Timor-Leste Journal of Engineering and Science

Vol.5, Issue 1, pp.23-30, 2026
Available online at: http://tljes.org/index.php/tljes/data

Blockchain-Based IoT Ecosystems: Design and Analysis of Incentive Mechanisms for Sustainable Participation

Jayashree. R
Department of Computer Science, Faculty of Engineering and Science, Dili Institute of Technology, Dili, Timor-Leste
E-Mail: jayashreeram77@gmail.com / jayashree@dit.edu.tl

ABSTRACT

Paradigms for decentralized, trust less data exchange and autonomous device collaboration are created by merging Blockchain (BC) and the Internet of Things (IoT). Limited resources and energy constraints are the factors for major challenges in achieving sustained participation of IoT devices in such decentralized networks. In this paper, we study incentive archetypes with IoT node participation in blockchain ecosystems. We emphasize the scalability, energy efficiency, and security implications along with token-based rewards, reputation systems, and hybrid incentive structures in this research work. Additionally, we propose an incentive framework integrated with an economic model for addressing challenges related to sybil resistance and incentive manipulation, known as Hybrid Sustainable Incentive Framework (HSIF). These challenges are analyzed with energy-based reward distribution using lightweight consensus and adaptive tokenomics, which assure sustainability and efficient IoT participations (Zimba et al., 2025). The main goal of this paper is to provide a roadmap for incentive design with IoT in decentralized blockchain networks.

Keywords: Blockchain, Internet of Things (IoT), Incentive Mechanisms, Tokenomics, Reputation Systems, Sustainability, Energy Efficiency

Received June 16, 2025; Revised Dezember 20, 2025; Accepted January 30, 2026

1. Introduction

The integration of blockchain with Internet-of-Things (IoT) infrastructures aim to provide decentralized trust, tamper-evident provenance, and automated settlements for device-to-device interactions. A recurrent theme in the literature is that economic incentives are crucial for bootstrapping and sustaining decentralized IoT networks, as they motivate private actors, such as device owners and gateway operators, to contribute resources like connectivity, computation, sensing (IoT), and storage (Khan et al., 2024; Obaidat et al., 2024). Tokenized reward systems in which devices or their human operators earn native tokens for verifiable contributions, represent one of the most widely adopted incentive mechanisms (Bertozzi et al., 2020; Rochman et al., 2023). The Helium network is a prominent example: it uses a Proof-of-Coverage (PoC) protocol to verify physical wireless coverage and mints tokens (HNT) to reward hotspot operators for providing LoRaWAN connectivity (Wang et al., 2022). While such token incentives have been shown to accelerate infrastructure deployment, empirical analyses of Helium also reveal associated operational and security challenges, underscoring the need for robust verification mechanisms.

Monetary incentives alone may not produce high-quality data or trustworthy data contributions (D'Aniello and Fotia, 2025; Maddikunta et al., 2022). As a result, reputation systems are proposed as either an alternative or a complement to token-based rewards. Decentralized reputation mechanisms stored on-chain (or anchored to chains) help reward sustained, honest participation and penalize low-quality or malicious contributors (Mahmoud et al., 2024). A major threat to both token- and reputation-based systems is the Sybil attack, in which adversaries generate multiple identities to exploit incentive mechanisms (Mohaisen and Kim, 2013; Oliveira et al., 2022). The literature documents three recurring defence patterns: (1) increasing the economic cost of identity through staking or bonding; (2) using physically-grounded proofs (e.g., Proof-of-Coverage, location/time challenges) to tie contributions to real-world constraints; and (3) employing hardware-based identity anchoring (TPM, secure elements) (Akashah Arshad et al., 2021; Zhang and Wen 2020).

Prior work explores energy-aware consensus and task offloading mechanisms to reduce on-device computation (Xu et al., 2021). Recognizing the limitations of any single incentive approach, a number of recent works propose hybrid incentive models that combine tokens, micropayments, reputation, and service-level-agreement (SLA) based smart contracts (Mays Alshaikhli et al., 2025).

