proposes block  $B$
- 4: **DPoS Execution**
- 5: **if**  $\geq \frac{2N}{3}$  validators approve  $B$  **then**
- 6:   Add  $B$  to blockchain
- 7: **else if** faults  $> \vartheta$  **then**
- 8:   Trigger PBFT consensus
- 9: **end if**
- 10: **Initialize PBFT**
- 11:    $l$  broadcasts  $B$ ; nodes validate and broadcast prepares
- 12: **PBFT Execution**
- 13: **if**  $\geq \frac{2N}{3}$  prepares **then**
- 14:   Nodes broadcast commit
- 15: **end if**
- 16: **if**  $\geq \frac{2N}{3}$  commits **then**
- 17:   Nodes add  $B$
- 18: **end if**
- 19: **Finalize Consensus**
- 20:   Update permissions, remove faulty nodes
- 21:   Add  $B$  if approved

---

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. Their comments explained the purpose of each function. This implements location-aware coordination logic to automate UAV search and rescue tasks via SC executed based on location data and events.

Algorithm 5 presents blockchain-based decentralized coordination among UAVs to achieve consensus on block additions. Each UAV is initialized using a blockchain ledger. A rotating schedule selects an UAV to propose the next block, gathering transactions and broadcasting the new block  $B+1$ . The other UAVs in the validator are set to check whether the block is valid, sign it, and broadcast approvals. When  $2/3$  approvals are received, a consensus is reached and the block is added to the blockchain. This achieves decentralized agreement on the appending of new blocks in a peer-to-peer manner, without a centralized authority.

## 4.6 Simulations and Discussions

### 4.6.1 Simulation Settings

In the context of our disaster management simulation, a  $25 \times 25$  km urban area severely affected by a natural disaster with extensive infrastructure damage forms the backdrop. This environment incorporates critical locations, such as a primary BS, a compromised BS in a power outage zone, an area under adversarial control, a disaster relief coordination hub, refugee camps, and essential medical facilities prioritized for aid delivery. The simulation involved a heterogeneous swarm of

**Algorithm 4** SearchAndRescue Contract

---

```

1: struct UAV
2:   id
3:   location
4:   battery
5:   status
6: Address owner
7: Location disasterZoneCenter
8: Radius searchRadius
9: UAV Location[] availableUAVs
10: function ASSIGNSEARCHGRID(UAV drone) ▷ Divide disaster zone into grids ▷ Assign
    grid to UAV for search & rescue
11: end function
12: function REPORTFINDINGS(Location location, FindingType type) ▷ Log findings
    (people, hazards) ▷ Notify authorities or UAVs
13: end function
14: function UPDATEUAVSTATUS(UAV drone, Status status)
    ▷ Update UAV status (battery, ops)
15: end function

```

---

200 drones, each equipped with autonomously functioning lithium-ion batteries. These drones, which are unique in terms of their identifiers and energy profiles, are equipped with navigation and networking sensors, processors, and A2A and A2G networking interfaces. They form a multi-tier mesh network 500 m above the ground, adhering to aviation safety protocols including collision avoidance systems. Key performance metrics evaluated include network performance, resilience against cyberattacks and malicious nodes, mobility and coordination of UAV flocks, packet delivery rate, and reliability.

The blockchain-enabled UAV coordination framework within this simulation achieved a throughput of 100 TPS, an average latency of 26 ms, and a packet delivery rate of 99.7%. The framework utilizes an DPoS consensus protocol complemented by PBFT for transactions that require immediate finality. The hybrid configuration balances resilience and computing demands with 20 DPoS delegates and five regional PBFT servers, thereby ensuring efficient and robust transaction processing. The simulation adheres to 3GPP standards for realism and industry alignment. It uses the 3GPP TR 36.777 urban macro-mobility model to emulate UAV mobility and 3GPP TR 36.842 for BS deployment. The communication models for the A2G and A2A links are 3GPP-compliant, encompassing probabilistic propagation for A2G and loss of the free-space path for A2A communications. The resilience to cyberattacks was validated by simulations of DDoS traffic, spoofing, and message tampering, with the system maintaining its stability under these conditions. In summary, this comprehensive simulation validates the applicability of the system to real-world disaster response scenarios, particularly where the ground infrastructure is compromised. The effectiveness of the architecture was further tested using UAV testbeds to confirm its real-world applicability.

Table 4.2: 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: 5s, Voting Margin: 66%
Node Distribution	DPoS Nodes: Globally, PBFT Nodes: Regionally
Finality	DPoS: Probabilistic, PBFT: Instant
Energy Use	Prioritize DPoS, Use PBFT for finality as needed
Throughput	Target: 100 Transaction 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 5** Blockchain-based UAV Coordination

---

```

1: Initialize: ▷ UAV  $u \in \mathcal{U}$  has blockchain
2: for each  $u \in \mathcal{U}$  do
3:    $u$  has blockchain height  $B$ 
4: end for
5: Propose Block: ▷ Rotating schedule
6: Select UAV  $P \in \mathcal{V}$ 
7:  $P$  gathers transactions, creates & broadcasts block  $B + 1$ 
8: Verify Block:
9: for each  $v \in \mathcal{V}$  do
10:   if  $v$  verifies  $B + 1$  valid then
11:      $v$  signs & broadcasts approval
12:   end if
13: end for
14: if approvals  $> (2/3)N$  then
15:   Add block  $B + 1$  to blockchain
16: end if

```

---

As seen in Fig. 4.4 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 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 between hundreds of UAV, which is necessary for wide-area post-disaster surveying. Linear throughput scaling to 500 nodes indicates 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.

Table 4.3: UAV Simulation Parameters

Parameter	Value
Total number of drones	200
Flock 1 (delivery services)	90
Flock 2 (connectivity support)	25
Flock 3 (monitoring)	85
Disaster region size	25 x 25 km
Total UAV networks 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
Pathloss exponent (n)	2.0

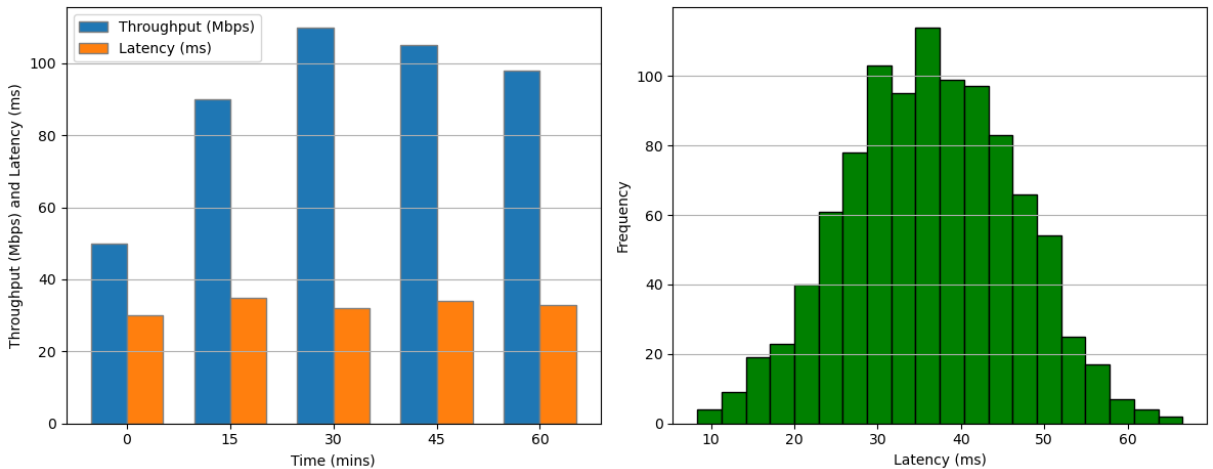


Figure 4.4: (a) Throughput, Latency over Time (b) Latency Distribution.

## 4.7 Novel DPoS-PBFT Consensus Results

This chapter presents a novel DPoS-PBFT consensus mechanism tailored for secure and reliable coordination of heterogeneous UAV fleets during disaster response. Extensive simulations modeled a  $25 \times 25 \text{ km}^2$  urban area impacted by a hurricane, with 200 drones meeting 3GPP NTN standards. The simulation environment consisted of 16 BSs positioned in a  $4 \times 4$  grid with a 10 km separation, four relief camps at city corners, and two adversary zones at opposite edges. The UAV fleet comprises 50 connectivity drones, 100 delivery drones, 25 search-and-rescue drones, and 25 damage assessment drones. UAV communications used a 915 MHz carrier with 1 W transmission power, 6 dBi antenna gains, and 10 MHz allocated bandwidth. The network topology included both aerial and ground links. UAVs had a maximum speed of 50 m/s with acceleration limits. We focus our evaluation on the benefits of blockchain, including decentralized coordination, resilience to cyberattacks, reduced tampering, and interoperability across agencies. The simulation results showed that the consensus architecture achieved 106 TPS throughput and

a median latency of 26 ms, satisfying the disaster response requirements. Despite the simulated DDoS attempts, GPS spoofing, and malicious tampering attacks, the framework exhibited less than 2% performance degradation in terms of throughput and latency, thereby highlighting its resilience. Analysis of Variance (ANOVA) testing revealed 15% longer latencies for rescue UAVs 20 km away from BSs compared to connectivity and delivery UAVs within 10 km proximity. Optimized clustering and routing policies are recommended based on UAV mission types and distances to the ground infrastructure. Overall, the results strongly validate the integration of blockchain technology to enable the secure, efficient, and reliable coordination of decentralized UAV fleets during disasters.

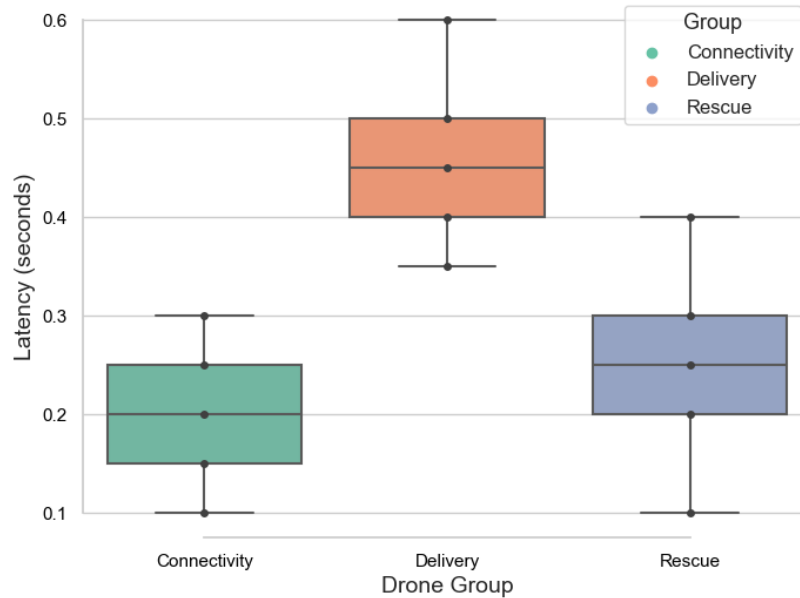


Figure 4.5: Latency Comparison of Consensus Protocols.

### 4.7.1 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, thereby demonstrating the system's capability to handle high traffic volumes seamlessly. In Fig. 4.5, we examined the latency variations across three different drone groups: Connectivity, delivery, and rescue. An ANOVA test was conducted to determine if there were statistically significant differences between the means of the three groups. The test yielded an F-statistic of 10.20 and a p-value of 0.003, indicating significant differences. Further post-hoc analysis is recommended to pinpoint the specific group



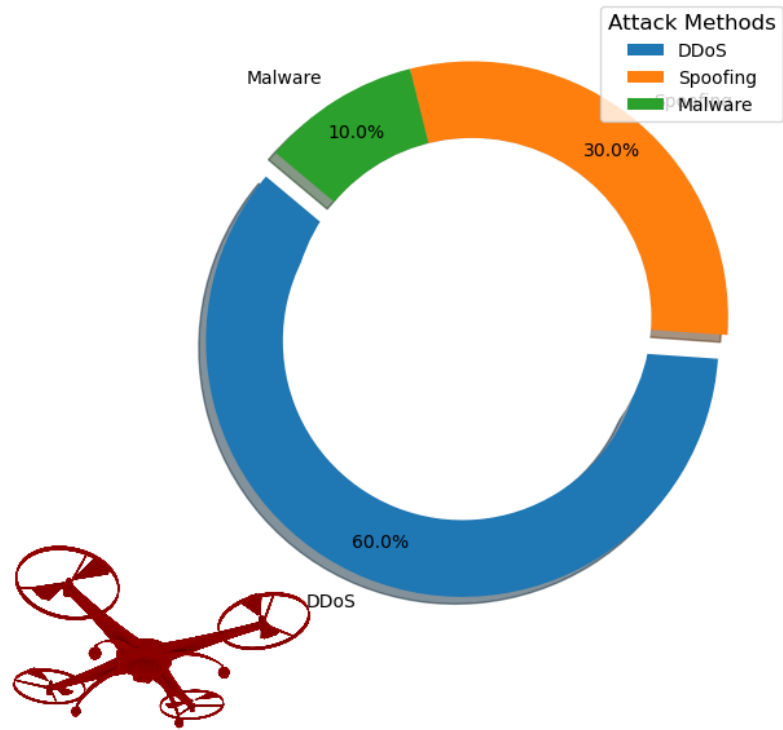


Figure 4.6: Resilience Comparison - Cyberattacks.

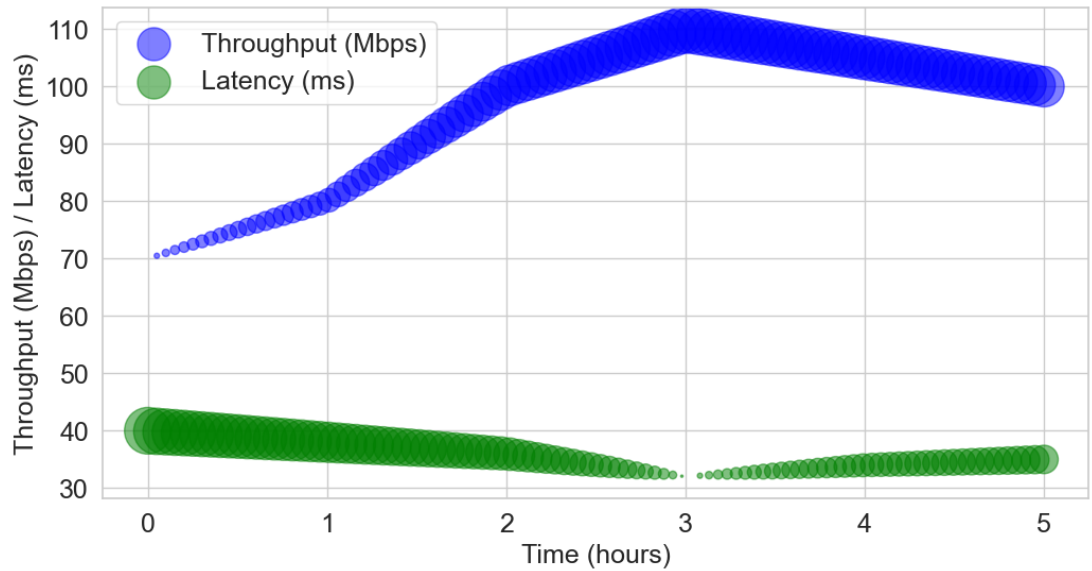


Figure 4.7: Throughput and Latency Over Time.

differences. The Fig. 4.6 highlights that displays the distribution of different attack methods used against a certain target, likely related to UAV (drone) networks given the presence of a drone image in the lower-left corner. The chart shows three categories of attack methods. DDoS represented by the blue section, which makes up 60.0% of the total attacks. Spoofing represented by the orange section, accounts for 30.0% of the attacks. Green section, which constitutes 10.0% of the attacks is for malware.

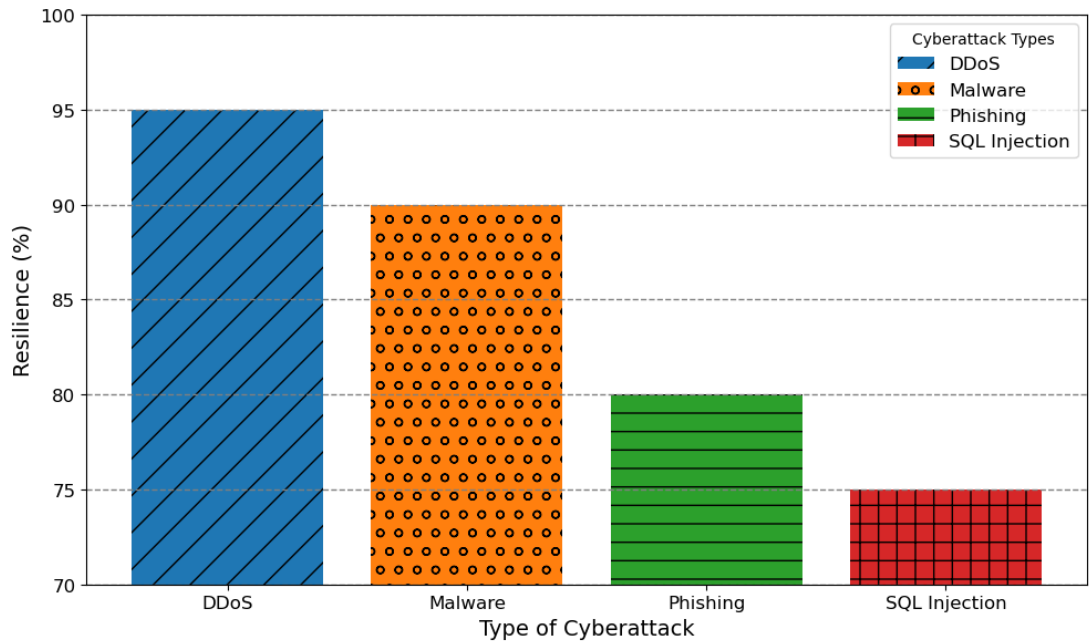


Figure 4.8: Resilience Against Cyberattacks.

### Latency Analysis

Fig. 4.7 reveals a lower median latency and tighter latency distribution for the consensus relative to DPoS and PBFT for different transaction loads. The mechanism balances DPoS swift block creation with rigorous validation of PBFT to minimize delays. Having detailed the proposed DPoS-PBFT consensus mechanism, we evaluated its performance for UAV coordination in disaster response scenarios through extensive simulations.

