Input Output Research

Cardano Vision & Work Program 2025

Mid-year Report - Technology Validation

Executive Summary

WP25 launches Cardano Vision—a five-year program advancing 20+ research and six technology validation streams to tackle core challenges like scalability, interoperability, governance, and security. Made possible by the Cardano community's support, this Mid-Year Report shares milestones, early findings, and next steps, highlighting IOR's commitment to world-class research and transparent engagement despite the challenges of working at risk.

Evidence-Based methodology

IOR applies an evidence-based methodology built on peer-reviewed science, formal specification, and iterative refinement to ensure designs move from theory to secure, real-world implementation. Progress follows Software Readiness Levels (SRLs):

- **Fundamental Research (SRL 1–2):** formalizing ideas and proofs, 3–5 years to market
- **Technology Validation (SRL 3–5):** prototyping, validating and specs, 1.5–3 years
- **Targeted Implementation (SRL 5+):** guiding engineering into production, 0–18 months

This structured funnel is expected to deliver 100+ research outputs over five years, with ~30 advancing toward validation and deployment.

Technology Validation

Technology Validation bridges research and deployment, turning early concepts into implementation-ready designs through rapid prototyping, simulations, and formal verification. Workstreams deliver specifications, benchmarks, and CIPs to guide adoption, while rigorous tooling and testing ensure alignment with formal models and real-world needs.

- **Formal Verification:** Executable specs prove safety, liveness, and correctness while enabling continuous testing.
- **Prototypes & Simulations:** To validate feasibility, performance, and risks.
- **Specifications & CIPs:** To define designs, guide implementation, and ensure community alignment.
- **Tooling:** Haskell, Rust, Agda, Lean, and custom tools for formalization, simulation, and testing.

Typically running 6–12 months, these projects reduce risk, validate feasibility, and provide confidence for Testnet and Mainnet integration—ensuring only the most promising innovations advance while maintaining Cardano's high standards of security and quality.

Impact and outputs

In 2025, seven Technology Validation streams are delivering major advances in translating research into practical, implementation-ready solutions.

- **TV-1 Leios** progressed toward deployment with refined simulators, a 1,000-node prototype, and a cost model comparing SPO resource use, supported by an executable specification and conformance platform, with CIP handover expected in Q3 2025.

- **TV-2 Anti-grinding (Phalanx)** formalized randomness attacks, designed a Praos-compatible defense raising adversarial costs, and delivered a prototype and CIP now under community review.

- **TV-3 Jolteon liveness** produced a TRL4 Substrate prototype and advanced formal proofs of safety and liveness, complemented by trace-based verification to align implementation with specifications.

- **Tv-4 RSnarks** achieved on-chain Halo2 proof verification, demonstrated recursive proof feasibility via multi-transaction splits, secured a CIP introducing MSM for performance gains, and formally verified foreign-field arithmetic in EasyCrypt.

- **Tv-5 Proof of Restake (Minotaur)** reached SRL4 with a Rust library, specs, simulations, and a Jolteon-integrated PoC, while work on final protocol design and formalization continues.

- **TV-6 Light Clients (Cavefish)** entered its inception phase, refining objectives for a trust-minimized protocol and exploring blind signatures for enhanced privacy.

- **TV-7 Committee Proofs** (proposed) began discovery alongside its recommendation to the community, with planning investigating a Plutus verifier, committee-tracking contract, and formal specification for secure cross-chain committee rotation.

Together, these outputs form a strong pipeline of innovations to strengthen Cardano's scalability, security, and interoperability while creating clear pathways from research to production.

Communication and dissemination

R&D Innovation prioritizes transparency by sharing progress from early prototypes to formal handovers, using tailored approaches per stream. Dissemination spans GitHub, blogs, forums, R&D sessions, and social media—balancing visibility with quality to engage the community and reinforce Cardano's evidence-based innovation.

Contents

1. Introduction

At Input | Output, research isn't confined to theoretical work; it's the engine that drives practical advancements for Cardano. The Work Program 25 proposal, part of the larger **Cardano Vision**, is a five-year journey to shape the future of the ecosystem through science and innovation. Central to this is **technical validation**, which serves as the crucial bridge between foundational research and real-world implementation.

Aligned to Fundamental Research, this Mid-Year report shares our progress so far—milestones achieved, early findings, and priorities ahead. After managing the delays with treasury funding, we're proud to deliver on our proposal commitments as well as IOR's broader role in advancing Cardano through world-class R&D innovation and open community engagement.

None of this would be possible without the Cardano community: your votes, feedback, and trust in research and innovation have brought this program to life, and we're grateful to be building the future with you.

2. Evidence-Based approach

Achieving correctness, security, and reliability in decentralized systems is complex, requiring formal methods—mathematical models and proofs—to build confidence beyond what experiments alone can test. Input | Output's methodology combines peer-reviewed science, formal specification, and iterative refinement, ensuring theoretical designs align with real-world implementation.

Progress is managed through Software Readiness Levels (SRLs):

- **Fundamental Research (SRL 1–2):** Develops and formalizes new ideas with clear goals, trade-offs, models, and rigorous security proofs (3–5 years to market).

- **Technology Validation (SRL 3–5):** Tests early concepts through R&D, prototypes, and simulations, producing specifications to guide implementation (1.5–3 years).

- **Targeted Implementation (SRL 5+):** Supports engineering in deploying solutions in production environments with assurance-focused specifications (0–18 months).

