

# zkUSD Feasibility Study

Mina Navigator Grant  
Nov 24

## 01 INTRODUCTION

- Overview
- Purpose of study
- Objective & Scope
- Key Requirements

## 02 ARCHITECTURE

- Analysis
- Solution

## 03 zkUSD Components

- Vaults
- Token
- Price Feed
- Protocol Vault

## 04 ECONOMICS & GOVERNANCE

- Protocol Economics
- Governance

## 05 NEXT STEPS

## Overview

The feasibility study addressed whether an exogenous algorithmic stablecoin and its essential components could be effectively implemented within Mina's unique blockchain architecture. Mina's lightweight, zero-knowledge-based design presented both opportunities and challenges, requiring innovative solutions. By overcoming these challenges and delivering a system that incorporates critical features necessary for a production-ready application, the study set the stage for advancing zkUSD into a robust and impactful tool for the Mina ecosystem.

# INTRODUCTION

## Objective & Scope

### Primary Goal

Develop a local Minimum Viable Product (MVP) for zkUSD that demonstrates core functionality with full test coverage

### Architecture Analysis

Conduct a comprehensive analysis of the systems architectural landscape to identify optimal system design for interoperability with Mina L1

### Validate Assumptions

- Computational Feasibility
- Concurrent use
- Protocol economics
- Decentralised price feed

### Planning Next Phase

Lay the groundwork for continued development of zkUSD to begin to move towards production.

# INTRODUCTION

## Key Requirements

### Collateralized Debt Positions (CDPs)

Users can create debt positions by depositing collateral, enabling them to mint zkUSD against these positions.

### Liquidation Mechanism

Positions that fall below collateralization requirements can be liquidated by any user, who can burn zkUSD to claim locked collateral.

### Peg Stability

To maintain its peg to the US Dollar, zkUSD requires a minimum collateralization ratio of 150% for all debt positions.

### Health Factor

A calculated health factor assesses each position's stability; a high factor indicates safety, while a low factor signals potential liquidation risk. Baselined at 100.

### Position Ownership

Only position owners can mint zkUSD, burn zkUSD, or adjust collateral, ensuring secure management of their assets.

### Accurate Price Feeds

The health factor relies on accurate external price feeds, which are essential for reliable collateral valuation and system integrity.

## Analysis

---

### Vanilla zkApp

- Concurrency issues with precondition violation mean this can't work

---

### Protokit (L2 App-chain)

- Solves concurrency problems
- Enables management through single orchestrator contract
- Hinders L1 interoperability

---

### L2 Chain (Zeko)

- Isolated from L1, meaning that zkUSD would only be able to be used within Zeko

---

### Action/Reducer (Batch)

- Account updates and state transitions need to occur atomically, which means we can't separate them to make use of this model
- As a single interaction can incur up to eight account updates, this is unfeasible.

---

### Offchain State

- Same issue with the Action/Reducer and the need to handle account updates and state transitions atomically
-

# ARCHITECTURE

## Solution - Individual zkUSD Vaults

### Independent zkApps

Each user deploys their own vault to manage their CDP. These vaults hold their own state, interacting with centralised token, oracle and protocol vault contracts.

### Access Control

Actions on each vault—such as depositing and redeeming collateral, as well as minting and burning zkUSD—are secured by the vault owner's unique secret, ensuring exclusive access. In contrast, liquidation is an open process that can be initiated by any participant if a vault becomes undercollateralized. This mechanism safeguards protocol stability by incentivizing timely corrective actions.

### Concurrency Management

As each vault is its own zkApp, updates happen within vaults, not interfering with other positions and preconditions, solving concurrency issues. Each transaction can effectively manage account updates and state transitions, solving atomicity issues.

### Vault Monitoring

Vault monitoring is facilitated through events, enabling anyone to track the financial health of individual vaults. This ensures timely liquidations and helps maintain overall protocol stability.

# ZKUSD COMPONENTS

## zkUSD Vaults

### User-Deployed Vaults

Each user deploys their own zkUSD Vault to handle their collateralized debt positions, ensuring independent operation and user-specific control.

### Ownership Security

Vaults utilize a user-provided secret stored as an ownership hash, requiring this secret for all critical actions to ensure only the owner can manage the vault.