As shown in Fig. 4.8, the system maintains 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, at 75%. DDoS attacks were most effectively mitigated by 95%. The system also showed strong resilience to 90% of malware 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, which require further database server hardening. Insufficient end-user device protection is likely to explain higher phishing and malware effectiveness. Fig. 4.9 provides a scatter plot that visualizes the geographical distribution of UAV operations, categorized into Connectivity (blue), Delivery (orange), and Rescue (green) across different latitudes and longitudes. The x-axis represents latitude, indicating north-south positioning with values north of the equator as positive. The y-axis indicates longitude, showing east-west positioning with values east of the Prime Meridian as positive. The dispersion of points and their clustering patterns suggest variability in where these UAV operations are concentrated. The ANOVA results, with

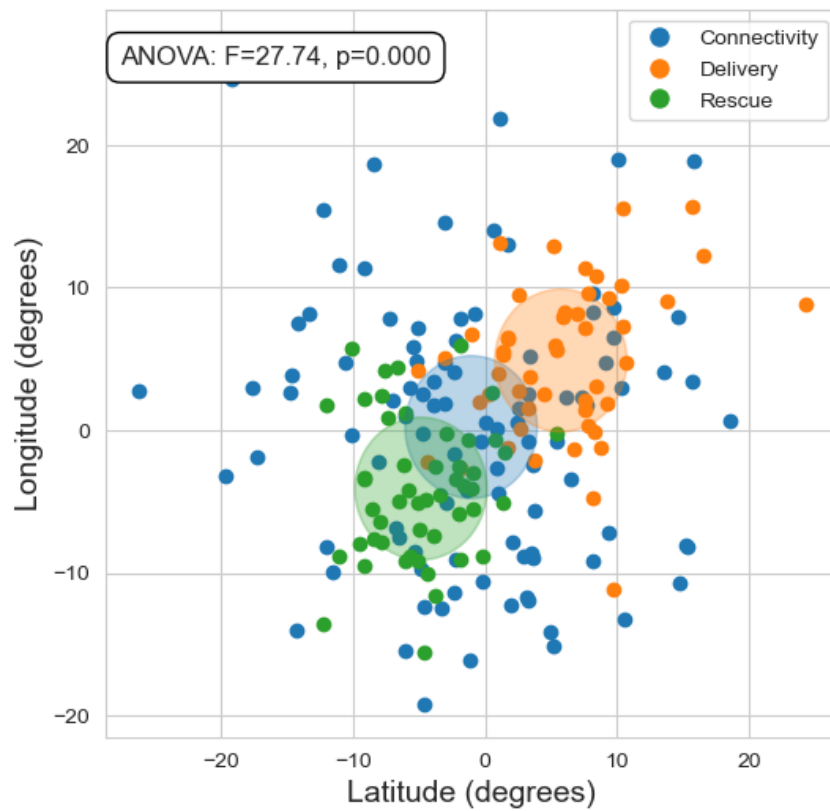


Figure 4.9: UAV Positioning Simulation with ANOVA Results.

an F-value of 27.74 and a p-value of 0.000, confirm statistically significant differences in the geographic distribution of these UAV operations, indicating distinct operational and logistical patterns that influence their deployment. Fig. 4.10 highlights the distribution of communica-

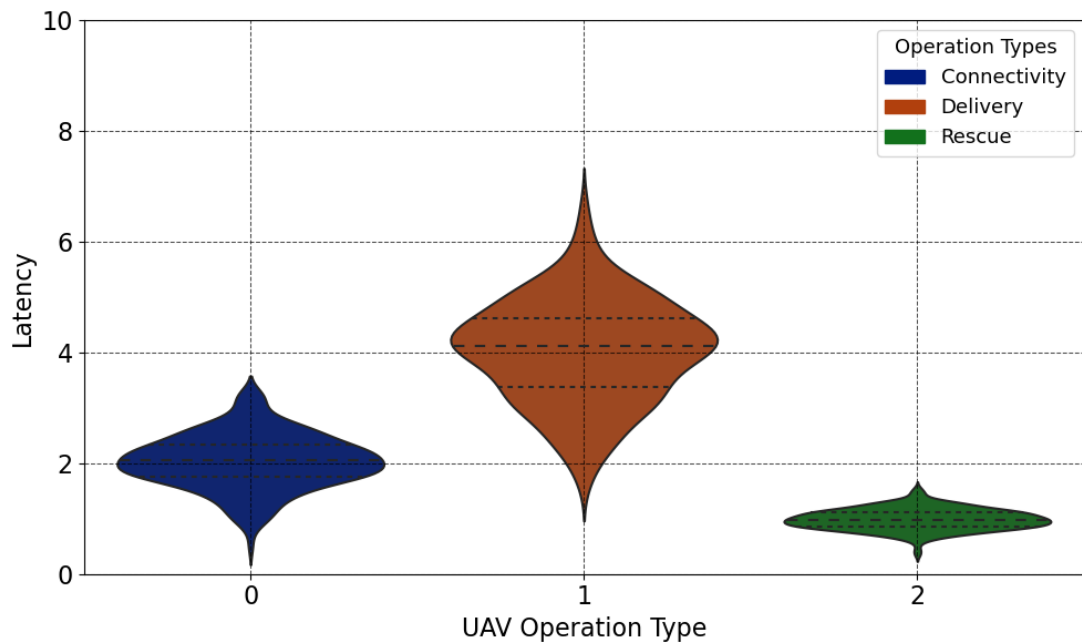


Figure 4.10: Distribution of Latency Across UAV Operations.

tion latency across UAV operational scenarios using violin plots. Latency remained under 10 ms in all cases, with a median value 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 a 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

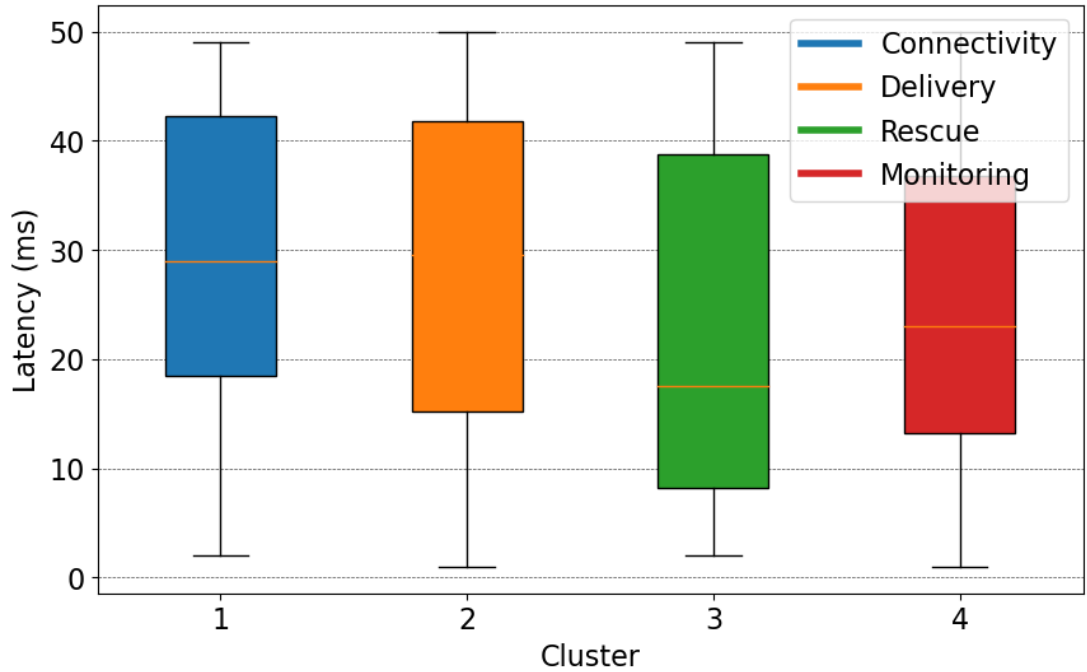


Figure 4.11: Within-Cluster Latency.

tracking. Minimal latency facilitates quick assessment. Network intelligence allows the self-optimization of the demands of each context.

In summary, the tuned latency distributions maintain medians of less than 5 ms for diverse UAV applications. Optimized profile shapes provide differentiated capabilities, allowing the network to conform to specific demands of post-disaster use cases through intelligent resource allocation. Fig. 4.11 compares within-cluster and across-cluster coordination communication latency. Within the 50-drone clusters, the latency ranges from to 1-50 ms (median 25 ms), enabling rapid in-group synchronization. In Fig. 4.12, across-cluster latency is higher at 50-100 ms between distant leaders, allowing necessary deconfliction. The divide profile validates efficient localized coordination within clusters while sustaining fleet visibility via across-cluster transactions. This hierarchy supports tight drone flocking and a high-level swarm oversight. In summary, the latency difference 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 a bifurcated latency that delivers both localized control and fleet coordination, which

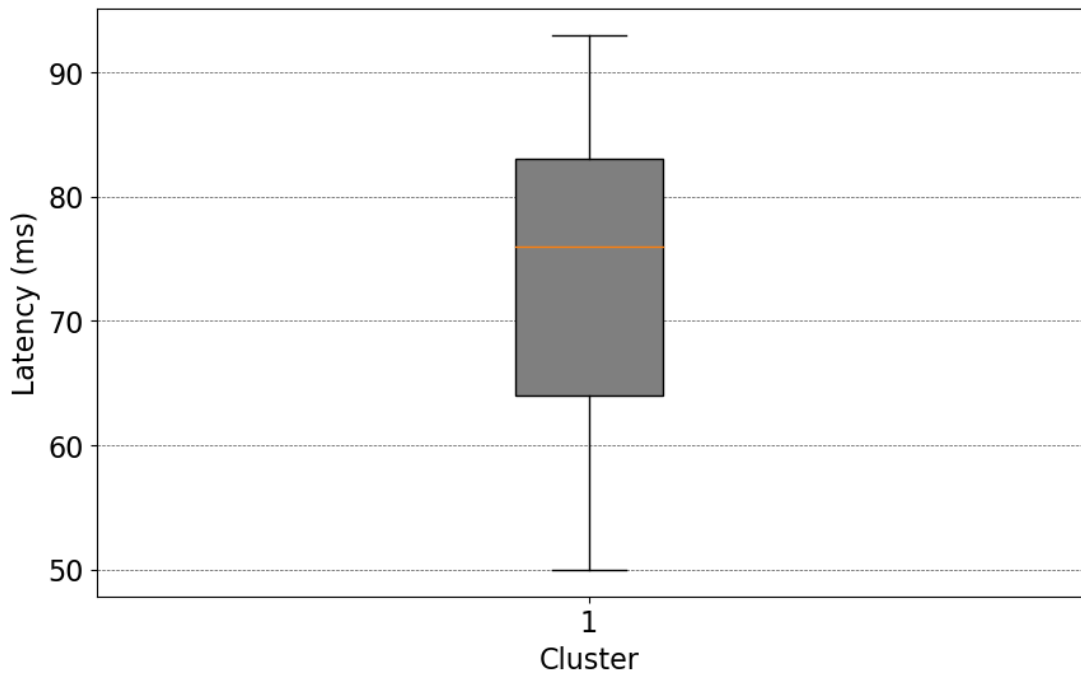


Figure 4.12: Accross-Cluster Latency.

is crucial for decentralized multi-UAV flocking at scale.

## 4.8 Conclusion

This study introduces a blockchain-based framework to enable the secure and efficient coordination of UAV networks for disaster response scenarios. The decentralized architecture enhances resilience against SPoF while overcoming limitations in autonomy, information sharing, and inter-agency collaboration. Key innovations include a consortium blockchain model that facilitates private and trusted data exchange across diverse stakeholders, an optimized hybrid DPoS-PBFT consensus protocol catered to resource-constrained UAV platforms, and bio-inspired flocking techniques for adaptable swarm coordination even with disrupted connectivity. Extensive simulations demonstrated the effectiveness of the integrated framework in improving transparency, scalability, reliability, and cyber-attack resilience during UAV-enabled emergency response operations with notable gains in throughput and latency metrics. Future research will focus on testbed validation and the incorporation of advanced technologies such as deep reinforcement learning, geospatial SC, and privacy-preserving data sharing. This study makes significant contributions towards reliable, intelligent UAV coordination for disaster management by synergistically combining distributed ledger technology, optimization, game theory, and collective autonomy.

### Linking the Chapters 4-5

1. *Progression to Practical Implementation*: Moving from the theoretical aspects of blockchain in UAV networks (Chapter 4) to the BIRDS framework's real-world applications (Chapter 5).
2. *Enhancing Concepts of Secure Coordination and Decentralization*: Building upon Chapter 4's foundational ideas like secure UAV fleet coordination and decentralization.
3. *Tackling Real-World UAV Delivery Challenges*: Utilizing blockchain capabilities established in Chapter 4 to address practical challenges in UAV delivery services.
4. *Paving the Way for Future Research and Development*: Sets the stage for further R&D by demonstrating blockchain's utility for UAV applications.

In Chapter 5, the focus shifts to the practical application of blockchain technology to optimize UAV delivery routes by introducing the BIRDS framework. This framework applies blockchain technology to essential UAV network operations, including authentication, registration, and node selection, building on the secure authentication schemes detailed in Section 3 for UAV authorization. BIRDS incorporates a novel Proof-of-Competence (PoC) consensus mechanism, using UAV-specific blockchain design and reputation scores to ensure efficient operation. This chapter also goes through strategies for optimizing the energy consumption within the UAV delivery network and utilizes UAV reputation scores to enhance the reliability of data transmission and resource allocation. This approach is underscored by presenting results demonstrating the effectiveness and efficiency of the BIRDS framework in real-world UAV delivery scenarios.

# Chapter 5

## Blockchain-Empowered Delivery Service

This chapter proposes a novel framework called BIRDS to address security and reliability challenges in UAV-assisted delivery services. BIRDS leverages blockchain technology to enable secure, decentralized, and cooperative communication among UAVs. The framework comprises four main stages: (1) secure UAV registration, (2) blockchain consensus inspection, (3) UAV node selection, and (4) reputation score assignment. In the registration phase, UAVs are registered with details, such as node ID, size, weight, battery capacity, flight duration, and travel distance. This is followed by a blockchain consensus stage in which a novel PoC consensus mechanism is introduced to ensure scalability and energy efficiency.

The PoC consensus mechanism evaluates UAVs based on their credibility, considering factors such as the timestamp, Proof-of-Identification (PoI), Proof-of-Resources (PoR), and the delivery time. The chosen UAV is awarded a certificate for the BIRDS global order fulfilment system. The node selection phase involves joint optimization considering the cost, arrival time, expected delivery time, PoI, PoR, and the reputation score. The chapter also discusses energy consumption in BIRDS, introducing a reward function designed to reduce system-weighted costs and optimize device energy provision. Additionally, the BIRDS reputation score is influenced by factors such as actual delivery time, delivery cost, carrying capacity, and certificate value, ensuring reliable UAV selection.

The simulation results demonstrate that BIRDS requires fewer UAV than conventional solutions, resulting in reduced costs and emissions. The proposed framework caters to the requirements of multiple users while requiring less network traffic and consuming low energy. The Chapter concludes by discussing limitations and future research directions, such as real-world large-scale evaluations, ML integration, diverse aerial vehicle support, edge computing integration, and reputation system enhancements.

Exploiting UAV for delivery services is expected to reduce the delivery time and human resource costs. However, the proximity of these UAV to the ground can make them ideal targets for opportunistic criminals. Consequently, UAV may be hacked, diverted from their destinations, or used for malicious purposes. Furthermore, as a decentralized (peer-to-peer) technology,

blockchain has immense potential to enable secure, decentralized, and cooperative communication among UAVs. With this goal in mind, we propose a BIRDS framework to address data-security challenges. BIRDS deploys communication hubs across a scalable network. Following the registration phase of BIRDS, UAV node selection is performed based on a specific consensus proof of competence PoC, where UAV is evaluated solely based on its credibility. The chosen finalist is awarded a certificate for the BIRDS global order fulfilment system. The simulation results demonstrate that BIRDS requires fewer UAV than conventional solutions, resulting in reduced costs and emissions. The proposed BIRDS framework caters to the requirements of numerous users, while requiring less network traffic and consuming low energy.

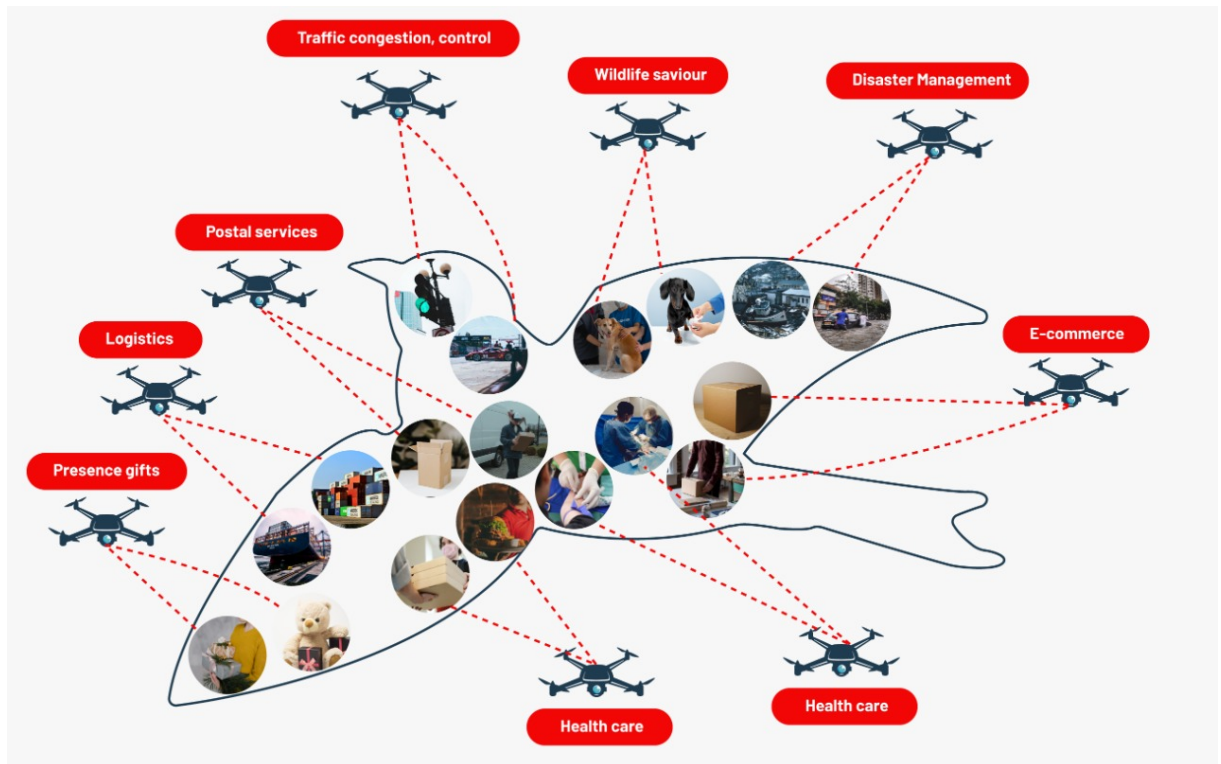


Figure 5.1: Applications of UAV Delivery Services.

## 5.1 Introduction

Owing to its efficiency and high mobility, UAV performs essential tasks including search and rescue, remote sensing, and delivery [123]. Anticipating a logistical challenge in achieving rapid and cost-effective delivery, commercial enterprises are increasingly exploring drone technology to reduce the delivery time and cost. UAV deployment proves efficient for final-mile delivery, considering environmental and economic factors, making it a promising aerial solution [5].

