Final report #1000005

Proposal name: A Zero Knowledge Proof framework for Cardano based on Hydra and ZK-SNARKS

Proposal link: **A Zero Knowledge Proof framework for Cardano based on Hydra and ZK-SNARKS**

Project number: #1000005

Challenge: Development & Infrastructure
Project manager: Agustín Salinas

Start Date: October 3rd, 2023

Close date: April 16th, 2024
Challenge KPIs

As stated in the challenge description, one of the goals of the challenge is to improve the scalability of Cardano. In alignment with this goal, we implemented two solutions improving this area, namely: a) the Hydra incremental commitment feature, and b) a Zero-Knowledge validator. The main contribution of this proposal to the challenge is the latter, the Zero-Knowledge validator. This validator enables improvements in scalability, since the verification of algorithms can be pre-processed offchain beforehand. By sending computations in the form of proofs, these can be checked on-chain with less use of resources than verifying the computation itself. We tested the performance of these validators, and the execution budget stats will be taken as KPIs:

Second iteration of the zk-validator (using Plutus V2 primitives). The benchmark can be executed in the following repository executing “cabal test plutus-groth-test”

Plutus V2	CPU	Memory
Maximum	10000000000	14000000
Script use (single pairing)	362874651295	443016679
Script use (full proof check)	1334647992336	1663887424

Third iteration of the zk-validator (using the Plutus V3 primitives). The benchmark can be executed in the following repository executing “aiken check”.

Plutus V3	CPU	Memory
Script use (full proof check)	3124490278	78221

As we can see, the performance using the Plutus V3 primitives is approximately 427 times faster in cpu units and 21271 times more efficient in the use of memory than the V2 validator. This shows the improvement we made leveraging the next advancements in the Plutus Core language.

Project KPIs

First of all, some important statistics of the overall github activity of the project can be found here . This includes metrics of all key repositories of this proposal which are detailed in the “in-depth summary of achievements” document (the link is at the end of this report).

In second place, to showcase our solution, we developed a demo (the Mastermind game) which had the following stats:

- 300 visits
- 40 plays

The demo was promoted on X (formerly Twitter) by a member of IOG’s Hydra team, which naturally helped with some metrics regarding the public impact of the project. The tweet can be checked here

- 47,000 visualizations
- 556 likes
- 162 retweets
- 27 comments

Key achievements

The achievements of this proposal were:

1. We successfully developed one of the first Zero-Knowledge validators in Cardano. This validator can take Zero-Knowledge proofs and check whether the proof is valid. This is the first version of the validator written in both PlutusTx and Aiken. These versions only use UPLC V2, and concretely, the PlutusTx version is the one that we use in our demo.
2. We successfully developed a library to build Zero-Knowledge dapps called ak-381: It includes the second version of the validator which is written in Aiken and uses the UPLC V3 primitives; and some utilities that allow developers to build the proofs and verification keys in a way that is interoperable with the PlutusVM.
3. We developed a Hydra feature called Incremental Commitment, which allows users to asynchronously join and leave the Hydra heads.
4. We created a demonstration Dapp to showcase the project which explains the use of Zero-Knowledge proofs and the use of Hydra. This is one of the first fully Zero-Knowledge dapps in the Cardano ecosystem, which was recognized by the Hydra team and viral on Twitter.

Key learnings

- We got experience about the mathematical foundations of elliptic curves and zero-knowledge cryptography, and documented it.
- We learned how to develop an end-to-end zk-dapp.
- We learned how to develop a Hydra dapp.

Next steps

1. We think that the AK-381 library will be an important resource for the Cardano ecosystem to build zk-dapps. Thus, we want to keep developing the library and include more ZK protocols

to work with. Right now we implemented a protocol that is called Groth-16 which is known by its efficient verification and its light-weight proofs, however the downside is that it requires a trusted multi-party ceremony to construct de verification keys. Therefore, we want to include other protocols that, although not as efficient, have the upside of not requiring a trusted setup ceremony to obtain the verification keys.

2. We will use the AK-381 library to build a protocol that will bring privacy capabilities to Cardano L1 such as anonymous authentication and messaging. This will show another use-case of our developments achieved in this proposal.

Final thoughts

We are very glad to be pioneers in the field of Zero-Knowledge cryptography on Cardano. For sure these achievements will be a huge contribution to the community and future developers that will want to build on top of this technology. For further detail about the accomplishments of this proposal I suggest visiting the in-depth summary.

Resources

- **In-depth summary of achievements:** link
- **Demo dapp:** link
- **Research document:**link

Close-out video link