Vol 6, Issue 1, January 2026 www.ijesti.com E-ISSN: 2582-9734
International Journal of Engineering, Science, Technology and Innovation (IJESTI)

High-Assurance Drone Delivery Networks Enabled by Blockchain Technology

B. Saritha [1]

[1] Research Scholar, Department of Computer Science, Mansarovar Global University, Sehore, M.P., India.

Dr. Dhirendra Kumar Tripathi [2]

[2] Supervisor, Department of Computer Science, Mansarovar Global University, Sehore, M.P., India.

ABSTRACT

Data security, communication dependability, and operational integrity have become key considerations due to the rapid usage of unmanned aerial vehicles (UAVs) for delivery services. This study compares traditional networks versus blockchain-enabled UAV networks in terms of performance and security across a range of load circumstances and fleet sizes. We looked at important indicators such gas usage, packet delay, authentication success, data integrity, delivery time, and battery use. Although the results show a little increase in latency, throughput overhead, and battery use with blockchain integration, the authentication reliability, data consistency, and delivery success rates are significantly improved across all fleet sizes. These results demonstrate how blockchain works to provide trustworthy, tamper-proof drone operations, drawing attention to the trade-off between relatively little performance overhead and strong operational reliability in delivery systems that use unmanned aerial vehicles.

Keywords: *Drone Delivery, Networks, Blockchain Technology.*

I. INTRODUCTION

Drones, also known as unmanned aerial vehicles (UAVs), have emerged as a game-changer in supply chain management because to the exponential growth of transportation and logistics networks. Especially in urban and rural regions, drone delivery networks provide unmatched accessibility, efficiency, and speed, reshaping the conventional delivery ecology. By using the autonomous capabilities of drones, these networks are able to transfer commodities, medical supplies, deliveries, and crucial resources. This way, they avoid the problems that typical road-based delivery systems have, such as traffic, infrastructural limits, and geographical obstacles. There is a growing need for delivery methods that are efficient, dependable, and secure due to the exponential growth of e-commerce, telemedicine, and on-demand delivery services. With their scalability, autonomy, and capacity to access inaccessible areas, drones provide a solution that can keep up with the demands of modern logistics. Concerns around data security, operational transparency, and stakeholder confidence are especially acute with the introduction of large-scale drone delivery networks. Flight routes, sensor readings, product details, and consumer data are just a few examples of the vast amounts of real-time data produced by drone operations. This data is then sent via wireless networks and stored in digital platforms for analytics, compliance, and monitoring. Drone networks are vulnerable to threats such data manipulation, illegal access, hacking, and system failures due to the sensitive nature of the data and the autonomous and decentralised nature of the networks. These threats might jeopardise operational integrity and public safety. Strong frameworks are required to address these risks and guarantee the availability, integrity, and security of data at every stage of delivery.

To solve the problems of trustworthiness and security in drone delivery networks, blockchain technology has arisen as an attractive option. To prevent unauthorised changes and promote transparency, blockchain records every transaction or data exchange inside the network securely, timestamps it, and makes it

immutable. All parties involved in drone delivery operations, from service providers to regulatory bodies and end-users, may rest certain that data integrity will be preserved thanks to blockchain integration, which will allow for confident verification and auditing of every stage of the delivery process. The distributed ledger technology known as blockchain makes the distribution network more resilient by eliminating the need for a central authority, which in turn reduces the likelihood of cyberattacks and single points of failure. Also, blockchain networks include smart contracts, which are protocols that can execute themselves. These contracts allow for the automatic verification of delivery milestones, which in turn triggers activities like payment settlements, compliance checks, and route optimisation. All of this happens without any human interaction. Because the blockchain records every activity publicly, this automation not only speeds up operational procedures but also improves accountability. This network will be the backbone of the supply chain infrastructure of the future because it combines the autonomous delivery capabilities of drones with the immutable and transparent ledger of blockchain. This synergy solves the problems of efficiency and security.

