© MAY 2026 | IRE Journals | Volume 9 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I11-1717649

A Blockchain-Driven Reputation-Aware Relay Selection Framework for Trustworthy Peer-to-Peer Communication in Web3 Networks

RITHIKA S[1], THRISHA S[2], UMA MAGESHWARI M[3], VAISHALI D[4], SAMUNDEESWARI M[5]
[1.2.3.4]*Students, Department of Computer Science and Engineering, Kingston Engineering College, Vellore.*
[5]*Assistant Professor, Department of Computer Science and Engineering, Kingston Engineering College, Vellore.*

Abstract- ***Peer-to-peer (P2P) interaction forms a foundational layer of Web3 ecosystems, enabling participants to exchange data directly without depending on centralized brokers. In practical deployments, however, end-to-end reachability is often obstructed by network address translation, firewalls, and transient routing paths, which pushes architects toward the use of intermediate relay nodes. Unfortunately, relays that behave inconsistently or act maliciously can introduce a range of undesirable effects, including dropped packets, elevated latency, selective forwarding, and denial-of-service conditions. To mitigate these risks, this work presents a reputation-aware relay selection framework that lever-ages a blockchain substrate to govern trust. Every participant in the overlay is issued a cryptographic identity; the quality of service delivered by each relay is then tracked at runtime through metrics such as delivery ratio, round-trip delay, and transmission failure rate. A smart contract layer aggregates these observations into a dynamic reputation score that is recorded on an immutable ledger. When a communication session is being established, relays with higher reputation are preferred, while those exhibiting suspicious or degraded behavior are deprioritized or excluded. Experimental results indicate that, compared with conventional relay-selection strategies, the proposed approach delivers higher reliability, lower effective latency, and stronger resistance to malicious participation, making it a practical candidate for secure Web3 P2P communication.***

Index Terms—Web3, Peer-to-Peer Communication, Relay Node Selection, Blockchain, Smart Contracts, Reputation Systems, Decentralized Trust, Secure Overlay Networks

I. INTRODUCTION

The ongoing evolution of the Internet has been marked by a gradual shift away from platform-centric services toward architectures where users retain ownership of their data and interactions occur without trusted third parties. This emerging paradigm, commonly referred to as Web3, rests on principles of decentralization, verifiable computation, and user sovereignty. Direct peer-to-peer (P2P) communication is a natural building block of this paradigm, and it underpins a wide range of services including decentralized applications, distributed ledgers, and content distribution networks [1]. Yet deploying P2P communication in real networks is rarely straightforward: nodes are frequently located behind NAT de-vices, are subject to firewall policies, or operate over dynamic IP assignments [2].

To address these obstacles, relay nodes are commonly introduced as intermediaries that forward traffic on behalf of peers that cannot reach one another directly. While this technique extends connectivity, it also expands the attack surface. Faulty or adversarial relays may drop, delay, or tamper with packets, degrading both throughput and the perceived quality of service. Traditional selection policies typically emphasize latency, bandwidth, or random allocation, and they seldom consider whether a relay has a history of trustworthy behavior. Establishing trust in a fully decentralized environment is inherently difficult: by design, there is no single authority empowered to arbitrate on behalf of all participants, and introducing one would contradict the very ideals of Web3. Moreover, any centralized oversight introduces a single point of failure [5]. Blockchain technology offers an attractive alternative, since consensus-driven ledgers can maintain tamper-resistant records across untrusted participants [6]. Combining such ledgers with reputation systems makes it possible to record and

share behavioral evidence about relays in a way that is difficult to manipulate [7]. Motivated by these observations, this paper proposes an architecture in which blockchain-anchored reputation drives the relay selection process.

A. Background and Motivation

Conventional relay-selection logic in P2P overlays usually reduces the problem to a shortest-path or least-loaded calculation. Such heuristics are effective when all relays are honest, but they offer no defense against repeat offenders. In a Web3 deployment, where no central monitor is available to blacklist misbehaving nodes, malicious relays can participate in many sessions, damage multiple peers, and escape accountability. The motivation behind the present work is therefore to construct a decentralized trust substrate in which relays are evaluated against observed behavior rather than static assumptions, and in which reputation data can be shared across the network through blockchain primitives and smart contracts.

