# Treasury Withdrawal - 2025 Input Output Engineering Core Development Proposal

## **Title**

Withdraw ₳96,817,080 for 2025 Input Output Engineering Core Development Proposal

## **Abstract**

This treasury withdrawal funds **2025 Input Output Engineering Core Development Proposal** which will provide the following services:

* Automatic Formal Verification (Plutus High Assurance)
* Property Based Testing Tool (Plutus High Assurance)
* Static Analyzer (Plutus High Assurance)
* Ouroboros Leios Implementation
* Cardano Node Architecture Refresh (Acropolis)
* Hydra Development
* Minotaur AVS
* Mithril Development
* KES Agent
* Ledger-HD
* Log-Structured Merge (LSM) including UTXO-HD
* Revised Stake Pool Incentive Scheme
* Nested Transactions (Babel Fees)
* Plutus Core Roadmap
* Tiered Pricing Models (Plutus High Assurance)
* Transaction Monitoring System (Plutus High Assurance)
* Maintenance and Support
* Audit & Security Assurance

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info action by also providing the details of the proposed solution, alignment to the budget, and amount to be withdrawn from the Cardano Treasury.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

Automatic Formal Verification (Plutus High Assurance):\*\* Develop automated formal verification tool for Plinth/Cardano DApps

\*\*Property Based Testing Tool (Plutus High Assurance):\*\* Develop Plinth PBT Tool to automatically generate diverse inputs/actions

\*\*Static Analyzer (Plutus High Assurance):\*\* Develop "one-click" static analysis tool for Plinth contracts

\*\*Ouroboros Leios Implementation:\*\* Begin core implementation of Leios L1 consensus protocol

\*\*Cardano Node Architecture Refresh (Acropolis):\*\* Re-architect the Cardano node into a modular model (Acropolis)

\*\*Hydra Development:\*\* Complete Hydra v1.0 mainnet and full audit, Cardano's L2 state channel solution

\*\*Minotaur AVS:\*\* Launch Minotaur, Actively Validated Service (AVS) leverage Cardano L1 security

\*\*Mithril Development:\*\* Enhance Mithril protocol for secure, efficient access. Speeds up sync, enables light clients

\*\*KES Agent:\*\* Implement security enhancement for SPO KES key storage and management

\*\*Ledger-HD:\*\* Move ledger state tables from memory to disk (LSM tech) to reduce RAM

\*\*Log-Structured Merge (LSM) including UTXO-HD:\*\* Integrate bespoke Well-Typed LSM-tree backend for managing on-disk state

\*\*Revised Stake Pool Incentive Scheme:\*\* Investigate potential adjustments to SPO incentive scheme

\*\*Nested Transactions (Babel Fees):\*\* Implement Nested Transactions ledger feature enabling tx batching. Facilitates Babel Fees

\*\*Plutus Core Roadmap:\*\* Execute roadmap for Plutus Core delivering key new primitives

\*\*Tiered Pricing Models (Plutus High Assurance):\*\* Introduce transaction prioritization mechanism to improve predictability during congestion

\*\*Transaction Monitoring System (Plutus High Assurance):\*\* Develop system to monitor transactions, detect potential fraud/anomalies

\*\*Maintenance and Support:\*\* Maintenance of existing code base, ongoing support. Includes cost of running Test & Tracing setup

\*\*Audit & Security Assurance:\*\* Engage independent audits and security assurance. Consolidated item

This proposal addresses several critical challenges and opportunities within the Cardano ecosystem necessary for its continued growth, competitiveness, and decentralization. Key problems include:

\* \*\*Scalability Limitations:\*\* The current L1 infrastructure faces throughput constraints during high demand, hindering user experience and application potential. There's a need for significant scaling solutions at both Layer 1 (consensus) and Layer 2.

\* \*\*Node Architecture & Performance:\*\* The existing node design presents limitations in terms of modularity, extensibility, performance (especially RAM usage), and ease of contribution from diverse development teams.

