BLOCKCHAIN FOR UxV NETWORKS

Vitor Vieira Neves
CINAV
vitor.vieira.neves@marinha.pt

António Grilo
INESC INOV-Lab
antonio.grilo@inov.pt

Mario Monteiro Marques
CINAV
mario.monteiro.marques@marinha.pt

Abstract

Many frameworks have emerged as a valuable communication protocol for lightweight, interoperable data exchange between distributed platforms and control stations. However, some of these frameworks was that a broker-centric architecture poses significant risks when applied to military-grade deployments where reliability, security, and operational continuity are non-negotiable. This study analyses the vulnerabilities of frameworks with a single point of failure, such as those based on Message Queuing Telemetry Transport (MQTT) in military contexts, and proposes a decentralised architecture that integrates hierarchical blockchain layers secured by zero-knowledge Scalable Transparent Arguments of Knowledge (zk-STARK) proofs. The approach aims to enhance survivability, auditability, and trust in UxV communication networks, offering a foundation for next-generation secure swarm coordination across multi-domain operations.

1 Introduction

Recent developments in autonomous systems have profoundly transformed modern combat operations, where coordination between aerial, ground, and maritime unmanned vehicles (UxV) plays a decisive role in mission success. Military command and control (C2) networks increasingly depend on reliable communication infrastructures that can support information exchange under contested and resource-constrained conditions. Protocols such as Message Queuing Telemetry Transport (MQTT) have gained prominence for enabling lightweight, interoperable communication between distributed platforms and control stations. However, the broker-centric architecture of MQTT presents inherent limitations when applied to military-grade deployments, particularly concerning security, scalability, and resilience against cyber and electronic warfare threats.

These challenges underscore the need for decentralised communication models capable of maintaining operational liveness even in the absence of centralised coordination. Blockchain technology emerges as a compelling alternative by distributing data validation and message dissemination across autonomous nodes, effectively eliminating single points of failure. Moreover, the combination of hierarchical blockchain architectures and advanced cryptographic mechanisms, especially zero-knowledge Scalable Transparent Arguments of Knowledge (zk-STARKs) introduces new paradigms for preserving confidentiality and integrity without compromising performance.

This study analyses the vulnerabilities of frameworks with a single point of failure, such as those based on MQTT in military contexts, and proposes a decentralised architecture that integrates hierarchical blockchain layers secured by zk-STARK proofs. The approach aims to enhance survivability, auditability, and trust in UxV communication networks, offering a foundation for next-generation secure swarm coordination across multi-domain operations.

2 The Example of REPMUS

Recent advances have facilitated the development of multi-domain control systems designed to integrate and coordinate the deployment of drones and robotic units in combat environments. These systems need secure and resilient communications in UxV-to-UxV in swarm and from swarm to command or ground control station, because they are sensitive to data [1]. They are engineered to aggregate and synthesise data from various sensor arrays, thus supporting cooperative swarm behaviour[2] and blockchain consensus makes the data shared by robotic units more trustworthy and resilient, as the information is collectively validated and remains secure even if some nodes are compromised [3].

STANAG 4817 standardises interfaces for data exchange and tasking of un-

manned systems. In Robotic Experimentation and Prototyping using Maritime Uncrewed Systems (REPMUS), this standard interface works with an MQTT Broker and enables mission-critical information to be seamlessly shared across platforms, regardless of origin or manufacturer, and supports connectivity, communication, and multi-domain operations among interoperable unmanned platforms within NATO member states[4].

However, military operational contexts impose conditions that expose critical vulnerabilities in this broker-centric approach. The reliance on a single broker introduces a substantial single point of failure. [5] any compromise of the broker—whether through kinetic attack, cyber intrusion, or electronic warfare techniques such as jamming, may result in complete loss of network connectivity, effectively fragmenting coordinated UxV operations[6]. Considering the communication-critical nature of UxVs for reconnaissance and command and control, such disruptions directly degrade situational awareness and increase the risk to human and robotic assets[7].

The security practices in MQTT commonly employ Transport Layer Security to ensure encrypted communication and certificate-based authentication. Although effective in controlled network environments, this model presents considerable challenges in dynamic military deployments, where key management, certificate revocation, and distribution are logistically complex and susceptible to disruption or compromise[8], [9].