B. Research Overview

The proposed framework takes a system-centric view of secure P2P communication. Each node is bound to a cryptographic identity, and the effectiveness of each relay is quantified in terms of packet delivery success, end-to-end delay, and failure rate. These observations are fed into a reputation engine whose output is written to a blockchain through smart contracts, ensuring that trust evidence is transparent and resistant to tampering. Relay selection is subsequently driven by the reputation ledger: high-scoring relays are preferred, while low-scoring ones are penalized or excluded. The resulting overlay supports transparent, scalable, and trust-aware communication without a central arbiter.

II. PROBLEM STATEMENT

Relay nodes play a pivotal role in Web3 P2P networks be-cause they bridge peers that cannot communicate directly due to network-layer restrictions. This role, however, makes them attractive targets for abuse. Without a trust-aware selection mechanism, adversarial relays can repeatedly drop packets, apply selective forwarding, or stage denial-of-service attacks against legitimate peers. Existing relay-selection techniques ignore the behavioral history of candidate nodes, which means that an attacker can re-engage with the network indefinitely after each incident.

Equally important, attempts to bolt centralized trust-management services onto a Web3 architecture reintroduce the very weaknesses that Web3 was designed to avoid: a single point of failure, a privileged administrator, and an opaque decision process. There is consequently a clear need for a decentralized, scalable, and tamper-resistant relay-selection mechanism that continuously evaluates the trustworthiness of relays and ensures that secure P2P communication can be sustained even in the presence of dishonest participants.

III. RELATED WORK

A growing body of literature has examined the use of blockchain and reputation mechanisms to harden distributed communication systems [6] [7]. Reid et al., for instance, investigated reputation-aware relay selection as a defense against malicious nodes in opportunistic and vehicular networks, demonstrating the value of historical behavior in routing decisions [8]. Work on smart contracts has further explored how trust policies and identity bindings can be encoded and enforced programmatically within Web3 environments [9]. However, comparatively little attention has been devoted to combining blockchain-backed reputation with relay-assisted P2P overlays, and existing proposals tend to address only isolated aspects of the problem. The present paper seeks to close this gap by presenting an integrated framework that jointly addresses identity, performance monitoring, reputation management, and selection policy.

IV. LIMITATIONS OF EXISTING SYSTEMS

The majority of relay-selection strategies currently deployed in P2P and Web3 networks concentrate on performance-centric indicators such as round-trip latency, available bandwidth, and hop count. While these metrics are important, they do not capture the long-term behavior of a relay, nor do they reveal whether the relay has historically acted in good faith. As a result, a sophisticated adversary can mimic the

© MAY 2026 | IRE Journals | Volume 9 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I11-1717649

statistical fingerprint of a well-behaved relay while intermittently engaging in selective forwarding or packet suppression, remaining undetected for extended periods.

Centralized trust monitors have been proposed as a stopgap, but they are fundamentally incompatible with the Web3 design philosophy. Beyond the ideological mismatch, such monitors become bottlenecks that limit scalability, attract adversarial attention, and collapse under load or targeted attack. Their lack of transparency also makes it difficult for peers to audit trust decisions independently.

A further weakness of many existing schemes is that they treat identity verification as a one-time event: a node is authenticated when it joins and then trusted indefinitely, which leaves no avenue for revoking privileges when behavior deteriorates. Finally, most deployments lack an automated penalty-and-incentive loop, so chronically unreliable relays continue to participate in message forwarding. Taken together, these limitations leave existing systems poorly equipped to guarantee secure and reliable P2P communication in Web3 settings.

V. PROPOSED SYSTEM ARCHITECTURE

The architecture proposed in this paper places a blockchain-anchored reputation layer at the heart of relay selection for Web3 P2P

Fig. 1. System architecture of the blockchain-based reputation-aware relay selection framework.

communication. Each node joining the overlay receives a cryptographic identity, which is used both for authentication and for binding reputation records to a specific principal. Relay behavior is observed continuously, and reputation scores are refreshed in real time according to measured delivery ratio, reliability, and failure rate. Scores are committed to a blockchain ledger under the control of smart contracts, which makes the trust state both transparent and tamper-proof. Selection of relays for new sessions is driven by the ledger, so that high-reputation nodes are favored while low-reputation nodes are excluded. Because all trust decisions are enforced on-chain, no centralized authority is required, and the design stays faithful to Web3 principles.

