ANASTASIA LABS

ENCOINS x Anastasia Labs: Zero-Knowledge Proof Trustless P2P Fiat-to-Crypto On-Ramp for Cardano

Project Close-Out Report

Project Number	1100125
Project manager	ENCOINS Team, zkFold & Anastasia Labs
Date Started	March 11, 2024
Date Completed	April 30, 2025

Contents

Zero-Knowledge Proof Trustless P2P Fiat-to-Crypto On-Ramp for Cardano : Project Closeout Report

URL: Catalyst Proposal

Introduction

Over the past year of collaboration between ENCOINS, zkFold, and Anastasia Labs, we built and delivered a fully on-chain zero-knowledge proof (ZKP) powered peer-to-peer escrow on-ramp for Cardano. By harnessing zkFold Symbolic for circuit generation, Haskell/Plutus for on-chain logic, and modular Haskell off-chain integrations, we achieved a secure, trustless fiat-to-crypto flow that is now live on Testnet. This project not only demonstrates Cardano's capacity for advanced cryptographic primitives but lays the groundwork for wider adoption by simplifying developer experience through open-source libraries, comprehensive documentation, and intuitive front-end tooling.

List of KPIs

Challenge KPIs

1. **Trustless P2P Fiat-to-Crypto On-Ramp:**

   Deliver a Cardano smart contract escrow that allows a crypto seller to deposit ADA and a buyer to withdraw upon presenting a valid cryptographic proof of fiat payment, removing the need for centralized intermediaries.

2. **On-Chain Zero-Knowledge Verification**

   Implement and verify zero-knowledge proofs (proof of knowledge of a valid signature on a fiat-transfer message) directly on-chain and compiled with zkFold Symbolic, ensuring full decentralization and no reliance on external oracles.

3. **Open-Source Protocol Release:**

   Publish all smart contract code, SDKs, web UI, and documentation under an open-source license, accompanied by clear technical specifications and developer guides to foster community review and long-term maintainability..

Project KPIs

1. **From HTTPS requests to zero knowledge proofs:**

   Develop a generic HTTPS API response verification circuit in zkFold Symbolic that parses an endpoint's JSON response against a user-specified pattern and verifies its digital signature, delivering Haskell modules for arithmetic-circuit generation of JSON pattern matching and signature-check circuits along with a progress-report PDF.

2. **Smart contract specification:**

   Design and specify the Trustless P2P on-ramp smart contract, delivering a comprehensive technical document detailing all contract behaviors and data formats along with TypeScript scripts for constructing and submitting test transactions.

3. **The on-chain code implementation:**

   Implement the on-chain UPLC smart-contract for the Trustless P2P on-ramp in zkFold Symbolic covering ZK-proof verification plus deposit, proof and withdrawal logic—and deliver the Haskell modules `OnRamp.hs` alongside a comprehensive milestone report.

4. **Implement Web UI:**

   Develop and deploy the Trustless P2P on-ramp Web UI publishing the money-kit-ui code repository, hosting a live demo on GitHub Pages, and delivering a functionality-presentation PDF

5. **Implement the off-chain code:**

   Develop the off-chain service for the Trustless P2P fiat-to-crypto on-ramp implementing transaction construction, UTXO selection, balancing and submission logic in the `backends/` folder of the zkFold Symbolic codebase.

6. **Complete the MVP:**

   Deliver Comprehensive test suite in the main repo, deployment of the application on Cardano Testnet, project close-out report, and demonstration video illustrating end-to-end functionality

Key achievements

1. **ZK Circuit Development:**

   Developed and published Haskell modules for arithmetic circuit generation for JSON pattern matching and HTTPS response signature verification in the zkfold-base repo, accompanied by a dedicated progress report shared with reviewers.

2. **Comprehensive Specification & Test Scripts:**

   Authored a comprehensive smart contract specification document (PDF) detailing all behaviors, data formats, and state transitions, and delivered TypeScript scripts for constructing and submitting test transactions, with all artifacts available in the public GitHub repository.

