# Treasury Withdrawal - ZK Bridge

## **Title**

Withdraw ₳700,000for ZK Bridge administered by Intersect

## **Abstract**

This treasury withdrawal funds **ZK Bridge** which will provide the following services:

Our proposal is building a ZK bridge for Cardano, which we will deploy on the Cardano testnet.

As part of this initiative, we will define a communication protocol for the bridge, provide the full source code of the smart contracts on the Cardano side, and produce comprehensive technical documentation detailing the protocol between Cardano and any other isomorphic blockchain.

We will provide a circuit that enables a relayer to generate the ZK proof that a locking transaction was successfully added to the chain, which can then be verified on the receiving blockchain. This way, any blockchain will be able to implement a ZK bridge with Cardano, leveraging its newly added capability to generate such proofs. This allows for a variety of uses, such as moving assets outside Cardano just by providing the proof that they’ve locked an equivalent amount in the Cardano Smart Contract. The resulting bridge can serve as a generic framework for interoperability between Cardano and any other blockchain willing to implement the corresponding counterpart contracts.

Furthermore, we will implement contracts in Aiken to mint assets on a Cardano-like (isomorphic) blockchain and deploy them on the Cardano testnet, providing a fully functional proof of concept. These building blocks will enable developers to create bridges between Cardano and other chains with minimal additional effort.

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info action by also providing the details of the proposed solution, alignment to the budget, and amount to be withdrawn from the Cardano Treasury.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:

Cross-chain interoperability remains one of the most critical yet unresolved challenges for Cardano. While the ecosystem is advancing in scalability through projects like Hydra and optimistic roll ups such as Midgard it still lacks a secure, trustless, and modular zk-based bridge infrastructure.

Current bridges rely on centralized validators or multi-signature schemes, introducing major security risks—as demonstrated by numerous high-profile exploits in other ecosystems. Without a native zero-knowledge bridge, Cardano is unable to safely connect with external chains, severely limiting access to external liquidity, composability with other ecosystems, and the ability to scale horizontally.

Furthermore, the Cardano ecosystem lacks a unified open-source toolkit for:

On-chain verification of zero-knowledge proofs

Secure and efficient cross-chain messaging

Asset wrapping and unwrapping under Cardano’s native token model

And trust-minimized interoperability with existing ZK-rollups.

This absence puts Cardano at a competitive disadvantage compared to platforms like Ethereum, which already benefit from multiple zk-based Layer 2 solutions and zk-enabled bridges.

A modular zkBridge is not only critical to unlock interoperability—it also lays the groundwork for a future Cardano-native zkRollup framework, by enabling the testing and deployment of foundational components such as provers, verifiers, and state synchronization mechanisms.

## **Rationale**

### Project Solution

Building a zero-knowledge bridge provides several key benefits to the Cardano ecosystem. A bridge between Cardano and other blockchains would make it much easier for value to flow in from external ecosystems, increasing the liquidity available within Cardano.

A zero-knowledge bridge, specifically, offers important advantages over alternative architectures such as optimistic bridges. In a ZK bridge, a single user action accompanied by a succinct proof of deposit is sufficient to release tokens on the destination blockchain. This eliminates the need for community-wide monitoring or challenge periods, significantly reducing latency and trust assumptions.

Additionally, by building a ZK bridge, Cardano positions itself as a more interoperable platform, capable of engaging with the broader ecosystem of zero-knowledge technologies. This lays the groundwork for future innovations in identity, privacy-preserving applications, and cross-chain collaboration.

### Vendor Profile

Eryx is a worker-owned labor cooperative with almost 15 years of experience solving complex problems involving mathematics and software. We are a group of nerdy PhDs with a solid background in math and computer science. Our team has extensive experience in blockchain development, cryptography, and privacy-focused protocols, which gives us the expertise required to successfully deliver the project.

Among other things, we’ve been core contributors to the Lambdaworks library and implemented the CircleSTARKS protocol in GPU alongside with Nethermind. This involved implementing several ZK cryptographic primitives (field operations, polynomial commitment schemes, FRI protocols, FFTs), in different platforms and languages. Furthermore, we implemented a proving system based on the Plonk protocol. During this project we wrote a simple interface to design circuits. It included basic operations and conditionals that made the building blocks for more complex cryptographic primitives. We also developed a Plonky2 backend for Aztec's Noir, funded by the Ethereum Foundation.

In relation to this proposal, we have extensive experience in Aiken smart contract development, including previously funded proposals under Project Catalyst focused on educational and technical infrastructure for Cardano. We also wrote zk circuits for cryptographic primitives such as hash functions and elliptic curve operations.

We are active contributors to the ENCOINS protocol, currently deployed on the Cardano mainnet with privacy-preserving features. Currently, we are researching the integration of ZK systems with the EUTxO model.

### 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**

ZkBridge Cardano Proposal (PDF)

* ipfs://bafybeic6onenqv7xguen3klpqlwly5dvxlfanaws4z4knfwg7w5vksp72q

Eryx Coop ACVM Backend Plonky2 GitHub Repository

* <https://github.com/eryxcoop/acvm-backend-plonky2>

Eryx Coop one-pager (PDF)

* ipfs://bafybeidoz5frkc4fd2lrn7gmoxvgl3ltognd7lm6kltnnj62qdw57r7u4i

ZKCity Educational Bootcamp where we were main lecturers

* <https://www.zkcity.xyz>

Eryx Coop ZK Adventures GitHub Repository

* <https://github.com/eryxcoop/zk-adventures>

Contributions to open source Zk projects 1

* <https://github.com/starkware-libs/stwo/commits/dev/?author=carlogf>

Contributions to open source Zk projects 2

* <https://github.com/starkware-libs/stwo/commits/dev/?author=jarnesino>

Contributions to open source Zk projects 3

* <https://github.com/starkware-libs/stwo-cairo/commits/main/?author=ajgara>

Contributions to open source Zk projects 4

* <https://github.com/starkware-libs/stwo-cairo/commits/main/?author=atgrosso>

Contributions to open source Zk projects 5

* <https://github.com/starkware-libs/stwo-cairo/commits/main/?author=schouhy>

Contributions to open source Zk projects 6

* <https://github.com/0xPolygonZero/plonky2/pull/1645>

Circle STARK GPU Acceleration Talk by our partner Julian

* <https://www.youtube.com/watch?v=7EOjrYnrE8g>

Project Proposal In Ekklesia

* <https://2025budget.intersectmbo.org/ballots/680d1b63565577986442d123/proposals/680d1b63565577986442d172>

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