Additionally, there are substantial benefits to improving privacy and compliance with regulatory frameworks using blockchain-enabled drone delivery networks. Because drone operations frequently capture sensitive information—such as geolocation data, recipient details, and real-time surveillance data—data privacy is still a major anxiety. Unauthorised individuals can alter, steal, or abuse data housed in traditional central data storage systems, making them susceptible to breaches. Blockchain technology guarantees that sensitive information is safeguarded from manipulation and unauthorised access by encrypting it, distributing it over numerous nodes, and making it available only through cryptographic keys. The General Data Protection Regulation (GDPR) and other national frameworks controlling data collection, storage, and processing may be more easily complied with with the help of this decentralised security mechanism. Service providers can track the whereabouts of each package, confirm its legitimacy, and keep detailed records of transactions thanks to blockchain's improved traceability in the delivery ecosystem. Users are able to monitor the progress of their orders in real time and ensure the process's authenticity, which boosts consumer confidence and operational efficiency. To improve public safety and accountability, blockchain-enabled traceability is essential in crucial applications like the supply of medical supplies, vaccinations, or disaster relief items. It guarantees that resources reach their intended destination without diversion, counterfeiting, or delay.

Intelligent and adaptable supply chain systems may be built around the integration of blockchain technology with drone delivery networks, which enables enhanced analytics and optimisation. Using blockchain platforms, drone data can be safely aggregated and used to train machine learning models, optimise flight routes, predict maintenance needs, and improve resource allocation. Drone data can include flight telemetry, environmental conditions, energy consumption, and package handling metrics. By reducing operational costs, improving energy efficiency, and enhancing service dependability, organisations may increase drone delivery services with minimal risks, thanks to data-driven insights. Collaborative operations, swarm intelligence, and dynamic scheduling are all made possible by blockchain, which also allows for decentralised coordination between several service hubs and drones. All stakeholders may review performance data, enforce compliance with airspace laws, and guarantee network resources are distributed fairly because all operational decisions are recorded on the blockchain. The scalability of drone delivery networks is improved by this decentralised coordination approach, which allows them to function successfully in places affected by disasters or complicated urban environments where centralised management may not be viable or safe.

II. REVIEW OF LITERATURE

Nar, Dharna & Kotecha, Radhika. (2022) Agriculture, energy and utilities, GIS, package delivery, cinematography, industrial inspection, and many more can benefit from DraaS (Drone-as-a-Service), thanks to the fast technological development of strong and intelligent UAVs, often known as drones. Drones have many practical uses in industry due to their capacity to transport payloads and collect data using onboard cameras and sensors. Autonomous mission execution, operations, management, safety assurance, and secure communications all present significant obstacles. The most recent findings in the areas of DraaS-related Artificial Intelligence and Blockchain are summarised in this study article. The distributed ledger technology known as blockchain encrypts all of the shared data using public key encryption and hash algorithms. In addition to enhancing the UAVs' security and transparency, it may be utilised to guarantee the accuracy of recorded data. Adding AI makes the system smarter, which means it can make better decisions and, in the long run, transform drones into vehicles that can fly themselves around and complete missions.

Babazade, Ayla & Gurtov, Andrei. (2022) The article delves at the possibility of registering drones using blockchain technology. Each drone may be granted a unique and immutable identification using blockchain technology. This allows for safe data transmission, real-time tracking, and enhanced compliance with laws and regulations. This paper argues that integrating blockchain into drone registration can increase security, transparency, and efficiency.

Wu, Yulei et al., (2021) Drones equipped with 5G might find use in many different fields, including the military and civilian sectors, for example, keeping tabs on protesters or implementing social and physical isolation measures during pandemics like COVID-19. Applications like this often use 5G networks to transfer (abundant) data collected by drones to distant data centres for analysis and storage. Therefore, 5G-enabled drone communications are based on security and privacy issues. After outlining the framework for 5G-enabled drone communications and blockchain, we examine current blockchain-based solutions to address our hypothesis about blockchain's ability to help with privacy protection. Additionally, we take a look at current laws and data protection rules that should be thought about when designing blockchain-based solutions. We also try to spot possible problems and unanswered questions that might guide future studies.

Du, Jianbo et al., (2021) Drones' adaptability, scalability, affordability, and ease of deployment have led to their widespread application in numerous industries in recent years. On the other hand, communication networks are particularly worried about their security. Data transmission for drone systems may be made more efficient, transparent, and safe with the use of blockchain technology, which is a distributed network. In addition, blockchain-based drone systems can benefit from enhanced data storage and processing capabilities offered by cloud and edge computing. Drones may serve as mobile terminals and base stations in many scenarios, including disaster assistance, concerts, sparsely populated region coverage, and crowd surveillance. In this paper, we present a blockchain-enabled edge-cloud computing network architecture (DBECN) that makes use of drones. The architecture can supply a wealth of caching and computing resources for processing tasks that are both time-sensitive and resource-intensive, as well as for analysing, caching, and processing large amounts of data, when coupled with terrestrial edge nodes and cloud centres. Specifically, our DBECN architecture introduces a trustworthy data sharing scheme that lets various terminal-based drones store and share data efficiently and securely through the use of blockchain technology deployed at the edge nodes.