Traditional delivery vehicles have become infeasible because of the high fuel costs, city problems, and environmental consequences of urban distribution problems [124]. Recently,



UAV has been poised to play a pivotal role in achieving the efficient and swift delivery of services by employing the distinct attributes of high mobility, adaptable deployment, and cost-effectiveness. Their mobility also positions the UAV as an airborne communication platform, enhancing the connectivity for ground-based operations. Nevertheless, UAVs can serve as intermediaries connecting ground users and spacecraft through LoS channels, suggesting a pivotal role for communication-based UAVs in 6G networks. A substantial power-consumption challenge in wireless networks, particularly for long-distance transmissions with notable path losses, has been acknowledged. The constrained power capacity of small UAV has further propelled recent research interest in the realm of environmentally conscious UAV communication [26]. Despite recent discussions on solutions [9]– [38], the privacy and security aspects remain incomplete. A significant challenge in UAV-enabled delivery services is the potential exploitation of malicious actors via hacking and malware [83]. A promising solution for addressing these issues is the involvement of blockchain. As a distributed decentralized network, the blockchain provides user privacy, immutability, transparency, and reliability [103]. Moreover, blockchains incorporate many desirable properties of back-end solutions, including decentralization, redundancy, fault tolerance, security, and scalability. As in the research area of UAVs, the application of conventional blockchains is a significant problem because multiple nodes are already resource-constrained UAVs. In [25], we introduced BETA-UAV blockchain-based efficient authentication for secure UAV communications. The objective is to enable mutual authentication and freshness identification, such that the UAV network can establish secure communication channels. PoF or authentication protocols allow UAVs to integrate with these systems with minimal hassle and maximum security.

Following this, [125] created a robust and lightweight authentication and key agreement scheme for a cloud-assisted UAV using a blockchain in a FANET to guarantee data-sharing decentralization and integrity. By streamlining these challenges, the proposed BIRDS framework can be used as an innovative solution to overcome them. The BIRDS framework uniquely integrates UAV registration, blockchain-based authentication, node selection, and reputation scoring to enhance the scalability, energy efficiency, and security. This distinguishes it from the state-of-the-art methods, as confirmed by rigorous simulations, by offering an innovative solution that combines privacy, security, and UAV operational efficiency. The BIRDS framework provides end-to-end security spanning rigorous authentication, optimized node assignment, and performance-based reputation management to enable safe, dependable, and energy-efficient delivery operations. The main contributions of this study are summarized as follows:

- We develop the BIRDS framework, which endures a detailed verification and registration, benchmark comparison, and eventual PoC generation, and provides solutions to traditional overheads.
- We introduce PoC as an advanced and credible consensus mechanism, ensuring both scalability and energy efficiency.

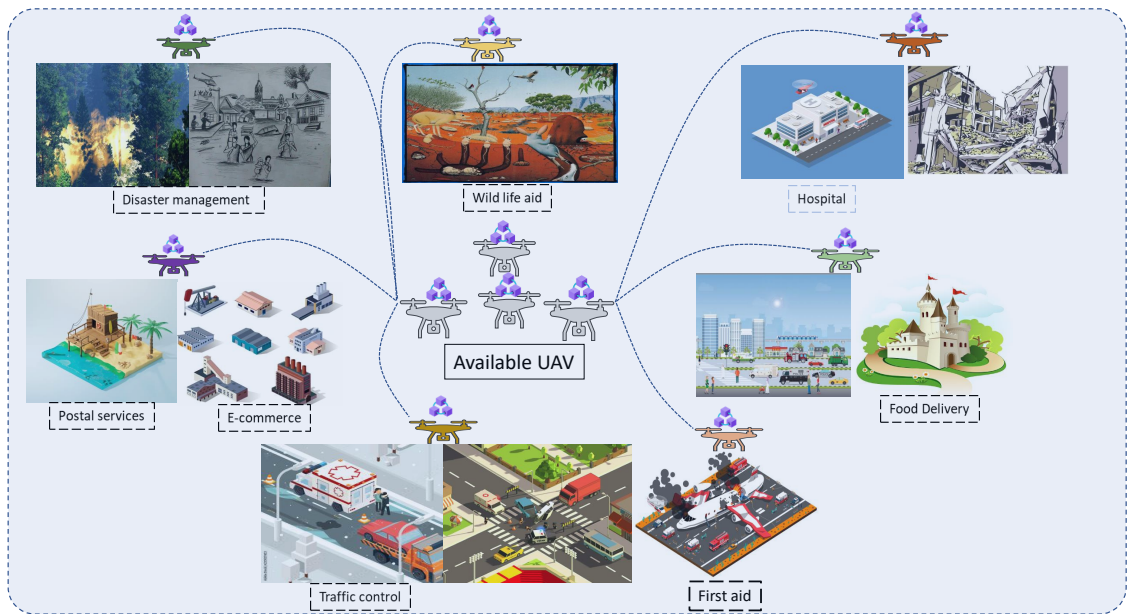


Figure 5.2: Blockchain-Assisted UAV Delivery Services.

- BIRDS consists of four stages: Initiating with secure UAV registration, it proceeds to blockchain consensus inspection, ensuring dual security for both UAVs and user-side registration. Subsequently, UAV node selection was involved, culminating in awarding a reputation score.
- We examine the novelty of our approach through competency and reputation scores. UAV node selection relies on key parameters: Timestamp, PoI, PoR, and delivery time.
- Finally, we perform numerical simulations to evaluate the performance of BIRDS compared with classical blockchain consensus algorithms and demonstrate its supremacy in delivery time and energy consumption.

The remainder of this chapter is organized as follows. Section 5.2 covers the system model and problem description of the UAV network, communication, and mobility models. Section 5.3 introduces the proposed BIRDS scheme, which briefly covers all the BIRDS insights. The results and discussion are explained in Section 5.4 and the conclusions are presented in Section 5.5.

## 5.2 System Model and Problem Description

Section 5.2 presents and explains the specifics of the system modelling and framework, covering all three aspects: the UAV network, communication, and mobility models.

Table 5.1: List of Notations

Notations	Descriptions	Notations	Descriptions
$\mathcal{U}$	UAV array	$\mathcal{Q}$	Channel resources set
$\mathbb{I}$	Set of users	$\mathbf{k}_v$	Average riding speed/velocity of UAV $v$
$\mathcal{D}$	Group of delivery data	$d, q$	Data packet, Coverage
$\mathbf{E}_u^R$	UAVs leftover energy of $R$ and $u$	$f_u^d$	Flying distance between $d$ and $u$
$h_i^q$	Channel power gain between $i$ and $q$	$p_i^t$	Transmission power among $i$ and $t$
$\gamma$	Additive white Gaussian noise	$L_u^i$	Link among UAV $u$ and user $i$
$\mathbb{B}$	Channel Bandwidth	$\mathcal{S}_i^u$	User's achievable transmission rate
$H_U^e$	UAV hovering expenditure of $e$ and $U$	$f_U^e$	Flying usage of UAV between $e$ and $U$
$\gamma^h$	Hovering energy used per unit time	$\gamma_f^p$	Cost of energy per unit distance traveled
$e_u^T$	Total energy consumption of UAV	$W(r), i(r)$	Weighted reward and each user reward
$\tau_i^d$	Transmission delay for delivering data	$\mathbf{E}_u^{\max}$	Maximum potential energy
$S_i$	Parameter of satisfaction degree	$\chi_0$	Timeline of for delivering data
$\mathcal{U}_i(s_i^c)$	Utility of UAV for delivering data	$\delta(r)$	Reward for successful consensus
		$\mathcal{D}_i(s_i^c)$	Utility of user for delivering data

### 5.2.1 UAV Network Model

In Fig. 5.1 the applications of UAVs, and in Fig. 5.2 the BIRDS delivery scenario involves adapting the ground infrastructure for diverse deliveries, which leads to communication complexities. Mobile network operators strategically deploy ABS and are equipped with UAV to facilitate efficient communication and data delivery services to individuals within UAV networks. Table 5.1 summarizes all relevant notations used in this section.

**UAV Selection:** UAVs deliver communication and data services from the air when a UAV delivery service is launched. BIRDS selects a credible UAV node so that the UAV behaves according to the ground infrastructures, Let  $\mathcal{U} = \{1, \dots, u, \dots, U\}$  denote the UAV array.

**Customers:** Users access cellular networks in emergency or disaster zones for delivery operations, and massive amounts of high-value data on wireless devices are at risk. Therefore, users require communication and data delivery services to reduce the risk of data breach.  $\mathcal{I} = \{1, \dots, i, \dots, I\}$  denotes the set of users in the study area, To permit users to communicate with UAVs, we consider large-scale emergency networks or a symmetric directed graph, where  $N$  is the group of nodes, that is, UAVs and users.

### 5.2.2 Communication Model

Every UAV creates multiple communication channels, and the series of channels within UAV's coverage is denoted by  $\mathcal{Q} = \{1, \dots, q, \dots, Q\}$ . Multiple users can simultaneously access the channels; consequently, channel interference from other users occurs during the data delivery. The signal-to-interference-plus-noise ratio (SINR) between user  $i$  and UAV  $u$  can be calculated

as follows.

$$\zeta_i^u = \frac{p_i^t h_i^q}{\sum_{i \in \mathbb{I}} h_i^q p_i^t + \gamma}. \quad (5.1)$$

where  $\gamma$  is Additive white Gaussian noise. Consequently, the available user transmission rate on track  $p$  for data delivery decreased by  $u$ . The user's achievable transmission rate can be expressed as

$$T_i^u = \mathbf{B} \log(1 + \zeta_i^u), \quad (5.2)$$

The delivery of a set of data packets is denoted as  $\mathcal{D} = \{1, \dots, d, \dots, D\}$ . The data size transmitted by user  $i$  is denoted as  $s_i^d$ .  $G$  represents the total amount of data delivered within the UAV's coverage area  $\sum_{i \in \mathcal{I}, d \in \mathcal{D}} \{S_i^d\}$ . UAV hovers in a specific spot through data delivery, and its altitude determines the effects of data delivery. Transmission delay in delivery of data UAV hovers in a fixed location during data delivery and the transmission delay for delivering data is determined by its altitude, where the transmission delay is shown by

$$\chi_i^d = \frac{s_i^d}{T_i^u}. \quad (5.3)$$

The data transmission delay  $\mu$  outperformed the target time. The target time for  $\mu$  is given by  $T^0$ , which indicates that data cannot be delivered if the transmission delay exceeds  $T^0$ . The primary role of BIRDS is to differentiate autonomously between reliable and unreliable UAV delivery channels in a decentralized manner. Specifically, the architecture employs SC to facilitate the initialization and registration of UAV or clients.

### 5.2.3 Mobility Model

The mobility model of a UAV incorporates communication and data delivery services. The UAV flight path consists of multiple distinct points in a three-dimensional Cartesian coordinate system. The velocity of a UAV is denoted by  $\mathbf{k}_v = \{k_v^x, k_v^y, k_v^z\}$ ,  $\forall u \in \mathcal{U}$ . Here,  $k_u^x, k_u^y$ , and  $k_u^z$  represent the specific speeds of the UAV in the 3D Cartesian coordinates. A UAV's flying distance can be calculated as

$$f_u^d = \tau_u^f \|\mathbf{k}_u\|_2, \forall u \in \mathcal{U}, \quad (5.4)$$

where  $\tau_u^f$  denotes the UAV flight duration of the UAV. Here, the energy consumed by a UAV is  $e_u^T$ , which depends on the flight power  $\sigma$ , and the hovering expenditure is represented by  $\mathbb{H} = \gamma^h \tau_i^d$ . Accordingly, the overall energy consumption of UAVs that provide users with data and communication delivery services can be expressed as

$$e_u^T = \sigma + \gamma^h \tau_i^d, \quad (5.5)$$

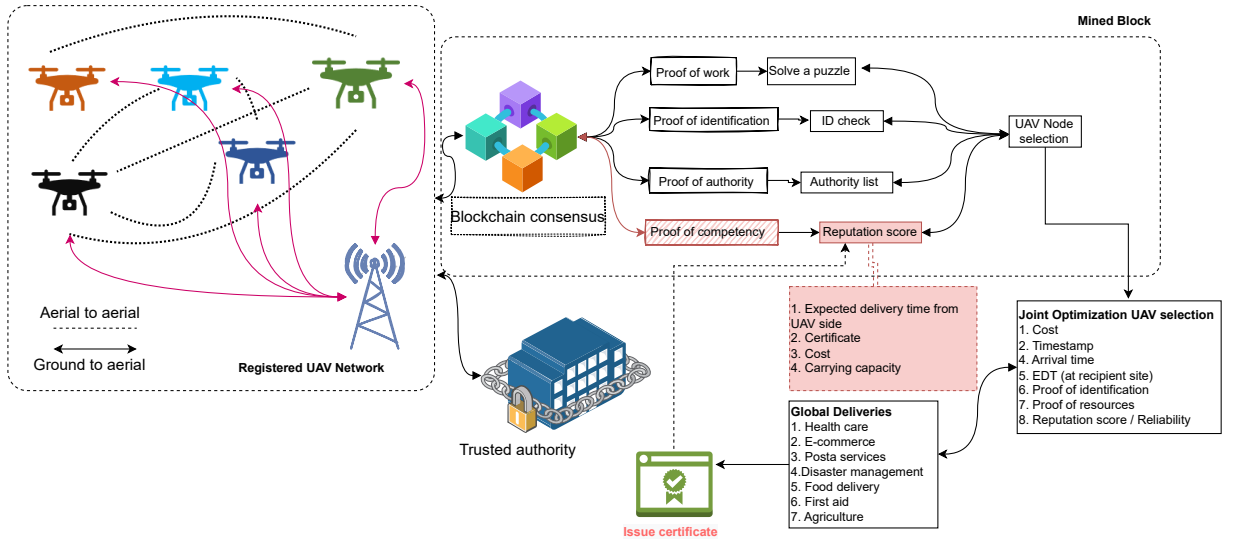


Figure 5.3: BIRDS Framework.

For UAVs to be able to return for recharging, their remaining energy must exceed a predetermined threshold

$$E_u^R > E_u^{\text{thr}}. \quad (5.6)$$

## 5.3 Proposed BIRDS Scheme

Based on the network model explained in Section 5.1, we present BIRDS, a decentralized framework designed to identify feasible UAV delivery routes. BIRDS comprises three primary contracts: Registration of UAVs, TA, and registered UAV identities. In addition, we exploit the subsequent blockchain consensus stage, along with an automated delivery tracker or UAV reputation score, to execute the third BIRDS phase, which involves UAV node selection for optimal job assignment.

### 5.3.1 Authentication and Registration Phase of BIRDS

The initial stage of the BIRDS framework involved UAV authentication and registration. In a network comprising 20 UAVs, each UAV is registered with details, including node ID, size, weight, battery capacity, flight duration, and travel distance. BIRDS supports both A2A communication and A2G delivery, as presented in Fig. 5.3. The red lines represent the A2A communication links between UAVs, indicating how they communicate during the flight. The different colors assigned to the UAVs signify their states: green, readiness, blue, information transmission, orange, queuing, black, registration entry, and waiting. Once registration is complete, participants proceed to the subsequent phase, focusing on security and privacy, which are fundamental attributes of BIRDS.

### 5.3.2 Proof-of-Competence in BIRDS

The BIRDS framework introduces PoC as a novel consensus mechanism tailored to address specific challenges in blockchain-empowered UAV networks. Unlike traditional consensus mechanisms like Proof-of-Work (PoW) or PoA, PoC is designed to ensure that only UAVs that meet certain competency criteria are selected for tasks.

#### Key Attributes of PoC

- **Cost:** This involves evaluating the financial implications of selecting a particular UAV for a task. The UAV with the least cost implication is often preferred, provided other competencies are met.
- **Timestamp:** This is used to log the precise timing of UAV operations, ensuring that transactions and deliveries are timestamped accurately for transparency and accountability.
- **Arrival Time:** This refers to the expected arrival time of the UAV at the recipient site. It is crucial for ensuring timely deliveries, especially in scenarios like healthcare and disaster management.
- **Expected Delivery Time (EDT):** This metric evaluates the UAV's ability to deliver within a specified time frame, ensuring efficiency and reliability in the delivery process.
- **Proof of Identification:** Ensures that the UAV is properly authenticated and authorized to perform the task. This prevents unauthorized UAV from participating in the network.
- **Proof of Resources:** Verifies that the UAV has sufficient resources (battery life, carrying capacity, etc.) to complete the delivery without interruption.
- **Reputation Score / Reliability:** This score is a composite metric derived from previous performance data, including successful deliveries, adherence to schedules, and overall reliability. UAV with higher reputation scores are prioritized.

The PoC consensus mechanism in the BIRDS framework ensures that UAV selected for delivery tasks are not only authenticated and authorized but also evaluated based on their competency in terms of cost, energy efficiency, reliability, and other critical factors. This approach enhances the efficiency, reliability, and security of the UAV delivery network, making it a robust solution for various applications ranging from healthcare to disaster management.

### 5.3.3 BIRDS Criteria for Miners

The key aspects of BIRDS blockchain design are as follows. The BIRDS framework uses a customized blockchain structure to enable a secure and reliable UAV delivery. Several architectural

choices in BIRDS blockchain design aim to enhance security, efficiency, and reliability. First, the block identification mechanism uniquely labels each block to avoid ambiguity and enable tracking. BIRDS *ID* assigns a distinct identifier to each block added to the chain. Second, BIRDS employed cryptographic hashing techniques to guarantee the integrity of blockchain data. A Merkle tree root hash securely consolidates all the transaction hashes into a final checksum. This preserves validity across blockchain updates. Third, chaining hash pointers chronologically link blocks through one-way cryptographic hashes. Each new block contained the hash of the previous block, thereby creating an immutable event record. The chaining of hashes also allows for an efficient data lookup. Furthermore, the accurate timestamping of blocks through BIRDS timestamps maintains an auditable timeline of blockchain activity. Timestamps enable sequence-to-block generation.

In addition, BIRDS allows variable transaction sizes through customized block headers and transaction lists. This provides flexibility and efficiency in block creation and chaining. Finally, the consensus mechanism in BIRDS was designed for scalability by using tweaked difficulty levels and hash requirements. This is critical for enabling low-latency confirmation of blocks.

### 5.3.4 Credibility of UAV Node Selection

In the BIRDS framework, after populating the blockchain with anonymized UAV data and encrypting the device data, an attacker leverages ML on the blockchain. To enhance privacy, we propose techniques such as multi-node ledgers, transaction delays, and confusion occurrence using cryptographic methods such as blind and ring signatures. UAV communication transactions are initiated by nodes, which can be data-empty or encrypted, ensuring adherence to communication protocols. Registered UAVs must validate their prior identity for a new one, addressing challenges. The selected UAV gains reputation scores, prioritizing reputable UAVs for the subsequent task allocation.

### 5.3.5 Energy Consumption in BIRDS

BIRDS aims to improve the sustainability of blockchain systems by mitigating energy-intensive miner operations, a primary contributor to overall consumption. Energy usage, quantified by the power of the framework, impacts work efficiency. Based on this concept, the energy consumption of the individual miners can be calculated as follows

$$E_{\eta} = \frac{E_u}{E_T}, \quad (5.7)$$

$E_{\eta}$  represents the energy efficiency of the UAV node/miner in the proposed BIRDS framework. So,  $E_{\eta} = \frac{E_u}{E_T}$  gives the ratio of the individual UAV's energy consumption to the total system energy consumption. This ratio essentially represents the energy efficiency of that particular

UAV node/miner within the overall BIRDS system. A lower value of  $E_\eta$  means the UAV is more energy efficient, consuming less of the total system energy for its operations compared to other UAVs. The BIRDS framework aims to optimize and improve this energy efficiency metric across UAV nodes in the delivery network.

$$E_T = \frac{e_u^T}{E_{max} - E_u}, \quad (5.8)$$

$$e_u^T = \frac{P^T}{E_u^{max} - p_i^t}, \quad (5.9)$$

where  $e_u^T$  represents the total energy consumption of the UAV and  $E_u^{max}$  is the maximum potential energy.