\* \*\*Smart Contract Assurance & Developer Experience:\*\* Developers require enhanced tools for ensuring the security, correctness, and efficiency of smart contracts to build trust and reduce risks. Improving the Plinth/Aiken/Plutarch ecosystem and providing robust testing/verification tools is essential.

\* \*\*SPO Viability & Security:\*\* Ensuring the operational security of Stake Pool Operators (SPOs) and investigating the fairness and sustainability of the incentive mechanism is vital for network health and decentralization.

\* \*\*User Experience & Adoption Barriers:\*\* Friction points like mandatory ADA fee payments and unpredictable transaction inclusion during congestion need addressing to improve usability and attract broader adoption.

\* \*\*Ecosystem Competitiveness:\*\* Cardano needs to integrate emerging blockchain paradigms like Actively Validated Services (AVS) to remain competitive and offer diverse functionalities.

\* \*\*Core Maintenance & Knowledge Transfer:\*\* The foundational codebase requires ongoing maintenance, modernization, technical debt reduction, and structured knowledge sharing to ensure stability and enable broader community participation in core development.

## **Rationale**

### Project Solution

In this proposal, IOE and its collaborators outline key core Cardano platform developments aimed at substantially improving network scalability, security, performance, and usability, while enhancing developer support.

Implementation of these initiatives offers substantial benefits across the Cardano community, which collectively, enhance Cardano's technical foundations, enabling it to support a larger, more complex, and more active ecosystem:

\* \*\*For the Ecosystem:\*\* Delivers massive L1 throughput increase (Leios), robust L2 scaling (Hydra, Mithril), and positions Cardano competitively in new areas like AVS (Minotaur). Enhances overall network security, resilience, and decentralization. Fosters supplier diversity through knowledge sharing and modular architecture (Acropolis). The ROI stems from increased network capacity, utility, and attractiveness, driving adoption and value.

\* \*\*For End Users:\*\* Experience significantly reduced network congestion and faster transaction processing (Leios), near-instant finality for specific applications (Hydra), the convenience of paying fees with native tokens (Nested Transactions/Babel Fees), and potentially more predictable transaction inclusion (Tiered Pricing). Enhanced security measures build user trust.

\* \*\*For Developers & dApp Builders:\*\* Gain access to advanced tools for building more secure and efficient smart contracts (Plutus High Assurance suite, Plutus Core enhancements). Benefit from a more extensible and accessible node architecture (Acropolis), easier integration with L2s and light clients (Hydra, Mithril), and improved transaction capabilities (Nested Transactions). This lowers development barriers and enables more sophisticated applications.

\* \*\*For Stake Pool Operators (SPOs):\*\* Benefit from significantly reduced node operational costs (lower RAM requirements via Ledger-HD, LSM/UTXO-HD), enhanced operational security (KES Agent), improved network performance, potential new revenue streams (Minotaur AVS), and a potentially fairer incentive structure (Revised Scheme investigation). Mithril improvements speed up node synchronization.

### Vendor Profile

Input Output (IO) realized Cardano's vision for a secure, scalable, decentralized platform through a research-driven, phased delivery (Byron to Voltaire). Leveraging formal methods, functional programming, and rigorous engineering, IO produced key achievements including Proof-of-Stake, Ouroboros consensus, Plutus smart contracts, native tokens, and scaling solutions like Hydra and Mithril.

IOE and its partners' involvement spans the entire existence of Cardano, and is demonstrated daily by its active development, support, and maintenance. Key personnel essential to this long-standing contribution are retained to continue this effort through 2025 and into 2026.

IO remains committed to furthering Cardano’s technical development, research and community engagement.

### 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 described **{to-do once done}.**

#### 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 knowledge base.

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. The 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.

## **References**

Input Output Engineering 2025 Core Development Proposal v1.1 (PDF)

* ipfs://bafybeicabpq4cu6eev53m3ywiczbidyn2ivos4tglq7vy3gkbklp3dk5zi

Project Proposal In Ekklesia

* <https://2025budget.intersectmbo.org/ballots/680d1b63565577986442d123/proposals/680d1b63565577986442d23a>

Approved Budget Info Action submitted by Intersect

* <https://gov.tools/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