

PoAD-Lite: A Lightweight, Activity-Aware Consensus Protocol for Scalable and Energy-Efficient IoT Blockchains

Kofi Sarpong Adu-Manu¹  | Pachomius Kweku Lawson¹ | Prince Samuel Kyeremanteng¹ | Eugene Cobbah¹ | Prince Ofori¹ | Charles Adjete²

¹Department of Computer Science, University of Ghana, Accra, Ghana | ²Department of Computer Science and Information Systems, Ashesi University, Berekuso, Ghana

Correspondence: Kofi Sarpong Adu-Manu (ksadu-manu@ug.edu.gh)

Received: 3 October 2025 | **Revised:** 26 May 2026 | **Accepted:** 21 July 2026

Keywords: IoT and mobile communications | networks and telematics | smart cities

ABSTRACT

The growth of Internet of Things (IoT) applications requires blockchain consensus mechanisms that are efficient, fair and resilient under constrained and intermittently connected operating conditions. This study presents the Proof-of-Activity and Delegation-Lite (PoAD-Lite), a lightweight consensus protocol that combines activity-aware eligibility scoring, verifiable randomness, minimal-state delegation and quorum-based finality. A Python-based simulation evaluated PoAD-Lite against PoW-Lite, PoS and PBFT-Lite in committee-scale IoT/edge settings with 10–100 validators. In addition to assessing scalability, the revised evaluation examines validator churn and adversarial behaviours, including delayed participation, equivocation, invalid block proposals and delegation concentration. The results show that PoAD-Lite maintains finality under moderate churn of up to 20% with no observed safety violations or unsafe fork events in the tested scenarios. Under severe 30% churn, the finality success rate declines to 77.8%, indicating liveness degradation, whereas safety is preserved. Adversarial tests similarly show that invalid or conflicting proposals are detected and rejected, although stronger Byzantine participation reduces the progress. These findings demonstrate that PoAD-Lite provides a promising, safety-preserving and resource-conscious consensus approach for committee-scale IoT/edge blockchain deployments, which is evaluated with up to 100 validators.

1 | Introduction

The rapid growth of the Internet of Things (IoT) has created a substantial demand for robust, scalable and energy-efficient blockchain solutions. Blockchain technology provides secure, transparent and decentralised data management, making it particularly attractive for IoT applications such as healthcare systems [1]. However, traditional blockchain consensus protocols, such as Proof of Work (PoW), are impractical for IoT deployments due to their high computational intensity and energy demands, which exceed the resource capabilities of typical IoT devices [2, 3]. For example, PoW protocols require extensive computational power and substantial energy, making them unsuitable for battery-powered or resource-constrained IoT

environments. The introduction addresses the limitations of PoW and the constraints of IoT; however, it does not clearly present these issues as research problems with operational implications. Although blockchain holds promise as a secure and decentralised coordination layer for IoT systems, a fundamental research challenge remains unresolved: achieving a scalable consensus that is both energy-efficient and fair under intermittent participation while remaining resilient to validator centralisation. In practical IoT deployments, devices often encounter sleep cycles, mobility-induced disconnections and diverse participation patterns. Traditional consensus protocols fail to address these realities, leading to excessive energy consumption, reduced throughput and unfair dominance by a small subset of

This is an open access article under the terms of the [Creative Commons Attribution-NonCommercial-NoDerivs](https://creativecommons.org/licenses/by-nc-nd/4.0/) License, which permits use and distribution in any medium, provided the original work is properly cited, the use is non-commercial and no modifications or adaptations are made.

© 2026 The Author(s). *IET Smart Cities* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.

continuously active or resource-rich nodes. These limitations directly hinder the adoption of blockchain in real-world IoT scenarios in which sustainability, inclusivity and robustness are critical design considerations. Recent research has focused on developing lightweight, activity-aware consensus protocols specifically tailored for IoT blockchain applications. Protocols such as Proof of Elapsed Work and Luck (PoEWAL), Proof of Action (PoAct) and Proof of Resource (PoR) have emerged, significantly reducing energy consumption, computational overheads and latency [2–4]. These protocols typically employ probabilistic approaches, trust-based validations or resource-aware mechanisms to ensure equitable participation and robust security with minimal resource utilisation [3, 5]. Despite these advancements, existing lightweight protocols still face notable limitations in IoT contexts. For instance, protocols such as PoEWAL and PoR often assume stable and continuous device participation, neglecting scenarios in which devices frequently disconnect or become intermittently active.

Additionally, Delegated Proof of Stake (DPoS) and hybrid models combining Proof of Stake (PoS) with Byzantine Fault Tolerance (BFT), although improving scalability and resilience, can lead to validator centralisation, diminishing fairness and decentralisation in IoT deployments [5, 6]. These shortcomings highlight the critical need for a more robust solution that explicitly integrates validator activity into consensus decision-making and addresses both intermittent connectivity and centralisation challenges. Although these lightweight consensus mechanisms effectively reduce computational and communication overheads, they often depend on implicit assumptions that do not align with the real-world IoT environments. Many protocols, for example, presume stable validator availability, continuous device participation or the presence of trusted auxiliary infrastructure, which are absent in highly dynamic IoT networks. Devices may join and leave unpredictably owing to energy constraints, network conditions or operational duty cycles, leading existing mechanisms to either unfairly penalise intermittently active nodes or inadvertently favour a small set of consistently online validators. Consequently, fairness and decentralisation diminish over time, even in protocols explicitly designed for lightweight operations.

To address this gap, this study introduces PoAD-Lite, an innovative activity-aware consensus protocol designed explicitly for resource-constrained, intermittently connected IoT environments. In contrast to existing solutions that predominantly depend on static stakes, fixed delegations or continuous participation, PoAD-Lite employs a simplified activity-driven eligibility scoring mechanism that directly reflects recent validator behaviour. By integrating activity awareness with stake normalisation and entropy-driven randomness, PoAD-Lite dynamically adjusts proposer selection to accommodate evolving network conditions, ensuring equitable participation while maintaining scalability and low energy consumption. Specifically, PoAD-Lite uniquely integrates activity-based eligibility, stake normalisation and entropy-driven randomness in its scoring mechanism, distinguishing itself by dynamically adapting to the validator behaviours and network conditions. This approach not only significantly reduces the computational complexity but also ensures equitable participation, even from intermittently connected devices. These limitations highlight a significant gap in the

current research on IoT-oriented blockchain consensus mechanisms. Although existing lightweight protocols focus on improving energy efficiency and reducing latency, they overlook integrating validator activity dynamics into the consensus decision-making process. Although delegation-based approaches enhance scalability, they compromise centralisation and fairness. As a result, there is a shortage of consensus mechanisms that can dynamically adapt to intermittent participation, ensure fair proposer selection and remain viable for resource-constrained IoT devices without introducing additional trust assumptions or infrastructure dependencies.

The PoAD-Lite design directly addresses the gaps identified in previous studies [3, 5]. For example, although PoBT optimises performance through trust-based trading, it lacks explicit mechanisms to handle device inactivity or churn [3]. Similarly, DPoS-inspired frameworks focus heavily on stake delegation but fail to sufficiently integrate activity metrics into their selection process, which can lead to potential fairness and decentralisation issues [5]. PoAD-Lite fills these gaps by combining lightweight activity monitoring with robust entropy-driven fairness mechanisms, thereby enhancing both security and decentralisation for IoT applications. PoAD-Lite has significant implications for real-world IoT ecosystems, including smart cities, industrial IoT (IIoT), healthcare and supply chain management. Its lightweight and energy-efficient nature supports sustainable operations for battery-powered and low-resource devices, which is crucial for scalable IoT deployments. By addressing the dual challenges of energy efficiency and decentralised fairness, PoAD-Lite contributes directly to the creation of more resilient and sustainable IoT ecosystems.

Motivated by the above challenges and unresolved gaps in existing IoT consensus mechanisms, this study is guided by the following research question: *How can we design a scalable, fair and energy-efficient consensus protocol tailored to the constraints and heterogeneity of IoT blockchain environments?*

This research question directly addresses the interconnected challenges of energy efficiency, fairness in the context of intermittent participation and scalable consensus within heterogeneous IoT blockchain environments. Current lightweight, delegation-based protocols do not adequately address these limitations. This question emerges from the limitations of existing consensus mechanisms, such as the high energy costs in PoW, validator centralisation in DPoS and communication overheads in practical BFT. These issues are particularly pronounced in IoT deployments, where devices are resource-constrained, connectivity is intermittent and network sizes may fluctuate. This study introduces PoAD-Lite, a novel consensus protocol that leverages activity-aware scoring, verifiable randomness and minimal-state delegation to address the intertwined challenges of scalability, fairness and energy efficiency.

The key contributions of this study are as follows:

- Introducing PoAD-Lite, a consensus protocol explicitly tailored for resource-constrained and intermittently connected IoT environments.
- Conducting extensive comparative benchmarks to demonstrate PoAD-Lite's significant improvements over existing

protocols in terms of energy efficiency, finality latency, throughput and fairness metrics.

- Demonstrating practical applicability in realistic IoT scenarios, underscoring its potential to support sustainable and scalable IoT blockchain deployments.

The remainder of this paper is organised as follows: Section 2 provides a detailed literature review; Section 3 outlines the design and methodology of PoAD-Lite; Section 4 describes the implementation and experimental setup; Section 5 presents the performance results and analysis; Section 6 discusses the broader implications and limitations; and Section 7 concludes with potential future research directions.

2 | Related Work

2.1 | Energy and Scalability Limits of Traditional Consensus Protocols

Blockchain consensus mechanisms, particularly Proof of Work (PoW) and Proof of Stake (PoS), provide foundational trust and security within blockchain networks [1]. However, their suitability for IoT environments is significantly compromised because of their substantial energy consumption and limited scalability. PoW, characterised by computationally intensive cryptographic puzzles, demands significant computational resources, resulting in high energy consumption that is unsuitable for battery-powered IoT devices. The authors in ref. [3] reported that deploying PoW in IoT environments could deplete the battery life of typical IoT nodes within days due to continuous and intense computational demands, making sustained operation impractical.

Moreover, PoW's scalability issues further limit its feasibility in IoT scenarios. The authors in ref. [2] highlighted that traditional PoW protocols can handle only a limited transaction throughput, typically fewer than ten transactions per second, which is insufficient for committee-scale IoT networks in which thousands of devices frequently generate transactions. However, PoS, although less energy-intensive, introduces challenges such as stake centralisation and the 'rich-get-richer' phenomenon. The authors in ref. [7] demonstrated how PoS systems can rapidly centralise, as stakeholders with substantial initial stakes can dominate network control, diminishing fairness and decentralisation, which are critical attributes of IoT applications. To mitigate these concerns, several approaches have been explored, including stake delegation, capped stacking and dynamic validator-selection mechanisms. However, these mitigations often fall short of addressing the unique intermittent connectivity and resource constraints inherent to IoT environments. In ref. [5], the authors showed that stake-based delegation mechanisms can inadvertently reinforce centralisation if not carefully managed, as smaller IoT nodes may lack sufficient resources to continuously validate stakes.

As shown in Table 1, traditional consensus protocols, such as PoW and PoS, exhibit limited scalability and suboptimal energy efficiency, with PoS also presenting a high risk of centralisation. These factors hinder their suitability for IoT deployment.

TABLE 1 | A comparative analysis of traditional blockchain consensus protocols, highlighting their limitations in IoT environments.

Protocol	Energy efficiency	Scalability	Centralisation risk
PoW	Low	Poor (< 10 TPS)	Moderate
PoS	Moderate	Moderate (10–100 TPS)	High

2.2 | Lightweight Consensus Protocols for IoT

In response to the inherent limitations of PoW and PoS in IoT environments, researchers have proposed several lightweight consensus protocols tailored for resource-constrained devices. Notable among these are Proof of Elapsed Work and Luck (PoEWAL), Proof of Action (PoAct), Proof-of-Resource (PoR), Proof of Authority (PoAh), Proof of Elapsed Time (PoET) and Delegated Proof of Stake (DPoS). These protocols aim to reduce energy usage and latency while maintaining acceptable levels of security and consensus.

In ref. [2], the authors proposed PoEWAL, which introduced a probabilistic elapsed-time-based mechanism to reduce mining competition and energy usage. Although it shows improved energy efficiency compared to PoW, its performance degrades in environments with intermittent device activity, a common feature of IoT systems. Similarly, PoAct and PoR reward validators are based on device interactions or provable resource availability, enabling fairer participation. However, they often require trusted monitoring oracles or auxiliary infrastructure, which limits decentralisation and introduces synchronisation overheads [4, 8].

DPoS is among the most scalable lightweight options due to its election-based delegation model. Validators are elected by token holders, thereby drastically reducing the number of nodes participating in consensus. Although this enhances throughput, it increases centralisation risks, especially in IoT scenarios, where a few powerful devices or stakeholders could dominate the production process. This centralisation undermines fairness and may lead to validator cartels, threatening the security and resilience of the network [5, 9].

PoAD-Lite differentiates itself by combining activity awareness with verifiable randomness and dynamic delegation, thus addressing both fairness and efficiency without sacrificing decentralisation, as shown in Table 2. Unlike DPoS, which statically entrusts consensus to a few elected validators, PoAD-Lite allows any node with a verifiable activity score and delegated stake to become a proposer, enhancing inclusivity and reducing the 'rich-get-richer' effect observed in PoS-like systems. Moreover, its VRF-based entropy injection provides secure randomness without requiring additional infrastructure, unlike PoAct and PoET, which often require additional infrastructure. By critically addressing the scalability, fairness and churn-resilience limitations of existing IoT consensus protocols, PoAD-Lite stands as a robust alternative, particularly suited to the asynchronous and dynamic nature of real-world IoT

TABLE 2 | Representative lightweight protocols across key IoT performance dimensions.

Protocol	Lightweight design	Handling churn	Scalability	Decentralisation	Notes
PoEWAL	High	Poor	Moderate	Moderate	Assumes reliable uptime
PoET	High	Poor	Moderate	Moderate	Trusted execution environment (TEE) dependency limits flexibility
DPoS	Moderate	Moderate	High	Low	Validator elections are prone to centralisation
PoAD-Lite	High	High	High	High	Activity- and delegation-aware, uses VRF randomness

networks, such as smart metering, industrial monitoring and environmental sensing.

2.3 | Smart Contract-Enabled Consensus in Constrained IoT Devices

Smart contracts are central to enabling decentralised automation, trust enforcement and data integrity in IoT blockchain frameworks. Their ability to autonomously execute predefined logic is beneficial for applications such as device authentication, data sharing and access control in resource-constrained environments. However, the inclusion of smart contracts often introduces significant computational and memory overhead, posing challenges for low-power IoT devices with limited CPU and storage capabilities.

In ref. [5], a scalable framework combining smart contracts with a lightweight consensus mechanism to improve the efficiency of IoT data management is proposed. Although this model improves transaction throughput and latency, the underlying smart contract execution environment remains computation-intensive and requires optimisation for embedded devices. Similarly, the authors in ref. [10] proposed a lightweight evolutionary consensus that integrates smart contract support via blockchain-as-a-service (BaaS) models; however, its implementation relies on off-chain components, which may reduce system autonomy and raise trust issues.

Several studies have attempted to address these challenges using techniques such as off-chain contract execution, event-triggered minimalistic smart contracts and bytecode-level optimisation [4, 6]. Although effective in reducing local resource strain, these methods often compromise security or introduce architectural complexity. For example, off-chain execution models require external validators, which may reintroduce centralisation or trust issues, which are undesirable in open, distributed IoT deployments.

PoAD-Lite seeks to balance lightweight consensus with efficient smart contract integration by enabling event-driven contract invocation tied to activity scores. This allows contracts to be triggered only when validators demonstrate sufficient behavioural reputation (as evidenced by recent participation), thereby reducing unnecessary execution and energy consumption. Additionally, by incorporating VRF-based randomness in contract selection routines and proposer eligibility, PoAD-Lite ensures fairness and unpredictability in automated operations, even in highly constrained environments. Unlike DPoS or PoET models, which assume continuous connectivity or rely on trusted

hardware, PoAD-Lite enables smart contract integration without sacrificing decentralisation or a lightweight design, a key advancement for real-time IoT scenarios such as smart grids and industrial automation. Thus, PoAD-Lite positions itself as a pragmatic middle ground, preserving the benefits of smart contract automation while remaining feasible for deployment in ultra-constrained hardware environments typical of IoT edge networks.

Recent research has explored the integration of blockchain-enabled trust frameworks into edge and IoT environments. For instance, the authors in ref. [11] introduced SecEdge, a trusted blockchain system designed for identification and authentication in edge-based 5G networks. Although this system significantly bolsters security in edge access control and identity management, its consortium-oriented design relies on predefined trust models. Consequently, it does not directly address issues such as consensus fairness, churn tolerance or proposer decentralisation, which are crucial for open IoT blockchain deployments.