The reward function in BIRDS is designed to reduce system-weighted costs and optimize the device energy provision, thereby helping to make better judgments. In this work, we specify the instant rewards as

$$I(r) = \begin{cases} \delta(r) - k \cdot \frac{W(r)}{i(r)} - \rho(r), & \text{if } UAV_n(r) \leq t_l \\ -k \cdot \frac{W(r)}{i(r)} - \rho(r), & \text{if } UAV_n(r) > t_l \end{cases}, \quad (5.10)$$

where  $\delta(r)$  represents the rewards for successful consensus if the consensus is shorter than the time limit. Moreover,  $k$  is the weighted coefficient of the system cost. Finally,  $\rho(r)$  denotes the penalty rewards and is given as

$$\rho(r) = p \frac{\mathbf{E}_u^{avg} - \mathbf{E}_u^R}{\gamma^f}, \quad (5.11)$$

where  $p$  is the penalty index that defines the ratio of rewards in the penalty  $n$  reward function,  $\mathbf{E}_u^{avg}$  represents the average energy of all the devices, and  $\gamma^f$  represents the energy consumed per unit time during hovering.

### 5.3.6 UAV Reputation Score in BIRDS

Within the BIRDS communication framework, consistent data transmission is essential for block commitment and resource allocation is required for block adoption. Delays in block commitment can arise from technical factors such as constrained bandwidth, computational resources, restricted throughput, and public blockchain latency.

$$Rep_i = EDT + Cv + cost + K, \quad (5.12)$$

In this context, we define  $Cv$  as the certificate value and  $K$  as the carrying capacity. Furthermore, consensus among UAV nodes regarding the ledger state is imperative. Thus, BIRDS solutions have been introduced to address these complexities.

Our model ensures a dynamic reputation set for reliable UAVs. The BIRDS reputation score



is influenced by factors such as actual delivery time (*ADT*), delivery cost, carrying capacity, and  $C_v$ . Initial scores of zero were assigned to unverified sources with the ability to change over time. In a registered drone network, drones are categorized by mission (e-commerce, emergency communication, delivery services, healthcare, etc.) based on attributes such as size, cost, and power consumption. The selected drone overcomes these obstructions and receives a reputation score and certificate, thereby contributing to the BIRDS framework of the UAV pool.

## 5.4 Results and Discussion

The simulation was conducted using MATLAB, where we modelled the behaviour of 20 UAVs with diverse capabilities, considering factors such as payload, velocity, and flight duration. We analyzed 20 UAVs with diverse capabilities, assuming universal low-altitude takeoff and landing. Each UAV exhibited a capacity ranging from 1 kg to 15 kg, achieved at velocities between 400 mph and 100 mph across different payload capacities. In particular, a fully charged drone operating at maximum payload one-hour flight for one hour. In the 100 km<sup>2</sup> region, we considered 80 randomly spaced waypoints. The evaluation of the effectiveness and design of our strategy is based on three established metrics: energy efficiency, reputation score, and scalability. The analysis reveals that the energy consumption of the BIRDS increases with increasing

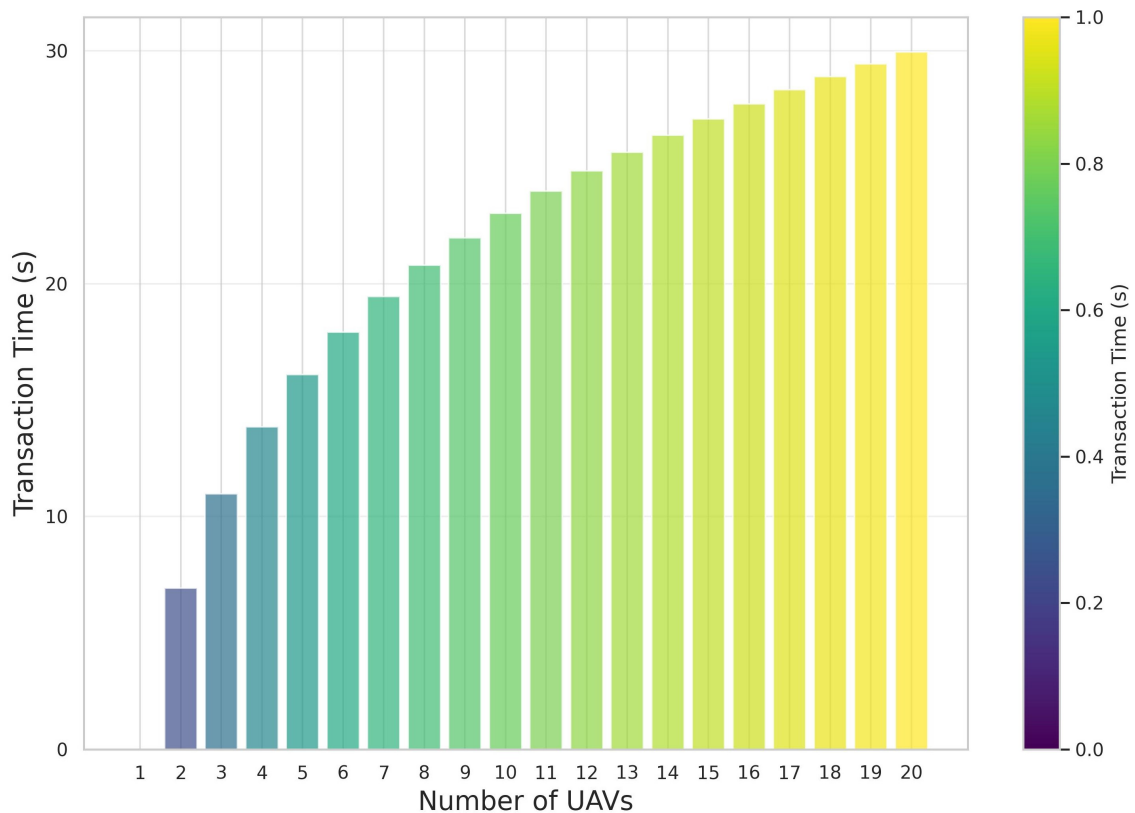


Figure 5.4: Blockchain Transaction Time vs Number of UAVs.

speed and time. Notably, lower speeds significantly reduced energy use, highlighting the trade-off between efficiency and speed. This information is vital for optimizing the balance between energy conservation and operational speed during the BIRDS deployment. The overall trend suggests that more UAVs in the system lead to longer transaction times, which may imply scalability issues in the blockchain system when dealing with a larger fleet of UAVs, as shown in Fig. 5.4. Fig. 5.5 displays the job count (deliveries) on the x-axis and the delivery time on the y-axis.

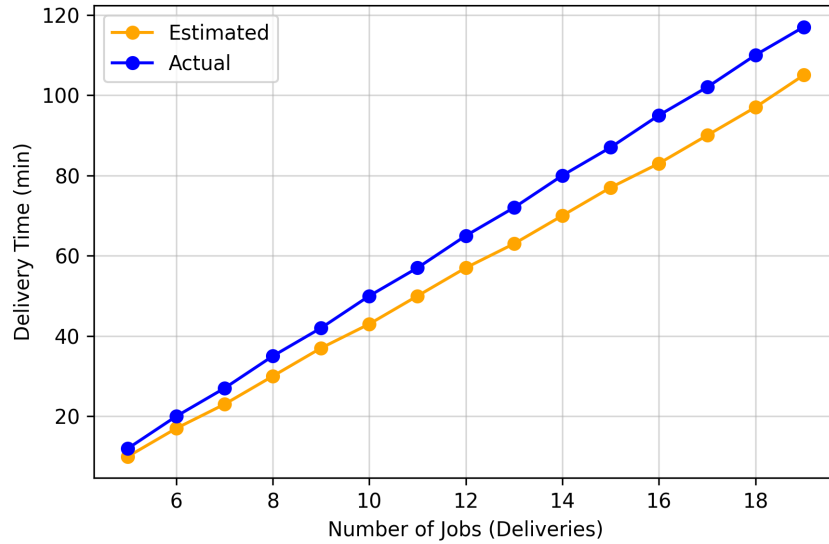


Figure 5.5: Estimated and Actual Delivery Time for UAV Tasks.

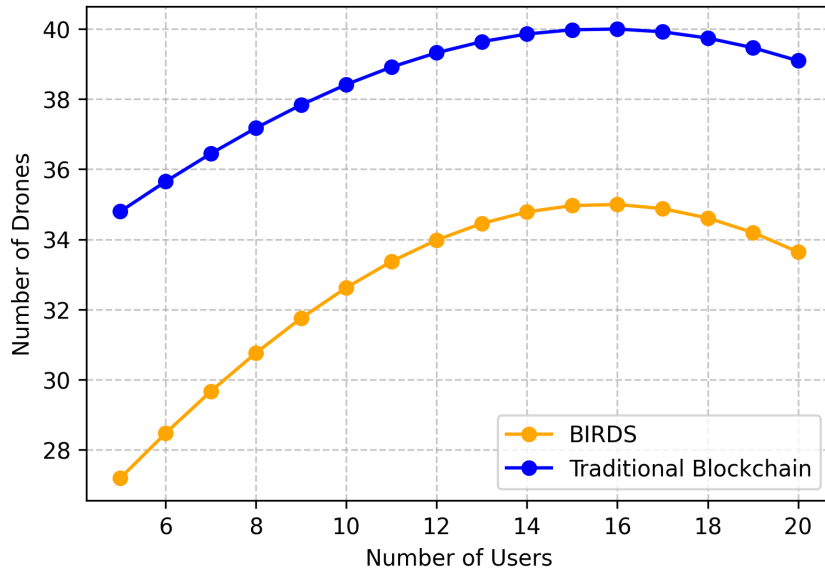


Figure 5.6: Traditional Blockchain vs BIRDS.

Efficient initial job processing created a bottleneck beyond 15 jobs. The effectiveness of PoC across various consensus mechanisms addresses these issues. Fig. 5.6 presents an efficiency comparison between the BIRDS framework and traditional blockchains (PoW, PoA) as the user

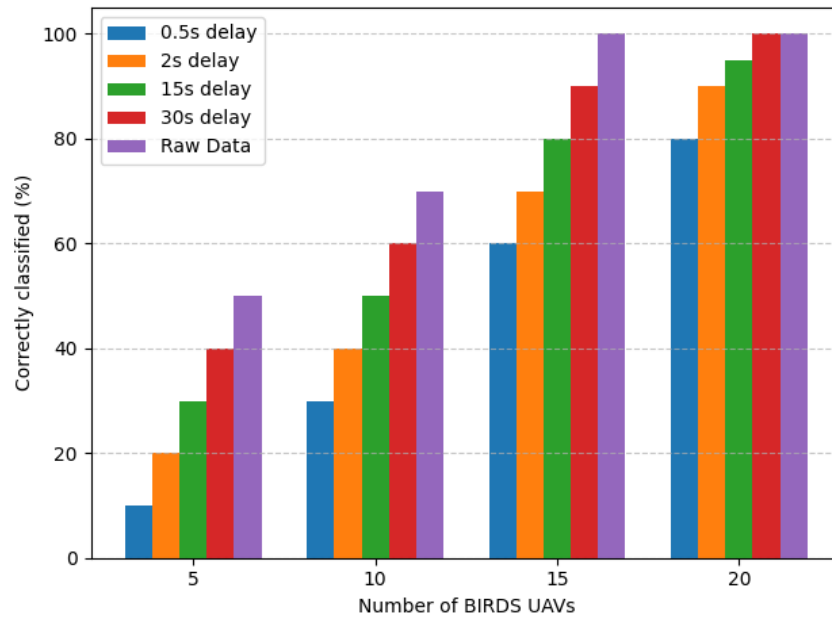


Figure 5.7: Impact of the Number of UAVs on the Delay.

count increases. Remarkably, the BIRDS network requires fewer UAVs under heightened user loads, highlighting its ability to manage multiple users while effectively mitigating network congestion. As conveyed in Fig. 5.7, this matrix effectively reduces the associated probability. However, the presence of communication delays can negatively affect accuracy, emphasizing the need for efficient data processing and communication protocols in UAV networks to maximize their operational effectiveness.

The variation in the UAV node count per ledger (x-axis) demonstrates significant accuracy in initially categorizing the device speeds, particularly with two or four devices. The success rate exceeded 50% when employing more than 15 UAVs.

## 5.5 Conclusions

This study introduced the BIRDS framework, an innovative lightweight blockchain solution that enables secure and reliable UAV delivery services. Through rigorous analysis, BIRDS demonstrated resilience to security threats, and underscored the effectiveness of the novel PoC algorithm in ensuring scalability and energy efficiency. BIRDS effectively addresses the energy consumption concerns associated with UAV delivery operations by optimizing throughput for rapid delivery, cost reduction, and environmental sustainability. A comprehensive performance evaluation was conducted to assess the job delivery capabilities across a diverse set of UAVs. The initial classification success rate concerning device speed exhibits remarkable proficiency, especially in dual or quadruple device scenarios, whereas it gradually stabilizes at 50% when the UAV count exceeds 15%. In addition, compared with existing schemes, the proposed framework

reduces communication costs, ensures lightweight computation and storage overhead, and provides superior security attributes. Moreover, it enables secure transactions between clients and UAV for deliveries from both the communication and blockchain perspectives. Although BIRDS demonstrated a promising performance, certain limitations present avenues for future research. First, evaluating BIRDS in real-world large-scale UAV delivery scenarios using hardware implementation provides credibility. Second, enhancing the FL capabilities for UAV profiling and job assignment can improve the overall workflow automation. Third, accommodating diverse types of aerial vehicles using adaptive protocols and algorithms can augment the framework versatility. Fourth, integrating edge-computing solutions can help address latency and bandwidth constraints. Finally, advancing the reputation system with more parameters and adaptive weighting schemes can enrich trust management across decentralized UAV platforms.

## Linking the Chapters 5-6

### Advancing Blockchain Applications in UAV Networks

1. *From Practical UAV Network Management to Advanced FL Integration: Chapter 5 Overview:* The BIRDS framework is introduced, focusing on the blockchain-based optimization of UAV delivery routes, encompassing UAV authentication, registration, node selection, and energy efficiency. Emphasize the practical implementation of blockchain for security, efficiency, and reliability in UAV operations. Chapter 6 expands blockchain applications in UAV networks with BCS-FL by integrating FL with large-scale UAV swarms. This chapter marks a significant leap in the complexity and potential of blockchains for enabling advanced FL within UAV networks.
2. *Key Developments in Chapter 6 BCS-FL:*
3. *Transition and Evolution of Blockchain Technology in UAV Networks:* The shift from blockchain for UAV network management is illustrated in Chapter 5 to sophisticated FL applications within these networks. Chapter 6 highlights the evolution and scaling of blockchain applications, enabling advanced capabilities, such as decentralized ML in UAV swarms.
4. *Setting the Stage for Future Research:* Taking advantage of blockchain's properties of security, transparency, and decentralization, BCS-FL tackles challenges in scalability, communication efficiency, and privacy. Opens avenues for further exploration of integrating blockchain with advanced ML techniques for innovative UAV network applications.

## Chapter 6

# Blockchain-enabled Federated Learning (BCS-FL)

This section presents a novel framework, BCS-FL, designed to implement FL in UAV networks. The BCS-FL framework aims to address the challenges of privacy, scalability, and reliability in distributed systems, and ML technologies that involve extensive data exchange. In the BCS-FL framework, UAV networks are organized into distinct clusters coordinated by UAVs, Cluster Heads (CHs). This structure facilitates efficient updates of the ML model. The framework employs SC for UAV registration, cluster formation, and decentralized model aggregation.

We introduced two model aggregation schemes within this clustered network: Fully Centralised Aggregation (FCA) and k-Hop Aggregation (kHA). In the FCA strategy, model updates from all Cluster Head (CH) UAVs were incorporated during each training round. Conversely, the kHA approach permits CH UAVs to share their locally aggregated models with neighboring CH UAVs within a k-hop maximum distance, thereby reducing the communication overhead. The system used UAVs trained to retrieve the global model from the previous round. These UAVs update their local models using Stochastic Gradient Descent (SGD) and their local datasets and then communicate these updates to their respective CH UAVs. CH UAVs exchange models are based on the chosen aggregation strategy FCA or kHA. This process is repeated until convergence or a predefined number of training rounds are completed.

Numerical simulations were conducted using Modified National Institute of Standards and Technology Database (MNIST) and CIFAR-10 datasets to evaluate the performance of the proposed schemes. The results show that the BCS-FL framework achieves convergence and elucidates the trade-offs between the training performance and communication efficiency. The FCA strategy offers accuracy comparable to that of centralized methods, whereas the kHA scheme, with its lower communication overhead, is more suited to resource-limited UAV networks. The chapter concludes with a discussion of the challenges and limitations of deploying the framework in real-world scenarios, including limited onboard computing capacity, unreliable connections between mobile UAVs, dynamic clustering precision, and coordination overheads. It

outlines future research directions focused on improving the incentives, security, optimization, adaptability, and applicability of the BCS-FL framework.

Privacy, scalability, and reliability remain significant challenges in UAV networks, particularly in distributed systems that employ ML technologies with substantial data exchange. Recently, the application of FL UAV networks has enhanced collaboration, privacy, resilience, and adaptability, thereby establishing them as promising frameworks for UAV applications. Nonetheless, implementing FL in UAV networks presents drawbacks, such as communication overhead, synchronization issues, scalability limitations, and resource constraints. This section introduces the BCS-FL framework for UAV networks to improve the decentralization, coordination, scalability, and efficiency of FL in large-scale UAV networks. The BCS-FL framework organizes the UAV networks into separate clusters coordinated by cluster-headed UAV CHs to form a connected graph. This clustering approach enhances the efficiency of updating the ML model. Moreover, hybrid inter-cluster and intra-cluster model aggregation schemes develop a global model after each training round, fostering collaboration and knowledge-sharing among clusters. Numerical findings highlight the achievement of convergence, while also emphasizing the trade-offs between training effectiveness and communication efficiency.

## 6.1 Introduction

FL has emerged as a pivotal privacy-preserving approach to collaborative ML without direct data-sharing. In FL, models are locally trained on individual devices using their respective data and only model updates are aggregated to enhance a shared global model. This approach enables collaborative learning, while safeguarding data privacy [126]. Coordinating a large, decentralized network of heterogeneous UAV for FL presents significant challenges. Traditional methods often rely on a centralized server to orchestrate participant roles, aggregate model updates, and allocate rewards. However, this centralization introduces vulnerabilities, trust issues, and inaccuracies in the reward distribution. Decentralized clustering schemes that group UAVs and rotate CH to reduce communication costs have been explored [84]; however, they still depend on centralized components for scheduling and global model aggregation.

