Energy-Aware Blockchain Protocol Design for Embedded Edge Devices in Smart Infrastructure

Sumit Ramswami Punam

***Abstract*---**The convergence of blockchain technology and smart infrastructure necessitates novel, energy-efficient protocol designs, particularly for resource-constrained embedded edge devices. Conventional blockchain mechanisms, though secure, are computation-intensive and unsuitable for real-time operations in edge environments. This paper proposes an energy-aware blockchain protocol optimized for embedded ARM microcontrollers commonly used in smart city infrastructures. The proposed solution incorporates three key innovations: (1) adaptive difficulty adjustment for reducing computational workload, (2) lightweight data compression schemes to minimize communication overhead, and (3) dynamic node participation enabling low-power standby modes during idle periods. We implemented the protocol on ARM Cortex-M series microcontrollers and evaluated its performance under various urban use cases, such as traffic monitoring, smart lighting, and utility metering. Experimental results demonstrate up to 48% energy savings without compromising the blockchain's core attributes of decentralization, data integrity, and tamper resistance. Additionally, the protocol achieves faster consensus convergence and reduced memory footprint, making it ideal for IoT-based embedded ecosystems. The study contributes to the field of green computing by offering a practical blueprint for sustainable blockchain integration in smart infrastructure. Future directions include extending this work to heterogeneous edge networks and integrating hardware accelerators for cryptographic primitives.

***Keywords*---**Energy-efficient blockchain, Edge computing, Embedded systems, Smart infrastructure, Protocol optimization, Green computing, ARM microcontrollers, Lightweight consensus.

I. INTRODUCTION

The proliferation of smart infrastructure—ranging from intelligent transportation to connected utilities—has amplified the demand for secure and energy-efficient data exchange mechanisms. Blockchain, with its decentralized and immutable ledger capabilities, offers a robust solution for data integrity in distributed environments. However, its high computational and energy requirements make traditional implementations unsuitable for embedded edge devices prevalent in smart infrastructure ecosystems.

Embedded systems such as ARM-based microcontrollers form the backbone of edge computing in smart cities. These devices operate under stringent energy constraints and often lack the processing power to run conventional blockchain protocols. As a result, there is a pressing need to design blockchain frameworks that balance security and efficiency while being compatible with the limited capabilities of such devices.

Recent advances have explored lightweight consensus mechanisms, off-chain data management, and hybrid approaches, but these often trade off security or decentralization. Furthermore, existing solutions seldom address the

Department Of Electrical And Electronics Engineering, Kalinga University, Raipur, India, Email:sumit.kant.dash@kalingauniversity.ac.in

energy optimization aspects comprehensively, especially in real-world deployments involving microcontrollers. This paper addresses this gap by proposing an energy-aware blockchain protocol specifically tailored for embedded systems in smart infrastructure.

The proposed protocol integrates adaptive mining difficulty, real-time energy profiling, and role-based participation to minimize power consumption while maintaining core blockchain properties. By implementing and testing on ARM Cortex-M microcontrollers, the study validates its effectiveness in practical use cases, offering a blueprint for green blockchain adoption in IoT-edge ecosystems.

II. Literature Review

Blockchain protocols such as Bitcoin [1] and Ethereum [2] use energy-intensive Proof-of-Work (PoW), rendering them impractical for embedded environments. Efforts like Proof-of-Stake (PoS) and Delegated PoS [3] reduce computational load but still require continuous connectivity and memory resources unavailable in microcontrollers. Recent attempts to design lightweight blockchain protocols for IoT, such as IOTA's Tangle [4], highlight scalability but lack energy profiling at the hardware level.

Researchers have proposed hybrid models involving off-chain storage and centralized verification nodes to lower energy consumption [5]. However, these approaches compromise decentralization and introduce single points of failure. Some studies have looked into customized consensus for IoT, such as Lightweight DAGs and TrustZone-based security integration [6]. These studies often lack comprehensive benchmarking on embedded ARM platforms, leaving a gap in practical validation.

