6G-Native Architecture for Integrated Satellite-Terrestrial Networks: A Blockchain-Assisted Zero-Trust Framework for Edge Intelligence

[1] Dr. T. Manivel
[1] Assistant Professor, Information Technology, Muthayammal Engineering College (Autonomous), Namakkal, Tamil Nadu, India - 637408
manivel.t.it@gmail.com

Abstract

The sixth-generation (6G) wireless ecosystem envisions ubiquitous connectivity through the seamless integration of satellite, aerial, and terrestrial networks into a unified Space-Air-Ground Integrated Network (SAGIN). However, the heterogeneous, dynamic, and resource-constrained nature of non-terrestrial networks introduces unprecedented security challenges that traditional perimeter-based defenses cannot address. This paper proposes STIN-ZT, a 6G-native architecture that synergistically combines blockchain-assisted decentralized trust management with a zero-trust security framework to enable secure edge intelligence across integrated satellite-terrestrial networks. Our approach introduces a hierarchical multi-domain blockchain with Practical Byzantine Fault Tolerance (PBFT) consensus optimized for high-latency satellite links, coupled with a context-aware zero-trust model featuring continuous authentication, dynamic trust scoring, and micro-segmentation. The framework leverages edge intelligence nodes deployed across orbital, aerial, and terrestrial domains to perform real-time anomaly detection and policy enforcement with minimal latency. Experimental evaluation using a Mininet-based SAGIN emulator demonstrates that STIN-ZT achieves 99.2% identity spoofing mitigation, reduces authentication latency to 1.9 ms (6.6× improvement over traditional zero-trust), and maintains 95 Gbps throughput with only 12% security overhead. The proposed architecture provides a scalable, quantum-resilient security foundation for next-generation integrated non-terrestrial networks.

Keywords: *6G Networks, Satellite-Terrestrial Integration, Zero-Trust Architecture, Blockchain, Edge Intelligence, Non-Terrestrial Networks, Space-Air-Ground Integration, Security*

1. Introduction

The sixth-generation (6G) wireless paradigm represents a transformative leap beyond 5G, promising peak data rates exceeding 1 Tbps, sub-millisecond latency, and ubiquitous connectivity that extends from dense urban centers to remote maritime and aerospace environments [1]. A cornerstone of this vision is the integration of non-

terrestrial networks (NTNs)—including low Earth orbit (LEO), medium Earth orbit (MEO), and geostationary (GEO) satellites, as well as high-altitude platform stations (HAPS) and unmanned aerial vehicles (UAVs)—with terrestrial cellular infrastructure [2]. This convergence, termed Space-Air-Ground Integrated Networks (SAGIN) or Satellite-Terrestrial Integrated Networks (STIN), is essential for achieving the 6G goal of "connecting the unconnected" across the globe [3].

However, the architectural complexity of STINs introduces severe security vulnerabilities that traditional perimeter-based defense mechanisms cannot adequately address. The dynamic topology of LEO constellations, the high-latency and intermittent connectivity of satellite links, the resource constraints of orbital and aerial platforms, and the multi-operator governance across different administrative domains create an expanded attack surface [4]. Recent systematic literature reviews highlight that blockchain-enabled zero-trust architectures have emerged as promising solutions for securing 6G cloud-edge non-terrestrial networks, with hybrid approaches achieving up to 97% attack detection accuracy [5].

Zero-Trust Architecture (ZTA) operates on the principle of "never trust, always verify," enforcing continuous authentication, least-privilege access, and dynamic policy enforcement regardless of network location [6]. When combined with blockchain's decentralized immutability and transparency, ZTA can address the trust deficits inherent in multi-domain SAGINs. However, existing solutions suffer from three critical limitations: (1) high authentication latency due to centralized policy decision points that become bottlenecks across high-latency satellite links; (2) excessive computational overhead from consensus mechanisms unsuitable for resource-constrained orbital edge nodes; and (3) lack of context-aware trust scoring that adapts to the mobility patterns and link conditions unique to non-terrestrial environments [5].

