2025 Vision & Roadmap

Vision

Cardano envisions a future where it serves as the robust and scalable foundation for a decentralized global economy. This will be achieved by significantly enhancing L1 performance through the Leios protocol and optimizing the current codebase, while simultaneously expanding the capabilities of L2 solutions like Hydra and Midgard. By improving developer experience through enhanced APIs, robust tooling, and a focus on decentralization, Cardano aims to empower developers to build innovative and impactful applications. Furthermore, the expansion of programmable assets, including advanced features like account abstraction and custodian regulated stablecoins, will unlock new possibilities for decentralized finance and beyond. This vision emphasizes a strong commitment to research, community collaboration, and the long-term sustainability of the Cardano ecosystem.

A thriving ecosystem is essential for realizing this vision. This requires a multi-faceted approach that fosters innovation, attracts new users and developers, and drives real-world adoption. A key component of this strategy is the cultivation of strategic partnerships with organizations across various sectors, focusing on developing and deploying Cardano-based solutions that address specific industry needs. We will prioritize collaborations that align with Cardano's core principles of security, scalability, and decentralization.

Beyond strategic partnerships, fostering a vibrant and engaged community is paramount. We will invest in initiatives that empower developers to build innovative dApps and tools on Cardano. This includes establishing incubator and accelerator programs, organizing regular hackathons and offering developer grants, and expanding an ecosystem fund to support promising projects. Furthermore, we will prioritize improving the developer experience through enhanced APIs, robust tooling, and comprehensive documentation, making it easier for developers to get started with Cardano and build impactful applications.

Finally, building a strong and supportive community is crucial for long-term success. We will focus on initiatives that nurture and engage the Cardano community, such as meetups, online forums, and ambassador programs. By combining strategic partnerships, developer support, and community engagement, we are confident in our ability to create a thriving ecosystem that drives the adoption of Cardano and realizes its full potential.

The general themes of the community's short-term vision, as analyzed through the community roadmap survey, focus on increasing scalability, interoperability, and usability.

Roadmap

The 2025 roadmap comprises a number of items that have been proposed by community members, as described below. It is expected that progress will be made on most or all of this roadmap. Importantly, the scope of the roadmap is not fixed, but is open to new community contributions.

Scaling the L1 Engine

L1 performance is crucial for widespread adoption and enabling Cardano to become a central hub for blockchain communication. This will be achieved through a combination of codebase optimization and architectural enhancements to increase parallelization.

Architectural Excellence

Cardano is committed to maintaining its position at the forefront of blockchain technology. This includes a continuous evaluation of software architecture best practices. We recognize the evolving landscape of architectural patterns and are dedicated to exploring and implementing the most suitable approaches for Cardano's unique needs including operating the world’s most reliable and globally decentralised blockchain.

- **Modular Design:** We will prioritize a modular design approach for Cardano's codebase, enabling independent development and deployment of components while maintaining a cohesive and efficient system that meets the timing, security and reliability requirements that are fundamental to Cardano. This allows for flexibility and adaptability as the platform evolves.

- **Performance Optimization:** We will continuously analyze and optimize the performance of Cardano's architecture, exploring and evaluating different architectural patterns to ensure maximum efficiency and scalability focusing on the worst-case behaviours that govern overall system behaviour, rather than deceptive average-case behaviours. This includes investigating and benchmarking promising alternatives to established patterns to determine the most suitable approach for various Cardano components.

- **Formal Methods and Verification:** Security and reliability are paramount for blockchain systems. We will leverage formal methods and verification techniques to rigorously specify and analyze critical components of Cardano's architecture including timeliness and worst-case behaviours. This will enable us to mathematically prove the correctness of these components and minimize the risk of vulnerabilities. We will continue to invest in research and development in formal methods to enhance their applicability and effectiveness in the context of Cardano.

- **Research and Exploration:** We will dedicate resources to research and explore cutting-edge architectural patterns and technologies, ensuring that Cardano remains at the forefront of technical excellence and can adapt to the ever-changing blockchain landscape. This will involve close monitoring of industry trends and collaboration with experts in software architecture especially for complex real-time distributed systems.

Leios

Leios is a groundbreaking innovation designed to significantly enhance Cardano's scalability and transaction throughput. It introduces a novel approach to block creation, moving away from the traditional sequential model.

- Leios leverages a parallel block creation process. Instead of a single linear chain of blocks, it introduces multiple "input blocks" that are independently created and endorsed by Stake Pool Operators (SPOs). These endorsements are then aggregated into "endorsement blocks," and finally, a "ranking block" determines the final order and validity of transactions across all input blocks.
- This parallel approach has the potential to dramatically increase transaction throughput while maintaining the security and decentralization of the Cardano blockchain.

