# Treasury Withdrawal - zkFold ZK Rollup

## **Title**

Withdraw ₳1,161,000 for zkFold ZK Rollup administered by Intersect

## **Abstract**

This treasury withdrawal funds zkFold ZK Rollup which will provide the following services:

ZK rollups address the scalability problem. Hundreds of transactions can be submitted as a single batch, reducing the load on the L1. Cardano can achieve higher throughput and lower transaction costs.

zkFold offers to build a general-purpose zero knowledge rollup solution for Cardano. A zero knowledge rollup is a technological layer (Layer 2) on top of a blockchain that increases the blockchain’s scalability potential by compressing many transactions into transaction batches. As batches offer a greater degree of information compression, it is reasonable to expect that hundreds of rollup smart contract transactions might fit into a single Cardano mainnet transaction. Zero knowledge proofs technology places a limit on the cost of on-chain verification of the validity of transaction batches. Specifically, the batch verification fits well within the Execution Unit limits set at the protocol level, as demonstrated by the prototype created by the zkFold team.

This Treasury Withdrawal is submitted by Intersect on behalf of the vendor. The following sections; Abstract, Motivation, Rationale and Vendor Profile have been sourced from the approved proposal submitted by the Vendor as part of the Intersect budget process.

This treasury withdrawal funds one of 39 proposals to give effect to the approved budget info action for ₳275,269,340, administered by Intersect via gov\_action1u9x73kwufaxa70lfy59g4ynwyrcsaxdcd0gxzzmh67s9fxq4j8hqqk2phgh. The information provided herein is intended to fulfill the spirit of the constitutional requirement for a treasury withdrawal info action by also providing the details of the proposed solution, alignment to the budget, and amount to be withdrawn from the Cardano Treasury.

## **Motivation**

This proposal aims to solve the following problem:

Scalability is a challenge for Cardano. As it grows, more dApps and users join, the demand for processing capacity increases, leading to congestion, slower transaction times, and higher fees.

## **Rationale**

### Project Solution

zkFold will develop and implement ZK rollups on Cardano to scale it efficiently, promoting broader adoption and supporting an ecosystem of decentralized applications and services.

Overall, the proposal will have the following positive impact on the Cardano ecosystem:

* Improved Scalability: ZK rollups enable Cardano to process significantly more transactions per second (TPS) by bundling and verifying transactions off-chain. This reduces congestion, benefiting users by ensuring faster and more efficient dApp interactions.
* Lower Transaction Costs: By reducing the number of transactions directly processed on-chain, ZK rollups lower the transaction fees, making Cardano more accessible and affordable, especially for smaller transactions or micro-payments.
* Enhanced User Experience: Lower fees create a smoother experience for users interacting with dApps, decentralized finance (DeFi) platforms, and NFT marketplaces.
* Increased Adoption: ZK rollups can make the Cardano ecosystem more attractive for developers and users, promoting the growth of dApps, DeFi, and other blockchain applications by offering higher performance and scalability.
* Maintained Security: ZK rollups allow for scalability improvements without compromising the security and decentralization of the Cardano base layer, as Cardano still plays the role of the settlement layer for the rollup transactions.

### Vendor Profile

zkFold team has successfully moving towards the TestNet of our ZK Rollup. The zkFold team consists of expert Haskell, Rust, and ZKP developers and Cryptographers.

### Contract Management

A written off-chain Legal Contract will be created between the Vendor and the Cardano Development Holdings (CDH), as mandated by the constitution, and will be administered by Intersect. This will include details of the project delivery schedule and dispute resolution.

### Project Delivery

All milestones, acceptance criteria, payment amounts and expected delivery dates will be agreed between the Vendor and Intersect, acting on behalf of the CDH. The vendor will deliver according to the agreed-upon project schedule within the Legal Contract, of which the necessary information will be made public via the budget management platform via transaction metadata.

Defined by the milestones within a Legal Contract, the vendor will submit and attest milestone acceptance to the community, Intersect or 3rd Party Assurer.

Project progress will be monitored via Intersect’s delivery assurance function which will be communicated to the community.

Acceptance of the above work is expected to be supported by a 3rd Party Assurer, who will be responsible for reviewing and signing off the work completed at each project milestone against the corresponding milestone deliverables detailed within the Legal Contract. This work is funded from a portion of this treasury withdrawal.

