ISSN 1648-7788 / eISSN 1822-4180

VILNIUS TECH
Vilnius Gediminas Technical University

AVIATION

2025
Volume 29
Issue 3
Pages 191–200
https://doi.org/10.3846/aviation.2025.24463

BLOCKCHAIN-BASED SECURE COMMUNICATION FOR UAV NETWORKS: A DECENTRALIZED APPROACH TO GNSS SPOOFING DETECTION

Paulina DRAUGELYTĖ [1]✉, Ivan SUZDALEV

Antanas Gustaitis Aviation Institute, Vilnius Gediminas Technical University, Vilnius, Lithuania

Article History:
- received 12 April 2025
- accepted 4 June 2025

Abstract. Ensuring secure communication in Unmanned Aerial Vehicle (UAV) networks is a critical challenge due to vulnerabilities such as GNSS (Global Navigation Satellite System) spoofing, jamming, and unauthorized data manipulation. This research investigates the feasibility of blockchain technology as a decentralized and immutable framework for enhancing UAV communication security. A blockchain-based GNSS spoofing detection system is designed, implemented, and validated within a simulated environment integrating AirSim, Ethereum blockchain (Ganache), smart contract (Solidity), and Python-based UAV simulations. The proposed system employs a consensus mechanism among UAVs to detect anomalous GNSS data and mitigate spoofing attacks in real-time. Performance evaluation metrics – transaction latency, blockchain throughput, gas consumption, detection accuracy, storage usage, and energy consumption – demonstrate the system's capability to securely validate UAV location data. Findings indicate that blockchain ensures data integrity and resilience against cyber threats, though challenges related to transaction latency, scalability and computational overhead persist. The study contributes to the field of aerospace cybersecurity and IoT-based UAV networks by proposing an innovative approach to autonomous, trustless UAV coordination. Future work will focus on optimizing the consensus mechanism and reducing blockchain resource consumption to enhance real-world applicability.

Keywords: UAV communication, blockchain technology, GNSS spoofing detection, smart contracts, consensus mechanism, decentralized networks, aerospace cybersecurity, UAV swarm resilience.

✉Corresponding author. E-mail: *paulinadraug@gmail.com*

Notations

Abbreviations

API – Application Programming Interface;
DAG – Directed Acyclic Graph;
DoS – Denial of Service;
FNR – False Negative Rate;
GNSS – Global Navigation Satellite System;
GPU – Graphics Processing Unit;
IMU – Inertial Measurement Unit;
IoT – Internet of Things;
JSON – JavaScript Object Notation;
PoS – Proof of Stake;
TPR – True Positive Rate;
tx/sec – transactions per second;
UAV – Unmanned Aerial Vehicle;
UNIX – Uniplexed Information and Computing System; refers here to UNIX epoch time, the standard for tracking time as the number of seconds since January 1, 1970 (00:00:00 UTC);
Web3.py – Python library for interacting with Ethereum blockchain nodes via Web3 interface.

1. Introduction

Unmanned Aerial Vehicles (UAVs) have become integral to a variety of missions, including military operations, rescue, logistics, and monitoring tasks (Sharma & Mehra, 2023). Their growing adoption across sectors is driven by advancements in communication networks and multi-UAV systems, enabling autonomous coordination and data exchange (Hafeez et al., 2023; Sihag et al., 2023). However, this increased interconnectivity also expands their attack surface, making UAV systems increasingly vulnerable to cyber threats that can compromise navigation, control, and mission integrity (Yaacoub et al., 2020). Among these, GNSS spoofing remains one of the most critical, allowing adversaries to manipulate positioning data through counterfeit signals, leading to navigation failures or system hijacking (Gupta et al., 2021).

While encryption and authentication protocols offer some protection, centralized UAV communication architectures suffer from single points of failure and limited scalability, rendering them ineffective against distributed and evolving attacks such as DoS and man-in-the-middle intrusions (Jensen et al., 2019; Riahi Manesh & Kaabouch,

2019). As UAV networks continue to expand in complexity and autonomy, these vulnerabilities are exacerbated (Kumar et al., 2022). To address these challenges, researchers increasingly advocate for decentralized and trustless security frameworks.

Blockchain, originally designed for secure financial transactions, offers decentralization, immutability, and cryptographic integrity-making it well-suited for UAV security challenges such as GNSS spoofing (Almotery, 2020; Atlam et al., 2018; Ghribi et al., 2020; Zheng et al., 2017). Unlike centralized security models, blockchain eliminates single points of failure and ensures that data integrity is preserved across a distributed network (Ghribi et al., 2020). In the context of UAV security, blockchain can provide real-time, tamper-proof validation of positional data, preventing adversaries from injecting false GNSS signals or manipulating UAV navigation (Almotery, 2020).

Despite extensive applications of blockchain in sectors like finance, supply chain management, and healthcare (Alladi et al., 2020), its deployment in UAV cybersecurity – particularly for real-time GNSS spoofing detection – remains underexplored. Current literature focuses largely on identity management, encrypted data sharing, and swarm coordination (Ferrag & Maglaras, 2019), while the development of blockchain-based spoofing detection mechanisms remains a critical gap. Addressing this void presents an opportunity to design a resilient, tamper-proof framework for positional data verification in UAV systems.

However, realizing this potential is not without obstacles. Despite the advantages of blockchain, its integration with UAV systems presents several challenges. These include transaction latency affecting real-time detection, high energy and computational demands, and scalability constraints as UAV network size increases (Alladi et al., 2020; Gugueoth et al., 2023; Zheng et al., 2017; Zhou et al., 2020).