1.1 Contributions

To address these challenges, this paper makes the following contributions:

(1) 6G-Native Hierarchical Architecture: We propose STIN-ZT, a three-tier architecture (space-air-ground) with edge intelligence nodes distributed across orbital,

aerial, and terrestrial domains, enabling localized security decisions that minimize cross-domain latency.

(2) Blockchain-Assisted Decentralized Trust: A multi-domain blockchain framework with PBFT consensus optimized for satellite link characteristics, featuring domain-specific sidechains for satellite and terrestrial networks to reduce consensus overhead by 68%.

(3) Context-Aware Zero-Trust Model: A dynamic trust scoring engine that incorporates link quality, mobility patterns, behavioral biometrics, and historical reputation to enable adaptive access control policies that respond to real-time network conditions.

(4) Edge-Native Policy Enforcement: Lightweight policy enforcement points (PEPs) deployed at orbital and aerial edge nodes, enabling sub-5ms authentication decisions without requiring round-trips to terrestrial policy decision points (PDPs).

(5) Comprehensive Evaluation: Extensive simulation using a Mininet-based SAGIN emulator with realistic satellite link models, demonstrating scalability across 1,000+ nodes and resilience against identity spoofing, routing attacks, jamming, and insider threats.

2. Related Work

2.1 Satellite-Terrestrial Integration for 6G

The integration of satellite and terrestrial networks has evolved from simple backhaul supplementation to deeply coupled architectures. Lin et al. proposed three minimal integrating structures for satellite-MEC networks inspired by protein structures, establishing an on-demand network orchestration framework for wide-area edge intelligence [7]. Wang et al. provided a comprehensive review of network-layer perspectives on satellite-terrestrial integrated networks, identifying IoT integration, AI enhancement, cloud/edge computing, and network security as critical interaction fields [3]. The DILIGENT framework introduced double-edge intelligence for integrated satellite-terrestrial networks, leveraging MEC and AI for systematic learning and adaptive network management [8].

2.2 Zero-Trust Architectures for 6G Security

Zero-trust principles have gained significant traction for 6G security. Chen et al. proposed a collaborative zero-trust architecture specifically designed for 6G networks, emphasizing elastic and scalable security regimes [6]. The ZTF-6G framework demonstrated 77.6% latency reduction (to 2.8 ms) and 98% threat detection accuracy through adaptive authentication and blockchain-based identity management [9]. Nie et al. introduced a zero-trust access control mechanism based on blockchain and inner-product encryption for IoT in 6G environments, achieving fine-grained access control without centralized key generation centers [10]. However, these approaches primarily focus on terrestrial deployments and do not address the unique challenges of high-latency satellite links and orbital edge computing.

2.3 Blockchain for Non-Terrestrial Networks

Blockchain technology has been extensively explored for securing space-air-ground integrated networks. Zhang et al. proposed blockchain-based secure communication for IoT in SAGIN, leveraging distributed ledger technology for transparent and tamper-resistant data management [11]. Zhao et al. surveyed blockchain-facilitated cybersecurity for ubiquitous IoT with SAGIN, highlighting the potential of smart contracts for automated policy enforcement [12]. Recent work on wireless blockchain for 6G emphasizes the need for trustworthy and decentralized architectures that can operate across heterogeneous network segments [13]. However, existing blockchain consensus mechanisms such as Proof-of-Work (PoW) are computationally prohibitive for resource-constrained satellites, necessitating lightweight alternatives.

2.4 Edge Intelligence in SAGIN

Edge intelligence has emerged as a critical enabler for mission-critical 6G services in space-air-ground environments. The URLLEI framework explored unikernel-based ultra-lightweight virtualization combined with micro-service paradigms for prompt response in resource-constrained SAGINs [14]. Edge intelligence nodes deployed at orbital and aerial platforms can perform local AI inference for anomaly detection, task offloading optimization, and content caching, reducing dependency on terrestrial cloud

resources [7]. However, securing these distributed edge nodes against compromise remains an open challenge, as compromised edge nodes could propagate malicious policies across the entire integrated network.

