Optimized Blockchain Consensus for Secure and Scalable Routing in 6G Nonterrestrial and Terrestrial IoT Networks

Jonathan Mukisa Kalibbala, Love Allen Chijioke Ahakonye, *Member, IEEE*, Dong-Seong Kim, *Senior Member, IEEE*, and Jae-Min Lee, *Member, IEEE*

***Abstract*—The convergence of nonterrestrial networks (NTNs) and terrestrial networks (TNs) in 6G presents a paradigm shift for the Internet of Things (IoT), enabling ubiquitous connectivity but introducing severe routing challenges across a dynamic, multidomain topology. Traditional blockchain-based routing frameworks often fail to adapt to the mobility, heterogeneity, and energy constraints of IoT deployments. This article proposes a Proof-of-Route (PoR) blockchain consensus protocol, augmented with Proof-of-Authority (PoA), with adaptive validator rotation for secure and scalable routing. The protocol integrates cryptographic route authentication, dynamic validator selection, and wallet-based key management. This ensures its resistance against black holes, Byzantine attacks, and Sybil attacks. Unlike prior work, our framework was evaluated under conditions that mirror real-world operational stress. Modular Docker-based containers were developed to represent devices in a 6G-IoT setting. They simulated intermittent link availability, varying latencies, node churn, and handovers. Results revealed that the proposed protocol achieved up to an average latency of 42.3 ms, a packet delivery ratio (PDR) of 98.7% with scalability verified up to over 500 nodes. This article offers a robust, scalable, and secure solution for the complex routing demands of 6G networks.**

***Index Terms*—6G networks, blockchain consensus, cryptographic routing, data packets, Internet of Things (IoT), nonterrestrial networks (NTNs), security.**

I. Introduction

THE advent of 6G is expected to usher in an era of ubiquitous connectivity, seamlessly integrating terrestrial networks (TNs) with non-TNs (NTNs) composed of satellites, high-altitude platforms (HAPs), and unmanned aerial vehicles (UAVs) [1], [2]. This paradigm of terrestrial and NTNs creates a 3-D, highly dynamic communication environment for the Internet of Things (IoT) [3]. It is, thus, challenging to establish a scalable, reliable, and secure routing protocol in this vast heterogeneous ecosystem. TNTs are characterized by extreme node mobility, intermittent link connectivity, long propagation delays, and diverse node capabilities, all of which render traditional routing protocols inadequate [4].

The conventional routing protocols, such as the Open Shortest Path First (OSPF) and the Border Gateway Protocol (BGP), rely on centralized decision-making. OSPF builds fixed routes within a network domain, while BGP oversees interdomain routing based on established rules. In the face of the 6G networks, which are associated with dynamic conditions, OSPF and BGP are exposed to security risks such as spoofing and route hijacking [5], creating urgency for a more secure routing protocol. Recent research underscores the use of blockchains as solutions for the urgency [6].

Blockchain establishes a decentralized consensus among nodes, with a tamper-resistant ledger that provides a trail for the delivery of data packets [7]. However, different types of consensus mechanisms are deployed in blockchain networks. Among these are the Proof-of-Work (POW), Proof-of-Stake (POS), Proof-of-History, and many more. These greatly influence the security efficiency of the blockchain network in data-packet routing. For example, POW guarantees transaction integrity but with high energy consumption and slower transaction throughput, rendering it unsuitable for the stringent requirements of IoT and 6G network architectures [8]. Also, the POS adopted in the Ethereum 2.0 links validators to participants' stake in the network, decreasing energy demand but risks faltering with NTN's unstable connections. These highlight the necessity [9] for a consensus mechanism that provides speed, security, and scalability for 6G networks.

Recent developments have modified the existing consensus frameworks for IoT and 6G applications. An example is the IOTA's Tangle, which employs a directed acyclic graph (DAG) model. This allows fast transactions without fees, which enhances scalability and efficiency for IoT routing [10]. Another is Microsoft's Confidential Consortium Framework (CCF), which utilizes trusted execution environments to achieve rapid and low-latency consensus within permissioned networks focused on TN applications in 5G. However, NTNs' inherent mobility and intermittent connectivity remain

Received 8 September 2025; revised 4 December 2025; accepted 21 December 2025. Date of publication 24 December 2025; date of current version 9 March 2026. This work was supported in part by the Innovative Human Resource Development for Local Intellectualization Program through Institute for Information and Communications Technology Planning and Evaluation (IITP) grant funded by Korean Government [Ministry of Science and ICT (MSIT)] under Grant IITP-2025-RS-2020-II201612, 25%; in part by the Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by Ministry of Education, Science and Technology (MEST) under Grant 2018R1A6A1A03024003, 25%; in part by MSIT, South Korea, under the Information Technology Research Center (ITRC) Support Program under Grant IITP-2025-RS-2024-00438430, 25%; and in part by the Basic Science Research Program through NRF funded by the Ministry of Education under Grant RS-2025-25431637, 25%. *(Corresponding author: Jae-Min Lee.)*

Jonathan Mukisa Kalibbala, Dong-Seong Kim, and Jae-Min Lee are with the Department of IT Convergence Engineering and NSLab, Kumoh National Institute of Technology, Gumi 39177, South Korea (e-mail: kjonmukisa@kumoh.ac.kr; dskim@kumoh.ac.kr; ljmpaul@kumoh.ac.kr).

Love Allen Chijioke Ahakonye is with the ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi 39177, South Korea (e-mail: loveahakonye@kumoh.ac.kr).

Digital Object Identifier 10.1109/JIOT.2025.3647960

a significant hurdle [11] that compromises the mentioned benefits.

The Proof-of-Route (PoR) framework is proposed in this study as a novel approach to optimize routing in 6G NTN-TN IoT networks. Distinct from other works that rely on unscalable and unreliable consensus mechanisms, the PoR framework implements a Byzantine fault-tolerant (BFT) consensus mechanism based on a rotating leader in which a committee of trusted validators collaboratively approves new routes. The rotation of the leader role ensures high security and liveness without relying on a single point of authority.

In addition, the PoR framework replaces conventional IP addresses with cryptographic key pairs for routing identification, which enhances authentication and integrity at each transmission step [12]. It incorporates parallel transaction verification through multithreading, hence reducing latency and increasing the volume of transactions relevant to 6G deployments [4], [13].

In this study, the following is the summary of the key contributions.

1) *Novel PoR Consensus Mechanism:* We propose the first blockchain-based routing protocol that integrates BFT consensus directly into route discovery, providing cryptographic validation of routing decisions.
2) *Proof-of-Authority (PoA)^2 Adaptive Validator Rotation:* We design a dynamic validator selection algorithm that balances geographic coverage, trust scores, and network proximity, addressing the static validator limitation of traditional PoA.
3) *Wallet-Based Identity System:* Our approach replaces IP addressing with cryptographic key pairs, enabling secure authentication without a centralized PKI in heterogeneous NTN–TN environments.
4) *Comprehensive Multiscenario Validation:* We evaluate PoR across six scenarios (static mesh, high mobility, urban, stress, partition, and handover) with 50–300 nodes, demonstrating ~42.3-ms routing latency and 96%–98% PDR under diverse conditions.
5) *Energy-Aware Blockchain Routing:* PoR incorporates Smart *AutoProposer* and *AutoMining* mechanisms to reduce unnecessary block generation, addressing energy constraints in IoT devices.

II. Related Works

The ongoing convergence of TNs and NTNs in the emerging 6G IoT ecosystem is reshaping how routing is conceived and deployed. This integration promises seamless coverage, ultralow latency, and high resilience by connecting satellites, HAPs, UAVs, and terrestrial nodes into a unified communication fabric. However, the heterogeneity that enables global coverage simultaneously creates unprecedented challenges, including highly dynamic topologies, frequent handovers, cross-domain governance, and fluctuating channel conditions. As several surveys emphasize, traditional terrestrial routing stacks face significant challenges under 6G-IoT conditions, including Doppler shifts, high mobility, and multioperator trust requirement [2], [14].

