Final Report #1100066

Proposal name: Cardano Privacy Layer: Zero-Knowledge Proof-Based Membership Verification and Anonymous Voting & Signaling PoC.

Proposal link: **Cardano Privacy Layer: Zero-Knowledge Proof-Based Membership Verification and Anonymous Voting & Signaling PoC.**

Project number: #1100066

Challenge: Concept

Project manager: Agustín Salinas

Start Date: February 28, 2024.

Close date: January 22th, 2025.

Challenge KPIs

The challenge description considers the following areas of interest:

1. Disruptive innovation for industrial use cases using blockchain and smart contracts such as but not limited to applications for: alternative finance (Defi, RealFi), authenticated ownership and provenance, digital identity, Internet of Things, impact and social good, gaming and entertainment, manufacturing, marketplaces, oracles, supply chain and logistics, tokenization, zero-knowledge and privacy-preservation.
2. Blockchain research as it converges with other exponential technologies such as artificial intelligence, machine-to-machine, next-generation distributed compute.
3. Projects and ventures porting from other ecosystems to deploy on Cardano or bridging to other ecosystems.
4. Projects which make use of Cardano-based scaling solutions such as Hydra or alternatives

The project satisfies respectively each area of interest in the following way:

1. Since, on one hand, the project showcases the use of Zero-Knowledge cryptography; and, on the other hand, the project achieves a novel application in the area of privacy that can have further applications in governance, digital identity and private Defi. Therefore, we can conclude that the project implies innovation in the Cardano ecosystem.
2. Although the project in its first milestone conducts research in the application of Zero-Knowledge cryptography in the area of privacy, the scope of the project is not tightly related to other areas such as AI, machine-to-machine or next generation distributed computing.
3. Yes, the project indeed ventures porting a privacy protocol from the Ethereum ecosystem.

4. Currently, the project doesn't use any scaling solution since it is intended to be used in the L1, but it can be deployed in other scaling solutions such as Hydra.

Project KPIs

1. **Technical research and protocol adaptation design.**
   - We delivered a technical document that extensively explains the Semaphore protocol, each step required to adapt it and the actual design of the prototype.
   - Moreover, we did an implementation of the design, which was not part of the original scope of the milestone. We wrote the prototype in Aiken and we achieved a minimal viable implementation to make it work in Cardano. Also, we did some testing on the protocol to have security that the protocol works.
2. **Conducting the Trusted Setup Phase 2 Ceremony.**
   - We successfully arranged a trusted setup ceremony to derive the public keys of the protocols. We had **X participants** in the ceremony, which is over the 15 participants intended in the milestone.
   - We documented the theory and process of conducting the ceremony, and we shared resources that can be used for other projects to make similar ceremonies.

Key achievements.

- We could successfully create a first iteration of the Cardano-Semaphore protocol.
- We created a theoretical investigation that can be useful for projects that want to use Cardano-Semaphore in their Dapps, and also it is a good reference about how to develop such a protocol for any projects developing in ZK.
- We could conduct a multi-party process to derive the public keys for Cardano Semaphore. These keys ensure that any project wanting to benefit from Cardano Semaphore can generate protocol proofs securely.

Key learnings.

- We learned how to implement a complete Zero-Knowledge Application in Cardano. We faced different challenges regarding the development of these types of applications.
- We learned how Merkle Trees and similar data structures are key for efficiently verification a set of data.

Next steps for the product or service developed

There are several steps for the continuation of this project:

1. Create the off-chain components. This implies progressing on the off-chain components that we created, such as the library to interact with the protocol. As well, the protocol relies on relays to broadcast the transactions, such relays must be developed too.
2. Iterate and exhaustively test the smart contracts of the protocol.
3. Adapt the protocol to be a Voting application.

Final thoughts/comments

This project was a groundbreaking experience, as we learned to implement a complete Zero-Knowledge application. This process involved designing circuits to generate proofs, implementing smart contracts, and conducting a trusted setup to ensure safe usage. We are excited to continue this project, as the progress achieved represents a significant innovation within Cardano. The Cardano-Semaphore protocol offers numerous applications in the privacy domain, including identity verification, private voting, and mixing applications. We are particularly interested in further developing this protocol to create the first fully private voting dApp on Cardano.

Relevant resources.

1. **Research:**
   https://github.com/Modulo-P/Cardano-Semaphore/blob/main/docs/Research/Research-Semaphore-Modp-09-2024.pdf
2. **Smart contracts:**

   https://github.com/Modulo-P/Cardano-Semaphore

3. **Cardano-Semaphore public keys:**

   https://github.com/Modulo-P/Cardano-Semaphore/blob/main/keys/semaphore_final.zkey

4. **Ceremony document:**

   https://github.com/Modulo-P/Cardano-Semaphore/blob/main/docs/Ceremony/Cardano%20Semaphore%20%7C%20Official%20Ceremony%20-%20December%202024/Final%20Ceremony%20Document..pdf

Link to Close-out video.

Catalyst Fund 11: Cardano Privacy Layer