Authors in [127] introduced a decentralized FL framework employing merged UAV clusters to enhance energy efficiency. However, this framework relies on centralized scheduling for model aggregation. In contrast, [128] formulated an Efficient Edge Intelligence Clustering Problem for UAV swarms and proposed an iterative algorithm using an optimal policy and local search techniques. To further improve energy efficiency, similarly in [129], authors proposed a clustering scheme for UAV in FL. However, this approach hinges on a leading UAV for coordination, thereby introducing vulnerability at a SPoF. Blockchain technology has shown a potential to address these challenges by enabling decentralized incentive mechanisms through SC, thereby enhancing security, transparency, and credibility [25]. Other authors in [130] ex-

explored the scalability of FL in large UAV swarms and examined the difficulties arising from reliance on a central server for model aggregation in extensive remote UAV networks with limited resources.

To bridge our introductory motivation with the technical aspects of our framework, we summarize the key components of our model. Our UAV network is organized into clusters based on proximity, with each cluster led by a head UAV that facilitates aggregation and coordination. CH forms an interconnected network that enables model updates between clusters. SC manage registration, cluster formation, and decentralized aggregation. Our framework's core concepts include UAV clustering, CH hierarchy, inter-cluster relationships, blockchain integration, and FL workflow. To address the current limitations of FL implementation, we introduce a comprehensive hybrid clustering method for diverse UAV swarm topologies. This method accommodates UAVs beyond the communication range, where CH UAVs establish a connected graph, thereby ensuring the interconnectivity among clusters. We present two model aggregation schemes, FCA and kHA. Numerical evaluations demonstrated convergence and a reduction in the communication overhead across the network.

The remainder of this chapter is organized as follows. Section 6.2 describes our system model for UAV networks. Section 6.3 outlines our blockchain-enabled FL framework including the dual-model aggregation approach. Section 6.3 presents numerical simulation results and discussion. Finally, we conclude the chapter in Section 6.5.

## 6.2 System Model for UAV Networks

In this section, we introduce the UAV network topology model and provide a comprehensive overview of its key components of the proposed framework. Subsequently, we detail our proposed clustering scheme, specifically tailored for UAV swarm networks.

### 6.2.1 UAV Network Topology Model

Our study focuses on a UAV swarm comprising  $U$  UAVs within a designated geographic region collectively engaging in ML model training using FL techniques. Individual UAVs, denoted by the set  $\mathcal{U} = 1, \dots, U$ , maintain a constant altitude and are characterized by two-dimensional coordinates. Each UAV  $u$  position is denoted as  $\mathbf{p}_u = (i_u, j_u)$ .

However, factors such as adverse weather conditions can lead to a UAV deviating from its intended location,  $\mathbf{p}_u^d$  during the  $d$ -th training round. The deviation  $\delta = \|\mathbf{p}_u^{d+1} - \mathbf{p}_u^d\|$  is measured using the Euclidean norm  $\|\cdot\|$ . To ensure collision avoidance and maintain stable flight trajectories, we introduce a maximum allowable distance  $\delta_{\max}$  that limits the extent of deviation from the initial position  $\mathbf{p}_u^0$ .



### 6.2.2 Communication Capabilities and Clustering in UAV Networks

We assume that each UAV within the swarm is equipped with a maximum communication range denoted by  $R_{\max}^{\text{com}}$ . This range facilitates data exchange among UAVs, enabling regional model updates during FL. In addition, we assume that the UAV swarm is sufficiently dense to ensure comprehensive coverage and interconnectivity while adhering to  $R_{\max}^{\text{com}}$  any  $\delta_{\max}$  constraints. This density allows each UAV to establish communication links with others either directly or through intermediaries. For efficient clustering, UAVs use beacon frames to identify and form clusters denoted by  $\mathcal{Q} = 1, \dots, Q$ . An UAV node within cluster  $q$  is denoted by  $u_q$ , and the set of UAVs in cluster  $q$  is  $\mathcal{U}_q$ . Each cluster  $q$  includes a designated CH UAV,  $u_q^{\text{CH}}$ , which is responsible for inter-cluster communication.

Direct communication links between all UAVs in real-world deployments may not always be feasible owing to factors such as a limited range or physical obstructions. Thus, complete collaboration may occur only within each network's connected subgraph. Our study focuses on scenarios in which the (BCS-FL) framework is applied to these subgraphs, disregarding the complexities of unlinked UAVs.

### 6.2.3 Clustering Architecture for UAV Networks

To optimize the local model-update aggregation in extensive UAV networks, we propose a hierarchical clustering strategy. Our goal is to determine the optimal number of clusters  $Q$  to balance the inter-cluster communication and CH connectivity. We employed an iterative  $k$ -means clustering algorithm starting with an initial cluster count  $Q$ .

The process continues until a minimal CH connectivity is achieved with the least  $Q$ . We also considered UAV movements during training by introducing a distance parameter  $\sigma = R_{\max}^{\text{com}} - 2\delta_{\max}$  to ensure CH connectivity. Hierarchical clustering significantly enhances the communication efficiency of FL.

### 6.2.4 Roles and Responsibilities of UAVs in the Collaborative Training Framework

Our proposed framework outlines three specific groups of UAV, each designated with key roles and responsibilities in the collaborative training process.

#### Blockchain-Assisted UAVs

These UAV are integral for interactions with the blockchain network, primarily handling the execution of SC. Their functions include registering a new UAV, aiding in the formation of UAV clusters, and overseeing the model aggregation process. This is achieved by deploying and executing SC within the blockchain to ensure a secure and efficient workflow.

### Registration UAVs

The UAV plays a pivotal role in orchestrating the cluster formation across networks. They employed beacon frames to locate and identify nearby UAV, leading to the formation of distinct UAV clusters. This clustering process is vital for efficiently organizing the network, thereby facilitating smoother communication and coordination within the proposed framework.

### Cluster Head (CH) UAVs

The CH-UAV serves specific functions within each cluster, separate from the role of training UAVs. The key responsibilities include the following.

- *Reception of Local Model Updates:* CH UAV are tasked with collecting updates of local models from training UAV within their cluster. At the beginning of each training round, the updated global model is distributed to all the UAV involved in training.
- *Facilitation of Inter-cluster Model Aggregation:* CH UAV are responsible for aggregating models across different clusters. They established a network with other CH UAV, ensuring effective communication and coordination throughout the network.

Effective communication necessitates that CH UAV have high node centrality within their clusters, which is why positioning them near the cluster center is critical. This strategic placement enhances their impact, particularly in the context of a distributed ML. The relationship between node centrality, communication efficiency, and Federated Averaging (FedAvg) aggregation algorithm is crucial. CH UAV, with their high centrality, improve communication efficiency, which is harness by the FedAvg algorithm. This prioritizes influential nodes during the aggregation process, promoting more effective collaboration and convergence towards the optimized final model.

## 6.3 Blockchain-Based Federated Learning

Our BCS-FL framework for UAV networks focuses on data privacy, collaborative training, and taps for secure data storage and communication protocols in FL. Here, we detail the key components and mechanisms, including the FCA and  $k$ -hop aggregation  $k$ HA strategies.

### 6.3.1 BCS-FL Overview

The BCS-FL framework, shown in Fig. 6.1, incorporates SC on the blockchain for cluster formation, UAV registration, and model aggregation. These contracts automate UAV registration and cluster creation based on proximity, managed by authorized users, such as UAVs.

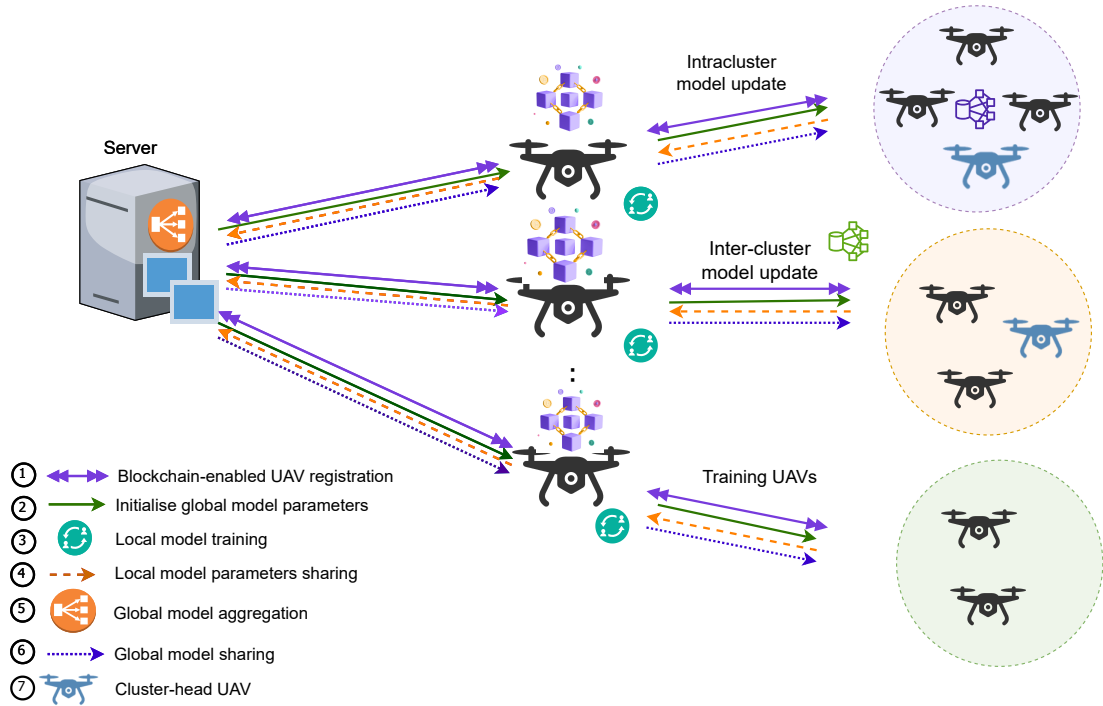


Figure 6.1: The BCS-FL Framework.

During model aggregation, SC calculate the weighted averages of the local model updates from the training UAV, thereby creating a global model. This model is then distributed to all training UAVs. The framework involves blockchain-assisted UAVs, registration UAVs, and CH UAVs, all of which play a crucial role in the training process. CH UAVs manage inter-cluster communication for global model exchange, while registration UAVs orchestrate cluster formation using beacon frames.

These terms are related to a blockchain-oriented architecture for executing FL with an UAV, offering a detailed explanation of the involved components and their functionalities.

1. **Blockchain Registered UAVs:** In the SC defined in Algorithm 1, a UAV node structure represents participating UAV nodes and their attributes. The contract stores these nodes in a mapping and is retrievable using the ID. The `joinBCSFL` function enables authorized users to register new UAV nodes in the blockchain. This function uses mapping to store and retrieve UAV nodes using ID, thereby facilitating node management within the BCS-FL network.
2. **Configuration of UAVs:** A typical FL task involves using multiple drones, denoted by  $U$ , for training. Each training UAV  $u$  accesses local datasets  $\mathcal{R}_u$  using  $|\mathcal{R}_u|$  data samples. For the model parameter vector  $fl$ , the loss is quantified by function  $l$ , and a local objective function for UAV  $u$ ,  $O_u(l)$ , is defined as

$$O_u(l) = \frac{1}{|\mathcal{R}_u|} \sum_{\zeta \in \mathcal{R}_u} l(\zeta). \quad (6.1)$$

The global objective function  $O(l)$  involves all the training clients:

$$O\mathbf{l} = \sum_{u=1}^U \chi_u O_u \mathbf{l}, \quad (6.2)$$

where  $\chi_u$  represents the weighting for training the UAV  $u$ .

3. **Cluster-Head UAV Swarms:** CH UAVs perform distinct functions for each cluster.
  - **Receiving Local Model Updates:** CH UAVs receive local model updates from training UAVs in their cluster. At the beginning of each training round, the aggregated global model is distributed to the participating training UAVs.
  - **Facilitating Inter-cluster Model Aggregation:** CH UAVs enable model aggregation between clusters, ensuring seamless communication and coordination within the network.

Effective communication requires the CH UAV to be centrally located within the clusters to maximize the impact. The FedAvg algorithm, which employs node centrality, enhances communication efficiency and collaborative training within UAV networks.

4. **Decentralized Model Aggregation:** SC are employed to aggregate local model updates from training UAVs within and across clusters, leading to the creation of a global model. This process is overseen by CH UAVs, which maintain decentralization and transparency.

Aggregated Model Representation for Clusters.

$$l_q^d = \sum_{u \in \mathcal{W}_q, u \neq u_q^{\text{CH}}} \gamma_u l_u^d, q, \quad (6.3)$$

where  $\gamma_u$  denotes the data-sample ratio between UAV  $u$  and cluster  $q$ , with  $|\mathcal{R}_u|$  representing the number of data samples from UAV  $u$  and  $|\mathcal{R}_q|$  representing the number of data samples in cluster  $q$ .

### 6.3.2 Role of Smart Contracts in BCS-FL Framework

SC are vital in the BCS-FL framework, offering secure, automated processes for key functions, such as UAV registration, cluster formation, and model aggregation. These contracts, which are self-executing and deployed on a blockchain network, are accessible to authorized users or entities.

**UAV Registration:** The contracts define the structure and functions for registering UAVs on the blockchain. Each UAV is assigned a unique identifier and linked to its owner's address to facilitate transparent and secure identification.

**Algorithm 6** BCSFLContract

---

```

1: struct UAVNode
2:   address owner
3:   string nodeId
4: mapping (uint256  $\rightarrow$  UAVNode) uavNodes
5: uint256 totalNodes
6: event NodeJoined
7:   uint256 id
8:   address owner
9:   string nodeId
10: function joinBCSFL(string nodeId)
11:   uint256 newNodeId  $\leftarrow$  totalNodes
12:   UAVNode newNode  $\leftarrow$  uavNodes[newNodeId]
13:   newNode.owner  $\leftarrow$  msg.sender
14:   newNode.nodeId  $\leftarrow$  nodeId
15:   totalNodes++
16:   emit NodeJoined(newNodeId, msg.sender, nodeId)
17: function getNodeById(uint256 id)
18:   UAVNode node  $\leftarrow$  uavNodes[id]
19:   return node.owner, node.nodeId

```

---

**Cluster Formation:** SC streamline cluster creation based on UAV proximity. Registration UAV uses beacon frames to identify neighboring UAVs, initiating cluster formation via SC interactions.

**Model Aggregation:** In this phase, SC compute weighted averages of local model updates from training UAVs within each cluster, forming aggregated local models. These were collectively aggregated across clusters by contract to create a global model for the network.

### 6.3.3 Federated Learning Workflow in BCS-FL Framework

The FL workflow in the BCS-FL involves several steps.

**Initial Setup:** Training UAVs start each iteration by fetching the globally aggregated model from the last round, receiving initial datasets from their CH UAVs for training.

**Local Model Training:** UAVs update their local models independently using optimization techniques like SGD, based on their local data.

**Intra-cluster Aggregation:** Training UAVs send local model updates to their CH UAV, which aggregates them to form a model for the cluster.

**Inter-cluster Aggregation:** CH UAVs share and aggregate models from different clusters using FCA or k-hop Aggregation (kHA), leading to a global model.

**Iteration:** This cycle of local training and aggregation repeats until convergence or a set number of global rounds are completed.

### 6.3.4 Model Aggregation Strategies in BCS-FL Framework

The BCS-FL framework incorporates two model aggregation strategies for inter-cluster aggregation: FCA and kHA.

**Fully Centralized Aggregation (FCA):** In the FCA, a CH UAV is chosen randomly in each training round to collect model updates from all CH UAVs. This UAV then computes the global model by averaging local models.

**k-hop Aggregation (kHA):** The kHA strategy aims to reduce the communication overhead across a wide geographical distribution of UAVs. Each CH UAV shares its local model with CH UAV within the maximum distance of  $k$  hops. The value of  $k$  can be adjusted to balance communication overhead and training efficiency.

### 6.3.5 Strategies for Inter-cluster Aggregation

Effective data utilization during ML model training is crucial for a decentralized FL framework. We introduced two distinct aggregation strategies, FCA and  $k$ -hop aggregation ( $k$ HA), to efficiently incorporate learning from local models across clusters. These strategies balance the training performance with communication overhead. Both dataset partitioning methods followed the guidelines established in [131].

We utilized a straightforward Convolutional Neural Network (CNN) model for image classification on the MNIST dataset. The model commences with a convolutional layer comprising 10 filters of size  $5 \times 5$ , adhering to an Rectified Linear Unit (ReLU) activation function and  $2 \times 2$  max pooling. Subsequently, the second layer of convergence incorporated 20 filters of size  $5 \times 5$  along with an ReLU activation function and  $2 \times 2$  max pooling. The model comprises two fully connected layers with ReLU activations, resulting in ten output features. A similar architecture is developed for the CIFAR-10 dataset. During ML model training, effective utilization of the available data is crucial. In our decentralized FL framework, we enabled the global model to efficiently incorporate learning from local models across various clusters. This fosters rapid convergence and improves training performance. Nevertheless, this approach might lead to a notable increase in message exchanges among CH UAVs, resulting in a substantial communication overhead. To address this challenge, we introduce two aggregation strategies, each offering distinct trade-offs between the training performance and overhead. These strategies are known as FCA and  $k$ HA.

- Fully Centralized Aggregation (FCA): This strategy forms its basis on incorporating model updates from every CH UAV during each training round. Formally, the global model representing the entire network is defined as

$$\check{l}^d = \frac{1}{Q} \sum_{q \in \mathcal{Q}} l_q^d. \quad (6.4)$$

In practice, in each training round, one CH UAV is randomly selected to receive model updates from all the other CH UAVs. The selected CH UAV then calculates the aggregated global model as described in Eq. 6.4.

In summary:

- $\chi_u$  in (6.2) is the weighting for training UAV  $u$  in the global context.
- $\gamma_u$  in (6.3) is the data-sample ratio used for aggregating local models within a cluster  $q$ .
- $l_q^d$  in (6.4) is the aggregated local model for cluster  $q$  at training round  $d$ .

Both weights serve to balance the contributions of individual UAVs based on their data and roles within the network.

- *k*-Hop Aggregation (*k*HA): To address the issue of communication overhead caused by the widespread distribution of UAV over a vast geographical area during model aggregation, we propose a *k*HA strategy. This approach permits each CH UAV to share its locally aggregated model with neighbouring CH UAVs located within a maximum distance of *k* hops. Refer to Fig. 6.2 for illustration, where each hop is represented by *k*. For example, when *k* is set to two, the source CH UAV in red transmits its locally aggregated model to seven neighbouring CH UAVs within a maximum of two hops (presented by the purple, orange, and green CH UAVs in Fig. 6.2).
  1. The Initial setup: Training UAVs retrieve the globally aggregated model from the previous round. At the start of each training iteration, the participating UAVs received the initial dataset from their respective CH UAVs, thereby forming the basis of the training process.
  2. Formation: Instruction UAVs independently update their local models using the SGD method and their local datasets.
  3. Intra-cluster Aggregation: Training UAVs within each cluster communicate their relevant CH UAV to their respective local model vectors. CH UAVs then used local model aggregation to derive an aggregated model representation for a cluster.
  4. Inter-cluster Aggregation: CH UAVs exchange models among themselves, sharing locally aggregated models based on the selected strategy FCA or *k*HA. This enables the computation of the globally aggregated model by integrating models across different clusters and preparing all the UAV for the next training phase.
  5. Repeat: The process of local model training on each UAV, followed by aggregated global model updates, is iterated until the training convergence criteria are met or the maximum predefined number of global rounds is reached.

Employing this workflow, our FL framework promotes effective collaboration and iterative model refinement among UAVs, ultimately driving the learning algorithm towards the convergence or completion of the maximum number of training rounds.

