1100125 - Project Progress Report (Milestone 3)

Project Title:

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

Project Overview:

Our objective is to create an escrow smart contract that utilizes zero-knowledge technology, enabling a fully trustless and decentralized peer-to-peer (P2P) exchange of fiat and cryptocurrency. This innovative feature will integrate seamlessly with the ENCOINS protocol, now operational on the Cardano mainnet. It also provides an adaptable solution that can function as a standalone application or be incorporated into wallets and other decentralized applications (DApps). Unlike prior proof-of-concept solutions, our approach incorporates an on-chain smart contract architecture optimized for Cardano's unique strengths, particularly its transaction determinism and parallelism, which support efficient, decentralized, and trustless operations.

Our solution will consist of a smart contract that enables crypto sellers to deposit funds into escrow while choosing preferred pricing and off-ramp options for fiat exchanges (such as fintech platforms, online banks, or centralized exchanges). This model requires all off-ramps to have systems capable of generating digital signatures as proof of fiat transfers, which the crypto buyers then use to create a zero-knowledge proof, verifying the legitimacy of the transfer on-chain and allowing the withdrawal of escrowed crypto. Additionally, a user-friendly frontend interface will be developed to provide direct access to the smart contract.

Project Impact:

This project aims to position the Cardano blockchain as the only known blockchain with an on-ramp feature accessible via a trustless, zero-knowledge proof-based escrow. With the deployment of this unique feature, we anticipate an increased flow of users and capital into the Cardano ecosystem. The open-source nature of the smart contract ensures that it will be available to the Cardano community, allowing for further enhancements and integrations. The success and impact of the project will be assessed based on the adoption and usage metrics of the smart contract and its front-end interface.

Progress on Milestones:

1. **Milestone 1** - *Implementation of HTTPS API Response Pattern Matching in zkFold Symbolic*:
   The first milestone focused on building foundational components that verify HTTPS API responses against predefined JSON patterns and ensure their signatures' validity. This involved developing two core modules in Haskell: one for generating arithmetic circuits for JSON pattern matching and another for signature verification on HTTPS responses. These modules are critical for the correct execution and security of API interactions, forming an essential part of the zero-knowledge proof infrastructure required for the smart contract's trustless operation.
2. **Milestone 2** - *Design of Smart Contract Specification and Development of Test Scripts*:
   In the second milestone, we concentrated on drafting a detailed technical document outlining the smart contract specification, covering all behaviors, data formats, and transaction workflows. Alongside this document, we implemented a suite of TypeScript scripts to simulate and test smart contract transactions. These scripts will enable thorough testing of various transaction types, assisting in the validation of contract functionality and robustness prior to mainnet deployment. This specification and testing framework ensures clear guidelines for the smart contract’s expected performance and is an essential reference for future integration.
3. **Milestone 3** - *On-Chain Code Implementation (zkFold Symbolic Smart Contract)*:
   The third milestone involved implementing the core on-chain code for the trustless P2P on-ramp smart contract in Haskell, utilizing the zkFold Symbolic library. This work encompasses the creation of modules responsible for managing the trustless, zero-knowledge P2P escrow transactions, thus fulfilling the project’s key requirement of on-chain zero-knowledge proof verification. The implementation has followed stringent quality standards to ensure security, performance, and usability.

Challenges and Resource Requirements:

This project is complex and demands a significant collaborative effort from both the development and research teams. Zero-knowledge technology integration with Cardano's smart contract architecture is a pioneering task, requiring a well-coordinated approach to problem-solving. High-quality communication between all stakeholders has been and will remain a top priority to address these challenges effectively and maintain alignment on project goals. Additionally, the public availability of our code underscores our commitment to code quality and transparency, as it will be open to scrutiny and contributions from the broader community.

Next Steps:

Following the completion of these milestones, our next focus is to continue with subsequent milestones, emphasizing rigorous testing, community engagement, and completion of any remaining components to ensure timely delivery of the project.