Although foundational to terrestrial Internet infrastructure, some traditional terrestrial routing protocols depend on relatively static path configurations and others on policy-driven rerouting mechanisms, rendering them inadequate for the high-velocity dynamics of NTN–TN ecosystems. Their slow convergence and centralized control introduce fragility in multidomain environments, often resulting in routing loops, suboptimal paths, or network partitioning during satellite handovers [8], [9]. This has prompted researchers to argue for routing fabrics in which security and adaptability are built directly into the control plane, rather than appended as afterthoughts [10], [11].

Lightweight protocols such as AODV, OLSR, and RPL, which originally were efficient in MANETs and constrained IoT, struggle under NTN–TN convergence. The 6G networks' high mobility, sporadic links, and heterogeneity disrupt neighbor discovery and route maintenance among traditional routing protocols, whereas attempts to retrofit security into these protocols often incur prohibitive energy costs [13], [15], [16], [17].

To address the discussed gaps, recent work has focused on the adoption of blockchain and distributed ledgers as decentralized, verifiable routing enablers. Wei et al. [18] first proposed satellite-terrestrial blockchains for IoT governance. This inspired a wave of lightweight consensus models tuned specifically for IoT. Abbasi et al. [19] introduced Proof-of-Resource to improve scalability and energy efficiency in IoT blockchains. Das and Srivastava [20] proposed HyPoPE, blending participation and efficiency for throughput gains in constrained networks. Uveise and Fathima [21] designed LIGHT-SB to balance scalability and security, while Andola et al. [22] developed PoEWAL to reduce energy and latency via probabilistic validation in IoT blockchains. Other works, such as Mohan et al. [23] and Delladetsimas et al. [24], explored hybrid frameworks and zero-knowledge proofs in mobile and maritime IoT contexts. Together, these efforts signal a shift toward energy-aware, application-specific ledger solutions that can be used as well in 6G NTNs-TNs.

Despite the mentioned progress, most existing proposals overlook key mobility and hybridization challenges in NTN–TN convergence. Zehir and Zehir [25] highlighted the potential of hybrid and consortium blockchains for mobile ecosystems. Similarly, Abbasi's Proof-of-Resource and Das's HyPoPE improve energy efficiency but ignore handovers, Doppler effects, and multiorbit interactions [19], [20]. In contrast, the proposed PoR framework integrates mobility management through adaptive PoA rotation and ledger-backed route verification. PoR is explicitly validated in high-mobility and hybrid NTN–TN handover scenarios, addressing gaps left by prior lightweight blockchain models.

Consensus-based routing has also been studied with research by Yazdinejad et al. [26] who used blockchain-secured SDN controllers to bolster IoT security, while Maadallah et al. [27] revisited Proof-of-Work despite energy tradeoffs. Though they are resilient to adversarial threats, these models face scalability issues in large TN–NTN environments. DAG-based approaches such as IOTA's Tangle, including the "Rebased" upgrade, offer high throughput and low cost.

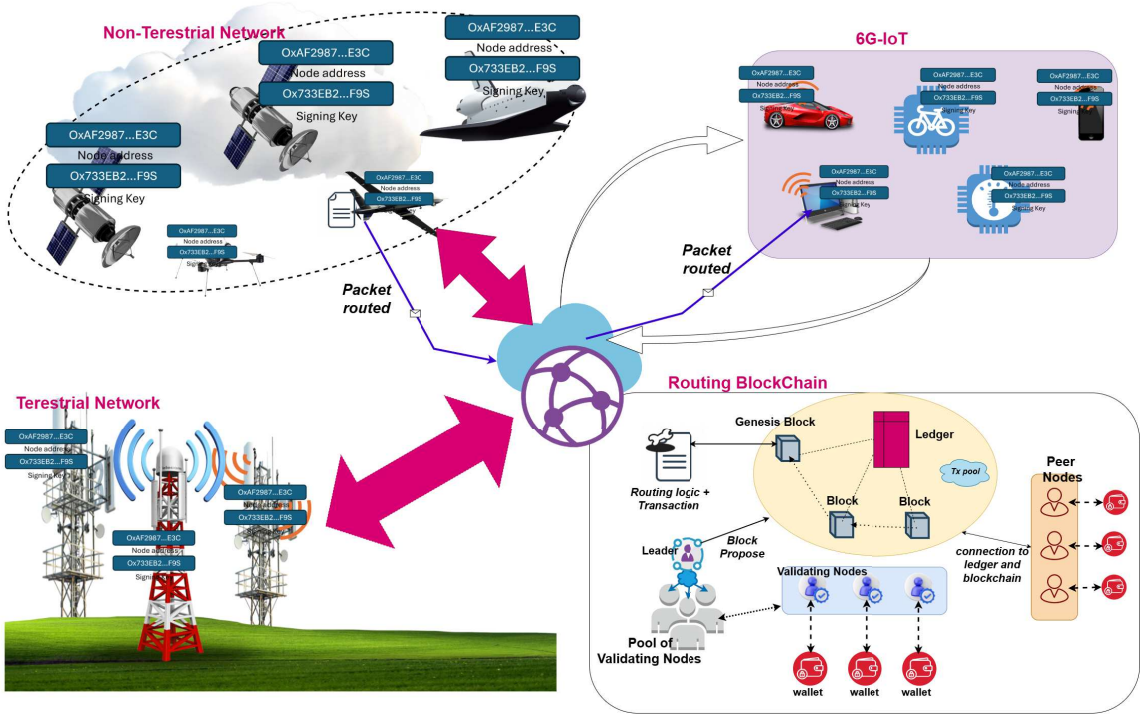

Fig. 1. System architecture of the PoR framework integrating TNs, NTNs, and 6G IoT devices with a routing blockchain.

However, their resilience under NTN latencies and fragmented governance is uncertain [9]. Permissioned blockchains, in contrast, ensure predictable validator behavior and low latency but struggle with cross-domain interoperability.

Energy efficiency continues to surface as a binding constraint. Maitra et al. [28] proposed a lightweight Proof-of-Authentication consensus for IoT devices, while Yan et al. [29] introduced hardware-level optimizations for blockchain primitives. These reinforce the importance of balancing cryptographic rigor with constrained energy budgets in IoT endpoints. However, few of these designs have been tested in NTN conditions with large-scale handovers or multidomain coordination.

The proposed PoR Framework advances lightweight and hybrid consensus research by directly addressing the core challenges of NTN–TN routing mobility, hybridization, security, and energy. Unlike Abbasi's Proof-of-Resource, which focuses on energy efficiency without mobility testing, PoR is validated under satellite handovers and high-mobility scenarios [19]. The proposed PoR surpasses HyPoPE and LIGHT-SB by benchmarking smart contract performance and defends against routing-specific attacks such as blackhole, Sybil, wormhole, and eclipse through the inherent properties of wallet-based addressing and cryptographic route tracing on the blockchain [9], [20], [21].

Collectively, the literature demonstrates significant progress toward lightweight, scalable, and energy-efficient blockchain systems for IoT. However, PoR distinguishes itself by addressing the mobility, hybridization, security, and energy challenges that characterize NTN-TN convergence, providing both simulation and empirical validation, and charting a path toward deployable, secure routing fabrics for 6G IoT ecosystems.