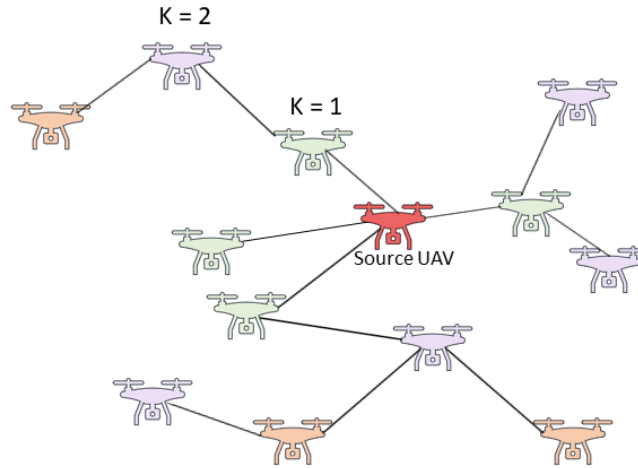


Figure 6.2: A Demonstration of the kHA Scheme.

### 6.3.6 Trade-offs in Aggregation Strategies within BCS-FL Framework

In the BCS-FL framework, the selection between the FCA and kHA strategies involves balancing communication overhead and training performance.

#### Communication Overhead:

- *FCA Strategy*: This approach leads to higher communication overhead due to the need for model exchanges among all CH UAVs in each training round.
- *kHA Strategy*: By restricting model exchanges to CH UAVs within a defined hop distance, kHA reduces communication overhead. However, this can result in a lower convergence rate.

#### Training Performance:

- *FCA Strategy*: FCA tends to offer faster convergence and enhanced training performance by integrating model updates from all CH UAVs each round.
- *kHA Strategy*: While potentially slower in convergence due to its localized model update diffusion within the k-hop vicinity, kHA can be more suitable under certain network conditions.

Selecting an appropriate aggregation strategy depends on the specific requirements and constraints of the UAV network. If rapid convergence and the availability of communication resources are priorities, the FCA strategy may be more suitable. Conversely, in scenarios where



communication resources are limited and overhead reduction is crucial, the kHA strategy could be more beneficial.

## 6.4 Numerical Results and Discussions

### 6.4.1 Simulation Settings

We deploy UAVs at random locations within a  $1000\text{ m} \times 1000\text{ m}$  area, ensuring that they form a connected graph based on predefined  $R_{\max}^{\text{com}}$  and  $\delta_{\max}$  values. We set  $R_{\max}^{\text{com}}$  to  $150\text{ m}$  and  $\delta_{\max} = 5\text{ m}$  in our simulations. All training UAV were actively involved in each global round. We performed an evaluation using two common benchmark datasets, namely, MNIST and CIFAR-10 [132], to assess the effectiveness of the proposed schemes. Using two dataset partitioning strategies, Independent and Identically Distributed (IID) and Non-Independent and Non-Identically Distributed (Non-IID) [133], we examine how data variations affect the model performance. Here, IID refers to independent and identically distributed data, implying that each data sample was generated independently and followed the same probability distribution. Non-IID means non-independent and non-identically distributed, indicating the data samples have correlations and come from different distributions. Both the dataset partitioning methods followed the guidelines established in [134]. We utilized a straightforward CNN model for image classification on the MNIST dataset. The model commences with a convolutional layer comprising 10 filters of size  $5 \times 5$ , adhering to an ReLU activation function, and  $2 \times 2$  max pooling. Subsequently, the second layer of convergence incorporated 20 filters of size  $5 \times 5$  along with an ReLU activation function and  $2 \times 2$  max pooling. The model comprises two fully connected layers with ReLU activations, resulting in ten output features. A similar architecture is developed for the CIFAR-10 dataset.

### 6.4.2 Model Efficiency

We employed 200 UAVs, where each training UAV ran a mini-batch SGD once per training round. The learning rates for the MNIST and CIFAR-10 datasets are 0.035 and 0.01, respectively, and the batch size is 10. We monitored the training process until convergence and reported the results. Fig. 6.3 shows the performance results for CIFAR-10. Training on CIFAR-10 poses greater challenges than training on MNIST, highlighting the differences between schemes. The findings show that conventional FL approaches, such as scalable FL, perform best when the data are IID. However, with Non-IID data and FCA, the accuracy decreases slightly. Notably, the  $k$ -hop scheme shows considerably slower convergence with Non-IID data. This behavior can be attributed to the disparate distribution of data instances across the UAV network. This impedes the diffusion of model updates between UAVs that have distinct local datasets. We simulated the scenarios by comparing the suggested aggregation schemes, specifically setting  $k = 1$  for the  $k$ -hop. Figs. 6.4-6.5 show model performance metrics for MNIST using FCA and

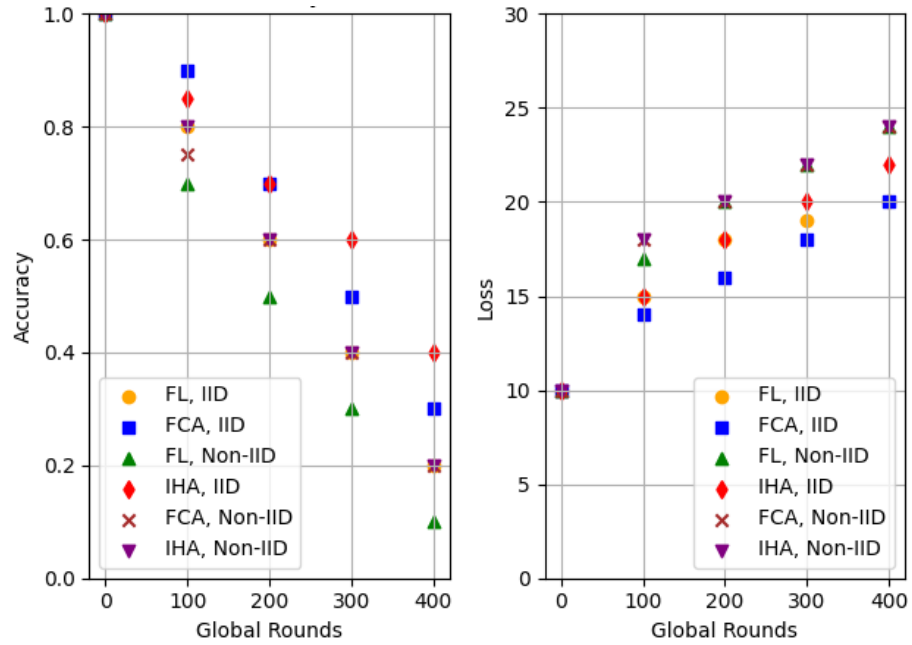


Figure 6.3: Performance of (a) Accuracy and (b) Loss, CIFAR-10 Dataset.

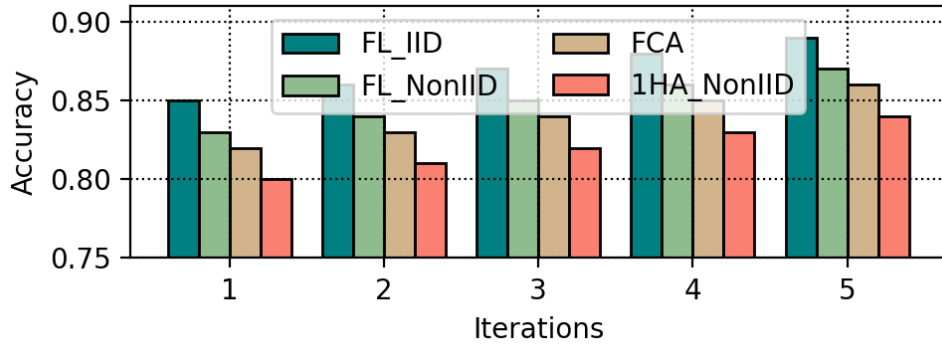


Figure 6.4: The BCS-FL Performance of Accuracy.

1HA. FCA demonstrates superior performance in both IID and Non-IID settings, as all UAVs participate in each global round for both schemes. However, 1HA requires approximately 50 additional rounds to match the accuracy of FCA, particularly for Non-IID data, because FCA interconnects all the UAV swarms.

### 6.4.3 Communication Overhead

We conducted simulations to evaluate the communication overhead of different aggregation schemes by varying the number of UAV ( $U$ ). Fig. 6.6 reveals that selecting  $k=1$  results in the slowest convergence, as the training information diffuses gradually. When  $k=3$ , the performance is comparable to that of FCA. However, larger  $k$  values can impose an excessive communication overhead. We recommend empirically determining  $k$  based on the network architecture and desired convergence/overhead trade-off. The overhead was measured by counting

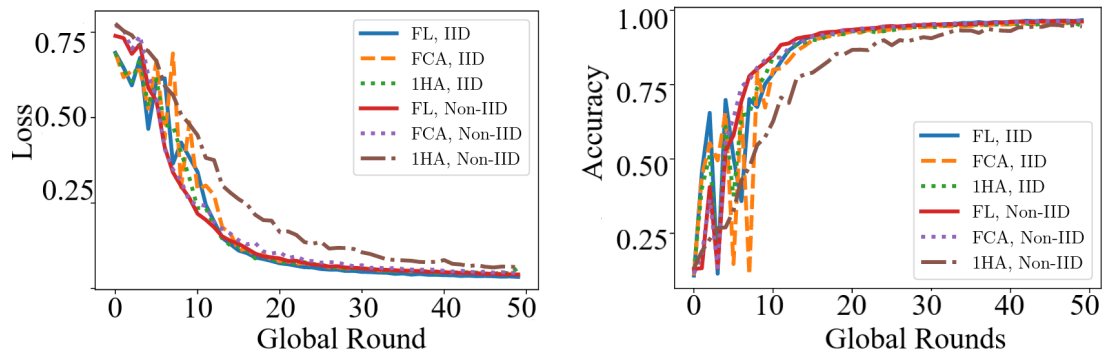


Figure 6.5: Performance on BCS-FL (a) Accuracy and (b) Loss MNIST Dataset.

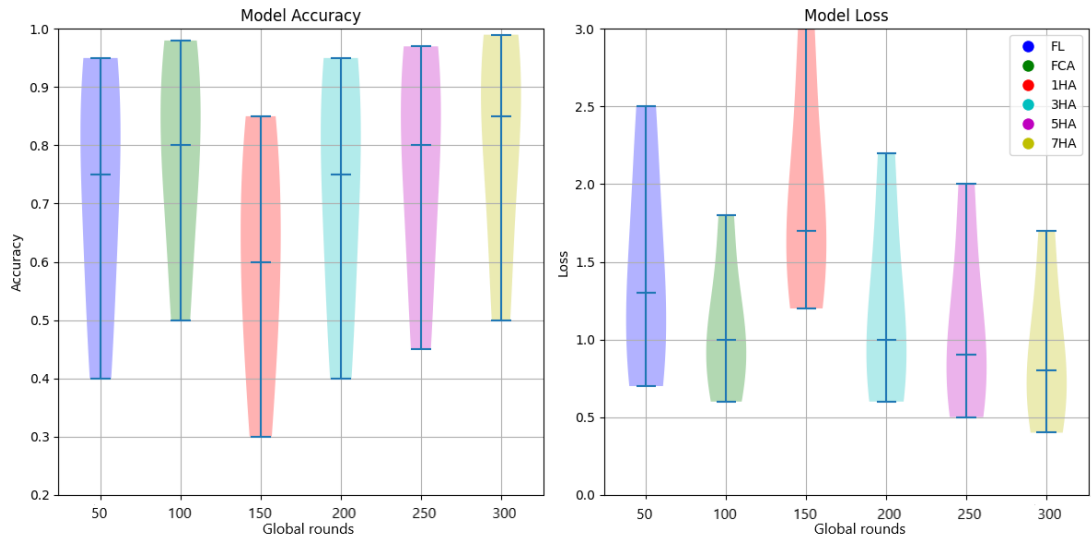


Figure 6.6: Influence of  $k$  on BCS-FL (a) Accuracy and (b) Loss.

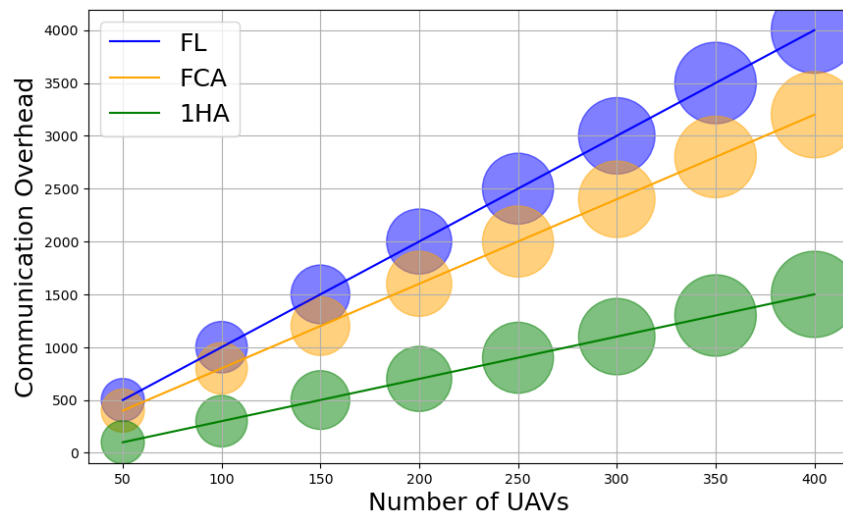


Figure 6.7: Impact of Inter-cluster Aggregation Scheme on Communication Overhead.

the model update exchanges within and between clusters per training round across 20 random network layouts. For conventional FL, aggregation UAVs were randomly chosen. Shortest-path routing was used where possible. The results in Fig. 6.7 show that 1HA is emerging as the most communication efficient among techniques. Despite the comparable model performance to that of conventional FL, FCA had a higher overhead. With 400 UAVs, the conventional FL required more than 3,500 message exchanges, compared to only 35% for FCA. In summary, simulations demonstrate 1HA's advantage in low overhead, offering efficient decentralized learning for UAV networks with limited resources. This guides the optimization of communication efficiency versus learning performance when designing the aggregation protocols.

## 6.5 Summary

In this study, we present a novel approach tailored to UAV swarms by integrating an iterative clustering algorithm to enable effective local model aggregation and robust connectivity among the CH UAVs. The hybrid iterative clustering approach groups UAVs to reduce the communication overhead for model aggregation. The inter-cluster aggregation schemes of FCA and  $k$ -hop further minimize the overhead compared with conventional FL. Simulations demonstrated the efficacy of BCS-FL in terms of learning performance, with FCA attaining an accuracy comparable to that of centralized methods. This study guides the optimization of the trade-off between convergence and efficiency by selecting the appropriate aggregation protocols. Overall, BCS-FL shows promise for collaborative learning in UAV swarms. However, real-world deployment poses challenges, including limited onboard computing, unreliable connections between mobile UAV, precise dynamic clustering, and coordination overhead. Although discussing these limitations provides a useful perspective, our results emphasize BCS-FL innovations in scalable and decentralized FL for UAV networks. Ongoing research aims to advance the incentives, security, optimization, adaptability, and applicability of BCS-FL.

This section investigates an BCS-FL framework to facilitate ML among large-scale UAV swarms. A key challenge is to enhance the scalability, efficiency, and security of FL when implemented in resource-constrained UAV networks spanning vast geographical regions. An optimization algorithm is proposed that leverages the hierarchical clustering of UAVs based on proximity as well as the selection of cluster heads UAVs to coordinate aggregated model updates between clusters. This reduces the communication overhead for the global model aggregation across a highly distributed network topology. Furthermore, the effectiveness of the proposed framework is enhanced through SC executed on a blockchain that automates essential processes including UAV registration, cluster formation, and decentralized aggregation.

Key insights include trade-offs between learning efficiency, communication overhead, and convergence speed enabled by inter-cluster aggregation schemes. Evaluations demonstrate that the FCA scheme achieves superior performance in terms of accuracy and loss convergence at the

expense of an additional communication overhead. Meanwhile, the k-hop aggregation scheme significantly reduces the overhead while attaining an acceptable model performance when k is optimally tuned.

In summary, this chapter proposed an innovative integration of UAV clustering, blockchain decentralization, and scalable federated averaging to unlock the potential of collaborative on-device learning across extensive UAV fleets with limited onboard capabilities. The proposed Blockchain-Enabled Clustered and Scalable Federated Learning (BCSFL) framework tackles pressing challenges regarding the scalability, security, efficiency, and resource constraints posed when deploying FL in highly dynamic and decentralized UAV networks spanning large geographical areas. Building on the comprehensive exploration of blockchain applications in UAV networks across Chapters 3, 4, 5, and 6, Chapter 7, serving as the conclusion and future work, provides a comprehensive understanding of the entire research journey and sets a clear path for future exploration in this rapidly evolving field.

### **Linking the Chapters 6-7 Paving the Way for Future Innovations:**

1. *Foundation Set in Previous Chapters*
2. *Chapter 3:* Introduced a secure authentication scheme, essential for the reliable operation of UAV networks.
3. *Chapter 4:* Expanded the application of blockchain in post-disaster communication, emphasizing decentralized control and resilient coordination.
4. *Chapter 5:* Implemented the BIRDS framework for optimizing UAV delivery routes, Tapping into blockchain for efficiency and reliability.
5. *Chapter 6:* Presented the BCS-FL framework, showcasing blockchain-enabled scalable FL in UAV networks, marking a significant advancement in the complexity of blockchain applications.

# Chapter 7

## Conclusions and Future Works

This chapter concludes the thesis and provides insights for further research in this field. This doctoral research endeavoured to seamlessly integrate blockchain technology into UAV networks to address the critical privacy and security challenges. Based on a comprehensive literature review [5], this study identifies the key limitations and opportunities and establishes a foundation for innovative solutions.

The first significant contribution is BETA-UAV, referred to in [25], a pioneering blockchain-based authentication framework tailored for UAV networks that address crucial security requirements. The investigation was then expanded to post-disaster scenarios, where the proposed blockchain-enhanced UAV flocking networks demonstrated resilience and reliability in communication, even amid infrastructure failure. These contributions [135]– [103] present a novel and comprehensive framework that synergistically combines distributed ledger technology, optimization algorithms, and coordination techniques to enable secure, efficient, and resilient UAV-assisted disaster response operations. It addresses key technical challenges related to consensus protocols, interoperability, security, and adaptive coordination, to unlock the full potential of decentralized and autonomous UAV networks in emergency scenarios. In addition, the research ventured into the logistics and supply chain domains, as presented in [24] in the BIRDS framework. This initiative synergizes the blockchain’s immutability with the UAV’s agility, thereby revolutionizing delivery services through enhanced transparency, security, and efficiency.

In this chapter, [26], an BCS-FL framework was developed, enabling clustered and scalable FL in UAV networks. This novel approach combines blockchain technology with FL principles, fostering collaborative, privacy-preserving model training across decentralized UAV networks and paves the way for intelligent and adaptive aerial systems.

Through rigorous simulations and experimental evaluations, the efficacy of the proposed solutions in enhancing the security, privacy, reliability, and intelligence of UAV communication networks is demonstrated. Research findings have been disseminated through numerous peer-reviewed publications in leading conferences and journals, thereby advancing state-of-the-art research in this domain.

