INTERSECT™

Research Working Group

Cardano Vision, Product Committee

Preface

The Research Working Group (RWG) was formed in October 2024 and currently has 4 members from Intersect MBO and Input Output Research (IOR).

The RWG has received one research proposal from IOR. This presentation provides a high level draft outline including IOR's track record, methodology and vision.

As part of an ongoing consultative process, the RWG invites feedback via its Discord channel on the Intersect server.

IO Research

> Currently IOR’s library contains over **200 peer reviewed and published papers**, involving over **150 academics from around the world**, which collectively have been **cited over 10,000 times**.

> Of these, around **50 papers** are central to the development of Cardano across its **5 eras**, providing the foundational research that has enabled Cardano to exist in the form it does today.

IOR Leadership

Aggelos Kiayias FRSE

Chief Scientist at Input Output, where Aggelos directs pioneering research efforts in blockchain and cryptography. He holds the Chair in Cyber Security and Privacy and serves as the Director of the Blockchain Technology Laboratory at the University of Edinburgh.

Kiayias has been instrumental in the development of Cardano's Ouroboros protocol, a cutting-edge proof-of-stake consensus algorithm, and is widely recognized for his contributions to the advancement of secure and scalable blockchain protocols.

He leads a network of research fellows specializing in areas including cryptography, distributed ledgers, algorithms, cybersecurity, formal methods, economics, and game theory.

Worldwide Academic Network

Two R&D teams; a research network with over 30 in-house and distributed research fellows, and innovation department of more than 35 architects and engineers that focus on rapid prototyping.

Blockchain Technology Laboratory (Edinburgh, Tokyo Tech, Wyoming) network who carry out industry-inspired open access research in blockchain technologies and decentralized systems in collaboration with industry and government partners.

IO Research Hubs (Edinburgh, Stanford) who tackle foundational questions in blockchain technologies, extensively increasing the blockchain industry's collation of scientific knowledge and research.

Embedded research partnerships integrate cutting-edge expertise across disciplines, facilitating cross-institutional research and innovation in blockchain science.

IOR Methodology

Fundamental Research
(Pre-seed / up to SRL 2)

IOR develops and formalizes ideas that go beyond the state of the art; finding the right requirements, identifying inherent tradeoffs/limitations, a meaningful mathematical model, well-defined design goals, a technical proposal/solution along with rigorous security proofs.

Rapid Innovation
(Seed / up to SRL4-6)

An interdisciplinary team that conducts lightweight validation of concepts; rigorous R&D to develop promising ideas, establish feasibility through prototypes, models and simulations, and write specifications that can be used to directly guide and validate full implementations.

Targeted Implementation
(Seed + / SRL 4-6 onwards)

IOR supports engineering teams implement solution in a target production environment, according to the specifications developed during the Innovation phase, ensuring an evidenced-based engineering approach with high assurance.

* **Software Readiness Levels (SRLs)** outline the lifecycle of a technology, from basic principles to commercial readiness.

Case Study: Ouroboros

Ouroboros serves as the foundation of the Cardano Ledger and achieves blockchain consensus via a longest chain proof of stake protocol which governs block production and validity.

First implemented in 2017 (Classic), subsequent implementations have enhanced and elevated the protocol. Praos is in production, Genesis in development, with Omega proposed below.

Classic
a significant achievement within proof of stake protocols, providing security assurances through longest-chain consensus, based on leader election via unbiased randomness generated on chain.

Praos
enhanced security and scalability by introducing private-leader selection and forward-secure, key-evolving signatures to protect against adaptive attacks and ensure block production.

Genesis
adding a strong chain selection rule, allowing parties to bootstrap from the origin/genesis block without trusted checkpoints under variable and dynamic participation levels.

