



# IO Q4 2025-Q1 2026 delivery report

This report provides the Cardano community with a clear view of what Input Output (IO) delivered in Q4 2025 - Q1 2026, why each outcome matters for Cardano, and how it connects to IO's treasury-funded commitments.

April 2026

Prepared by IO

## The bottom line

---

In Q4 2025 and Q1 2026, IO delivered measurable progress across 18 treasury-funded commitments. Sixteen were progressed successfully. Two – Acropolis and tiered pricing – were [canceled, and their funding returned](#). Every outcome in this report is publicly verifiable.

The following outcomes define IO's deliverables:

**1. Institutional adoption accelerated.** LayerZero integration went live, and USDCx launched on Cardano within 84 days – [reaching real users in its first week](#).

**2. Three scaling solutions advanced to working code.** Mithril reached its first stable release, Hydra progressed toward production use cases, and Leios prototype development continued on track.

**3. Builders got new tools.** Improvements to Plutus performance, Cardano High Assurance tooling, and static analysis capabilities made it easier and safer to build on Cardano.

**4. The network shipped two major node releases and helped [resolve a mainnet incident](#).**

**5. The nested transactions** framework has made significant progress, with CIP-118 merged and changes to the ledger rules defined. Preparations for the v11 hard fork are underway.

**6. Research remained publicly accountable.** Work is peer-reviewed, openly published, and entering its next phase under the new treasury funding model.

The sections below expand on each of these outcomes with supporting evidence.

## 1. Adoption is showing up, and the ecosystem is gaining momentum

---

IO's infrastructure work creates the conditions for adoption. In Q4 2025 and Q1 2026, that adoption became increasingly visible – from institutional partnerships to wallet capabilities to real-world payment use cases.

### Lace Wallet

Lace has become the first wallet to integrate Midnight, bringing privacy-enabled assets alongside existing Cardano holdings in a single interface. The team actively supported the Midnight mainnet launch on March 30th, 2026. Development on Lace's mobile application and LaceID (a native identity feature for managing verifiable credentials) also continues.

## USDCx launched on Cardano

USDCx [launched on Cardano](#) in Q1 2026, delivered through the Pentad and the community-funded Critical Integrations program. In the first week, more than 15 million USDCx was minted, decentralized finance total value locked grew from \$127M to \$142M, and major protocols, including Minswap, Liqwid, and SundaeSwap, had live liquidity pools. The infrastructure ran without errors. It is a concrete example of what community-funded delivery produces.

## LayerZero integration announced

LayerZero is an omnichain messaging protocol connecting over 160 blockchains. Its integration with Cardano and Midnight represents the single largest interoperability unlock in the ecosystem's history, providing direct access to over \$80 billion in omnichain assets. For Midnight specifically, the integration acts as a technical force multiplier, allowing selective disclosure and zero-knowledge proofs to extend across blockchain networks. Announced at [Consensus Hong Kong 2026](#), it marks a concrete step toward connecting Cardano's infrastructure with the broader multi-chain economy.

## Ecosystem milestones

IO's engineering work in Q4 2025 and Q1 2026 took place alongside a series of milestones that reflect Cardano's growing maturity and institutional credibility:

- CME Group launched Cardano futures in February
- Midnight Network mainnet launched at the end of March 2026, with MoneyGram and Blockdaemon as federated node operators
- The Cardano constitution was ratified by a super-majority of the constitutional committee and DReps at the start of 2026
- The Cardano Pentad established – Input Output, EMURGO, Cardano Foundation, Intersect, and the Midnight Foundation – as a coordinated, treasury-supported coalition for network-wide infrastructure
- Intersect committee elections for 2026 announced, with candidate applications opening March 30
- Ada accepted as payment in 137 SPAR stores across Switzerland
- Coinbase expanded on-chain loans to include ada as collateral
- Cardano will be a block sponsor at Consensus 2026 in Miami (May 5–7).

## 2. World-class research, openly accountable

---

IO's research arm, Input Output Research (IOR), is the scientific foundation behind Cardano's protocol design. IO's world-class research department closed out its 2025 commitments, transitioned to new workstreams, and continued publishing at the highest levels of academic recognition.