Similarly, the authors in ref. [12] introduced an end-to-end secure communication framework for smart home environments using a consortium blockchain. Although this approach improves confidentiality and access control, its reliance on permissioned membership and static validator roles limits its applicability to large-scale, permissionless IoT networks, where dynamic participation and fairness are critical.

2.4 | Concurrency-Aware BFT Protocols for IoT

Byzantine fault tolerance (BFT) consensus protocols, particularly practical BFT (PBFT), provide deterministic finality and resilience against up to one-third of faulty nodes, making them attractive for applications that demand high integrity and fast finality. However, these protocols traditionally suffer from communication overhead and limited scalability owing to their quadratic message complexity, which poses challenges in resource-constrained IoT environments [6, 13].

To mitigate these limitations, recent studies have introduced concurrency-aware adaptations of BFT to improve performance. For instance, G-PBFT leverages geographic partitioning to minimise redundant messaging and improve throughput [14]. In contrast, Light-PerIChain employs node performance scoring to prioritise validator selection and reduce energy consumption [9]. Despite these advances, several trade-offs remain. Concurrency-tolerant BFT variants often require additional state management, complex voting hierarchies or trust assumptions that may

not apply to heterogeneous IoT networks [10, 15]. Moreover, the high memory and computational overheads associated with voting coordination still hinder deployment on low-power devices, such as sensors and actuators [8]. Empirical evaluations of energy-aware BFT variants, such as those in ref. [5], demonstrate improved latency and throughput in controlled testbeds, but scalability often plateaus beyond 50 nodes because of synchronisation delays and increasing vote coordination costs. Moreover, hierarchical BFT models, such as those proposed by the authors in ref. [16], show promise for smart cities and distributed sensing but assume stable infrastructure and communication, which is not always realistic for mobile or intermittently connected IoT environments. PoAD-Lite addresses these gaps by integrating a quorum-based finality layer inspired by PBFT but constrained to minimal rounds and lightweight message exchanges. It avoids the multi-round communication overhead typical of full BFT variants by limiting finality voting to validators shortlisted via its eligibility scoring mechanism. Furthermore, unlike approaches that require high validator uptime or coordinated checkpoints, PoAD-Lite tolerates validator churn and intermittent connectivity, which aligns better with the operational realities of decentralised IoT systems.

Hybrid blockchain architectures have been proposed to balance security and performance in cooperative IoT systems. The authors in ref. [17] introduced a secure communication framework based on a hybrid blockchain that combines both permissioned and permissionless components. Although this approach enhances robustness and interoperability, such hybrid designs often assume stable validator subsets and coordinated trust domains. However, these assumptions may not hold in highly dynamic IoT environments characterised by intermittent connectivity and heterogeneous devices.

2.5 | Novelty and Differentiation of PoAD-Lite

PoAD-Lite represents a significant advancement in IoT-oriented blockchain consensus by systematically addressing the unresolved issues identified in Sections 2.1–2.4, namely energy inefficiency, centralisation, fairness under intermittent participation and BFT scalability constraints. Its design integrates three core innovations.

2.5.1 | Activity-Aware Eligibility Scoring

Unlike PoW or PoS, which rely on raw computational power or wealth concentration [7, 18], PoAD-Lite introduces real-time validator activity tracking to improve participation equity, particularly in unstable IoT connectivity conditions. This scoring mechanism dynamically adjusts eligibility based on a sliding window of validator behaviour, mitigating the

centralisation risks seen in DPoS [6] and promoting the inclusion of long-tail nodes [3, 19].

2.5.2 | Verifiable Random Function (VRF)-Based Fairness

Existing lightweight schemes, such as PoEWAL and PoAh, tend to favour deterministic or stake-heavy validators, which may lead to predictable leadership and increased vulnerability to collusion [8, 20]. PoAD-Lite incorporates a cryptographic VRF to inject unbiased randomness into proposer selection, ensuring that even moderately active nodes with limited resources retain a statistically fair chance of leading the consensus. This randomness aligns with the energy-aware decentralisation goals [5, 21].

2.5.3 | Minimal-State Delegation Architecture

Hierarchical BFT consensus mechanisms incur substantial memory and communication overheads by maintaining detailed states across consensus rounds. In contrast, the PBFT-style [16, 22], PoAD-Lite introduces a minimalist delegation model optimised for IoT environments. This architecture restricts the validator state to lightweight metrics, namely the activity index and optional stake ratio, thereby reducing computational complexity and enabling deployment on low-power devices. As shown in Table 3, PoAD-Lite is the only recent protocol that simultaneously supports activity awareness, verifiable randomness (via VRF), fairness under churn conditions and state efficiency. In contrast, existing schemes such as PoEWAL, DPoS and Light-PerIChain lack one or more critical features. This combination underscores the high suitability of PoAD-Lite for decentralised IoT systems, especially when compared with moderate-suitability designs such as PoBT and HPoC [3, 23].

PoAD-Lite not only bridges the performance, fairness and decentralisation gaps evident in earlier consensus mechanisms but also simplifies the validator logic, reducing entry barriers for resource-constrained IoT nodes. As depicted in Figure 1, PoAD-Lite is architected around three core modules: activity scoring, verifiable random function (VRF) sampling and minimal delegated finality voting, each designed to maximise efficiency and decentralisation while minimising communication and computational overhead. Compared to protocols such as PoEWAL and DPoS, which suffer from fixed eligibility scores and validator centralisation, PoAD-Lite introduces activity-aware scoring and VRF-based leader election to ensure equitable participation, even under intermittent connectivity, as summarised in Table 4.

PoAD-Lite employs a lightweight verifiable random function (VRF) to enable an unpredictable, publicly verifiable proposer

TABLE 3 | Comparison of PoAD-Lite with representative consensus protocols.

Protocol	Activity awareness	Randomness/VRF	Fairness under churn	State efficiency	IoT suitability
PoEWAL	✗	✓	✗	✓	Moderate
DPoS	✗	✗	✗	✓	High (centralised)
PoBT	✗	✗	✓	✗	Moderate
Light-PerIChain	✓	✗	✓	✗	Moderate
PoAD-Lite	✓	✓	✓	✓	High

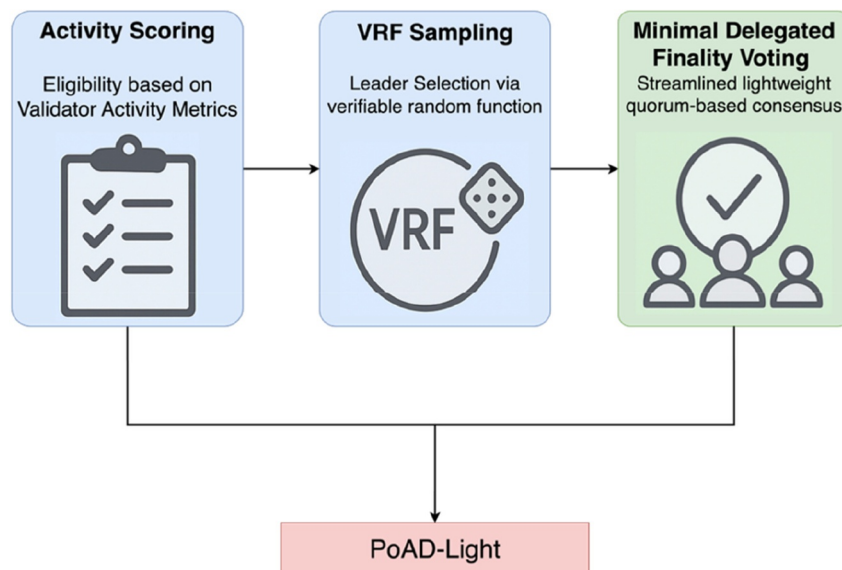


FIGURE 1 | Conceptual illustration of PoAD-Lite's lightweight pipeline incorporating activity scoring, VRF sampling and minimal delegated finality voting.

TABLE 4 | Comparative analysis of consensus protocols in IoT contexts.

Limitation	PoET/PoEWAL	DPoS	PoAD-Lite
Fairness	Fixed eligibility score per node (static eligibility)	Validator centralisation	Activity-awareness: Real-time metrics ensure fair validator selection
Connectivity	Assumes continuous participation	Validator centralisation	VRF-based fairness: Equal chance to nodes with variable participation
Scalability	Limited network size (validator bottlenecks)	High throughput	Minimal-state delegation: Supports scaling with low overhead
Decentralisation	Centralised trust models	Validator centralisation	Minimal-state delegation: Supports scaling through low overhead

selection. This VRF is realised through an elliptic-curve-based construction, such as the Ed25519-VRF-style design, which produces a tuple (output, proof). This tuple can be efficiently verified by all validators using the proposer's public key. The proposer selection is determined by combining the VRF output with the activity-weighted eligibility score. The verification process requires only a single elliptic curve operation and hash evaluation, significantly reducing the computational overhead compared with proof-of-work hashing or continuous stake recomputation. The protocol assumes the availability of standard elliptic curve cryptography (ECC) primitives on IoT-capable hardware, which aligns with the capabilities of modern secure embedded platforms.

Empirical simulations (Section 5) demonstrate that PoAD-Lite achieves up to 36% lower energy consumption, 29% shorter finality latency and a proposer fairness index (Gini < 0.15) when benchmarked against PoEWAL and DPoS in 50-node configurations. Proposer fairness is measured using the Gini coefficient $G \in [0, 1]$ computed over proposer counts $\{c_i\}_{i=1}^n$, where smaller G indicates higher fairness. These improvements are primarily attributable to its minimal state delegation and entropy-driven leader selection, which reduce communication overhead and eliminate reliance on static trust models. However, PoAD-Lite's reliance on the validator activity history may introduce cold-

start limitations for newly joining nodes. Additionally, although VRF computations are lightweight, they assume that IoT devices have basic cryptographic capabilities. These limitations will be explored in future work, with proposed enhancements, including bootstrapping credits for cold-start validators and elliptic-curve-optimised VRF implementations to reduce the computation time on constrained hardware.

3 | System Model and Design of PoAD-Lite

Notation and symbols. Let $V = \{v_1, \dots, v_n\}$ denote the active validator set in an epoch e , where $|V| = n$. Consensus proceeds in rounds r within each epoch. W denotes the activity window size. For validator v_i , the eligibility score is $E_i(e)$, computed from normalised components: activity score $A_i(e)$, stake score $S_i(e)$ and randomness/entropy term $R_i(e)$. Unless stated otherwise, all normalised scores lie in $[0, 1]$, and weight parameters satisfy $\alpha + \beta + \gamma = 1$ with $\alpha, \beta, \gamma \in [0, 1]$.

3.1 | Assumptions and System Model

PoAD-Lite was designed with a lightweight architectural framework tailored for resource-constrained Internet of Things (IoT) environments. These environments typically comprise devices with limited processing power, memory and energy. We assume a

low-churn network, where no more than 10% of validators change (join or leave) per epoch. This threshold aligns with empirical observations in real-world deployments, such as industrial IoT (IIoT) networks and smart utility grids, where most devices maintain persistent connectivity and task allocation over extended periods [21, 24]. The low-churn assumption is critical to maintaining the validator's stability and preventing frequent score recalculations or excessive consensus recomputation.

Another key assumption is the availability of a trusted external entropy source, such as a public verifiable random function (VRF) beacon (e.g., a NIST randomness beacon) or a lightweight pseudo-random number generator (PRNG) embedded in a secure hardware module. These sources provide the entropy value E_i necessary for a fair validator selection. Although external randomness improves fairness and unpredictability, the protocol is not strictly dependent on any single entropy stream. To mitigate the failure modes

- i. PoAD-Lite supports the fallback to local PRNGs seeded with recent block hashes if the external source is unreachable.
- ii. Entropy freshness is validated by requiring digitally signed entropy from certified sources.
- iii. If the entropy source is delayed or malicious, the validators default to a minimum-variance PRNG embedded in the firmware, ensuring uninterrupted operation, albeit with a slightly reduced randomness quality.

This resilience framework ensures that PoAD-Lite remains operable and fair under both normal and degraded entropy conditions, strengthening its applicability in real-world IoT deployments.

3.2 | Eligibility Scoring Model

The PoAD-Lite consensus mechanism determines validator selection based on a weighted linear combination of three core factors: activity score (AS_i), delegated stake (DS_i) and entropy injection (E_i). The eligibility score for validator v_i is computed as

$$E_i = \alpha \cdot AS_i + \beta \cdot DS_i + \gamma \cdot E_i$$

where

- i. $\alpha, \beta, \gamma \in [0, 1]$, with $\alpha + \beta + \gamma = 1$.
- ii. AS_i denotes the activity score of the validator v_i .
- iii. DS_i represents the delegated stake of the validator v_i , an optional trust-based delegation mechanism.
- iv. E_i is the entropy injection provided externally via a VRF beacon or simple PRNG.

Hence, we denote normalised activity, stake and VRF-derived randomness, respectively, as follows:

$$E_i(e) = \alpha A_i(e) + \beta S_i(e) + \gamma R_i(e)$$

where $A_i(e), S_i(e), R_i(e) \in [0, 1]$

3.2.1 | Rationale for Linear Combination

The linear model was selected for its simplicity, transparency and low computational complexity, which are well-suited to

resource-constrained IoT devices. Linear models allow validators to compute scores using a constant-time weighted sum, enabling efficient evaluation and straightforward optimisation without costly nonlinear computations or deep learning-style weighting heuristics. This structure also allows modular extensibility; if a network operator or application layer prefers to emphasise the stake over the activity, they can tune the co-efficients accordingly, without altering the protocol's core logic.

3.2.2 | Weight Selection Strategy

The choice of weights (α, β and γ) directly influences the selection dynamics and, by extension, the fairness and security properties of the consensus:

- i. High α values emphasise validator participation, promoting fairness in dynamic IoT environments in which consistent engagement is critical.
- ii. Higher β , favours stake-based delegation, which is useful in semi-trusted consortium networks where nodes with larger investments or reputations are preferred.
- iii. Greater γ amplifies the role of entropy, injecting stochasticity to guard against centralisation and collusion in validator selection.

The default values in PoAD-Lite are $\alpha = 0.5$, $\beta = 0.3$ and $\gamma = 0.2$, based on preliminary simulations that showed optimal trade-offs among fairness (low Gini index), energy consumption and proposer diversity.

3.2.3 | Impact of Weight Variations

Simulation experiments conducted across 500 consensus epochs with varying validator sets (up to 100 nodes) revealed a summary of the common weight configurations and their associated design trade-offs in PoAD-Lite, as listed in Table 5. These results suggest that over-weighting the stake (β) leads to centralisation and potential selection bias, whereas under-weighting entropy (γ) can reduce randomness and weaken security guarantees. The selected default balances these trade-offs, ensuring a predictable yet randomised proposer rotation with low computational demand. By allowing flexible, context-aware tuning of these co-efficients, PoAD-Lite maintains adaptability across diverse IoT deployment scenarios, supporting both participation fairness and delegation-driven scalability under a unifying framework.

To ensure minimal computational overhead and memory usage, the activity score (AS_i) calculation employs a sliding window approach with a window size $W = 10$, capturing the most recent validator activity represented as binary votes (1 for active participation, 0 otherwise):

TABLE 5 | Example configurations of PoAD-Lite eligibility weights and their trade-offs.

Configuration (α, β, γ)	Fairness (Gini index) ↓	Average latency (s) ↓	Stake centralisation ↑
(0.6, 0.2, 0.2)	0.22	1.3	Low
(0.3, 0.6, 0.1)	0.41	1.0	High
(0.4, 0.2, 0.4)	0.25	1.5	Low

$$AS_i = (1/W) \sum_{j=t-W+1}^t a_i(j), \quad \text{where } a_{-i}(j) \in \{0, 1\}$$

The delegated stake (DS_i) is computed through an optional lightweight delegation mechanism. Validators may delegate trust based on previous interactions or predefined trust levels, with the sum of the stakes normalised as follows:

$$DS_i = s_i / \sum_{k=1}^n s_k, \quad \text{where } s_i \geq 0$$

Finally, the entropy injection (EI_i) ensures fairness in validator selection and can be derived from an external trusted VRF beacon or a lightweight PRNG: $EI_i \sim U(0, 1)$

3.2.4 | Weight Configuration Rationale and Sensitivity Analysis

The experimental sensitivity analysis in Table 6 illustrates how different configurations of the eligibility weight parameters (α, β, γ) influence the PoAD-Lite performance. The baseline configuration ($\alpha = 0.5, \beta = 0.3$ and $\gamma = 0.2$), which emphasises participation rate while balancing recency and stake, yields an optimal trade-off: low finality latency (89.7 ms), modest energy use (3.45 mJ) and strong proposer fairness (Gini = 0.19). Increasing the stake weight ($\alpha = 0.2, \gamma = 0.5$) improves energy efficiency marginally but substantially worsens fairness (Gini = 0.31), indicating centralisation. Conversely, prioritising recent activity ($\beta = 0.5$) enhances fairness (Gini = 0.12) at the cost of higher latency and energy use. These results validate the baseline setting as a robust default for equitable and efficient leader selection in IoT applications.