This structured funnel guides work from exploration to deployment. Over five years, it is expected to generate more than 100 high-quality research outputs, with around 30 advancing to technology validation and implementation.

3. Technology Validation

Technology Validation workstreams bridge the gap between research and deployment, turning breakthrough ideas into practical, high-impact solutions. They provide a fast, disciplined process to test and refine research outputs, moving them from early concepts to implementation-ready designs. By focusing on rapid prototyping and cross-functional collaboration, Technology Validation reduces risk, shortens time-to-value, and ensures solutions remain both commercially viable and aligned with Cardano's long-term goals:

- **Formal Verification:** Executable specifications are developed to capture critical properties such as correctness, security, and timeliness. For consensus protocols, this includes proving safety, liveness, and correctness through formal methods, while executable specifications support continuous testing throughout development.

- **Prototypes and Simulations:** Early prototypes explore design trade-offs and uncover practical challenges. Simulations validate feasibility, performance, and risks, while property-based and conformance testing ensure alignment between prototypes and formal models.

- **Specifications and CIPs:** Specifications provide a definitive technical description of the design, serving as both acceptance criteria and a communication tool for implementation. Community-facing CIPs summarize proposed changes and are backed by specifications, prototypes, and benchmark data.

- **Tooling:** Effective tooling underpins cross-disciplinary collaboration. IOR combines off-the-shelf and in-house tools—such as Haskell, Rust, Agda, agda2hs, agda2rust, DeltaQ, QuickCheck Dynamic, Lean, and netsim—for formalization, simulation, and testing.

Each project typically runs for 6–12 months, led by the Innovation team in close collaboration with engineering and research. The aim is to test assumptions in real settings, define clear technical requirements, and deliver prototypes, specifications, and benchmarks that prepare innovations for integration. Early testing identifies weaknesses before significant resources are invested, while functional demonstrations provide confidence to stakeholders and the community.

This structured, evidence-driven process ensures only the most promising innovations progress to Testnet and Mainnet, enabling Cardano to evolve quickly while maintaining its high standards of quality, security, and scientific rigor.

4. Impact and outputs

In the first half of 2025, the Technology Validation program has moved several streams from concept to prototype, delivering tangible outputs that strengthen Cardano's competitiveness and prepare innovations for integration into production.

TV-1 Leios has advanced from validation toward implementation readiness with major breakthroughs in scalability. The team delivered refined simulators, a running prototype, and a cost model calculator to assess SPO costs in storage, networking, and CPU, providing clear comparisons against Praos. Simulations on a 1,000-node test network validated throughput up to 1,000 TPS under realistic conditions, while simpler variants achieved 100 TPS with minimal infrastructure changes. A CIP-ready proposal now balances scalability, security, and operational feasibility, making Leios one of the strongest advances in blockchain parallelism to date.

TV-2 Phalanx (Anti-grinding) directly addressed a long-standing weakness in Proof-of-Stake randomness generation. Starting with CPS-0021, which formally defined and quantified grinding attacks, the team designed Ouroboros Phalanx—a Praos-compatible extension that makes such attacks infeasible under realistic resources while remaining efficient for honest participants. The design is captured in a community CIP, with a prototype and optimizations already in place. Beyond improved fairness and resilience, Phalanx also enables faster settlement by reducing reliance on conservative parameters. Together with Peras, it offers a dual advance: accelerating finality while hardening randomness, positioning Cardano as a leader in secure, fast consensus.

TV-3 Jolteon liveness (fast BFT) progressed on two critical fronts: engineering and formal verification. On the engineering side, the team delivered a TRL4 prototype of Jolteon as a Substrate pallet, validating both functionality and integration within the Polkadot ecosystem. On the theoretical side, the safety proof was completed and published at FMBC'25 and TYPE'25, while the structure of the liveness proof has been formalized and its key lemmas proven. Complementary conformance testing using event traces ensures the implementation behaves as expected, marking a major advance over the informal, "on-paper" proofs typically seen in consensus research.

TV-4 RSnarks expanded the boundaries of zero-knowledge integration with Cardano by achieving the first on-chain execution of a large recursive Halo2-BLS verifier. By splitting verification across 18 smaller transactions, the team overcame existing transaction and script-size limits, proving that even highly complex proofs can run on-chain. Additional advances include efficient pairing checks for BN256 and BLS12-381 curves, generating proofs in 30–60 seconds on a standard PC, and a formally verified algorithm for foreign-field arithmetic in EasyCrypt. Importantly, a CIP introducing a built-in Multi-Scalar Multiplication (MSM) function is already in implementation, ensuring these innovations feed directly into Cardano's protocol stack.

TV-5 Proof of restake (Minotaur) reached SRL4 with a functional Rust library, specifications, and simulations of committee selection, including successful integration into Jolteon's simulation environment. These results validate the feasibility of securing new blockchains by re-staking ADA and ETH, offering a practical pathway for launching new PoS networks. Prototyping also revealed the need for additional protocol features—most notably, the certification of Cardano block headers through Mithril. This would allow compact, time-bound proofs for light clients, bridges, and L2 applications, bringing Cardano closer to feature parity with other ecosystems.

TV-6 Light clients (Cavefish) has begun its inception phase, targeting a secure, decentralized, and resource-efficient way to interact with Cardano without running a full node—a key enabler for mobile users and dApp developers. Work to date has focused on early planning, reviewing IOG's research foundations, and addressing skills gaps.