These challenges lead to the following key research questions:

- How effectively can blockchain-based systems detect GNSS spoofing in UAV networks?
- What is the trade-off between detection performance, latency, and computational efficiency?
- How scalable is the proposed solution for large UAV fleets?
- What are the energy efficiency implications of blockchain integration in resource-limited UAVs?

Accordingly, this study aims to design, implement, and evaluate a blockchain-based GNSS spoofing detection system tailored for UAV networks. The proposed system integrates a simulated multi-UAV environment using AirSim and Python with an Ethereum-based blockchain backend (via Ganache) and smart contract logic (Solidity) to enable decentralized geolocation verification. By leveraging consensus among UAVs, the system autonomously detects and mitigates spoofing attacks in real time, eliminating reliance on centralized infrastructure and enhancing network resilience.

The key contributions of this work are as follows:

- A security-oriented analysis of UAV communication vulnerabilities, with a focus on GNSS spoofing threats and their operational impact.
- The development of a modular, blockchain-enabled framework for spoofing detection, employing smart contracts and consensus voting among UAVs.
- A comprehensive performance evaluation of the system across critical metrics including detection accuracy, transaction latency, throughput, gas consumption, energy efficiency, and storage overhead.
- A comparative assessment of blockchain-based detection against traditional and state-of-the-art approaches in terms of scalability, efficiency, and feasibility in real-world UAV networks.

To achieve these objectives, the study undertakes the following methodology:

- Analyze current challenges in UAV cybersecurity and evaluate the implications of GNSS spoofing attacks.
- Design a decentralized detection architecture utilizing blockchain technology.
- Implement and simulate coordinated multi-UAV validation scenarios within a high-fidelity virtual environment.
- Quantitatively evaluate the proposed system's performance, trade-offs, and scalability under varying workloads.

Based on the outlined research objectives and guiding questions, the following section presents the methodology adopted to design, implement, and evaluate the proposed blockchain-based GNSS spoofing detection framework for UAV networks.

2. Methodology

To investigate the feasibility and performance of blockchain-based GNSS spoofing detection in UAV networks, a simulation-based experimental architecture was developed. This architecture integrates distributed consensus via Ethereum smart contracts, UAV behavioral modeling, and realistic GNSS coordinate generation through high-fidelity flight simulations using AirSim. The methodology encompasses system architecture design, consensus algorithm development, spoofing scenario simulation, and quantitative performance evaluation.

2.1. System architecture

The proposed system establishes a decentralized verification framework for UAV positional data using a permissionless blockchain network. Each UAV periodically submits its GNSS coordinates to a smart contract deployed on an Ethereum-compatible testnet, where a validation algorithm assesses the spatial-temporal consistency of the data. The architecture is designed to support real-time operation, trustless consensus, and scalability for swarms of autonomous UAVs operating in adversarial environments.

The high-level layered structure is inspired by Han et al. (2019), which delineates a three-tier model comprising a user

layer, data sharing layer, and cloud-based data storage. In contrast, proposed system replaces centralized cloud components with on-chain storage and smart contract-driven validation. It introduces a GNSS spoofing simulation environment, validator UAVs, and a blockchain consensus layer tailored to detect and classify spoofed GNSS data in real time.

The system comprises four main subsystems:

- GNSS Data Simulation Layer: UAV behavior and spoofing events are emulated in Microsoft AirSim, with randomized offsets used to inject false GNSS data along predefined trajectories.
- Blockchain Interface Layer: GNSS data is transmitted asynchronously via Web3.py to a smart contract on a local Ethereum blockchain (Ganache), with cryptographic signing to ensure data integrity.
- Validation and Consensus Layer: A Solidity smart contract calculates motion vectors and applies speed-based plausibility checks. Validator UAVs cast votes, and majority consensus determines spoofing classification.
- Blockchain Logging Layer: All validation outcomes are immutably stored on-chain for auditability and post-simulation analysis.

Figure 1 presents the layered architectural breakdown of the system, outlining how GNSS spoofing simulation, consensus validation, and blockchain logging components are organized across four interoperable layers.

Ethereum was selected as the blockchain framework due to its active open-source ecosystem, compatibility with Solidity-based smart contracts, and extensive tooling for prototyping decentralized applications. The use of Ganache enables rapid local deployment and testing without mining overhead. AirSim was chosen for its physics-accurate UAV flight modeling, and native support for multi-agent simulation. Web3.py provides a modular and well-documented interface for interacting with Ethereum from Python, ensuring seamless integration of the control logic with the blockchain backend.

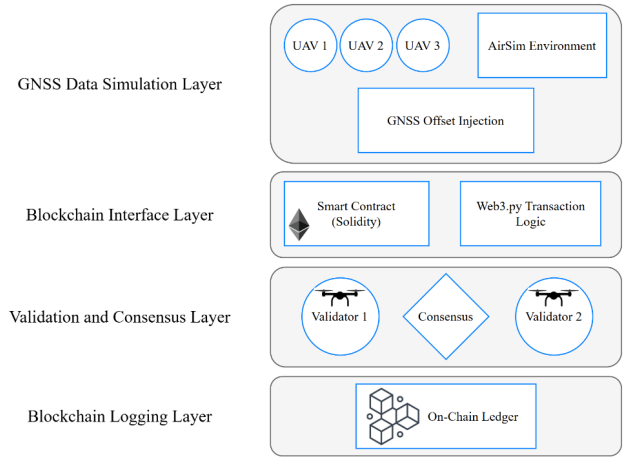

Figure 1. Layered system architecture illustrating GNSS spoofing simulation, blockchain interaction, consensus logic, and logging mechanisms. Architecture adapted from Han et al. (2019)