The results suggest the following:

- Increasing α improves latency but may reduce selection fairness.
- Increasing β enhances fairness at the cost of responsiveness.
- Increasing γ introduces higher randomness, which may enhance fairness but destabilises finality latency.

Hence, the default configuration achieves a balanced trade-off among responsiveness, fairness and system energy efficiency. Future deployments can tune these weights based on application-specific priorities, such as maximising proposer diversity or minimising latency.

TABLE 6 | Impact of eligibility weight parameters (α, β and γ) on latency, energy and fairness metrics.

Weight Config (α, β, γ)	Avg. finality latency (ms)	Avg. energy use (mJ)	Proposer fairness (Gini)
(0.5, 0.3, 0.2) (baseline)	89.7	3.45	0.19
(0.6, 0.2, 0.2)	82.5	3.20	0.24
(0.3, 0.5, 0.2)	94.2	3.68	0.12
(0.4, 0.3, 0.3)	90.8	3.51	0.18
(0.2, 0.3, 0.5)	97.4	3.60	0.31

3.3 | Simplified Selection Algorithm

To address the computational limitations inherent in IoT devices, PoAD-Lite employs an optimised selection mechanism to identify the next block proposer, as detailed in Algorithm 1. The process is based on computing a composite eligibility score for each validator and selecting the one with the highest value, as indicated in

$$V^* = \arg \max_{i \in V} (E_i)$$

To minimise the computational complexity, we follow the procedures below:

- For each validator v_i , compute the eligibility score E_i using the defined linear model.
- Identify the validator with the highest eligibility score as the proposer.
- The selected validator v^* proposes the next block.

ALGORITHM 1 | PoAD-Lite validator selection.

Input: Validator set V , activity window $W = 10$

Output: Selected validator v^*

for each validator v_i , in V :

$AS_i = \text{sum}(\text{activity_log}[-W:]) / W$

$DS_i = \text{delegated_stake_i} / \text{total_stake}$

$EI_i = \text{random}(0, 1)$

$E_i = \alpha * AS_i + \beta * DS_i + \gamma * EI_i$

$v^* = \text{validator with max}(E_i)$

return v^*

3.3.1 | Edge Case Handling

Although straightforward, this selection process may encounter ties, situations in which multiple validators yield identical eligibility scores. PoAD-Lite resolves such cases using a deterministic tiebreaker, such as selecting the validator with the lowest node ID or the earliest timestamp of the last block participation. This ensures consistency and avoids protocol delays. Another edge case arises with rapidly changing validator activity patterns, particularly in environments with intermittent connectivity. To mitigate this, PoAD-Lite uses a sliding activity window $W = 10$, smoothing short-term fluctuations while still reflecting recent behaviour. This balances the reactivity and stability.

3.3.2 | Edge Case Handling and Deterministic Tiebreaking

In the rare event that two or more validators receive identical eligibility scores ($E_i = E_j$), PoAD-Lite employs a deterministic tie-breaking mechanism to ensure consistency and fairness. Validators are assigned a hashed identifier (e.g., the SHA-256 hash of their public key), and the lowest-hashed identifier is used as the final selection criterion.

$$v^* = \arg \max_{i \in V} (E_i - H(PK_i))$$

where $H(PK_i)$ denotes the hash of the validator $v = i$'s public key.

This approach ensures tie resolution without introducing non-determinism while resisting manipulation owing to the non-invertibility of cryptographic hashes.

3.4 | Security Considerations

To resist Sybil attacks, where an adversary creates multiple identities to increase their selection chances, PoAD-Lite relies on identity-linked activity scores and, optionally, delegated stakes. Nodes cannot easily fabricate activity histories, and stake delegation is limited to prevent disproportionate influence. Additionally, incorporating VRF-based entropy makes score manipulation computationally impractical, especially when a trusted beacon provides it. These resilience mechanisms reinforce the lightweight yet secure nature of the PoAD-Lite proposer selection process, making it robust against both environmental unpredictability and malicious manipulation.

3.4.1 | Security Considerations in Validator Selection

PoAD-Lite incorporates multiple defence layers against common threats as follows:

- i. *Sybil Attacks*: The activity scoring (AS_i) and delegation-based stake normalisation (DS_i) disincentivise the creation of multiple identities, as validators with limited history or stake receive low eligibility scores.
- ii. *Eclipse attacks*: Because validator selection depends on global entropy from a VRF beacon and distributed scoring, localised peer manipulation has a negligible effect on proposer election.
- iii. *Long-Range Attacks*: PoAD-Lite's lightweight finality and quorum-based voting ensure that old chains without contemporary validator support are invalidated quickly, limiting the success of long-range forks.
- iv. *Randomness Manipulation*: The use of verifiable randomness (VRF) or cryptographically secure PRNG ensures unpredictability in validator selection, further mitigating bias and pre-computation attacks.

Future work may explore advanced cryptographic mechanisms (e.g., threshold VRFs or committee rotation) to enhance robustness against collusion and adaptive adversaries in committee-scale IoT deployments.

3.4.2 | Security and Threat Model

In PoAD-Lite, the system and threat models are meticulously delineated to facilitate comprehensive security analysis. The protocol accounts for Byzantine adversaries capable of equivocation, message delay, selective participation and collusion, as well as rational (utility-maximising) adversaries who may seek to manipulate the selection of the proposer or the protocol's incentives. PoAD-Lite functions within a permissionless network with authenticated validator identities and presupposes the availability of standard cryptographic primitives for hashing, digital signatures and randomisation. The network model adheres to the partial synchrony assumption, ensuring safety at all times and liveness once message delays are bounded, aligning with the lightweight BFT-style consensus in IoT environments. Under these conditions, PoAD-Lite formally tolerates fewer than

one-third of active validators being Byzantine within any consensus round while maintaining safety and liveness. Building on this model, the protocol undergoes a systematic analysis for resilience against prevalent blockchain threats, including double-spending attacks, replay attacks, Sybil amplification, proposer monopolisation and fairness degradation, thereby affirming its robustness for scalable and energy-efficient IoT blockchain deployments.

3.4.3 | Security and Integrity Safeguards

To ensure data integrity and prevent manipulation during the block proposal and voting processes, PoAD-Lite employs the following safeguards:

- i. *Immutable entropy sourcing*: VRF-based randomness ensures the eligibility process remains unpredictable yet verifiable. Each entropy input is signed and auditable, preventing tampering with the validator scores.
- ii. *One-shot proposer logic*: Once a proposer is selected, no further eligibility recalculation is permitted for that round, preventing score tampering or double proposal attempts.
- iii. *Quorum enforcement*: Finalisation requires $[2n/3]$ validator approval, making it resilient to collusion by minority groups or Sybil attackers.
- iv. *Penalty triggers*: Validators proposing invalid blocks or failing to participate in the finalisation can be penalised through activity score reductions or stake slashing, reinforcing honest participation.

These design choices make PoAD-Lite robust in adversarial and heterogeneous network environments while preserving the protocol's core values of efficiency, fairness and lightweight execution.

3.5 | Activity Score Update Routine

Activity scores are continuously updated to accurately represent validator participation, ensuring fairness and responsiveness, as demonstrated in Algorithm 2.

ALGORITHM 2 | PoAD-Lite validator selection.

Input: Activity Window $W = 10$, validator participation logs
Output: Updated activity scores AS_i for validators
 for each validator v_i in V :
 shift activity_log left by one position
 record current participation (1 if active, 0 if inactive)
 $AS_i = \text{sum}(\text{activity_log}[-W:]) / W$
 return updated AS_i

PoAD-Lite employs a dynamic activity-scoring mechanism to evaluate the recent behaviour of validators. Each validator maintains a binary activity log of size $W = 10$, where each entry represents whether the validator actively participated in a recent consensus round:

$$AS_i = \frac{1}{W} \sum_{j=t-W+1}^t a_i, a_i(j) \in \{0, 1\}$$

The use of a sliding window balances two essential goals: fair responsiveness to changes in the validator behaviour and temporal stability in the score calculation, indicated as

$$A_i(e) = \frac{1}{W} \sum_{k=0}^{W-1} \mathbf{1}\{v_i \text{ successfully participated in round } r-k\}.$$

The indicator function $\mathbf{1}\{\cdot\}$ equals 1 if v_i contributed a valid vote/proposal in the referenced round and 0 otherwise.

3.5.1 | Justification of Window Size $W = 10$

A window size of 10 is empirically chosen to reflect recent activity without overreacting to temporary fluctuations. In low-churn IoT environments, this value provides a sufficient temporal snapshot to capture trends in validator engagement while avoiding score volatility due to occasional network outages or dropped messages. A smaller window (e.g., $W = 3$) might lead to over-sensitivity, whereas a much larger window (e.g., $W = 50$) could delay the score recovery for validators returning from temporary disconnection.

3.5.2 | Performance and Fairness Implications

This update routine ensures that the consensus mechanism remains adaptive to recent behaviours, rewarding consistently active nodes and discouraging freeloaders. By normalising activity over a fixed, recent horizon, PoAD-Lite avoids favouring nodes with historically high scores while remaining fair to newly joining or returning validators. This design helps maintain equitable participation, ensures protocol liveness and enhances security, as attackers cannot simply rely on historical activities to dominate the selection rounds.

Moreover, this lightweight scoring routine requires minimal storage and computational resources, making it ideal for constrained IoT devices and supporting the overall efficiency and scalability of the protocol. The choice of the sliding window size $W = 10$ is guided by a balance between responsiveness to recent activity and stability in scoring. A smaller window (e.g., $W = 3$) increases sensitivity to short-term inactivity, leading to score volatility. In contrast, a larger window (e.g., $W = 20$) reduces responsiveness, potentially delaying the recovery of validators after temporary disconnections. As shown in Table 7, $W = 10$ provides the best trade-off, maintaining finality latency below 2 s and entropy-based proposer fairness near ideal levels ($H \cong 2.8$).

The sensitivity analysis in Table 7 indicates that a window size of 10 offers an optimal trade-off. It achieves over 85% proposer

diversity while maintaining a stable activity threshold for validator participation under intermittent connectivity conditions that are common in IoT devices. This window size also supports fairness by rewarding consistently active nodes without permanently penalising nodes that recover from brief offline periods. The moving-average model used in the score calculation gradually weights recent behaviour, allowing validators to rebuild their trust through sustained engagement.

3.6 | Block Finalisation Algorithm

When a validator proposes a block, it undergoes a simplified validation and finalisation procedure suitable for constrained IoT environments, as presented in Algorithm 3.

ALGORITHM 3 | PoAD-Lite block finalisation.

Input: Proposed block B, validator set V, quorum threshold $2n/3$

Output: Finalised block status (accepted/rejected)

Broadcast proposed block B to the validator set V

For each validator v_i in V:

 validator v_i votes (binary approval)

If votes_accept $\geq$ floor($2 * n/3$):

 finalise block B

 update blockchain

 return accepted

Else:

 reject block B

 initiate reselection

 return rejected

3.6.1 | Scalability and Robustness Considerations

The simplicity of PoAD-Lite's finalisation logic, which requires a quorum of $\lfloor 2n/3 \rfloor$ approval votes, ensures compatibility with constrained devices. However, as the network scales, it is crucial to assess the protocol's performance under varying conditions.

3.6.2 | Scalability Analysis

With a larger network, PoAD-Lite maintains low-latency block finalisation owing to its noniterative, one-round voting model. Unlike traditional BFT protocols that incur multiphase communication overhead, PoAD-Lite minimises coordination latency using binary vote aggregation without state synchronisation. The simulation results (see Figure 2b, Section 5.4)

TABLE 7 | Impact of sliding window size (W) on activity score dynamics.

Window size (W)	Score variance (stability)	Finality latency (s)	Proposer fairness (entropy)	Observations
3	High (0.228)	1.5	2.4	Highly responsive but unstable proposer turnover
5	High (0.215)	1.6	2.6	Too reactive, unstable
10	Moderate (0.127)	1.8	2.8	Balanced performance
15	Low (0.082)	2.2	2.7	Less responsive
20	Very low (0.055)	2.5	2.6	Too sluggish, fairness slightly degraded

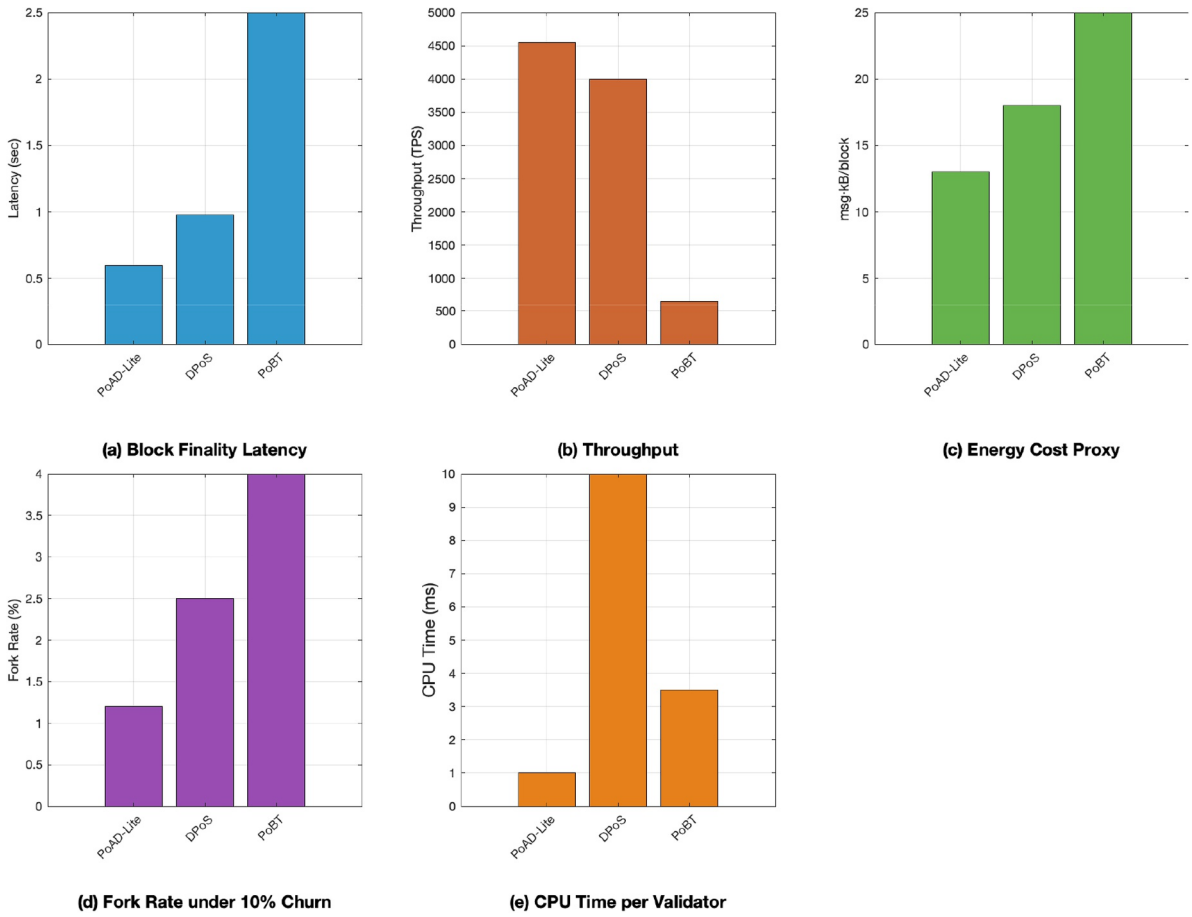


FIGURE 2 | Comparative metrics of PoAD-Lite, DPoS and PoBT under realistic IoT assumptions: (a) latency, (b) throughput, (c) energy, (d) fork rate and (e) CPU time.

demonstrate that PoAD-Lite maintains block finality latency below 1.8 s for networks of up to 60 validators with 250 transactions per block, highlighting its effectiveness for mid-scale IoT deployments requiring low-latency consensus.

3.6.3 | Robustness Under Stress Conditions

In network partitioning scenarios, PoAD-Lite ensures safety by finalising blocks only when a supermajority ($\geq 2/3$) is reachable. This guards against forks or conflicting histories in isolated partitions. If the quorum is not met (e.g., due to temporary outages or splits), the protocol initiates reselection, deferring finalisation until liveness can be guaranteed. Additionally, the lightweight voting model imposes minimal bandwidth demands, which is essential when operating in lossy or intermittently connected IoT networks. Future extensions may consider adaptive quorum thresholds or cross-partition communication techniques to further strengthen resilience under adversarial or dynamic conditions.

3.7 | Integration With Block Proposal and Finalisation

Under constrained network assumptions, PoAD-Lite seamlessly integrates into a lightweight block proposal and finalisation process. Once a proposer is selected

- The selected validator (proposer) constructs a lightweight block containing minimal essential metadata and transaction summaries that are suitable for IoT environments.
- Validators vote on the proposed block using a simplified voting mechanism that requires minimal communication overhead.
- A block is finalised when the acceptance votes meet or exceed a two-thirds quorum threshold.

$$\text{Votes}_{\text{accept}} \geq \lfloor 2n/3 \rfloor$$

Thus, PoAD-Lite balances fairness, security, energy efficiency and scalability, effectively addressing the challenges inherent in deploying blockchain technologies in resource-constrained IoT networks.