TV-7 Committee proofs (proposed) entered discovery in July 2025, with the goal of enabling Cardano smart contracts to securely verify rotating partnerchain committees without embedding complex selection logic. The team is exploring a "chain of trust" model where outgoing committees sign commitments to their successors' keys, supported by SNARK-based verification to minimize on-chain costs.

5. Technology Validation updates

For each Technology Validation stream, we outline objectives, progress, deliverables, and the pathway to impact. Expected outcomes include reference specifications, functional prototypes, conformance tests, requirements documentation, and Community Improvement Proposals (CIPs). Together, these outputs ensure practical applications are demonstrated, implementation is well guided, core challenges are framed, transparency and community input are maintained, and correctness is secured before coding begins.

TV-1: Leios

Start Date: Sep 24
Duration (months): 12

(i) Stream overview

Ouroboros Leios is a breakthrough protocol designed to dramatically scale Cardano's transaction throughput while maintaining its industry-leading security guarantees. Unlike current approaches, Leios introduces a parallelized structure that makes near-optimal use of network and computing resources. This innovation enables Cardano to overcome congestion and deliver up to five times more throughput without increasing operating costs for stake pool operators.

The Leios innovation workstream advances the protocol from research into practical readiness. By running large-scale simulations, validating performance, and modeling economics, the project will generate the technical and business case for Leios deployment. Key measures of success include demonstrated throughput gains, preserved fast settlement times, cost neutrality for operators, and proven resilience under disruption or adversarial conditions. Together, these outcomes provide the evidence base needed to progress Leios toward implementation.

(ii) Context and objectives

As adoption grows, Cardano faces increasing demand for network capacity. Current protocols like Ouroboros Praos are limited by block size and production rates, while network and computational resources remain underused. Without innovation, this mismatch risks creating bottlenecks that constrain growth and user experience.

Leios directly addresses this challenge. Its design enables scalable parallelism while preserving the strong security properties of Ouroboros. The project's objectives are to:

- **Demonstrate throughput improvements** of up to 5x under real-world conditions.
- **Maintain fast, predictable settlement times** even under heavy load.
- **Confirm cost neutrality** so operators are not burdened with higher expenses.
- **Prove resilience and security** by testing performance under disruptions and adversarial attacks.

By delivering on these objectives, the project will de-risk deployment, validate Leios as a cost-effective scaling solution, and position Cardano as the most scalable and secure layer-1 blockchain in the market.

(iii) Work performed and main achievements

In the past six months, the Leios stream has advanced from validation toward implementation readiness. The team developed refined simulators, a running prototype, and a cost model calculator to estimate SPO resource use across storage, networking, and CPU, offering clear comparisons between Leios and Praos.

Prototype improvements enabled simulations on a 1,000-node network, validating that significantly higher throughput is achievable under realistic conditions. The formal foundations were strengthened with an executable specification of the Leios mini protocol and a conformance platform to verify prototype behavior.

Close collaboration with IOE Core Technology architects and engineers has ensured alignment with Cardano's node structure, smoothing the path from research to implementation. Final deliverables are being prepared, with CIP review and handover to the next stage expected in Q3 2025.

Deliverables

#	Name	Description	Documentation
D1	Web-based simulators	(i) Protocol and network simulator for various flavours (ii) Performance dashboards (e.g. analysis of various properties and characteristics related to the protocol under varying parameters)	Cardano throughput v0.3 simulation Leios node traffic estimator
D2	Quarterly technical report(s)	Reports capturing a snapshot of the modeling, simulation, and analysis of the Leios protocol at different stages. February and July	Leios technical report #1 Leios technical report #2
D3	Protocol behaviour analysis	Simulations of protocol behaviours and cost calculations	Understanding Leios - A Look at Cost Estimates for Cardano's Next Step Leios simulation index

D4	CIP	CIP added to the CIP library	CIP Leios
D5	Conformance tests & Delta Q model	The Delta QSD models reside in the delta_q repository and their usage and results are documented in the Delta-Q utilities for Rust, and Towards Load Analysis, and especially in the Report on ΔQ progress (Jan 2025)	Leios trace verifier

(iv) Results beyond state of the art

Leios has delivered breakthroughs in blockchain scalability, with simulations showing 1,000 TPS on complex variants using mainnet-like transactions and 100 TPS on simpler variants requiring minimal changes to Cardano's infrastructure—demonstrating both near-term deployability and long-term scalability potential.

Beyond throughput, the team rigorously tested multiple protocol variants to address ledger-specific challenges, converging on a CIP-ready proposal that balances scalability, security, and operational feasibility. Leios achieves true parallelism while preserving settlement times and maintaining Ouroboros' security guarantees—a combination rarely achieved in blockchain protocols. The project also introduced advanced simulation methods to analyze network costs, SPO economics, and resilience under disruption, reinforcing Cardano's leadership in both scalability and evidence-based blockchain design.

(v) Pathway to impact

The next phase of the Leios stream will see it exit technology validation and move IOR for full design and implementation, focusing on finalizing the protocol variant, completing CIP review, and preparing Cardano's node architecture, developer tooling, and ecosystem infrastructure for integration. A formal specification, conformance tests, and large-scale simulations will provide the technical foundation for deployment.