Figure 2 illustrates the complete end-to-end data flow across both simulation and blockchain environments. The process begins with simulated GNSS signal broadcasting from virtual satellites to all UAVs. UAV 1, randomly designated as the spoofed agent, transmits falsified GNSS data to the blockchain. Validator UAVs (e.g., UAV 2 and UAV 3) independently retrieve and assess this data. Their votes are cast

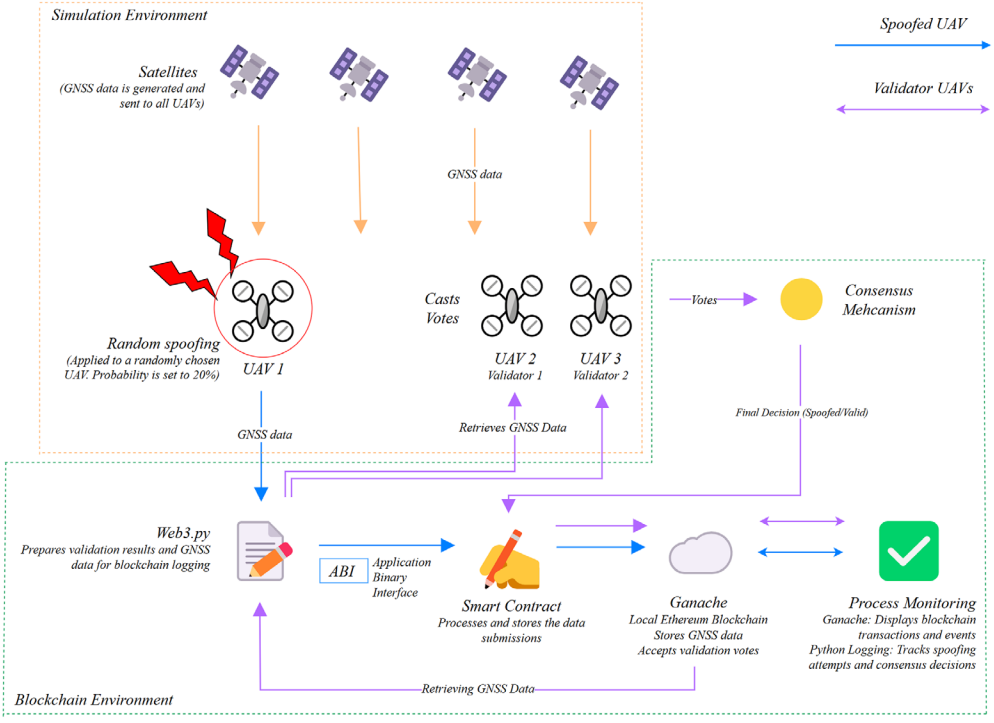

Figure 2. Overall system data flow architecture integrating UAV simulation, spoofing logic, smart contract processing, and decentralized consensus

via the blockchain interface and aggregated on-chain by the smart contract. Final results – whether valid or spoofed – are logged immutably on the local Ethereum ledger.

This architecture offers several key advantages. First, it eliminates the single point of failure characteristic of centralized validation systems, which are often targeted in spoofing and denial-of-service attacks. Second, it enables horizontal scalability: additional UAVs can act as validators without compromising the integrity or latency of the verification process. Finally, the modular design facilitates rapid iteration and testing of alternative spoofing scenarios, consensus rules, or blockchain configurations.

To maximize realism and flexibility, the system permits dynamic reconfiguration of parameters such as spoofing probability, validator count, communication delays, and flight trajectories. These features collectively support rigorous evaluation of detection performance across a range of operational conditions and threat models.

2.2. Smart contract and consensus design

At the core of the spoofing detection framework lies a custom-built smart contract developed in Solidity and deployed on a local Ethereum blockchain via Ganache. The contract serves as a trustless validator for GNSS data submitted by UAVs, ensuring that all positional information is stored and verified on-chain in a transparent and tamper-resistant manner.

Each UAV is assigned a unique identifier and maintains a history of its most recent GNSS coordinates and associated timestamps within the smart contract. Upon receiving a new data point, the contract calculates the displacement between the current and previous positions based on the Euclidean distance in a two-dimensional space:

$$d = \sqrt{\left(\Delta lat\right)^2 + \left(\Delta lon\right)^2}, \quad (1)$$

where Δlat and Δlon represent the changes in latitude and longitude, respectively. These are computed as:

$$\Delta lat = lat_2 - lat_1; \quad (2)$$

$$\Delta lon = lon_2 - lon_1. \quad (3)$$

The time difference between submissions is calculated using the block timestamps recorded on-chain:

$$\Delta t = t_{current} - t_{last}. \quad (4)$$

A simplified kinematic model is used intentionally, as the primary objective of this study is not to develop complex spoofing detection algorithms, but to evaluate the feasibility, performance, and scalability of a blockchain-based validation and consensus mechanism under realistic UAV network conditions.

The smart contract compares the computed distance against a predefined maximum plausible displacement based on the UAV's speed threshold. If the distance exceeds this threshold, the data is provisionally classified as spoofed:

$$d \geq maxDistancePerSecond \times \Delta t, \quad (5)$$

where Δt represents the elapsed time between the current and previous GNSS submissions.

Validator UAVs operate asynchronously and autonomously. Each validator retrieves the GNSS submission from the blockchain and independently assesses its plausibility using internal logic (e.g., expected formation geometry, relative position, or kinematic feasibility). A vote is cast – either valid or invalid – and submitted to the smart contract via Web3.py. The contract aggregates all validator votes and applies a majority rule: if more than 50% of the votes classify the data as invalid, the entry is flagged as spoofed and permanently recorded.