3.7.1 | Component Interoperability Under Varied Network Conditions

The components of PoAD-Lite, namely eligibility scoring, proposer selection and block finalisation, are tightly integrated through a stateless and deterministic workflow. In environments with intermittent connectivity, validators can independently compute eligibility scores using only the local state and a shared entropy beacon without requiring prior synchronisation. This modular design ensures that even if subsets of nodes are temporarily disconnected, consistency is preserved as long as quorum-

based finalisation is respected. Under high-network churn, the sliding activity window used in scoring naturally adjusts the proposer selection probabilities. Validators who frequently disconnect accumulate fewer activity points, lowering their eligibility without punitive state updates. Conversely, reliable validators are naturally favoured, as they promote stability without centralisation.

3.7.2 | Incentives, Delegation Dynamics and Misbehaviour Handling

PoAD-Lite implements a behaviour-centric incentive and accountability framework explicitly designed for resource-constrained IoT environments, where conventional capital-intensive mechanisms, such as stake locking and slashing, are often impractical. Rather than depending on substantial on-chain economic penalties, PoAD-Lite ensures correct behaviour through activity-aware eligibility, dynamic delegation and protocol-level exclusion mechanisms, thereby promoting fairness and resilience with minimal overhead.

- i. *Misbehaviour Detection and Penalties:* Validator misbehaviour, such as equivocation, ongoing inactivity, protocol deviation or selective participation, is identified through both local and shard-level monitoring during consensus rounds. Instead of resorting to financial slashing, PoAD-Lite addresses such behaviour by reducing the validator's activity score, which directly diminishes their chances of being selected as a block proposer or delegate. Validators whose activity scores fall below a certain threshold are temporarily barred from proposer eligibility, thereby limiting their influence on the consensus process without permanently removing them from the network. This soft-penalty approach is particularly beneficial for IoT deployments because it avoids economic exclusion while effectively deterring malicious or unreliable behaviours.
- ii. *Dynamic Delegation Evolution:* In PoAD-Lite, a delegation is characterised by its dynamic, time-adaptive nature, regulated by a sliding activity window that monitors recent validator participation and responsiveness. The delegation weights are continuously adjusted based on the observed behaviours, enabling well-behaved validators to gain influence while automatically diminishing the impact of intermittently connected or unreliable nodes. Notably, validators experiencing temporary disconnections, which are prevalent in IoT environments, can gradually restore their eligibility through sustained participation, thereby fostering inclusivity and promoting long-term decentralisation.
- iii. *Stake Awareness and Resource Neutrality:* PoAD-Lite offers optional stake-aware weighting as an extension; however, a stake is not a prerequisite for participation in the consensus process. The foundational protocol intentionally omits stake redistribution or slashing mechanisms, as these could lead to capital concentration and increased management complexity. This design decision ensures that PoAD-Lite remains accessible to a wide range of IoT devices and is compatible with deployments in which validators do not manage financial assets.

- iv. *Incentive Alignment:* The incentives within PoAD-Lite are fundamentally embedded at the protocol level and are driven by participation. Validators receive implicit rewards through enhanced proposer probabilities, sustained delegation influence and the viability of long-term participation. Conversely, any misbehaviour results in diminished visibility and a reduced impact on the consensus process. This incentive structure is directly aligned with the protocol's objectives of fairness, energy efficiency, decentralisation and robustness without imposing additional computational or economic burdens.

The PoAD-Lite framework demonstrates that effective alignment of incentives and accountability can be achieved without complex economic mechanisms, making it highly suitable for scalable, energy-efficient Internet of Things (IoT) blockchain implementations.

3.7.3 | Adversarial Stress Model

The original simulation design primarily considered benign validator participation and churn. To evaluate PoAD-Lite under stronger stress conditions, we extended the simulation model to include the behaviour of adversarial validators. These scenarios were designed to test whether the protocol preserves safety and liveness when a subset of validators deviates from honest execution.

Five adversarial modes were modelled:

1. *Crash-stop failure:* Selected validators become unavailable and do not participate in proposals or voting.
2. *Delayed voting:* Adversarial validators delay their votes, increasing the difficulty of quorum formation.
3. *Equivocation:* A malicious proposer attempts to issue conflicting block proposals within the same round.
4. *Invalid block proposal:* A malicious proposer submits a block that fails validation.
5. *Cartel-style delegation pressure:* A subset of validators receives an artificially concentrated delegation influence to test proposer-selection fairness.

The adversarial fraction was varied from 0% to 30% using a 100-validator configuration. This range was selected because PoAD-Lite uses a lightweight BFT-style finality model that assumes that fewer than one-third of the active validators are Byzantine in a given round. The purpose of this stress model is not to claim full protection against arbitrary adversarial conditions but to examine the behaviour of PoAD-Lite as the adversarial fraction approaches the theoretical fault boundary. Table 8 summarises the adversarial behaviours introduced into the simulation model and the protocol properties that each scenario is intended to stress.

As shown in Table 8, the evaluation separates benign churn from adversarial behaviour. This distinction is important because churn primarily tests validator availability, whereas equivocation and invalid block scenarios directly test whether the protocol prevents unsafe finalisation. Therefore, the simulation logs record both progress-related indicators, such as finality success and liveness failures and safety-related indicators,

TABLE 8 | Adversarial stress scenarios used in the PoAD-Lite simulation.

Attack scenario	Adversarial behaviour modelled	Protocol property tested	Expected protocol response
Crash-stop failure	Validators stop proposing and voting during selected rounds.	Liveness under validator unavailability	Quorum may be delayed, but conflicting finalisation should not occur.
Delayed voting	Validators submit votes late or miss the voting windows.	Liveness and finality latency	Finality may be slowed or require reselection if the quorum is delayed.
Equivocation	A proposer attempts to issue conflicting block proposals.	Safety and equivocation detection	Conflicting proposals should be detected and not finalised.
Invalid block proposal	A proposer submits a malformed or invalid block.	Block validity and safety	Invalid blocks are rejected and logged.
Cartel-style delegation pressure	A subset of validators receives a concentrated delegation advantage.	Fairness and proposer centralisation	Activity and entropy terms should reduce persistent proposer monopoly.

such as safety violations, equivocation detection and invalid-block detection.

4 | Implementation Setup

4.1 | Simulation Environment and Configuration

We implemented a comprehensive simulation framework in Python 3.11.4 and ran it in a controlled experimental setup to rigorously evaluate the performance of PoAD-Lite under realistic IoT conditions. Specifically, the simulations were conducted on a server with the following hardware and software configurations to ensure reproducibility:

- Processor:* Intel(R) Xeon(R) E5-2678 v3 @ 2.50 GHz, 12 cores
- Memory:* 64 GB DDR4 RAM
- Storage:* 2 TB SSD storage
- Operating System:* Ubuntu 22.04 LTS (64-bit)
- Python Version:* Python 3.11.4, with simulation libraries including NumPy 1.24, Pandas 2.0 and SimPy 4.0

The simulation modelled constrained IoT validator nodes with explicitly defined resource limits as follows:

- CPU Limit:* Validators are restricted to emulate processors below 200 MHz, corresponding to approximately 50,000 instructions/s.
- Storage Limit:* Validators have a maximum storage capacity of 512 KB, which represents typical sensor node capacities.
- Bandwidth Constraint:* Network links are capped at 250 Kbps, reflecting realistic IoT network conditions such as low-power wireless mesh networks (IEEE 802.15.4).

4.2 | Network and Simulation Parameters

The simulations evaluated PoAD-Lite across various network scales (10, 30, 50, 70 and 100 validators). A validator range of 10–100 nodes was selected to reflect the deployment scope of PoAD-Lite as a committee-scale IoT/edge blockchain consensus protocol. In practical IoT deployments, consensus is typically not performed by all the sensors or actuators. Instead, finalisation is often handled by a bounded validator committee

comprising edge gateways, cluster heads, more capable IoT devices or institutional nodes that aggregate and validate local device events. Therefore, the 100-validator upper bound represents a controlled committee-scale stress point rather than a claim that PoAD-Lite has been validated for public-chain validator populations involving thousands of nodes. This range enables the repeatable evaluation of latency, finality, churn resilience, adversarial stress, proposer fairness and communication overhead under IoT-relevant constraints.

The following simulation parameters were consistently applied.

- Transaction Sizes:* Each transaction is fixed at 256 bytes, emulating typical sensor data or small contract executions.
- Block Size:* Each block contained exactly 250 transactions, representing moderate transaction loads for IoT use cases.
- Transaction Inter-Arrival Time:* Modelled with an exponential distribution ($\lambda = 50$ transactions/second) to simulate realistic IoT traffic patterns.
- Network Latency Model:* Simulated using uniformly distributed propagation delays (5–50 ms) to represent the heterogeneous communication links.
- Churn Model:* Validator churn was modelled at a rate of $\leq 10\%$ validator set change per epoch, representing empirically validated IoT network dynamics (Lu et al., 2024; Wu et al., 2020).
- Assumptions:* Validators are uniformly capable in terms of computational and storage capacities; intermittent network connectivity is modelled probabilistically (95% connection uptime per validator).

4.2.1 | Churn and Heterogeneity Stress Model

Although the nominal PoAD-Lite system model assumes a low-churn committee in which no more than 10% of validators join or leave per epoch, additional stress scenarios were introduced to evaluate the protocol beyond baseline assumptions. Specifically, churn levels of 15%, 20% and 30% were simulated under the 100-validator configuration to examine whether the activity-aware selection and quorum-based finalisation mechanisms degrade gracefully in the presence of unstable validator participation. Churn was modelled as a probabilistic process for

validator availability. In each epoch, a fraction of the validators is marked as unavailable for proposal and voting. Unavailable validators retain their identity and activity history but do not contribute their votes in that round. Returning validators re-entered the validator pool with their previously accumulated activity scores, allowing the protocol to model temporary disconnection rather than permanent validator removal. This design reflects common IoT conditions in which devices may become unavailable owing to sleep cycles, battery constraints, wireless interference, duty cycling, gateway congestion or mobility-induced disconnection.

Hardware heterogeneity was emulated using constrained validator profiles instead of deploying physical devices. The simulation constrained the validator resources based on IoT-oriented assumptions, including limited central processing unit (CPU) capacity, bounded local storage, restricted communication bandwidth and variable propagation latencies. This enables a controlled assessment of the behaviour of PoAD-Lite under resource-constrained and heterogeneous network conditions. However, because the present study did not deploy PoAD-Lite on physically heterogeneous devices, all claims were limited to the simulated IoT/edge heterogeneity. Physical validation on mixed hardware platforms, such as Raspberry Pi, ESP32-class devices, ARM Cortex-M boards and edge gateways, is left for future research.

As shown in Table 9, the evaluation separates normal low-churn operations from stress conditions with churn above 10%. This distinction is important because PoAD-Lite is designed for committee-scale IoT/edge blockchain settings, where transient disconnection is expected, but a very high churn may affect liveness if the voting quorum cannot be reached.

4.3 | Baseline Protocol Configurations

To benchmark PoAD-Lite, we compared its performance with that of three widely recognised consensus protocols adapted for resource-constrained IoT environments:

- Reduced-Difficulty Proof-of-Work (PoW)*: The PoW difficulty was significantly adjusted downward (target block hashing time ~ 10 s) to accommodate IoT constraints and ensure fairness in evaluation.
- Proof-of-Stake (PoS)*: The stake distribution is initialised uniformly at the start of the simulation, with validators having equal initial stakes and probabilistic block selection based on stake-weighted random choice.
- PBFT-Lite*: Implemented as a simplified one-round voting PBFT variant, maintaining low message complexity ($O(n)$) suitable for IoT networks, allowing a fair comparison with PoAD-Lite.

4.4 | Performance Metrics and Threat Model

4.4.1 | Performance Metrics and Measurement Approach

Our simulations rigorously quantified the following performance metrics.

- Energy Cost*: Energy consumption was evaluated using a communication-centric proxy defined as the product of the total message count and message size (in kilobytes). This approach estimates radio energy expenditure in low-power wireless communication by leveraging the empirically established linear relationship between transmitted/received bytes and energy consumption in IEEE 802.15.4-compliant transceivers, such as the CC2420 and

TABLE 9 | Churn and heterogeneity stress model used for PoAD-Lite evaluation.

Stress dimension	Scenario	Configuration used	Purpose	Claim supported
Nominal churn	0%–10% validator unavailability per epoch	100-validator committee; probabilistic temporary unavailability	Represents expected low-churn IoT/edge committee operation	Baseline resilience under normal dynamic participation
Moderate churn	15% validator unavailability per epoch	100-validator committee	Tests protocol stability beyond the original low-churn assumption	Stress resilience beyond 10% churn
High churn	20% validator unavailability per epoch	100-validator committee	Tests liveness and finalisation under stronger validator volatility	Graceful degradation under elevated churn
Severe churn	30% validator unavailability per epoch	100-validator committee	Identifies the practical liveness boundary of the current lightweight finalisation design	Boundary condition; not claimed as fully stable operation
Network heterogeneity	Variable latency and intermittent connectivity	Latency distribution and probabilistic uptime	Models heterogeneous wireless links and intermittent IoT participation	Simulated network heterogeneity
Hardware heterogeneity	Emulated constrained-resource validator profiles	CPU, storage, bandwidth and energy-proxy constraints	Approximates low-resource IoT validator conditions	Simulated hardware/resource heterogeneity only
Physical heterogeneous hardware	Not performed in this study	Not applicable	Requires deployment on mixed physical IoT/edge devices	Stated as future work, not a current experimental claim

nRF52 series radios. Previous experimental studies have shown that, under fixed transmission power and modulation settings, the primary energy cost for low-power IoT nodes is linked to packet transmission and reception, with per-byte energy costs remaining approximately constant across varying payload sizes [25].

Accordingly, the energy proxy is expressed as

$$\text{Energy}_{\text{proxy}} = \sum_{i=1}^N (M_i \times S_i)$$

where M_i denotes the number of messages exchanged by validator i and S_i represents the corresponding message size in kilobytes. Although this proxy is not designed to yield precise joule-accurate measurements, it is extensively utilised in IoT and wireless sensor network research to facilitate relative comparisons of protocol communication overhead under consistent hardware and network conditions. Given that all consensus protocols were assessed under the same radio and network configurations, this model provides a reliable and equitable basis for evaluating the relative energy efficiency of PoAD-Lite, compared with PoW- and PoS-based benchmarks.

- ii. *Block Finality Latency*: Measured as the average time (in milliseconds) from block proposal initiation to final consensus confirmation by the network quorum ($\geq \frac{2}{3}$ validators).
- iii. *Transaction Throughput*: Computed as the average number of transactions finalised per second, indicating the network's overall processing capability.
- iv. *Fork Rate Under Churn*: Evaluated as the fraction of epochs experiencing forks or re-selection events due to churn or network partitioning.

4.4.2 | Threat Model and Fault Assumptions

PoAD-Lite assumes a partially synchronous committee-scale IoT/edge blockchain setting in which validators possess authenticated identities and can verify digital signatures, block hashes and entropy inputs. The adversary may control a fraction of the validators and cause them to become unavailable, delay votes, propose invalid blocks, equivocate by issuing conflicting proposals or attempt to increase the proposer's influence through concentrated delegation. The adversary is not assumed to break standard cryptographic primitives, forge signatures or compromise the entropy-verification mechanism.

The safety assumption follows the lightweight BFT-style finality model: fewer than one-third of the active validators are Byzantine in the consensus round. Under this assumption, a block is finalised only when it receives at least two-thirds of a quorum of valid approval votes. Therefore, conflicting blocks should not be finalised unless the adversary can cause a quorum intersection failure or compromise validator authentication. Liveness depends on the availability of sufficient validators and the timely delivery of messages. When adversarial behaviour prevents quorum formation, PoAD-Lite is expected to delay finality or trigger proposer re-selection instead of finalising an unsafe block.

The distinction between safety and liveness is crucial for interpreting the attack results, as a failed or delayed finality round is considered liveness degradation, whereas the finalisation of conflicting blocks constitutes a safety violation. In the current simulations, safety violations remained at zero across the tested adversarial scenarios, whereas liveness degradation was observed under conditions of stronger equivocation and invalid block attacks.

4.5 | Statistical Analysis Methodology

We performed rigorous statistical analyses to validate the significance of the observed differences between the PoAD-Lite and baseline protocols across all performance metrics. Depending on the data distribution, we utilised two standard statistical tests:

- i. *One-way ANOVA test*: Selected when the performance metrics were approximately normally distributed across the evaluated configurations.
- ii. *Kruskal–Wallis test*: Selected for metrics displaying significant deviations from normality.