A. System Components

- Node Registration Module: issues cryptographic identities to every participating node and records them on-chain.
- Reputation Evaluation Module: consumes observed communication metrics and computes per-relay reputation values.
- Blockchain Ledger: stores reputation records in an im-mutable and publicly auditable form, enabling decentralized sharing of trust state.
- Relay Selection Module: ranks candidate relays by reputation and filters out those deemed malicious or unreliable.
- Penalty and Incentive Mechanism: automatically re-wards honest relays and sanctions misbehaving ones through smart contracts.

B. Role of Relay-Assisted Networking

Relay assistance becomes essential whenever direct peer-to-peer reachability is blocked by NAT translation, firewalling, or unstable paths. Relays restore connectivity by forwarding traffic on behalf of peers that cannot otherwise meet. The catch is that relays themselves may behave irregularly or adversarially, so the reliability of the entire overlay ultimately hinges on how relays are chosen.

C. Role of Reputation-Based Trust Management

In a decentralized network, there is no authority to vouch for any given node, so trust must be derived from empirical evidence. Reputation-based trust management achieves this by continuously scoring nodes against their observed reliability, responsiveness, and consistency. In the proposed system, these scores feed directly into relay selection,

so that the most dependable nodes are chosen for each session.

D. Role of Blockchain Technology

Blockchain provides the storage substrate for trust data. Because entries on the ledger cannot be altered retroactively and are replicated across many participants, they yield a decentralized record that neither a malicious relay nor a corrupted administrator can rewrite. The proposed framework uses this property to guarantee that reputation values remain authentic throughout the lifetime of a node.

E. Role of Smart Contracts

Smart contracts express the trust policy in executable form. Instead of relying on human operators, the framework delegates reputation updates, penalty enforcement, and relay-selection bookkeeping to on-chain code that runs deterministically on every node. This mechanization makes the system consistent, auditable, and resistant to arbitrary policy changes.

F. Role of Cryptographic Identity

Cryptographic identities anchor each node to a verifiable key pair, preventing spoofing and Sybil-style impersonation. With identity binding in place, reputation values can be attributed unambiguously to the entity that produced the corresponding behavior, so that malicious actors cannot discard a tainted identity and reappear unburdened.

G. Role of Decentralized Trust and Security

Decentralized trust is the connective tissue of the architecture. By layering cryptographic identities, reputation evaluation, blockchain storage, and smart-contract policies, the system builds a defense-in-depth posture in which each component reinforces the others and closes a category of attacks that the others cannot cover alone.

H. System Design and Architecture

The overall design follows a modular and layered philosophy so as to balance scalability, transparency, and resilience against misbehavior, all of which are central concerns in Web3 networks [1], [5]. At a high level the system is composed of P2P client nodes, a pool of candidate relays, a relay performance monitor, a reputation evaluation engine, and a blockchain-anchored trust ledger backed by smart contracts. Each element is described in the subsections that follow.

1) P2P Nodes (Web3 Clients): Communication in the over-lay originates with end-user clients that participate in Web3 services and need to exchange data with one another. Although direct communication is always attempted first, restrictions such as NAT, asymmetric firewalls, or heterogeneous network stacks may force the use of a relay path [1], [6]. Every peer is bound to a unique cryptographic identity, giving it a stable and verifiable presence on the network and preventing impersonation within the decentralized environment [2].

2) Relay Nodes: Relay nodes bridge pairs of peers that cannot reach each other directly. While they make the overlay substantially more reachable, they also introduce risk: a relay may forward packets selectively, behave selfishly, or collude with attackers [6], [8]. In contrast to traditional relay deployments, the proposed architecture treats relays as inherently un-trusted and qualifies each one through its behavioral footprint as captured by its reputation record.

3) Relay Performance Monitoring Module: During active communication, this module collects objective performance indicators for each relay in use, including packet delivery ratio, end-to-end delay, and transmission failure rate [3], [8]. These indicators form the raw material from which reputation is later derived, and they are gathered in a decentralized fashion so that no single observer becomes a point of failure.

4) Reputation Evaluation Engine: The reputation evaluation engine converts monitoring data into a numerical trust value for each relay. Its scoring logic blends recent and historical observations so that a relay cannot manipulate its reputation through brief, isolated bursts of honest behavior [4], [7]. The resulting score is then handed over to the blockchain layer for durable storage and enforcement.