This mechanism ensures that:

- No single UAV can dominate or manipulate the validation process.
- The network can collectively determine whether the positional data should be accepted or rejected.
- Decisions are based on swarm intelligence, improving robustness against isolated node failures or compromises.
- The validation logic is verifiable, auditable, and immutable due to on-chain execution.

Figure 3 presents the logical flow of the spoofing detection protocol. From GNSS data generation and logging to validator votes and final classification, each step is modular and blockchain-integrated, allowing for traceable validation decisions without central coordination.

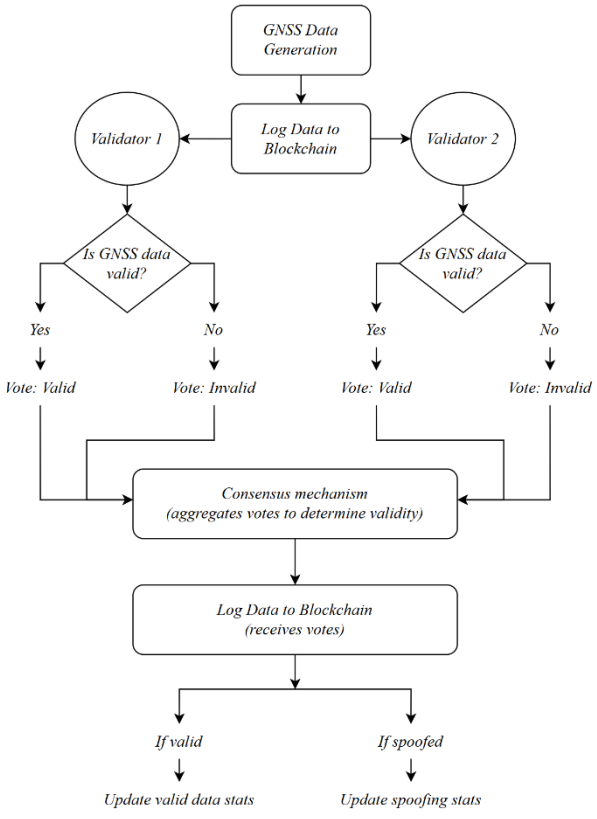

Figure 3. Logical flow diagram of the validator system: data submission, vote aggregation, and final spoofing classification

This consensus mechanism mirrors key design principles of fault-tolerant distributed systems. It is lightweight in computation, enabling deployment even in constrained UAV platforms, and generalizable to a variety of decision-making contexts beyond GNSS spoofing – including swarm formation control, intrusion detection, and mission-critical data validation.

In the present implementation, consensus is achieved through a simple majority vote; however, the modularity of the system permits the integration of more complex schemes such as weighted trust scoring, federated learning, or Byzantine fault-tolerant voting in future extensions.

While the current implementation utilizes a basic Euclidean distance–based plausibility check, future work should explore more sophisticated models incorporating UAV dynamics, IMU-based fusion, or learning-based classifiers. This would enhance resilience against adversarial spoofing patterns in complex flight scenarios.

2.3. Simulation framework and scenario design

The simulation architecture integrates an Unreal Engine–based environment via Microsoft's AirSim platform with Python-based flight logic, spoofing attack injection mechanisms, and a local Ethereum blockchain. This design enables rigorous testing of the spoofing detection consensus algorithm under spatially and temporally variable conditions while ensuring full data immutability and verifiability.

The simulation environment was constructed using AirSim, an open-source robotics simulator that provides photo-realistic 3D worlds and physically accurate multirotor dynamics. Each UAV instantiated in the environment was represented as an independent agent controlled via the MultirotorClient API. UAVs were initialized at distinct coordinates and programmed to follow a closed-loop square trajectory at a fixed altitude of 15 meters.

Each UAV agent executed its flight behavior asynchronously, simulating distributed operation. The number of agents in each simulation run was configurable, with typical scenarios involving 3 to 5 UAVs. All UAVs continuously monitored their own state and submitted positional data – including latitude, longitude, altitude, and spoofing flags – to the blockchain at predefined intervals.

Spoofing attacks were modeled probabilistically using a Bernoulli distribution. At each movement iteration, a UAV had a 20% probability of becoming spoofed. Upon spoofing activation, a random offset was applied to both the latitude and longitude coordinates, with displacements drawn uniformly from the range of [−0.05, +0.05] meters. These offsets were retained until the UAV reached the next waypoint, mimicking transient GNSS manipulation events observed in real-world spoofing incidents.

This form of attack modeling enabled the system to emulate a diverse range of anomalies, including abrupt location jumps, nonphysical acceleration patterns, and invalid trajectory geometries. The ground-truth positions and spoofed positions were logged separately to facilitate comparative evaluation.

Three primary mission scenarios were designed to stress-test the spoofing detection mechanism under different spatial constraints:

- Uniform Linear Flight: UAVs traverse a fixed axis, periodically subjected to spoofing to simulate corridor surveillance missions with minimal maneuvering.