### Why it matters

Cardano is the only major blockchain whose core protocol is built on peer-reviewed science. Every protocol change goes through formal academic review before it reaches the network. That process protects the network from design flaws that could cost the community billions, and it gives Cardano a credibility advantage that no amount of marketing can replicate.

### What IO delivered

#### Completed the Cardano Vision Work Package 25 transition

IOR published its end-of-year 2025 reports covering Foundational Research and Technology Validation, ran a three-week public consultation that reached over 24,000 people across ecosystem platforms, and submitted the final reports to Intersect. Work Package 25 – the first under the Cardano Vision program – is now formally closed with all funding milestones complete. Work Package 26 is underway, with new research proposals being assessed following stakeholder interviews.

#### Published two papers at Financial Cryptography 2026

- The first [paper](#), on incentivizing geographic diversity, proposes a way to measure and reward decentralization across physical locations – ensuring Cardano's network isn't concentrated in just a handful of regions.
- The second [paper](#), on restaking security, demonstrates a fundamental limitation in penalty systems for restaking networks – an important finding for anyone designing multi-service staking products, including on Cardano.

#### IO's chief scientist recognized as an ACM Fellow

Professor Aggelos Kiayias was named a Fellow of the Association for Computing Machinery, one of the highest honors in computer science, a distinction held by roughly the top 1% of the global computing community.

This reflects the caliber of scientific leadership behind Cardano's design and marks a monumental academic achievement in Professor Kiayias's career, who is being recognized for his outstanding contributions to cybersecurity and cryptography.

## Preparing the 'Cryptographic Tools for the Blockchain' workshop at Eurocrypt 2026

Scheduled for May, this workshop brings together cryptography researchers from across different blockchain ecosystems. The IOR team is currently reviewing submissions.

### Published research-focused content

- [Cardano Vision 2025 end-of-year reports](#)
- [Peer recognition at the highest level – ACM Fellow](#)
- [From research to reality – building Midnight on peer-reviewed foundations](#)

### 3. The groundwork for Cardano's core stack was laid seamlessly

---

Cardano's node software is the backbone of the entire network. Every stake pool operator (SPO) runs it. Every transaction depends on it. In Q4 2025 and Q1 2026, Input Output Engineering (IOE) shipped two major node releases, improved performance monitoring, and laid the groundwork for the next protocol upgrade. They also helped resolve the mainnet incident in November, maintaining [Cardano's core commitment to security and decentralization](#).

#### Why it matters

When the node works well, nobody notices. If it doesn't, everything stops. IO's ongoing investment in node reliability, performance testing, and upgrade preparation is what keeps the network running smoothly for the 3,000+ stake pools and millions of users who depend on it.

#### What IO delivered

##### Released Node v.10.5.4 and v.10.6.2

In Q1, IOG Engineering (IOE) released node versions 10.5.4 and 10.6.2. These releases improved network connectivity, removed the legacy networking stack, strengthened system monitoring, and introduced foundational support for Cardano's next two protocol versions (v11 and v12, the Dijkstra era). For stake pool operators (SPOs), this means a more stable, better-monitored node with a clear upgrade path.

This was built directly on Q4 groundwork: node v.10.6 had integrated KES agent code changes and LSM-tree support, with node v.10.6.1 deployed to a relay for preliminary performance benchmarking ahead of broader rollout.

##### Released the KES agent v.1.0

The KES agent is a dedicated security component that separates cryptographic key management from the main node process. Rather than keeping signing keys inside the node itself, the agent handles key storage and rotation independently – reducing the attack surface and the risk of key-related incidents for SPOs.

Development was completed and integrated into node 10.6 during Q4 2025, with release, a full security audit, and integration testing. That work concluded in Q1 2026, and the KES agent shipped its 1.0 release alongside node v.10.6.2. Support for running the Cardano testnet with the KES agent was also added. The next steps are to perform performance benchmarking, gather SPO feedback, and identify further improvements.

##### Re-established performance baselines

IOE published benchmarks for nodes v.10.5.4 and v.10.6.2, and deployed an isolated testing environment to safely benchmark security-sensitive changes. This ensures every release is measured against a known

standard before it reaches mainnet. The approach continued from Q4, when performance measurements were gathered from an early LSM-tree-enabled relay deployment.