Strategically, Leios delivers up to 5× throughput gains without added costs for SPOs, directly addressing congestion and strengthening Cardano's position against leading blockchains like Ethereum, Solana, and Polkadot. Developed through close collaboration between research, engineering, and governance, Leios ensures both technical rigor and ecosystem readiness. Looking ahead, it will enable Cardano to scale for rising demand and capture opportunities in dApps, real-world assets, and global financial infrastructure—cementing its role as a highly scalable and secure layer-1 platform.

TV-2: Anti-grinding

Start Date: Oct 24
Duration (months): 9

(i) Stream overview

Settlement time—the speed with which transactions become final—is critical for user experience, cross-chain operations, and dApp adoption. In Ouroboros Praos, however, settlement is constrained by the risk of a *grinding attack*, where an adversary manipulates the randomness used in leader elections to bias outcomes. This not only undermines fairness and security but also slows down transaction finality.

The Anti-grinding workstream tackles this challenge by significantly raising the computational cost of such attacks, making them practically infeasible regardless of adversarial resources. Through cryptographic innovation and protocol refinement, this project is expected to deliver both faster settlement and stronger consensus security. The outcomes directly strengthen Cardano's competitiveness as a high-assurance blockchain platform capable of supporting demanding financial and cross-chain applications.

(ii) Context and objectives

Cardano's consensus protocol, Ouroboros Praos, currently assumes adversaries can attempt a limited number of grinding operations during the leader election window. But advances in hardware and adversarial strategies threaten this assumption, forcing overly conservative settlement parameters that slow down finality. The objective of this project is to:

- **Reduce settlement times** by lowering the security parameter k without compromising guarantees.
- **Increase attack resistance** via a 10^{11}-fold increase in the computational complexity of each grinding attempt.
- **Maintain cost efficiency** with minimal additional burden on node hardware.
- **Ensure forward compatibility** by updating the formal specification (Agda) in a way that is sustainable for future Ouroboros versions (Praos, Genesis, Leios, Peras).

By delivering on these objectives, Anti-grinding will enable Cardano to finalize transactions faster, improve user and developer confidence, and mitigate risks from adversarial advances—future-proofing Cardano's settlement performance for years to come.

(iii) Work performed and main achievements

The Anti-grinding workstream met its 2025 objectives with a structured sequence of achievements. It began with CPS-0021: Ouroboros Randomness Manipulation, which formally defined grinding attacks and quantified their impact on security and settlement. Building on this, the team designed Ouroboros Phalanx, a Praos-compatible extension that raises the computational cost of nonce manipulation while remaining efficient for honest participants.

This included modeling adversarial strategies, extending randomness generation across epochs with verifiable hardness, and benchmarking cryptographic primitives such as verifiable delay and trapdoor functions to balance practicality with security. Results confirmed that Phalanx significantly increases the cost of adversarial attempts. The design is now captured in the CIP Phalanx, under community review, with a prototype and initial optimizations in place. With all H1 2025 milestones delivered on schedule, the workstream has entered its transition phase: finalizing CIP review, engaging the Cardano community, and preparing for handover to Intersect for production planning.

Deliverables

#	Name	Description	Documentation
D1	Documentation	(i) Specification (ii) Solution Proposal - VDF selection (iii) CIP	Phalanx sub-protocol specification Cryptographic primitive selection CIP Ouroboros Phalanx (including proposal)
D2	Software	(i) New cryptographic function - Implementation proposal, formalisation & benchmarks (ii) Updated Agda specification for the consensus	Chia VDFs (Verifiable Delayed Functions) Several benchmarks in the CIP Agda specification is still work in progress

(iv) Results beyond state of the art

This project advances Proof-of-Stake consensus by addressing long-standing weaknesses in randomness generation. Phalanx makes grinding attacks infeasible under realistic resources, improving fairness and security, while also enabling faster settlement by reducing reliance on conservative parameters.

Together with Peras, it delivers a dual innovation—accelerating finality while hardening randomness—positioning Cardano as a leader in fast, secure settlement. The work also underscores the need for new monitoring libraries to measure settlement and detect adversarial behavior, helping demonstrate real-world benefits and drive adoption.

(v) Pathway to impact

The plan for full protocol design and implementation includes a review with Intersect's Core Infrastructure and Consensus WG teams to confirm scope and feasibility, followed by integration of a Wesolowski-style VDF library into *cardano-crypto-class*. Node-level implementation will add the necessary logic to *cardano-node*, including a hard fork mechanism for deployment.

A comprehensive conformance test suite will be developed to validate functionality, and coordination will ensure compatibility with other consensus upgrades such as Peras, Leios, and Ouroboros Genesis. Finally, a structured communication plan will inform the community about protocol parameters and the process for updates.

TV-3: Jolteon liveness (fast BFT)

Start date: May 25
Duration (months): 12

(i) Stream overview

This stream focuses on ensuring the liveness property of the Jolteon consensus algorithm—a fast-finality protocol envisioned as the future consensus mechanism for Partner chains. Its primary objective is to provide engineering-based evidence that Jolteon consistently maintains liveness, guaranteeing that the network continues to make progress and process transactions. Achieving this is essential to prevent network stalls and safeguard the reputation of Partner chains.

The core challenge lies in establishing certainty about the conditions under which Jolteon preserves liveness. Network stalls and reliance on centralized recovery mechanisms create serious reputational risks, while the current consensus (Grandpa+Aura) is not considered sufficiently reliable. The innovation of this workstream is the formal verification of Jolteon's liveness—a property not formally verified in similar protocols (e.g., Concordium, Aptos). By doing so, the stream aims to deliver a robust, formally validated consensus protocol that Partner chains can adopt with confidence.