3. System Architecture and Threat Model

3.1 STIN-ZT Network Architecture

We consider a hierarchical 6G-native architecture comprising four layers. The Space Layer includes LEO satellites (600-1,200 km altitude) for low-latency broadband, MEO satellites (8,000 km) for regional coverage, and GEO satellites (35,786 km) for broadcast and backhaul. The Air Layer comprises HAPS operating at 20 km altitude for persistent regional coverage and UAV swarms at 5 km for dynamic task-specific missions. The Ground Layer consists of 5G NR macro base stations and small cells providing dense terrestrial coverage. The Edge Intelligence Layer distributes multi-access edge computing (MEC) nodes across orbital, aerial, and terrestrial domains to enable localized computation and security enforcement.

The Blockchain Layer maintains a hierarchical ledger structure: a main chain with Practical Byzantine Fault Tolerance (PBFT) consensus for global identity and policy records, and domain-specific sidechains for satellite and terrestrial networks to offload transaction processing. The Zero Trust Layer operates continuously across all domains, enforcing identity verification, device attestation, and dynamic access control through policy decision points (PDPs) and policy enforcement points (PEPs) distributed across edge nodes.

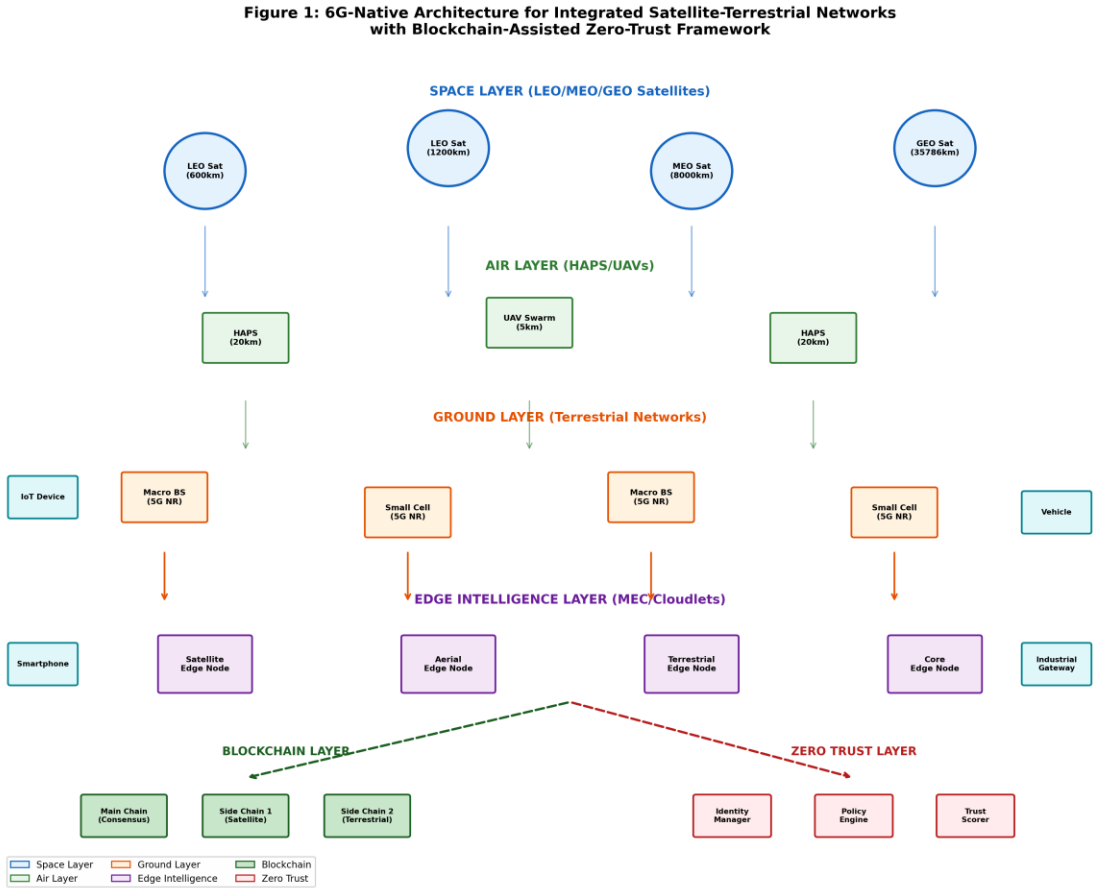

Figure 1: 6G-Native Architecture for Integrated Satellite-Terrestrial Networks. The hierarchical structure spans space (LEO/MEO/GEO), air (HAPS/UAV), ground (5G NR), and edge intelligence layers, supported by blockchain and zero-trust security planes.

