**A DAG-Based Trust Verification Layer for Distributed Networks and Edge Systems**

Author: Chris Prinsloo

Affiliation: Independent Researcher / FORUS Digital

Email: (to be added per submission requirements)

Abstract

Distributed networks increasingly depend on autonomous coordination across heterogeneous nodes, including IoT devices, edge systems, and AI agents. While significant advances have been made in consensus, security, and fault tolerance, existing architectures lack a verifiable and continuously updateable notion of trust state that can be computed, propagated, and validated across network participants. Current approaches rely on static credentials, probabilistic reputation scores, or heavyweight consensus mechanisms that do not scale effectively to dynamic, multi-domain environments.

This paper introduces a Directed Acyclic Graph (DAG)-based trust verification layer designed to function as a system-level primitive for distributed networks. The proposed architecture models trust as a measurable and reproducible state that evolves over time through verified interactions between nodes. Trust values are locally computed, cryptographically anchored, and globally reconciled through a DAG structure that enables resilience against adversarial behavior, partial failures, and network asynchrony.

We present the system architecture, trust computation model, and propagation mechanisms, followed by a simulation-based evaluation assessing stability, convergence, and robustness under adversarial conditions. Results demonstrate that the proposed layer maintains trust consistency and reproducibility across varying network sizes and attack scenarios, making it suitable for IoT, edge AI coordination, and cross-domain distributed systems.

Keywords

Distributed Systems; DAG; Trust Verification; IoT Networks; Edge Computing; Network Security

1. Introduction

Distributed networks increasingly operate without centralized authority while requiring reliable coordination among heterogeneous participants. Examples include IoT ecosystems, edge computing platforms, decentralized AI systems, and cross-organizational data networks. While cryptographic identity, consensus protocols, and secure messaging address authentication and data integrity, they do not provide a continuously verifiable representation of trust within the system.

Trust is often implicitly assumed rather than explicitly modeled. Static credentials confirm identity but do not reflect behavioral reliability over time. Reputation systems provide probabilistic signals but lack reproducibility and resistance to coordinated manipulation. Blockchain-based consensus offers strong guarantees but introduces latency, energy costs, and scalability constraints unsuitable for many real-time or resource-constrained environments.

This gap becomes critical as networks move toward autonomous decision-making, where nodes must assess not only what data is received but whether the system state itself is trustworthy enough to act upon. Without a verifiable trust substrate, networks either over-centralize control or accept unquantified risk.

This paper proposes a DAG-based trust verification layer that treats trust as a system primitive rather than an emergent by-product. The approach enables trust to be computed, updated, and validated across distributed nodes in a scalable and adversarially resilient manner.

2. Related Work

Trust in distributed systems has been approached through several paradigms:

Public Key Infrastructure (PKI) establishes identity authenticity but does not encode behavioral trust or temporal reliability. Once issued, credentials remain valid independent of system behavior.

Reputation Systems aggregate feedback or interaction histories to estimate trustworthiness. While useful in open systems, they are susceptible to Sybil attacks, collusion, and non-reproducibility across observers.

Blockchain and Consensus Protocols provide strong guarantees of state agreement but are optimized for transactional finality rather than continuous trust assessment. Their cost and latency limit applicability to large-scale IoT and edge environments.

DAG-Based Ledgers improve scalability and throughput by relaxing total ordering, but primarily focus on transaction validation rather than trust semantics.

IoT Trust Frameworks often rely on centralized scoring or domain-specific heuristics, limiting interoperability and long-term reliability.

The proposed approach differs by introducing a trust-native DAG layer that explicitly models trust propagation, validation, and convergence independently of transaction consensus.

3. System Architecture

3.1 Overview

The system introduces a logical trust layer operating alongside existing network and application stacks. Nodes participate by producing and validating trust events derived from verifiable interactions.

The architecture consists of:

Nodes: Network participants (devices, services, agents)

Trust Events: Signed records of verified interactions

Trust DAG: A directed acyclic graph anchoring trust events

Validators: Nodes responsible for verifying event consistency

Observers: Nodes that consume trust state without validation duties

3.2 Trust DAG Structure

Each trust event references one or more prior events, forming a DAG. This structure:

Avoids single-chain bottlenecks

Enables parallel trust updates

Preserves causal ordering without global synchronization

Edges represent verified relationships, while vertices encode trust updates with timestamps and cryptographic signatures.

4. Trust Computation Model

Each node maintains a local trust vector representing its trust assessment of relevant peers. Trust updates occur when:

A verifiable interaction takes place

The interaction is validated locally

A trust event is generated and signed

The event is anchored into the DAG

Trust values evolve as a function of:

Interaction validity

Historical consistency

Network-wide corroboration

Formally, trust for node i at time t can be represented as:

Where:

� denotes verified events

� denotes validation outcomes

� is a bounded update function ensuring convergence

Global trust state emerges through aggregation of locally verified DAG paths rather than centralized scoring.

5. Simulation and Evaluation

5.1 Setup

Simulations were conducted on synthetic networks ranging from 30 to 500 nodes, with varying connectivity and interaction frequencies. Adversarial scenarios included:

Random faulty nodes

Coordinated malicious clusters

Event injection attempts

Network partitioning

5.2 Metrics

Evaluation focused on:

Stability: variance of trust values over time

Convergence: time to trust consistency across observers

Resilience: impact of adversarial behavior on trust integrity

Reproducibility: consistency of trust outcomes across simulations

5.3 Results

Results show:

Stable trust convergence under normal conditions

Bounded trust degradation under attack

Rapid recovery after adversarial removal

High reproducibility across independent runs

The DAG structure prevented single-point trust corruption and enabled localized containment of malicious behavior.

6. Application Scenarios

6.1 IoT Networks

Resource-constrained devices can rely on lightweight trust verification without participating in heavy consensus, improving security and autonomy.

6.2 Edge AI Coordination

Trust-aware scheduling allows edge nodes to determine when collective system state is reliable enough to trigger autonomous actions.

6.3 Cross-Domain Networks

The model supports trust interoperability across organizational and jurisdictional boundaries without requiring shared governance infrastructure.

7. Conclusion and Future Work

This paper introduced a DAG-based trust verification layer that elevates trust to a first-class system primitive in distributed networks. By decoupling trust from static identity and transactional consensus, the approach enables scalable, reproducible, and adversarially resilient trust assessment suitable for IoT and edge systems.

Future work includes:

Formal verification of convergence bounds

Integration with network control planes

Hardware-assisted trust validation

Interoperability with existing security frameworks

The results suggest that trust-native architectures are a necessary evolution for next-generation distributed systems.

End of paper. Author- Christiaan Prinsloo [Chris.prinsloo@forus.digital](mailto:Chris.prinsloo@forus.digital)