Despite these advances, existing hybrid incentive models largely treat tokenomics, reputation, and energy efficiency as loosely coupled components, often relying on static reward rules and limited adaptability to heterogeneous device capabilities. Few approaches provide a unified framework that dynamically adjusts incentives based on both device energy constraints and contribution quality, while simultaneously addressing fairness and Sybil resistance. This lack of tightly integrated, adaptive, and energy-aware incentive design represents a key gap in current blockchain-enabled IoT research.

Vol.5, Issue 1, pp.23-30, 2026
Available online at: http://tljes.org/index.php/tljes/data

To address this gap, this paper proposes a Hybrid Sustainable Incentive Framework (HSIF) for blockchain-based IoT environments. Unlike prior hybrid approaches that combine multiple incentive mechanisms in a static or modular manner, HSIF tightly integrates adaptive tokenomics, decentralized reputation management, and energy-aware participation control within a unified framework. The proposed model employs adaptive reward functions that dynamically adjust incentives according to device energy levels and verified contribution quality, thereby promoting fairness, scalability, and long-term participation. Additionally, a decentralized reputation archetype is incorporated to enhance data trustworthiness and improve resistance to Sybil attacks.

The objectives of this study are as follows:

1. To investigate existing incentive models applied in blockchain-based IoT environments, including token-based, reputation-based, and hybrid mechanisms.
2. To identify key challenges affecting sustainable IoT participation.
3. To analyze the strengths, limitations, and performance trade-offs of current incentive models using theoretical and comparative perspectives.
4. To propose an energy-aware, hybrid incentive framework that integrates adaptive tokenomics and reputation systems for sustainable IoT engagement.
5. To evaluate the proposed model's feasibility in promoting fairness, scalability, and long-term participation through simulation or analytical modelling.

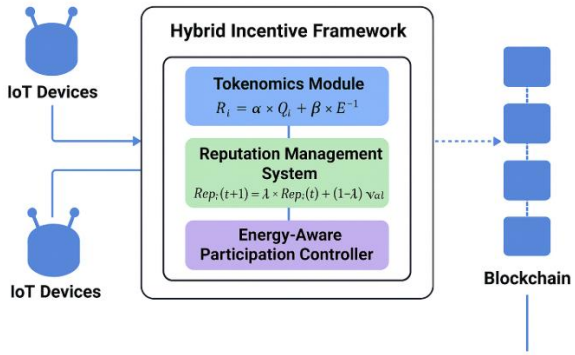

Figure.1 Data flow between IoT devices, the Blockchain layer, and the incentive modules

Figure.1 depicts the data flow between IoT devices, the Blockchain layer, and the incentive modules. Evaluation using simulation helps to demonstrate improved fairness, sustainability, and participation compared to traditional incentive models.

2. Literature Review

2.1 Overview of Blockchain–IoT Incentives

Several comprehensive surveys summarize the landscape of blockchain–IoT applications, identify incentive design as a core research focus, and emphasize the interplay between economic mechanisms and system constraints (latency, energy, and storage) (Al-Matari et al., 2024; Obaidat et al., 2024). Overall, these studies establish incentives as a foundational requirement but differ in how explicitly they integrate system-level constraints into incentive mechanisms.

2.2 Lightweight DLTs and DAG Architectures for IoT

Resource cost is the reason for preventing many IoT devices from participating continuously in the conventional blockchains. Directed Acyclic Graph (DAG) approaches and non-blockchain DLTs enable low-fee transactions for huge IoT devices, which are called micropayment-enabled IoT incentive models (Nzakuna et al., 2025). While these architectures reduce transaction overhead, they often rely on weaker consistency guarantees and introduce new trust and coordination challenges.

2.3 Micropayments, Layer-2, and Off-Chain Architectures

For fine-grained pay-per-use interactions (per-sensor-reading, per-packet forwarding, or short compute tasks), on-chain settlement is often impractical. The literature therefore emphasizes Layer-2 and payment-channel architectures (e.g., state channels, rollups, Lightning-like networks) to enable frequent, low-value transactions with low fees and low latency (Benedetti et al., 2025). Survey and systems papers show that payment channels are essential for viable M2M markets but also flag open problems in channel rebalancing, routing, and privacy when scaled to thousands or millions of devices. (Kang et al., 2025). These limitations suggest that micropayment efficiency alone is insufficient without complementary trust and verification mechanisms.