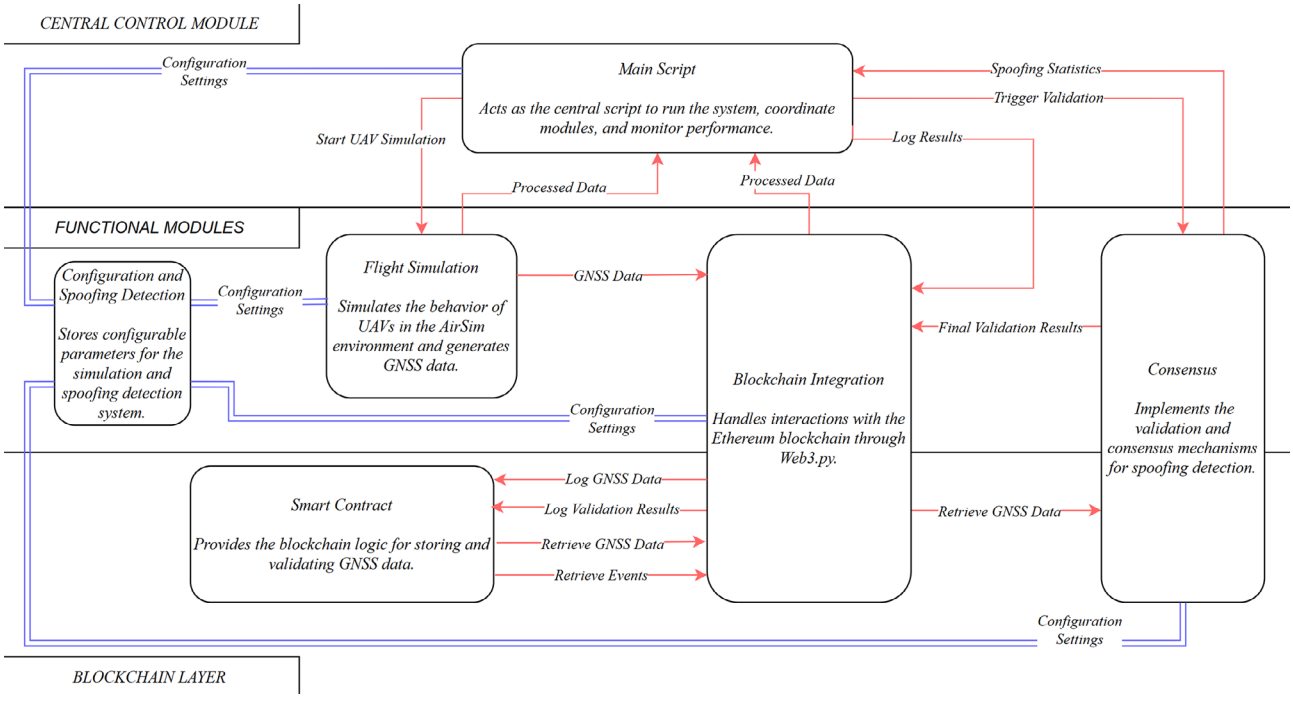

Figure 4. High-level modular software architecture showing interaction between UAV simulation, blockchain interaction, spoofing detection, and validation modules

- Closed-Loop Path Execution: Each UAV executes a square pattern, introducing frequent directional changes that test dynamic position verification.
- Formation Flight with Re-Tasking: UAVs maintain fixed spacing in coordinated formations, with dynamic waypoint reallocation mimicking wind-induced drift or emergency re-routing.

All behavioral and environmental parameters – including spoofing probability, UAV velocity, waypoint density, and GNSS noise margins – were externally configurable via structured JSON files. This design enabled experimental reproducibility and scalability across varying mission conditions.

Due to the asynchronous nature of UAV operations, blockchain interactions, and consensus evaluations, system-wide coordination was achieved through an event-driven simulation controller. This controller managed UAV telemetry polling, spoofing activation, and the submission of GNSS data to the blockchain. A dedicated blockchain interface layer encoded and optimized each transaction for on-chain logging, ensuring minimal gas consumption.

The consensus mechanism was executed at regular intervals to validate submitted location data and detect spoofing behavior. The modularity of the system architecture supports seamless integration of alternative consensus strategies, including trust-weighted voting, federated learning-based classifiers, or Byzantine fault-tolerant algorithms, without requiring changes to the underlying simulation workflow.

As illustrated in Figure 4, the architecture consists of three interconnected layers: a central control module, functional components for flight, spoofing, and validation, and the underlying blockchain layer. Configuration settings and results propagate through clearly defined interfaces, supporting dynamic experimentation and flexible extension of the framework.

This simulation framework balances computational tractability with physical fidelity. It allows for rapid experimentation while preserving physical realism, enabling robust evaluation of the system's resilience to spoofing under a range of operational and adversarial scenarios.

2.4. Performance evaluation metrics

The performance of the proposed blockchain-based GNSS spoofing detection framework was evaluated through a series of controlled simulations. For reproducibility, the evaluation was carried out under two main scenarios: 3 UAVs and 5 UAVs, each executing a predefined number of simulation iterations. The framework monitored and recorded a comprehensive set of performance metrics, including spoofing detection rate, false negative rate, transaction latency, smart contract execution time, gas consumption, blockchain throughput (transactions per second), on-chain storage utilization, and energy consumption per UAV session.

Real-time statistics were collected using a multi-threaded Python script that emulates UAV telemetry submissions, introduces randomized spoofing attacks, and logs detection outcomes. Blockchain performance data such as gas usage, latency, and storage footprint were extracted via Web3 calls to the deployed smart contract. Energy metrics were derived by estimating the energy consumed per transaction in an Ethereum Proof-of-Stake model, using a baseline of 0.03 kWh per transaction. All metrics were visualized post-simulation using the matplotlib library to analyze scalability, responsiveness, and fault tolerance.

Table 1 summarizes the simulation configuration parameters and control conditions used in the performance evaluation. It includes both static inputs (e.g., UAV start positions, spoofing probability) and dynamic system-level configurations (e.g., consensus protocol, blockchain platform) necessary for reproducing the experimental environment.