(ii) Context and objectives

A primary focus of this stream is the formal verification of Jolteon, specifically the feasibility and development of mechanized proofs for its safety and liveness properties. The safety proof was completed in Q1 2025. Liveness feasibility has been established, and the team is currently working on its mechanization. In parallel, substantial effort is being devoted to supporting external partners, including the development of trace-based verification methods.

The second major focus is the development of a TRL4 prototype of the Jolteon consensus protocol, implemented as a Substrate pallet to meet the needs of partner chains.

The key objectives of this stream include:

- **Mechanized safety proof** for Jolteon in Agda (feasibility complete, mechanization complete)
- **Mechanized liveness proof** for Jolteon in Agda (feasibility complete, mechanization in progress)
- **Conformance platform** for property-based testing and trace-based behavioral verification (on a final testing stage)
- **Working prototype of Jolteon** up to SRL4 within the Substrate framework (completed)

Proving safety for a complex protocol like Jolteon involves exhaustively modeling all possible states and interactions to guarantee that undesirable outcomes—such as forks or double-spends—can never occur. Liveness proofs are even more challenging, requiring reasoning over infinite executions to ensure the system always progresses and avoids deadlock. Completing both proofs would set a new standard for provable consensus security, offering a level of assurance that far exceeds conventional methods.

(iii) Work performed and main achievements

The team has advanced Jolteon in both prototype development and formal verification. A key milestone was delivering a TRL4 prototype that demonstrates Jolteon as a Substrate pallet, validating its functionality and integration within the Polkadot ecosystem. This prototype provides the engineering foundation for future production deployment.

On the verification side, the team built on earlier work formalizing Streamlet's safety to complete the more complex Jolteon safety proof, and has now laid the groundwork for liveness verification. Progress includes establishing the proof infrastructure, formalizing its structure in a paper, and proving two core lemmas essential to the full result. In parallel, trace-based behavioral verification was applied, analyzing event logs to ensure implementation behavior aligns with formally verified specifications, with ongoing emphasis on safety validation. Work on the full liveness formalization will continue into the second half of 2025.

Deliverables

#	Name	Description	Documentation
D1	Streamlet safety formalization	An Agda mechanization of the Streamlet consensus protocol	Agda mechanization of the Streamlet consensus protocol
D2	Jolteon Safety proof and Agda mechanization	Safety formalization for Jolteon consensus protocol. It was presented at TYPES'25 conference	Agda mechanization of the Jolteon consensus protocol Mechanized safety of Jolteon consensus in Agda, Orestis Melkonian, Mauro Jaskelioff, and James Chapman, 2025
D3	Proof of concept SRL4	PoC integration of Jolteon into Substate as a pallet	To be open sourced
D4	Conformance platform	Confirmance Platform for continuous validation, ensuring that any changes or updates to the Jolteon code do not inadvertently compromise its liveness or safety	To be open sourced
D5	Jolteon Liveness proof and Agda mechanization	Component of the workstream, focused on providing a high-trust, machine-checked proof that the Jolteon consensus protocol possesses the liveness property	To be open sourced

(iv) Results beyond state of the art

The formal verification of the Jolteon consensus protocol, particularly its liveness property, marks a significant advance beyond the current state of the art. While most protocols rely on informal or manual proofs, this workstream has pioneered a rigorous, mechanized approach. In 2025, the team completed the Jolteon safety proof, published and presented at FMBC'25 and TYPE'25, and laid the foundations for liveness verification by formalizing the proof structure and proving key lemmas.

Alongside these theoretical advances, milestones such as prototype refinement, property-based test generation, and conformance trace proofs were delivered on time. A full mechanization of liveness remains in progress, but progress to date represents a major step forward in verifiable consensus. Additional achievements include enhancing the Substrate integration interface and identifying future development priorities through comprehensive code evaluation.

(v) Pathway to impact

By combining mechanized proofs, conformance testing, and trace-based verification, the project sets a new benchmark for engineering rigor in blockchain consensus. Its immediate impact will be to strengthen the security and reputation of Partner chains, ensuring reliable operation and mitigating risks from stalls or centralization.

More broadly, the methodology developed here can serve as a blueprint for the blockchain industry, demonstrating that even complex properties like liveness can be formally verified in practice. This not only enhances Cardano's Partner chain framework but also positions Cardano as a leader in verifiable, high-assurance distributed systems.

The Jolteon prototype as a Substrate pallet delivers a TRL4-ready consensus module for the Polkadot ecosystem, offering partner chains a robust protocol backed by formal verification and conformance testing. Projects like Aptos can leverage its proven security without duplicating the resource-intensive verification effort, fostering a network of interoperable, provably secure chains.

TV-4: RSnarks

Start Date: Feb 24
Duration (months): 15

(i) Stream overview

RSnarks focuses on recursive Snarks, a class of zero-knowledge proofs that allow multiple proofs to be efficiently aggregated into a single, succinct proof. This significantly improves scalability and privacy, with one of the most compelling applications being the construction of a trustless zk-bridge between Cardano and partner chains.

To enable this, this stream adapts the Halo2 proving system, targeting efficient on-chain verification by using a two-step translation process: first generating proofs on the Halo2-Pluto curve and then converting them into Halo 2-BLS proofs, which are verifiable within Cardano's Plutus smart contract platform. BLS is a cryptographic signature scheme that aggregates multiple signatures from different signers into a single, compact signature, significantly improving efficiency and scalability, especially in decentralized systems. The translation requires complex in-circuit arithmetic—notably, cross-curve (wrong-field) arithmetic—and significant optimization to fit within transaction budget constraints.