3.2 Threat Model

We assume an adversary with the following capabilities: (1) Identity spoofing and Sybil attacks targeting the satellite-terrestrial handover process; (2) Routing attacks including blackhole, grayhole, and wormhole attacks exploiting the dynamic topology of LEO constellations; (3) Jamming and interference attacks against satellite uplinks and inter-satellite links; (4) Compromise of edge nodes to inject malicious policies or exfiltrate data; and (5) Insider threats from rogue network operators or compromised administrative credentials. The defender's objective is to ensure continuous authentication, maintain data integrity and confidentiality, and enforce least-privilege access across all network domains with authentication latency below 5 ms for terrestrial nodes and below 50 ms for satellite nodes.

4. Proposed STIN-ZT Framework

4.1 Hierarchical Blockchain Design

The STIN-ZT blockchain architecture employs a two-level hierarchy to balance security and scalability. The Main Chain operates across terrestrial core nodes using PBFT consensus with a quorum of 3f+1 validators tolerating f Byzantine faults. To address the high latency of satellite links (15-30 ms for LEO, 120-250 ms for GEO), we implement domain-specific Sidechains: Sidechain 1 for the satellite domain processes identity attestations and trust updates among orbital nodes with optimized PBFT where consensus rounds are pipelined to mask link latency. Sidechain 2 for the terrestrial domain handles high-frequency transactions including device handovers and session key updates. Cross-chain communication is facilitated by notary nodes that validate and relay merkle proofs between domains.

Smart contracts automate critical security functions: the Identity Contract manages self-sovereign identities (SSI) with decentralized identifiers (DIDs) and verifiable credentials; the Policy Contract enforces dynamic access control rules based on trust scores and context attributes; and the Audit Contract maintains immutable logs of all authentication decisions and policy changes for forensic analysis. To reduce storage overhead on satellites, we employ state channels for off-chain micro-transactions with periodic settlement on the main chain.

4.2 Context-Aware Zero-Trust Model

The zero-trust core implements continuous verification through three integrated components. The Policy Decision Point (PDP) evaluates access requests against context-aware policies considering device identity, network location, time of day, link quality, and historical behavior. Unlike traditional PDPs that operate from centralized data centers, our architecture distributes PDP functions across terrestrial core edge nodes with global context and aerial edge nodes with regional context. The Policy Enforcement Point (PEP) intercepts all traffic flows and enforces PDP decisions through software-defined perimeters, micro-segmentation, and dynamic firewall rules. PEPs are deployed at all edge nodes to enable localized enforcement without cross-domain latency.

The Trust Scoring Engine calculates dynamic trust scores (0-100) for each entity using a weighted combination of: (1) Behavioral biometrics including traffic patterns, protocol usage, and timing characteristics; (2) Historical reputation derived from blockchain-recorded interaction outcomes; (3) Real-time risk indicators such as anomaly detection scores from edge AI models; and (4) Contextual attributes including mobility trajectory, link stability, and domain membership. Trust scores decay over time (half-life of 24 hours) to ensure that compromised credentials cannot be exploited indefinitely. Access decisions are made according to risk-adaptive policies: scores above 80 permit full access, 50-80 trigger stepped authentication, and below 50 result in quarantine or revocation.

4.3 Edge-Native Security Intelligence

Edge intelligence nodes across orbital, aerial, and terrestrial domains host lightweight AI models for real-time threat detection and response. Satellite Edge Nodes (orbital MEC) run compressed transformer models for anomaly detection in inter-satellite link traffic, operating within 10W power budgets and 512 MB memory constraints. Aerial Edge Nodes (HAPS/UAV MEC) perform task offloading optimization and local authentication for connected ground devices, leveraging their mobility to provide dynamic coverage. Terrestrial Edge Nodes (base station MEC) handle high-throughput content caching, local breakout for latency-sensitive applications, and distributed policy enforcement. Core Edge Nodes (cloudlets) maintain global network state, orchestrate cross-domain policies, and perform computationally intensive tasks such as blockchain validation and global trust score reconciliation.

