Remote BLS Signing on Raspberry Pi: A Study in Lightweight Cryptographic Infrastructure

Dalhousie University of British Columbia
Department of Attestation and Ledger Studies (DALS)

August 2025

Abstract

This paper presents an investigation into the feasibility of deploying a Boneh–Lynn–Shacham (BLS) remote signer on Raspberry Pi-class commodity hardware in the context of the Tezos blockchain. The project, operated under the auspices of the fictional *Dalhousie University of British Columbia (DUBC)*, explores whether such constrained hardware can perform remote signing duties with sufficient reliability and security for participation in consensus.

Our work leverages the `tezos-rpi-bls-signer` implementation and targets the Seoulnet test network, with emphasis on aggregated attestations and the operational requirements discussed in the Tezos Agora ecosystem. Metrics include signing latency, attest throughput, and resource utilization under varying load conditions.

We argue that BLS-based cryptographic infrastructure need not be confined to industrial-scale clusters. By demonstrating viability on Raspberry Pi, we show that threshold signatures, multiparty cryptography, and future extensions can be prototyped on low-power, widely available hardware. This accessibility aligns with the decentralization ethos, widening the scope of participation in advanced consensus research.

Keywords: Tezos; BLS Signatures; Remote Signer; Raspberry Pi; Aggregated Attestations; Commodity Hardware; Distributed Ledger; Cryptographic Infrastructure

1 Introduction

The design of secure remote signers is critical to the operation of proof-of-stake blockchains such as Tezos. Recent advances, including the introduction of BLS signatures and aggregated attestations, impose new requirements on signing infrastructure. While production deployments often rely on dedicated HSMs and enterprise-class servers, the role of commodity hardware as a research and educational platform has not been fully explored.

This paper investigates the deployment of a BLS signer on Raspberry Pi hardware. We seek to answer whether such devices can produce reliable cryptographic attestations in a live test network environment, and what trade-offs emerge in terms of performance, security, and maintainability.

2 Related Work

The Tezos community has documented operational considerations for aggregated attestations on public forums such as Tezos Agora (Heads-Up for Bakers). In parallel, remote signing frameworks and hardware-backed approaches (e.g., enterprise HSMs) have been evaluated for security and throughput. Our contribution is to examine the feasibility envelope on a low-power, readily available single-board computer while focusing specifically on BLS signing requirements.

3 Methodology

We deployed `tezos-rpi-bls-signer` on a Raspberry Pi 4B with 4 GB RAM, networked to a Seoulnet test node. Systemd hardening, firewall rules, and monitoring were configured to simulate a responsible operator environment. Metrics were collected on signing latency, CPU/memory utilization, and attest success rates under both nominal and stressed conditions.

The experiment spanned multiple epochs on Seoulnet to observe signer behavior under differing chain conditions. Configuration artifacts included a systemd service unit, read-only root filesystem for the signer user, and IP allowlists between the node and signer. Logs and metrics were exported for later analysis.

4 Results and Discussion

Preliminary results indicate that the Raspberry Pi platform is capable of meeting the minimum requirements for BLS attestation signing. Median signing latency remained within acceptable thresholds for timely inclusion. CPU utilization increased under peak attestation aggregation but did not compromise availability, and memory consumption remained stable throughout the observation window.

These findings suggest that Pi-class hardware can serve as a viable environment for prototyping threshold signatures and remote signer research. While single-board devices are unlikely to replace industrial setups for high-value mainnet operations, they provide an accessible platform for education, testing, and iterative development, thereby broadening participation in consensus research.

5 Conclusion

The Dalhousie Baker project demonstrates that BLS signing can be explored on lightweight, accessible hardware without compromising the spirit of research and participation. Future work includes multi-party key sharing experiments, comparisons with industrial remote signing frameworks such as Signatory, and the integration of longer-term monitoring to capture degradation or drift in resource profiles over time.

Acknowledgments

We thank the Tezos community for open discussions on aggregated attestations (Agora thread), and our industrial cousin DalekBaker.io for inspiration and methodological contrast.