Research x Innovation

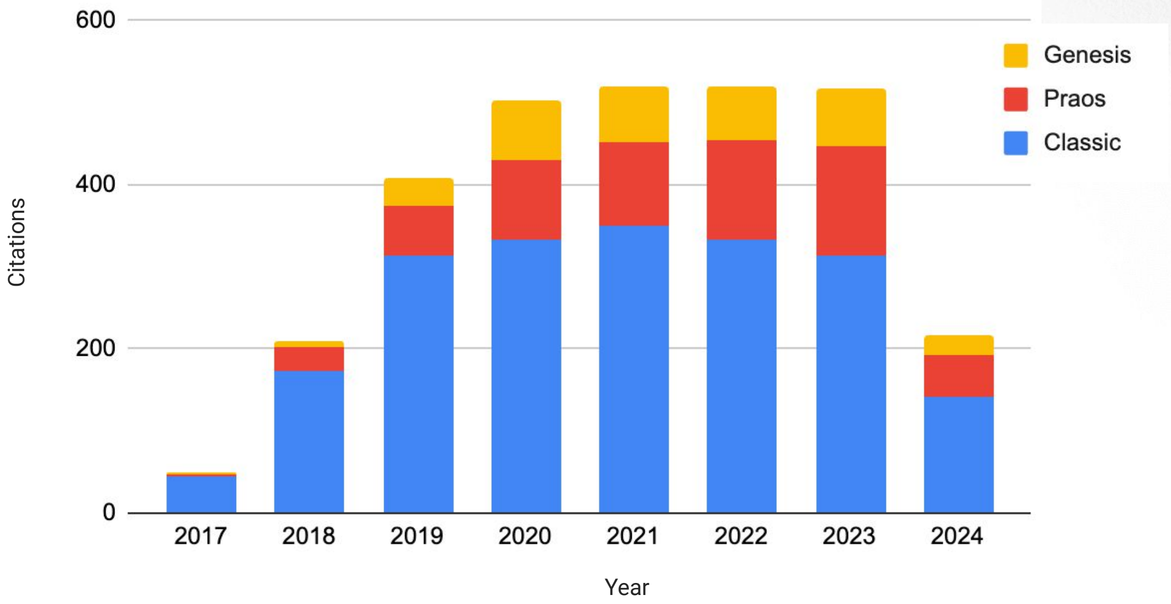
IOR is supporting several innovation work streams including two that significantly enhance fast settlement and high throughput performance of Ouroboros Praos.

Peras
focuses on optimizing blockchain sustainability by improving fast settlement times for Cardano, ensuring long-term viability and efficiency of the decentralized network.

Leios
enhances scalability by optimizing block propagation, increasing throughput and improving network efficiency while maintaining the high degree of security.

Case Study: Ouroboros

Ouroboros represents a significant innovation achievement in the development and execution of distributed ledger technologies, especially within proof of stake protocols.



Citations & Adoption

The Ouroboros protocol is designed for the Cardano blockchain and as an underlying consensus layer defines rules and parameters.

To highlight the impact of Ouroboros, its papers have been cited over 3,000 times, with the protocol being widely adopted by Cardano and other prominent blockchains such as Polkadot, Mina, and Horizen.

The Voltaire Era

Voltaire marks the completion of Cardano's era roadmap, establishing the technological foundation for the network to become a self-sustaining system.

By introducing a voting and treasury system, participants can utilize their stake and voting rights to influence the network's future and propose improvements to Cardano, building on its existing staking and delegation framework.

Papers

- A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence
- Updatable Blockchains
- SoK: Blockchain Governance
- Reward Schemes and Committee Sizes in Proof of Stake Governance
- On the Potential and Limitations of Proxy Voting: Delegation with Incomplete Votes.
- Decentralized Update Selection with Semi-strategic Experts

Specifications

- CIP-1694: An On-Chain Decentralized Governance Mechanism for Voltaire

Digital Nation States

We envision Cardano, along with the broader blockchain ecosystem, evolving into a decentralized compute and storage platform—a “world’s operating system”—where blockchain networks interoperate effortlessly, much like the seamless connectivity we experience in Web2.

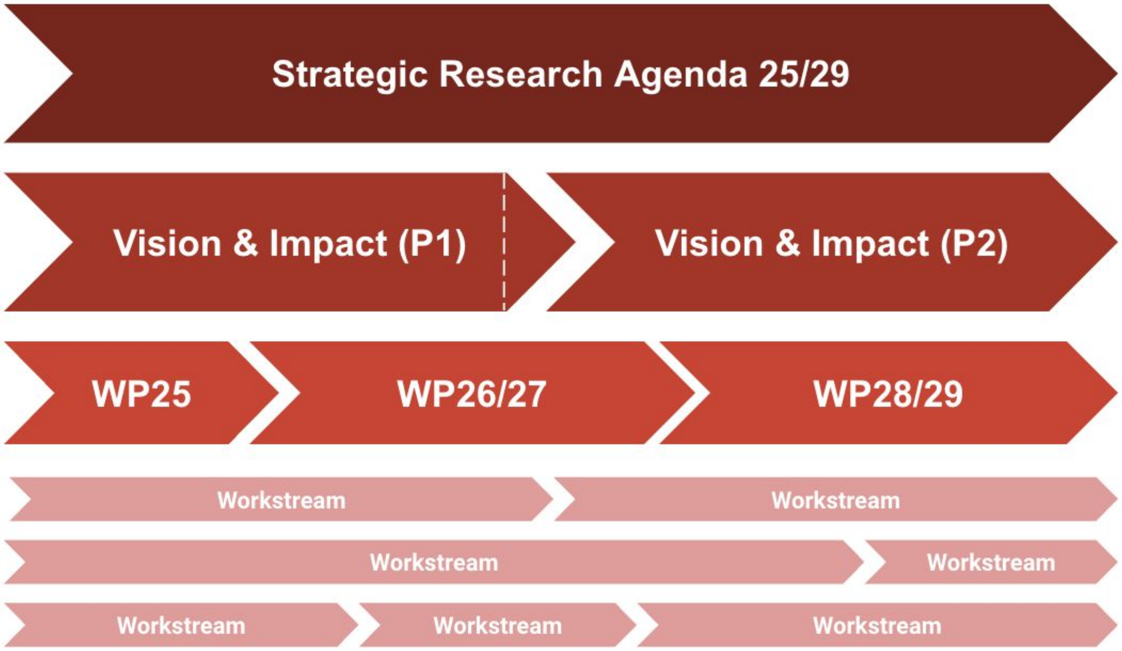
This vision supports the emergence of digital nation-states, where blockchains play a transformative role in defining identity, governance, and power structures. Our strategic research agenda lays out specific R&D pathways, detailing their purpose, the technical challenges involved, and the resulting enhancements they will bring to Cardano, positioning it to lead these advancements.

