# Treasury Withdrawal - Intersect metadata - MLabs Research towards Tooling for Elliptical Curves - GrumpleStiltSkin

## **Title**

Withdraw ₳104,347 for MLabs Research towards Tooling for Elliptical Curves…

## **Abstract**

This treasury withdrawal funds MLabs **Research towards Tooling for Elliptical Curves - GrumpleStiltSkin** which will provide the following services:

GrumpleStiltSkin will deliver an open-source, parameterized elliptic curve and Galois field framework implemented in Plutarch. The goal is to allow smart contracts on Cardano to verify cryptographic proofs over customizable curves and fields. This will include:

* Plutarch support for Galois field arithmetic
* Plutarch support for elliptic curve arithmetic
* A generic ZK verifier in Plutarch
* A validation test suite over BLS12-381
* A composable YTxP-compatible Plutarch wrapper

This tool empowers developers with on-chain cryptographic flexibility, expands Cardano’s ZK application capabilities, and sets the stage for future innovations in privacy and authentication.

Deliver a parameterized elliptic curve and finite field cryptography framework in Plutarch, enabling developers to build smart contracts that verify zero-knowledge proofs over arbitrary curves. This flexibility empowers privacy-focused dApps, improves composability, and advances Cardano's technical capabilities. It creates a foundation for a wide range of ZK-powered features while reducing duplication of effort across the ecosystem.

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info action by also providing the details of the proposed solution, alignment to the budget, and amount to be withdrawn from the Cardano Treasury.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

Cardano currently lacks reusable and composable on-chain cryptographic tooling for elliptic curves and finite fields. Developers building ZK or privacy-preserving applications must either hardcode specific cryptographic primitives (limiting generality) or implement complex curve logic themselves (introducing security risks and inefficiencies). There is no widely accepted, verifiable standard for parameterized zero-knowledge verification on Cardano***.***

## **Rationale**

### Project Solution

MLabs will create a two-part proof-of-concept system, named Grumpelstilskin, designed to allow application developers to easily use any curve of their choice for zero-knowledge proof verification on-chain. The first part of Grumpelstilskin will be a 'working script' which, when given appropriate parameters via its datum, will verify a zero-knowledge proof over a user-specified curve. This script will be tested for correctness.

The second part of Grumpelstiltskin will be a YTxP-based interface to the 'working script', implemented in Plutarch. This interface will be well-documented, easy to use, and flexible, with a focus of making life easy for application developers who want to use zero-knowledge proofs. Thanks to their use of YTxP, future performance, security and functionality improvements will not be the responsibility of application developers who use Grumpelstilskin. This second part will be distributed as an open-source project.

MLabs aims to build a minimum viable product, with the future goals of expanded functionality, improved performance, as well as a full audit of the 'working script'. The choice of YTxP will make it minimally difficult to achieve this,and will impose minimal friction on any application developers using Grumpelstiltskin to build their products.

### Vendor Profile

MLabs has extensive experience in cryptography, Plutarch smart contracts, and zero-knowledge systems. Our past work includes Plutarch, the Cardano Transaction Library, and zkApp R&D. We are contributors to multiple community standards and tooling projects (e.g., CTL, Ply, Cardano.nix).

Also we have done work towards bitwise operators previously in CIP-123 which is related to this work and can possibly be used towards its implementation.

### 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**

mLabs Elliptical Curves Proposal

* <https://docs.google.com/document/d/1G7EbN9atd7MwvaesSEc7E7iXne_e49lTK90IRrgSSxw/edit?usp=sharing>

mLabs-haskell Grumplestiltskin Github Repository

* <https://github.com/mlabs-haskell/grumplestiltskin>

Project Proposal In Ekklesia

* <https://2025budget.intersectmbo.org/ballots/680d1b63565577986442d123/proposals/680d1b63565577986442d1a6>

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://

Budget Management Smart Contracts MLabs Audit Report

* ipfs://

## Authors

* Intersect