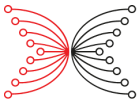
Call Overview



Input | Output Research

First call for 2026 proposals

Fundamental research in blockchain technology advancing the Cardano ecosystem

Introduction

Input | Output Research (IOR) welcomes expressions of interest to contribute to *Cardano Vision* – a multi-year research initiative designed to strengthen Cardano's leadership in blockchain science and decentralized systems. Building on IOR's history of peer-reviewed research and real-world impact, this call invites academics, research groups, and consortia to propose work across a set of priority thematic focus areas. Additional themes may be introduced in future calls.

Evidence-based methodology

IOR advances the foundational science of blockchain and decentralized systems through **first-principles thinking** and a rigorous **evidence-based methodology**. Our mission is to deliver scientific excellence that supports IOR's long-term vision for decentralization, transparency, resilience, and global accessibility in the ecosystem.

IOR follows a clear maturation lifecycle – from fundamental research to technology validation and ultimately production deployment. This process is grounded in peer-reviewed computer science, formal methods, and precise specification. We formalize ideas that extend beyond the state of the art by defining requirements, identifying trade-offs, developing mathematical models, and delivering solutions supported by rigorous security proofs.

Through close collaboration with leading academic institutions, IOR publishes peer-reviewed research and applied innovations that tackle three essential challenges for global blockchain adoption: sustainability, scalability, and interoperability. By uniting foundational research with practical engineering, we help ensure breakthroughs in cryptography, consensus, and protocol design translate into robust, real-world impact across the Cardano ecosystem.

Research areas

By expanding its world-class research portfolio, we aim to reinforce Cardano's global and unique standing in the blockchain landscape. We invite proposals for the following thematic areas detailed in the respective sections of this document.

I. **DSL for smart contracts:** domain-specific languages **(**DSLs) enable domain experts to create smart contracts without extensive software development. Cardano's Marlowe DSL has shown the value of this approach in finance, and this research area aims to identify further domains – legal, tokenization, and supply chains – where new DSLs could support high-value applications.

II. **Global identity:** decentralized identity enables privacy-preserving, user-centric, and interoperable digital credentials. This research area focuses on defining the foundations

of a global identity framework and integrating it seamlessly into the Cardano ecosystem.

III. **Proof of useful work:** proof of useful work remains underrepresented in consensus research, yet it holds significant potential to create more robust, inclusive protocols by rewarding meaningful computational effort. This area explores several promising directions to advance useful work–based consensus mechanisms.

IV. **TPS decision making toolsets**: effective decision-making in Cardano relies on the ability to quantify impact across dimensions such as decentralization, cost, utility, interoperability, and performance. This workstream refines how ecosystem throughput is defined and measured, going beyond simple Transactions Per Second (TPS) counts to reflect the actual utility of processing computations and data of varying complexity.

Proposal requirements

Each thematic Call For Proposal (CFP) sets out a defined goal and specific objectives that proposals should align to as best as possible given the scope and timeline. Applicants are expected to demonstrate a solid understanding of the current state of the art and present a clear, well-reasoned plan for advancing research beyond it in line with the call.

Research proposals should not exceed **4-6 pages** and must include:

1. Title and abstract (max. 250 words)
2. Research team and institutional profile
3. Scope and objectives
4. Work plan and approach
5. Deliverables and milestones
6. Staffing, budget, and justification
7. References.

Teams should include a balanced mix of experience – from junior researchers to senior academics, research engineers, PhD candidates, PostDocs, and professors – to ensure strong methodological depth and effective execution.

Change requests will only be considered in cases of extraordinary and unforeseen circumstances, which will be determined at the sole discretion of IOR. IOR is under no obligation to grant any requested change.

Budget guidelines

Each thematic CFP specifies an estimated budget for 2026 that proposals should consider. Budgets should be clearly itemized and include a concise justification for all requested costs.

Proposals should include an indicative Full-time equivalent (FTE) commitment per year, reflecting the level of effort expected from the selected team. Eligible costs include researcher time, essential equipment, overheads, and dissemination activities.