This doctoral study presents a coherent and progressive exploration of blockchain technology for UAV networks. This study consistently focuses on enhancing UAV network security, privacy, and collective intelligence by establishing secure authentication to enable resilient post-disaster communication, transforming logistics, and empowering FL. The findings and frameworks proposed not only address current challenges, but also pave the way for future research on envisioning UAV networks operating with unparalleled security, resilience, and collective intelligence, enabling a wide range of applications across various domains, including disaster response and logistics.

This thesis highlights the potential benefits of integrating blockchain technology into UAV networks. This study presents a comprehensive analysis of this integration and demonstrates the significant improvements in network security and efficiency. Blockchain technology can greatly enhance UAV operations. Furthermore, this study conducted a thorough evaluation and comparison of various blockchain-based solutions for UAV networks. This analysis offers researchers a valuable resource for inspiring innovation and developing robust UAV systems.

## 7.1 Limitations and Challenges

Identifying and acknowledging the limitations and challenges of this thesis is important for providing a comprehensive assessment. The potential limitations and challenges must be addressed in future studies. These challenges present new opportunities for future research.

1. *Scalability*: Integrating blockchain technology into UAV networks poses scalability challenges due to the inherent limitations of current blockchain platforms regarding transaction throughput and latency. Handling numerous UAV and their associated transactions can strain networks.
2. *Energy efficiency*: UAVs have limited battery life, and the computationally intensive nature of blockchain operations could drain their energy resources quickly. Finding energy-efficient consensus mechanisms and optimizations is crucial.
3. *Resource constraints*: UAVs often have limited computational power, storage, and bandwidth, which can hinder the deployment of resource-intensive blockchain solutions and SCs.
4. *Regulatory and legal aspects*: The integration of blockchain technology into UAV networks raises legal and regulatory concerns regarding data ownership, liability, and compliance with aviation regulations, which can vary across different regions and jurisdictions.

## 7.2 Future works

This domain has a significant potential for ongoing research and development. Many potential paths for future exploration include examining new designs for privacy and security in UAV communication schemes that are specifically designed for different uses in UAV communication systems. The following subsections provide a brief overview of the potential research directions.

### 7.2.1 AI-Driven Network Optimization and Automation

1. *AI-Driven Self-Optimization and Healing in UAV Networks*: Leverage AI and ML techniques to develop self-optimizing and self-healing UAV networks capable of adapting to dynamic conditions and mission requirements.
2. *AI-Based Resource Allocation and Path Planning in UAV Swarms*: Explore AI-based resource allocation, path planning, and task scheduling algorithms for efficient and autonomous UAV swarm operations.
3. *Integration of AI-Powered Digital Twins for UAV Network Design*: Investigate the integration of AI-powered digital twins for UAVs, enabling virtual testing, simulation, and optimization of network designs.

### 7.2.2 FL and Privacy-Preserving UAV Networks

1. *Federated Learning for UAVs: Algorithms and Protocols*: Develop FL algorithms and protocols for distributed model training and knowledge sharing among UAVs, without compromising data privacy.
2. *Secure Multiparty Computation and Homomorphic Encryption in UAV Networks*: Explore secure multiparty computation and homomorphic encryption techniques to enable privacy-preserving data aggregation and analysis in UAV networks.
3. *Integrating FL with Blockchain Technology in UAVs*: Investigate the integration of FL with blockchain technology, enabling decentralized and transparent model updates and verification.

### 7.2.3 Digital Twin Integration and Virtual Testing

1. *Digital Twin Development for UAVs and Communication Networks*: Develop high-fidelity digital twins of UAVs and their communication networks, enabling virtual testing, simulation, and optimization of network designs.



2. *Predictive Maintenance and Optimization via UAV Digital Twins*: Explore the use of digital twins for predictive maintenance, fault detection, and performance optimization of UAV networks.
3. *Integration of Digital Twins with AI, Blockchain, and FL in UAV Networks*: Investigate the integration of digital twins with AI, blockchain, and FL techniques for collaborative model training and network optimization.

#### **7.2.4 Cross-Domain Interoperability and Standardization**

1. Develop interoperability standards and interfaces for seamless integration of UAV networks with other emerging technologies, such as 5G/6G, Internet of Things IoT, and edge computing.
2. Explore cross-domain collaboration and interdisciplinary approaches to address the complex challenges of secure, efficient, and autonomous UAV network operations.

#### **7.2.5 Cyber-Physical Resilience, Security, and Robustness of UAV Networks**

From any Cyber-Physical System (CPS) perspective, ensuring the resilience, security, and robustness of UAV networks requires a holistic approach that addresses the interdependencies between cyber (computational and communication) and physical (mechanical and environmental) components. Future research directions and strategies for developing resilient, secure, and robust CPS architectures for UAV networks are outlined.

1. *Cyber-Physical Resilience and Robustness*: Develop CPS architectures for UAV networks to enhance resilience against cyber threats, like denial-of-service attacks and malware, and physical challenges, including adverse weather and interference. We focus on resilient control strategies and fault-tolerant mechanisms to ensure stable UAV operation during system failures or environmental disturbances. Prioritize self-healing and self-reconfiguring capabilities for autonomous adaptation and recovery from disruption. Implement redundancy and diversification strategies to boost system robustness and fault tolerance.
2. *Cyber-Physical Security*: Research and implement advanced cryptographic techniques to fortify communication, data transmission, and storage within UAV networks. Delve into secure multiparty computation and privacy-centric protocols designed for CPS environments to facilitate secure, privacy-preserving data sharing, and collaborative decision-making. Incorporate blockchain technology for decentralized trust and transparency, and

explore secure remote attestation and runtime monitoring methods to continuously verify system integrity and detect cyber-physical threats.

3. *Cyber-Physical System Integration and Interoperability*: Focus on creating interoperability standards and interfaces for integrating UAV networks with various CPS. This effort enhances security and resilience by enabling coordinated situational awareness and response strategies across the domains. In addition, we investigated the use of digital twins and virtual simulations to test and validate the resilience, security, and robustness of these systems against diverse attack scenarios and environmental conditions.

The research presented in this dissertation represents a comprehensive exploration of the role of blockchain technology in addressing critical challenges in UAV network design and applications. Through a narrative spanning multiple chapters, this study systematically advances from foundational concepts to sophisticated implementations, culminating in a cohesive vision for the future of blockchain-assisted UAV networks. This concluding chapter synthesizes key findings and establishes a foundation for future technological advancements in this rapidly evolving domain. Addressing the current limitations and fostering future research directions, this study paves the way for innovative solutions that will enhance the efficiency, security, and autonomy of UAV network operations. The successful integration of blockchain technology with UAV networks holds immense promise for a wide range of applications and establishes a comprehensive framework for future advancement in this field.

# Bibliography

- [1] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, “A Survey of Cyber Security Threats and Solutions for UAV Communications and Flying Ad-Hoc Networks,” *Ad Hoc Networks*, p. 102894, 2022.
- [2] M. Martalò, G. Pettorru, and L. Atzori, “A Cross-Layer Survey on Secure and Low-Latency Communications in Next-Generation IoT,” *IEEE Transactions on Network and Service Management*, 2024.
- [3] L. Zhao, H. Xu, S. Qu, Z. Wei, and Y. Liu, “Joint Trajectory and Communication Design for UAV-assisted Symbiotic Radio Networks,” *IEEE Transactions on Vehicular Technology*, 2024.
- [4] M. C. Bumalod and R. M. A. Velasco, “Synergistic Information Security Design Implementation based on Role-Based Access Control, Information Classification, and AES Cryptographic Encryption,” *International Journal in Information Technology in Governance, Education and Business*, vol. 6, no. 1, pp. 68–85, 2024.
- [5] S. Hafeez, A. R. Khan, M. Al-Quraan, L. Mohjazi, A. Zoha, M. A. Imran, and Y. Sun, “Blockchain-Assisted UAV Communication Systems: A Comprehensive Survey,” *IEEE Open Journal of Vehicular Technology*, 2023.
- [6] D. Sousa-Dias, “Data Security and Privacy in Transactive Energy Markets,” Ph.D. dissertation, Université d’Ottawal University of Ottawa, 2024.
- [7] L. Zhou, A. Diro, A. Saini, S. Kaisar, and P. C. Hiep, “Leveraging Zero Knowledge Proofs for Blockchain-based Identity Sharing: A Survey of Advancements, Challenges and Opportunities,” *Journal of Information Security and Applications*, vol. 80, p. 103678, 2024.
- [8] H. Kang, J. Joung, J. Kim, J. Kang, and Y. S. Cho, “Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems,” *IEEE Access*, vol. 8, pp. 168 671–168 710, 2020.

- [9] S. Aggarwal, N. Kumar, and S. Tanwar, "Blockchain-Envisioned UAV Communication Using 6G Networks: Open Issues, Use Cases, and Future Directions," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5416–5441, 2020.
- [10] B. Li, Z. Fei, Y. Zhang, and M. Guizani, "Secure UAV Communication Networks over 5G," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 114–120, 2019.
- [11] Y. Zeng, Q. Wu, and R. Zhang, "Accessing From the Sky: A Tutorial on UAV Communications for 5G and Beyond," *Proceedings of the IEEE*, vol. 107, no. 12, pp. 2327–2375, 2019.
- [12] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain envisioned UAV Networks: Challenges, Solutions, and Comparisons," *Computer Communications*, vol. 151, pp. 518–538, 2020.
- [13] R. Gupta, A. Nair, S. Tanwar, and N. Kumar, "Blockchain-Assisted Secure UAV Communication in 6G Environment: Architecture, Opportunities, and Challenges," *IET Communications*, 2021.
- [14] D. Saraswat, A. Verma, P. Bhattacharya, S. Tanwar, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain-Based Federated Learning in UAVs Beyond 5G Networks: A Solution Taxonomy and Future Directions," *IEEE Access*, vol. 10, pp. 33 154–33 182, 2022.
- [15] V. Hassija, V. Chamola, A. Agrawal, A. Goyal, N. C. Luong, D. Niyato, F. R. Yu, and M. Guizani, "Fast, Reliable, and Secure Drone Communication: A Comprehensive Survey," *arXiv preprint arXiv:2105.01347*, 2021.
- [16] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*. IEEE, 2020, pp. 1–5.
- [17] A. Sanober and S. Anwar, "Blockchain for Content Protection in E-Healthcare: A Case Study for COVID-19," in *2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS)*, vol. 1. IEEE, 2022, pp. 661–666.
- [18] M. Ghamari, P. Rangel, M. Mehrubeoglu, G. S. Tewolde, and R. S. Sherratt, "Unmanned Aerial Vehicle Communications for Civil Applications: A Review," *IEEE Access*, vol. 10, pp. 102 492–102 531, 2022.
- [19] M. Nguyen, H. Nguyen, L. Truong, T. Le, and T. Tran, "UAV Communication Networks: Benefits, Research Challenges and Opening Issues," 09 2021.

- [20] W. Wang, X. Liu, Y. Yao, Z. Chi, S. Ray, T. Zhu, and Y. Zhang, "Simultaneous Data Dissemination Among WiFi and ZigBee Devices," *IEEE/ACM Transactions on Networking*, 2023.
- [21] I. A. Ridhawi, S. Otoum, and M. Aloqaily, "Decentralized Zero-Trust Framework for Digital Twin-based 6G," *arXiv preprint arXiv:2302.03107*, 2023.
- [22] A. E. Omolara, M. Alawida, and O. I. Abiodun, "Drone Cybersecurity Issues, Solutions, trend Insights and Future Perspectives: A Survey," *Neural Computing and Applications*, vol. 35, no. 31, pp. 23 063–23 101, 2023.
- [23] Z. A. Khan, "Cyber Security Analysis of UAVs in Emergency Medical Services," 2023.
- [24] S. Hafeez, H. U. Manzoor, L. Mohjazi, A. Zoha, M. A. Imran, and Y. Sun, "Blockchain-Empowered Immutable and Reliable Delivery Service (BIRDS) Using UAV Networks," 2023.
- [25] S. Hafeez, M. A. Shawky, M. Al-Quraan, L. Mohjazi, M. A. Imran, and 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.
- [26] S. Hafeez, L. Mohjazi, M. A. Imran, and Y. Sun, "Blockchain-enabled Clustered and Scalable Federated Learning (BCS-FL) Framework in UAV Networks," *arXiv preprint arXiv:2402.05973*, 2024.
- [27] M. W. Ahmad and M. U. Akram, "UAV Sensor Failures Dataset: Biomisa Arducopter Sensory Critique (BASiC)," *Data in Brief*, vol. 52, p. 110069, 2024.
- [28] M. Fan, Z. Zhang, Z. Li, G. Sun, H. Yu, and M. Guizani, "Blockchain-Based Decentralized and Lightweight Anonymous Authentication for Federated Learning," *IEEE Transactions on Vehicular Technology*, 2023.
- [29] M. A. Akram, H. Ahmad, A. N. Mian, A. D. Jurcut, and S. Kumari, "Blockchain-based Privacy-preserving Authentication Protocol for UAV Networks," *Computer Networks*, p. 109638, 2023.
- [30] Y. Wu, H.-N. Dai, H. Wang, and K.-K. R. Choo, "Blockchain-based privacy preservation for 5g-enabled drone communications," *IEEE Network*, vol. 35, no. 1, pp. 50–56, 2021.
- [31] L. Zhang, H. Zhao, S. Hou, Z. Zhao, H. Xu, X. Wu, Q. Wu, and R. Zhang, "A Survey on 5G Millimeter Wave Communications for UAV-Assisted Wireless Networks," *IEEE Access*, vol. 7, pp. 117 460–117 504, 2019.

- [32] J. Li, H. Zhao, H. Wang, F. Gu, J. Wei, H. Yin, and B. Ren, "Joint Optimization on Trajectory, Altitude, Velocity, and Link Scheduling for Minimum Mission Time in UAV-Aided Data Collection," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1464–1475, 2020.
- [33] A. Alhammedi, A. Abraham, A. Fakhreddine, Y. Tian, J. Du, and F. Bader, "Envisioning the Future Role of 3D Wireless Networks in Preventing and Managing Disasters and Emergency Situations," *arXiv preprint arXiv:2402.10600*, 2024.
- [34] P. Álvares, L. Silva, and N. Magaia, "Blockchain-Based Solutions for UAV-Assisted Connected Vehicle Networks in Smart Cities: A Review, Open Issues, and Future Perspectives," in *Telecom*, vol. 2, no. 1. Multidisciplinary Digital Publishing Institute, 2021, pp. 108–140.
- [35] G. Asaamoning, P. Mendes, D. Rosário, and E. Cerqueira, "Drone Swarms as Networked Control Systems by Integration of Networking and Computing," *Sensors*, vol. 21, no. 8, p. 2642, 2021.
- [36] M. Asad, S. Shaukat, E. Javanmardi, J. Nakazato, N. Bao, and M. Tsukada, "Secure and Efficient Blockchain-Based Federated Learning Approach for VANETs," *IEEE Internet of Things Journal*, 2023.
- [37] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "Mitigating Byzantine Attacks in Ad hoc Wireless Networks," *Department of Computer Science, Johns Hopkins University, Tech. Rep. Version*, vol. 1, p. 16, 2004.
- [38] F. Ayaz, Z. Sheng, D. Tian, and Y. L. Guan, "A Blockchain Based Federated Learning for Message Dissemination in Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 2, pp. 1927–1940, 2021.
- [39] A. T. Azar, A. Koubaa, N. Ali Mohamed, H. A. Ibrahim, Z. F. Ibrahim, M. Kazim, A. Ammar, B. Benjdira, A. M. Khamis, I. A. Hameed *et al.*, "Drone Deep Reinforcement Learning: A Review," *Electronics*, vol. 10, no. 9, p. 999, 2021.
- [40] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative Analysis of Blockchain Consensus Algorithms," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. Ieee, 2018, pp. 1545–1550.
- [41] S. J. Basha and J. M. R. Danda, "A Review on Challenges and Threats to Unmanned Aerial Vehicles (UAVs)," *Unmanned Aerial Vehicles for Internet of Things (IoT) Concepts, Techniques, and Applications*, pp. 89–104, 2021.

- [42] Y. M. Balakrishna and V. Shivashetty, "Device-to-Device based Path Selection for Post Disaster Communication using Hybrid Intelligence," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 1, pp. 796–810, 2024.
- [43] E. Barka, C. A. Kerrache, H. Benkraouda, K. Shuaib, F. Ahmad, and F. Kurugollu, "Towards a Trusted Unmanned Aerial System using Blockchain for the Protection of Critical Infrastructure," *Transactions on Emerging Telecommunications Technologies*, p. e3706, 2019.
- [44] Y. Cai, Z. Wei, R. Li, D. W. K. Ng, and J. Yuan, "Joint Trajectory and Resource Allocation Design for Energy-Efficient Secure UAV Communication Systems," *IEEE Transactions on Communications*, vol. 68, no. 7, pp. 4536–4553, 2020.
- [45] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. Alazab, "Blockchain-envisioned Secure Data Delivery and Collection Scheme for 5G-based IoT-enabled Internet of Drones Environment," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9097–9111, 2020.
- [46] B. Cao, X. Wang, W. Zhang, H. Song, and Z. Lv, "A Many-Objective Optimization Model of Industrial Internet of Things Based on Private Blockchain," *IEEE Network*, vol. 34, no. 5, pp. 78–83, 2020.
- [47] B. Cao, Z. Wang, L. Zhang, D. Feng, M. Peng, and L. Zhang, "Blockchain Systems, Technologies and Applications: A Methodology Perspective," *arXiv preprint arXiv:2105.03572*, 2021.
- [48] R. Ch, G. Srivastava, T. R. Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "Security and Privacy of UAV Data Using Blockchain Technology," *Journal of Information Security and Applications*, vol. 55, p. 102670, 2020.
- [49] A. Chaer, K. Salah, C. Lima, P. P. Ray, and T. Sheltami, "Blockchain for 5G: Opportunities and Challenges," in *2019 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2019, pp. 1–6.
- [50] Z. Chang, W. Guo, X. Guo, T. Chen, G. Min, K. M. Abualnaja, and S. Mumtaz, "Blockchain-Empowered Drone Networks: Architecture, Features, and Future," *IEEE Network*, vol. 35, no. 1, pp. 86–93, 2021.
- [51] H. Chao, A. Maheshwari, V. Sudarsanan, S. Tamaskar, and D. A. DeLaurentis, "UAV Traffic Information Exchange Network," in *2018 Aviation Technology, Integration, and Operations Conference*, 2018, p. 3347.

