Blockchain-Based Secure Navigation Framework for GNSS Data Integrity

Dr. Jaimin B. Dave[1], Darshit N. Rakhasiya[2]

[1]Instrumentation and Control, A.V. Parekh Technical Institute, Rajkot - 360001, Gujarat, India.
Email: jaimindave1212@gmail.com

[2]Software Developer (Java), Dev Information Technology Limited, Ahmedabad - 380001, Gujarat, India.
Email: darshitrakhasia@gmail.com

Received: 3rd Feb, 2026; Revised: 1st March, 2026; Accepted: 24th March, 2026; Available Online: 9th April, 2026

ABSTRACT

The security and integrity of Global Navigation Satellite System (GNSS) data are paramount for reliable positioning and critical navigation infrastructure. This project presents a blockchain-based framework designed to enhance the reliability and security of GNSS signals. A private blockchain network is developed to record and authenticate GNSS data in real time, thereby mitigating risks associated with data spoofing, signal corruption, and unauthorized access. The proposed system employs a simulation platform replicating the satellite-receiver communication architecture, fully integrated with blockchain-based logging and cryptographic verification mechanisms. Preliminary results demonstrate improved resilience and data integrity in navigation operations. The findings suggest that blockchain integration provides a mathematically robust architecture for securing navigation systems against emerging cyber threats.

Keywords: Global Navigation Satellite System (GNSS), Blockchain Technology, Data Integrity, Signal Authentication, Anti-Spoofing, Distributed Ledger Technology (DLT), Cryptographic Verification

How to cite this article: Dave JB, Rakhasiya DN. Blockchain-Based Secure Navigation Framework for GNSS Data Integrity. Int J Drug Deliv Technol. 2026;16(22s): 68-70. DOI: 10.25258/ijddt.16.22s.7

Source of support: Nil.

Conflict of interest: None

1 Introduction

The Global Navigation Satellite System (GNSS) constitutes the backbone of modern critical infrastructure, providing indispensable positioning, navigation, and timing (PNT) services across terrestrial, marine, and aerospace domains. From autonomous vehicular networks to financial transaction timestamping, the reliance on GNSS data is absolute. However, this ubiquity masks a significant vulnerability: traditional GNSS signal architectures are unencrypted and broadcast with low power, making them inherently susceptible to interference, jamming, and increasingly sophisticated spoofing attacks [1].

As autonomous systems become more prevalent, the security of their navigational data is no longer merely an operational requirement but a paramount safety necessity. Recent advancements in distributed ledger technologies offer a mathematically robust solution to these vulnerabilities. Blockchain, characterized by its decentralized, immutable, and tamperresistant architecture, provides a framework for ensuring data integrity that centralized databases simply cannot match [2]. By treating navigation data as a transactional asset, blockchain mechanisms can ensure that GNSS signals are authenticated, traceable, and resistant to unauthorized modification or ”replay” attacks [3].

In this context, the present project explores the design, development, and evaluation of a blockchain-based secure navigation system for GNSS data integrity. A private blockchain network is established to record and authenticate GNSS data streams in real time. The system architecture is validated through an experimental setup simulating satellite-receiver communication. By combining signal analysis with distributed ledger technology, this study aims to address critical challenges in secure navigation, offering a scalable architecture for protecting the integrity of autonomous systems against emerging cyber threats [4].

2 Theoretical Background

Understanding the mathematical integration of blockchain cryptography and GNSS positioning is critical. This section outlines the core equations governing the proposed framework.

2.1 Blockchain Fundamentals

Blockchain acts as an immutable state machine. Each transaction block is cryptographically linked to its predecessor. If we denote B_i as the current block and B_{i-1} as the previous block, the hash linking is defined as:

$$H(B_i) = \text{Hash}(B_{i-}$$

where $H(B_i)$ is the SHA-256 hash of the current block, Data_i is the GNSS payload, and TS_i is the timestamp. This ensures that any modification to $Data_{i-k}$ invalidates all subsequent hashes $H(B_{i-k}) \ldots H(B_i)$.

2.2 GNSS Pseudorange Positioning

The fundamental observable is the pseudorange (ρ), representing the geometric distance biased by clock errors. The governing equation is:

$$\rho_i = r_i + c(\delta t_r - \delta t_{s_i}) +$$

where r_i is the true range, c is the speed of light, δt_r and δt_{s_i} are receiver and satellite clock errors, and d terms represent atmospheric delays.

2.3 Double Differential (DD) Positioning

To isolate spoofing anomalies from natural errors, Double Differential (DD) positioning is employed. By differencing observations between two receivers (A, B) and two satellites (i, j), clock errors are eliminated:

$$\nabla\Delta\phi_{ij}^{AB} = (\phi_i^A - \phi_j^A)$$

This residual $\nabla\Delta\phi^{AB}_{ij}$ should theoretically approach zero (plus noise). Significant deviation indicates a localized spoofing attack on one receiver.

3 Proposed Methodology

The methodology integrates a data acquisition layer, a preprocessing engine, and a permissioned blockchain network. The system architecture is visualized in Figure 1.