Payment schedules will follow a standard structure, with disbursements made up-front, mid-year, and at year-end.

It is anticipated that research efforts will be multi-year, subject to budget availability, though the scope for the first call for proposals is for 2026 *only*.

Evaluation criteria

Proposals will be evaluated by an IOR review panel against the following core criteria:

- Alignment with the thematic focus
- Scientific excellence and contribution beyond the state of the art
- Methodology and feasibility of the proposed approach
- Team expertise, capacity, and balance
- Budget clarity and appropriateness.

Timeline and next steps

Cardano Vision follows a multi-stage process to ensure strong alignment between proposed research and IOR's priorities.

- **Call launch:** November 17, 2025
- **Proposal submission deadline:** December 16, 2025
- **Invitations to interview**: mid-January 2026
- **Final evaluation:** January / February 2026
- **Project start:** soon thereafter.

Proposals for each thematic CFP should be submitted as a single document to Mirjam Wester at mirjam.wester@iohk.io with the subject line: **'CFP26 – Expression of Interest'**.

Please also contact Mirjam with any queries or for pre-submission discussions.

26.1 Global Identity

INPUT | OUTPUT

CFP26.1 Global identity

Overview

This workstream explores the design of a global identity system that gives Cardano users full, cross-platform control over their digital identities, allowing selective sharing of personal information. It focuses on defining a general, implementation-independent framework built on formal abstractions of trusted components like credential systems and public key infrastructures. The goal is to identify trade-offs between different design choices and develop practical, efficient implementations. The work also examines how identity systems interact with applications, including cross-platform identity portability, and how to integrate these systems into the broader digital identity landscape.

Research goal

While formal definitions of global identity are still rare and no commonly accepted notion exists, terms like ‘decentralized,’ ‘privacy-preserving,’ ‘user-centric,’ and ‘self-sovereign’ frequently appear in digital identity discussions. This research aims to define the foundations of a global identity system, connect it to current and emerging trends – such as decentralized identifiers, verifiable credentials, and anonymous credentials –, identify tradeoffs that arise in practice (eg, how different combinations of each building block facilitates/complicates recurrent operations like key rotation or revocation), and finally explore how to integrate these concepts natively within the Cardano ecosystem. A key focus will be understanding Cardano’s role as a potential backbone for this evolving identity framework.

Applications

To integrate the notion of global identity (or, rather, an instantiation of it) within Cardano’s core (transactions, smart contracts, governance) and the wider Cardano ecosystem. Additional applications include augmenting existing stacks to be compatible with this notion of global identity.

Objectives and deliverables

We expect proposals to align with a subset of the following main objectives and deliverables:

- A universal definition of global identities that acknowledges their anticipated use in applications. Aspects like decentralization, interoperability, portability, multi-authority, self-certification, privacy, and reputation should be considered. The main deliverable here is a research paper.

- Concrete constructions of digital identity systems, respecting their use across different platforms (blockchains, traditional public key infrastructure (PKI)) and exploring different trust models and efficiency or operational tradeoffs to build credentials for identities, with a focus on interoperability and portability. The main deliverable is a research paper with early benchmarks.

- Applications: construct the required protocols to support one or more high-value applications using digital identities, where the application is properly formalized with functional and security requirements. The main deliverable is a research paper with associated artifacts to assess practicality.

- Integration of the proposed protocols into a known protocol stack, such as Hyperledger Identus, for a concrete prototype.

Budget and timeline

We expect expressions of interest in the region of $360,000 for 2026.

This workstream is anticipated to run for two years or more, subject to scope refinement, budget availability, and delivery performance.