- **Interoperability.** Usability, performance, scalability, security and utility for developers and builders.
- **Identity, Governance and Democracy.** Extending smart contract systems with identity-related data.
- **Usability.** Developer productivity, operational efficiency and economic viability.
- **Utility.** Massive compute and data will be required to become the world’s OS.
- **Consensus.** The heart of any blockchain must evolve to support needs around security, performance and reliability.
- **Tokenomics.** As a decentralized system actors need the right economic incentives to participate or utilize the system.
- **Scalability.** Layer 2 protocols to match Web2 applications.
- **ZK-Proofs.** Standardizing a common technical core for all zero-knowledge instances.
- **Security.** The ongoing threats to security will rise dramatically in the quantum era.

2030 Outlook

A five year Strategic Research Agenda (SRA), structured into two 2.5-year Vision and Impact (V&I) phases, and organized into consecutive (bi)annual Work Programs (WP).

2030 Outlook for Cardano Vision



Strategic Research Agenda 25/29

Vision & Impact (P1)

Vision & Impact (P2)

WP25

WP26/27

WP28/29

Workstream

Workstream

Workstream

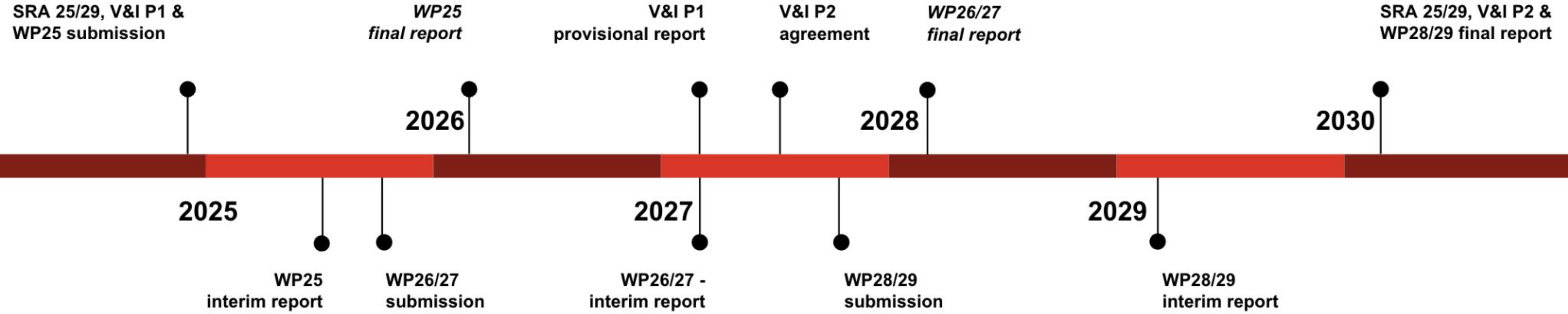
Workstream

Workstream

Workstream

Workstream

Delivery & Reporting



SRA 25/29, V&I P1 &
WP25 submission

2025

WP25
interim report

WP26/27
submission

WP25
final report

2026

V&I P1
provisional report

2027

WP26/27 -
interim report

V&I P2
agreement

WP28/29
submission

2028

WP26/27
final report

2029

WP28/29
interim report

2030

SRA 25/29, V&I P2 &
WP28/29 final report

Cardano Vision - 9 Thematic Focus Areas

An ambitious Strategic Research Agenda across nine thematic focus areas to deliver blockchain’s promise to the world:

1. The world’s operating system
2. Ouroboros Omega
3. Tokenomicon
4. Global Identity
5. Democracy 4.0
6. The internet Hydra-ted
7. Interchains
8. Core Zero-knowledge capabilities
9. The post-quantum landscape

Blockchain Tenets

A set of guiding principles that help blockchain communities evaluate and prioritize improvement proposals by aligning them with the fundamental rights and expectations of users

T
01

Your transaction cannot be slowed down or censored and will be expediently served for its purpose

System must scale - throughput, sharding, settlement and dynamically price, layer 2

T
02

The cost of a transaction should be predictable and cannot be unreasonable

System should facilitate an accessible predictable pricing

T
03

You will not be prevented from developing and deploying your application as you intended it

System offers DSLs, formal verification support, pub/sub location services, oracles, partnerchains

T
04

Your contributions to the system will be recognized, recorded and assessed fairly

Rewards sharing for SPOs, tokenomics, multi-resource consensus

T
05

The system will not lock the value that you store in it without your consent

Interoperability, partnerchains

T
06

The system will safely preserve the value and information that you decide to store in it

Integrity, post-quantum security, decentralization, storage, stablecoins, key management, ownership

Blockchain Tenets

T 07

The system will not unnecessarily spend resources

Proofs of useful work, efficient design, memory, storage

T 08

The system will treat users equally and will evolve according to their collective will aiming at its long term sustainability and viability

Fairness, neutrality, sustainability and governance, decentralized identity, multi-resource consensus, democracy 4.0

T 09

The system will preserve the privacy of the users' actions to the degree that is possible while facilitating the other tenets

Privacy preserving techniques for identity, secure MPC

T 10

The system will offer users ways to engage that do not require them to break local laws and regulations to the degree that is possible while facilitating the other tenets

Regulatory compliance, RVTP

T 11

The dynamics of the system shall be transparent, open, verifiable and interpretable to the degree that is possible while facilitating the other tenets

Transparency, democracy 4.0

Intersect Product Committee Goals

A set of goals that prioritizes key areas of focus, fosters stability for future governance, while advancing a product vision that guides and empowers the community.

G1 **Get more usage. Attract DApps, users and protocols.**

A. Reduce barriers and simplify processes

B. Improve speed of transactions & development

C. Effective & accessible funding mechanisms

D. Increase recognition & reputation

G2 **Open and reliable governance system**

G3 **Ensure Cardano remains trustworthy, reliable and competitive**

G4 **Create as a community the next path forward**

1. The world's operating system

Problem

To become a core layer of modern IT infrastructure, blockchain technology must enable applications to securely transfer value and support complex operations including decentralized finance. Achieving this requires platforms to offer smart contract programmability, ensuring secure, feature-rich environments for diverse applications.

Solution

Decentralized storage	Develop a system where smart contracts can access a wider array of data, including in Byzantine-resilient Distributed Hash Tables (DHT). Competitors such as Ethereum are also adopting this trend.	To keep up with the increasing demand and need for storage, smart contracts must be enhanced with an efficient and secure way to manage and share data in a decentralized way, achieving resilience by avoiding single points of failure. Enhances NFT storage capabilities and offers a persistence layer in pub/sub systems and other subsystems.
Pub/sub communications	Developing a Byzantine-resilient pub/sub (publish-subscribe) system that facilitates streamlined, secure information flow from publishers to subscribers	The increasing set of tasks by various actors (SPOs, DReps, DApps, storage nodes etc) mandate efficient and untamperable communication with stakeholders (including delegators). This highlights the need for an efficient automated mechanism for information exchange to enhance overall functionality and reliability that enables effective governance.

1. The world's operating system

Formal verification of smart contracts	Cardano is in a good position to aim for end-to-end smart contracts on Plutus based on a notion of state machines, which requires certified compilation, contract front ends and support for mechanized formal reasoning.	Smart contracts are high-assurance systems, evident from the extensive audits required (and the entire auditing industry that has emerged around Ethereum). Our advantage lies in leveraging the benefits of functional programming languages to offer the essential tools that uphold high standards, making Cardano the preferred choice for security-critical DApps.
State-machine contract environment	*Develop EasySM into an application programming framework in Agda or Haskell. Define formal semantics to facilitate mechanized reasoning*.	Simplify smart contract and DApp development for Cardano to increase developer adoption via a more accessible application development framework, enabling developers to create high-assurance contracts more quickly and efficiently. A distinctive advantage of Cardano should be that smart contracts can be developed more reliably within the same timeframe.
Location-based services and smart contracts	*Spearhead novel research through enforcing a stake distribution that is as diverse as possible. Extending a location verification mechanism to end users and DApps.*	The system currently does not use verifiable geographic location, which may pose challenges in the future. Incentivization mechanisms should guide Cardano towards geographic diversity. In addition, on the application layer smart contracts may need access to location data to provide location-specific services or comply with local laws