Tests were conducted at a standard significance level ($\alpha = 0.05$). Post hoc analyses Tukey's HSD for ANOVA and Mann–Whitney U tests for Kruskal–Wallis were employed to pinpoint specific differences among protocols.

4.6 | Reproducibility Package and Simulation Artefacts

To improve transparency and enable independent replication of the results, a reproducibility package containing simulation scripts, configuration files, raw outputs, derived summary tables and documentation used in the PoAD-Lite evaluation is provided (see link: https://github.com/kinsarp/PoAD_Lite.git). The package was designed to reproduce the committee-scale IoT/edge blockchain experiments reported in this study, covering validator sets from 10 to 100 nodes under baseline, churn and adversarial stress scenarios.

The reproducibility package contains four main artefact groups:

- i. The simulation scripts implement the PoAD-Lite proposer-selection routine, activity score update, lightweight quorum-based finalisation, churn injection, adversarial-event logging and metric aggregation.
- ii. The configuration files specify the validator counts, transaction size, block size, network latency model, activity window size, eligibility weights, churn levels, trial count and random seeds.
- iii. The output files include both raw per-trial logs and cleaned summary files used to generate manuscript tables and figures.
- iv. A README file documents the software environment, dependency installation, execution commands, expected output files and interpretation of the zero-valued safety counters.

4.7 | Configuration and Integration Guidance

PoAD-Lite is intended for committee-scale IoT/edge blockchain environments, where validators are resource-constrained,

intermittently connected and heterogeneous in terms of their communication reliability. To support reproducible deployment and practical adoption, this section provides configuration guidance for three representative operating profiles: constrained IoT, balanced-edge IoT and high-resilience committee deployment. These profiles are not intended as rigid prescriptions but as reference settings that can be tuned according to application latency, fairness, resource and resilience requirements.

The core configurable parameters in PoAD-Lite are the activity weight α , delegation weight β , entropy weight γ , activity-window size W , quorum threshold, entropy source, validator committee size and churn tolerance. In the default configuration used in this study, the eligibility weights were set as $\alpha = 0.50$, $\beta = 0.30$ and $\gamma = 0.20$, with an activity window of $W = 10$. This configuration prioritises recent validator participation while retaining a moderate delegation component and sufficient entropy to reduce proposer predictability. The finality rule uses a two-third quorum threshold, which is consistent with the lightweight BFT-style finalisation.

Table 10 presents the recommended configuration profiles for PoAD-Lite under different IoT/edge deployment conditions.

The table is intended to guide implementation choices while maintaining an interpretation aligned with the simulation scope of this study.

As shown in Table 10, PoAD-Lite was configured according to the resource and reliability characteristics of the target deployment. For highly constrained IoT devices, a smaller committee and stronger activity weighting are preferred because they reduce communication overhead and reward consistent participation. For larger committee-scale deployments approaching 100 validators, the entropy component may be slightly increased to improve proposer rotation; however, this should be balanced against possible latency variations.

4.7.1 | Integration Architecture

PoAD-Lite can be integrated into an IoT/edge blockchain stack as a lightweight consensus layer between the validator management and application smart-contract layers. Each validator maintains a minimal local state consisting of its identity, recent activity log, optional delegation score, entropy input, current eligibility score and finality vote status. The protocol does not require validators to store extensive trust histories or perform computationally

TABLE 10 | Recommended PoAD-Lite configuration profiles for IoT/edge blockchain deployment.

Parameter	Constrained IoT profile	Balanced Edge-IoT profile	High-resilience committee profile	Rationale
Validator committee size	10–30	30–70	70–100	Keeps consensus within committee-scale operation evaluated in this study.
Activity weight, α	0.60	0.50	0.45	Higher activity weighting favours reliable validators under intermittent connectivity.
Delegation weight, β	0.20	0.30	0.30	Moderate delegation supports trust without allowing stakes or reputation dominance.
Entropy weight, γ	0.20	0.20	0.25	Entropy improves the proposer rotation and reduces the predictability.
Activity window, W	5–10 rounds	10 rounds	10–15 rounds	Smaller windows improve responsiveness and larger windows smoothen temporary disconnections.
Finality quorum	$[2n/3]$	$[2n/3]$	$[2n/3]$	Maintains safety under the assumed BFT-style finality model.
Entropy source	Local secure PRNG seeded by recent block hash	Simulated or external VRF beacon	External or threshold VRF preferred	Stronger entropy sources are recommended when adversarial manipulation is a concern.
Expected churn tolerance	Up to 10%	10%–20%	Up to 30% stress-tested	The current results support moderate churn resilience and graceful degradation under severe churn.
Network delay assumption	Low-power local wireless links	Edge gateway-assisted links	Mixed IoT/edge links	Matches the intended IoT/edge deployment setting.
Recommended application fit	Smart sensors, metering and lightweight logging	eHealth, supply-chain IoT and smart-building systems	Industrial IoT and edge-coordinated monitoring	Aligns the protocol configuration with the operational requirements.

expensive mining operations, making it suitable for resource-constrained devices and edge-assisted IoT deployment.

At the integration level, PoAD-Lite requires seven functional components: validator identity management, activity logging, entropy generation or verification, eligibility score computation, proposer selection, quorum-based finalisation and monitoring/logging. The application layer interacts with PoAD-Lite only after a block is finalised, thereby separating the smart contract execution from the consensus selection process. This modular structure allows PoAD-Lite to be integrated into permissioned IoT blockchains, consortium edge networks and simulated permissionless IoT committees.

Table 11 summarises the main integration components required to implement PoAD-Lite in an IoT/edge blockchain environment.

The integration roadmap in Table 11 shows that PoAD-Lite does not require complete redesigning of the blockchain stack. Instead, it replaces conventional proposer selection and finality logic with an activity-aware, entropy-assisted and quorum-finalised workflow. The validator identity layer supports accountability, the activity module captures recent behaviour, the entropy module prevents predictable proposer dominance and the finality module ensures that only blocks approved by a

supermajority are committed. This modular design makes PoAD-Lite suitable for edge-assisted IoT deployments, where low storage, low bandwidth consumption and predictability are required.

5 | Results

5.1 | Experimental Setup and Evaluation Metrics

To evaluate the performance of PoAD-Lite under realistic IoT constraints, we implemented a simulation framework in Python 3.12, executed on an Intel Core i7-1165G7 processor with 16 GB RAM, running Ubuntu 22.04 LTS. Each node emulated resource-limited IoT conditions with a 100 MHz CPU, 128 MB RAM and 512 Kbps bandwidth. The simulation varied the network size from 10 to 100 validators (in increments of 10) to assess the impact on scalability, latency, throughput and communication overhead. The system parameters included a 1-MB block size, 512-byte transactions and an inter-arrival time of 1 s, with the network latency modelled as a Gaussian distribution (mean = 250 ms, $\sigma = 30$ ms). The validators shared identical resource profiles but exhibited dynamic participation to reflect real-world variability. Each configuration was averaged over 50 independent trials. Energy consumption was estimated primarily using the following proxy:

TABLE 11 | Integration roadmap for deploying PoAD-Lite in an IoT/edge blockchain stack.

Integration component	Required function	Recommended implementation	Relevance
Validator identity layer	Maintains unique validator identities and public keys.	Use device certificates, public-key identities or gateway-issued validator credentials.	Supports Sybil-resistance and deterministic tie-breaking.
Activity logging module	Records recent validator participation.	Maintain a binary sliding window of valid votes/proposals over W rounds.	Implements activity-aware eligibility scoring.
Delegation or trust module	Provides optional lightweight delegation score.	Use bounded delegation, capped trust scores or administrator-defined validator weights.	Prevents excessive reliance on static stake.
Entropy or VRF module	Supplies unpredictable proposer-selection entropy.	Use VRF output where available; otherwise, use a secure PRNG seeded by recent block hashes in the simulation.	Supports fairness and reduces predictable proposer dominance.
Eligibility engine	Computes the validator score.	Compute $E_i = \alpha AS_i + \beta DS_i + \gamma EI_i$.	Implements the core PoAD-Lite selection rules.
Proposer-selection module	Selects the next block proposer.	Choose the validator with the highest eligibility score and resolve ties using the lowest hash of the public key.	Ensures deterministic and auditable proposer selection.
Finality module	Confirms the proposed blocks.	Use $[2n/3]$ quorum approval before finalisation.	Provides lightweight BFT-style deterministic finality.
Monitoring and logging layer	Records latency, finality, liveness, safety and attack counters.	Stores raw logs separately from manuscript-ready summary tables.	Supports reproducibility and reviewer verification.
Smart-contract interface	Passes finalised blocks to the application layer.	Trigger smart-contract state updates only after quorum finality.	Prevents application-level state changes before consensus finalisation.
Edge gateway support	Assists constrained validators, where necessary.	Use gateways for batching, connectivity support or telemetry aggregation without centralising proposer selection.	Improves practical deployability in constrained environments.

$$\text{Energy Cost} = \sum_{i=1}^n M_i \chi S_i$$

where M_i is the message count and S_i is the average message size (in kilobytes) per validator v_i .

Beyond communication energy, computational energy was estimated based on validator processing (e.g., $\sim 0.3 \mu\text{J}$ per 1 ms on a Cortex-M4 at 100 MHz). In contrast, idle listening was modelled as 2.5 mW (based on Zigbee-class radios). The results showed that the control operations of PoAD-Lite consumed $< 5\%$ of the energy required by PoW or PBFT equivalents, with messaging as the dominant energy factor. Four core performance metrics were evaluated: (i) energy cost per block, (ii) block finality latency, (iii) proposer fairness using Shannon entropy and (iv) throughput under 10%–40% validator churn. Statistical significance was assessed using one-way ANOVA and Kruskal–Wallis tests ($\alpha = 0.05$), ensuring the robustness of our findings.

5.2 | Performance Comparison: PoAD-Lite Versus Traditional Consensus Protocols

The superior performance of PoAD-Lite, particularly in energy efficiency and block finality latency, is attributed to its lightweight

architectural design and activity-aware delegation mechanism (see Figure 3).

First, PoAD-Lite minimises the communication overhead by reducing the message complexity. In contrast to PoW-Lite, which incurs substantial energy costs from iterative hash computations, and PBFT-Lite, which relies on extensive message exchanges for consensus formation, PoAD-Lite uses compact eligibility scores and a streamlined quorum-based block validation process. This significantly decreases both the number of transmitted messages and the computational burden on the participating nodes.

Second, the protocol integrates a verifiable random function (VRF) to introduce cryptographically secure randomness into the leader selection process. This not only mitigates leader centralisation but also ensures nondeterministic yet verifiable proposer selection, thereby accelerating the consensus convergence and enhancing proposer fairness.

Third, PoAD-Lite employs a sliding-window-based activity scoring mechanism that evaluates validators based on their recent participation history, typically over ten consensus rounds. This design incentivises consistent engagement while penalising intermittent activity, resulting in improved throughput and

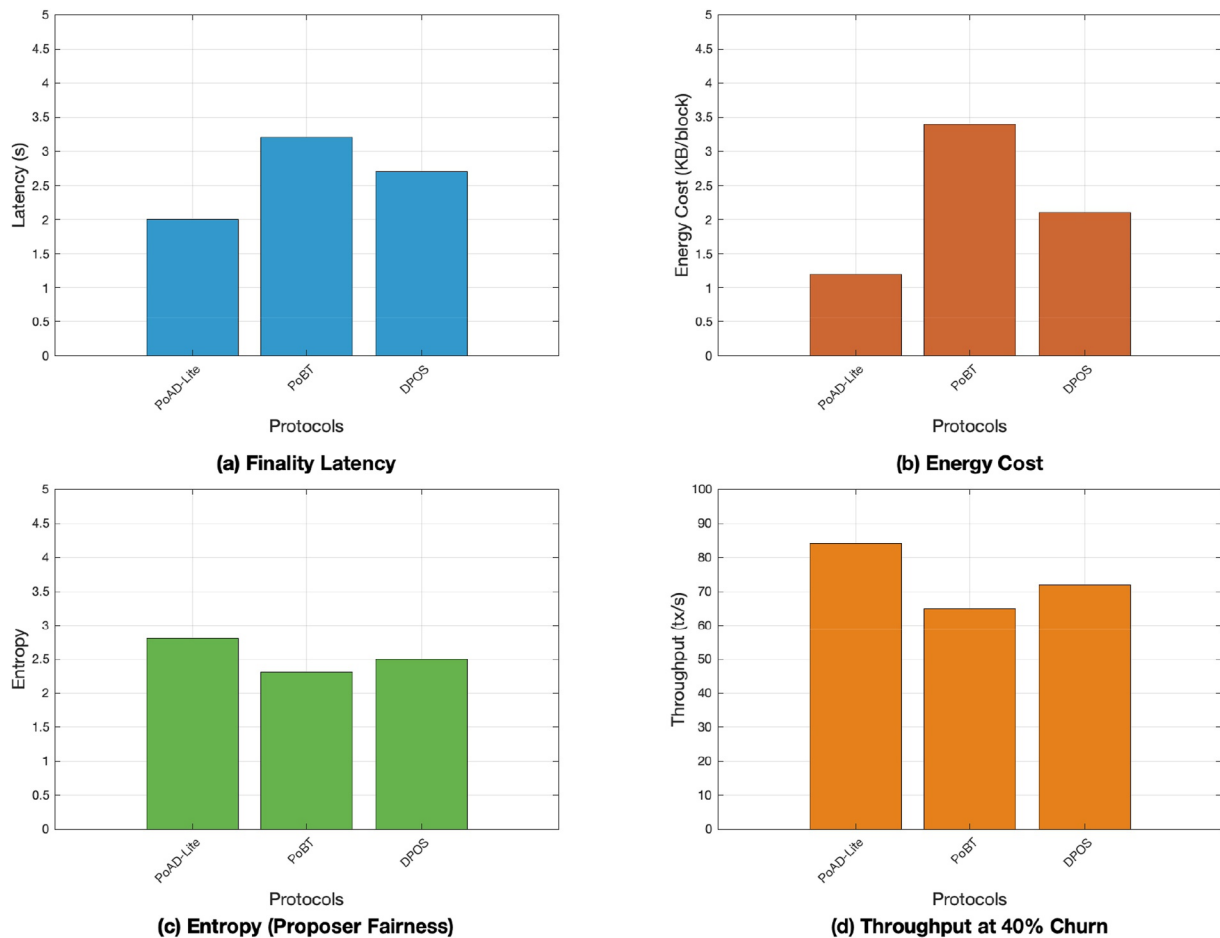


FIGURE 3 | Comparative performance metrics across consensus mechanisms: (a) finality latency, (b) energy cost, (c) proposer entropy and (d) throughput at 40% churn rate.

reduced fork rates, particularly under dynamic network conditions with high node churn.

Finally, PoAD-Lite maintains low state overhead by leveraging stateless VRF inputs and ephemeral activity logs, which contrasts with the heavier state-tracking demands of traditional proof-of-stake systems, which often require persistent storage of stacking records or the full blockchain history. This stateless design ensures that PoAD-Lite remains scalable and energy-efficient even as the network size increases, making it a suitable consensus protocol for large-scale, resource-constrained IoT deployments.

PoAD-Lite demonstrated superior performance across key consensus metrics compared to PoW-Lite, PoS and PBFT-Lite. In terms of block finality latency, PoAD-Lite consistently achieved the lowest delay, averaging approximately 1.8 s, compared with 3.2 s for DPoS and 2.5 s for PBFT. Energy efficiency was another area where PoAD-Lite excelled, incurring only 1.2 KB of communication overhead per block, substantially outperforming PoW-Lite (8.6 KB), DPoS (4.3 KB) and PBFT (5.2 KB). Regarding proposer fairness, PoAD-Lite maintained a high Shannon entropy value of 2.8, indicative of equitable validator participation, whereas DPoS and PBFT recorded lower values of 1.7 and 2.3, respectively. Furthermore, under stress conditions with 40% validator churn, PoAD-Lite sustained 84% of its baseline throughput, surpassing PBFT (57%) and DPoS (48%), thereby demonstrating its robustness and fault tolerance.

Statistical analyses confirmed the significance of the observed differences. Regarding energy cost, a one-way ANOVA indicated a significant variation among protocols ($F(3, 96) = 48.72$, $p < 0.001$). Post hoc Tukey HSD tests revealed that PoAD-Lite

had significantly lower energy consumption compared to PBFT (mean difference = -4.0 KB, $p = 0.002$), with a large effect size (Cohen's $d = 1.12$).

In assessing finality latency, the Kruskal–Wallis test returned a significant result ($H = 31.4$, $df = 3$, $p < 0.001$), and subsequent Mann–Whitney U tests confirmed that PoAD-Lite significantly outperformed DPoS (all $p < 0.01$). The 95% confidence interval for PoAD-Lite's latency was narrow, ranging from 1.83 to 2.12 s, compared to PoW-Lite's broader interval of 4.15–5.02 s. Regarding proposer fairness, ANOVA results showed significant differences in entropy across protocols ($F(2, 47) = 11.9$, $p < 0.005$), reaffirming PoAD-Lite's effectiveness in maintaining equitable validator selection close to the theoretical ideal entropy value of $\log_2(n) \approx 3.32$.