Selected references

- Foundations of Anonymous Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions (Bobolz et al., 2024)
- What DIDComm Out of It? Analysis and Improvements of DIDComm Messaging (Badertscher et al., 2024**)**
- Hyperledger Identus
- SyRA: Sybil-Resilient Anonymous Signatures with Applications to Decentralized Identity

26.2 DSL for Smart Contracts

INPUT | OUTPUT

CFP26.2 Domain-specific languages for smart contracts

Overview

Domain-specific languages (DSLs) enable domain experts to implement smart contracts and decentralized applications within their domain of expertise, eliminating the need for full-scale software development and significantly lowering the barrier to entry. Within Cardano, we have already demonstrated the feasibility and utility of this approach by developing, implementing, and launching the Marlowe DSL for financial contracts [1]. Building on this previous work, the purpose of this area is to investigate other domains to find suitable candidates for DSLs for other high-value applications, such as legal applications, asset tokenization, and supply chain management.

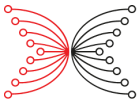
Research goal

While there is work on formalizing core notions in domains such as legal applications, asset tokenization, and supply chain management in a more formal manner, there is little in terms of utilizing this to open these domains for applications on blockchains. The goal of this research is to improve upon this current state.

As an initial subgoal, we require a suitable formal language (such as a calculus or formal logic) that can capture the required operations in the domains of interest. Such a formal language is the basis for the second subgoal, namely the development of a domain-specific protocol for the interaction of several parties facilitated by Cardano. Finally, as a third subgoal, the formal language, together with the interaction protocol, facilitate building a development environment for domain-specific applications on Cardano, much as this was done with Marlowe.

Applications

The development environments for Cardano applications in the specified domains – legal applications, asset tokenization, and supply chain management – will facilitate the development of end-user applications by domain experts without requiring them to learn about the intricate details of developing general-purpose smart contracts on Cardano. As such, this research aims to lower the barrier to entry and encourage the use of Cardano in these domains. Other domains beyond those identified above are also eligible if they make a strong case for being relevant to practice and the Cardano ecosystem.



Objectives and deliverables

The main objective is to investigate domains of high-value applications on blockchains, specifically, (1) legal contracts, (2) supply chain contracts, and (3) asset tokenization contracts (such as the tokenization of real estate). This includes, for each of these domains, the development of a suitable formal language able to capture the required operations in the domain, the development of a domain-specific protocol that facilitates interaction among multiple parties via Cardano, and building a development environment that enables domain-specific applications on Cardano with minimal development experience.

In the course of pursuing these objectives, we expect the following deliverables for each DSL domain. Applicants may submit more than one DSL proposal.

1. A semi-formal or formal description capturing the core operations in the domain of discourse, including the specification of a semantics for these operations. Ideally, the description is formal and mechanized in a theorem prover such as Agda, Rocq, or Lean.

2. A semi-formal or formal description of the protocol that facilitates several parties to interact in the domain of discourse in a manner that can be realized on the basis of Cardano's EUTXO ledger model.

3. A prototype implementation for a DSL built on the basis of the above two deliverables. This also includes a development environment and an interpreter or compiler that enables a DSL application to be launched on Cardano.

4. A paper covering the formal language underlying the DSL, prototype implementation, and the underlying semantics.

Budget and timeline

We expect expressions of interest in the region of $180,000 per DSL (legal, supply chain, asset tokenization) for 2026.

The workstream is anticipated to run for two years or more, subject to scope refinement, budget availability, and delivery performance.

Selected references:

[1] Marlowe: implementing and analyzing financial contracts on blockchain (Lamela et al., 2020).

26.3 Proof of Useful Work

CFP26.3 Proof of useful work

Overview

Blockchain protocols based on proof of work (PoW) capitalize on the work performed by the miners to ensure the security of the transaction ledger they maintain, which is the work's only purpose.

The motivation for proof of useful work (PoUW) is to base the PoW on computation that solves real-world problems, and hence, the energy spent has a dual purpose outside the scope of the consensus protocol. The benefits of such effort for Cardano can be exemplified in extensions of the Ouroboros protocol, such as Minotaur [6], that enable blending proof of stake (PoS) and PoW for better security and incentive alignment.

Prominent solutions of PoUW are targeted to perform computation-intensive tasks, such as machine learning (ML) (eg, via stochastic gradient descent or local search [1]) or generating non-interactive zero-knowledge proofs/arguments (NIZKs) [2]. An example application of PoUW ML is training Large Language Models (LLMs). A particular application of PoUW NIZK generation is the computation of succinct ledger-state proofs for the very blockchain whose mining is based on the PoUW.