1. The world’s operating system

Intent-based ledgers and decision making	Allow users to declare and specify their intents, and allow competitive systems to fulfill and settle them on-chain.	Intent-based ledgers are gaining traction, and Cardano maintain its leadership by keeping pace with this trend. We have already taken initial steps with Babel fees and validation zones, which can be seen as first instances of intent-based functionality. It is advantageous to maintain this momentum, working towards enabling Cardano’s blockchain and smart services to respond to user intents, rather than solely fully-specified transactions.
Domain-specific languages (DSLs) for high-value applications	Building on Marlowe, research DSLs for other high-value applications including legal, asset tokenization, and supply chain management.	IO has a track record developing DSLs and providing them to the community. More domains are possible, such as governance (for example, with partners such as Argentina) or other emerging industrial needs (for which we would welcome Intersect product involvement).

Outlook

Strengthen Cardano’s capabilities to develop smart contracts efficiently and securely, while building infrastructure that enables more services on a comprehensive, feature-rich, and accessible operating system. This approach positions Cardano as a leader in decentralized finance and other specialized domains.

2. Ouroboros Omega

Problem

Enables energy-efficient proof-of-stake operation, allowing for a large number of participants to maintain the blockchain, similar to Nakamoto's longest chain protocol. As the Cardano ecosystem grows, improvements to Ouroboros are necessary to handle increased transaction throughput and processing demands.

Solution

Peras: Faster settlement	Further investigation to incorporate fast settlement to the Ouroboros family of protocols without compromising on the robustness properties they provide. This will enable more efficient bridging and support cross-domain applications.	Cardano offers a robust Nakamoto-style consensus, allowing individual clients to choose the number of confirmations required for their transactions. However, if a decision on what should be considered "sufficiently deep" on Cardano needs to be made on behalf of an entire ecosystem (such as Midnight or other partnerchains), it becomes essential to achieve the required security level more quickly.
Leios: Throughput to the physical limits	Further investigation to maximize throughput of the Ouroboros line of protocols to the physical limits of the underlying network and dealing with highly concurrent transaction processing.	Improving efficiency through increased throughput is not solely a task for layer 2 but also for layer 1. Utilizing the available block space and computational resources on layer 1 as efficiently as possible will keep us competitive with other blockchains, such as Ethereum, that aim to function as "settlement layers."

2. Ouroboros Omega

Fair transaction processing	Explore techniques that provide order-fairness and enable the ledger to serialize transactions in a consistent way when diffused in the network.	Maximal Extractable Value (MEV) has both benefits and drawbacks. While it encourages SPO adoption, it can have adverse effects on users, who may be treated unfairly due to the system's asymmetric roles. Additionally, MEV can disrupt the system's operation. This research aims to mitigate these adverse effects, providing users with reassurance against manipulation and aligning with ongoing developments across the industry.
Byzantine-resilient networking	First principles to improve the security of the Byzantine-resilient gossip layer while also optimizing its efficiency and inclusivity.	Blockchain systems are built on top of P2P networks, which must themselves be robust to deliver the guarantees required by the consensus algorithm, prevent congestion, and defend against network attacks that could hinder information diffusion. Further development is needed as Cardano currently lacks a strong network layer.
Multi-resource consensus - Minotaur	Using multi-resource consensus enables sidechains to base their security on a mix of ada and other tokens (or even proof of work).	Cardano initiated multi-resource consensus three years ago, a concept closely related to but distinct from re-staking, which focuses on sharing resources across chains. As independent systems become more interconnected, security concerns arise necessitating an algorithm that is flexible, adjustable and resilient under adverse conditions.

2. Ouroboros Omega

Proofs of useful work	Increasing security and providing an on ramp to the ecosystem via computational effort with Proof-of-Useful-Work (PoUW) schemes.	Blockchain service providers increasingly perform costly tasks, such as computing distributed zero-knowledge proofs or SNARKs. Similar computational demands and potential synergies exist in AI and machine learning. One opportunity is to leverage intensive tasks as proof-of-useful-work, repurposing necessary computations to support consensus simultaneously.
Congestion control	Investigate more deeply the provable guarantees of utility / cost minimization and the hybrid mechanisms offering a trade-off between fee adjustment and user inclusivity through tiered pricing.	While transaction fees are a central concern for users of the system's service platform, the platform must offer more diverse options to address network congestion. This built-in support will allow developers to build with greater confidence, reducing risks for DApp developers when launching new projects.
Cardano sharding	Investigate the full horizontal scaling of Cardano in the sense that more nodes joining the system imply less data to be stored and less work to be performed by every single node, thus allowing for better system performance	Sharding distributes tasks among nodes to manage load, offering a foundational approach to scalability as increasingly distinct roles emerge to support system operations. These include maintaining partner chains, bridges, governance, storage, and privacy. Functionality can expand only if we scale on multiple levels (layer 1 and layer 2) and recognize that different roles contribute unique resources toward varied goals.