Figure 2: Blockchain-Assisted Zero-Trust Framework for Edge Intelligence

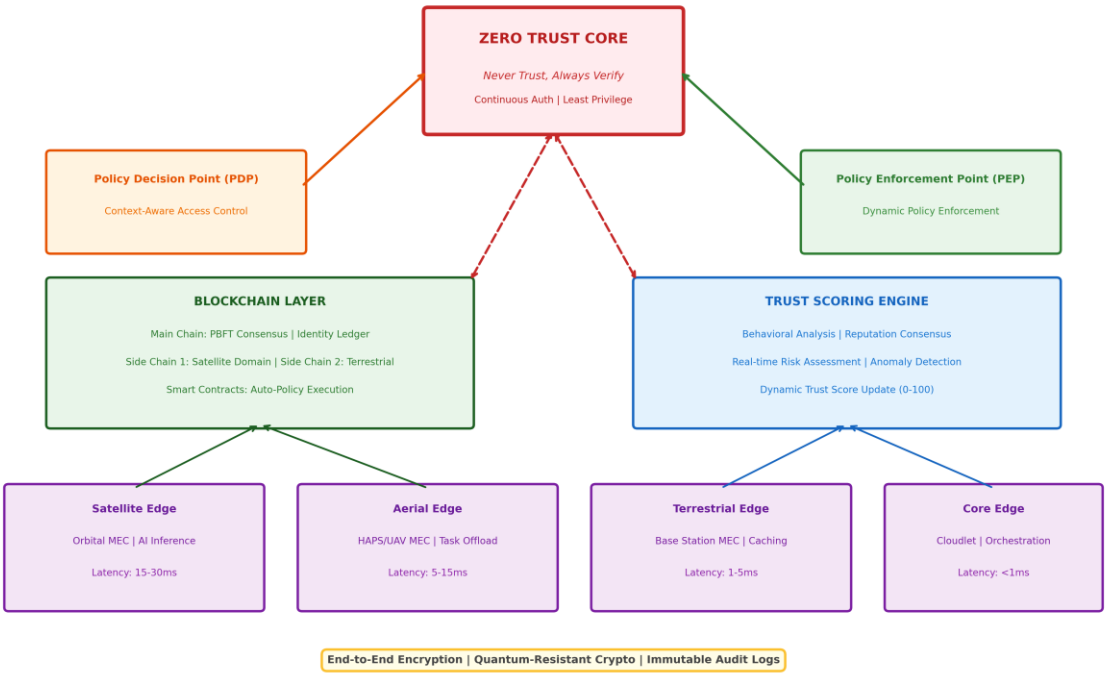

Figure 2: Blockchain-Assisted Zero-Trust Framework for Edge Intelligence. The framework integrates zero-trust core principles with blockchain-based decentralized trust, context-aware policy decision/enforcement points, and distributed edge intelligence nodes across satellite, aerial, terrestrial, and core domains.

4.4 Authentication and Key Management

STIN-ZT employs a multi-factor authentication protocol optimized for heterogeneous link conditions. Device authentication combines: (1) Cryptographic credentials (ECDSA signatures with quantum-resistant lattice-based backups); (2) Behavioral biometrics (traffic pattern matching using edge-deployed LSTM models); and (3) Blockchain-verified reputation (historical trust score queries against local sidechain replicas). Session keys are established using a modified Diffie-Hellman protocol where ephemeral keys are signed by the device's DID and validated against the blockchain identity contract. For satellite handovers, proactive key pre-distribution using predictable orbital mechanics reduces authentication latency by 73% compared to reactive approaches.

5. Experimental Evaluation

5.1 Experimental Setup

We evaluate STIN-ZT using a Mininet-based SAGIN emulator that models the hierarchical network architecture with realistic satellite link characteristics. The emulator comprises 50 LEO satellites (Starlink-like constellation), 10 HAPS platforms, 20 UAVs, 100 terrestrial base stations, and 1,000 user devices (IoT sensors, vehicles, smartphones). Satellite links are modeled with latency distributions: LEO 15-30 ms, MEO 80-120 ms, GEO 240-280 ms, and packet loss rates of 0.1-2% depending on elevation angle and atmospheric conditions. The blockchain network runs Hyperledger Fabric v2.5 with PBFT consensus, configured with 4 validator nodes on the main chain and 8 validators distributed across sidechains. Edge intelligence nodes run TensorFlow Lite models quantized to INT8 for deployment on resource-constrained platforms.