This research stream explores improvements over existing PoUW solutions with a focus on its use in blockchain mining in two different directions, each assigned to a separate workstream below.

Research goal

Current constructions for PoUW are based on strong (non-standard) security assumptions (eg, [1,4]) or involve parameter constraints that are not well-suited to the case of blockchain mining (eg, [2]). Additionally, existing solutions are not privacy-preserving in the sense that the PoUW problem and its solution are revealed to the public.

We scope two *separate* workstreams as follows, where we invite applicants to select one of them in their proposal as the main focus.

Application

Beyond a better alignment of security, participation, and incentives, blockchain systems are in constant development to anticipate future trends, such as the better integration of succinct non-interactive argument of knowledge (SNARKs) and coSNARKs (joint privacy-preserving generation of SNARKs), or the emerging interest in AI and ML training. Performing useful work

as part of securing a blockchain system offers new opportunities to leverage existing hardware to solve these problems while securing a platform at the same time.

Workstream A. ML PoUW

Objectives and deliverables

Explore PoUW for solving ML problems. Another high-value target may also be proposed, with proper justification. The goal is to further research solving ML problems via PoUW (cf. [1,3]) in the following aspects:

1. **Security assumptions.** A novel protocol is to be provided that relies on weaker-than-previous security assumptions; and/or, the notion of 'moderate hardness' from [1] (and variants thereof) is to be explored with the goal of providing new insights about the security of PoUW, and PoUW-based blockchain mining in particular.

2. **Heterogeneous problem solving.** In a productive PoUW system solved problem instances must be sequentially replaced by new ones, and multiple instances may even need to be computed concurrently. Additionally, for broad usability, we require the ability to process instances from a wide range of problem classes, implying different computational characteristics for different PoUW instances. A solution is to be provided that allows for integrating different problem classes into the same PoUW protocol while maintaining the same level of (moderate) hardness for solving PoUW challenges across instances of different problem classes. In particular, the protocol must guarantee that multiple problem instances can be worked on via PoUW concurrently, and that solved instances get seamlessly replaced by new ones without enforcing any idle time on the miners.

3. **Privacy.** A solution is to be provided that enables the problem poser to publish the problem in a manner that allows miners to compute and publish the solution while keeping the problem instance and the solution private to the problem poser.

As a requirement, any resulting PoUW protocol should deliver problem solutions of comparable quality to state-of-the-art ML algorithms, and with minimal computational overhead (to maximize 'usefulness' of the computation). A prototype realizing the protocol, or specific components such as the PoUW algorithm, is also highly desirable.

The deliverable is a research paper that makes a substantial step towards solving one (or more) of the above aspects. All relevant artifacts, such as code, simulation results, etc, should additionally be delivered.

INPUT | OUTPUT

Workstream B. NIZK PoUW

Objectives and deliverables

The goal is to further research the computation of NIZKs via PoUW (cf, eg, [2]). A new PoUW protocol is to be provided that performs PoUW by computing NIZKs with characteristics that allow for its use as a substitute for plain PoW in blockchain mining (in particular, time required for solving a single PoUW challenge, verification time, and variance in mining success times). For broad usability, we need the ability to create NIZKs for a wide range of statements/relations with emphasis on proofs of classes of statements that can be of high value to the Cardano ecosystem. As an example, one important application is to create state proofs for blockchains [5] (and, for instance, for a PoUW blockchain specifically). As many applications do not require it, the solution may optionally maintain the zero-knowledge property (ie, the proof witness may be leaked during the process).

A research paper that makes a substantial step towards making PoUW NIZK computation feasible for use as a PoW substitute in blockchain mining, for a wide variety of statements/relations, and for blockchain state proofs in particular. A prototype realizing the protocol, or specific components such as the PoUW algorithm, is also highly desirable.

Budget and timeline

We expect expressions of interest in the region of $180,000 per workstream for 2026.

This workstream is anticipated to run for two years or more, subject to scope refinement, budget availability, and delivery performance.