2.4 Reputation Systems and Trustable Data Markets

Recent surveys and prototype systems investigate blockchain-backed reputation for IIoT and data marketplaces, showing that reputation reduces reliance on volatile token values but raises its own challenges, namely collusion, long-term bias, and the difficulty of initializing trust for new entrants (Mahmoud et al., 2024). Compared to pure token-based approaches, reputation mechanisms improve data quality assurance but require careful integration to avoid reinforcing structural inequalities.

2.5 Sybil Resistance and Verification Mechanisms

Survey and experimental works show that hybrid defences combining economic and physical verification are more effective than any single measure, but they also increase onboarding costs and can reduce openness (Akashah Arshad et al., 2021). This trade-off between robustness and accessibility remains a recurring concern across incentive designs.

Vol.5, Issue 1, pp.23-30, 2026
Available online at: http://tljes.org/index.php/tljes/data

2.6 Energy-Aware Consensus and Sustainability Concerns

Empirical work suggests that embedding energy-awareness into incentives (rewarding energy-efficient behaviour, adapting duty cycles) materially extends device lifetime and thus improves long-term network participation. However, achieving a sound trade-off among energy, security, and decentralization remains an open problem (Wadhwa et al., 2022). Existing studies typically address energy efficiency at the protocol level rather than within adaptive incentive formulations.

2.7 Hybrid and Mechanism-Design Approaches

Mechanism-design and game-theoretic analyses have been applied to derive fair payment rules (e.g., Shapley-value allocations, Stackelberg formulations) in heterogeneous networks. While these theoretical approaches provide principled allocation rules, their practicality depends heavily on the availability of low-cost, verifiable metrics and efficient on/off-chain computation (Mays Alshaikhli et al., 2025). As a result, many hybrid models remain difficult to deploy in real-world IoT environments.

2.8 Empirical Deployments, Gaps, and Open Problems

Field deployments (Helium and other experimental networks) provide valuable empirical feedback: token incentives can generate rapid infrastructure growth but can also be gamed or destabilized without strong verification, sound tokenomics, and regulatory clarity (Enaya et al., 2025). From the literature, four research gaps are repeatedly highlighted: (1) energy-sensitive tokenomics that explicitly account for device lifetime in reward formulas; (2) low-cost, Sybil-resistant verification/oracle frameworks for common IoT contributions; (3) long-term economic sustainability studies modelling speculation and secondary-market effects; and (4) cross-chain interoperability to enable incentives across heterogeneous ledgers and legacy IoT systems. These gaps motivate hybrid frameworks that jointly consider economic modelling, energy-awareness, and robust verification (Mays Alshaikhli et al., 2025).

Table.1 Literature Review-Summary Table

Incentive Models	Methodology	Limitations	Relevance to HSIF
Token-Based Incentives	Blockchain tokens, PoW/PoS rewards, Helium PoC	Vulnerable to Sybil attacks; limited consideration of device energy constraints	HSIF incorporates token incentives but augments them with adaptive reward control and verification
Micropayment-Based Incentives	Payment channels, DAG-based DLTs	Channel management complexity, privacy challenges	HSIF leverages micropayment concepts within a trusted and reputation-aware framework
Reputation-Based Incentives	On-chain/off-chain reputation scores, Trust indices	Cold-start problems, limited energy-awareness	HSIF integrates decentralized reputation with energy-aware participation to ensure fairness
Sybil-Resistance Mechanisms	Staking/bonding, physical proofs, hardware-based identity	Increased onboarding cost, reduced openness, potential centralization	HSIF adopts lightweight, hybrid Sybil defences aligned with energy and scalability constraints
Energy-Aware Incentive Models	Energy-efficient consensus, duty-cycle adaptation	Often treated at protocol level, weak integration with economic incentives	HSIF tightly coupled energy-awareness with incentive formulation
Hybrid Incentive Frameworks	Token + reputation + micropayments + SLAs	Typically static, loosely coupled, difficult to deploy, limited adaptability	HSIF introduces a unified, adaptive, and tightly integrated hybrid incentive design

To improve clarity and comparison, a summary table, Table.1, is provided to contrast existing incentive mechanisms, their strengths, and their limitations across energy efficiency, scalability, trust, and deployment complexity.

