Blockchain-Assisted Trust Management for Secure Service Placement at the Edge

Mid-semester Presentation

Pedireddla Surya Venkata Mourya
(122CS0563)

Dept. of Computer Science & Engg., NIT Rourkela

October 22, 2025

Outline

Introduction

- **Edge Computing:** Processing data closer to its source (sensors, IoT devices, gateways) to reduce latency and enable real-time applications.
- **Security Challenge:** Edge nodes are distributed, resource-constrained, and vulnerable to attacks like unauthorized access, DDoS, and data tampering.
- **Current Problem:** Traditional centralized security creates single points of failure and lacks transparency.
- **Our Solution:** A blockchain-based trust management system that provides:
  - Decentralized security (no central authority)
  - Tamper-proof trust records
  - Secure service placement based on node trustworthiness

Motivation

- Edge computing brings data processing closer to sources (IoT, smart cities, autonomous vehicles) but introduces **new security challenges**.
- Traditional **centralized security mechanisms** create single points of failure and cannot scale for distributed multi-stakeholder environments.
- Edge nodes are **vulnerable to attacks**: unauthorized access, DDoS, data tampering, and service disruption.
- **Blockchain technology** offers decentralized, tamper-proof, and transparent trust management without relying on central authority.
- **Need:** A **lightweight blockchain-based system** for secure and trusted service placement in resource-constrained edge networks.

Literature Review

Survey of Related Work: We reviewed 5 key papers on blockchain and edge computing security.

Reference	Year	Main Focus	Limitations
Xiong et al., IEEE Comm. Mag.	2018	Blockchain with edge for mobile resource sharing	Heavy consensus overhead; unsuitable for constrained edge devices
Hasan et al., IEEE Access	2020	Comprehensive survey on blockchain-based edge security	Mostly theoretical; lacks practical lightweight implementation
Wang et al., Future Gen. Comp. Sys.	2021	Blockchain ledger for node reputation and task offloading	Does not evaluate scalability; consensus cost not optimized
Kumar & Panda, J. Network Comp. App.	2022	Lightweight blockchain (PBFT-Lite) for IoT edge	Prototype limited to small networks; no trust score adaptation
Kumar et al., IEEE IoT Journal	2023	Smart contracts for trust score calculation	High storage usage; performance degradation for large ledgers

Gap: Existing works lack lightweight, scalable frameworks with integrated trust-based service placement.

Research Gaps

From our literature analysis, we identified key gaps:

- **Resource Constraints Ignored:** Current blockchain solutions are too computationally expensive for resource-limited edge devices (limited CPU, memory, battery).
- **No Service Placement Integration:** Existing trust management models don't connect with actual service placement decisions – trust scores are calculated but not used.
- **Lack of Working Prototypes:** Most research is purely theoretical without real implementations or practical validation.
- **Scalability Issues:** High consensus and storage costs make existing systems impractical for large-scale edge networks.

⇒ **Our Contribution:** We address these gaps by developing a lightweight, practical blockchain framework with integrated trust-based service placement.

Objectives

The main objectives of this research project are:

1. **System Architecture Design:** Design a lightweight blockchain-based architecture seamlessly integrated with edge network orchestration and service management.
2. **Trust Management System:** Develop adaptive trust score calculation algorithms that track node behavior, reward reliability, and penalize failures.
3. **Working Prototype Implementation:** Implement a functional prototype demonstrating blockchain operations (block creation, chain verification, trust updates).
4. **Service Placement Policy:** Create a trust-based service placement mechanism that selects nodes based on trust thresholds and resource availability.
5. **Validation and Testing:** Validate the approach through simulation testing with 3-10 edge nodes and prepare for future SDN integration.

Methodology

Our Proposed Approach:

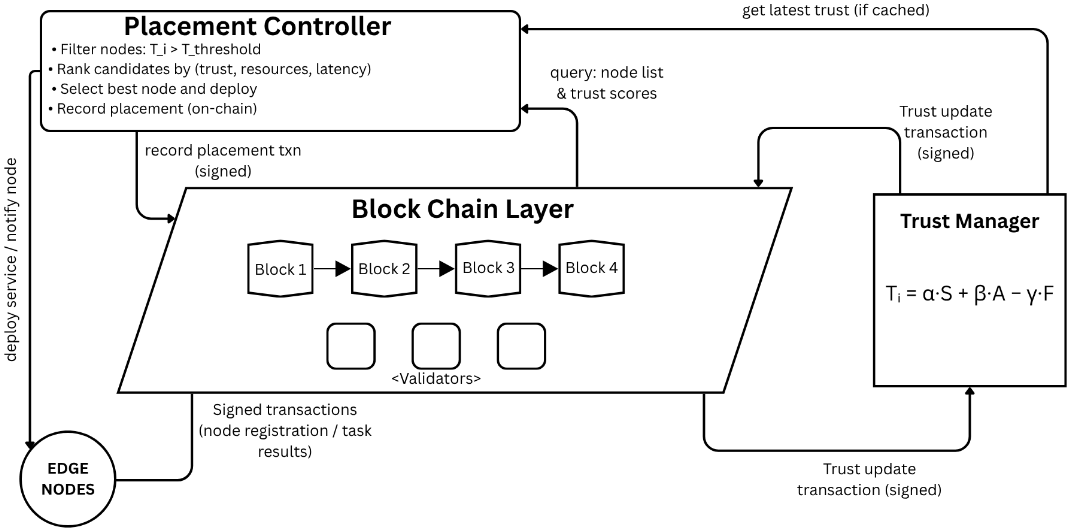
- **System Components:**
  - Edge Nodes: Register, execute services, report completion status
  - Blockchain Layer: Maintains distributed ledger of trust records and placements
  - Trust Manager: Calculates and updates trust scores based on behavior
  - Placement Controller: Makes service placement decisions (under development)
- **Trust Score Calculation:**

$$T_{new} = T_{old} + \alpha \cdot S - \beta \cdot F$$

  where S = success indicator, F = failure indicator, $\alpha = 5$ (reward), $\beta = 10$ (penalty)

- **Consensus Mechanism:** Proof-of-Authority (PoA) - lightweight, fast, and energy-efficient for resource-constrained edge devices.
- **Service Placement Policy:** Select nodes with $T_i > T_{threshold}$ (default: 60) based on highest trust and available resources.

System Architecture



Experimental Setup and Implementation

Development Environment:

Component	Technology
Language	Python 3.10
Cryptography	SHA-256 (hashlib)
Data Storage	JSON format
IDE	VS Code
Simulation	Single machine

Test Configuration:

- 5 edge nodes (varied resources)
- Initial trust score: 50
- Trust threshold: 60
- 10 test tasks executed

Implementation Status:

- Block creation & linking
- SHA-256 hash verification
- Trust score calculation
- Node registration
- Service placement (partial)

Initial Performance Results:

Metric	Value
Block creation time	0.15-0.25s
Trust update latency	< 0.05s
Chain verification	0.30-0.45s
Avg block size	2.5-3.2 KB

All operations complete in real-time

Discussion

Key Findings and Observations:

- **Blockchain Integrity:** Successfully demonstrated tamper-proof record keeping with chain verification detecting any modification attempts.
- **Trust Management Effectiveness:** Adaptive scoring accurately reflects node behavior with +5 rewards for success and -10 penalties for failures.
- **Performance Validation:** Efficient operation within edge constraints - block creation 0.2s, trust updates $<$0.05s, blocks 3KB.
- **Decentralization Benefits:** Eliminates single points of failure without requiring central authority for trust decisions.

Current Challenges:

- Limited to simulation environment (5 nodes) - physical hardware testing pending
- Basic consensus mechanism - Byzantine fault tolerance not yet implemented
- Security hardening needed (encryption, advanced authentication)

Conclusion & Future Work

green!20 **Completed (25-30%)**	**Remaining Work (70%)**
- System architecture design	▪ Full PoA consensus implementation
- Working blockchain prototype	▪ Service placement controller
- Trust score algorithms	▪ Testing with 10-50 nodes
- Basic testing & validation	▪ SDN integration
- Core operations verified	▪ Real edge hardware deployment
- Chain integrity proven	▪ Security hardening & encryption

Foundation established for full-scale implementation

References

- Z. Xiong, Y. Zhang, D. Niyato, and P. Wang, *"When Mobile Blockchain Meets Edge Computing,"* IEEE Communications Magazine, vol. 56, no. 11, pp. 75-81, 2018.
- M. Z. Hasan, M. H. Rehmani, and J. Chen, *"A Survey on Blockchain-Based Edge and Fog Computing Security,"* IEEE Access, vol. 8, pp. 182321-182344, 2020.
- L. Wang, X. Li, and J. Wu, *"Blockchain-Based Trust Management in Edge Computing,"* Future Generation Computer Systems, vol. 115, pp. 68-79, 2021.
- A. Kumar and S. K. Panda, *"Lightweight Blockchain for IoT and Edge Devices,"* Journal of Network and Computer Applications, vol. 175, pp. 103-115, 2022.
- S. R. Kumar, P. Gupta, and R. Singh, *"Decentralized Trust and Reputation Model Using Blockchain for IoT Edge,"* IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2451-2463, 2023.

Thank You!

Questions?