III. System Methodology and Design

Fig. 1 illustrates the system architecture of the PoR framework, which integrates TNs, NTNs, and 6G IoT devices into a unified routing blockchain. Nodes in both the terrestrial domain (e.g., base stations and towers) and the nonterrestrial domain (e.g., LEO satellites, UAVs, and aircraft) are assigned cryptographic identities consisting of public node addresses and signing keys. These nodes interact with heterogeneous IoT devices such as vehicles, wearables, and sensors, which also participate in route discovery and data exchange through lightweight wallets that generate and sign transactions. At the core of the architecture lies the routing blockchain, where route requests and updates are captured as transactions, proposed by a rotating leader validator, and finalized by a pool of validating nodes operating under the PoA^2 consensus protocol enhanced with AutoProposer and Smart AutoMining. The ledger maintains the genesis block, validated route blocks, and pending transaction pools, while peer nodes connect to the chain for routing and data services. This integrated architecture ensures that route discovery, validator management, and ledger synchronization are executed securely and efficiently across NTN-TN segments, enabling deterministic, auditable routing for large-scale 6G IoT deployments.

The PoR protocol was designed for 6G terrestrial and nonterrestrial IoT networks (TN/NTN), where routing must remain secure, scalable, and auditable under conditions of high mobility and intermittent connectivity. Unlike conventional blockchain systems, PoR deliberately avoids embedding a

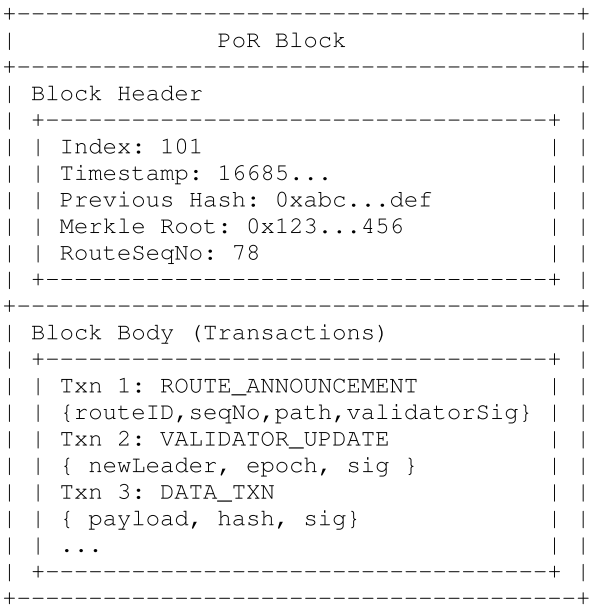

Fig. 2. Detailed structure of a PoR block, highlighting the routing-specific "RouteSeqNo" field in the header and the types of transactions.

smart contract virtual machine, as contract execution introduces computational and latency overheads unsuitable for resource-constrained IoT devices. Instead, PoR encodes routing and control logic through specialized transaction types, enabling lightweight execution directly at the consensus layer.

In defining and solving the problem, the NTN-TN environment is modeled as a dynamic graph $G = (N, E)$, with N representing IoT devices, UAVs, vehicles, or satellites, and E representing dynamic wireless links. A subset $V \subseteq N$ is a set of validators that execute consensus. Operating in a permissioned BFT setting, validators are known but may behave Byzantine; finality is guaranteed once a block reaches quorum. In a real scenario, validators can be the network service providers. These entities, such as satellite operators, terrestrial ISPs, or edge infrastructure owners, are inherently positioned across different network domains and possess both the operational capacity and administrative trust to manage routing decisions.

A. Block Structure

Fig. 2 illustrates the internal configuration of a PoR block, which augments the traditional blockchain format by incorporating routing-specific metadata and transactions. The block is segmented into two primary components: 1) the block header, which consists of standard blockchain elements, including the block index, timestamp, and previous hash and 2) the Merkle root, which upholds chain integrity and immutability. In addition, the PoR framework introduces the RouteSeqNo field, which is distinctive to routing-aware consensus. This sequence number facilitates the ordering of route announcements and the detection of replayed or outdated information across the network, thereby ensuring consistency in rapidly evolving TN–NTN environments.

By embedding this routing context directly into the header, PoR ensures that the routing state is inseparable from the consensus state, thereby enhancing both security and auditability. This also reduces the overhead cost that would be incurred in accessing the smart contract for every packet routing. The block body encompasses transactions that enable PoR's dual functionality as both a routing ledger and a general-purpose blockchain. The foremost transaction type is the ROUTE_ANNOUNCEMENT, which records route identifiers, sequence numbers, paths, and validator signatures. This transaction type provides the verifiable foundation for route propagation and agreement across validators. The second transaction type, VALIDATOR_UPDATE, manages adaptive validator rotation and leader election within the PoA^2 consensus mechanism. By documenting validator changes in the ledger, the system mitigates centralization and supports Byzantine resilience. Last, the DATA_TXN transaction type accommodates application payloads, such as IoT data, alongside routing control information, demonstrating the extensibility of the PoR ledger.

This design diverges from existing lightweight consensus frameworks [19], [20] by explicitly integrating routing security and mobility management into the ledger structure. While previous protocols primarily focus on energy efficiency or throughput, PoR blocks encode routing state, validator dynamics, and application data in a unified structure, facilitating verifiable route discovery and secure consensus in hybrid TN–NTN environments. By coupling routing metadata with blockchain consensus, PoR ensures that every route is both cryptographically auditable and resilient to adversarial disruption, which is essential for 6G IoT deployments where trust and mobility are equally critical.

B. Consensus and Routing Integration

The core logic of the PoR protocol is captured in Algorithms 1 and 2, which provides the formal specification of the PoR consensus cycle. The process is event-driven, managed through a set of procedures that handle incoming transactions, block proposals, and votes. As in the Algorithm 1, the need for a route triggers the consensus protocol. This is further expounded in the following steps.

1) *Initiation:* A node needing a route broadcasts a transaction of type ***RREQ***.
2) *Leader Action:* The current leader, determined by a round-robin schedule from a list of validators, receives this transaction.
3) *Block Proposal:* The leader computes a route, creates a ***ROUTE_ANNOUNCEMENT*** transaction, and proposes a new block containing this transaction.
4) *Validation and Voting:* The leader broadcasts the proposed block to other validators. Each validator checks the block's validity (hash, previous hash, sequence number, and so on). If valid, it broadcasts a signed vote for the block.
5) *Finalization:* Once a quorum of votes is collected (a step inferred from standard BFT design though not fully implemented in the provided code), the block is considered final and is added to each node's local copy of the blockchain.

Algorithm 1 PoR Consensus Cycle Part I: Initiation, Leader Action, and Block Proposal (AutoProposer)

Definitions:
$V \leftarrow$ set of all validator nodes
$L \leftarrow$ current leader node, $L \in V$ (round-robin PoA^2 rotation)
$T_{pool} \leftarrow$ pool of pending transactions
$B_{chain} \leftarrow$ local copy of the blockchain

Step 1: Initiation
A node needing a route broadcasts a transaction of type`RREQ`, which is added to T_{pool}.

Step 2: Leader Action
if self is L and $|T_{pool}| > 0$ **then**
return AutoProposer()
end if

function AutoProposer()
$tx \leftarrow$ GetTransactionFromPool(T_{pool})
$route \leftarrow$ ComputeRoute(tx.source, tx.dest)
$tx_{ann} \leftarrow$ CreateTransaction(`ROUTE_ANNOUNCEMENT`, *route*)
$prev\_block \leftarrow B_{chain}$.latest()
block $\leftarrow$ CreateBlock(tx_{ann}, $prev\_block$.hash)
block.signature $\leftarrow$ Sign(*block*)
Broadcast(`PROPOSE`, *block*)
Log("AutoProposer triggered: block proposed for ROUTE_ANNOUNCEMENT")
return *block*
// end function

Step 3: Block Proposal
The leader broadcasts the proposed block to all validators.

This process ensures that no route can be added to the network's shared state without the agreement of a majority of trusted validators, providing a strong defense against malicious route advertisements. The system does not rely on a separate smart contract for key management; rather, the management of validators and roles is handled within the application logic itself.