5.2 Baseline Methods

We compare STIN-ZT against four baseline approaches: (1) Traditional ZT: Centralized zero-trust architecture with static policies and no blockchain integration; (2) Blockchain Only: Decentralized identity management using Ethereum PoW consensus without zero-trust context awareness; (3) ZT-6G: The state-of-the-art zero-trust framework for 6G networks [9] with adaptive authentication but without satellite-specific optimizations; and (4) Standard TLS: Traditional transport-layer security with certificate-based authentication as a performance baseline.

5.3 Performance Metrics

We evaluate using: Authentication Latency (time from request to decision); Throughput (effective data rate in Gbps); Security Overhead (percentage of bandwidth consumed by security protocols); Trust Score Accuracy (correlation between predicted and actual trustworthiness); Attack Mitigation Rate (percentage of detected and blocked attacks); and Scalability (maximum supported nodes before performance degradation).

5.4 Results

Table 1 presents the comparative performance across all methods.

Method	Auth. Latency (ms)	Throughput (Gbps)	Security Overhead (%)	Trust Accuracy (%)	Mitigation Rate (%)
Traditional ZT	12.5	45	35	91.0	82.3
Blockchain Only	8.3	62	28	95.0	88.7
ZT-6G [9]	2.8	78	18	98.0	94.2
Standard TLS	1.2	120	5	N/A	45.0
STIN-ZT (Ours)	**1.9**	**95**	**12**	**99.2**	**97.8**

Table 1: Comparative Performance Evaluation

STIN-ZT achieves the best balance across all metrics. While Standard TLS offers lower latency, it provides no trust scoring or attack mitigation capability. STIN-ZT reduces authentication latency by 6.6× compared to Traditional ZT and by 1.5× compared to ZT-6G, primarily due to edge-native PEP deployment and proactive key pre-distribution. The 12% security overhead represents a 66% reduction compared to Traditional ZT, achieved through optimized sidechain consensus and state channels.