The configuration in Table 1 defines the experimental foundation for evaluating the system's performance. The UAVs were deployed in diverse initial positions and subjected to randomized GNSS spoofing events with controlled probability and offset magnitudes. The use of a majority-vote consensus mechanism ensured distributed decision-making in detecting spoofed data. All data submissions, validations, and blockchain interactions were executed and recorded under consistent simulation parameters, enabling reliable measurement of key performance

Table 1. Simulation setup parameters and configurations

Parameter	Description	Value / Range
UAV initial coordinates	Starting positions of UAVs in the AirSim environment	(0,0,–15), (10,0,0), (–10,0,0), (20,0,0), (–20,0,0)
UAV identifiers	Unique labels assigned to UAV agents	Drone1, Drone2, ..., DroneN
Simulation time	Number of iterations and update interval	60 iterations, updates every 1–5 seconds
Maximum speed	UAV waypoint velocity constraint (imposed by AirSim)	5 m/s (AirSim default)
Random spoofing probability	Probability of spoofed GNSS injection per UAV per iteration	20%
Spoofing offset range	Latitude and longitude offsets applied to spoofed data	Latitude: [–0.05, 0.05], Longitude: [–0.05, 0.05]
Blockchain platform	Ethereum test blockchain for logging UAV data	Ganache
Smart contract interface	Method used to log UAV location and spoofing status	Python Web3.py and Solidity contract
Consensus mechanism	Spoofing detection logic based on validator agreement	Majority vote among validator UAVs
Data logging frequency	Rate of GNSS data submission to blockchain	One submission per UAV per iteration
Timestamp generation	Method of recording submission times on-chain	UNIX epoch time

indicators. This controlled setup allowed for repeatable comparisons across different UAV network sizes in the subsequent analysis.

The chosen configuration balances simulation realism and computational feasibility, enabling extensive testing while maintaining fidelity to real-world UAV swarm behaviors and spoofing threat models. Parameter values – such as spoofing offset range and GNSS logging frequency – were selected to emulate short-duration, low-amplitude GNSS anomalies commonly observed in practical adversarial scenarios, ensuring the relevance of the evaluation to real-world UAV deployments.

3. Results

The evaluation focuses on assessing the performance of the proposed blockchain-based GPS spoofing detection framework for UAV networks. Key performance metrics include spoofing detection rate, false negative rate, blockchain transaction latency, throughput, smart contract execution time, gas usage, energy consumption, and on-chain storage utilization. Results are presented using comparative tables to highlight patterns, performance trade-offs, and system behavior across different UAV network sizes and operational scenarios.

3.1. Spoofing detection performance

The system demonstrated high spoofing detection capability in both scenarios. Table 2 presents the detection outcomes, including True Positive Rate (TPR), False Negative Rate (FNR), and overall transaction success.

The spoofing detection system demonstrated consistently high detection performance across both simulation scenarios. With a True Positive Rate (TPR) of 97.22% in the 3-UAV case and 93.94% in the 5-UAV case, the consensus-based mechanism effectively identified spoofed GNSS data in real time. The False Negative Rate (FNR) remained low overall, increasing slightly from 2.78% to 6.06% as the swarm size grew.

The decrease in accuracy with 5 UAVs is primarily attributed to the higher volume of GNSS updates and concurrent validation activity, which increases consensus latency and may lead to timing mismatches in spoofing detection. With more UAVs casting votes asynchronously, brief delays in receiving validator data or in achieving consensus can lead to occasional misclassifications, especially when spoofing occurs in rapid succession. This limitation can be mitigated by optimizing block confirmation time, prioritizing spoofing-related transactions, or implementing lightweight pre-validation at the UAV level to filter out obvious anomalies before on-chain voting.

Despite this, the system sustained 100% transaction reliability, with no failed submissions or blockchain inconsistencies recorded across all test cases. These results highlight the scalability and resilience of the decentralized architecture. The ability to maintain high detection rates – even under increased throughput – demonstrates the robustness of the majority-vote consensus strategy. This design ensures that even when individual UAVs face spoofed input, the swarm can collectively verify legitimacy without relying on centralized infrastructure.

Overall, this evaluation confirms the practical viability of blockchain-based consensus mechanisms for spoofing detection in UAV networks. The architecture shows strong potential for real-world applications such as formation flight coordination, border patrols, and autonomous search-and-rescue, where real-time, decentralized geolocation integrity is mission-critical.

3.2. Blockchain performance metrics

Blockchain-level performance is summarized in Table 3, comparing latency, throughput, gas usage, energy efficiency, and on-chain storage across scenarios.

As the number of UAVs increased from 3 to 5, the system exhibited predictable and controlled scaling behavior across all blockchain-related performance metrics. The number of logged entries, total gas consumption, and on-chain storage usage increased linearly (+66.7%), in proportion to the number of UAVs and their data submission frequency. This reflects the scalability of the underlying smart contract design and the modular architecture of the blockchain integration layer.

The most pronounced scaling effect was observed in the average transaction latency, which more than doubled from 1.85 seconds to 3.95 seconds (+113.5%). This increase is attributed to the cumulative overhead of validating and processing a higher volume of transactions in a synchronous consensus system. Although the throughput experienced a modest decline (−13.2%), it remained above 1 transaction per second, which is generally acceptable for decentralized UAV telemetry systems that do not require millisecond-scale responsiveness.

