

ENCOINS V2 Close-out report

Name of project and Project URL on IdeaScale/Fund

ENCOINS v2

<https://milestones.projectcatalyst.io/projects/1100124>

Project Number

Project ID: 1100124

Name of project manager

Vladimir Sinyakov

Date project started

1 March 2024

Date project completed

23 July 2025

List of challenge KPIs and how the project addressed them

Produce ENCOINS v2 smart contract specification: A technical document containing ENCOINS v2 smart contract specification (PDF) was produced and shared publicly on GitHub.

Produce the guide to integrate ENCOINS v2 with other DApps: A technical document containing ENCOINS v2 integration guide (PDF) was produced and shared publicly on GitHub.

Produce the corresponding design concepts for the ENCOINS v2 UI: A Figma file with the Web UI assets was produced and shared publicly on GitHub.

ENCOINS v2 smart contract implementation: Modules for the ENCOINS v2 on-chain script (Haskell) were implemented and shared publicly on GitHub.

Implement the test suite to check the key properties of the smart contract: Modules to test the key properties of the ENCOINS v2 smart contract (Haskell) were implemented and shared publicly on GitHub.

Implement the off-chain code for the ENCOINS v2 smart contract: Modules containing the off-chain code to build transactions for ENCOINS v2 contract (Haskell) were implemented and shared publicly on GitHub.

Upgrade the ENCOINS relay to support v2 user requests: A new ENCOINS relay release that supports ENCOINS v2 requests made with CLI (Haskell) was developed and shared publicly on GitHub.

Implement ENCOINS v2 frontend UI: The code for ENCOINS v2 Web UI was implemented and shared publicly on GitHub.

Produce a fully functional application and run the application test on the Cardano Testnet: The complete code of ENCOINS v2 and a running application on the Cardano Testnet were produced. A video illustrating the main functions of the application was created and shared publicly. A close-out report detailing the results of the project was uploaded on GitHub.

List of project KPIs and how the project addressed them

Milestone 1: ENCOINS v2 documentation

- **Outputs:** A technical document containing ENCOINS v2 smart contract specification (PDF), a technical document containing ENCOINS v2 integration guide (PDF), and a Figma file with the Web UI assets were delivered.
- **Acceptance criteria:** The outputs were shared publicly with the community and uploaded on GitHub (<https://github.com/encryptedcoins/>).
- **Evidence of milestone completion:** The outputs are in the public repository on GitHub.

Milestone 2: ENCOINS v2 on-chain code

- **Outputs:** Modules for the ENCOINS v2 on-chain script (Haskell) and modules to test the key properties of the ENCOINS v2 smart contract (Haskell) were delivered.
- **Acceptance criteria:** The outputs were shared publicly with the community and uploaded on GitHub (<https://github.com/encryptedcoins/>).
- **Evidence of milestone completion:** The outputs are in the public repository on GitHub.

Milestone 3: ENCOINS v2 backend

- **Outputs:** Modules containing the off-chain code to build transactions for ENCOINS v2 contract (Haskell) and a new ENCOINS relay release that supports ENCOINS v2 requests made with CLI (Haskell) were delivered.
- **Acceptance criteria:** The outputs were shared publicly with the community and uploaded on GitHub (<https://github.com/encryptedcoins/>).
- **Evidence of milestone completion:** The outputs are in the public repository on GitHub.

Milestone 4: ENCOINS v2 frontend

- **Outputs:** The code for ENCOINS v2 Web UI was delivered.
- **Acceptance criteria:** The outputs were shared publicly with the community and uploaded on GitHub (<https://github.com/encryptedcoins/>).
- **Evidence of milestone completion:** The outputs are in the public repository on GitHub.

Final Milestone: ENCOINS v2 Testnet

- **Outputs:** The complete code of ENCOINS v2, a running application on the Cardano Testnet, a video illustrating the main functions of the application, and a close-out report detailing the results of the project were delivered.
- **Acceptance criteria:** The application website and the video were shared publicly. The video was uploaded on YouTube and shared on Twitter, with links provided to reviewers. The close-out report (pdf) was uploaded on GitHub and shared with reviewers.
- **Evidence of milestone completion:** Reviewers and testers can access the application through a website and watch the completion video.

Key achievements

The project successfully developed and deployed ENCOINS v2, a privacy protocol on Cardano, demonstrating its functionality on the Testnet. All planned documentation, smart contract code (on-chain and off-chain), and frontend UI were completed and publicly shared. A close-out video was also produced, illustrating the application's capabilities.

Key learnings

- **Deepened our understanding of Cardano architecture:** Throughout the development of ENCOINS v2, especially during the implementation of the on-chain smart contracts and their off-chain interactions, our team gained a profound understanding of Cardano's unique Extended UTXO (EUTXO) model, concurrency management, and transaction building processes. This practical experience was crucial in optimizing the protocol for efficiency and security on the Cardano blockchain.

- **Enhanced our software development practices:** The rigorous demands of developing a privacy protocol on a public blockchain, including stringent testing and the need for public documentation and integration guides, significantly enhanced our software development lifecycle. We refined our practices in areas such as robust testing methodologies, collaborative development, version control (GitHub), and creating comprehensive technical documentation for both developers and the wider community.

Next steps for the product or service developed

The immediate next steps for ENCOINS v2 involve **extensive testing on the Testnet**. This period will be crucial for identifying any potential issues, stress-testing the protocol's capabilities under various conditions, and ensuring its stability and security. Following this rigorous testing phase, and once we **get enough user feedback** to confidently address any discovered areas for improvement, we will proceed with **progressing to the Mainnet**. Concurrently, we **will try to do the audit next** to further validate the security and integrity of the ENCOINS v2 smart contracts and codebase by independent third-party experts.

Final thoughts/comments

-

Links to other relevant project sources or documents

Main project outputs:

<https://github.com/encryptedcoins/encoins-v2>

Application backend:

<https://github.com/zkFold/utxo-accumulator-server>

The smart contract code is available at

<https://github.com/zkFold/zkfold-cardano/blob/main/zkfold-cardano-scripts/src/ZkFold/Cardano/UPLC/UtxoAccumulator.hs>

Link to Close-out video

Close out video:

<https://www.youtube.com/watch?v=3qijQzgmFus>