### Advanced node diversity

The team progressed the formal trace schema definition and tested native Rust trace forwarding – key steps toward enabling non-Haskell node implementations. The Sandstone community team has already released Torsten, a Rust-based full node, demonstrating that this work is unlocking real options for node diversity.

### Improved developer and operator tooling

IOE updated the node-to-client protocol to version 23 – enabling new queries for wallets and tools – and unified all consensus packages into a single package for simpler integration. It also added a snapshot converter daemon that automatically processes new ledger snapshots – useful for operators managing different storage setups – and published new developer documentation for inspecting a node's chain.

### Preparing node v.10.7

Integration is ongoing, bringing together the latest consensus, ledger, networking, and KES agent updates into the next release.

### Ledger and protocol evolution

The ledger team made significant progress in Q4 2025 and Q1 2026 on several proposals that shape Cardano's next ledger era.

**Nested transactions (CIP-112 and CIP-118).** CIP-112 introduced 'Dijkstra native scripts', allowing a Plutus script to be enforced as part of transaction validation. Building on this, CIP-118 finalized the nested transaction design with significant simplifications. Both milestones – a complete CDDL specification and Haskell definition, and the sub-transaction/top-level transaction distinction – were completed in Q4. Work on nested transactions is continuing alongside additional Dijkstra era items, including the first phase of CIP-159. All features are delivered together as part of a single era upgrade, and the Dijkstra era is currently targeted for Q3 2026.

**Canonical ledger state (led by Tweag).** Work focused on creating a stable ledger state representation with canonical, fully specified serialization in CDDL, decoupled from the ledger state serialization and representation used by the actual running node. The result is a cleaner, more reliable data model for downstream tools and implementers.

### UTXO HD, LedgerHD, and LSM trees

UTXO HD moved the UTXO set from memory to disk, reducing cardano-node memory utilization by up to 80%. LedgerHD picks up where that left off, targeting the remaining in-memory ledger state. Underpinning both is the integration of log-structured merge (LSM) trees, which provide the on-disk storage layer.

Core LSM integration into the consensus layer was completed in Q4, with node 10.6.1 deployed to a relay to gather early performance data. The remaining work – API, CLI, and node plumbing – is targeted for node 10.7, with preparatory LedgerHD work already prototyped for node 10.8.

In Q4, the team also produced a report detailing the LedgerHD data migration strategy and the required consensus and ledger adaptations. Q1 implementation began with consensus refactoring – establishing a framework that extends support from the UTXO set alone to multiple distinct data tables with varying key and value structures. Parallel work includes disk-based state storage after each block application and ledger-side preparation for more efficient stake pool distribution computations via pulsing.

## 4. Three scaling solutions, all shipping

---

Cardano's long-term competitiveness depends on its ability to handle significantly more transactions, faster, at lower cost. IO is advancing three complementary scaling solutions – each at a different stage of maturity, all producing working code.

### Why it matters

Scaling is the single most common question from the community, builders, and potential partners. The answer is not one technology but three, each solving a different part of the problem. Mithril makes it faster and cheaper to verify the chain. Hydra enables high-speed transactions for specific use cases. Leios will increase the base layer's throughput capacity. Together, they form a scaling strategy that addresses Cardano's needs at every level.

### Mithril: faster, lighter chain verification

Mithril allows anyone to verify Cardano's state without downloading and replaying the entire blockchain. Think of it as a secure shortcut that lets wallets, apps, and services confirm information on the chain in seconds rather than hours.

Released Mithril 2543.0 and 2603.1.

Q4 saw the release of distribution 2543.0, which added support for the default incremental backend (v2) for Cardano database restoration and introduced enhanced integrity verification – reporting tampered or missing files on failure. A 2543.1 hotfix followed shortly after. In Q1, distribution 2603.1 added support for the decentralized message queue (DMQ) protocol, moving Mithril closer to operating without any central coordinator. The team also integrated support for the Blockfrost API for stake pool metadata and tested the DMQ node v.0.3.0 pre-release, improving accessibility for builders looking to use Mithril.