Enhancement efforts for MQTT, such as the integration of Software-Defined Networking to decouple control and forwarding functions[10], partially mitigate latency but do not fully address systemic vulnerabilities associated with broker centralisation. Consequently, the growing emphasis in military communications on survivability, operational continuity, and cryptographic assurance under contested electromagnetic conditions has stimulated exploration of decentralised communication paradigms.

3 Replacing MQTT with Blockchain

To provide security, ensure privacy, and establish trust between entities, Satoshi Nakamoto introduced blockchain technology in 2008 [11].

Akram et al. emphasise the criticality of resilient design communication architectures that integrate decentralised trust and layered cryptography to counteract privacy breaches, spoofing, and denial of service in dynamic UxV fleets [12]. These architectures ensure operational continuity, force protection, and mission success in complex coalition campaigns.

Blockchain technology offers a transformative alternative to centralised MQTT brokers by decentralising message validation and dissemination across all participating UxV nodes [13], [14]. Each node maintains a copy of a distributed ledger that records all transactions immutably, eliminating the single point of failure inherent to broker-centric systems and isolating malicious

nodes, thus protecting the coherence of the swarm [15]. These decentralised governance models provide layered defence mechanisms that are immune to centralised attack vectors, a critical advantage in heavy theatres of electronic warfare [16].

Consensus algorithms that provide Byzantine fault tolerance properties enable the network to maintain operational liveness and data consistency even in the presence of adversarial nodes attempting to inject false or disruptive information, was demonstrated by [3] and [17].

Given limited computational power in robotic assets, storage capacity, and bandwidth, these devices struggle to sustain the costs associated with blockchain consensus mechanisms and ledger maintenance [18]. To solve these limitations, lightweight blockchain architectures are tailored to resource-constrained environments and minimise consensus overhead [19], [20].

The dynamic scalability of blockchain consensus protocols has been demonstrated to maintain throughput and latency performance as coalition sizes and node counts fluctuate, which proves to be suitable for the demands of large UxV swarms [21].

4 Hierarchical Blockchain and Multi-Level Architectures

The concept of a hierarchical blockchain has emerged to address the scalability, interoperability, and performance challenges inherent in monolithic distributed ledger systems. A hierarchical blockchain architecture organises multiple blockchains into structured layers, typically referred to as Layer 1 (L1) and Layer 2 (L2), where each layer serves a distinct functional purpose within the ecosystem [22]. This model promotes modularity and enables different consensus mechanisms or transaction validation schemes to coexist under a unified governance framework, improving both efficiency and adaptability across diverse applications.

Layer 1 (L1) blockchains constitute the foundational infrastructure of the system, handling consensus, transaction completion, and security guarantees. Well-known examples include Bitcoin and Ethereum, which maintain decentralised trust through global consensus protocols [23]. However, computational and storage demands to maintain the full L1 consensus can limit throughput and increase transaction latency. To alleviate this, hierarchical approaches introduce secondary layers that offload transactional processing while preserving L1's security and decentralisation guarantees.

Layer 2 (L2) solutions are built on top of the base layer to provide high-performance transaction execution through mechanisms such as Roll-up, side chain, and state channels [24]. Roll-up, for example, aggregates multiple off-chain transactions into a single cryptographic proof submitted to the L1 chain, thereby improving scalability without compromising trust. In this context, the

use of zk-proofs, particularly zk-STARKs, is becoming essential to ensure verifiable computation with minimal overhead on-chain [25].

A key advantage of hierarchical blockchain architectures lies in their ability to support heterogeneous trust domains and dynamic interoperability. Each subchain or side chain can implement customised protocols tailored to domain-specific requirements, such as privacy-preserving computation, low-latency data transfer, or regulatory compliance [26].

5 Benefits of Using zk-STARK in Blockchain

Although blockchain ensures transparency and immutability, exposure of metadata in open ledgers may compromise tactical secrecy. zk-STARKs provide a cryptographic solution that allows nodes to prove transaction validity without revealing the underlying data [27]. This privacy-preserving approach is essential in military contexts where command secrecy and sensor data confidentiality are paramount.