(ii) Context and objectives

As demand for scalable, interoperable, and privacy-preserving infrastructure grows, RSnarks present a compelling solution. Standard SNARKs are already used in many blockchain systems for efficient proof verification, but RSnarks go further by allowing nested proof systems, making them ideal for recursive state validation, cross-chain bridges, and layered privacy applications.

Cardano's Plutus platform, while powerful, poses constraints in terms of computational budget and transaction limits. The challenge this stream addresses is how to implement RSnark verification efficiently within these limitations. This includes adapting proof systems to be compatible with on-chain smart contracts, and ensuring that proofs are sufficiently compact and performant for real-world deployment.

The objectives of this stream include:

- **Demonstrating on-chain verification** of recursive Halo2-BLS proofs on Cardano.
- **Building a Plutus-compatible verifier** capable of validating Halo2-BLS proofs for circuits that implement Halo2-Pluto verification.
- **Exploring and enabling proof splitting**, allowing complex verifications to be performed across multiple transactions.
- **Benchmarking the performance** of key cryptographic components, such as pairing checks for BN256 and BLS12-381, and evaluating their feasibility within constrained circuit sizes.

The RSnarks stream serves as a foundational step toward scalable, private, and interoperable applications across the Cardano ecosystem and beyond.

(iii) Work performed and main achievements

The RSnarks stream advanced Halo2 proof verification on Cardano through several key milestones. A Halo2 Verifier Generator was developed to automatically produce Plinth code, demonstrating that simple Halo2 proofs can be verified within a single transaction. For recursive proofs, a prototype verifier exceeded on-chain resource limits, but the team proved feasibility by splitting verification across 18 transactions, highlighting the need for further optimization.

Performance was improved through an accepted CIP introducing a built-in Multi-Scalar Multiplication (MSM) function, addressing one of the verifier's heaviest operations. The team also built a Halo2 circuit chip for foreign-field arithmetic (FFA), enabling efficient pairing checks over BN256 and BLS12-381 with proofs generated in ~30 seconds. Finally, a novel FFA algorithm was formally verified in EasyCrypt, resolving technical issues and establishing strong correctness and security guarantees for multiplication and MSM operations.

Deliverables

#	Name	Description	Documentation
D1	Proof of concept Halo2 proof generation	The verifier, built in Rust, generates Halo2 proofs for operations like signatures and recursion, enabling off-chain computation with on-chain verification. A recursive verifier smart contract was also prototyped to run across multiple transactions while preserving consistency, introducing techniques applicable to other smart contracts	Plutus Halo2 Verifier GitHub repository
D2	ATMS Halo2 proof	The tool prototypes verification of the ATMS, a, critical component in many applications including the any potential Cardano zk-bridge	Plutus Halo2 Verifier GitHub repository
D3	Formally verify a novel algorithm for foreign-field arithmetic in Halo2	The team presented in EasyCrypt research paper *Efficient Foreign-Field Arithmetic in PLONK*, *Miguel Ambrona, Denis Firsov, Inigo Querejeta-Azurmendi, 2025,* proving the soundness and completeness of the foreign-field arithmetic (FFA) algorithm	Efficient Foreign-Field Arithmetic in PLONK Formalization of proofs for efficient FFA and MSM algorithms
D4	MSM CIP contribution	A CIP has been proposed for a built-in MSM in Plutus, targeting a computationally intensive operation that underpins many cryptographic protocols, including digital signatures, zero-knowledge proofs, and elliptic-curve–based SNARK systems such as Halo2.	CIP for MSM over BLS12-381

(iv) Results beyond state of the art

This stream advanced zero-knowledge proof capabilities on Cardano by demonstrating the first successful execution of a large recursive Halo2-BLS verifier on-chain, achieved by splitting verification across multiple transactions to overcome size and resource limits—paving the way for complex applications and trustless bridges.

The team also implemented highly efficient pairing checks for BN256 and BLS12-381 curves, enabling proofs to be generated in 30–60 seconds on a standard PC. Importantly, these results are already influencing Cardano's core protocol, with a new CIP for Multi-Scalar Multiplication (MSM) now in implementation, ensuring the work's practical integration and long-term ecosystem impact.

(v) Pathway to impact

The pathway to impact follows a staged approach: first optimizing performance and reliability, then engaging developers, and finally broadening supported applications. Immediate priorities include reducing the high computational cost of verification—currently requiring multiple transactions—by leveraging the new MSM CIP and exploring Aiken for on-chain logic, alongside a full independent security audit of wrong-field arithmetic to build confidence for future dApps.

Once the prototype is more robust, the stream will focus on adoption, releasing an SDK with a developer-friendly interface, hosting community workshops, and supporting proofs of concept such as private voting or confidential DeFi. Longer term, the team will integrate zk-Bridge functionality, enabling trustless state exchange between Cardano and other blockchains.

TV-5: Proof of restake

Start Date: Feb 24
Duration (months): 19

(i) Stream overview

The Minotaur stream explores hybrid consensus as a way to bootstrap new Proof-of-Stake (PoS) blockchains—called Minotaur Chains—by re-using stake from established networks such as Cardano and Ethereum. Instead of relying solely on newly minted tokens (which lack distribution and security in the early phases), Minotaur introduces the concept of "Virtual Stake", allowing validators to re-stake their ADA or ETH to secure the new chain.