Overall, the reviewed literature enlightens the design of the proposed Hybrid Sustainable Incentive Framework (HSIF), which integrates adaptive tokenomics, decentralized reputation, and energy-aware participation to address the identified limitations in a unified manner.

Vol.5, Issue 1, pp.23-30, 2026
Available online at: http://tljes.org/index.php/tljes/data

The research gap identified from the literature review helped us to formulate the following hypotheses in the evaluation of the HSIF against the conventional mechanisms. These hypotheses connect theoretical insights with the simulation-based evaluation.

H1: Compared to the token-only or reputation-only framework, HSIF improves the participation rate of IoT nodes, particularly under varying network and energy conditions.

H2: The proposed model reduces energy consumption while maintaining incentives. Our model ensures low-energy nodes are not overburdened, leading to lower overall energy consumption compared to the baseline archetype.

H3: HSIF improves fairness in reward distribution, considering both contribution quality and energy expenditure. Producing the Gini coefficient relative to the token-only or reputation-only framework.

H4: The integration of a decentralized reputation module and stake-weighted participation rules HSIF enhances data trustworthiness and Sybil resistance.

H5: Sensitivity analysis of reward and reputation parameters proves that HSIF maintains stable participation, fairness and trust with adaptability and resilience.

Hypotheses, H1 to H5, provide a structured framework for evaluating HSIF through simulation based on the literature review and experimental results. They also allow clear comparison against benchmark token-based and reputation-based incentive mechanisms to validate the theoretical contributions of the proposed framework.

3. Research Methodology

3.1 Research Framework Overview

We developed and evaluated an analytical and conceptually-based model for a sustainable incentive mechanism. The model HSIF is a Blockchain based IoT Ecosystem designed to support fair and long-term device participation. The framework is grounded in commonly adopted assumptions in blockchain-enabled IoT literature, including stable token valuation during short evaluation horizons and bounded reputation dynamics, which allow tractable analytical modelling while capturing essential system behaviour. These assumptions are later relaxed and empirically examined through simulation-based evaluation. This proposed hybrid incentive system integrates 3 key concepts for fair and long-term IoT participation, such as,

a. Economic-based modelling,
b. energy-based usage, and
c. reputation-based validation

There are 4 phases in this system. They are,

a. Exploratory Analysis
b. Framework Design
c. Comparative Evaluation
d. Performance Validation

The analytical component focuses on formalizing incentive relationships and parameter interactions, while the simulation component is used to evaluate system-level performance under realistic network dynamics.

3.2 Phase 1: Exploratory Analysis

Comparative analysis is conducted to examine state-of-the-art incentive mechanisms in BC-enabled IoT systems to identify the key parameters affecting participation. The analysis considers:

a. Reward distribution - This scheme relates to the token and reputation
b. Consensus models - Energy-aware mechanisms using PoW, PoS, and DAG
c. Device constraints – Model based on energy, bandwidth, and latency
d. Security challenges – Inclusion of Sybil, collusion, and false reporting

This analysis aims to define the benchmark parameters and design constraints that guide both the analytical formulation and the subsequent simulation-based evaluation of the proposed incentive framework.

3.3 Phase 2: Framework Design and Modelling

3.3.1 Conceptual Model

The proposed archetype balances economic-based, trustful, and energy-based with the integration of 3 interconnected components:

Tokenomics Module:
This module allocates digital tokens to IoT devices based on verified task completion like, data sensing, transmission, or computation. Since the proposed model is economic-based, nodes are rewarded dynamically according to consumption of energy and contribution of network. Rewards are dynamically adjusted according to device contribution quality and relative energy expenditure, as expressed in Equation (1):

$$R_i = \alpha \times Q_i + \beta \times E_i^{-1} \quad (1)$$

were,
R_i - Reward for device *i*,
Q_i - represents data quality or contribution value, and
E_i - normalized energy expenditure.
This formulation reflects the trade-off between incentivizing high-quality contributions and discouraging excessive energy consumption, thereby promoting sustainable participation.