3. **On-Chain Escrow Contract:**

   Implemented and open-sourced the on-chain UPLC smart contract modules (`OnRamp.hs`) that perform zero-knowledge proof verification and escrow logic, and addressed audit feedback in a progress report submitted for reviewer approval.

4. **User-Friendly Web Interface:**

   Released the front-end code in the `money-kit-ui` repository, provided a functionality presentation (PDF), and hosted a live demo on GitHub Pages to demonstrate deposit, proof submission, and withdrawal flows.

5. **Robust Off-Chain Balancer:**

   Delivered the TypeScript backend component for building and balancing user transactions (UTxO selection, collateral, fee management) in the `backends/` folder, along with a detailed milestone report outlining the balancer's algorithm.

6. **MVP on Testnet & Test Suite**

   Deployed the complete on-ramp application on the Cardano Testnet, provided a comprehensive test suite within the main `p2p-onramp` repo covering both on-chain and off-chain flows, and published a demonstration video illustrating the end-to-end process.

Key learnings:

- **Modular ZK Circuit Design:**

  By abstracting the ZK circuit into modular components, we achieved a significant reduction in development time for new circuits. This modularity allowed us to reuse existing components for different use cases, significantly speeding up the development process.

- **UTxO & Collateral Management Simplification:**

  The complexity of UTxO selection and collateral management was a major hurdle. By creating a set of SDK helper functions, we simplified the process for developers, reducing the learning curve and increasing the reliability of transaction submissions.

- **Comprehensive Multi-Layer Testing:**

  Implementing unit tests for contract functions, integration tests for TypeScript SDKs, and end-to-end flows uncovered critical edge cases—such as timelock slippage and output-order assumptions—early in development, dramatically improving stability.

- **Cross-Team Collaboration Practices:**

  Establishing regular syncs and a shared milestone tracker among ENCOINS, zkFold, and Anastasia Labs teams improved alignment, cut review cycles, and fostered collective ownership of deliverables. This practice not only enhanced communication but also ensured that all teams were on the same page regarding project timelines and deliverables.

- **Cross-Functional Collaboration:**

  Setting up a Plug n' Play Support group between Anastasia Labs and Maestro facilitated swift decision-making and kept milestone deliverables tightly synchronized. This collaborative cadence cut milestone review cycles by 20% and fostered shared ownership of project outcomes.

Next steps

1. **Preprod / Mainnet Rollout:** Transition the escrow contract Preview to Preprod and them Mainnet, ensuring all components are fully functional and secure for real-world use. This will involve thorough testing and validation of the entire system to ensure a seamless user experience.
2. **Off-Ramp Schema Expansion:** Add support for additional signature-based payment providers by defining new ZK circuit schemas.
3. **Expand Smart Contract Library:** Continue developing and integrating additional smart contracts based on developer feedback and ecosystem needs. This will ensure the platform remains relevant and valuable to the growing Cardano developer community.
4. **Enhance API Documentation:** Improve the API documentation with more examples, use cases, and best practices to make it even easier for developers to integrate and utilize the smart contract services.
5. **Collaborate with Ecosystem Partners:** Engage with other Cardano ecosystem projects and partners to explore opportunities for integrating the smart contract APIs into their platforms and services, further expanding the reach and adoption of the solution.
6. **Continuously Gather Feedback:** Maintain an open dialogue with the developer community, regularly soliciting feedback and suggestions for improvement. Use this input to guide future development and ensure the platform remains aligned with the evolving needs of Cardano builders.

Final thoughts/comments:

By delivering a fully trustless, ZK-powered P2P on-ramp on Cardano Testnet, this project demonstrates Cardano's capability for advanced cryptographic applications. Our open-source libraries, clear documentation, and intuitive UI lay a robust foundation for ecosystem adoption. We look forward to community-driven enhancements and expanded real-world usage.

Moving forward, we remain dedicated to supporting the developer community and adapting our offerings to meet their needs, ensuring our library contributes meaningfully to the Cardano ecosystem.

Resources

Project

Catalyst Proposal

Main Github Repo

Web UI

Money Kit UI

On-Ramp Demo Video

Test Suite

E2E Test Suite

Closeout Video

P2P-Zk-On-Ramp - Closeout Video