Selected references

[1] Fitzi, Matthias, et al. ‘Ofelimos: Combinatorial optimization via proof-of-useful-work: A provably secure blockchain protocol.’ Annual International Cryptology Conference. 2022.

[2] Kattis, Assimakis, and Joseph Bonneau. ‘Proof of necessary work: Succinct state verification with fairness guarantees.’ International Conference on Financial Cryptography and Data Security. 2023.

[3] Su, Xiangyu, Mario Larangeira, and Keisuke Tanaka. ‘Provably Secure Blockchain Protocols from Distributed Proof-of-Deep-Learning.’ *International Conference on Network and System Security*. 2023.

[4] Fitzi, Matthias et al. ‘Efficient and Proof-of-Useful-Work Friendly Local-Search for Distributed Consensus.’ Manuscript. 2025.

[5] Bonneau, Joseph, et al. ‘Coda: Decentralized cryptocurrency at scale.’ Cryptology ePrint Archive (2020).

[6] Fitzi, Matthias, et al. ‘Minotaur: Multi-resource blockchain consensus.’ *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. 2022.

26.4 Decision Making Toolsets TPS

INPUT | OUTPUT

CFP26.4 Effective TPS metrics

Overview

This workstream focuses on defining and measuring the *throughput* of an ecosystem. Traditionally, system throughput is measured (and compared) by means of the number of transactions per second (TPS) that it can process – regardless of the actual utility that the settlement of the given transactions provides as a decentralized validation service for computations of variable complexity and for long-term storage of data of variable size.

Research goal

The goal is to develop meaningful methods for measuring the throughput of a blockchain (or traditional) ecosystem that allow for a better comparison of throughput across different systems (or the system before and after a modification in its codebase) than using the traditional TPS measure.

Specifically, we ask for a throughput measure that accounts for utility as described above, recognizing that, for example, settling a complex smart contract transaction creates more value than settling a simple payment transaction. For example, a single transaction in one system may have an array of effects, which can only be achieved by many transactions in another system. Further aspects beyond the computational and space complexity of a transaction may need to be considered as part of the utility, eg, the level of decentralization that the system offers.

Applications

The availability of a broad range of decision-making tools will help businesses make informed decisions about which ecosystems to engage with and how to design their smart contracts and DApps to best suit customer needs, considering the technical guarantees and constraints imposed by the underlying system. In particular, a better notion of throughput will help to more accurately assess whether a system is capable of serving the anticipated number of clients, and whether additional tools (such as layer 2 protocols) are required to achieve the business goals.

Most critically, such tools will be an indispensable tool in governance and decision making as they bring an objective viewpoint when evaluating the impact of a protocol or parameter change proposed in a governance action. In this way, we expect that the developed metric will be important in the context of Cardano governance.

INPUT | OUTPUT

Objectives and deliverables

New throughput measures for (blockchain) ecosystems are to be developed and compared as follows:

1. **Definition and comparison.** Define new meaningful throughput measures and qualitatively compare them against each other (and previous notions).

2. **Quantitative comparison.** Evaluate the throughput of different prominent ecosystems (at least Bitcoin, Ethereum, and Cardano) under the suggested (and previous) measures, and compare them against each other.

A research paper is to be delivered, defining new meaningful throughput measures for (blockchain) ecosystems and evaluating them against each other (and previously suggested ones). Based on these results, a quantitative throughput comparison between prominent blockchain systems is to be provided, similarly to how [2] compares the decentralization of different systems. All relevant artifacts, such as code, measurement results, etc, should also be delivered.

Budget and timeline

We expect expressions of interest in the region of $180,000 for 2026.

This workstream is anticipated to run for two years or more, subject to scope refinement, budget availability, and delivery performance.

Selected references

[1] Ovezik, Christina, Dimitris Karakostas, and Aggelos Kiayias. ‘SoK: A stratified approach to blockchain decentralization.’ *International Conference on Financial Cryptography and Data Security*. Springer Nature Switzerland, 2024.

[2] Edinburgh Decentralization Index.