The zk-STARKs enable succinct, transparent and post-quantum secure proofs of correctness, making them ideal for hierarchical blockchains scalable and privacy-preserving [25].

The zk-STARKs differ from earlier zero-knowledge proofs such as zk-SNARKs by removing the requirement for trusted setup ceremonies, avoiding a major vector for backdoor vulnerabilities, especially problematic in multinational and coalition environments or dynamic environments [27]. Moreover, zk-STARKs offer enhanced scalability, allowing efficient validation of large volumes of UxV communications within swarm operations without imposing prohibitive computational overhead or latency [28].

Critically, ZK-STARKs provide post-quantum security, protecting UxV communication records and proofs against future quantum-based adversarial capabilities [27], [28]. This future proofs military communication networks, extending their operational viability and trustworthiness over extended campaign durations.

When combined with ZK-STARKs, these architectures further enhance integrity by allowing participants to verify large batches of off-chain computations efficiently, without having to reveal the underlying data. This balance between transparency and confidentiality is a defining feature of modern L2 designs.

6 Proposed Architecture

The proposed communication architecture integrates blockchain nodes directly within each UxV platform, decentralising control, and eliminating the reliance on vulnerable centralised brokers. Each node maintains versions of a

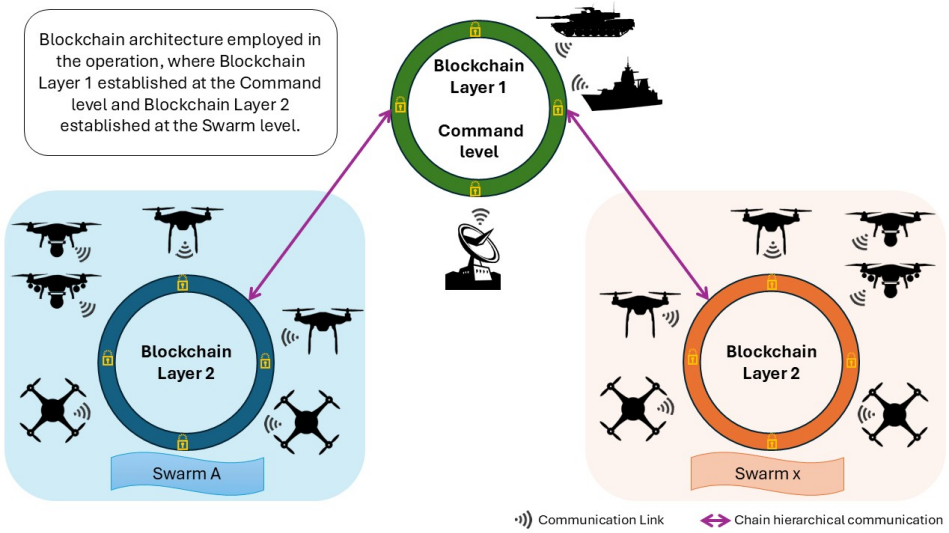

Figure 1: Proposed blockchain architecture.

cryptographically verifiable ledger, recording sensor data, command acknowledgements, and operational events.

ZK-STARK-based cryptographic proofs secure transaction authenticity and data integrity without disclosing sensitive information, preserving operational confidentiality while enabling transparent auditing. The network relies on Byzantine fault-tolerant consensus protocols to maintain synchronisation and isolate anomalous nodes, thus securing swarm coherence [15], [29].

Smart contracts within the blockchain automate task allocation, resource distribution, and dynamic mission adjustments, addressing communication disruptions with adaptive reconfiguration [29]. Hierarchical and federated blockchain frameworks support multi-partner coalitions with controlled data sharing and mutual authentication, as explored in vehicular network contexts [22].

The hierarchical blockchain architecture used in the operation, L1, located at the command level, provides global coordination, data integrity, and control the main goals, while L2, established at the Swarm level, manages local interactions, consensus, and real-time operational data exchange as shown in Figure 1.

7 Conclusion

The analysis demonstrates that while MQTT remains a valuable communication protocol for lightweight and interoperable data exchange, its broker-centric architecture poses significant risks in military environments where reliability, security, and operational continuity are non-negotiable. The inherent

single point of failure, vulnerability to cyber and electronic warfare, and limitations in key management and auditability highlight the necessity of transitioning to decentralised communication paradigms.