Table 2. Spoofing detection evaluation

Metrics	3 UAVs	5 UAVs	Percentage
Total location updates	180 (60 per UAV)	300 (60 per UAV)	100%
Normal movements	144	267	80–89%
Spoofing attempts	36	33	11–20%
True Positive Rate (TPR)	97.22 % (35 detections, 1 missed)	93.94% (31 detections, 2 missed)	High accuracy
False Negative Rate (FNR)	2.77%	6.06%	Minimal error

Table 3. Blockchain performance results summary

Metric	3 UAVs	5 UAVs	Comparison
Logged entries	180	300	+66.7%
Simulation duration	149.33 sec	285.79 sec	+91.4%
Successful transactions	180	300	+66.7%
Failed transactions	0	0	No change
Average transaction latency	1.85 sec	3.95 sec	+113.5%
Throughput	1.21 tx/sec	1.05 tx/sec	−13.2%
Total gas used	20,761,860	34,617,818	+66.7%
Energy per transaction	0.03 kWh	0.03 kWh	No change
Total energy consumption	5.40 kWh	9.00 kWh	+66.7%
Energy per UAV session	1.80 kWh	1.80 kWh	No change
Total on-chain storage used	28.16 KB	46.91 KB	+66.7%

Energy consumption per transaction remained constant at 0.03 kWh, consistent with the assumed PoS baseline. However, total energy consumption scaled proportionally with the number of UAVs, as expected. Storage growth followed a similar trend, reinforcing the idea that system resource demands can be anticipated and managed based on UAV network size.

Importantly, no failed transactions were recorded in either scenario, confirming the system's stability under increased workload. The smart contract maintained reliable operation without breakdowns, queuing failures, or execution bottlenecks. These results collectively demonstrate that the proposed framework is operationally robust and exhibits predictable scaling behavior.

However, the observed latency increase highlights a limitation of synchronous public-blockchain models when applied to real-time UAV swarm applications. These findings underscore the need to explore optimization strategies such as asynchronous consensus mechanisms, off-chain transaction batching, or migration to lower-latency platforms (e.g., DAG-based ledgers or private blockchain networks) for future large-scale deployments.

3.3. Comparative analysis with other spoofing detection approaches

To contextualize the performance of the proposed blockchain-based spoofing detection framework, a comparative analysis was conducted against state-of-the-art GNSS spoofing detection techniques reported in the literature. Table 4 summarizes key characteristics of each method, including detection accuracy, scalability, energy consumption, and implementation requirements. The table is adapted from the work of Mykytyn et al. (2023), with modifications based on the present study's performance metrics and architectural assumptions.

When compared to state-of-the-art GNSS spoofing detection techniques, the blockchain-based framework demonstrates a compelling trade-off between detection accuracy, system decentralization, and data integrity. Achieving a detection rate of 97.22%, it outperforms traditional IMU-based machine learning systems while offering greater transparency and resistance to tampering through its tamper-proof logging and consensus mechanism.

Unlike methods relying on hardware-intensive approaches – such as antenna arrays and multi-receiver systems, which deliver higher accuracy but lack scalability and

Table 4. Comparative analysis of blockchain-based and alternative GPS spoofing detection mechanisms (source: Authors elaboration based on Mykytyn et al., 2023)

Mechanism	Approach	Detection Rate	Scalability	Energy Use	Limitations and Drawbacks
Cellular network based	Position validity cross-check	95%	Moderate	Moderate	Requires a cellular module and network coverage
Gyroscope + Accelerometer	Position estimation	96%	Moderate	Moderate	Requires accurate motion sensors for spoofing detection
IMU-based	Machine Learning	96.30%	High	Moderate	Computational overhead; limited by training data
Blockchain-based	Tamper-proof logging + voting	97.22%	Moderate (blockchain scalability)	High	Blockchain, smart contracts, stable connectivity
Multi-receiver	Multiple devices for position checking	99%	Low (hardware bound)	Low	Requires additional hardware; not suitable for small UAVs
Antenna Array	Direction-of-arrival of GNSS signals	99%	Low (not scalable)	Moderate	Complex antennas, limited to larger UAVs

are unsuitable for lightweight UAVs – the blockchain-based solution requires no additional physical components. This renders it more adaptable to diverse mission environments, especially those involving resource-constrained platforms.

While its moderate scalability and high energy consumption, inherent to blockchain consensus and transaction validation, pose limitations for real-time or large-scale deployments, the framework's security, auditability, and autonomy make it particularly well-suited for UAV networks operating in adversarial or GNSS-contested environments.

The results suggest that blockchain-based spoofing detection is best positioned for use cases where data authenticity, traceability, and distributed decision-making outweigh low-latency constraints. As such, it establishes a strong foundation for future integration of secure, decentralized communication protocols in autonomous aerial systems.

4. Conclusions

This study introduces a modular, blockchain-enabled architecture for GNSS spoofing detection in UAV swarms, combining high-fidelity AirSim simulations with decentralized consensus mechanisms deployed via Ethereum smart contracts. The proposed framework facilitates autonomous geolocation validation, spoofing anomaly detection, and tamper-resistant data logging in adversarial and untrusted environments.

Experimental results demonstrate the robustness and feasibility of the approach, achieving a spoofing detection accuracy of 97.22% in the 3-UAV scenario and 93.94% in the 5-UAV configuration. The system maintained 100% transaction reliability and exhibited low false negative rates (2.77% and 6.06%, respectively). Its software-defined architecture supports reconfigurable simulation parameters and seamless UAV integration without requiring changes to the underlying blockchain logic, underscoring its adaptability to diverse mission profiles.

It is important to acknowledge that the current evaluation was conducted entirely within a simulated environment, utilizing AirSim for UAV dynamics and Ganache for local blockchain deployment. While this setup provides valuable insights into system behavior under controlled conditions, future validation on physical UAV platforms is essential to address practical implementation challenges, such as environmental uncertainty, communication latency, sensor noise, and computational resource limitations.

Despite the system's functional scalability, performance trade-offs were identified. Notably, average transaction latency increased from 1.85 to 3.95 seconds (+113.5%), cumulative gas consumption rose by 66.7%, and total energy consumption also increased by 66.7% as the UAV count increased from three to five. These limitations highlight the importance of efficiency-oriented design when deploying blockchain systems in resource-constrained UAV environments.