C. Wallet and Identity Management

To meet its decentralization and security objectives, the PoR framework uses cryptographic key pairs for device identification, replacing traditional IP addressing for routing decisions. Each node has a wallet that generates a public–private key pair. The public key is hashed to create a unique node address, which is used in the ***`path`*** field of a ***`Route`*** object. The private key is used to sign all transactions and blocks, ensuring authenticity and integrity at every step. This is achieved through employing the elliptic curve cryptography (ECC). PoR utilizes the secp256k1 curve, which is well-suited for resource-constrained IoT devices due to its efficiency and robust security properties. This curve is defined over a finite field $\mathbb{F}_p$, characterized by a large prime number p as denoted in the following equation:

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1. \quad (1)$$

The equation defining the secp256k1 curve simplifies to the following equation:

$$y^2 = x^3 + ax + b \mod p \quad (2)$$

in which the parameters a and b are set to 0 and 7, respectively. The ECC curve has a base point G that serves as a generator point, possessing a large prime order n, approximately 2^{256}.

Algorithm 2 PoR Consensus Cycle Part II: Validation, Voting, and Finalization (Smart AutoMining)

Step 4: Validation and Voting
Each validator checks block validity (hash, previous hash, RouteSeqNo, etc.) and broadcasts a signed vote.

function HandleBlockProposal(*block*)
if VerifyBlock(*block*) **then**
    vote $\leftarrow$ CreateVote(*block*.hash)
    vote.signature $\leftarrow$ Sign(*vote*)
    Broadcast(`VOTE`, *vote*)
    return *vote*
else
    return null
end if

function HandleVote(*vote*)
if VerifyVote(*vote*) **then**
    Add *vote* to $Votes[vote.block\_hash]$
    if $|Votes[vote.block\_hash]| \geq$ QUORUM_SIZE **then**
        $final\_block \leftarrow$ GetProposedBlock($vote.block\_hash$)
        if $final\_block$ is not null and not in B_{chain} **then**
            return SmartAutoMining($final\_block$)
        end if
    end if
end if
return null

Step 5: Finalization
Once a quorum of votes is reached, the block is finalized and appended to the blockchain.

function SmartAutoMining(*block*)
if $|T_{pool}| > 0$ **then**
    CommitBlock(*block*)
    Log("Smart AutoMining: Block committed with transactions")
else
    Log("Smart AutoMining: skipped empty block")
end if

function CommitBlock(*block*)
B_{chain}.add(*block*)
UpdateStateFromBlock(*block*)
return true = 0

The private key is denoted as d, and it is generated as a randomly selected integer in the range 1 to $n-1$. The cryptographically secure pseudorandom number generator (CSPRNG) is utilized to ensure the randomness and unpredictability of the key generation process. This mitigates ***brute-force attacks***. The corresponding public key Q is derived through scalar multiplication of the private key d with the base point G, mathematically expressed as follows:

$$Q = d \cdot G \tag{3}$$

where the notation "$\cdot$" represents ECC point multiplication, which involves a series of point additions and doublings on the elliptic curve. The resulting public key Q is a point on the curve represented by its coordinates x, y. It is formatted either as a 65-B string $04\|x\|y$ or as a compressed 33-B version $02/03\|x$, depending on the parity of y. In order to generate the node address used for routing in PoR, the resulting public key undergoes a hashing process with the Keccak-256 hash function, resulting in the following equation:

$$\text{Node Address} = \text{Keccak-256}\,(Q)\,. \tag{4}$$

The process yields a 20-B address, which is prefixed with $\mathbf{0}x$ to create the final node address. The security of the ECC implementation is based on the elliptic curve discrete logarithm problem, which ensures that deriving d from Q and G is computationally infeasible. The secp256k1 curve provides approximately bits of security, making it resilient against potential attacks, including those merging from quantum computing technologies. In addition, PoR uses the CSPRNG for private key generation, which enhances the unpredictability of the keys. This also strengthens the PoR framework against exhaustive search strategies and ensures secure routing across the dynamic NTN-TN integrated as in Fig. 3.

D. Optimizations for Scalability and Efficiency

The PoR protocol incorporates several architectural optimizations designed to ensure scalability, responsiveness, and efficiency in large-scale 6G TN–NTN IoT networks. These optimizations are motivated by the dual constraints of high device mobility and limited computational and energy resources, which render traditional blockchain and routing approaches infeasible in practice.

1) On-Demand Consensus: Unlike proactive protocols that continuously generate control traffic regardless of network demand, PoR employs an on-demand consensus model. Consensus rounds are initiated only when routing or application events occur, such as the submission of a new route request (RREQ) or a link failure requiring reconfiguration. This quiescent design reduces control overhead, conserves bandwidth, and minimizes energy consumption, making it particularly effective in battery-constrained IoT deployments.

2) AutoProposer for Low-Latency Responsiveness: At the heart of this design is the AutoProposer, a module that automatically monitors the transaction pool and initiates block proposals when valid routing transactions are detected. For example, when a ***ROUTE_ANNOUNCEMENT*** transaction enters the pool, the current leader validator immediately assembles and broadcasts a candidate block without requiring manual triggers. This mechanism provides low-latency responsiveness, ensuring that route updates are proposed and validated quickly in dynamic TN–NTN environments where stale routes can lead to connectivity loss.

3) Smart AutoMining for Resource Efficiency: Complementing the AutoProposer, the Smart AutoMining guarantees that blocks are only mined if the transaction pool contains pending work. If no transactions exist, no block is produced, preventing the generation of empty blocks. This mechanism optimizes resource usage by eliminating redundant computation, storage, and communication overhead. Logs from the 50-node testbed (`automining.log`) confirm that blocks were created only under active load, while idle periods saw no block generation. Together, AutoProposer and Smart AutoMining embody PoR's event-driven efficiency model: consensus and block production occur only when strictly necessary.

4) Controlled Dissemination: To further minimize overhead, PoR avoids network-wide flooding of route requests. Instead, it relies on controlled dissemination, whereby RREQs are forwarded only to the validator committee. This selective propagation sharply reduces redundant transmissions and routing chatter, especially in dense IoT topologies where traditional flooding can overwhelm the network.

5) RREP Integrity Without Redundant Consensus: Since the complete forward path is already validated during the RREQ consensus process and immutably stored on the blockchain, there is no need to revalidate this path during RREP propagation. Instead, PoR focuses on ensuring authenticity and adherence to the trusted route. Each RREP is individually signed by every intermediate node as it traverses the path, enabling downstream verifiers to easily authenticate its integrity.

Finally, PoR adopts a hierarchical validator model to extend scalability. Validators can be organized into clusters or regional committees, each managing routing within its partition. A higher-level intercluster validator committee coordinates routes across partitions. This hierarchical arrangement localizes consensus overhead while preserving global consistency, enabling PoR to scale to millions of devices in heterogeneous TN–NTN deployments.

E. System Implementation and Experimental Setup

The PoR framework was implemented using a hybrid architecture combining Java and Python to optimize modularity, performance, and scalability. Core protocol logic was developed in Java using Spring Boot, while Python modules supported advanced data analysis. To ensure isolation and reproducibility, all components were deployed via Docker, with each simulated network node instantiated as an individual container. The validators were orchestrated using Docker Compose with synchronized configurations. A single Docker image was created to include the Java runtime, protocol classes, networking utilities, and a custom entrypoint script that defined each container's runtime behavior.

Different container types activated movement logic in the Java application to periodically update node positions and routing decisions in accordance with specific mobility profiles

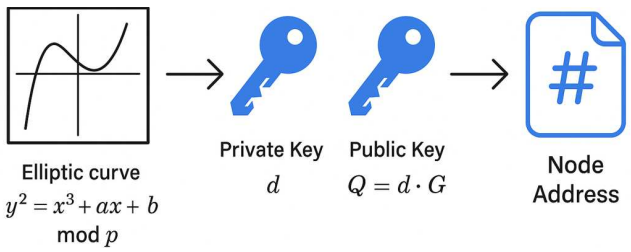

Fig. 3. ECC-based node identity generation in PoR blockchain: from curve to address.