5) Blockchain Network and Smart Contracts: The blockchain layer serves as the decentralized backbone of trust. It maintains an immutable ledger of reputation records, node identities, and related

© MAY 2026 | IRE Journals | Volume 9 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I11-1717649

metadata, offering transparency, tamper-evidence, and replication by design [5], [6], [7], [9]. Smart contracts deployed on the ledger automate reputation updates, enforce penalty and incentive policies, and encode the rules of relay selection, eliminating any need for a centralized arbiter [9], [10].

6) Reputation-Aware Relay Selection Module: Selection is driven by the on-chain ledger. The module queries the current reputation of candidate relays, ranks them, and issues bindings for the session at hand. Relays that exhibit suspicious behavior are demoted or filtered out, and repeated offenses trigger on-chain penalties [7]. The mechanism sustains the reliability of message delivery while keeping communication latency within acceptable bounds.

7) Secure P2P Communication Channel: Once a trust-worthy relay has been selected, a secure channel is established between the endpoints, with confidentiality, integrity, and availability backed by cryptographic identities and the reputation state of the chosen relay [2], [5].

I. Architectural Advantages

- The proposed design yields several advantages:
- Decentralized and tamper-resistant trust management via blockchain [5].
- Continuous, behavior-driven reputation assessment [3].
- Automated trust enforcement through smart contracts [9].
- Scalability and resilience suitable for large-scale Web3 deployments [1], [10].

In summary, the architecture integrates blockchain-backed trust with reputation-driven relay selection to deliver secure P2P communication for Web3 environments.

Class Diagram: ER Diagram:

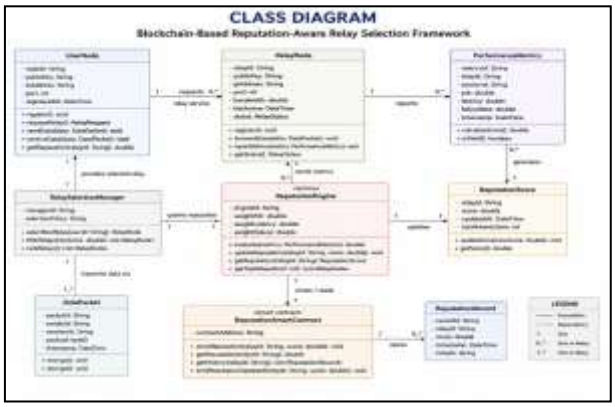

Fig. 2. Class diagram of the proposed reputation-aware relay selection system.

VI. METHODOLOGY

The methodology translates the architectural vision into a sequence of concrete procedures that together deliver de-centralized, reputation-aware relay assistance for Web3 P2P communication. The design draws on recent advances in behavior-driven trust enforcement for decentralized networks [1], [4], [6], and it weaves together identity management, live performance monitoring, reputation computation, on-chain storage, and intelligent selection into an end-to-end pipeline

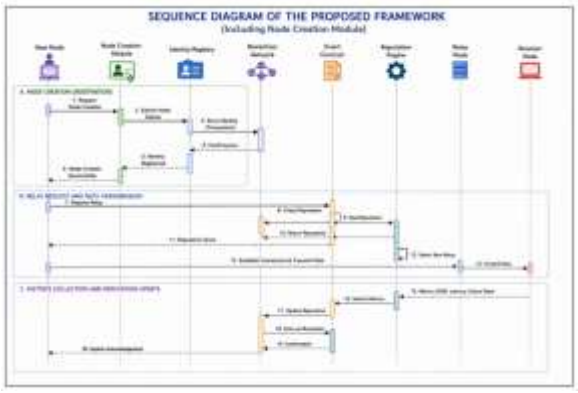

Fig. 3. Sequence diagram of secure relay-assisted communication.

A. Node Registration and Cryptographic Identity Management

Before any node can act as a sender, receiver, or relay, it must register with the system and obtain a key pair generated through public-key cryptography. This binding produces a tamper-evident link between the node and its identity, ruling out impersonation

attacks that would otherwise be straight-forward in a permissionless environment [2]. The resulting identity is committed to a blockchain-hosted registry, enabling transparent participation without reliance on a central authority [5].