Reputation Management System:

Reputation Management System assigns reputation scores to IoT devices based on prior reliability, accuracy of data, and

Vol.5, Issue 1, pp.23-30, 2026
Available online at: http://tljes.org/index.php/tljes/data

validation of feedback from other nodes. In consensus decisions, reward scaling is influenced by reputation and trustworthiness as in equation (2).

$$Rep_i(t+1) = \lambda \times Rep_i(t) + (1-\lambda) \times Val_i \qquad (2)$$

were,

λ - the decay factor and

Val_i - the validation score of the latest contribution.

This formulation ensures that recent behaviour is emphasized while still preserving the long-term trust history of each device.

Energy-Aware Participation Control:

Energy-Aware Participation monitors device resource usage and adjusts participation frequency to prevent energy depletion. This ensures sustainability and fair opportunity for low-power nodes.

3.3.2 Blockchain Integration

The following integration supports decentralized governance and traceable incentive delivery,

- Verified transactions record and allocate reward transparently.
- Automate incentive distribution using smart contracts based on predefined energy–reputation thresholds.
- Maintain reputation records securely by preventing tampering or forgery.

3.4 Phase 3: Simulation and Evaluation

A simulation-based evaluation is conducted to complement the analytical modelling and to validate system behaviour under dynamic network conditions. Simulations are implemented using a discrete-event IoT network simulator with custom incentive modules integrated at the application layer. This separation allows analytical assumptions to be examined under realistic operational constraints.

Under IoT network simulation-based method is used to evaluate HSIF with parameters as follows,

- Number of IoT nodes – ranging from 100 to 1000
- Communication model – simulation consist of wireless mesh with energy constrains
- Consensus protocol – which is based on a lightweight PoS or DAG consensus
- Evaluation period – with 100 simulation rounds

Although simulations are conducted with up to 1000 IoT nodes, the framework's reliance on localized reputation updates and lightweight consensus protocols suggests that HSIF can scale to larger networks. However, scalability claims beyond 1000 nodes remain theoretical and must be validated in future studies with larger deployments. For Performance metrics consider the participation rate in percentage, average energy consumption is calculated as Joules per node, Gini coefficient is used for evaluating fairness of reward distribution, reputation accuracy represents trust percentage and finally, Sybil-resistance score represents success probability of an attack. The proposed HSIF archetype is compared against benchmark token-based and reputation-based incentive models to assess relative performance improvements.

4. Result and Discussion

We conducted this simulation in a controlled environment with simplified real-world dynamic networks. Token volatility and factors related with marker-driven are statically modelled and this may not reflect on actual economic fluctuations. We assume reputation module as fairness in behaviour which may be vulnerable to collusion in large-scale environments.

4.1 Overview

The experimental results of the proposed model are analysed and evaluated. The key performance factors are the rate of participation, consumption of energy, accuracy of reputation, and resistance of Sybil. This comparative study is analyzed with the following benchmark incentive systems: (I) Token-based and (II) Reputation-based. The result reveals that our proposed model achieves balanced improvements for all participants, and it has energy efficiency with strong incentive manipulation

4.2 Simulation Setup

Controlled IoT scenario with 500 nodes of heterogeneous types are used for conducting simulation under a lightweight PoS (Proof of Stake) using Blockchain protocol. Every node in this simulation has varying energy capacity and different task contribution levels. This simulation is executed for 100 epoch along with different network load and assigning task dynamically as shown in Table.2.