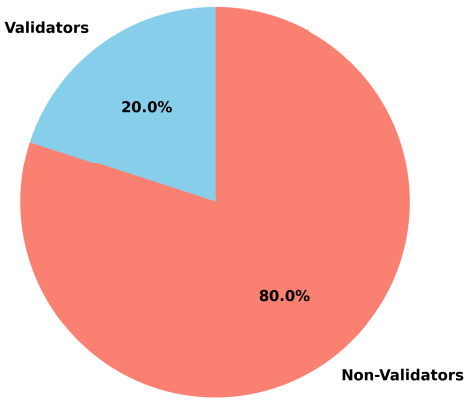

Fig. 4. Role distribution in the 50-node scale test. Validator nodes represent 20% of participants, demonstrating the efficiency of PoA^2's adaptive rotation in balancing decentralization with low overhead for constrained IoT devices.

mirroring real-life scenarios. All nodes were connected via a shared Docker bridge network using static IPs and a common multicast group, enabling controlled, large-scale experimentation.

The evaluation covered six distinct scenarios: static mesh, high mobility (LEO satellite emulation), dense urban deployment, stress testing, partition and self-healing, and TN–NTN handover, each targeting unique challenges in hybrid 6G-IoT topologies. These simulations, ranging from 50 to 500 nodes, generated over 1000 data points measuring latency, packet delivery ratio (PDR), consensus success, and network overhead. PoR was benchmarked against established protocols such as AODV, OLSR, and DSR, with results demonstrating superior convergence speed and resilience under high-load and adversarial conditions as discussed in the following.

IV. Results and Discussion

The PoR framework was evaluated across multiple scenarios representing the diverse operating conditions of integrated TN–NTN networks. Figs. 4–10 illustrate how the design principles of validator rotation, lightweight consensus, and cryptographic routing translate into quantifiable performance outcomes. The results demonstrate that PoR not only sustains the scalability expected in 6G IoT ecosystems but also addresses reliability and mobility challenges that hinder conventional approaches.

Fig. 4 presents the distribution of validators versus non-validators in the 50-node scale test. A validator ratio of 20% proved sufficient to sustain consensus finality while

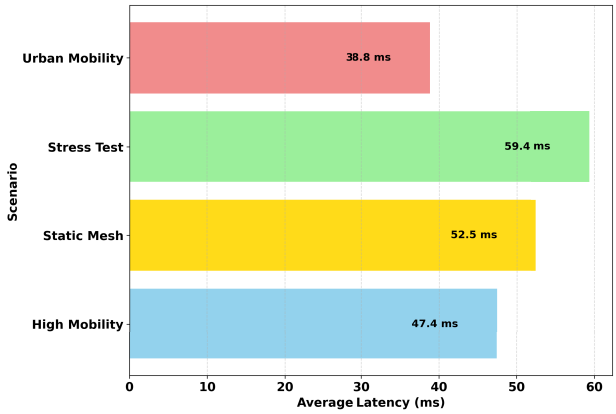

Fig. 5. Blockchain performance across scenarios. PoR sustains average latency below 60 ms across static, mobility, urban, and stress scenarios, highlighting suitability for dynamic TN–NTN routing.

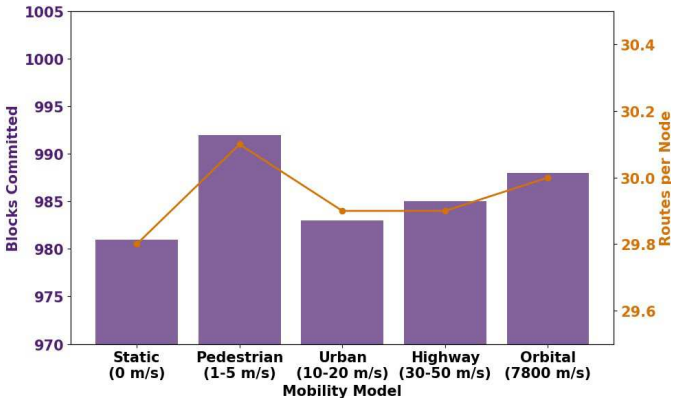

Fig. 6. Mobility impact on blockchain commitments and route distribution in PoR protocol.

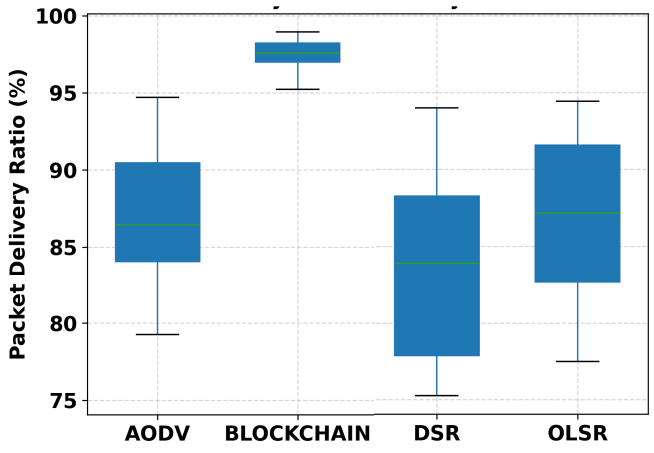

Fig. 7. Reliability distribution across protocols. PoR achieves PDR above 97% with low variance, outperforming legacy MANET protocols that show reduced reliability under mobility.

minimizing computational and energy overhead across the network. This balance reflects the efficiency of PoA^2's adaptive validator rotation: consensus responsibility is shared across a manageable subset of nodes, ensuring decentralization without burdening all devices. This PoR design aligns well with the resource-constrained IoT setting, where not all participants

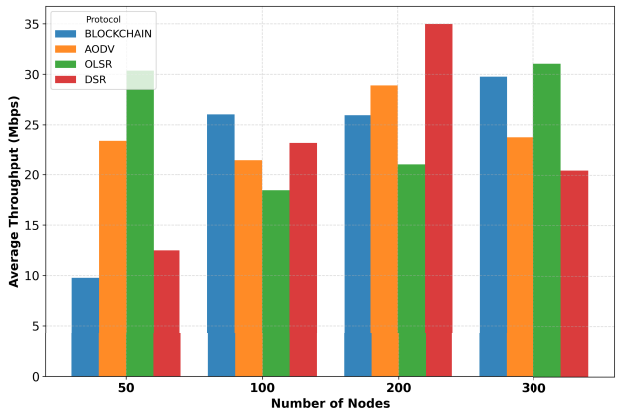

Fig. 8. Throughput scaling by node count. PoR maintains stable throughput up to 300 nodes, whereas conventional protocols fluctuate, confirming scalability for dense IoT deployments.

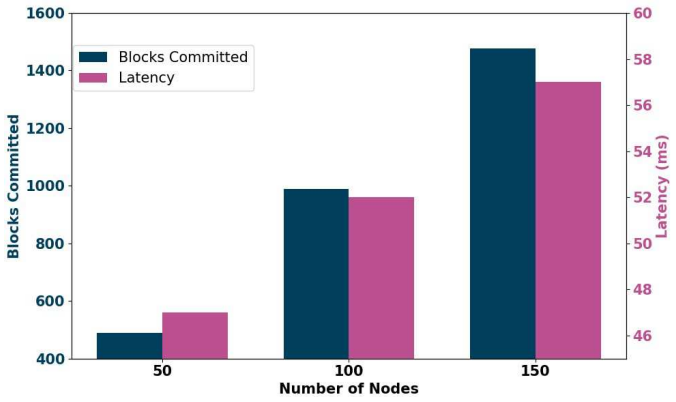

Fig. 9. Impact of network size on blockchain load and latency in PoR protocol.