B. Relay-Assisted Communication Initiation

When one peer intends to communicate with another, the system initially attempts to establish a direct peer-to-peer connection. However, if direct connectivity cannot be achieved due to factors such as NAT/firewall restrictions or asymmetric routing domains [1], the communication request is redirected through a candidate relay node that has been previously validated based on its reputation score.

C. Relay Performance Monitoring

While a relay is actively forwarding traffic, the system records metrics that capture its operational quality: packet delivery ratio, end-to-end latency, and failure rate [3], [8]. These indicators are standard in the detection of unreliable or adversarial forwarding behavior, and they are collected in a distributed manner to avoid creating a monitoring bottleneck.

D. Reputation Score Computation

Collected metrics are forwarded to the reputation evaluation engine, which condenses them into a scalar reputation value for each relay. The computation blends short-term and long-term observations so that a relay cannot inflate its score by alternating bursts of cooperative and adversarial behavior [4], [7]. Configurable trust thresholds govern when a score triggers promotion, demotion, or outright exclusion.

E. Blockchain-Based Reputation Management

Every computed reputation value is committed to the blockchain through a smart-contract interface. Immutability and decentralization guarantee that the trust record cannot be modified or erased without authorization, which protects the system from silent tampering [5], [9]. Because the update logic is encoded in contract code, the system scales without requiring a central trust manager [6], [10].

F. Reputation-Aware Relay Selection

When a new session is initiated, the selection module retrieves the current reputation values of all candidate relays from the ledger and ranks them. Higher-scoring relays are preferred, while those flagged as malicious or unreliable are penalized and deprioritized, reinforcing both the security and the quality of service of the overlay [7], [8].

G. Secure Data Transmission

After a trustworthy relay has been chosen, a secured trans-mission protocol is instantiated between the endpoints. The combination of cryptographic identities, blockchain-backed reputation, and verified relay selection secures the three classical properties of confidentiality, integrity, and availability that are mandatory in Web3 communication [2], [5].

H. Continuous Reputation Update and Enforcement

Reputation management is not a one-off event: as sessions proceed, fresh performance observations update the reputation of each relay in near real time. Smart contracts continue to apply incentives and penalties automatically, giving the system the ability to adapt to shifting network conditions and emerging threats [4], [9].

Methodological Significance:

- Decentralized, tamper-resistant trust evaluation [5].
- Continuous, behavior-grounded reputation scoring [3], [4].
- Automated trust enforcement through smart contracts [9].
- Effective identification and isolation of malicious relays [8].
- Scalability suitable for large Web3 P2P deployments [1], [10].

VII. IMPLEMENTATION TECHNOLOGY AND TOOLS

A. Technologies Used

- Blockchain Platform: Ethereum
- Smart Contract Language: Solidity
- Backend Framework: Java with Spring Boot
- Frontend Stack: HTML, CSS, and React.js
- Development Environment: Visual Studio Code, Ganache, Remix IDE

B. Implementation Overview

© MAY 2026 | IRE Journals | Volume 9 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I11-1717649

The prototype follows a layered and modular blueprint. Every node must first register with the backend, which is built on Spring Boot and manages identity generation, verification, and the subsequent commit of node metadata to the Ethereum network .During a relay-assisted session, data flows from the sender to the receiver via a selected relay, while the backend tracks the relay's observations feed the Java-based reputation engine, which updates the corresponding trust value accordingly [2], [6].Updated scores are then persisted on-chain through Solidity smart contracts, which both store the data and enforce the as-sociated rules .When a new communication request arrives, the relay selection module consults the ledger, picks the highest-scoring trustworthy relay, and filters out any participants that have accumulated evidence of misbehavior. This design choice strengthens both the reliability and the security of the overlay [4], [7].The reference implementation is openly available at https://github.com/RithikaSaravanakumar/relay-network-project.

VIII. EXPERIMENTAL RESULTS AND ANALYSIS

An empirical evaluation was conducted in order to characterize the behavior of the proposed system and to determine the practical benefits of reputation-driven relay selection. The framework was exercised along three axes: packet delivery ratio, end-to-end communication delay, and the detection rate of malicious nodes.