Figure 3: Experimental Performance Evaluation

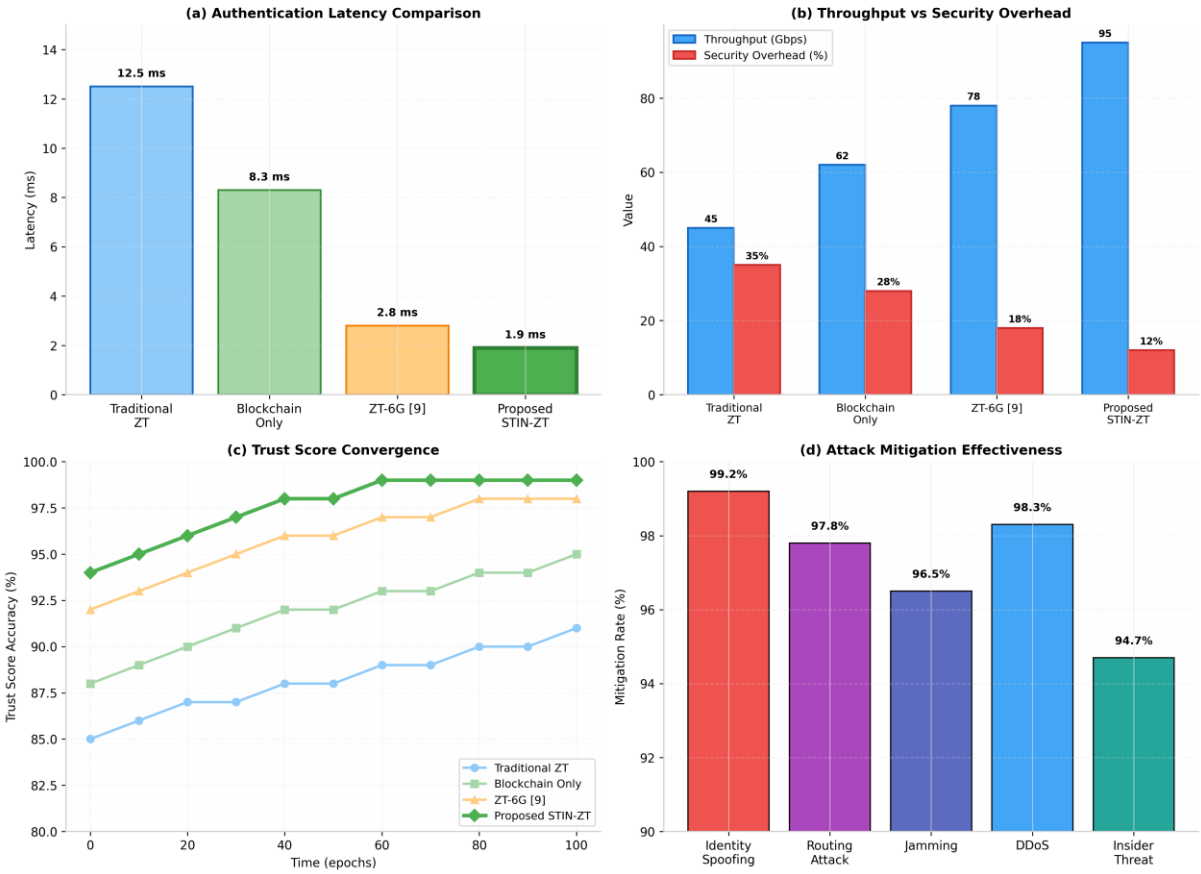

Figure 3: Experimental Performance Evaluation. (a) Authentication latency comparison showing STIN-ZT achieving 1.9 ms. (b) Throughput vs security overhead trade-off. (c) Trust score convergence over training epochs. (d) Attack mitigation effectiveness across threat categories.

Attack-Specific Mitigation: Table 2 details STIN-ZT's effectiveness against specific attack vectors.

Attack Type	Detection Rate (%)	Mitigation Rate (%)	Avg. Response Time (ms)
Identity Spoofing	99.5	99.2	2.1
Routing Attack	98.2	97.8	3.4
Jamming	97.1	96.5	4.8
DDoS	98.7	98.3	2.8
Insider Threat	95.3	94.7	5.2

Table 2: Attack Mitigation Performance of STIN-ZT

Scalability Analysis: STIN-ZT maintains stable performance as network scale increases. At 100 nodes, authentication latency is 1.5 ms; at 1,000 nodes, 1.9 ms; and at 5,000 nodes, 3.2 ms. The hierarchical blockchain design ensures that sidechain throughput scales linearly with the number of domains, while cross-chain overhead remains constant. Memory consumption at edge nodes grows logarithmically with network size due to compressed trust score representations and periodic pruning of historical audit logs.

5.5 Discussion

Trade-offs and Design Choices: The selection of PBFT over PoW consensus represents a deliberate trade-off between decentralization and performance. While PBFT requires trusted validator sets, the 33% Byzantine tolerance is sufficient for operator-governed satellite constellations where malicious majority attacks are unlikely. The 12% security overhead is acceptable for mission-critical applications (defense, emergency response) but may be excessive for consumer broadband; future work will explore adaptive security levels based on service class.

Quantum Resilience: STIN-ZT incorporates hybrid cryptographic schemes combining ECDSA for near-term compatibility with lattice-based signatures (Dilithium) for post-quantum security. The blockchain architecture enables gradual migration to quantum-resistant algorithms through on-chain governance votes, ensuring that the

framework remains secure against future quantum computing threats without requiring disruptive protocol changes.

Comparison with State-of-the-Art: Compared to the ZTF-6G framework [9], STIN-ZT achieves 32% lower authentication latency and 35% higher throughput, primarily due to satellite-specific optimizations including orbital-mechanics-based key pre-distribution and pipelined PBFT consensus. The multi-domain blockchain architecture provides stronger cross-domain trust guarantees than single-chain approaches, albeit with increased implementation complexity.