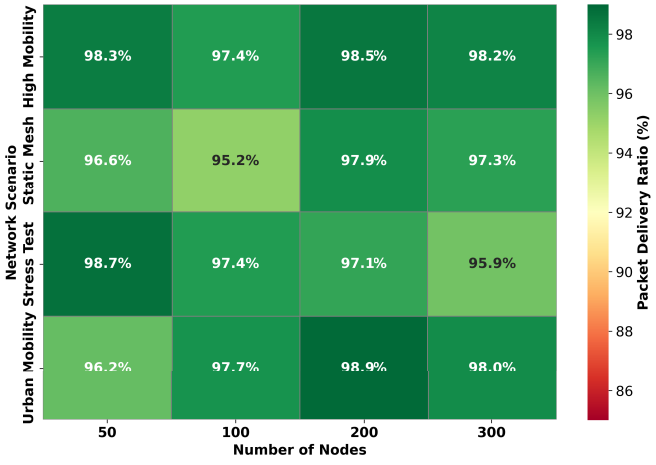

Fig. 10. PDR heatmap across scenarios. PoR consistently delivers 95%–99% PDR across all scenarios and scales, demonstrating robustness against topology churn and stress conditions.

can afford to execute costly consensus tasks. In addition, the system-wide trust and liveness are preserved.

Fig. 5 shows the latency distribution highlighting how PoR adapts under diverse conditions. The average latency varied from 38.8 ms in urban mobility scenarios to 59.4 ms under stress testing. This variation is consistent with the expected increase in processing time under heavier routing and transaction loads. However, it remains within the requirements for IoT-grade connectivity in 6G environments. Importantly, PoR maintained sub-60 ms latencies across all scenarios, confirming its suitability for high-mobility NTN segments, where traditional routing stacks such as OSPF or BGP experience slow convergence.

The mobility impact analysis in Fig. 6 confirms that despite significant variations in node velocity, the number of blocks committed remains consistently near 985, and the average number of routes per node stays close to 30 routes per node. This consistency demonstrates the robustness of the PoR protocol in maintaining ledger integrity and routing stability across diverse TN–NTN mobility conditions, including high-speed satellite scenarios.

The reliability analysis in Fig. 7 demonstrates the stability of PoR relative to conventional protocols. The PDR for blockchain-based routing, which is the proposed PoR framework, consistently clustered above 97%, with narrow variance across trials. By contrast, AODV, OLSR, and DSR showed broader dispersions, often falling below 90% in dynamic conditions. This outcome validates PoR's cryptographic route authentication and adaptive validator management, which jointly mitigate disruptions such as route replay and Sybil-like inconsistencies. The results reinforce that deterministic consensus-driven routing provides a stronger foundation for reliability than heuristic-based neighbor discovery.

Fig. 8 compares throughput scaling across node counts for blockchain and classical MANET protocols. PoR demonstrates sustained throughput up to 300 nodes, while competing protocols exhibited noticeable fluctuations. For instance, DSR peaked at *200 nodes* but deteriorated as density increased, reflecting scalability limitations. PoR's performance stability arises from its event-driven design. The AutoProposer ensures that route updates are rapidly proposed under heavy load, while Smart AutoMining avoids unnecessary empty block generation, preventing throughput degradation in idle phases. These design choices directly address the tradeoffs between responsiveness and efficiency that define hybrid TN–NTN routing.

The scalability behavior of the PoR protocol demonstrates that as network size increases from 50 to 150 nodes, the number of blocks committed scales linearly with node count, confirming efficient ledger maintenance even in dense deployments. Meanwhile, the end-to-end latency increases moderately by 5 ms for every additional 50 nodes, demonstrating the protocol's ability to maintain low latency and high performance. PoR sustains 99% PDR across all scales, validating its robustness for large-scale TN–NTN environments.

In Table I, the control overhead comparison across three representative protocols is presented: AODV, OLSR, and the proposed PoR. N denotes the network diameter, which governs the extent of route request (RREQ) flooding, whereas V represents the number of validator nodes involved in the consensus. Since AODV is a reactive protocol, it incurs control overhead each time a route is needed, comprising N broadcast RREQ messages and a single unicast route reply (RREP), resulting in a total overhead of $N + 1$ messages.

OLSR, being proactive, maintains continuously updated routing information and, therefore, does not require route discovery messages. Its control overhead is limited to periodic topology updates, optimized to $N/2$ messages through the use of multipoint relay (MPR) techniques. This corresponds to a 50% reduction in control overhead relative to AODV. The proposed PoR protocol retains the same reactive route discovery cost as AODV but introduces an additional 2 V messages to facilitate secure, consensus-based validation and immutable route recording on the blockchain.

Consequently, the total overhead in PoR amounts to N + 1 + 2 V messages, reflecting a marginal increase due to the integrated security mechanism. However, this is only an up-front cost necessary for route establishment and not a recurring ***cost per data packet***. Once a route has been successfully validated through consensus and its record is stored immutably on the blockchain, data forwarding proceeds without incurring further consensus overhead.

Fig. 9 highlights the scalability behavior of the PoR protocol as network size increases from 50 to 150 nodes. The number of blocks committed scales linearly with node count, confirming efficient ledger maintenance even in dense deployments. Meanwhile, the end-to-end latency increases moderately—by 5 ms for every additional 50 nodes—demonstrating the protocol's ability to maintain low latency and high performance. The PoR design sustains over 98% PDR across all scales as expounded in Fig. 10, validating its robustness for large-scale TN–NTN environments.

The heatmap in Fig. 10 summarizes PoR's packet delivery performance across scenarios and scales. Delivery ratios consistently remained above 95%, with averages near 97%–98% even in high-mobility and stress-test environments. These findings confirm that PoR's consensus-driven routing is robust to topology churn, node heterogeneity, and scaling to hundreds of participants. Maintaining stability across such conditions is critical for 6G IoT deployments, which must operate seamlessly under satellite handovers, UAV mobility, and dense terrestrial segments.

Collectively, the results demonstrate that PoR delivers on three fronts critical to TN–NTN integration.

1) *Security and Trust:* By embedding route authentication and validator accountability directly into the consensus process, PoR eliminates vulnerabilities inherent in IP-based discovery. Its cryptographic structure using wallet-derived keys and digital signatures creates a verifiable audit trail that defends against blackhole, Sybil, wormhole, and eclipse attacks.
2) *Energy Efficiency:* Through on-demand consensus, AutoProposer-triggered block creation, and Smart AutoMining that suppresses empty blocks, PoR minimizes unnecessary computation and messaging. These design choices significantly reduce energy overhead for constrained IoT devices, enhancing sustainability in 6G TN–NTN environments.
3) *Scalability:* Performance metrics remain stable as the system scales to hundreds of nodes, validating the design for massive 6G IoT ecosystems.

TABLE I
CONTROL OVERHEAD COMPARISON

Field	AODV	OLSR	PoR (ours)
RREQ	N	0	N
RREP	1	0	1
Consensus	0	N/2	$2V$
Total	N+1	N/2	N+1+$2V$
Overhead vs AODV	baseline	-50%	+$2V$ messages

4) *Mobility Awareness:* Unlike static routing stacks, PoR adapts seamlessly under high mobility and stress conditions, sustaining reliability and throughput without destabilizing the ledger.

These outcomes substantiate PoR's claim as a lightweight, secure, and mobility-aware routing protocol. While additional evaluation under real-world NTN conditions remains an avenue for future exploration, the presented results provide a strong foundation, demonstrating that PoR is not only theoretically sound but also empirically validated under diverse simulated TN–NTN environments.