Outlook

Accelerate the worldwide adoption of Ouroboros by Cardano and other blockchains.

3. Tokenomicon

Problem

Tokenization is a key blockchain innovation, allowing users to create tokens representing real-world value for seamless global transfers. Cardano leads with features like native user-defined assets and upcoming Babel fees for flexible transaction payments. However despite its importance, tokenomics remains under-researched in blockchain technology.

Solution

Tokenomics design	Investigate first principles to inform optimal long-term macroeconomic token policies. Produce mathematical models and identify key Cardano parameters that impact token price evolution, optimal parameter choices and system design including treasury policies.	Blockchain is developing into a broad and interconnected ecosystem. It's crucial to ensure strong support (staking) and decentralization, even as requirements shift and external price shocks occur that could destabilize the system. Poor decisions could easily lead to centralization effects, as seen in Ethereum.
Rewards sharing and transaction fees	Fair, predictable service fees and optimal reward-sharing mechanisms for providers. Inclusivity and decentralization, exploring diverse and alternative reward schemes and game theory models, such as those with low variance for small ada holders.	This approach empowers network growth and evolution (in both usage and service) by offering an appealing user experience with fair and predictable service fees, along with equitable reward sharing for service providers (SPOs, DReps, Project Catalyst, and Mithril certification). To remain competitive, it must surpass alternatives such as EIP-1559.

3. Tokenomicon

Tokenomics design	Perform first principles research in price stabilization mechanisms and stablecoin design to create a protocol stable to market forces and price fluctuations. Ensure that the stablecoin is highly liquid, manages risk, maintains its peg and is interoperable.	Djed is a working product but has design limitations. USDC is also coming to Cardano. This stream provides the opportunity for a community owned stablecoin, which is not proprietary, and combines game theory, economics, security and mechanism design - governed by the community.

Outlook

Different blockchains use diverse tokenomic and service fee models. Ethereum employs controlled inflation (via fee burning vs. block rewards) to manage demand, while Polkadot auctions validator security shares. Cardano's predictable ADA cost model supports transaction planning but places FX risk on users. To lead in tokenomics, Cardano must continually refine its platform for users and service providers (like SPOs and DReps), enhancing stability, fostering innovation, and supporting fair service pricing. This focus on tokenomics will strengthen Cardano's position, driving growth while maintaining decentralization.

4. Global Identity

Problem

Digital identity is central to every real-world application and has recently experienced a major paradigm shift, aiming to give users full control over their identifying information, including selective disclosure to protect privacy while complying with regulations. However, formal research on Self-Sovereign Identity (SSI) remains limited, especially in connecting legacy identity systems with new ones built on decentralized infrastructures like blockchains, while ensuring interoperability.

Solution

Decentralized identity and reputation management	Investigate approaches to augment Cardano's governance, consensus, and transaction systems with identity-related data. Formally define general and formal abstractions for self-sovereign identity solutions (e.g., Decentralized Identifiers and Verifiable Credentials), and identify trade-offs in various implementation methods.	Decentralized identity provides improved security, usability, and features such as decentralized reputation management. Built with a focus on standards and interoperability, it has the potential to redefine digital identity and enable seamless integration across transactional and smart contract systems.

Outlook

Key focus areas include embedding global identity within Cardano's core functionalities—such as transactions, smart contracts, and governance—and enhancing compatibility across its broader ecosystem. This research aims to establish robust decentralized identity frameworks as modern implementations of Public Key Infrastructures (PKIs), equipping Cardano with the theoretical and practical tools to integrate identity in a privacy-preserving, interoperable manner, ultimately supporting decentralized governance and community growth.

5. Democracy 4.0

Problem

Democracy has evolved from small-scale foraging communities (1.0) to technologically enhanced systems of modern nation-states (3.0). The rise of the internet, social media, and AI presents both challenges and opportunities for rethinking democratic processes, potentially ushering in a new era of technologies while preserving democratic principles (4.0).

Solution

Next-level governance protocols	Design layer 2 voting protocols that build on Cardano's ecosystem, offering high levels of vote confidentiality, user privacy, end-to-end verifiability of election results, and resilience to censorship, DoS, and coercion attacks.	Current public voting by representatives is a minimal viable product. Privacy features and the application of democratic rights through technology empower voters to exercise their rights efficiently. Achieving this requires a new set of governance protocols.
Governance incentives	By leveraging modern techniques from mechanism design and voting protocols in social choice theory, governance models can align participant goals, ensure positive contributions are rewarded, and prevent the concentration of power at a single point of failure.	Blockchain's frequent and automated voting requires active participation, rewarding users for ongoing support. Incentives are crucial for early detection of poor proposals and must encourage truthful voting, especially among DReps, ultimately enabling governance decisions based on individual votes rather than solely ADA-based weighting.