To enhance real-time responsiveness and scalability, future research should explore lightweight consensus protocols, off-chain transaction batching, and hybrid architectures that combine public and private ledger frameworks. Furthermore, the adoption of alternative distributed ledger technologies – such as DAG-based platforms, IOTA, or Hyperledger Fabric – may reduce transaction latency and computational overhead, making the architecture more suitable for time-critical aerial operations.

The proposed framework is particularly suited for mission-critical UAV operations where secure, real-time geolocation verification is paramount – such as cross-border surveillance, autonomous delivery in GNSS-contested regions, infrastructure monitoring, and emergency response missions. Its decentralized architecture eliminates single points of failure, while the tamper-proof blockchain ledger supports auditability and accountability – key features in safety-critical deployments. By aligning high-fidelity UAV simulation with blockchain-based consensus, this work offers a scalable and trustless foundation for deploying resilient UAV swarms in real-world scenarios where cybersecurity and autonomy are mission enablers.

To the best of gained knowledge, this is among the first implementations to integrate blockchain consensus, smart contracts, and high-fidelity UAV simulation for real-time GNSS spoofing detection – representing a significant advancement in resilient and decentralized aerial cybersecurity systems.

Disclosure statement

The Authors have no conflicts of interest to declare that are relevant to the content of this article. The Authors did not receive support from any organization for the submitted work.

References

Alladi, T., Chamola, V., Sahu, N., & Guizani, M. (2020). Applications of blockchain in unmanned aerial vehicles: A review. *Vehicular communications, 23*, Article 100249. https://doi.org/10.1016/j.vehcom.2020.100249

Almotery, O. (2020). Blockchain as solution to drone cybersecurity. In *IEEE World Forum on Internet of Things: 2020 Symposium Proceedings*. IEEE.

Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2018). Blockchain with Internet of Things: Benefits, challenges, and future directions. *International Journal of Intelligent Systems and Applications*, *10*(6), 40–48. https://doi.org/10.5815/ijisa.2018.06.05

Ferrag, M. A., & Maglaras, L. (2019). Deliverycoin: An IDS and blockchain-based delivery framework for drone-delivered services. *Computers*, *8*(3), Article 58. https://doi.org/10.3390/computers8030058

Ghribi, E., Khoei, T. T., Gorji, H. T., Ranganathan, P., & Kaabouch, N. (2020, July). A secure blockchain-based communication approach for UAV networks. In *IEEE International Conference on Electro Information Technology* (pp. 411–415). IEEE. https://doi.org/10.1109/EIT48999.2020.9208314

Gugueoth, V., Safavat, S., Shetty, S., & Rawat, D. (2023). A review of IoT security and privacy using decentralized blockchain

techniques. *Computer Science Review*, *50*, Article 100585. https://doi.org/10.1016/j.cosrev.2023.100585

Gupta, R., Nair, A., Tanwar, S., & Kumar, N. (2021). Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges. *IET Communications*, *15*(10), 1352–1367. https://doi.org/10.1049/cmu2.12113

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

Han, R., Bai, L., Liu, J., & Chen, P. (2019). Blockchain-based GNSS spoofing detection for multiple UAV systems. *Journal of Communications and Information Networks*, *4*(2), 81–88. https://doi.org/10.23919/JCIN.2019.8917874

Jensen, I., Selvaraj, D., & Ranganathan, P. (2019, 10–12 June). Blockchain technology for networked swarms of unmanned aerial vehicle (UAVs). In *20th IEEE International Symposium on a World of Wireless*, *Mobile and Multimedia Networks* (*IEEE WoWMoM 2019*) (pp. 456–462), Washington DC, United States. IEEE. https://doi.org/10.1109/WoWMoM.2019.8793027

Kumar, R., Aljuhani, A., Kumar, P., Kumar, A., Franklin, A., & Jolfaei, A. (2022). Blockchain-enabled secure communication for unmanned aerial vehicle (UAV) networks. In *DroneCom 2022 – Proceedings of the 5th International ACM Mobicom Workshop on Drone Assisted Wireless Communications for 5G and Beyond* (pp. 37–42). ACM Digital Library. https://doi.org/10.1145/3555661.3560861

Mykytyn, P., Brzozowski, M., Dyka, Z., & Langendoerfer, P. (2023). *GPS-spoofing attack detection mechanism for UAV swarms*. IEEE. https://doi.org/10.1109/MECO58584.2023.10154998

Riahi Manesh, M., & Kaabouch, N. (2019). Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. *Computers and Security*, *85*, 386–401. https://doi.org/10.1016/j.cose.2019.05.003

Sharma, J., & Mehra, P. S. (2023). Secure communication in IOT-based UAV networks: A systematic survey. *Internet of Things 23*, Article 100883. https://doi.org/10.1016/j.iot.2023.100883

Sihag, V., Choudhary, G., Choudhary, P., & Dragoni, N. (2023). Cyber4Drone: A systematic review of cyber security and forensics in next-generation drones. *Drones*, *7*(7), Article 430. https://doi.org/10.3390/drones7070430

Yaacoub, J. P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things*, *11*, Article 100218. https://doi.org/10.1016/j.iot.2020.100218

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Proceedings of 2017 IEEE 6th International Congress on Big Data* (*BigData Congress*) (pp. 557–564). IEEE. https://doi.org/10.1109/BigDataCongress.2017.85

Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to scalability of blockchain: A survey. *IEEE Access*, *8*, 16440–16455. https://doi.org/10.1109/ACCESS.2020.2967218