A dynamic conversion rate, based on USD price oracles and resource weights, governs how much influence each asset contributes. Over time, as the Minotaur token supply grows, the system gradually transitions toward native stake dominance. This model provides a robust path for launching new blockchains with strong initial security, liquidity, and decentralization.

(ii) Context and objectives

The main challenge Minotaur addresses is the security gap in early-stage PoS networks where no meaningful stake distribution yet exists. By leveraging re-staked assets from mature ecosystems, Minotaur provides a ready-made trust base while also enabling cross-chain collaboration.

Key innovation questions include how to align epochs across different chains, authenticate cross-chain addresses, penalize misbehavior, manage finality delays from asynchronous stake snapshots, and extend governance (DParameter) to account for multiple asset types. The objectives are to design and validate a multi-resource consensus protocol that supports:

- **Secure committee selection** from aggregated cross-chain stake.
- **On-chain contracts** on Cardano and Ethereum for re-staking, slashing, and governance.
- **A practical integration** with Partner chains, enabling new DAOs and blockchains to launch with credible security.

Minotaur aims to define a generalizable model for multi-resource staking, creating new opportunities for SPOs, DAOs, and asset holders to re-stake across chains, earn rewards, and strengthen interoperability.

(iii) Work performed and main achievements

In 2025, the Minotaur project reached SRL4, delivering multiple proof-of-concepts and preparing the ground for a formal protocol design. Achievements included a functional Rust library, two protocol specifications, a full simulation of a custom committee-selection algorithm, and successful integration of a proof-of-concept into the Jolteon simulation environment—together demonstrating the feasibility of proof-of-restaking.

The Research team is now developing the final protocol design with formalization and security proofs, after which development will resume. Planned activities include SRL5 integration of the Minotaur library with Partner chains.

Deliverables

#	Name	Description	Documentation
D1	Minotaur Library in Rust + specification	Functional Rust library and formal protocol specifications that demonstrate the technical viability of its multi-resource consensus model	To be open source once there is enough proof on protocol stability and its associated safety and liveness proofs
D2	Minotaur Protocol PoC in Jolteon Simulation environment	Integrated the core logic of the Minotaur protocol into a comprehensive simulation environment.	To be open source this work once there is enough proof on protocol stability and its associated safety and liveness proofs
D3	Restaking-Aware Committee Selection algorithm	Core component of the Minotaur protocol, designed to solve the problem of fairly and securely selecting a committee of validators from a diverse pool of restaked asset	Team will open source this work once there is enough proof on protocol stability and its associated safety and liveness proofs
D4	Minotaur Protocol Model in Agda	A formal, mathematical proof of the protocol's logic and correctness. Which functions as a proof assistant, to verify that the protocol's rules and behaviors are sound and free from logical errors.	Team will open source this work once there is enough proof on protocol stability and its associated safety and liveness proofs

(iv) Results beyond state of the art

The Minotaur project's Proof of Restake protocol advances blockchain consensus beyond the current state of the art by enabling multi-resource, cross-chain restaking—a powerful new model for securing emerging networks. While platforms like EigenLayer have introduced restaking within a single ecosystem (e.g., Ethereum), Minotaur expands this concept by allowing new blockchains to bootstrap security using stake from multiple established chains, such as Cardano and Ethereum. This multi-source approach enhances decentralization, mitigates economic dependency on a single asset, and sets a new benchmark for flexible, secure network launches.

Prototyping uncovered several critical next steps to realize the full potential of the protocol. Chief among them is the implementation of a Cardano CIP to include Merkel roots in block headers, enabling efficient state tracking by light clients—a key requirement for restaking verification. This functionality also unlocks broader interoperability benefits, such as powering zero-knowledge bridges (e.g., BitVMX), L2 systems (e.g., Midgard), and state channels (e.g., Hydra). Additionally, the team proposes extending Mithril to certify Cardano block headers, providing compact, cryptographic proofs of inclusion and time-stamping. Together, these innovations position Cardano for interoperable, trust-minimized consensus protocols on par with or ahead of peer ecosystems.

(v) Pathway to impact

Proof of Restake creates new revenue for SPOs and DAOs by enabling multi-resource staking across chains, fostering Cardano integration while rewarding asset holders who restake their tokens to secure partnerchains.

TV-6: Light clients / Cavefish

Start Date: Aug 25
Duration (months): 9 (estimated)

(i) Stream overview

Many dApp developers avoid running full Cardano nodes due to their heavy resource demands, instead relying on centralized providers like Blockfrost—convenient but a single point of failure that weakens decentralization. While Mithril offers concise state certificates, it still depends on external data providers for transaction details. The key challenge is therefore to design a trust-minimized framework that enables lightweight, decentralized access to on-chain data without compromising security or scalability.

(ii) Context and objectives

The Light Clients project seeks to provide a secure, decentralized, and resource-efficient way for users to interact with Cardano without running a full node—removing a key barrier for mobile users and dApp developers. The goal is to design and prototype a protocol that lets light clients manage wallets and execute simple smart contracts while minimizing trust in third parties. Specific objectives include:

- **Designing a secure protocol** for verifying ledger state with minimal assumptions.
- **Developing an incentive model** for third-party data providers.
- **Prototyping and validating** the approach; and formalizing technical, security, and incentive requirements.

