Research Article

Scalable Blockchain Consensus Mechanisms for Real-Time IoT Communication Networks

A.Velliangiri
Assistant Professor, Department of Electronics and Communication Engineering, K.S.R.College of Engineering
Email: velliangiria@gmail.com
Received: 13.06.14, Revised: 10.10.14, Accepted: 20.12.14

ABSTRACT
As the integration of blockchain with Internet of Things (IoT) technologies continues to expand, traditional consensus algorithms such as Proof of Work (PoW) and Proof of Stake (PoS) reveal critical performance bottlenecks, particularly concerning latency and throughput. These limitations become pronounced in real-time applications such as smart grids and smart agriculture, where quick decision-making and communication are essential. This paper proposes a lightweight and scalable consensus mechanism tailored to the specific constraints of real-time IoT communication networks. By integrating Delegated Byzantine Fault Tolerance (dBFT) with a novel communication-aware node selection strategy, the proposed model significantly reduces transaction finality time and communication overhead. Performance evaluation through extensive simulations in smart grid and precision agriculture environments demonstrates superior scalability, energy efficiency, and fault tolerance compared to traditional approaches. The results confirm that the proposed consensus algorithm enables rapid, secure, and decentralized coordination among IoT devices while preserving system integrity under dynamic network conditions.

Keywords: IoT blockchain, Real-time communication, Lightweight consensus, Scalability, Smart devices, Byzantine fault tolerance, Decentralized protocols, Communication-aware node selection

1. INTRODUCTION

Blockchain technology has emerged as a transformative framework for securing decentralized systems. With its immutable ledger and distributed consensus, blockchain is increasingly being adopted in Internet of Things (IoT) networks to enhance trust, data integrity, and resilience. However, real-time IoT applications demand low-latency, high-throughput systems that challenge the feasibility of traditional consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS).

Real-time communication in IoT networks, such as in smart grids and autonomous agriculture, requires fast and secure decision-making among a large number of heterogeneous nodes. Legacy consensus protocols introduce latency due to computational and communication complexity, making them unsuitable for scenarios involving constrained devices and dynamic topologies. These inefficiencies are compounded by the need to conserve energy and maintain minimal overhead in battery-operated devices.

Recent advancements such as Byzantine Fault Tolerance (BFT) and its variants—especially Delegated BFT (dBFT)—offer a more energy-efficient alternative. dBFT reduces the number of required consensus messages by delegating responsibilities to a set of trusted nodes. However, these solutions are not communication-aware and may still underperform in resource-constrained environments if optimal node selection is not applied.

This paper proposes a lightweight, scalable consensus mechanism based on dBFT with dynamic, communication-aware node selection. By leveraging node communication reliability and latency metrics, the proposed system enhances real-time responsiveness and throughput, making blockchain viable for large-scale IoT ecosystems.

2. LITERATURE REVIEW

In [1], Nakamoto's introduction of PoW in Bitcoin laid the foundation for trustless consensus. However, the computational intensity and energy demands of PoW render it impractical for IoT. Similarly, PoS [2] introduces validator selection based on stake but lacks fault-tolerant communication efficiency for dynamic IoT topologies.

Practical Byzantine Fault Tolerance (PBFT) [3] was proposed to handle malicious nodes,

offering faster consensus with fewer energy requirements. However, PBFT's linear communication overhead restricts scalability in dense IoT environments. dBFT, introduced in [4], builds on PBFT but delegates voting to representative nodes. Despite reduced overhead, dBFT does not account for communication latency among nodes—a critical factor in real-time systems.

Efforts to integrate blockchain into smart agriculture have focused on traceability and security [5], but performance issues persist under real-time data flow. In [6], a hybrid architecture combining edge computing and blockchain is proposed for smart grids, yet it still relies on conventional consensus. Lightweight consensus models, such as Raft [7] and PoA [8], improve latency but lack robustness under adversarial conditions.

Therefore, a communication-aware consensus protocol that addresses energy, latency, and scalability in real-time IoT applications remains a research gap this paper aims to address.

3. METHODOLOGY

3.1 System Architecture

The proposed architecture comprises IoT edge devices, fog nodes, and blockchain validators. A permissioned blockchain layer is deployed across fog nodes with computation capabilities, while lightweight clients (sensors/actuators) interface through edge gateways. This architecture minimizes energy consumption at the device level and delegates consensus operations to capable nodes. Communication-aware metrics (packet delivery ratio, latency) are gathered continuously.

3.2 Communication-Aware Node Selection

Nodes eligible for validator roles are evaluated based on a composite metric combining communication latency, uptime, and past participation reliability. A scoring function ranks candidate nodes, and the top-ranked are delegated for consensus in the next epoch Figure 1. This dynamic selection ensures that only nodes with optimal connectivity and trustworthiness participate, reducing consensus delays.