### Advanced next-generation cryptographic proofs

A major Q4 investment was the design and early implementation of a SNARK-friendly STM cryptographic library – a technology that can create a very succinct certificate. The team completed the library's architecture, implemented the Schnorr signature scheme, and began prototyping recursive SNARK circuits. Q1 built on this foundation, completing core proof-building components, signer registration, and individual signature, and continued progress on recursive proof circuits, with a full security impact assessment complete.

### Built certification for individual blocks and transactions

This feature will allow anyone to verify that a specific transaction or block is genuine, with fine-grained control over finality, without trusting a third party – a fundamental building block for secure light clients and cross-chain bridges.

## Integrated documentation into the Cardano Developer Portal

The team worked on adding Mithril explainers and how-to guides to the [Cardano Developer Portal](#). This improves documentation visibility and ensures that builders can easily find Mithril documentation and references to concrete tutorials from a central development portal.

## Hydra: high-speed transactions for real-world use

Hydra creates dedicated, high-speed layer two state channels alongside the main Cardano chain. Transactions happen almost instantly and at very low cost, while the main chain guarantees final settlement. It's designed for use cases that need speed – payments, gaming, marketplaces, and AI agent interactions.

### Released versions 1.0.0, 1.1.0, and 1.2.0.

Q4 marked Hydra's transition from experimental to production-ready, with three releases shipped across the quarter. Version 1.0.0 arrived in October, followed by 1.1.0 in November – which included deposit improvements and a completed hash time-locked contract (HTLC) demo – and 1.2.0 in December, which added Blockfrost support to the TUI and a new API for retrieving head timestamps.

### Released version 1.3.0 and shipped major protocol work

January and February were focused on stability, performance, and groundwork for the 2.0.0 release. Version 1.3.0 shipped in early March, incorporating most of this work.

### Faster node restarts

Nodes now resume chain sync from the last observed tick rather than the last head state transition, cutting re-sync time significantly after periods of inactivity [#2407](#).

### Chain sync status and drift reporting

The node now tracks and exposes how far out of sync it is with the chain. When drift exceeds 50% of the contestation period, the node rejects client and network inputs, with clear `NodeUnsynced` / `NodeSynced` events and a `RejectedInputBecauseUnsynced` message [#2453](#), [#2505](#).

### Performance and reliability improvements

- Default contestation period changed from 10 minutes to 12 hours to align with Cardano's mainnet safe zone [#2427](#).
- Logging is now buffered and batched for lower I/O overhead [#2452](#).
- Transactions per snapshot are now capped to the bound snapshot size [#2444](#).

- Internal wallet fee estimation was fixed – it defaulted to the max Plutus execution units, making head operations ~4x more expensive than necessary [#2473](#).

## Deposit and decommit bug fixes

Several correctness issues were resolved: deposits and decommits were not always handled correctly on chain rollbacks [#2491](#), a race condition could cause a decommit to be dropped [#2501](#), and the leader node could loop infinitely on `AckSn` after `DecommitFinalized` [#2510](#).

## Re-engaged the community with production-focused working groups

[Monthly sessions](#) now feature real users sharing their experience. DeltaDeFi and Masumi Network presented how they're building on Hydra, and the IO team is collaborating directly with Masumi to deploy their AI agent payment network on Hydra.

## Resolved multiple stability issues

The team fixed several scenarios where nodes could become unresponsive under specific conditions, ensuring more reliable operation for anyone running Hydra in production. Q4 also introduced 'SafeClose' – a safeguard that helps avoid closing a head when unburned minted tokens are present, reducing the risk of fund loss in edge cases.

## Progressed partial fanout

This feature allows users to settle parts of their Hydra state back to the main chain without closing the entire channel – a significant usability improvement for real-world applications. Work progressed across all three months of Q4 and continued into Q1.

## Growing ecosystem adoption

Pondora launched Echo, the first non-custodial Hydra implementation that lets smart contracts participate directly in Hydra channels. This kind of third-party innovation shows Hydra's foundation is mature enough for others to build on. The VTech Hydra SDK was also linked during Q4, and a Raspberry Pi demo using the SDK began development.

## **Leios: next-generation throughput for the base layer**

Leios is Cardano's protocol-level scaling upgrade. It will allow the network to process many more transactions by enabling blocks to be produced and validated in parallel. This is the deepest, most fundamental scaling work – and it's moving from theory into working prototypes.