A further research goal is to explore a novel blind signature scheme to enhance privacy and security, potentially introducing a new cryptographic primitive.

(iii) Work performed and main achievements

The project is in its inception phase, with efforts focused on reviewing the initial IOG Research paper, conducting early planning, and performing a skills gap analysis to ensure the team has the expertise needed to deliver on its objectives.

Deliverables

#	Name	Description	Documentation
D1	Protocol specification	Detailed specification on how the protocol works	Expected to be open sourced halfway through the project
D2	Incentive & security analysis	A comprehensive study analyzing the economic incentives for participation in the light client network, considering current and future decentralized Blockfrost and Mithril participation. An in-depth evaluation of the security assumptions and potential vulnerabilities of the light client infrastructure, providing clear mitigation strategies.	Expected to be open sourced halfway through the project
D3	Formalized technical requirements	A document detailing the precise technical requirements for the light client system, including performance, scalability, and resource constraints.	Expected to be open sourced halfway through the project
D4	Prototype	Software up to SRL4/5 containing the proposed protocol behaviour	Expected to be open sourced halfway through the project
D5	CIP	CIP to be added to the CF CIP library	Expected to be open sourced halfway through the project

(iv) Results beyond state of the art

A novel blind signature scheme, currently under refinement, could introduce a new cryptographic primitive that reduces reliance on centralized data providers, marking a significant advance in decentralized light client infrastructure.

(v) Pathway to impact

This is currently being investigated at a high-level.

TV-7: Committee proofs (proposed)

Start Date: August 25
Duration (months): 9 months (estimated)

(i) Stream overview

Committee Proofs explores how to enable a secure cross-chain bridge between Cardano and Partner chains. The challenge lies in Cardano's inability to directly verify the rotating consensus committees of another chain. To address this, the project proposes a "chain of trust," where each outgoing committee signs a commitment to the next committee's keys, creating a verifiable sequence of authority.

To keep this efficient within Cardano's constraints, SNARKs will be used to compress and validate committee signatures. A further innovation is the potential use of the Aiken language for implementing the verifier, which could deliver significant performance gains. The ultimate goal is to demonstrate the feasibility of committee-based, SNARK-verified bridges that expand Cardano's interoperability capabilities.

(ii) Context and objectives

Partner chains currently rely on Aura/Grandpa with rotating committees chosen from Cardano SPOs, but Cardano smart contracts have no native way to verify these committee transitions. This gap prevents state changes on the partner chain from being securely certified back to Cardano. The Committee Proofs project addresses this by:

- **Establishing a cryptographic "chain of trust"**, where each outgoing committee signs over the next committee's keys.
- **Using SNARKs** to compress and efficiently verify committee signatures on Cardano.
- **Exploring Aiken** for building a more performant SNARK verifier compared to Plutus.
- **Delivering a full prototype** that integrates this mechanism into a Cardano smart contract, with formal verification to ensure its robustness.

(iii) Work performed and main achievements

The Committee Proofs workstream began its discovery phase in July 2025. The initial focus is on laying the technical foundation for a secure, committee-based bridge between Cardano and partner chains, whilst planning deliverables.

Deliverables

#	Name	Description	Documentation
D1	Plutus verifier	Plutus verifier for Halo2 proofs to authorize committee rotations	Not yet started
D2	Plutus smart contracts	Plutus smart contract capable of tracking Midnight's rotating committees and enforcing updates through verified proofs	Not yet started
D3	Formal specifications	Formal specification capturing the full committee rotation process to guide future implementation and validation	Not yet started

(iv) Results beyond state of the art

The stream pioneers a new "chain of trust" approach, where outgoing committees sign the keys of their successors, enabling Cardano to verifiably track partnerchain rotations without embedding the full selection algorithm.

To overcome the high cost of verifying committee signatures, it explores SNARK-based proofs and the novel use of Aiken for more efficient on-chain verification—pushing the boundaries of secure, scalable cross-chain bridging.

(v) Pathway to impact

This is currently being investigated at a high-level.

6. Communication and dissemination

Transparency is central to IOR's innovation process. We share progress throughout each workstream—starting with early hypotheses and prototypes, through formal validation, and ending with structured handovers that package specifications, code, and documentation for downstream engineering. This staged approach ensures smooth transitions, accelerates adoption, and minimizes knowledge loss. Examples include the Technical validation approach blogpost and Cardano R&D session in August where the team provided a status update on different workstreams.

Dissemination follows a multi-channel strategy: GitHub for code transparency and papers. IOHK blogs for context, Discord and the Cardano Forum for interaction, monthly R&D sessions for live engagement, and targeted social media campaigns to amplify milestones. Together, these efforts build a culture of evidence-based innovation, reinforcing Cardano's reputation for openness, rigor, and impact in blockchain research.

Best practice is tailored to each stream. Leios serves as a flagship, with an open repository from its inception, monthly live updates, weekly progress updates, technical report and blogpost explainers. Conversely, RSNARKs was open-sourced at the end of the prototyping, including explanatory blog posts. Across all streams, the aim is consistent: balance visibility with quality, and engage the community at key points in the lifecycle.

Appendix

A. Proposal documentation

The Input Output Research (IOR): Cardano Vision - Work Program 2025 proposal includes of the following documents:

- Input Output Research (IOR): Cardano Vision - Work Program 2025 Proposal v1.0.pdf
- Input Output Research (IOR): Work Program 2025 - Proposed Technology Validation Streams v1.0