Kumar, Adarsh et al., (2020) A recently identified coronavirus causes an infectious condition known as coronavirus disease (COVID-19). Its severe and alarmingly rapid spread has sparked global worry and is reminiscent of influenza viruses, which have caused a global pandemic. It infected 5.89 million people

over the world within five months (by May 2020), and 357 thousand of them perished. When dealing with the COVID-19 outbreak, Unmanned Aerial Vehicles (UAVs), sometimes known as drones, are incredibly useful. By analysing real-time and simulated case studies, this paper delves into drone-based systems, COVID-19 pandemic scenarios, and offers architectural solutions for managing these crises. The suggested design incorporates a push-pull data retrieval system that records observations in Body Area Networks (BANs) using wearable sensors. In locations where wireless or Internet access is poor or where the likelihood of COVID-19 spreading is high, the suggested design is advantageous, especially in rural and heavily populated pandemic zones. It aids in taking the necessary actions when needed by collecting and storing a large volume of data within a certain time frame. It has been noted that a vast area may be sanitised, thermal images collected, patients identified, etc., in a short amount of time (2 KMs within 10 minutes approx.) via the aerial route in the real-time drone-based healthcare system deployment for COVID-19 operations. The simulation shows the same data with the inclusion of collision-resistant tactics that are effective for both indoor and outdoor healthcare operations.

III. METHODOLOGY

The research used a blockchain architecture to test the effectiveness of UAV networks. Transaction performance indicators such as throughput, confirmation time, gas consumption, and transaction delay were analysed using three operating scenarios: low load, moderate load, and heavy load. Data integrity detection, authentication success rate, network performance, average packet delay, and other communication QoS metrics were also assessed. Using parameters such as average delivery time, battery consumption, and delivery success rate, the performance of drone fleets with 10, 30, and 50 drones was evaluated.

In order to gather data, we used both regular networks and blockchain-secured networks to model drone delivery operations in a controlled setting.

IV. RESULTS AND DISCUSSION

Table 1: Blockchain Transaction Performance Metrics in Drone Delivery Frameworks

Metric	Low Load Scenario	Moderate Load Scenario	High Load Scenario
Transaction Latency (sec)	2.1	3.5	5.0
Gas Consumption (Gwei)	21	28	35
Confirmation Time (sec)	12	18	24
Throughput (tx/sec)	15	12	8

The blockchain-based drone delivery system experiences an increase in gas consumption, confirmation time, transaction delay, and a drop in throughput as the load on the system grows (Table 1). Transactions are quick (2.1 sec) and efficient (15 tx/sec) when there is little to no demand, but when there is a lot of it, processing capacity drops to 8 tx/sec, computational expenses go up to 35 Gwei, and delays go down to 5 sec. This exemplifies the challenge of balancing security and performance in UAV networks that are enabled by blockchain technology.

Table 2: Communication QoS Metrics for Secure UAV Networks

Metric	Standard Network	Blockchain Secured Network
Average Packet Delay (ms)	85	110
Throughput (Mbps)	11.2	9.8
Authentication Success Rate (%)	94	99
Data Integrity (Detected Tampering)	98	100

Table 2 presents a comparison of communication quality indicators between blockchain-secured networks and conventional UAV networks. The overhead of blockchain validation and encryption causes the blockchain-secured network to have a little lower throughput (9.8 Mbps vs. 11.2 Mbps) and a slightly greater average packet latency (110 ms vs. 85 ms). But with data integrity reaching 100% and authentication success rates increasing from 94% to 99%, it greatly boosts security and guarantees dependable, tamper-free connections. This demonstrates the trade-off in blockchain-enabled UAV networks between a small performance overhead and improved security.