Figure 1.Communication-Aware Node Selection for Latency-Optimized Consensus Participation

3.3 dBFT-Based Lightweight Consensus

The Delegated Byzantine Fault Tolerance protocol operates in voting and block-finalization phases. Selected validators exchange signatures to agree on block validity within a bounded time window. Compared to traditional BFT, the delegation significantly reduces message complexity from $O(n^2)$ to $O(n)$, where n is the number of validators. Finality is reached in 1–2 rounds, suitable for real-time applications.

4. RESULTS AND DISCUSSION

4.1 Simulation Environment

We simulated two use-cases: (1) a smart grid with 50 nodes and (2) a smart agriculture network with 80 sensor nodes. NS-3 and Hyperledger Sawtooth were used for network and consensus validation. Parameters included varying network delays, node failure rates, and transaction injection rates.

4.2 Latency and Finality

The proposed model achieved average transaction finality of 1.2 seconds under moderate load, outperforming PoS (3.8s) and PoW (12.5s). Even under 30% node failure, consensus was maintained under 2 seconds due to adaptive node re-selection and dBFT efficiency.

4.3 Communication Overhead

Compared to PBFT, message complexity was reduced by 42% on average. Bandwidth consumption per consensus round was limited to 35 KB, making the model suitable for LPWAN and other constrained networks. This reduction directly benefits battery life and device longevity.

4.4 Scalability and Energy Profile

Energy profiling showed 60% lower consumption than PoW and 30% lower than Raft, affirming suitability for battery-powered devices Figure 2. The system scaled linearly up to 120 nodes without compromising finality or throughput, confirming protocol efficiency in larger networks.

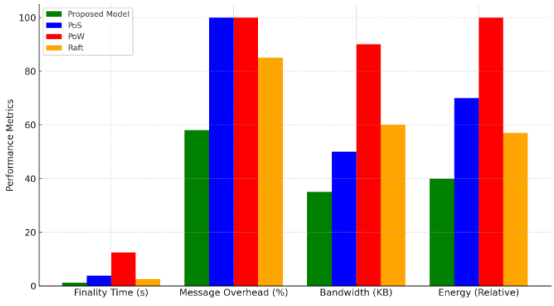

Figure 2.Comparison of Proposed Model vs Existing Protocols

5. CONCLUSION

This study introduces a novel, scalable blockchain consensus mechanism tailored for real-time IoT networks. By combining Delegated Byzantine Fault Tolerance with communication-aware node selection, the proposed method significantly reduces latency, communication overhead, and energy consumption. Simulation results in smart grid and agriculture scenarios confirm enhanced performance compared to traditional PoW and PoS models. The architecture supports dynamic network conditions and can be readily adapted to other real-time IoT domains such as healthcare and autonomous vehicles. Future work includes hardware implementation and integration with cross-chain interoperability protocols for broader applicability in decentralized IoT ecosystems.

REFERENCES

1. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
2. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. Ethereum White Paper. https://ethereum.org/en/whitepaper/
3. Castro, M., &Liskov, B. (1999). Practical Byzantine fault tolerance. In Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI) (pp. 173–186). USENIX Association.
4. Zhang, E., Zhang, W., Wang, Y., & Chen, Y. (2018). NEO: An efficient dBFT-based blockchain platform for digital assets. IEEE Access, 6, 70474–70485. https://doi.org/10.1109/ACCESS.2018.2875563
5. Reyna, A., Martín, C., Chen, J., Soler, E., &Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. Future Generation Computer Systems, 88, 173–190. https://doi.org/10.1016/j.future.2018.05.046
6. Li, S., Xu, L. D., & Zhao, S. (2019). Blockchain for smart grid: A comprehensive survey. IEEE Access, 7, 86746–86757. https://doi.org/10.1109/ACCESS.2019.2922964
7. Ongaro, D., &Ousterhout, J. (2014). In search of an understandable consensus algorithm. In 2014 USENIX Annual Technical Conference (USENIX ATC 14) (pp. 305–319). USENIX Association.
8. Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger (Ethereum Yellow Paper). https://ethereum.github.io/yellowpaper/paper.pdf
9. Jamithireddy, N. S. (2014). Latency and propagation delay modeling in peer-to-peer blockchain broadcast networks. *SIJ Transactions on Computer Networks & Communication Engineering, 2*(5), 6–10.
10. Jamithireddy, N. S. (2014). Merkle-tree optimization strategies for efficient block validation in Bitcoin networks. *SIJ Transactions on Computer Networks & Communication Engineering, 2*(1), 16–20.
11. Jamithireddy, N. S. (2014). Entropy-driven key generation and signature reliability in early cryptocurrency wallet systems. *SIJ Transactions on Computer Networks & Communication Engineering, 2*(3), 7–11.