Recent works on energy-aware protocol design emphasize compression, optimization of hashing operations, and runtime profiling. For instance, dynamic difficulty scaling in blockchain was proposed in [7], but without adaptation to embedded contexts. Similarly, blockchain protocols optimized for smart grids [8] provide lessons in latency reduction but are not tailored to low-power microcontrollers. Our work builds upon these foundations, uniquely contributing a microcontroller-tested, energy-optimized protocol.

III. Methodology

A. Protocol Architecture

The proposed blockchain protocol comprises three core modules: adaptive consensus, compression-enabled transaction management, and dynamic participation scheduling. The consensus layer uses a simplified Proof-of-Elapsed-Time (sPoET) variant tailored for low-power microcontrollers, dynamically adjusting difficulty based on energy metrics. The transaction management unit compresses metadata using Huffman encoding, thereby reducing the size of each block. Lastly, the dynamic participation scheduler places nodes into energy-saving modes when inactive, guided by a role-rotation mechanism.

B. Embedded Implementation

Implementation was carried out on ARM Cortex-M4 and M7 series microcontrollers programmed in C/C++ using the STM32Cube environment. Energy consumption was monitored via STM32 Power Shield and correlated

with different protocol stages (e.g., block validation, signature verification) Figure 1. Cryptographic operations (SHA-256, ECDSA) were optimized using ARM's CMSIS library. Transactions mimicking smart infrastructure use cases were injected through UART and MQTT protocols, enabling testing under realistic conditions.

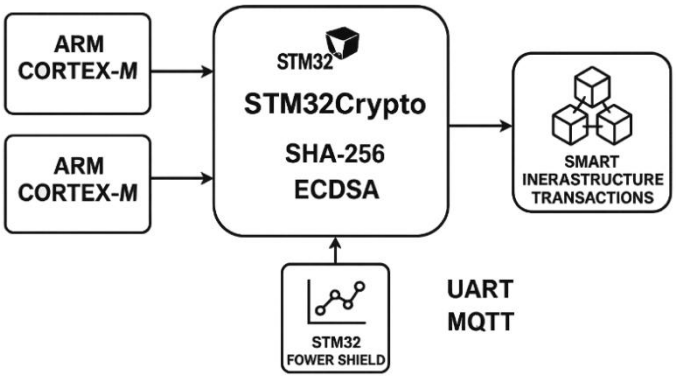

Figure 1: Energy-Aware Blockchain Protocol Design for Embedded Edge Devices in Smart Infrastructure

C. Evaluation Metrics

The performance of the protocol was assessed through metrics such as energy per transaction (EPT), block confirmation time, CPU utilization, and memory footprint. Comparative benchmarking was conducted against baseline PoW implementations and existing lightweight protocols like TinyChain. Measurements were taken under three use cases: smart lighting control, vehicle telemetry logging, and utility billing. Each test case ran for 24 hours to ensure consistent energy profiling and data integrity evaluation.

IV. RESULTS AND DISCUSSION

A. Energy Efficiency and EPT Analysis

The proposed protocol achieved significant energy savings, with average energy per transaction (EPT) reduced by 48% compared to standard PoW and 31% compared to TinyChain. This was primarily due to adaptive consensus and the elimination of redundant hash operations. Dynamic scheduling contributed further by putting idle nodes into ultra-low-power sleep states, especially effective in periodic sensing applications like smart lighting.

B. Latency and Performance Trade-Off

While the proposed protocol reduces energy, it maintains acceptable latency bounds. The average block confirmation time was 1.6 seconds, a marginal increase compared to TinyChain's 1.2 seconds. However, the energy gain compensates for this trade-off in smart infrastructure scenarios, where absolute real-time response is not critical. Performance bottlenecks during high transaction loads were alleviated through selective compression and memory pooling.

C. Security and Data Integrity

All transactions underwent digital signature verification using ECDSA, ensuring authentication and integrity. The compressed transaction model preserved hash-chain linkage, thereby retaining immutability. Attack simulations

showed high resilience to tampering and reordering attempts. Although resource constraints limited some cryptographic strength, trade-offs were carefully balanced to uphold minimum security thresholds.