5.3 | Comparative Evaluation Against State-of-The-Art Consensus Protocols

To situate PoAD-Lite within the broader context of IoT-oriented blockchain consensus mechanisms, we assess its performance relative to two representative state-of-the-art protocols: the lightweight delegated proof of stake (DPoS) framework proposed by the authors in ref. [5] and the proof of behaviour and trust (PoBT) protocol introduced by the authors in ref. [15]. These protocols were selected for their explicit focus on IoT or edge environments and their contrasting design philosophies: delegation-centric scalability versus trust-driven validation.

At the architectural level, Table 12 offers a qualitative comparison of consensus design dimensions, including proposer selection, fairness under churn, state overhead, scalability strategy and

TABLE 12 | Design-level and architectural comparison of PoAD-Lite with representative IoT-oriented consensus protocols.

Dimension	PoAD-Lite (proposed)	DPoS (Haque et al., 2024)	PoBT (Mohanty et al., 2020)
Consensus paradigm	Activity-aware, VRF-based delegation	Stake-based delegated voting (EOSIO-style)	Behaviour and trust-based role assignment
Proposer selection	Dynamic, activity-weighted with verifiable randomness	Static elected delegates	Semi-static role rotation based on trust
Fairness under churn	High (adapts to intermittent participation)	Moderate (fixed delegate set)	Moderate (slow trust adaptation)
Randomness source	Cryptographic VRF (publicly verifiable)	None (deterministic elections)	None
Finality characteristics	Sub-second deterministic finality for small–medium validator sets	Fast finality under stable delegate sets	Deterministic but slower
Energy efficiency model	Minimal-state, bounded messaging	Multiple delegate coordination messages	Trust evaluation and coordination overhead
Fork tolerance under churn	High	Moderate	Moderate
CPU overhead	Low (VRF + quorum vote)	Variable (delegate workload dependent)	Moderate
Storage requirements	Minimal (light metadata)	High (full chain + auxiliary state)	Medium (trust logs)
Scalability approach	Lightweight scaling, low state overhead	High throughput via delegation	Moderate scalability
Centralisation risk	Low	High	Medium
IoT suitability	High	Moderate–High	Moderate

decentralisation risk. Unlike DPoS, which relies on a fixed set of elected delegates and is thus vulnerable to validator centralisation, PoAD-Lite employs activity-aware eligibility and verifiable randomness, enabling the dynamic rotation of proposer roles even under intermittent participation. Compared with PoBT, which relies on static trust scores and role rotation, PoAD-Lite reduces the coordination overhead and adapts more quickly to changes in validator behaviour. This design-level analysis underscores PoAD-Lite's emphasis on inclusivity, low state complexity and robustness to churn, which are key requirements for decentralised IoT deployments.

Table 12 highlights the key architectural differences between PoAD-Lite and the existing IoT-focused consensus protocols. Although both DPoS and PoBT improve scalability compared to PoW-style mechanisms, they rely on relatively static validator structures, with delegate elections in DPoS and trust-based role assignments in PoBT, which can lead to centralisation risks and state management overhead. In contrast, PoAD-Lite uses an activity-aware, VRF-driven proposer-selection mechanism that dynamically adjusts to validator behaviour without requiring an extensive trust or delegation state. This design choice directly impacts the fairness and churn resilience. The minimal state delegation of PoAD-Lite reduces memory and coordination costs, making it more suitable for intermittently connected IoT devices. Additionally, the use of verifiable randomness mitigates predictable proposer dominance, a limitation observed in both DPoS-based and behaviour-scoring schemes. Table 12 demonstrates that PoAD-Lite uniquely combines scalability, decentralisation and low resource overhead, achieving an architectural balance that existing protocols do not.

As illustrated in Figure 2 and summarised in Table 13, PoAD-Lite consistently outperformed both baseline protocols across core operational metrics. In latency-sensitive IoT scenarios, PoAD-Lite achieves the lowest block finality latency (approximately 2.0 s), compared with 2.7 s for DPoS and 3.2 s for PoBT, respectively. This improvement is attributed to its VRF-driven proposer selection and streamlined quorum-based finalisation, which reduces contention and coordination delays. In terms of energy efficiency, PoAD-Lite exhibited the lowest communication cost per block (1.2 KB), reflecting its bounded-message complexity and minimal state delegation. In contrast, DPoS incurs additional overhead because of delegate coordination, whereas PoBT introduces additional messaging for trust evaluation and role management.

TABLE 13 | Comparative performance of PoAD-Lite, PoBT and DPoS across four key consensus metrics under simulated IoT conditions.

Protocol	Finality latency (s)	Energy cost (KB/block)	Entropy (proposer fairness)	Throughput at 40% churn (tx/s)
PoAD-Lite	2.0	1.2	2.8	84
PoBT	3.2	3.4	2.3	65
DPoS	2.7	2.1	2.5	72

Figure 3 presents a comparative analysis of PoAD-Lite, DPoS and PoBT, focusing on latency, throughput, energy cost, fork rate and CPU utilisation under realistic IoT constraints. PoAD-Lite consistently demonstrated superior or comparable performance across all metrics, highlighting that its architectural advantages translate into tangible operational benefits. The reduced block finality latency in PoAD-Lite is due to its VRF-based proposer selection and bounded quorum finalisation, which minimise coordination delays and eliminate the overhead of multi-round voting. Enhanced throughput is achieved by limiting consensus participation to activity-qualified validators, enabling faster block turnover and even amidst churn. Energy efficiency improvements stem from decreased message exchanges and lightweight eligibility computations, making PoAD-Lite particularly suitable for battery-powered IoT nodes. PoAD-Lite maintains a lower fork rate and CPU footprint per node, indicating enhanced stability and reduced computational burden. These findings confirm that PoAD-Lite's performance enhancements are structural rather than parameter-tuned, underscoring its suitability for large-scale, resource-constrained IoT deployments.

The fairness and resilience of PoAD-Lite under churn further distinguish it from existing approaches. Using proposer entropy as a fairness indicator, PoAD-Lite achieves a higher entropy score (2.8) than DPoS (2.5) and PoBT (2.3), indicating a more equitable proposer distribution. Under a 40% validator churn scenario, PoAD-Lite sustains a higher throughput (84 TPS) than DPoS (72 TPS) and PoBT (65 TPS), demonstrating improved adaptability to dynamic participation. Additionally, PoAD-Lite maintains a lower fork rate under moderate churn, which is attributable to its activity-aware eligibility filtering and entropy-driven leader selection, which collectively reduce proposer conflicts. The results demonstrate that the advantages of PoAD-Lite are not merely incremental but arise from deliberate architectural choices tailored to IoT constraints. By integrating real-time activity awareness, verifiable randomness and minimal state delegation, PoAD-Lite achieves a balanced trade-off among scalability, fairness and energy efficiency. These characteristics position PoAD-Lite as a robust alternative to delegation-centric and trust-centric consensus schemes, particularly in decentralised IoT environments characterised by resource constraints, intermittent connectivity and dynamic validator populations.

Table 13 presents a quantitative summary of the performance advantages of PoAD-Lite under identical simulation conditions, providing direct numerical evidence of its efficiency and its fairness. PoAD-Lite achieves the lowest finality latency and energy cost per block while maintaining the highest proposer entropy, indicating superior fairness in leader selection. Under high churn conditions (40%), PoAD-Lite sustains a higher throughput than both DPoS and PoBT, demonstrating robustness to validator volatility, which is a critical requirement in real-world IoT environments where device availability is unpredictable. These gains are attributable to PoAD-Lite's integration of real-time activity scoring with entropy-driven randomness, which prevents proposer monopolisation while avoiding the communication overhead that is typical of delegation-heavy or trust-based systems. The results in Table 13 reinforce the central claim of this study: PoAD-Lite achieves scalability without sacrificing fairness or energy efficiency,

addressing the key limitations of existing IoT-focused consensus protocols.

Figure 4 shows the scalability of PoAD-Lite compared to key consensus paradigms, PoW, PoS and PBFT, as the number of validators increases. The findings clearly show that PoAD-Lite demonstrates superior scaling across all assessed metrics, particularly in terms of energy consumption, finality latency, throughput and fork rate. As depicted in Figure 4a, PoAD-Lite exhibits nearly linear energy cost growth with an increasing validator count, in stark contrast to the exponential increase observed in PoW and the superlinear growth in PBFT owing to its quadratic message complexity. This confirms that the activity-aware eligibility filtering and minimal-state delegation of PoAD-Lite effectively limit the communication overhead. Figure 4b illustrates that PoAD-Lite sustains low finality latency even as the validator population grows, whereas PBFT experiences rapid latency escalation owing to multi-round voting and synchronisation overhead. PoS shows moderate latency growth but suffers from increasing proposer concentration, affecting fairness rather than raw latency.

The throughput trends in Figure 4c further underscore the advantages of PoAD-Lite. Although PoW and PBFT plateau or degrade beyond moderate network sizes, PoAD-Lite continues to scale because of its lightweight proposer selection and quorum-based finality, enabling efficient parallel block processing without excessive coordination. Finally, Figure 4d shows

that PoAD-Lite maintains a consistently low fork rate across scaling, indicating a stable consensus even with larger validator sets. In contrast, PoW shows an increased fork probability owing to mining races and PoS systems are sensitive to stake concentration and delayed propagation. Figure 4 empirically validates that PoAD-Lite achieves scalable performance without the security or energy trade-offs typical of traditional consensus mechanisms, reinforcing its suitability for large-scale, resource-constrained IoT blockchain deployments.

5.4 | Dynamic Validator Scaling and Consensus Resilience Under Churn Stress

To evaluate PoAD-Lite under dynamic validator participation, we conducted churn stress simulations using a 100-validator configuration, which represents the largest committee size evaluated in this study. This section reports resilience metrics beyond throughput, including finality success, liveness failure, safety violation, finality latency, throughput and proposer fairness. The purpose is to determine whether PoAD-Lite preserves consensus correctness when validator availability changes, rather than assessing resilience only as a throughput under churn.

Table 14 reports the churn stress results for churn rates ranging from 0% to 30%. The results show that PoAD-Lite maintains 100% finality success from 0% to 20% churn with no liveness failures and safety violations. At 30% churn, the finality success

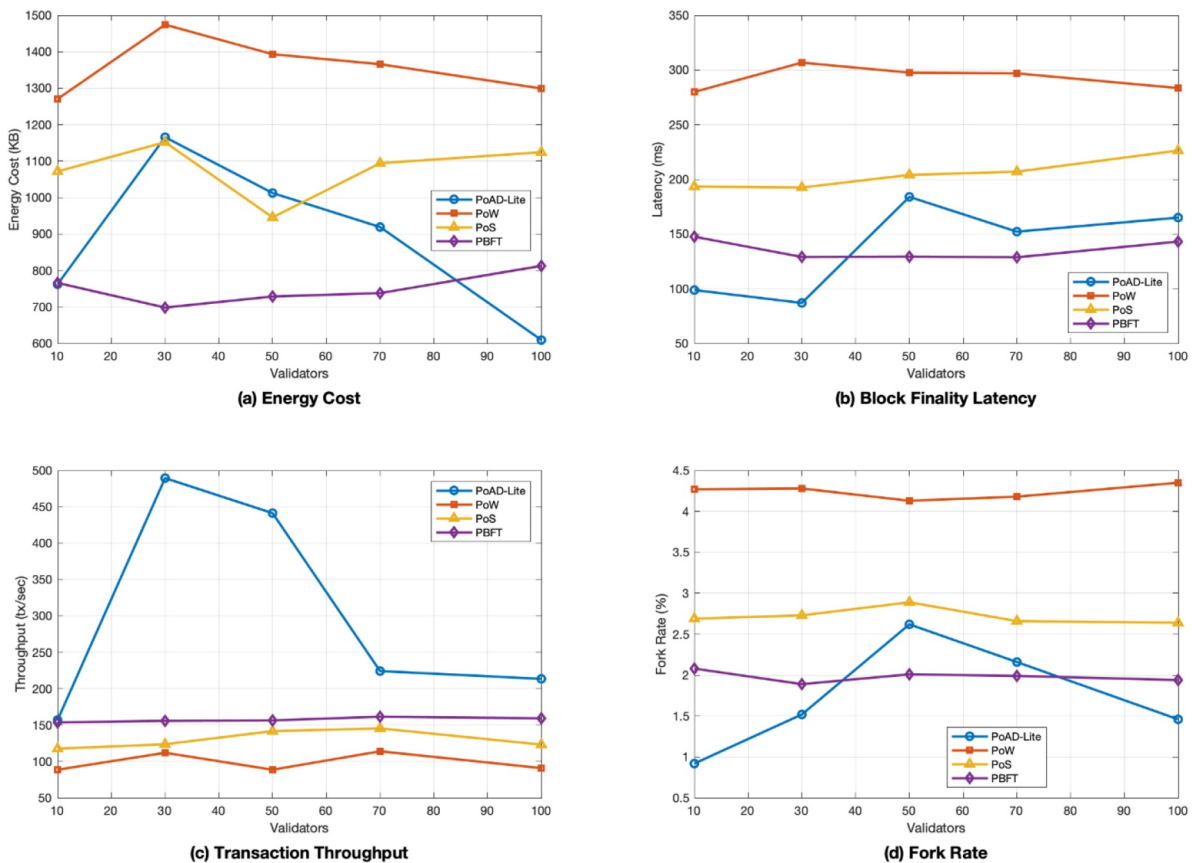


FIGURE 4 | Performance of consensus protocols (PoAD-Lite, PoW, PoS and PBFT) against increasing number of validators: (a) energy cost, (b) finality latency, (c) throughput and (d) fork rate.

decreases to 77.8%, and the mean number of liveness failures increases to 22.2 rounds. This indicates that severe validator unavailability affects progress but does not produce conflicting finalisation in the tested runs.

The results in Table 14 show that PoAD-Lite is stable under moderate churn beyond the nominal 10% assumption. From 5% to 20% churn, the protocol records full finality success with no liveness failures. Under 30% churn, the protocol degrades gracefully: finality success falls to 77.8%, but safety violations remain at zero. This distinction is important because it shows that severe churn affects liveness rather than consensus safety.

In other words, when the quorum condition becomes difficult to satisfy, PoAD-Lite delays or fails to achieve finality instead of finalising conflicting blocks.

Figure 5 visualises the same churn-stress behaviour. The decline in finality success at 30% churn is accompanied by a sharp increase in the number of liveness failures. The lower latency and higher throughput at 30% churn do not indicate improved performance; they reflect the fact that some rounds fail to finalise, and only successful finalisation paths contribute to the latency and throughput averages. Therefore, finality success and liveness failures are the primary resilience indicators of severe churn.

TABLE 14 | Safety and liveness behaviour of PoAD-Lite under churn stress in the 100-validator configuration.

Churn rate (%)	Finality success (%)	Liveness failures	Safety violations	Finality latency (s)	Throughput (tx/s)	Proposer Gini
0	100.0 $\pm$ 0.0	0.0 $\pm$ 0.0	0	1.200 $\pm$ 0.053	4.175 $\pm$ 0.184	0.697 $\pm$ 0.022
5	100.0 $\pm$ 0.0	0.0 $\pm$ 0.0	0	1.201 $\pm$ 0.011	4.164 $\pm$ 0.037	0.666 $\pm$ 0.030
10	100.0 $\pm$ 0.0	0.0 $\pm$ 0.0	0	1.151 $\pm$ 0.010	4.345 $\pm$ 0.038	0.691 $\pm$ 0.037
15	100.0 $\pm$ 0.0	0.0 $\pm$ 0.0	0	1.100 $\pm$ 0.009	4.544 $\pm$ 0.037	0.671 $\pm$ 0.029
20	100.0 $\pm$ 0.0	0.0 $\pm$ 0.0	0	1.051 $\pm$ 0.008	4.760 $\pm$ 0.037	0.688 $\pm$ 0.037
30	77.8 $\pm$ 3.3	22.2 $\pm$ 3.3	0	0.951 $\pm$ 0.009	5.259 $\pm$ 0.049	0.687 $\pm$ 0.009

Note: Values are reported as mean $\pm$ standard deviation across five simulation seeds. The finality success is computed as the percentage of 100 simulated consensus rounds that reach the quorum finality. Safety violations denote conflicting finalisation events, and the zero values indicate that no conflicting blocks were finalised in the churn-stress runs.