### Budget Management Tooling

To administrate treasury funds on-chain, Intersect will utilize the treasury management smart contract framework developed by Sundae Labs. The smart contracts have been [extensively tested](https://github.com/SundaeSwap-finance/treasury-contracts/tree/main/offchain/tests) including audits from TxPipe and MLabs. Examples of the usage of these contracts can be seen across mainnet described across Intersect authored [Blog 1](https://www.intersectmbo.org/news/smart-contract-mainnet-demo-a-step-toward-on-chain-treasury-withdrawals), [Blog 2](https://www.intersectmbo.org/news/smart-contract-mainnet-demo-day-two-update) and [Blog 3](https://www.intersectmbo.org/news/smart-contract-mainnet-demo-day-three-update).

Final mainnet validation test can be seen via the Disburse action within transaction: 0f591dc544ae14102dbb4a74d5311a6acffc1772b163d8b7a9656b9525950b17

With the confirmed treasury reserve contract address being: stake17xzc8pt7fgf0lc0x7eq6z7z6puhsxmzktna7dluahrj6g6ghh5qjr

#### Specifics

Intersect will utilize a single Treasury Reserve Smart Contract (TRSC), with many Project-Specific Smart Contracts (PSSC), managed by Intersect. Intersect’s management consists of three ‘admin’ and two Intersect ‘leadership’ roles. An Oversight Committee consisting of five external, independent third-party entities will provide checks and balances on Intersect, and safeguard against errors and unilateral control. The administration of both TRSC and PSSCs will be managed by Intersect, with external oversight on certain actions from the Oversight Committee.

The Oversight Committee consists of Sundae Labs, Cardano Foundation, Dquadrant, Xerberus and NMKR. Their role is to independently verify key administrative actions using on-chain logic, ensuring accuracy and consistency without exercising discretion over governance decisions.

For all details on Intersect’s configuration please see the [**Smart Contract Guide**](https://docs.intersectmbo.org/cardano-facilitation-services/cardano-budget/intersect-administration-services/smart-contracts-as-part-of-our-administration) on the knowledgebase.

The high level permissions are as follows:

* TRSC Fund and PSSC Modify
  + Two of the three Intersect admins, two of the five trusted entities and one of the two Intersect leadership sign-off must authorize
* TRSC Disperse
  + Two of three Intersect admins, three of five trusted entities and two of two Intersect leadership sign-off must authorize
* TRSC Pause and Resume
  + Two of three Intersect admins, and one of two Intersect leadership sign-off must authorize
* TRSC Sweep
  + One of three Intersect admins, and one of two Intersect leadership sign-off must authorize
* TRSC Reorganize
  + Two of three Intersect admins and three of five trusted entities must authorize

#### Processes

Upon enactment of this governance action, funding for this project will be directed into the TRSC’s stake account. All instances of TRSC and PSSC can not be staked with a SPO and will be delegated to the auto-abstain predefined DRep. From here funds will be withdrawn into a UTxO remaining at the TRSC.

When the Legal contract is prepared and the vendor is ready, funding for this project will be transferred using the Fund action to a PSSC. All milestones will be outlined within the metadata.

A dashboard will be available for the community to audit the TRSC or PSSC and track metrics related to this withdrawn ada as well as being immutably verifiable on chain.

The subsections; Contract Management, Project Delivery, and Budget Management Tooling described above cover the constitutional requirements specified in Article IV section 4 and 5.

## **References**

Project Proposal In Ekklesia

* <https://2025budget.intersectmbo.org/ballots/680d1b63565577986442d123/proposals/680d1b63565577986442d1c4>

Approved Budget Info Action submitted by Intersect via GovTool

* https://gov.tools/outcomes/governance\_actions/e14de8d9dc4f4ddf3fe9250a8a926e20f10e99b86bd0610b77d7a054981591ee#0

Details of all successful proposals (CSV)

* ipfs://bafybeicwrop4q7xvnyjdd5drumbe56sqtm5lbe2ul3c262zt4hgguzdycm

Automating Accountability: Cardano’s Smart Contract Framework Blog

* ipfs://bafybeihqx4ae72z7suqfnxrpqpqithp43cai7o2uuewnqtezgaoyc3ptyq

Sundae Labs Budget Management Smart Contracts Github Repository

* https://github.com/SundaeSwap-finance/treasury-contracts

Budget Management Smart Contracts TxPipe Audit Report

* ipfs://bafybeiccnwejbgj43wo6hrlseckkkmprtoqc5cfuy2hesm6c6yealwho3e

Budget Management Smart Contracts MLabs Audit Report

* ipfs://bafybeiah5fnjhda5hemj3qvaehc4mre3qllqzw2l7mkdsguytn4ftgafw4

## **Authors**

* Intersect