Blockchain technology, particularly in its hierarchical and L2 augmented forms, offers a robust foundation for replacing centralised brokers by distributing trust, ensuring data integrity, and maintaining operational resilience even under adversarial conditions. The integration of ZK-STARK proofs further enhances this framework by introducing post-quantum security and privacy-preserving verifiability, enabling secure, scalable, and confidential coordination among unmanned systems.

The proposed architecture, which combines hierarchical blockchain layers, Byzantine fault-tolerant consensus, and ZK-STARK-based verification, transforms the communication model of UxV swarms into a self-sustaining, tamper-resistant, and adaptable ecosystem. Support mission-critical decision making while maintaining secrecy and interoperability. Ultimately, this decentralised approach aligns with the future direction of resilient military communication systems, merging cryptographic assurance, distributed autonomy, and operational survivability into a unified next-generation control paradigm.

References

[1] Y. Ko et al., "Drone secure communication protocol for future sensitive applications in military zone," *Sensors*, vol. 21, no. 6, 2021, ISSN: 1424-8220. DOI: 10.3390/s21062057.

[2] D. Yu, J. Li, Z. Wang, and X. Li, "An Overview of Swarm Coordinated Control," *IEEE Transactions on Artificial Intelligence*, vol. 5, no. 5, pp. 1918–1938, May 2024, ISSN: 2691-4581. DOI: 10.1109/TAI.2023.3314581.

[3] V. Strobel, E. Castelló Ferrer, and M. Dorigo, "Blockchain technology secures robot swarms: A comparison of consensus protocols and their resilience to byzantine robots," *Frontiers in Robotics and AI*, vol. Volume 7 - 2020, 2020, ISSN: 2296-9144. DOI: 10.3389/frobt.2020.00054.

[4] NATO Standardization Office, "Stanag 4817 – interoperability of unmanned systems," NATO, Tech. Rep., 2021.

[5] B. M. Agostinho, S. Chessa, R. Perego, M. A. Ribeiro Dantas, and A. Sandro Roschildt Pinto, "MQTT-Chain: An MQTT approach using blockchain and smart contracts to achieve a new Quality of Service level," in *2024 11th International Conference on Future Internet of Things and Cloud (FiCloud)*, IEEE, Aug. 2024, pp. 316–323, ISBN: 979-8-3315-2719-8. DOI: 10.1109/FiCloud62933.2024.00056.

[6] N. Kumar and A. Chaudhary, "Surveying cybersecurity vulnerabilities and countermeasures for enhancing UAV security," *Computer Networks*, vol. 252, p. 110 695, Oct. 2024, ISSN: 1389-1286. DOI: 10.1016/J.COMNET.2024.110695.

[7] T. Rana, A. Shankar, M. K. Sultan, R. Patan, and B. Balusamy, "An Intelligent approach for UAV and Drone Privacy Security Using Blockchain Methodology," in *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, IEEE, Jan. 2019, pp. 162–167, ISBN: 978-1-5386-5933-5. DOI: 10.1109/CONFLUENCE.2019.8776613.

[8] H. Hassan et al., "A comprehensive survey on security, privacy issues and emerging defence technologies for uavs," *Journal of Network and Computer Applications*, vol. 213, p. 103 607, 2023, ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2023.103607.

[9] A. Aljumah, "Uav-based secure data communication: Multilevel authentication perspective," *Sensors*, vol. 24, no. 3, 2024, ISSN: 1424-8220. DOI: 10.3390/s24030996.

[10] Y. Yuan, H. Sun, Y. Li, and C. Wang, "An sdn-mqtt based communication system for battlefield uav swarms," *IEEE Communications Magazine*, vol. 57, no. 8, pp. 41–47, 2019. DOI: 10.1109/MCOM.2019.1900291.

[11] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. [Online]. Available: www.bitcoin.org.

[12] R. N. Akram et al., "Security, privacy and safety evaluation of dynamic and static fleets of drones," in *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*, vol. 2017-September, IEEE, Sep. 2017, pp. 1–12, ISBN: 978-1-5386-0365-9. DOI: 10.1109/DASC.2017.8101984.