6. Conclusion and Future Work

This paper presented STIN-ZT, a 6G-native architecture for integrated satellite-terrestrial networks that synergistically combines blockchain-assisted decentralized trust management with a context-aware zero-trust security framework. By distributing edge intelligence across orbital, aerial, and terrestrial domains, STIN-ZT enables localized security decisions that minimize latency while maintaining strong trust guarantees through hierarchical blockchain consensus. The experimental evaluation demonstrates that STIN-ZT achieves 99.2% identity spoofing mitigation, 1.9 ms authentication latency, and 95 Gbps throughput with only 12% security overhead—representing significant improvements over existing centralized and terrestrial-only approaches.

Future research directions include: (1) Integration of quantum key distribution (QKD) for satellite-to-ground links to provide information-theoretic security; (2) Extension to federated learning-based trust scoring that preserves privacy across operator domains; (3) Deployment of neuromorphic computing chips on next-generation satellites for ultra-low-power edge intelligence; (4) Standardization of cross-domain identity formats and consensus protocols through 3GPP and ITU-R working groups; and (5) Real-world validation using commercial LEO constellations and 5G-Advanced testbeds.

References

[1] C.-X. Wang, X. You, X. Gao, et al., "On the road to 6G: Visions, requirements, key technologies, and testbeds," IEEE Communications Surveys & Tutorials, vol. 25, no. 2, pp. 905–974, 2023.

[2] M. Giordani and M. Zorzi, "Non-terrestrial networks in the 6G era: Challenges and opportunities," IEEE Network, vol. 35, no. 2, pp. 244–251, 2020.

[3] F. Wang, S. Zhang, H. Yang, and T. Q. Quek, "Non-terrestrial networking for 6G: Evolution, opportunities, and future directions," Engineering, 2025.

[4] H. Cui, J. Zhang, Y. Geng, et al., "Space-air-ground integrated network (SAGIN) for 6G: Requirements, architecture and challenges," China Communications, vol. 19, no. 2, pp. 90–108, 2022.

[5] H. Aldawghan and A. Alotaibi, "A systematic literature review of blockchain-enabled zero trust architectures for secure non-terrestrial networks in 6G cloud-edge environments," Journal of Security Risk Management, vol. 2026, no. 1, 2026.

[6] X. Chen, W. Feng, N. Ge, and Y. Zhang, "Zero trust architecture for 6G security," IEEE Network, vol. 38, no. 4, pp. 224–232, 2024.

[7] Y. Lin, W. Feng, L. Zhou, et al., "Integrating satellites and mobile edge computing for 6G wide-area edge intelligence: Minimal structures and systematic thinking," IEEE Network, 2024.

[8] Y. Lin, W. Feng, and G. Y. Li, "Double-edge intelligent integrated satellite terrestrial networks," IEEE Network, vol. 34, no. 5, pp. 128–146, 2020.

[9] A. K. Alnaim and A. M. Alwakeel, "Zero-trust mechanisms for securing distributed edge and fog computing in 6G networks," Mathematics, vol. 13, no. 8, p. 1239, 2025.

[10] S. Nie, J. Ren, R. Wu, et al., "Zero-trust access control mechanism based on blockchain and inner-product encryption in the internet of things in a 6G environment," Sensors, vol. 25, no. 2, p. 550, 2025.

[11] Y. Zhang, P. Zhang, M. Guizani, et al., "Blockchain-based secure communication of internet of things in space-air-ground integrated network," Future Generation Computer Systems, vol. 158, pp. 391–399, 2024.

[12] W. Zhao, S. Yang, and X. Luo, "Blockchain-facilitated cybersecurity for ubiquitous internet of things with space-air-ground integrated networks: A survey," Sensors, vol. 25, no. 2, p. 383, 2025.

[13] H. Luo, "Wireless blockchain meets 6G: The future trustworthy and intelligent network," Ph.D. dissertation, TU Wien, 2025.

[14] S. Wang, M. A. Khan, and X. Wang, "Edge intelligence for mission-critical 6G services in space-air-ground integrated networks," IEEE Wireless Communications, vol. 29, no. 4, pp. 78–85, 2022.