## Produced a working prototype

In Q4, the teams defined the scope for the first Leios demo and began prototyping mini-protocols, new components, and demo infrastructure using the actual Cardano node as a base. Prototypes were presented on each monthly demo, starting with the first burst scenarios in October. The team also implemented and

audited the cryptographic primitives underpinning both Leios and Peras, providing a verified foundation for the prototype. By Q1, the prototype produces and distributes endorser blocks – including large blocks containing hundreds of transactions – in a local multi-node network, optionally with simulated network delays. This is the first tangible demonstration that the Leios design works in practice.

### **Built simulation and testing tools**

Observability infrastructure using Grafana and Prometheus was built out in Q4 to support load testing and monitoring. Mempool simulations were conducted to study transaction ordering behavior and front-running and MEV risks under Leios. DeltaQ modeling produced a formal report on expected network performance, and network-level experiments led to improvements in multiplexing and transaction submission protocols. Q1 extended this with a trace verification tool to validate protocol correctness and a CLI to configure, run, and observe simulated Cardano networks. These tools enable fast local testing and help catch implementation issues early.

### **Strengthened protocol security**

In Q4, the team merged documentation of the Leios Protocol Burst attack threat model and identified a 'bufferbloat' pathology in early demos, opening an investigation into mitigation strategies. Committee selection underwent benchmarking, simulation, and security analysis across the quarter, culminating in further protocol simplifications that reduce complexity without compromising safety. In Q1, the formal safety property statement has been completed, and the mathematical proof is underway. A joint summary document consolidating findings on safe protocol parameters is on track – drawing from mainnet measurements, simulations, mathematical models, and prior research.

### **Maintained Peras compatibility**

Peras – a complementary protocol enhancement focused on settlement speed, in development by Tweag and ModusCreate – progressed through Q4 alongside Leios. IO's consensus team helped maintain coordination throughout, ensuring compatibility between the two protocols as both move toward a hard fork release.

## 5. Better tools for builders

---

A blockchain is only as useful as the applications built on it. IO is investing in tools that make Cardano easier to build on, safer to deploy to, and more accessible to the next generation of developers.

### Why it matters

Builder adoption drives ecosystem growth, which in turn drives demand for ada, sustaining the treasury. Every tool that lowers the barrier to building on Cardano or raises the security standard for deployed applications makes the entire network more valuable.

### What IO delivered

Plutus: smarter, faster smart contracts, and improved user experience

**Completed Van Rossem hard fork features.** The team completed the Van Rossem hard fork features, including native case analysis for selected built-in types such as Bool, Integer, List, Pair, and Unit; a range of new built-in functions, including built-ins for Value and arrays, modular exponentiation, multi-scalar multiplication, and dropList; and enabling all built-in functions in Plutus V1 and V2. These features have all been implemented, tested, and specified.

**Improved Flat decoding.** Flat decoding for built-in lists was improved, noticeably speeding up Plutus script deserialization. In benchmarks, some scripts now show double-digit performance gains in deserialization time.

**Optimized conversion between bytestrings and integers.** The `byteStringToInteger` and `integerToByteString` primitives were optimized. Both primitives now run in linear time instead of quadratic time. These improvements use the `ghc-bignum` library, which became possible after dropping support for GHC 8.

**Improved the UPLC command-line tool.** The team made significant improvements to the UPLC command-line tool, including support for blueprint JSON as input, the ability to optimize all scripts contained in a blueprint, certifying the optimizations with per-validator certifier reports, and new flags that give users more control over optimization behavior.

**Improved Plinth.** The team made several significant improvements to Plinth. These include a type checker plugin that preserves source locations and produces clearer error messages; a second type checker plugin that detects unsupported Haskell features and further improves error reporting; a driver plugin that automatically sets the required compiler flags and enables the Strict extension; and an enhancement to `AsData` so that it now generates a destructor function for each data type. For sum types, this destructor function is more efficient than pattern synonyms.

## Cardano High Assurance: verifiable smart contract security

Cardano High Assurance delivers all the tools needed for verification and security on Cardano – formal verification, static analysis, property-based testing, profilers, transaction monitoring, and more. It goes beyond formal verification alone, covering every stage of the development lifecycle.