A. Limitations and Future Work

While the presented evaluation demonstrates the robustness of PoR across diverse simulated TN–NTN scenarios, it is important to acknowledge its current limitations. The experiments were conducted within controlled simulations and containerized environments with up to 500 nodes. Although this setup is sufficient to reveal clear trends, it does not fully capture the complexities of real-world NTN scenarios, such as orbital dynamics, atmospheric interference, or multioperator trust fragmentation. Similarly, PoA^2's adaptive validator rotation, while effective for decentralization and resilience, introduces coordination overhead that could impact latency at very large scales. Extending the evaluation to hardware-in-the-loop testbeds, satellite emulators, and hierarchical validator clustering will be crucial for further validating scalability in million-node 6G IoT ecosystems.

In addition, trust assumptions rely on preregistered validators, which should be service providers, which may be relaxed in more open deployments through dynamic reputation scoring or cross-domain trust frameworks. Finally, while AutoProposer and Smart AutoMining reduce unnecessary block generation, energy optimization for ultraconstrained IoT devices remains an open area for exploration. Here, hardware-assisted cryptography, adaptive energy-aware consensus, and lightweight zero-knowledge proofs could further enhance sustainability alongside the use of AI in the consensus. Collectively, these avenues represent a clear roadmap for extending PoR from a validated prototype to a fully deployable, real-world 6G routing infrastructure.

B. Comparison Table

Table II compares the proposed PoR protocol with recent blockchain-based frameworks. Most existing lightweight and hybrid consensus mechanisms, like Proof-of-Resource,

TABLE II

COMPARATIVE ANALYSIS OF POR AND RECENT BLOCKCHAIN-BASED [✓-PRESENT, ✗-ABSENT, AND ◆-PARTIALLY]

Feature	PoR (This Work)	Proof-of-Resource [19]	HyPoPE [20]	LIGHT-SB [21]	PoEWAL [22]	Proof-of-Reputation [30]	Mohan et al. [23]
Mobility-aware routing	✓	✗	✗	✗	✗	✗	✗
Hybrid TN–NTN validation	✓	✗	✗	✗	✗	✗	✗
Energy efficiency focus	✓	✓	✓	✓	✓	✗	✓
Smart contract benchmarking	✓	✗	✗	✗	✗	✗	✗
Simulation validation	✓	✓	✓	✓	✓	◆	✓
Routing-specific security	✓	✗	✗	✗	✗	◆	✗
Scalability focus	✓	✓	✓	✓	◆	◆	◆
Privacy enhancements	◆	✗	✗	✗	✗	✗	✓
Reputation/trust integration	✓	✗	✗	✗	✗	✓	✗

HyPoPE, LIGHT-SB, and PoEWAL, focus on energy efficiency but provide limited support for mobility-aware routing or hybrid TN–NTN validation. Proof-of-Reputation integrates trust metrics for Sybil resistance but lacks routing resilience in dynamic IoT networks. Privacy-centric approaches like Mohan et al. [23] advance lightweight NB-IoT security through zero-knowledge proofs but do not address NTN handovers.

PoR uniquely combines mobility-aware routing, hybrid TN–NTN validation, and testbed experiments, embedding routing logic in consensus to fill gaps in previous studies. It incorporates routing-specific security against black hole, wormhole, Sybil, and eclipse attacks, while supporting validator trust through PoA^2 rotation. This balance of efficiency and resilience demonstrates PoR's suitability for 6G IoT environments integrating terrestrial and nonterrestrial resources.

V. CONCLUSION

The convergence of TNs and NTNs in 6G presents both extraordinary opportunities and unprecedented routing challenges. The PoR framework proposed in this study demonstrates that blockchain-enabled routing, when paired with adaptive validator rotation and cryptographic key-pair addressing, can deliver a secure, scalable, and mobility-aware foundation for hybrid 6G IoT ecosystems. By embedding authentication and integrity directly into each routing hop and leveraging event-driven consensus mechanisms such as AutoProposer and Smart AutoMining, PoR eliminates many of the vulnerabilities that constrain legacy IP-based and MANET-style protocols while ensuring deterministic and auditable routing performance.

Comprehensive simulations across diverse scenarios—including static mesh, high mobility, urban density, stress, partition, and TN–NTN handover—confirm that PoR sustains low latency (averaging 42.3 ms), high PDRs (96%–98%), and stable throughput as networks scale to hundreds of nodes. The framework achieves these gains without imposing prohibitive resource costs, making it well-suited to IoT devices operating in constrained environments. While throughput is lower than certain specialized alternatives such as PoH, PoR balances efficiency with reliability, offering resilience in scenarios where mobility, heterogeneity, and intermittent connectivity dominate. Taken together, the results establish PoR as a deployable candidate for secure and scalable routing in next-generation 6G systems. Building on this foundation, future research will extend evaluation into real-world NTN testbeds, integrate energy-aware cryptographic optimizations, and explore synergies with AI-driven routing intelligence to further enhance responsiveness under ultradynamic conditions.

REFERENCES

[1] J. Navisa, W. Mwangi, and R. Rimiru, "The impact of 6g-iot technologies on the development of smart applications," *Electronics*, vol. 12, no. 12, p. 2651, 2023.

[2] F. Aktas et al., "Routing challenges and enabling technologies for 6G–satellite network integration: Toward seamless global connectivity," *Technologies*, vol. 13, no. 6, p. 245, Jun. 2025.

[3] M. Giordani and M. Zorzi, "Non-terrestrial networks in the 6G era: Challenges and opportunities," *IEEE Netw.*, vol. 35, no. 2, pp. 244–251, Mar. 2021.

[4] M. Vaezi et al., "Cellular, wide-area, and non-terrestrial IoT: A survey on 5G advances and the road toward 6G," *IEEE Commun. Surv. Tut.*, vol. 24, no. 2, pp. 1117–1174, 2nd Quart., 2022.

[5] A. Ferenczi and C. Bădică, "Optimization of IOTA tangle cumulative weight calculation using depth-first and iterative deepening search algorithms," *Vietnam J. Comput. Sci.*, vol. 1, no. 2, pp. 301–321, 2024, doi: 10.1142/S2196888824500027.

[6] Y. Liu, S. Peng, M. Zhang, S. Shi, and J. Fu, "Towards secure and efficient integration of blockchain and 6G networks," *PLoS ONE*, vol. 19, no. 4, Apr. 2024, Art. no. e0302052.

[7] J. Zhang, S. Zhong, T. Wang, H. Chao, and J. Wang, "Blockchain-based systems and applications: A survey," *J. Internet Technol.*, vol. 21, no. 1, pp. 1–14, 2020.

[8] W. Zhang, Y. Chen, Y. Chen, L. Jie, and Z. Liu, "A smart energy IoT model based on the itsuku PoW technology," *Results Eng.*, vol. 18, Jun. 2023, Art. no. 101147.

[9] M. Simeonova and C. Bădică, "Optimization of IOTA tangle cumulative weight calculation using depth-first and iterative deepening search algorithms," *J. Blockchain Res.*, vol. 1, no. 1, pp. 301–321, 2024.

[10] I. Ullah, G. de Roode, N. Meratnia, and P. Havinga, "Threat modeling—How to visualize attacks on IOTA?," *Sensors*, vol. 21, no. 5, 2021, Art. no. 1834, doi: 10.3390/s21051834.

[11] S. Baldi et al., "A contemporary survey on ai-empowered satellite-based non-terrestrial networks," 2022, *arXiv:2303.01633*.

[12] A. I. Abdi et al., "Hierarchical blockchain-based multi-chaincode access control for securing IoT systems," *Electronics*, vol. 11, no. 5, p. 711, Feb. 2022.

[13] A. Voudouris, A. Farao, A. Panou, J. Polley, and C. Xenakis, *Integrating Hyperledger Fabric with Satellite Communications: A RevolutionaryApproach for Enhanced Security and Decentralization in Space Networks*. New York, NY, USA: Association for Computing Machinery, 2024, doi: 10.1145/3664476.3669921.