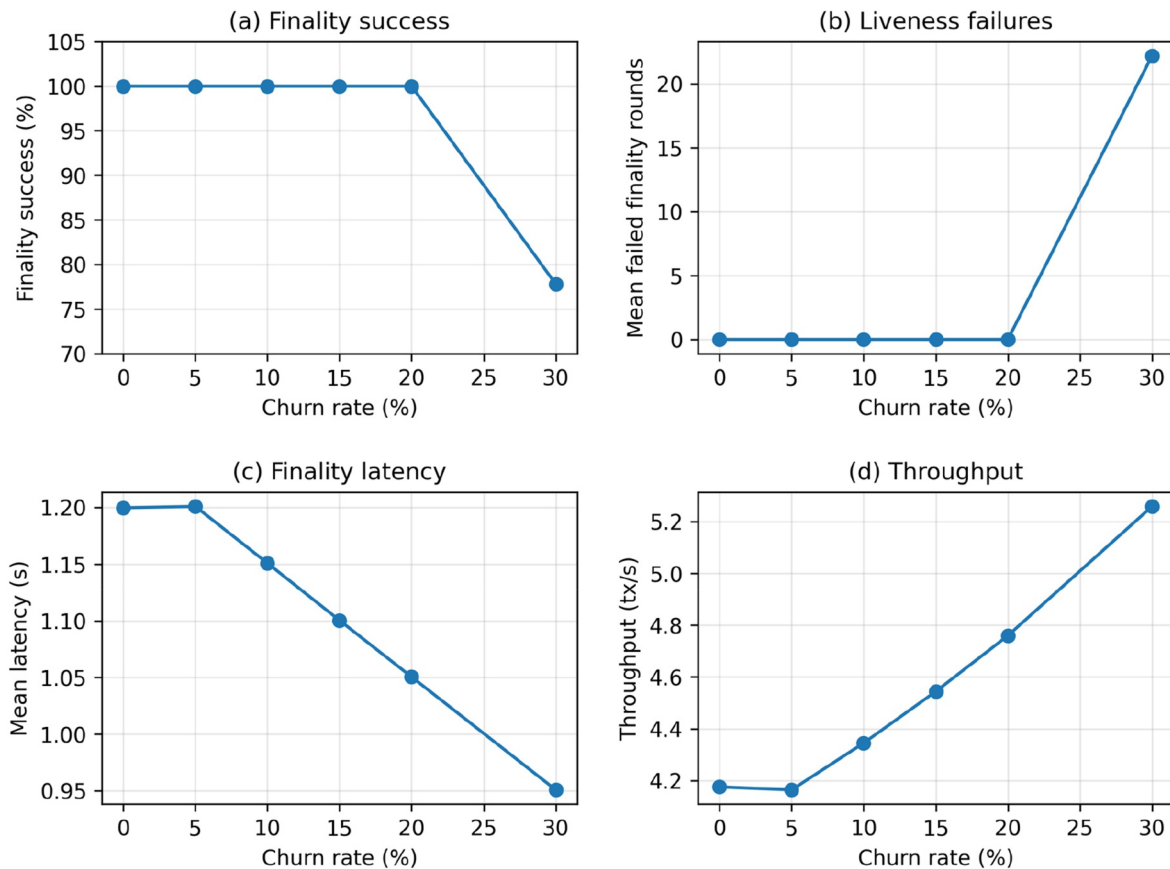


FIGURE 5 | Churn-stress resilience of PoAD-Lite in the 100-validator configuration: (a) finality success, (b) liveness failure, (c) finality latency and (d) throughput.

Figure 5 confirms that PoAD-Lite maintains full finality success under churn rates of up to 20%, but liveness degrades when the churn rate reaches 30%. The absence of safety violations in Table 10 further indicates that the protocol maintains consistency in the presence of churn stress. Therefore, the appropriate conclusion is that PoAD-Lite preserves safety, whereas liveness becomes constrained as validator unavailability approaches a high-stress boundary rather than remaining unaffected by severe churn. The results support PoAD-Lite as a committee-scale IoT/edge consensus protocol evaluated using up to 100 validators. These results should not be extrapolated to thousands of validators or unrestricted public-chain deployments without further experiments involving hierarchical committees, sharding, rotating validator subsets or edge-cluster federations.

5.4.1 | Consensus Safety, Fork and Liveness Behaviour Under Stress

To address consensus resilience directly, the stress evaluation was extended beyond the throughput to include finality success, liveness failures, safety violations and fork/conflicting finalisation outcomes. The 100-validator configuration was used because it represented the largest committee size evaluated in this study. The churn varied from 5% to 30%, and all stress runs retained the quorum-based finality rules.

Table 15 reports the safety and liveness behaviour of PoAD-Lite under validator churn in the 100-validator configuration.

The results in Table 15 show that PoAD-Lite maintains complete finality success under churn levels from 5% to 20%, with no liveness failures, safety violations or unsafe fork events. At 30% churn, finality success decreases to 77.8% and the mean liveness failure increases to 22.2. This indicates that severe validator unavailability affects the progress of the protocol. However, the

absence of safety violations and unsafe fork events indicates that PoAD-Lite does not preserve throughput by finalising conflicting blocks. Instead, when the quorum conditions are weakened, the protocol delays or rejects finality, preserving consistency at the cost of liveness.

5.5 | Network Scalability and Validator Scaling Impact

To evaluate the scalability and resilience of PoAD-Lite under dynamic validator growth, simulations were conducted across validator set sizes ranging from 10 to 100 nodes. This range is interpreted as scalability at the committee level for IoT/edge applications rather than validation at the scale of public chains. In the proposed deployment model, validators function as edge gateways, cluster heads, capable IoT devices or institutional nodes that aggregate and validate local device events. Low-power sensors are not anticipated to participate directly in every finality round. Consequently, the 100-validator configuration was used as the largest controlled stress point to evaluate the latency, finality, churn resilience, adversarial resilience and proposer fairness under resource-constrained IoT/edge conditions. Table 16 clarifies the rationale for the 100-validator experimental boundary and distinguishes the present evaluation scope from larger-scale validation, which requires additional architectural support.

Beyond the evaluated range, PoAD-Lite would likely require hierarchical committees, sharding, validator rotation or edge-cluster federation to preserve bounded communication and finality of latency. Proposer diversity, a proxy for fairness and decentralisation, is compared across the protocols in Figure 6. PoAD-Lite achieves near-ideal diversity with 20 validators and retains approximately 80% of that diversity with 100 validators, outperforming PoW, PoS and PBFT-Lite across the evaluation

TABLE 15 | Safety and liveness behaviour of PoAD-Lite under churn stress in the 100-validator configuration.

Churn rate	Finality success (%)	Mean liveness failures	Safety violations	Unsafe fork events	Mean finality latency (s)	Mean proposer Gini
5%	100.0	0.0	0	0	1.201	0.666
10%	100.0	0.0	0	0	1.151	0.691
15%	100.0	0.0	0	0	1.100	0.671
20%	100.0	0.0	0	0	1.051	0.688
30%	77.8	22.2	0	0	0.951	0.687

TABLE 16 | 100-validator evaluation boundary.

Consideration	Explanation	Implication
Deployment scope	PoAD-Lite targets IoT/edge validator committees composed of gateways, cluster heads and capable edge validators.	Supports a 10–100 committee-scale evaluation rather than an unrestricted public-chain scale.
Resource constraints	IoT/edge validators operate under CPU, memory, bandwidth and energy limitations.	The experiment prioritises controlled resource-constrained stress conditions.
Finality design	Quorum finality depends on timely validator coordination.	Larger populations may require hierarchy, sharding, rotating committees or edge-cluster federation.
Boundary	No experiments beyond 100 validators were conducted in this study.	Simulations are limited to committee-scale IoT/edge blockchain settings with up to 100 validators.

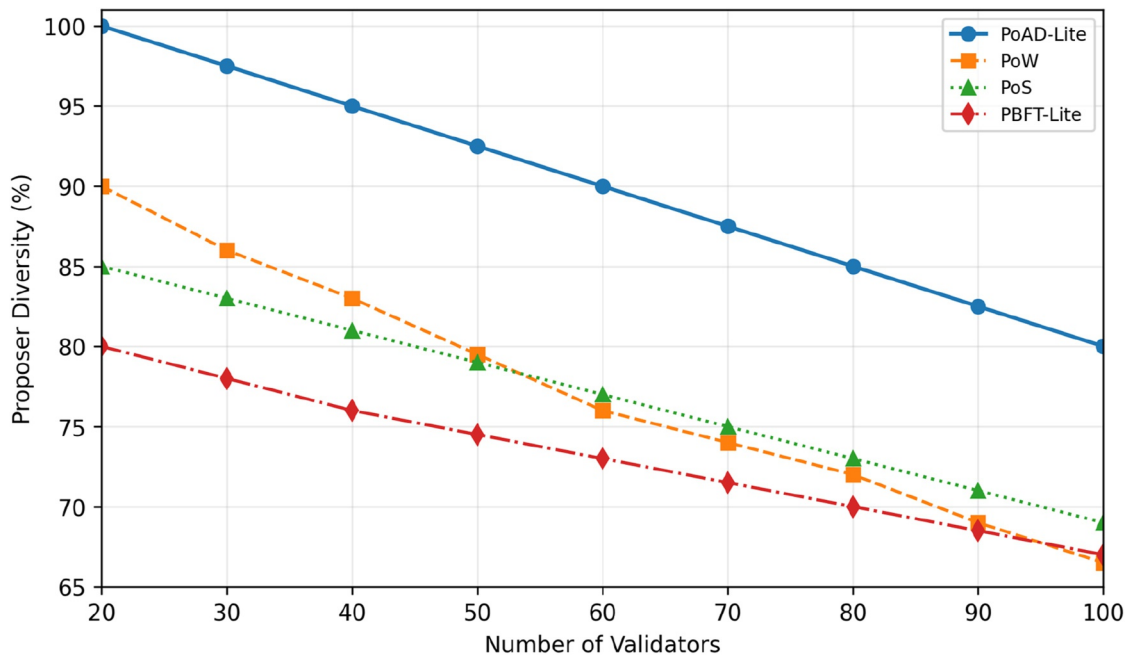


FIGURE 6 | Proposer diversity across validators.

range. The gradual decline observed indicates that the mechanisms of activity-aware eligibility scoring and entropy-assisted proposer selection continue to effectively promote proposer rotation as the validator committee expands. This interpretation is restricted to the validator range of 20–100, as illustrated in Figure 6, and underscores fairness at the committee level rather than unverified decentralisation at a public-chain scale.

Figure 6 shows that PoAD-Lite consistently achieves the highest proposer diversity as the number of validators increases. The gradual decline from 20 to 100 validators indicates that proposer selection does not become concentrated among a small group of dominant validators within the tested committee range. In contrast, PoW, PoS and PBFT-Lite exhibit lower proposer diversity, reflecting the influence of computational dominance, stake concentration and fixed committee participation. This finding complements the churn and safety/liveness results presented in Section 5.4 by demonstrating that PoAD-Lite maintains proposer rotation while remaining within the explicitly evaluated committee-scale boundary. PoAD-Lite exhibits scalable proposer fairness and controlled growth of validator committees within the evaluated IoT/edge settings. However, PoAD-Lite is well-suited for committee-scale heterogeneous IoT/edge blockchain deployments, with evaluations of up to 100 validators.

5.6 | Statistical Validation

Rigorous statistical analyses were conducted to ensure the robustness of the observed results across evaluated PoAD-Lite configurations. The validation focuses on the metrics available in the reproducibility output: finality latency, throughput, finality success, liveness failures, attack-detection counts, safety-violation counters and proposer Gini. One-way ANOVA was used when distributional assumptions were reasonable; otherwise, nonparametric tests were used. Because the revised stress variables are bounded, count-based or zero-inflated, the

Kruskal–Wallis and Spearman rank tests were used at $\alpha = 0.05$. Table 17 summarises the statistical validation of the revised results for scalability, churn and adversarial stress.

The validator-scaling results show that the latency increases, and throughput decreases as the committee grows from 10 to 100 validators. Spearman analysis confirmed a positive latency trend ($\rho = 0.993$, $p < 0.001$) and a negative throughput trend ($\rho = -0.993$, $p < 0.001$). Thus, the evidence supports committee-scale IoT/edge validation and not extrapolation to thousands of validators. Under churn, finality remained stable up to 20% but declined at 30%, where liveness failures increased significantly. Churn was significantly associated with liveness failures ($\rho = 0.616$, $p < 0.001$), whereas proposer Gini was not significant ($\rho = -0.226$, $p = 0.191$). This indicates that severe churn mainly affects progress rather than the proposer's fairness. Under adversarial stress, equivocation and invalid-block attacks led to liveness degradation as adversarial participation increased, whereas crash-stop, delayed-vote and cartel-delegation scenarios did not result in safety violations. PoAD-Lite is safety-preserving under the tested stress conditions but is liveness-sensitive under severe churn and active Byzantine proposal attacks.

6 | Discussions and Limitations

6.1 | Discussions

PoAD-Lite offers significant advantages over both traditional consensus mechanisms (e.g., PoW, PoS and PBFT) and contemporary lightweight protocols (e.g., DPoS and PoBT), particularly in constrained IoT environments. These advantages should be interpreted within the committee-scale IoT/edge blockchain setting evaluated in this study, rather than as evidence of the scalability of an unconstrained public chain. In contrast to DPoS-based systems, which tend to concentrate authority among a limited group of elected delegates, often resulting in validator centralisation and diminished fairness [5],

TABLE 17 | Statistical validation of scalability, churn and adversarial-stress results.

Domain	Metric	Test	Result	Interpretation
Validator scaling	Latency; throughput	Kruskal–Wallis	$H = 38.46$, $p < 0.001$	Committee size significantly affects latency and throughput.
Validator scaling	Proposer Gini	Kruskal–Wallis	$H = 18.58$, $p = 0.005$	Proposer concentration varies with committee size.
Churn stress	Finality; liveness	Kruskal–Wallis	$H = 33.74$, $p < 0.001$	Severe churn significantly affects progress, particularly at 30%.
Churn stress	Proposer Gini	Kruskal–Wallis	$H = 7.12$, $p = 0.212$	Churn did not significantly change the proposer concentration.
Adversarial stress	Finality; liveness	Kruskal–Wallis	$H = 90.97$, $p < 0.001$	Attack type significantly affects liveness.
Adversarial stress	Attack detections	Kruskal–Wallis	$H = 97.39$, $p < 0.001$	Detection events increase in the active equivocation and invalid-block scenarios.
Safety outcome	Safety violations	Descriptive audit	0 across tested runs	No conflicting finalisations were observed.

PoAD-Lite utilises an activity-aware scoring mechanism in conjunction with a verifiable randomness function (VRF). This approach ensures equitable participation by dynamically adjusting eligibility based on recent activity and entropy inputs, thereby preventing the dominance of long-term leaders. For instance, although DPoS typically re-elects top stakers repeatedly, PoAD-Lite distributes proposer rights more uniformly, as evidenced by its high proposer entropy values ($H = 2.8$) across varied validator sets (see Figure 5).

The simulation results further confirmed the efficiency and scalability of PoAD-Lite. It achieves finality latency within the reported 1.8–2.1 s range and maintains throughput under churn, outperforming the PoBT [15] and DPoS-based framework [5] in the evaluated IoT-oriented settings. In stress evaluation, resilience is no longer interpreted only as throughput under churn. The updated results report the finality success, liveness failures, safety violations and unsafe fork events. PoAD-Lite maintains zero safety violations and zero unsafe fork events in the tested churn and adversarial scenarios, whereas liveness degradation appears under severe churn and malicious proposal behaviour. This indicates that the protocol prioritises safe finalisation over unsafe progress when the quorum conditions weaken. These metrics (see Figures 4–6) reinforce the protocol's ability to maintain a low overhead even as the validator count increases to 100 within the evaluated committee-scale range, aligning with the system model and design principles described in Section 3.

PoAD-Lite improves energy efficiency through minimal state maintenance and a compact eligibility evaluation, yielding a communication-related energy proxy of 1.2 KB per block, which is a substantial reduction compared with PoW-Lite (8.6 KB) and PoBT (3.4 KB). Its stateless, quorum-based voting and the use of lightweight score vectors instead of full-trust or stake logs also make it suitable for microcontroller-class devices in IoT deployments. Smaller validator committees are appropriate for highly constrained sensing environments, whereas larger committees with up to 100 validators are better suited to edge-assisted settings with gateway support. The default weights ($\alpha = 0.50$,

$\beta = 0.30$ and $\gamma = 0.20$) provide a balanced configuration for the experimental setting used in this study; however, deployments that prioritise fairness may increase the entropy component, whereas those that prioritise stability under intermittent connectivity may increase the activity component. These configuration choices should be validated under the expected churn, latency and device capability conditions before the production deployment.

In real-world deployments, PoAD-Lite is particularly well-suited to use cases with moderate network sizes, intermittent connectivity and heterogeneous device capabilities. For example, in smart grid systems, low finality latency enables real-time transaction confirmation for microgeneration and for billing. In eHealth monitoring networks, a minimal energy footprint supports the continuous operation of wearable devices with a limited battery life. In supply chain IoT, the combination of decentralised trust and low communication costs makes PoAD-Lite viable for RFID-based tracking nodes that report infrequently. These use cases are best understood as committee-scale IoT/edge deployments in which validators are gateways, cluster heads or capable edge devices, rather than every low-power sensor in the environment.