- [52] A. Afaq, Z. Ahmed, N. Haider, and M. Imran, "Blockchain-based Collaborated Federated Learning for Improved Security, Privacy and Reliability," *arXiv preprint arXiv:2201.08551*, 2022.
- [53] J. Chen, W. Wang, Y. Zhou, S. H. Ahmed, and W. Wei, "Exploiting 5G and Blockchain for Medical Applications of Drones," *IEEE Network*, vol. 35, no. 1, pp. 30–36, 2021.
- [54] N. Cheng, W. Xu, W. Shi, Y. Zhou, N. Lu, H. Zhou, and X. Shen, "Air-Ground Integrated Mobile edge Networks: Architecture, Challenges, and Opportunities," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 26–32, 2018.
- [55] R. Cheng, Y. Sun, Y. Liu, L. Xia, D. Feng, and M. A. Imran, "Blockchain-empowered Federated Learning Approach for An Intelligent and Reliable D2D Caching Scheme," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 7879–7890, 2021.
- [56] O. Chughtai, N. Nawaz, Z. Kaleem, and C. Yuen, "Drone-Assisted Cooperative Routing Scheme for Seamless Connectivity in V2X Communication," *IEEE Access*, 2024.
- [57] R. Clarke, "The regulation of Civilian Drones, Impacts on Behavioural Privacy," *Computer Law & Security Review*, vol. 30, no. 3, pp. 286–305, 2014.
- [58] J. R. Douceur, "The Sybil Attack," in *Peer-to-Peer Systems: First International Workshop, IPTPS 2002 Cambridge, MA, USA, March 7–8, 2002 Revised Papers 1*. Springer, 2002, pp. 251–260.
- [59] A. Derhab, O. Cheikhrouhou, A. Allouch, A. Koubaa, B. Qureshi, M. A. Ferrag, L. Maglaras, and F. A. Khan, "Internet of Drones Security: Taxonomies, Open Issues, and Future Directions," *Vehicular Communications*, vol. 39, p. 100552, 2023.
- [60] R. Dong, B. Wang, K. Cao, J. Tian, and T. Cheng, "Secure Transmission Design of RIS Enabled UAV Communication Networks Exploiting Deep Reinforcement Learning," *IEEE Transactions on Vehicular Technology*, 2024.
- [61] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an Optimized Blockchain for IoT," in *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, 2017, pp. 173–178.
- [62] A. M. Elbir, B. Soner, and S. Coleri, "Federated Learning in Vehicular Networks," *arXiv preprint arXiv:2006.01412*, 2020.
- [63] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-Based Efficient p Privacy Preserving and Data Sharing Scheme of Content-Centric Network in 5G," *IET communications*, vol. 12, no. 5, pp. 527–532, 2018.



- [64] F. Fei, Z. Tu, R. Yu, T. Kim, X. Zhang, D. Xu, and X. Deng, "Cross-Layer Retrofitting of UAVs Against Cyber-Physical Attacks," in *2018 IEEE International Conference on Robotics and Automation (ICRA)*. IEEE, 2018, pp. 550–557.
- [65] X. Feng, J. Ma, Y. Miao, Q. Meng, X. Liu, Q. Jiang, and H. Li, "Pruneable Sharding-based Blockchain Protocol," *Peer-to-Peer Networking and Applications*, vol. 12, no. 4, pp. 934–950, 2019.
- [66] Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, and W. Yi, "An Efficient UAV Hijacking Detection Method Using Onboard Inertial Measurement Unit," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 17, no. 6, pp. 1–19, 2018.
- [67] M. A. Farzaneh, S. Rezapour, A. Baghaian, and M. H. Amini, "An Integrative Framework for Coordination of Damage Assessment, Road Restoration, and Relief Distribution in Disasters," *Omega*, vol. 115, p. 102748, 2023.
- [68] R. Alkadi, N. Alnuaimi, C. Y. Yeun, and A. Shoufan, "Blockchain Interoperability in Unmanned Aerial Vehicles Networks: State-of-the-Art and Open Issues," *IEEE Access*, vol. 10, pp. 14 463–14 479, 2022.
- [69] Q. Wu, L. Liu, and R. Zhang, "Fundamental Trade-offs in Communication and Trajectory Design for UAV-enabled Wireless Networks," *IEEE Wireless Communications*, vol. 26, no. 1, pp. 36–44, 2019.
- [70] Y. Qian, Y. Jiang, L. Hu, M. S. Hossain, M. Alrashoud, and M. Al-Hammadi, "Blockchain-based Privacy-Aware Content Caching in Cognitive Internet of Vehicles," *IEEE Network*, vol. 34, no. 2, pp. 46–51, 2020.
- [71] W. Xiao, M. Li, B. Alzahrani, R. Alotaibi, A. Barnawi, and Q. Ai, "A Blockchain-Based Secure Crowd Monitoring System Using UAV Swarm," *IEEE Network*, vol. 35, no. 1, pp. 108–115, 2021.
- [72] E. Ghribi, T. T. Khoei, H. T. Gorji, P. Ranganathan, and N. Kaabouch, "A Secure Blockchain-based Communication Approach for UAV Networks," in *2020 IEEE International Conference on Electro Information Technology (EIT)*. IEEE, 2020, pp. 411–415.
- [73] Z. Lv, L. Qiao, M. S. Hossain, and B. J. Choi, "Analysis of Using Blockchain to Protect the Privacy of Drone Big Data," *IEEE Network*, vol. 35, no. 1, pp. 44–49, 2021.
- [74] A. Islam and S. Y. Shin, "A Blockchain-based Secure Healthcare Scheme with the Assistance of Unmanned Aerial Vehicle in Internet of Things," *Computers & Electrical Engineering*, vol. 84, p. 106627, 2020.

- [75] M. Singh, G. S. Aujla, and R. S. Bali, "Odob: One Drone one Block-based Lightweight Blockchain Architecture for Internet of Drones," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2020, pp. 249–254.
- [76] V. A. Kanade, "Securing Drone-based Ad Hoc Network Using Blockchain," in *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*. IEEE, 2021, pp. 1314–1318.
- [77] A. Ossamah, "Blockchain As a Solution to Drone Cybersecurity," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*. IEEE, 2020, pp. 1–9.
- [78] A. Kapitonov, I. Berman, V. Manaenko, V. Rzhhevskiy, V. Bulatov, and A. Zenkin, "Robotics as a blockchain-based Platform for Unmanned Traffic Management of Mobile Vehicles," in *2019 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED UAS)*. IEEE, 2019, pp. 9–17.
- [79] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling Drones in the Internet of Things with Decentralized Blockchain-based Security," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6406–6415, 2020.
- [80] M. S. Kumar, S. Vimal, N. Jhanjhi, S. S. Dhanabalan, and H. A. Alhumyani, "Blockchain based Peer to Peer Communication in Autonomous Drone Operation," *Energy Reports*, vol. 7, pp. 7925–7939, 2021.
- [81] M. A. Cheema, M. K. Shehzad, H. K. Qureshi, S. A. Hassan, and H. Jung, "A Drone-Aided Blockchain-Based smart Vehicular Network," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4160–4170, 2020.
- [82] J. Cui, Y. Zhu, H. Zhong, Q. Zhang, C. Gu, and D. He, "Efficient Blockchain-Based Mutual Authentication and Session Key Agreement for Cross-Domain IIoT," *IEEE Internet of Things Journal*, 2024.
- [83] M. Banafaa, Ö. Pepeoğlu, I. Shayea, A. Alhammadi, Z. Shamsan, M. A. Razaz, M. Al-sagabi, and S. Al-Sowayan, "A Comprehensive Survey on 5G-and-Beyond Networks with UAVs: Applications, Emerging Technologies, Regulatory Aspects, Research Trends and Challenges," *IEEE Access*, 2024.
- [84] J. Xu, H. Yao, R. Zhang, T. Mai, S. Huang, and S. Guo, "Federated Learning Powered Semantic Communication for UAV Swarm Cooperation," *IEEE Wireless Communications*, 2024.

- [85] S. Javed, A. Hassan, R. Ahmad, W. Ahmed, R. Ahmed, A. Saadat, and M. Guizani, "State-of-the-Art and Future Research Challenges in UAV Swarms," *IEEE Internet of Things Journal*, 2024.
- [86] M. Khan, I. Ullah, A. Alkhalifah, S. Rehman, J. Shah, M. Uddin, M. Alsharif, and F. Algarni, *IEEE Transactions On Industrial Informatics*, vol. 18, no. 5, pp. 3416–3425, May 2022.
- [87] M. Rodrigues, J. Amaro, F. Osório, and B. Kalinka, "Authentication Methods for UAV Communication," in *2019 IEEE Symposium On Computers And Communications (ISCC)*, Jul 2019, pp. 1210–1215.
- [88] M. Tanveer, A. Alkhayyat, A. Naushad, N. Kumar, A. Alharbi *et al.*, "RUAM-IOD: A Robust User Authentication Mechanism for the Internet of Drones," *IEEE Access*, vol. 10, pp. 19 836–19 851, 2022.
- [89] M. Wazid, A. Das, N. Kumar, and M. Alazab, "Designing Authenticated key Management Scheme in 6G-enabled Network in a Box Deployed for Industrial Applications," *IEEE Transactions On Industrial Informatics*, vol. 17, pp. 7174–7184, 2020.
- [90] H. Li, D. Han, and M. Tang, "A Privacy-Preserving Storage Scheme for Logistics Data With Assistance of Blockchain," *IEEE Internet Of Things Journal*, vol. 9, pp. 4704–4720, 2022.
- [91] A. Sutrala, M. Obaidat, S. Saha, A. Das, M. Alazab, and Y. Park, "Authenticated Key Agreement Scheme With User Anonymity and Untraceability for 5G-Enabled Softwarized Industrial Cyber-Physical Systems," *IEEE Transactions On Intelligent Transportation Systems*, vol. 23, pp. 2316–2330, 2022.
- [92] H. Khalid, S. Hashim, S. Mumtazah Syed Ahamed, F. Hashim, and M. Chaudhary, "Secure Real-time Data Access Using Two-Factor Authentication Scheme for the Internet of Drones," in *2021 IEEE 19th Student Conference On Research And Development (SCOReD)*, 2021, pp. 168–173.
- [93] D. Kwon, S. Son, Y. Park, H. Kim, Y. Park, S. Lee, and Y. Jeon, "Design of Secure Handover Authentication Scheme for Urban Air Mobility Environments," *IEEE Access*, vol. 10, pp. 42 529–42 541, 2022.
- [94] E. A. Keller and D. E. DeVecchio, *Natural hazards: earth's processes as hazards, disasters, and catastrophes*. Routledge, 2019.
- [95] Y. Wang, Z. Su, Q. Xu, R. Li, T. H. Luan, and P. Wang, "A Secure and Intelligent Data Sharing Scheme for UAV-assisted Disaster Rescue," *IEEE/ACM Transactions on Networking*, 2023.

- [96] R. Damaševičius, N. Bacanin, and S. Misra, “From Sensors to Safety: Internet of Emergency Services (IoES) for Emergency Response and Disaster Management,” *Journal of Sensor and Actuator Networks*, vol. 12, no. 3, p. 41, 2023.
- [97] A. Ahad, Z. Jiangbina, M. Tahir, I. Shayea, M. A. Sheikh, and F. Rasheed, “6G and Intelligent Healthcare: Taxonomy, Technologies, Open Issues and Future Research Directions,” *Internet of Things*, p. 101068, 2024.
- [98] T. Li, T. Meng, G. Meng, C. Wang, B. Wang, M. Zhou, and X. Han, “Formation Optimization of Airborne Radar Coordinated Detection System using an Improved Artificial Fish Swarm Algorithm,” *Scientific Reports*, vol. 14, no. 1, p. 248, 2024.
- [99] J. Yang, X. Liu, X. Jiang, Y. Zhang, S. Chen, and H. He, “Toward Trusted Unmanned Aerial Vehicle Swarm Networks: A Blockchain-Based Approach,” *IEEE Vehicular Technology Magazine*, vol. 18, no. 2, pp. 98–108, 2023.
- [100] A. Aldaej, T. A. Ahanger, and I. Ullah, “Blockchain-Enabled M2M Communications for UAV-Assisted Data Transmission,” *Mathematics*, vol. 11, no. 10, 2023. [Online]. Available: <https://www.mdpi.com/2227-7390/11/10/2262>
- [101] Y. Zhang, X. Lin, J. Wu, B. Pei, and 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.
- [102] T. Liu, G. Bai, J. Tao, Y.-A. Zhang, and Y. Fang, “A Multistate Network Approach for Resilience Analysis of UAV Swarm Considering Information Exchange Capacity,” *Reliability Engineering & System Safety*, vol. 241, p. 109606, 2024.
- [103] S. Hafeez, R. Cheng, L. Mohjazi, M. A. Imran, and Y. Sun, “A Blockchain-Enabled Framework of UAV Coordination for Post-Disaster Networks,” 2024.
- [104] X. Wang, Y. Guo, and Y. Gao, “Unmanned Autonomous Intelligent System in 6G Non-Terrestrial Network,” *Information*, vol. 15, no. 1, p. 38, 2024.
- [105] R. Olfati-Saber, “Flocking for Multi-Agent Dynamic Systems: Algorithms and Theory,” *IEEE Transactions on automatic control*, vol. 51, no. 3, pp. 401–420, 2006.
- [106] K. Venkatesan and S. B. Rahayu, “Blockchain Security Enhancement: An Approach Towards Hybrid Consensus Algorithms and Machine Learning Techniques,” *Scientific Reports*, vol. 14, no. 1, p. 1149, 2024.

- [107] G. Raja, A. Manoharan, and H. Siljak, "UGEN: UAV and GAN-Aided Ensemble Network for Post-Disaster Survivor Detection through ORAN," *IEEE Transactions on Vehicular Technology*, 2024.
- [108] X. Duan, Y. Guo, and Y. Guo, "Design of Anonymous Authentication Scheme for Vehicle Fog Services using Blockchain," *Wireless Networks*, vol. 30, no. 1, pp. 193–207, 2024.
- [109] D. GC and C. Politis, "Optimal 3D Trajectory Design for UAV-Assisted Cellular Communications in the Post-Disaster Scenarios," *Internet Technology Letters*, p. e423, 2023.
- [110] G. Sun, L. He, Z. Sun, Q. Wu, S. Liang, J. Li, D. Niyato, and V. C. 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*, 2024.
- [111] Z. Wang, J. Li, J. Li, and C. Liu, "A Decentralized Decision-making Algorithm of UAV Swarm with Information Fusion Strategy," *Expert Systems with Applications*, vol. 237, p. 121444, 2024.
- [112] R. Xing, Z. Su, T. H. Luan, Q. Xu, Y. Wang, and R. Li, "UAVs-aided Delay-Tolerant Blockchain Secure Offline Transactions in Post-Disaster Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 11, pp. 12 030–12 043, 2022.
- [113] A. AFOTANWO, "Exploring Blockchain based Smart Contracts and Privacy Preserving Cryptocurrencies," *FUPRE Journal of Scientific and Industrial Research (FJSIR)*, vol. 8, no. 2, pp. 55–68, 2024.
- [114] G. Paulin, S. Sambolek, and 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*, vol. 237, p. 121495, 2024.
- [115] C. K. Iyer, S. Ganguli, and V. Pandey, "Perspectives on Geospatial Artificial Intelligence Platforms for Multimodal Spatiotemporal Datasets," *Advances in Scalable and Intelligent Geospatial Analytics*, pp. 17–63, 2023.
- [116] S. Nicolazzo, M. Arazzi, A. Nocera, M. Conti *et al.*, "Privacy-preserving in blockchain-based federated learning systems," *arXiv preprint arXiv:2401.03552*, 2024.
- [117] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends," *Intelligent Service Robotics*, vol. 16, no. 1, pp. 109–137, 2023.

- [118] H. J. Hadi, Y. Cao, K. U. Nisa, A. M. Jamil, and Q. Ni, "A Comprehensive Survey on Security, Privacy Issues and Emerging Defence Technologies for UAVs," *Journal of Network and Computer Applications*, vol. 213, p. 103607, 2023.
- [119] S. E. Bibri, J. Krogstie, A. Kaboli, and A. Alahi, "Smarter Eco-cities and Their Leading-edge Artificial Intelligence of Things Solutions for Environmental Sustainability: A Comprehensive Systematic Review," *Environmental Science and Ecotechnology*, vol. 19, p. 100330, 2024.
- [120] D. Kirli, B. Couraud, V. Robu, M. Salgado-Bravo, S. Norbu, M. Andoni, I. Antonopoulos, M. Negrete-Pincetic, D. Flynn, and A. Kiprakis, "Smart Contracts in Energy Systems: A Systematic Review of Fundamental Approaches and Implementations," *Renewable and Sustainable Energy Reviews*, vol. 158, p. 112013, 2022.
- [121] A. Burger, C. Cichiwskyj, S. Schmeißer, and 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*, vol. 113, pp. 607–619, 2020.
- [122] Q. Qu, I. Nurgaliev, M. Muzammal, C. S. Jensen, and J. Fan, "On Spatio-temporal Blockchain Query Processing," *Future Generation Computer Systems*, vol. 98, pp. 208–218, 2019.
- [123] T. L. Nguyen, G. Kaddoum, T. N. Do, and Z. J. Haas, "Statistical Characterization of RIS-assisted UAV Communications in Terrestrial and Non-Terrestrial Networks Under Channel Aging," *arXiv preprint arXiv:2401.14203*, 2024.
- [124] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.
- [125] S. Yuan, B. Cao, Y. Sun, Z. Wan, and M. Peng, "Secure and Efficient Federated Learning Through Layering and Sharding Blockchain," *arXiv preprint arXiv:2104.13130*, 2021.
- [126] J. Zheng, J. Xu, H. Du, D. Niyato, J. Kang, J. Nie, and Z. Wang, "Trust Management of Tiny Federated Learning in Internet of Unmanned Aerial Vehicles," *IEEE Internet of Things Journal*, 2024.
- [127] M. Aloqaily, I. Al Ridhawi, and M. Guizani, "Energy-Aware Blockchain and Federated Learning-Supported Vehicular Networks," *IEEE Transactions on Intelligent Transportation Systems*, 2021.
- [128] S. M. Azimi-Abarghouyi and V. Fodor, "Scalable Hierarchical Over-the-air Federated Learning," *IEEE Transactions on Wireless Communications*, 2024.

- [129] Y. Qu, H. Dai, Y. Zhuang, J. Chen, C. Dong, F. Wu, and S. Guo, “Decentralized Federated Learning for UAV Networks: Architecture, Challenges, and Opportunities,” *IEEE Network*, vol. 35, no. 6, pp. 156–162, 2021.
- [130] X. Hou, J. Wang, C. Jiang, X. Zhang, Y. Ren, and M. Debbah, “UAV-enabled Covert Federated Learning,” *IEEE Transactions on Wireless Communications*, 2023.
- [131] H. Tian, H. Zhang, J. Jia, M. Dong, and K. Ota, “FedBroadcast: Exploit Broadcast Channel for Fast Convergence in Wireless Federated Learning,” *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 4652–4663, 2022.
- [132] T. M. Hoang, N. M. Nguyen, and T. Q. Duong, “Detection of Eavesdropping Attack in UAV-Aided Wireless Systems: Unsupervised Learning with One-Class SVM and K-Means Clustering,” *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 139–142, 2019.
- [133] M. Arafah, H. Ould-Slimane, H. Otrok, A. Mourad, C. Talhi, and E. Damiani, “Data Independent Warmup Scheme for Non-IID Federated Learning,” *Information Sciences*, vol. 623, pp. 342–360, 2023.
- [134] H. Tian, H. Zhang, J. Jia, M. Dong, and K. Ota, “FedBroadcast: Exploit Broadcast Channel for Fast Convergence in Wireless Federated Learning,” *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 4652–4663, 2023.
- [135] S. Hafeez, R. Cheng, L. Mohjazi, Y. Sun, and M. A. Imran, “Blockchain-Enhanced UAV Networks for Post-Disaster Communication: A Decentralized Flocking Approach,” 2024.