[13] M. Dorigo et al., "Blockchain technology for mobile multi-robot systems," *Nature Reviews Electrical Engineering*, vol. 1, pp. 264–274, 2024. DOI: https://doi.org/10.1038/s44287-024-00034-9.

[14] D. Hawashin et al., "Blockchain applications in uav industry: Review, opportunities, and challenges," *Journal of Network and Computer Applications*, vol. 230, p. 103 932, 2024, ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2024.103932.

[15] V. Strobel et al., "Robot swarms neutralize harmful byzantine robots using a blockchain-based token economy," *Science Robotics*, vol. 8, no. 79, eabm4636, 2023. DOI: 10.1126/scirobotics.abm4636.

[16] B. Li, Y. Chen, Z. Zuo, and J. Huang, "Blockchain-based data integrity and privacy protection method for swarm robotics," in *Proceedings of 2021 Chinese Intelligent Systems Conference*, Singapore: Springer Singapore, 2022, pp. 698–707.

[17] S. Alsamhi et al., "Blockchain-empowered security and energy efficiency of drone swarm consensus for environment exploration," *IEEE Transactions on Green Communications and Networking*, vol. 7, no. 1, pp. 328–338, 2023. DOI: 10.1109/TGCN.2022.3195479.

[18] K. Mershad, "COSIER: A comprehensive lightweight blockchain system for IoT networks," *Computer Communications*, vol. 224, pp. 125–144, Aug. 2024, ISSN: 01403664. DOI: 10.1016/j.comcom.2024.06.007.

[19] C. Li, J. Zhang, X. Yang, and L. Youlong, "Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices," *Information Processing & Management*, vol. 58, no. 4, p. 102 602, Jul. 2021, ISSN: 03064573. DOI: 10.1016/j.ipm.2021.102602.

[20] 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, ISSN: 21693536. DOI: 10.1109/ACCESS.2022.3145199.

[21] J. Queralta et al., "Blockchain and distributed ledger technologies for decentralized multi-robot systems," *Current Robotics Reports*, vol. 4, pp. 1–12, Sep. 2023. DOI: 10.1007/s43154-023-00101-3.

[22] C. Divakarala et al., "Hierarchical blockchain architecture for secure data sharing in vehicular networks," *International Journal of Information Technology*, vol. 15, pp. 1689–1697, 2023. DOI: https://doi.org/10.1007/s41870-023-01175-0.

[23] S. Hafeez et al., "Blockchain-assisted uav communication systems: A comprehensive survey," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 558–580, 2023, ISSN: 2644-1330. DOI: 10.1109/OJVT.2023.3295208.

[24] N. Kostopoulos, Y. C. Stamatiou, C. Halkiopoulos, and H. Antonopoulou, "Blockchain Applications in the Military Domain: A Systematic Review," *Technologies 2025, Vol. 13, Page 23*, vol. 13, no. 1, p. 23, Jan. 2025, ISSN: 2227-7080. DOI: 10.3390/TECHNOLOGIES13010023.

[25] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, *Scalable, transparent, and post-quantum secure computational integrity*, Cryptology ePrint Archive, Paper 2018/046, 2018. [Online]. Available: https://eprint.iacr.org/2018/046.

[26] K. Srinivasan, U. Divakarala, K. Chandrasekaran, K. Hemant, and K. Reddy, "A hierarchical blockchain architecture for secure data sharing for vehicular networks," *Int. j. inf. tecnol*, vol. 15, no. 3, pp. 1689–1697, 2023. DOI: https://doi.org/10.1007/s41870-023-01175-0.

[27] 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. 103 678, 2024, ISSN: 2214-2126. DOI: https://doi.org/10.1016/j.jisa.2023.103678.

[28] M. El-Hajj and B. Oude Roelink, "Evaluating the efficiency of zk-snark, zk-stark, and bulletproof in real-world scenarios: A benchmark study," *Information*, vol. 15, no. 8, 2024, ISSN: 2078-2489. DOI: 10.3390/info15080463.

[29] L. Zhang, L. Hang, K. Zu, and Y. Wang, "A smart contract-based algorithm for offline uav task collaboration: A new solution for managing communication interruptions," *Drones*, vol. 8, p. 781, Dec. 2024. DOI: 10.3390/drones8120781.