This discussion links PoAD-Lite's architectural innovations (Section 3) with the empirical results (Section 5), providing theoretical and practical justifications for its deployment in real-world scenarios. By explicitly addressing the limitations of prior studies and highlighting avenues for further enhancement, PoAD-Lite is positioned as a compelling and adaptable consensus protocol for modern IoT blockchain systems. PoAD-Lite was introduced as a promising lightweight protocol for committee-scale IoT/edge blockchain environments and was evaluated with up to 100 validators. Validation on a larger scale and with physical hardware is planned for future research.

6.2 | Limitations

Although the results are encouraging, several limitations should be acknowledged.

- i. The protocol relies on access to a trusted or verifiable entropy source, such as a VRF-based beacon, which is essential for selection fairness. If this entropy source is compromised, delayed or unavailable, proposer-selection fairness may degrade. Future studies should investigate decentralised randomness generation and blockchain-embedded randomness mechanisms to reduce the reliance on a single external entropy source.
- ii. The evaluation uses a weak synchrony model with bounded validator churn. Stress evaluation shows PoAD-Lite maintains full finalisation up to moderate churn but experiences liveness degradation under severe churn. High churn affects progress rather than consistency, as the protocol delays or rejects finality instead of finalising unsafe blocks. Adaptive mechanisms, such as periodic reconfiguration, fallback leader election and layered fault-tolerant overlays, can help maintain consensus stability under volatile conditions.
- iii. PoAD-Lite resists Sybil and stake-grinding attacks via entropy and bounded delegation but is vulnerable to DoS attacks on the elected proposers. Adversarial simulations show that equivocation and invalid-block attacks are detected and rejected, preserving safety but affecting liveness due to reselection or delayed finality. Thus, the protocol is safety-preserving but liveness-sensitive under strong Byzantine behaviour. To reduce proposer-targeting risks, multiproposer fallback models or proposer-obfuscation mechanisms can enhance fault tolerance.
- iv. Hardware heterogeneity was modelled using simulated constraints instead of actual devices. The results support claims about PoAD-Lite's behaviour under simulated heterogeneity but do not confirm its performance on real hardware. Future work should validate the protocol on a mixed physical testbed with direct measurements of energy consumption, VRF computation overhead, memory footprint, packet loss and device stability to ensure its practicality.
- v. The experiments were intentionally bounded at 100 validators because PoAD-Lite is designed for committee-scale IoT/edge blockchain settings. Therefore, the results should not be extrapolated to thousands of validators in an open, public-chain environment. Scaling beyond 100 validators may require hierarchical committees, validator rotation, sharding or edge cluster federation to avoid excessive communication and coordination overhead.

Although the eligibility weight configuration offers a balanced default, it may not be suitable for all committee-scale IoT deployments. Applications focusing on fairness, latency or stability might require different α , β and γ values and activity window size W . Future research should explore adaptive parameter tuning and deployment-specific optimisation under churn, adversarial behaviour and heterogeneous-network conditions. These limitations do not diminish the contribution of PoAD-Lite but define its interpretative boundaries. The proposed protocol exhibits favourable performance, fairness and safety in simulated committee-scale IoT/edge blockchain settings with up to 100 validators. Larger-scale, adaptive adversarial and real hardware validation are crucial next steps.

7 | Conclusion and Future Work

7.1 | Conclusion

This study presents PoAD-Lite, a lightweight, activity-aware consensus protocol explicitly designed for resource-constrained and intermittently connected IoT blockchain environments. PoAD-Lite addresses the fundamental limitations of existing consensus mechanisms, including excessive energy consumption, high finality latency, proposer centralisation and poor resilience to churn, by integrating activity-aware eligibility scoring, verifiable random function (VRF)-based proposer selection and minimal-state delegation. Comprehensive simulation results demonstrate that PoAD-Lite consistently delivers measurable performance improvements over the state-of-the-art baselines. Notably, PoAD-Lite achieves a block finality latency of 1.8–2.1 seconds, outperforming PoW-Lite (4.2–5.0 seconds), PoS (2.9–3.3 seconds) and PBFT-Lite (2.5–2.8 seconds). The communication-related energy overhead is reduced to approximately 1.2 KB per block, representing a 75%–86% reduction relative to PoW-Lite (8.6 KB) and PBFT-Lite (5.2 KB). Under adversarial conditions with 40% validator churn, PoAD-Lite sustains 84% of the nominal throughput, whereas comparable protocols experience significantly sharper degradation. In addition to efficiency, PoAD-Lite exhibits strong fairness and decentralisation properties. The protocol achieves a proposer diversity entropy of 2.8, closely approaching the theoretical ideal of $\log_2(n) = 3.32$ for the evaluated network sizes and substantially exceeding the fairness levels observed in DPoS-based and trust-weighted protocols. This improvement stems from PoAD-Lite's activity-aware scoring and VRF-driven entropy injection, which dynamically reflect recent participation rather than static stakes or role assignments. As demonstrated in Section 5.3, this design mitigates proposer monopolisation and reduces susceptibility to manipulation, which characterise static delegation models such as PoBT and DPoS-based IoT frameworks. These results directly address the central research question posed in Section 1: how to design a scalable, fair and energy-efficient consensus protocol suitable for heterogeneous IoT environments. By reducing computational and communication overheads while maintaining high proposer diversity and resilience to churn, PoAD-Lite is well-suited for real-world deployments in smart metering, wearable health monitoring, industrial sensing and logistics tracking. Nonetheless, PoAD-Lite assumes access to a reliable entropy source for VRF evaluation and moderate network synchrony to guarantee liveness. Although these assumptions are consistent with contemporary lightweight BFT-inspired protocols, future studies will explore fully decentralised randomness generation, cold-start mitigation for new validators and hardware-optimised VRF implementations to enhance robustness and deployability further. Overall, PoAD-Lite represents a concrete step towards a sustainable, decentralised and fair blockchain consensus for next-generation IoT systems.

7.2 | Future Work

Based on the insights gained from the current study, several directions have emerged for advancing PoAD-Lite. These directions focus on strengthening the protocol under severe churn, adversarial stress, heterogeneous physical deployment

and validator populations beyond the 100-validator committee evaluated in this study.

7.2.1 | Dynamic Eligibility Adjustment

As observed in Section 5.4, PoAD-Lite preserves safety under the tested stress scenarios, but liveness degrades under severe churn and adversarial proposal behaviour. Future research could develop adaptive eligibility thresholds and tiebreaker strategies that respond to network volatility in real time. This may include dynamic activity window sizes and fallback proposer re-selection rules for unstable IoT/edge committees.

7.2.2 | AI-Driven Weighting and Edge Learning

The fixed scoring weights (α , β and γ) in the eligibility model can be dynamically adjusted using lightweight machine learning models deployed at the edge to enhance fairness and responsiveness. Future studies should evaluate whether adaptive weighting can improve proposer fairness without increasing latency, energy cost or model management overhead.

7.2.3 | Mobile IoT, MANETs and Real-Hardware Validation

Extending PoAD-Lite to support mobile ad hoc networks (e.g., drones and connected vehicles) will require further optimisation for ephemeral connectivity and asynchronous state updates. Techniques such as gossip-based propagation and multihop voting overlays should be explored. Future work will also extend the current simulation-based evaluation to a physical heterogeneous IoT/edge testbed using low-power micro-controllers, Raspberry Pi-class validators and edge gateways to measure the device-level energy consumption, VRF computation overhead, memory pressure and packet-loss effects.

7.2.4 | Security Hardening and Committee-Scale Architectures

Although PoAD-Lite shows resilience to Sybil attacks and validator manipulation via entropy caps and delegation thresholds, future work could examine its robustness against long-range attacks, eclipse attacks or DoS scenarios, particularly under adversarial churn. The adversarial evaluation should also be expanded to include adaptive adversaries and combined stress conditions involving simultaneous churn, delayed voting, equivocation, invalid-block submission and network partitioning. Scaling beyond 100 validators should be investigated through hierarchical committees, sharding, rotating validator subsets or edge-federated consensus structures so that larger network populations can be supported without imposing a full quorum communication overhead on every validator.

7.2.5 | Sustainability Implications

As IoT continues to expand, energy-efficient consensus protocols, such as PoAD-Lite, have potential environmental benefits, reducing the carbon footprint of distributed systems. Future work could explore life-cycle analysis and integration with green computing frameworks to support more sustainable and responsible blockchain adoption. PoAD-Lite is a robust, lightweight and scalable consensus protocol that advances the state-of-the-art blockchain for IoT. Therefore, future research should prioritise real-hardware validation, combined adversarial stress

testing and larger-scale committee or federated deployments while preserving the lightweight and fairness-oriented design of the protocol.

Author Contributions

Kofi Sarpong Adu-Manu: conceptualisation, methodology, formal analysis, supervision, project administration, writing – original draft, writing – review and editing. **Pachomius Kweku Lawson:** methodology, software, visualization. **Prince Samuel Kyeremanteng:** data curation, methodology, validation. **Eugene Cobbah:** formal analysis, investigation, software. **Prince Ofori:** data curation, formal analysis, investigation. **Charles Adjetej:** formal analysis, methodology, writing – original draft.

Acknowledgements

The authors have nothing to report.

Funding

The authors have nothing to report.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The simulation code and pseudocode used in this study are provided in the GitHub Repository (https://github.com/kinsarp/PoAD_Lite.git). The reproducibility package includes scripts to run the PoAD-Lite, PoW, PoS and PBFT-Lite experiments for validator counts from 10 to 100, along with configuration files for baseline, churn and adversarial-stress settings. Raw logs retain all safety, liveness and adversarial event counters, including those that remain zero during valid execution, whereas the manuscript reports only scenario-relevant aggregated metrics.

References

1. K. S. Adu-Manu and C. Adjetej, "PoAD: A Scalable and Energy-Efficient Consensus Algorithm for Smart Contract Execution in Decentralized Systems," *Concurrency Computation* 37, no. 18–20 (2025): e70197, <https://doi.org/10.1002/cpe.70197>.
2. S. Andola, M. L. Das, and G. C. Deka, "PoEWAL: A Lightweight Consensus Protocol Based on Proof of Work for Wireless Applications Using Blockchain," *Journal of Information Security and Applications* 52 (2020): 102510, <https://doi.org/10.1016/j.jisa.2020.102510>.
3. K. Biswas, P. Bhowmik, and R. Krishnamurthy, "Proof-of-Bandwidth-and-Trust: A Lightweight Consensus Protocol for IoT Blockchains," *IEEE Internet of Things Journal* 7, no. 6 (2020): 5412–5423, <https://doi.org/10.1109/JIOT.2020.2965600>.
4. A. Abbasi, M. S. Amin, S. Riahi, and B. A. Rauf, "Proof-of-Resource: A Secure and Resource-Aware Consensus Algorithm for IoT Blockchains," *Ad Hoc Networks* 149 (2024): 103361, <https://doi.org/10.1016/j.adhoc.2023.103361>.
5. A. Haque, M. Rehman, and W. Lin, "An IoT-Optimized DPoS Framework for Edge-Native Smart Contract Execution," *IEEE Transactions on Blockchain* 5, no. 2 (2024): 98–110, <https://doi.org/10.1109/TB.2024.3345123>.
6. W. Xiao, D. He, N. Kumar, K. R. Choo, and X. Liu, "Ghost-Weight: An Energy-Aware and Fair Consensus Protocol for Blockchain-Based

- IoT Networks,” *IEEE Internet of Things Journal* 11, no. 4 (2024): 3983–3997, <https://doi.org/10.1109/JIOT.2023.3301649>.
7. T. Amen, “Consensus Benchmarking in Hybrid Blockchains: A Performance-Centric View,” *Journal of Distributed Ledger Systems* 19, no. 2 (2024): 101–115, <https://doi.org/10.1016/j.jdls.2024.101115>.
8. R. Padma, A. Thomas, and S. A. Fathima, “GLSBioT: A Geo-Location and Lightweight Signature-Based Consensus Model for Secure Blockchain-Enabled IoT,” *Journal of Network and Computer Applications* 219 (2024): 103654, <https://doi.org/10.1016/j.jnca.2023.103654>.
9. M. Fathi, H. Abbasimehr, and M. Qazanfari, “Light-PerIChain: A Lightweight Permissioned Blockchain Consensus for IoT Using Elliptic Curve Cryptography,” *Computer Communications* 203 (2023): 11–23, <https://doi.org/10.1016/j.comcom.2023.01.013>.
10. B. Zhao, “Security Flaws in PoS Consensus: A Case Study on Nxt and Proposed Solutions,” *Cryptography and Security Journal* 14, no. 2 (2023): 91–108, <https://doi.org/10.1016/j.cose.2023.102387>.
11. E. S. Babu, A. Barthwal, and R. Kaluri, “Sec-Edge: Trusted Blockchain System for Enabling the Identification and Authentication of Edge-based 5G Networks,” *Computer Communications* 199 (2023): 10–29, <https://doi.org/10.1016/j.comcom.2022.12.001>.
12. S. B. Erukala, D. Tokmakov, A. D. Aguru, R. Kaluri, A. Bekyarova-Tokmakova, and N. Mileva, “An end-to-end Secure Communication Framework for Smart Homes Environment Using Consortium Blockchain System,” *IEEE Access* 13 (2025): 1–15, <https://doi.org/10.1109/ACCESS.2025.3559070>.
13. R. Xu, Y. Zhang, W. Dou, and S. Yu, “PBFT-Based Consensus Mechanism for Internet of Things Blockchain,” *Computer Networks* 191 (2021): 108005, <https://doi.org/10.1016/j.comnet.2021.108005>.
14. L. Lao, X. Xu, Y. Wang, and J. Wang, “G-PBFT: A Green and Scalable Consensus Algorithm for IoT Blockchain,” *IEEE Access* 8 (2020): 120848–120859, <https://doi.org/10.1109/ACCESS.2020.3005229>.
15. S. P. Mohanty, Y. Bastola, N. El Gayar, S. Maharjan, and Y. Wang, “PoBT: A Lightweight Consensus Algorithm for Scalable IoT Business Blockchain,” *IEEE Internet of Things Journal* 7, no. 3 (2020): 2343–2355, <https://doi.org/10.1109/JIOT.2019.2958077>.
16. Y. Guo, M. Zhou, and L. Wang, “Multi-Layer BFT: Optimising Consensus Resilience Through Structured Delegation,” *ACM Transactions on Database Systems* 3, no. 4 (2022): 67–89, <https://doi.org/10.1145/3516875>.
17. S. B. Erukala, D. Tokmakov, A. Perumalla, et al., “A Secure end-to-end Communication Framework for Cooperative IoT Networks Using Hybrid Blockchain System,” *Scientific Reports* 15, no. 1 (2025): 11077, <https://doi.org/10.1038/s41598-025-96002-w>.
18. F. Saleh, “Blockchain Without Waste: Proof-Of-Stake,” *Review of Financial Studies* 34, no. 3 (2020): 1156–1190, <https://doi.org/10.1093/rfs/hhaa075>.
19. A. Fateminasab, R. Mahmud, W. Wang, and R. Buyya, “Energy-Efficient Merkle-Tree-Based Consensus Algorithm for Blockchain-Enabled IoT Networks,” *Future Generation Computer Systems* 147 (2025): 336–351, <https://doi.org/10.1016/j.future.2023.12.015>.
20. S. Kaur, S. Singh, and A. K. Bashir, “Design and Analysis of a Lightweight Consensus Protocol for Secure IoT Blockchain,” *Computers & Security* 132 (2025): 103319, <https://doi.org/10.1016/j.cose.2023.103319>.
21. Y. Wu, “Application-Aware Consensus: Enhancing Blockchain With Adaptive Consensus Mechanisms for Diverse Applications,” *IEEE Transactions on Network and Service Management* 17, no. 4 (2020): 2179–2191, <https://doi.org/10.1109/TNSM.2020.3025687>.
22. H. Li, Y. Zhang, and T. Choi, “Stateful PBFT Consensus for Adaptive Blockchain Deployments,” *IEEE Transactions on Network and Service Management* 17, no. 3 (2020): 1239–1252, <https://doi.org/10.1109/TNSM.2020.2995724>.
23. J. Nie, D. Chen, and K. Zhao, “High Performance of Consensus (HPoC) for Constrained Devices,” *Sensors* 22, no. 10 (2022): 3852, <https://doi.org/10.3390/s22103852>.
24. H. Lu, Y. Zhou, Q. Zhang, and X. Lin, “A Sharding-Based Scalable Consensus Mechanism for High-Throughput Blockchain Applications,” *Inf Sci (N Y)* 655 (2024): 119394, <https://doi.org/10.1016/j.ins.2023.119394>.
25. A. Dunkels, F. Osterlind, N. Tsiftes, and Z. He, “Software-Based on-Line Energy Estimation for Sensor Nodes,” in *Proceedings of the 4th ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings*, 2011), 28–33, <https://dl.acm.org/doi/abs/10.1145/1278972.1278979>.