**Launched the early access program.** Five companies are already testing IO's automated formal verification tooling. The team has achieved a significant reduction in processing time and has proven complex smart contracts directly at the UPLC level. They demonstrated this at the Buidler Fest in March.

**Completed a full formalization of the Cardano ledger API.** In Q4, the team delivered a complete formalization of the Cardano ledger API for Lean 4. Together with prior formalizations of PlutusCore, UPLC, and the CEK machine – and the automated formal reasoning backend, Blaster – this enables anyone in the community to express and formally verify smart contracts without needing to write a formal proof themselves.

**Demonstrated real-world vulnerability discovery.** The team formalized a complete example from the [Invariant0 Capture-the-Flag](#), showing how users can apply [formal verification](#) to their own smart contracts and surface vulnerabilities that testing alone would miss.

**Preparing a static analysis tool for Plinth developers.** Plu-Stan is a static analysis tool for Cardano smart contracts written in Plinth. It is based on the Stan static analysis tool. The goal of the project is to help Plinth developers write better code by providing meaningful insights and suggestions to improve code security and performance. The tool has been built and [delivered here](#).

**Building a property-based testing tool.** [This tool](#) automatically generates thousands of test scenarios – including adversarial ones – to find vulnerabilities that manual testing might miss. The core components, including the testing interface, threat model, and example library, are now being integrated.

**Building a Transaction Monitoring System.** The Transaction Monitoring System (TMS) is a new tool for the Cardano ecosystem designed to detect attacks and exploits across the network in near real time. Built in collaboration among IO, AP901, and Politecnico di Milano, the TMS monitors on-chain activity and flags suspicious patterns, including UTXO-level attacks, transaction-logic exploits, market manipulation (front-running, sandwich), and token-based social engineering. Aimed at SPOs and node operators, it provides an early-warning layer that strengthens both individual operations and Cardano's overall security posture.

## Looking ahead: Q2 2026

---

IO's delivery momentum carries directly into Q2 with several high-visibility milestones:

- **Protocol version 11 intra-era hard fork** – coordinated by Intersect, this upgrade brings the latest ledger and smart contract improvements to mainnet
- **Node v.10.7 release** – incorporating the latest consensus, ledger, networking, and security updates
- **Mithril 2608 distribution** – expected to advance SNARK proof integration and block/transaction certification
- **Leios public testnet** – building on the working prototype demonstrated in Q1
- **IOR Work Package 26** – new research underway, informed by stakeholder input
- **Eurocrypt 2026** – Cryptographic Tools for the Blockchain workshop in May

## About Input Output

---

Since 2015, Input Output has been one of the primary architects and builders of Cardano's infrastructure. That work has always been open, accountable, and focused on one goal: making Cardano a network that lasts.

Q1 2026 is a clear example of that commitment in action.

IO closed a major research work package and moved into the next. It shipped two node releases that keep thousands of stake pools running reliably. It launched an early access program for formal verification tools that will raise the security standard for every builder on the network. It released Mithril with decentralized infrastructure support, brought Hydra closer to production with real users shaping the roadmap, and demonstrated a working Leios prototype that shows Cardano's throughput scaling path is real and progressing.

All of this work is done in the open. Research is published in peer-reviewed venues. Engineering milestones are submitted to Intersect for community review and approval. Development progress is reported weekly and publicly for anyone to read. This is how IO has always operated: transparency as a default, not a concession.

The results show in the caliber of partners and institutions now building around Cardano. USDCx. CME Group. LayerZero. MoneyGram. Coinbase. These partnerships happen because the protocol foundations are sound, the delivery track record is credible, and the technology roadmap is progressing on schedule.

IO built those foundations. It continues to build them. And every milestone delivered, every paper published, every tool released is public evidence that treasury funding directed to IO translates into tangible, verifiable progress for Cardano.

Governance is about making informed decisions based on real evidence. This report is that evidence. IO's track record is a pattern, sustained over nearly a decade, of delivering the infrastructure that makes Cardano possible.

---

*This report is compiled from IO's weekly development reports (October 2025–March 2026), IOR quarterly updates, and milestone acceptance documentation submitted to Intersect. All referenced work is publicly verifiable through IO's GitHub repositories, the Essential Cardano development updates, and Intersect's milestone tracking.*