Table 3: Drone Fleet Performance Metrics

Fleet Size	Network Type	Average Delivery Time (min)	Battery Consumption (%)	Delivery Success Rate (%)
10	Standard Network	12.5	18	94
	Blockchain-Secured Network	13.8	20	99
30	Standard Network	15.0	35	90
	Blockchain-Secured Network	17.2	38	97
50	Standard Network	19.0	55	88
	Blockchain-Secured Network	21.5	60	95

Table 3 displays the results of various sized drone fleets that were operated over both regular and blockchain-protected networks. The larger the fleet, the higher the operating load, which in turn causes the average delivery time and battery usage to climb. Delivery times and battery use for blockchain-secured networks are somewhat greater than those for regular networks because of encryption and blockchain processing. Success rates increased from 94% to 99% with 10 drones, 90% to 97% with 30 drones, and 88% to 95% with 50 drones, demonstrating their constant improvement in delivery dependability. While there may be a little impact on efficiency, this proves that integrating blockchain technology improves operational security and dependability.

V. CONCLUSION

Drone delivery systems are far more secure, trustworthy, and reliable after implementing blockchain technology, according to the study. Adopting this system guarantees practically flawless authentication, data that cannot be tampered with, and increased delivery success rates, especially in operations involving large fleets of vehicles, but it does so at the expense of somewhat increased energy consumption, packet delays, and transaction latency. Blockchain technology reduces vulnerabilities to hacking, data corruption, and system outages by creating a decentralised and transparent framework. These findings highlight the practicality of incorporating blockchain technology into UAV networks as a means to provide reliable drone delivery services, with reasonable efficiency sacrifices that can be easily tolerated. This opens the door to scalable, high-assurance airborne logistics.

REFERENCES

1. G. Jitender, S. Dobhal, V. Kumar, and M. Singh, "Drone Technology to Enhance Healthcare Delivery Access," *Indian Journal of Community Health*, vol. 36, no. 5, pp. 629–632, 2024.
2. A. Taheri, A. Ghodousian, and R. Abedian, "Review of path planning models, environmental constraints, and application domains in drone delivery systems," *J. Algorithms Comput.*, vol. 56, no. 1, pp. 15–33, 2024.
3. M. Raivi, S. M. A. Huda, M. M. Alam, and S. Moh, "Drone routing for drone-based delivery systems: A review of trajectory planning, charging, and security," *Sensors*, vol. 23, no. 3, pp. 1463–1489, 2023.

4. R. Sham, C. S. Siau, S. Tan, D. Kiu, H. Z. Thew, G. Selvachandran, S. Quek, N. Ahmad, and M. H. Mohd Ramli, "Drone Usage for Medicine and Vaccine Delivery during the COVID-19 Pandemic: Attitude of Health Care Workers in Rural Medical Centres," *Drones*, vol. 6, no. 1, pp. 1–10, 2022.
5. M. Singh, G. S. Aujla, R. S. Bali, R. S. Batth, A. Singh, S. Vashisht, and A. Jindal, "CovaDel: A blockchain-enabled secure and QoS-aware drone delivery framework for COVID-like pandemics," *Computing*, vol. 104, no. 7, pp. 1589–1613, 2022.
6. D. Nar and R. Kotecha, "Enhancement of Drone-as-a-Service Using Blockchain and AI," *International Journal of Next-Generation Computing*, vol. 13, no. 4, pp. 885–900, 2022.
7. A. Babazade and A. Gurtov, "Registration of Drones through Blockchains," *Azerbaijan Journal of High Performance Computing*, vol. 5, no. 2, pp. 318–325, 2022.
8. 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.
9. J. Du, H. Cao, A. Sun, G. Lu, H. Anisi, and A. Jindal, "Drone-Assisted and Blockchain-Enabled Edge-Cloud Computing Networks: Architecture Design, Case Study, and Future Directions," *IEEE Internet of Things Magazine*, vol. 4, no. 4, pp. 54–59, 2021.
10. A. Kumar, K. Sharma, H. Singh, S. Naugriya, S. S. Gill, and R. Buyya, "A Drone-based Networked System and Methods for Combating Coronavirus Disease (COVID-19) Pandemic," *Future Generation Computer Systems*, vol. 115, no. 2, pp. 1–12, 2020.
11. A. Lin, D. He, N. Kumar, K. K. R. Choo, A. Vinel, and X. Huang, "Security and Privacy for the Internet of Drones: Challenges and Solutions," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 64–69, 2018.
12. A. Claesson *et al*., "Drones May Be Used to Save Lives in Out of Hospital Cardiac Arrest Due to Drowning," *Resuscitation*, vol. 114, no. 1, pp. 152–156, 2017.