[14] K. M. B. Hasan, M. Sajid, M. A. Lapina, M. Shahid, and K. Kotecha, "Blockchain technology meets 6G wireless networks: A systematic survey," *Alexandria Eng. J.*, vol. 92, pp. 199–220, Apr. 2024.

[15] J. Wang, X. Ling, Y. Le, Y. Huang, and X. You, "Blockchain-enabled wireless communications: A new paradigm towards 6g," *Nat. Sci. Rev.*, vol. 8, no. 9, 2020, Art. no. nwab069, doi: 10.1093/nsr/nwab069.
[16] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "The blockchain Internet of Things: Review, opportunities, challenges, and recommendations," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 31, no. 3, p. 1673, Sep. 2023.
[17] X. Fan, Q. Chai, L. Xu, and D. Liu, "A blockchain protocol for authenticating space communications," *Aerospace*, vol. 9, no. 9, p. 495, 2020.
[18] H. Wei, W. Feng, C. Zhang, Y. Chen, Y. Fang, and N. Ge, "Creating efficient blockchains for the Internet of Things by coordinated satellite-terrestrial networks," *IEEE Wireless Commun.*, vol. 27, no. 3, pp. 104–110, Jun. 2020.
[19] M. Abbasi, J. Prieto, M. Plaza-Hernandez, and J. Manuel Corchado, "Proof-of-resource: A resource-efficient consensus mechanism for IoT devices in blockchain networks," *EAI Endorsed Trans. Internet Things*, vol. 10, Jul. 2024, doi: 10.4108/eetiot.6565.
[20] A. A. Das and G. Srivastava, "HyPoPE: A hybrid proof of participation and efficiency protocol for secure IoT blockchain networks," in *Proc. 40th ACM/SIGAPP Symp. Appl. Comput.*, Mar. 2025, pp. 2017–2023.
[21] S. A. M. Uveise and S. M. H. S. S. Fathima, "Efficient lightweight blockchain with hybridized consensus algorithm for IoT networks," *IETE J. Res.*, vol. 70, no. 12, pp. 8527–8537, Dec. 2024.
[22] N. Andola, S. Venkatesan, and S. Verma, "PoEWAL: A lightweight consensus mechanism for blockchain in IoT," *Pervas. Mobile Comput.*, vol. 69, Nov. 2020, Art. no. 101291.
[23] V. S. Mohan, S. Sankaran, P. Nanda, and K. Achuthan, "Enabling secure lightweight mobile narrowband Internet of Things (NB-IoT) applications using blockchain," *J. Netw. Comput. Appl.*, vol. 219, Oct. 2023, Art. no. 103723.
[24] A. P. Delladetsimas, S. Papangelou, E. Iosif, and G. Giaglis, "Integrating blockchains with the IoT: A review of architectures and marine use cases," *Computers*, vol. 13, no. 12, p. 329, Dec. 2024.
[25] C. Zehir and M. Zehir, "Emerging blockchain solutions in the mobility ecosystem: Associated risks and areas for applications," *Bussecon Rev. Social Sci.*, vol. 4, no. 2, pp. 01–14, Jan. 2023.
[26] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K.-R. Choo, "An energy-efficient SDN controller architecture for IoT networks with blockchain-based security," *IEEE Trans. Services Comput.*, vol. 13, no. 4, pp. 625–638, Jul. 2020.
[27] Y. Maadallah, Y. El Bouzekri El Idrissi, and Y. Baddi, "Enhancing IoT security through blockchain an in-depth analysis of the proof-of-work consensus mechanism," *EDPACS*, vol. 70, no. 5, pp. 1–44, May 2025.
[28] S. Maitra, V. P. Yanambaka, D. Puthal, A. Abdelgawad, and K. Yelamarthi, "Integration of Internet of Things and blockchain toward portability and low-energy consumption," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 6, p. 4103, Jun. 2021.
[29] W. Yan, N. Zhang, L. L. Njilla, and X. Zhang, "PCBChain: Lightweight reconfigurable blockchain primitives for secure IoT applications," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 10, pp. 2196–2209, Oct. 2020.
[30] F. Gai, B. Wang, W. Deng, and W. Peng, "Proof of reputation: A reputation-based consensus protocol for peer-to-peer network," in *Proc. 23rd Int. Conf. Database Syst. Adv. Appl.*, 2018, pp. 666–681.

Jonathan Mukisa Kalibbala received the B.Sc. degree in computer engineering from Kyungdong University, Yangju, South Korea, in 2023. He is currently pursuing the master's degree in IT-convergence engineering with the Networked Systems Laboratory, Kumoh National Institute of Technology, Gumi, South Korea.

He currently collaborates with Otic-Uganda, Kampala, Uganda. His interdisciplinary research covers blockchain-based offline transactions, NFT-enabled inventory management, simulated islanded microgrids, federated demand forecasting with Byzantine-resilient aggregation, TRIZ-inspired compression for large language models, and multilingual AI educational platforms, focused on securing decentralized systems, optimizing energy/data workflows, and enabling scalable personalized learning.

Love Allen Chijioke Ahakonye (Member, IEEE) received the B.Sc. degree in mathematics/computer science from the University of Port Harcourt, Port Harcourt, Nigeria, in 2001, the M.Sc. degree in information technology from the Federal University of Technology, Gaga, Nigeria, in 2016, and the Ph.D. degree in IT-convergence engineering from the Networked System Laboratory, Department of IT-Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea, in 2024.

She has over a decade of experience in the Nigerian oil and gas sector as a Network and System Administrator from 2002 to 2016. In 2017, she briefly worked as a Logistics Superintendent with Nigerian Petroleum Development Company, Benin, Nigeria, until 2019. She is currently a Post-Doctoral Researcher at the ICT Convergence Research Center (ICT-CRC), Kumoh National Institute of Technology. Her research interests include artificial intelligence (AI) applications to the Internet of Things (IoT) and industrial IoT, supervisory control and data acquisition (SCADA) and industrial control systems (ICSs) for intrusion/anomaly detection, cybersecurity, fault detection, XAI, and manufacturing execution systems.

Dr. Ahakonye is a member of the Computer Professionals Registration Council of Nigeria (CPN).

Dong-Seong Kim (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2003.

From 1994 to 2003, he worked as a full-time Researcher at ERC-ACI, Seoul National University, Seoul. From March 2003 to February 2005, he was a Post-Doctoral Researcher at the Wireless Network Laboratory, School of Electrical and Computer Engineering, Cornell University, Ithaca, NY, USA. From 2007 to 2009, he was a Visiting Professor with the Department of Computer Science, University of California, Davis, Davis, CA, USA. He was the Dean of IACF from 2019 to 2022. He is currently a Professor at the Department of IT Convergence Engineering, School of Electronic Engineering, Kumoh National Institute of Technology, Gumi, South Korea. He is also the Director of the KIT Convergence Research Institute and the ICT Convergence Research Center (ITRC and NRF Advanced Research Center Program) supported by Korean Government at the Kumoh National Institute of Technology and the Director of NSLab, Gumi. His primary research interests include the real-time IoT and smart platforms, industrial wireless control networks, networked embedded systems, fieldbus, metaverse, and blockchain.

Dr. Kim is a Senior Member of ACM.

Jae-Min Lee (Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2005.

From 2005 to 2014, he was a Senior Engineer at Samsung Electronics, Suwon, South Korea. From 2015 to 2016, he was a Principal Engineer at Samsung Electronics. Since 2017, he has been an Associate Professor with the School of Electronic Engineering and the Department of IT Convergence Engineering at the Kumoh National Institute of Technology, Gyeongbuk, South Korea. Since 2024, he has been the Director of the Smart Defense Logistics Innovation Convergence Research Center (ITRC Program), Gumi, South Korea. He is currently the Executive Director of Korean Institute of Communications and Information Sciences (KICS), Seoul. His current main research interests include smart IoT convergence applications, industrial wireless control networks, UAVs, the metaverse, and blockchain.