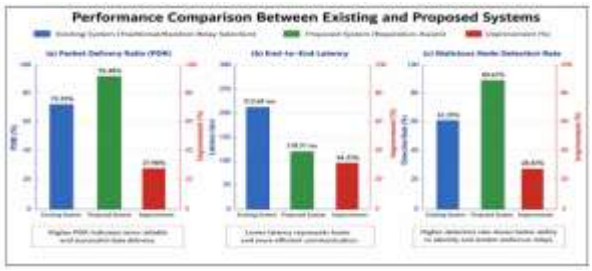

Fig. 5. Performance comparison between existing and proposed systems.

The measurements show that, relative to baseline selection strategies that rely solely on performance-level heuristics, the reputation-aware mechanism delivers a noticeably higher packet delivery ratio because traffic is routed preferentially through relays with a demonstrated history of reliability. Communication delay also decreases on average, as unreliable nodes are removed from the candidate pool before they can slow down sessions. In parallel, the continuous monitoring loop flags malicious behavior early, allowing the system to isolate offending relays promptly. Although the blockchain interaction introduces a non-negligible computational over-head, the resulting gains in security and auditability justify the cost, and the experimental findings confirm that the framework meets the security expectations associated with Web3 P2P communication [5], [10].

IX. ADVANTAGES

The principal benefits of the proposed framework can be summarized as follows:

- A decentralized and tamper-resistant reputation store grounded in blockchain.
- Continuous, behavior-based trust evaluation of every re-lay.
- Timely detection and isolation of misbehaving relays.
- No reliance on centralized trust authorities, and hence no single point of failure.
- Higher packet delivery ratio together with reduced effective communication latency.
- Transparent, auditable trust records accessible to all participants.
- Scalability suitable for large Web3 P2P deployments.

Collectively, these properties raise the trustworthiness and dependability of relay-assisted P2P communication and make the framework a credible candidate for production-grade Web3 systems.

X. CONCLUSION AND FUTURE WORK

This paper has introduced a blockchain-driven, reputation-aware relay selection framework for secure peer-to-peer communication in Web3 networks. By fusing immutable on-chain reputation management with intelligent relay selection, the framework directly addresses the trust and reliability challenges that arise from the use of untrusted

intermediaries. Experimental evidence indicates that the proposed design improves communication reliability, reduces effective latency, and increases the detection rate of malicious relays in com-parison with conventional strategies.

Several directions remain open for future investigation. We intend to incorporate machine-learning techniques for predictive reputation modeling so that the system can anticipate misbehavior rather than merely react to it. We also plan to optimize smart-contract gas costs, and to extend the framework to heterogeneous real-world Web3 deployments that exhibit diverse network conditions and adversarial models [8], [10].

REFERENCES

[1] M. Zhang, Y. Li, and X. Chen, “Trust-aware relay selection for secure peer-to-peer communication,” IEEE Access, vol. 10, pp. 112345–112358, 2022.

[2] S. Kumar, R. Verma, and A. Singh, “Detection of malicious nodes in P2P networks using behavior-based monitoring,” Wireless Networks, vol. 28, no. 4, pp. 1891–1904, 2022.

[3] J. Li, H. Wang, and Q. Zhou, “Secure node communication in peer-to-peer networks using cryptographic identity,” Computer Networks, vol. 215, art. 109214, 2023.

[4] X. Wang, Y. Liu, and Z. Huang, “Blockchain-based reputation management in distributed systems,” Sensors, vol. 23, no. 6, art. 3124, 2023.

[5] Y. Chen, L. Zhao, and M. Guo, “Decentralized trust management using blockchain technology,” IEEE Transactions on Network and Service Management, vol. 21, no. 1, pp. 456–468, 2024.

[6] A. Patel and K. Shah, “Performance-aware relay selection in decentralized communication networks,” in Proc. ACM Int. Conf. Distributed Computing Systems, 2023, pp. 211–220.

[7] R. Singh, P. Mehta, and N. Joshi, “Secure relay communication using a blockchain-enabled trust framework,” in Proc. IEEE Int. Conf. Blockchain and Cryptocurrency, 2024, pp. 98–105.

[8] S. Rao, D. Kannan, and V. Subramaniam, “Monitoring and mitigation of malicious relay behavior in P2P networks,” J. Network and Computer Applications, vol. 225, art. 103567, 2024.

[9] A. Ghazali and S. Saleh, “Blockchain-based trust evaluation for decentralized systems,” IEEE Access, vol. 9, pp. 154321–154334, 2021.

[10] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” Ethereum Yellow Paper, revised version, 2022.