Table.2 List of parameters and its value

Parameter	Value
Number of nodes	500
Simulation duration	100 rounds
Consensus mechanism	Lightweight PoS
Average task load per node	10–30 transactions/round
Initial energy per node	1000 J
Reward factors (α, β)	0.7, 0.3
Reputation decay factor (λ)	0.8

The proposed HSIF framework demonstrates improved performance across multiple metrics compared to baseline token or reputation-based incentive models. Simulation results

Vol.5, Issue 1, pp.23-30, 2026
Available online at: http://tljes.org/index.php/tljes/data

show higher participation rates, lower average energy consumption, more equitable reward distribution, and enhanced reputation accuracy. Each experiment is repeated over 10 independent simulation runs, and the reported values represent the mean ± standard deviation, providing a measure of variability and supporting the robustness of observed improvements. The improvements in fairness, as measured by the Gini coefficient, arise from the adaptive reward scaling mechanism, which balances token allocation with contribution quality and energy consumption.

Low-energy nodes are assigned fewer tasks to prevent depletion, while high-quality contributors remain incentivized. Reputation-based validation prioritizes trustworthy nodes, discouraging malicious or low-quality contributions, and reputation scores are stabilized by historical validation and decay factors to limit the impact of isolated false reports.

4.3 Results

4.3.1 Participation Rate

The number of IoT nodes are active or the rate of participation factor measures number of resources computable per epoch. From the result of our experiment, we obtained 92% as the rate of average participation. Compared to token-based and reputation-based system, our proposed model is 18% and 24% respectively produce better performance. This is the success of this proposed hybrid model with reputation and token incentives, where IoT nodes stay active even when different network criteria occur. When token volatility increased by 20%, participation in the pure token archetype dropped sharply (to 61%), while HSIF remained stable (at 89%), proving economic resilience.

4.3.2 Energy Efficiency

Sustainability is maintained with efficient usage of energy. Our model's average consumption of energy is 18% less than benchmark models because of the participation of a controller with energy awareness as shown in Table.3. This controller effectively and dynamically monitors the frequency contribution. Through this method, low power nodes stay active for longer time thus improv fairness and longevity of network.

Table.3 Model with Average Energy Consumption per Node

Model	Average Energy Consumption per Node (J)	Improvement vs. Token Model
Token-based	830	—
Reputation-based	720	13.2%
HSIF (Proposed)	680	18.1%

4.3.3 Fairness in Reward Distribution

The Gini coefficient is used to measure the fairness of this system. When values are lower, that represent reward distributions are equal as shown in Table.4.

Table.4 Model with Gini coefficient

Model	Gini Coefficient
Token-based	0.36
Reputation-based	0.31
HSIF (Proposed)	0.18

From the table, we get that the proposed model achieves the lowest Gini coefficient, thus providing high fairness even for devices with varying capacities. The hybrid archetype prevents domination efferently by high-resource nodes using adaptive token weighting and reputation scaling.

4.3.4 Reputation Accuracy

The ability of the system to identify the trustworthiness of each node and to identify a malicious node is determined by the accuracy of the reputation. Our proposed framework obtains 94% in reputation accuracy, which is 8% higher than the standalone reputation-based system. The standalone token-based system lacks in reputation tracking.

4.3.5 Sybil Resistance

The introduction of false nodes that attempt to exploit the incentive mechanism is the common method of testing the robustness of the system against Sybil attacks. In token-based system 25% and in reputation-based system 14% the attack is successful whereas in the proposed method success rate is less than 7%. This proves the resistance of the proposed system against Sybil attack. This enhancement is possible with the combination of reputation-based validation and stake-weighted participation rules.

4.3.6 Sensitivity Analysis

A sensitivity analysis examines the impact of key parameters on performance. Varying the energy weight in the reward function by ±20% produced consistent patterns in participation and fairness, indicating that HSIF's performance is relatively robust to moderate changes in parameter settings. Similarly, adjusting the reputation decay factor showed minor effects on overall trust accuracy, demonstrating stability of the reputation management component under different configurations.

4.4 Discussion of Findings

Key findings from the simulation outcomes are as follows:

1. Balanced Incentivization:
   For both high-resource and low-resource IoT nodes, this Hybrid incentive framework provides sustained

Vol.5, Issue 1, pp.23-30, 2026
Available online at: http://tljes.org/index.php/tljes/data

support and helps to avoid the participation collapse common which is common in any standalone-model.