### Liquidation

If a vault's health factor drops below the threshold, liquidation can be initiated by anyone, allowing liquidators to burn zkUSD debt and claim locked collateral.

### Price Feed

Vaults depend on a decentralized price feed for accurate collateral valuation, ensuring the health factor reflects real-time market conditions.



# ZKUSD COMPONENTS

## zkUSD Token

### 01 Balancing Interoperability and User Experience

The Mina Fungible Token (MFT) standard offers interoperability but at a high cost in account updates. For zkUSD, the required updates exceeded practical limits.

### 02 Prioritizing User Experience

User experience was prioritized over strict MFT compliance, ensuring efficient operations for users despite a minor reduction in interoperability.

### 03 Customized Token Design

The token contract was tailored to internalize key administrative functions, allowing zkUSD tokens to be minted only through valid vault interactions, reducing account updates.

# ZKUSD COMPONENTS

10

## Price Feed

### Decentralized and Robust Price Feed

The zkUSD protocol adopts a decentralized, incentive-driven approach for a secure and reliable price feed mechanism.

### Trusted Oracle Whitelist

The protocol maintains a curated whitelist of trusted oracles. Oracles are incentive to submit prices on-chain by earning a oracle fee

### Median Price Calculation

Submitted prices are dispatched as actions and reduced to calculate the median price from all submissions. This ensures accuracy, presents outliers and maintains robust price integrity

### Dual-State Mechanism

The oracle maintains two price states, `evenPriceState` and `oddPriceState`. Vaults read from the opposite price that is updated ensuring preconditions remain valid during updates

# ZKUSD COMPONENTS

## Protocol Vault

### Overview

The Protocol Vault is a core component of zkUSD, responsible for managing funds and administrative tasks to ensure smooth and secure protocol operation

### Funds Management

The Protocol Vault collects fees generated from staking rewards on delegated collateral held in user vaults. It manages these funds to support the protocol's ongoing operations.

### Oracle Funding

It funds the Oracle Contract by paying the oracle fee for submitting price updates, ensuring a robust and accurate price feed mechanism.

### Administrative Tasks

The vault manages administrative tasks such as access control, setting the protocol fees, and managing the oracle whitelist

# ECONOMICS & GOVERNANCE

12

## Protocol economics

### 01 Delegated Staking Rewards

The zkUSD protocol utilizes Mina's delegated staking to build a self-sustaining economic model, enhancing rewards for both users and the platform.

### 02 Protocol Fee Structure

A percentage fee from staking rewards is applied, allowing users to earn while contributing to protocol sustainability.

### 03 Funding Allocation

Protocol fees fund decentralized oracle price feeds, development initiatives, and maintain solvency for platform stability.

### 04 User Benefits

This model allows for negative interest loans, where staking rewards effectively pay off user debt.

# ECONOMICS & GOVERNANCE

13

## Progressive Decentralisation

### Current Governance Model

The Protocol Vault is currently governed by a single Administrator Key, allowing for rapid development and oversight during the early stages of the protocol.

### Future Plans for Governance

Thorough research will be conducted on governance models suitable for Mina's architecture, including multi-signature setups and community-driven structures such as DAOs.

### End Goal

The ultimate objective is to achieve maximum decentralization, ensuring security, transparency, and resilience aligned with Mina's ethos.

# NEXT STEPS

14

01

## Integration Testing

Conduct a comprehensive suite of integration tests on Lightnet and Devnet to ensure seamless interactions between vaults, oracles, and the zkUSD token.

02

## Smart Contract Audit

Engage a reputable security auditing firm to perform an in-depth audit of all smart contracts, addressing potential vulnerabilities before mainnet deployment.

03

## Protocol Governance Development

Research governance models suited for Mina's architecture and define a roadmap for progressive decentralization towards multi-signature setups or a DAO.

04

## Oracle Software Development

Build software for the price feed mechanism, enabling selected oracle providers to submit reliable, incentivized price updates.

05

## User Interface (UI)

Develop an intuitive UI for end-users to interact with zkUSD, focusing on user experience to drive adoption and engagement.

06

## Exchange Partnerships

Initiate discussions with exchanges to list zkUSD post-launch and explore partnerships to increase adoption and liquidity.