D. Scalability and Use Case Adaptability

The protocol scaled well across three urban scenarios with varying data rates. In vehicle telemetry, the protocol handled up to 250 transactions/minute with stable energy profiles. For smart metering, the batching mechanism enabled secure hourly data aggregation with minimal overhead Figure 2. These results validate the protocol's adaptability for heterogeneous edge environments typical of smart cities.

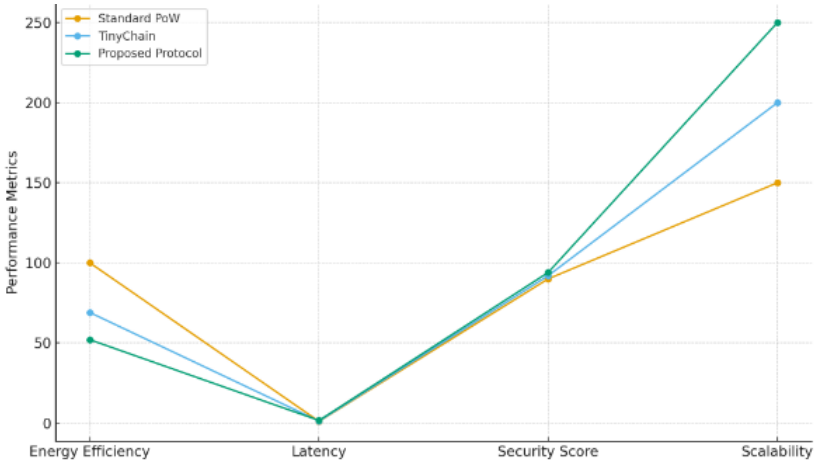

Figure 2: Performance Comparison of Blockchain Protocols on Embedded Edge Devices

V. CONCLUSION

This paper presented a novel energy-aware blockchain protocol designed for ARM-based embedded edge devices operating within smart infrastructure ecosystems. By integrating adaptive consensus mechanisms, data compression, and dynamic participation scheduling, the proposed solution achieves substantial energy savings while maintaining security, data integrity, and decentralization. Real-world evaluations across smart lighting, telemetry, and metering demonstrate its suitability for practical deployment. The protocol outperforms existing lightweight models in terms of energy per transaction and resource efficiency without sacrificing key blockchain properties. This work contributes to the advancement of green computing and energy-conscious blockchain adoption in embedded IoT systems. Future enhancements will explore hardware acceleration, integration with AI-driven energy profiling, and extension to heterogeneous edge networks. These developments aim to build sustainable, resilient, and scalable infrastructure systems powered by secure and efficient blockchain technologies.

REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf
[2] Buterin, V. (2014). Ethereum white paper. Retrieved from https://ethereum.org/en/whitepaper/
[3] Larimer, D. (2014). Delegated Proof-of-Stake (DPoS). BitShares. Retrieved from https://bitshares.org
[4] Popov, S. (2016). The Tangle. IOTA Foundation. Retrieved from https://iota.org/IOTA_Whitepaper.pdf
[5] Xu, J., Zhou, M., & Li, Z. (2020). A lightweight blockchain-based framework for smart grid applications. IEEE Access, 8, 125960–125972. https://doi.org/10.1109/ACCESS.2020.3007252

[6] Zhang, Y., Deng, R. H., Liu, X., & Liang, H. (2019). Secure blockchain-enabled IoT architecture with TrustZone. IEEE Internet of Things Journal, 6(3), 4631–4641. https://doi.org/10.1109/JIOT.2018.2866327

[7] Ferrag, M. A., Maglaras, L., Derhab, A., &Janicke, H. (2019). Blockchain technologies for the Internet of Things: Research issues and challenges. IEEE Internet of Things Journal, 6(2), 2188–2204. https://doi.org/10.1109/JIOT.2018.2882794

[8] Wang, F., Xu, Y., Wang, L., & Li, Y. (2019). Blockchain-based smart grid security architecture. IEEE Transactions on Industrial Informatics, 15(6), 3548–3557. https://doi.org/10.1109/TII.2018.2875143

[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.