FINAL REPORT

ZERO-KNOWLEDGE PROOF OF

INNOCENCE IN CARDANO

Project #1300197

Name of the project: Zero-Knowledge Proof of innocence on Cardano - Encoins + Módulo P + Eryx

Project number: #1300197

Name of project manager: Agustín Salinas

Date project started: Jan 20, 2025

Date project completed: May 30, 2025

Challenge KPIs and how the project addressed them

Challenge: Cardano Use Cases - Concept

1. *Disruptive ideas for industrial innovation using Cardano blockchain and smart contracts.*
   We generated a framework that, when on mainnet, is going to facilitate the onboarding of different applications to Cardano, some of which are existent in other chains and some, completely new.
2. *DeFi solutions that learn from and improve on projects in other ecosystems.*
   The need for a proof of innocence protocol has come to the attention of all blockchains as a solution to legal issues around the implementation of on-chain mixers. Other ecosystems are already actively using this protocol. We implemented a framework to make it possible in Cardano.
3. *Web3 identity, privacy, oracles, and zero knowledge applications and implementations.*
   We created a tool to enhance privacy in the ecosystem using ZK technologies, integrated with oracles of different sets of banned transactions.

Furthermore, the project:

1. Works as a solution to a real world problem. to help the regulation of anonymous transaction systems like mixers.
2. Acts as a proof of concept implementation:
   a. Implementing this technology for the first time in Cardano.
   b. Working as a prototype for a future mainnet implementation.
   c. Helped learn about the challenges of implementing this in a product discovery stage.
3. Is open source.

Project KPIs and how the project addressed them

1. *Contribute to link the applied cryptography ecosystem with Cardano.*
   We're fostering the joint work of people from different backgrounds, in order to generate multidisciplinary solutions for the chain's needs.
2. *Improve the privacy of Cardano users.*
   We achieved this by getting the community closer to having PoI in mainnet.
3. *Improve the liquidity for Cardano.*
   As it'll be safer for people to trust their funds in Cardano without risking being linked to malicious activities.

Key achievements (in particular around collaboration and engagement)

1. We have done extensive research about the Proof of Innocence protocol:
    a. We detailed explained how the protocol works both from a technical and solution perspective;
    b. We defined an implementation of the protocol in the context of the Cardano blockchain;
    c. We specified security and cryptographic guidelines about how to integrate this protocol in production.
2. We implemented the circuits used to build the Zero-Knowledge proofs of the protocol.
3. We implemented the smart contracts with the logic of the protocol, these validators were designed in a modular fashion so services can embed them in its services.
4. We integrated the above in a CLI interface that can run transactions with the key features and interactions of the protocol. This application demonstrated how an actual PoI application works in the pre-production testnet.

Key learnings

1. We learnt how to build a ZK application in Cardano.
2. We worked with testing frameworks both for Circom and Aiken.
3. We used MeshJS to build transactions to interact with the blockchain.
4. We can verify Groth16 proofs for an on-chain real application, within the processing and memory usage limits of Cardano transactions.
5. We found huge potential for more ZK frameworks in Cardano.

Next steps for the product or service developed

1. Integration with suitable hash functions
2. Make an application with a UI that is focused in usability
3. Extensive audits
4. Deploy in mainnet

Final thoughts/comments

We successfully implemented a prototype of the Proof of Innocence protocol in a minimum viable product form, which is able to perfectly run on the preprod chain. With our ZK and blockchain experience, we were able to successfully execute the implementation plan.

This should serve as a motivation to facilitate more privacy-forward solutions.

Links to other relevant project sources or documents.

1. Original research document detailing basic concepts and initial challenges.
2. Practical report explaining how to run tests and use the protocol in the preprod chain with the CLI.

Link to Close-out video - must be either YouTube or Vimeo link only

Close-out video link