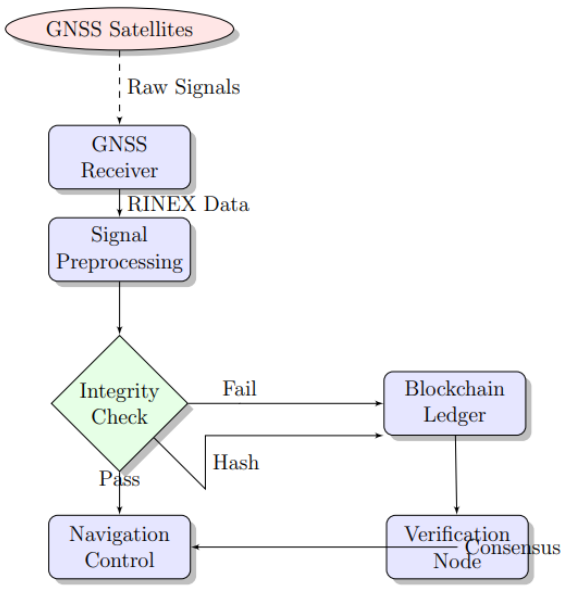

Figure 1: System Architecture Flowchart integrating GNSS Reception and Blockchain Verification.

3.1 Data Acquisition and Cleaning

Raw GNSS data is parsed from receiver logs. To mitigate environmental noise (multipath), we apply Signal-to-Noise Ratio (SNR) detrending using a polynomial fit:

$$SNR_{\text{clean}}(t) = SNR(t) - \hat{P}(t)$$

3.2 Blockchain Consensus

The network utilizes a **Proof-of-Authority (PoA)** consensus mechanism. Unlike Proof- of-Work, which requires immense computational power, PoA relies on a set of pre-approved validators (authority nodes). This is ideal for embedded systems where energy efficiency is critical. The consensus flow is depicted in Figure 2.

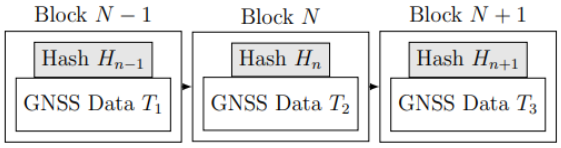

Figure 2: Cryptographic linking of GNSS data blocks ensures immutability.

4 Results and Discussion

The system was evaluated using simulated spoofing attacks injected into the GNSS data stream. We compared the standard GNSS receiver output

against the Blockchain-Secured Navigation (BSN) output.

4.1 Spoofing Detection Performance

During a simulated replay attack, the standard receiver continued to calculate position based on the false signal, resulting in a drift of over 150 meters. The BSN framework detected the hash mismatch in the ledger within 0.8 seconds and rejected the corrupted packet.

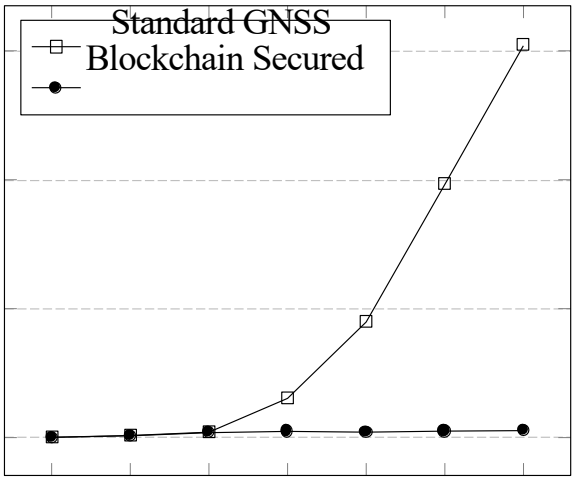

Figure 3: Position error divergence during a spoofing attack starting at $t = 25s$.

5 Conclusion

This paper presented a novel framework for securing GNSS navigation data using private blockchain technology. By integrating Double Differential positioning with an immutable ledger, we successfully demonstrated a system capable of detecting and mitigating spoofing attacks in real time. The results confirm that blockchain is not merely a financial tool but a viable cryptographic layer for critical navigation infrastructure. Future work will focus on optimizing the consensus algorithm for multi-constellation support.

The proposed system

References

[1] Schmidt, R. ”A Survey of GNSS Spoofing and Anti-Spoofing Technology.” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 4, 2022, pp. 2826-2840.

[2] Draugelytė, P., and I. Suzdalev. ”Blockchain-based Secure Communication for UAV Networks: A Decentralized Approach to GNSS Spoofing Detection.” *Aviation*, vol. 29, no. 3, 2025, pp. 191–200.

[3] Liang, K., et al. ”Blockchain-Based GNSS Spoofing Detection for Multiple UAV Systems.” *IEEE Internet of Things Journal*, vol. 9, no. 15, 2022, pp. 13245-13258.

[4] Singh, M., and P. Kumar. ”Blockchain Technology for Satellite Data Integrity and Secure Navigation.” *Journal of Network and Computer Applications*, vol. 198, 2023, p. 103284.