2. Energy–Reward Trade-off:
   Combining energy awareness directly in the reward calculation helps to improve network longevity without significantly reducing throughput.

3. Fairness and Trust:
   Integrating Reputation in the model yields fairness and trustworthiness that make the network more resilient against false data and collusion submissions.

4. Security and Sustainability:
   Tokenomics is combined with reputation to enhances Sybil resistance and this ensure the contribution of consistent network over time.

5. Scalability Considerations:
   The proposed system performs highly up to 1000 nodes, thus provide lability potential for large IoT networks with minimal computational overhead.

4.5 Summary of Results

The results of evaluating benchmark models such as Token and Reputation with the proposed HSIF is shown on the below table (Table.5). From this table our model outperforms other two models in balancing energy use, reputation driven trust and improves participation rate to 24%. It establishes a sustainable and secure archetype suitable for future BC-IoT ecosystems, addressing both economic and technical challenges identified in prior research.

Table.5 Evaluation Metrics for Token model, Reputation model and HSIF model

Metric	Token Model	Reputation Model	HSIF (Proposed)	Improvement (%)
Participation Rate (%)	74	68	92	+24
Avg. Energy Use (J)	830	720	680	-18
Fairness (Gini Index)	0.36	0.31	0.18	+42
Reputation Accuracy (%)	—	86	94	+9
Sybil Attack Success (%)	25	14	7	-72

While HSIF improves sustainability and fairness, several limitations remain. The static token valuation simplifies the analytical model but may not fully capture market-driven fluctuations, which could influence incentive stability in real deployments. The reputation mechanism, although robust to Sybil attacks, is still vulnerable to coordinated collusion among nodes, particularly in large-scale or highly adversarial environments. Furthermore, the simulation environment abstracts certain network effects, such as dynamic topology changes or variable communication delays, which may impact performance in real-world IoT deployments. Future work will focus on addressing these limitations through dynamic token modelling, enhanced trust aggregation, and deployment on testbed networks.

5. Conclusion and Future Work

5.1 Conclusion

The simulation results demonstrate that HSIF significantly enhances network performance in terms of participation, energy efficiency, and fairness compared to benchmark models. This work contributes to the theoretical understanding of hybrid incentive mechanisms by integrating tokenomics, reputation management, and energy-aware participation control into a unified framework for sustainable BC-IoT networks. Incorporating decentralized reputation mechanism improves trustworthiness and Sybil resistance of the system by ensuring only reliable nodes are rewarded consistently. Furthermore, this framework balances incentives with resource usages with long-term viability of BC-IoT integrated systems. The HSIF model emphasis on sustainable participation by integrating financial, reputational, and ecological motivations instead of depending on a single reward structure. While HSIF demonstrates improved performance under simulation, the study assumes simplified token valuation and network conditions, and real-world deployment may face challenges such as dynamic network topology, device heterogeneity, and potential collusion in reputation systems.

In future, this work will be extended to implement in a real industrial IoT environment to validate its practical performance under live network conditions. To enable seamless performance in heterogeneous IoT system, explore this archetype across multiple BC platforms. On real-time networks, reinforcement learning or adaptive optimization algorithms can be incorporated to dynamically provide reward parameters. Furthermore, including carbon footprint awareness and renewable energy incentives can align with green IoT and sustainable computing objectives.

References:

Akashah Arshad, Zurina Mohd Hanapi, Shamala Subramaniam & Rohaya Latip (2021). A survey of Sybil attack countermeasures in IoT-based wireless sensor networks. PeerJ Computer Science. https://DOI 10.7717/peerj-cs.673.

Al-Matari, N. Y., Zahary, A. T., & Al-Shargabi, A. A. (2024). A survey on advancements in blockchain-enabled security mechanisms for spectrum access and IoT applications. *Scientific Reports, 14*, 30990. https://doi.org/10.1038/s41598-024-82126-y

Benedetti, M., De Sclavis, F., & Favorito, M. (2025). An analysis of pervasive payment channel networks for scalable micropayments. *Computer Communications, 240*, 108199. https://doi.org/10.1016/j.comcom.2025.108199

Bertozzi, M., Damiani, E., & Mancini, L. (2020). *Iota Tangle: A cryptocurrency to communicate Internet-of-Things data*. *Future Generation Computer Systems, 112*, 307-319. DOI: 10.1016/j.future.2020.05.047

D'Aniello, G., & Fotia, L. (2025). *Blockchain and AI-based methods for trust management in IoT: A comprehensive survey*. *Internet of Things, 34*, 101755.