5. Democracy 4.0

Decision-making toolset	Explore methods to assess the impact of technical proposals across various dimensions, including decentralization, cost, token value, system utility, interoperability, regulatory alignment, and transaction throughput.	Governance on a technology platform like Cardano requires broad support to ensure security. Achieving this depends on tools that facilitate efficient decision-making and trustworthy proposal assessment. Clear criteria for evaluating proposals enable the community to vote responsibly, establishing Cardano as a stable voting platform competitive with industry peers like Tezos and Polkadot.

Outlook

Ensure the safe execution of voting rights, incentivize and enable exercising of voting rights. This approach to governance would provide greater accessibility and place Cardano ahead of Tezos, Polkadot and other chains.

6. The Internet Hydra-ted

Problem

To enhance Cardano's speed and performance to the level of Web2 applications, layer 2 solutions like Hydra enable off-chain transaction settlement, helping to scale, reduce load, and accelerate transactions. While the Hydra head protocol has been implemented, further research and development are required to complete the full Hydra protocol suite.

Solution

Hydra Tail	Design and analyze a zk-rollup protocol from first principles through a provable security perspective, including for UTxO-based scenarios, whilst balancing simplicity and mainchain footprint.	To lead industry advancements in zk-rollups, a new version of Hydra is needed that integrates SNARK technology, enabling anyone to transact off-chain and verifiably update ledger states. This novel layer 2 architecture enhances adoption through increased efficiency and capability.
Inter-Head / Tail	Design secure ways to compose Hydra instances, enhancing layer 2 flexibility with minimal layer 1 involvement. Build models and prove security within a composable security framework.	Layer 2 instances rely on layer 1 for security, limiting their interoperability. Isolated layer 2 instances hinder scalability and adoption and increase costs due to required communication with layer 1.

6. The Internet Hydra-ted

Optimization tools	Develop companion protocols for the Hydra Suite to address issues like funds rebalancing, message routing, head synchronization, and the best possible liveness guarantees.	As with other layer 2 instances, Hydra is bound to parameters that may require adjustments over time. Currently, such changes necessitate interaction with layer 1 (e.g., closing and reopening heads). These functionalities support a broader range of DApps.
Auditing tools	Develop protocols that would allow third parties, such as a regulator, to submit audit or compliance queries under certain conditions, while protecting participants' privacy.	As a technology provider Cardano has a responsibility to offer solutions that balance privacy with accountability. This approach builds trust, facilitates market access, and aligns with market trends.

Outlook

Hydra significantly enhances Cardano's scalability by enabling faster transaction processing with lower fees and reduced latency, making it ideal for high-throughput applications such as gaming and supply chains. Compared to blockchains like Ethereum and Bitcoin, the Hydra suite gives Cardano a competitive edge for enterprise applications.

T01 T02 T03 T04 T05 T06 T07 T08 T09 T10 T11

G1a G1b G1c G1d G2 G3 G4

7. Interchains

Problem

The growing need for interoperability across blockchain systems, including legacy platforms and real-world applications, is driving increased functionality while introducing new security challenges. Blockchain bridges, which are often targeted by attackers, are essential for secure integration and seamless communication between different networks.

Solution

State proofs and blockchain bridges	Construct and study secure bridges (trustless and committee-based) to enable the secure transfer of assets and information. Analyze different design approaches and underlying trust assumptions.	Currently, no fully secure bridging infrastructure exists, despite its critical importance for adoption and interoperability. This is essential to ensure Cardano maintains its leadership as the ecosystem becomes more interconnected.
Light client infrastructure	Explore trade offs in light client infrastructure for varying use cases (bandwidth / storage) relevant to DApp development and mobile wallets. Consider data retention, bandwidth and processing limitations.	Cardano needs light clients that can flexibly balance security with bandwidth and storage requirements across various settings (e.g., end users, bridges). Challenges include monitoring smart contract states and enabling participation with limited resources—complex issues that require effective solutions.

7. Interchains

Partnerchains: (i) Tokenomics (ii) Consensus	Explore fundamental principles of tokenomics to enable the launch of new side chains or partnerchains that leverage Cardano's security. Design and develop innovative approaches to consensus for proof-of-stake protocols.	This approach strengthens Cardano's layer 1 offerings and enhances opportunities for re-staking, ensuring security and resilience while remaining competitive with systems like Polkadot and Eigenlayer. It also supports monetary expansion, adoption, growth, and the success of partnerchains.
Privacy preserving and cross-chain DApps and oracles	Develop a privacy-preserving data processing framework and supporting toolset to enable efficient, private execution of DApp smart contracts.	Fully harness the potential of partnerchains and facilitate the seamless development of cross-chain DApps, allowing access to multiple states while preserving privacy. This ensures scalability, performance, and maximizes the benefits of cross-chain interoperability.