Enaya, A., Fernando, X., & Kashef, R. (2025). *Survey of blockchain-based applications for the Internet of Things*. *Applied Sciences*, 15(8), Article 4562.

Kang, C., Woo, J., & Hong, J. W.-K. (2025). A comprehensive survey of Lightning Network technology and research. *International Journal of Network Management, 35*(5). https://doi.org/10.1002/nem.70023

Khan, I., Majib, Y., Ullah, R., & Rana, O. (2024). *Blockchain applications for Internet of Things — A survey*. Internet of Things, 27, Article 101254. https://doi.org/10.1016/j.iot.2024.101254

Mahmoud, H., Arshad, J., & Aneiba, A. (2024). A systematic review of blockchain-based privacy-preserving reputation systems for IoT applications. *Distributed Ledger Technologies, 3*(4), Article 31, 1–40. https://doi.org/10.1145/3674156

Maddikunta, P. K. R., et al. (2022). Incentive techniques for the Internet of Things: A survey. *Journal of Network and Computer Applications, 205*, 103437. https://doi.org/10.1016/j.jnca.2022.103437

Mays Alshaikhli, Somaya Al-Maadeed, & Saleh, M. (2025). Enhancing fairness and scalability in IOTA tangle networks: a POMDP-based tip selection algorithm for decentralized systems. *Cluster Computing*, *28*(14). https://doi.org/10.1007/s10586-025-05432-8

Mohaisen, A., & Kim, J. (2013). *The Sybil Attacks and Defenses: A Survey*. Smart Computing Review, 3(6), 480–489.

Nzakuna, P. S., et al. (2025). From IOTA Tangle 2.0 to Rebased: A comparative analysis for IoT applications. *Sensors, 25*(11), 3408. https://doi.org/10.3390/s25113408

Obaidat, M. A., et al. (2024). Exploring IoT and Blockchain: A comprehensive survey. *Big Data and Cognitive Computing, 8*(12), 174. https://doi.org/10.3390/bdcc8120174

Oliveira, G. H. C., de Souza Batista, A., Nogueira, M., & Santos, A. L. (2022). *An access control for IoT based on network community perception and social trust against Sybil attacks.* International Journal of Network Management, 32(1).

Rochman, S., Istiyanto, J. E., Dharmawan, A., Handika, V., & Purnama, S. R. (2023). Optimization of tips selection on the IOTA tangle for securing blockchain-based IoT transactions. *Procedia Computer Science*, 216, 230–236.

Wadhwa, S., et al. (2022). Energy-efficient consensus approach of blockchain for IoT. *Sensors, 22*(10), 3733. https://doi.org/10.3390/s22073733

Wang, W., Chen, J., Jiao, Y., Kang, J., Dai, W., & Xu, Y. (2022). *Connectivity-aware contract for incentivizing IoT devices in complex wireless blockchain*. *IEEE Access*.

Xu, X., et al. (2021). Blockchain-enabled IoT for energy-efficient incentive mechanisms. *IEEE Internet of Things Journal, 8*(11), 8925–8938. https://doi.org/10.1109/JIOT.2021.3058749

Zhang, Y., & Wen, J. (2020). The IoT blockchain: Challenges and opportunities. *Future Generation Computer Systems, 105*, 719–729. https://doi.org/10.1016/j.future.2019.12.022

Zimba, A., Phiri, K. O., Mulenga, M., & Mukupa, G. (2025). *A systematic literature review of blockchain technology and energy efficiency based on consensus mechanisms, architectural innovations, and sustainable solutions*. Springer. Discover Analytics, 3, Article 14. https://doi.org/10.1007/s44257-025-00041-6