Outlook

Cardano can leverage its strong security track record to position itself as a leader, offering a more robust solution for cross-chain transactions compared to competitors like Ethereum, Polkadot, and Solana. As blockchain ecosystems evolve, Cardano's support for both layer 1 and layer 2 cross-chain DApps with enhanced privacy and scalability could make it a preferred choice for developers and enterprises seeking a secure and efficient multi-chain environment.

8. Core Zero-knowledge capabilities

Problem

Standardizing a technical core for all zero-knowledge instances in the Cardano ecosystem, including infrastructure like light clients, state proofs, and blockchain bridges, is crucial for ensuring long-term functionality and security. Given the rapid advancements in zero-knowledge protocol design, it's important that the tooling remains "pluggable" and updatable to seamlessly integrate future developments, maintaining the ecosystem's competitiveness and safety.

Solution

Core Zero-knowledge capabilities	Active engagement in standardization efforts, such as the Halo2 proving system. Enable ZK capabilities within Plutus smart contracts, and proving arbitrarily long computations through incrementally verifiable computation, achieved by recursive proofs and folding schemes. Ensure that the ZK proving systems under development are also extendable and configurable.	Cardano’s zero-knowledge tooling must remain “pluggable” and easily updatable to integrate the latest advancements in ZK research seamlessly and securely. Ensuring Cardano’s long-term viability requires a commitment to adaptable and sustainable cryptographic algorithms, especially as zero-knowledge protocols continue to evolve rapidly, necessitating updates to newer, more secure protocols.

Outlook

This adaptability secures Cardano’s cryptographic foundation and strengthens its long-term resilience within the blockchain ecosystem. By prioritizing pluggable ZK tooling, Cardano positions itself as a leader in privacy-preserving and secure transactions, aligning with future advancements and supporting sustainable growth and innovation throughout the ecosystem.

9. The post-quantum landscape

Problem

Recent advancements in quantum computing underscore the need for blockchain systems to be resilient against future quantum-based attacks to ensure long-term sustainability. Beyond defense, quantum technology also has the potential to enhance blockchain security and performance, introducing techniques that could transform its capabilities.

Solution

Post-quantum readiness	Investigate the design and integration of post-quantum secure cryptographic primitives. While some primitives have well-understood post-quantum alternatives, others—such as VRFs and threshold signatures—require novel research and design to balance security and efficiency effectively. This includes analyzing overarching protocols in the context of quantum threats.	Quantum readiness is increasingly critical and will impact the system at multiple levels. Although the quantum threat may not be imminent within the next few years, it is essential to prepare for a smooth transition to post-quantum security when necessary. This preparation involves not only replacing signature schemes and verifiable random functions but also implementing a secure update mechanism that is itself quantum-resistant.

9. The post-quantum landscape

Post-quantum enhancements	Leveraging primitives like one-shot signatures can address fundamental security challenges in proof-of-stake blockchain security, offering significant performance improvements for blockchain functions.	Quantum technology presents promising security opportunities, particularly through the no-cloning theorem, enabling unprecedented protection with quantum devices. This could provide Cardano a long-term edge as the technology matures. Early collaboration with companies and universities will prevent a cold start when adopting quantum advancements. Strong community interest, notably from ecosystems like Ethereum, has already spurred early collaborations.

Outlook

The post-quantum landscape is evolving rapidly, making readiness essential for maintaining secure and resilient blockchain systems in the coming years. As quantum computing advances, traditional cryptographic methods face growing vulnerabilities. Preparing for this shift involves integrating quantum-resistant algorithms, such as one-shot signatures and quantum key distribution, to ensure forward security and mitigate risks from quantum-enabled attacks. These enhancements, aimed at reducing computational demands and bolstering scalability, will fortify Cardano’s infrastructure with adaptable, future-proof cryptographic solutions.

Ethics

Ethics and research integrity are prerequisites for research excellence, ensuring that all academic activities are conducted with honesty, transparency, and respect for societal impact.

- Commitment to integrity and transparency
- Respect for privacy and data security
- Ethical use of technology
- Collaboration and inclusivity
- Accountability and continuous improvement

Upholding these values is essential for fostering trust, advancing knowledge and delivering innovations that benefit Cardano’s global community.

INTERSECT™

Research Working Group

Cardano Vision, Product Committee