The roadmap for 2025 includes several key steps to achieve in preparation for the development and implementation of Leios:

- Develop formal specifications to guide node implementations and ensure correctness.
- Conduct extensive simulations to validate the theoretical design of Leios in real-world network conditions and identify optimal parameters.
- Refactor the Cardano node to facilitate the integration of Leios and ensure smooth and efficient operation.

Optimizations

- Optimize the current codebase and address technical debt to improve performance. This will enable more flexible parameter adjustments by the parameter committee, allowing for increased scalability without requiring a hard fork.

- Enhance Mithril's decentralization by integrating it more closely with the node and utilizing existing networking layers.

Anti-grinding

- Introduce measures to mitigate CPU-based grinding attacks, improving settlement speed and network security.

LSM Integration

- Reduce memory requirements for nodes by integrating Log-Structured Merge (LSM) trees, initially focusing on the UTxO set.

Incoming Liquidity

Increasing liquidity from other ecosystems is vital for expanding Cardano's user base.

- Utilize zero-knowledge proofs to enable Cardano to serve as a decentralized DeFi layer for Bitcoin.
- Babel Fees (Nested Transactions) facilitate transactions on the L1 for users without initial ADA holdings through a decentralized marketplace that allows partial transactions to be accepted and combined from multiple parties, where a marketplace can arbitrage the value in ADA for a user to get ADA to spend the transaction and have the minimum ADA required without having to purchase ADA first through an exchange.

L2 Expansion

To accommodate increasing transaction volume, Cardano will focus on expanding the capabilities of L2 solutions.

Actively Validated Services (AVS) Layer for Partner Chains

This framework outlines a method for creating independent, customizable blockchain networks (partner chains) leveraging a robust and secure underlying value *validation* layer. This approach allows for greater flexibility and experimentation while benefiting from the security and reliability of the Ouroboros Proof Of Stake consensus mechanism on Cardano. This framework is designed to facilitate seamless value transfer between partner chains, forming the basis of a decentralized open standard.

Key benefits include customizable partner chain parameters, prototyping of new features without impacting AVS stability, inheritance of AVS security, and increased partner chain scalability. The technical approach involves extending existing consensus mechanisms to operate in multiple modes, such as adding a FastBFT mode. This includes creating a slimmed-down version of core blockchain components and developing standardized messaging and transaction formats for inter-chain communication.

Use cases include customized partner chains for dApps, testing new technologies on partner chains, and private partner chains for consortiums.

Future development will focus on integrating multiple consensus sources, enabling seamless cross-chain communication, defining a clear protocol for inter-chain transactions, developing a standardized interface for AVS interaction, and establishing community governance.

Hydra

Explore new use cases for Hydra, such as governance tools, and continue to enhance its scalability and performance.

- Build upon the success of Hydra Doom by identifying and developing further use cases that can leverage Hydra's scalability to benefit the Cardano ecosystem.
- Explore the use of Hydra as a platform for decentralized governance discussions and voting, addressing the challenges of managing large volumes of information on the L1.

Midgard

Midgard is Cardano’s first optimistic rollup framework, leveraging the EUTxO model to achieve permissionless operation, efficient fraud proofs, and censorship resistance, without relying on centralized sequencers or custodial multisigs. This unique design enables high-throughput, low-fee transactions while maintaining Cardano's robust security and decentralization. By aggregating off-chain transactions into compact representations on-chain, Midgard ensures that increased activity directly benefits Cardano’s L1, enabling a sustainable and innovative ecosystem for decentralized applications.

Finality (Peras)

Peras is an enhancement to the Ouroboros Praos protocol that aims to accelerate transaction settlement times. In the current Praos protocol, new blocks are added

probabilistically, and the longest chain of blocks is generally considered the valid one. Peras introduces a novel approach by incorporating a voting mechanism among Stake Pool Operators (SPOs).

SPOs can vote to endorse specific blocks, effectively increasing their weight within the chain. This "voting" mechanism allows for a faster consensus on the most valid chain, leading to quicker transaction finality. Faster transaction finality can significantly improve the user experience and enable more efficient and timely transactions.

Developer/User Experience

Improving developer and user experience is crucial for driving broader adoption.

- Generate libraries in various languages to simplify blockchain interaction for developers.
- Expand RPC capabilities to support queries and transaction building, enabling seamless integration with node services.
- Empower developers to create custom chain indexers for specific needs, such as supporting partner chains. Creating a translation layer of blocks and ledger events to a Nats Core pub/sub messaging system can be used as an example indexer framework.
- Decentralize data API services to reduce reliance on centralized providers and empower SPOs.
- Promote the use of local nodes and develop standards for wallet interaction with full nodes.
- Establish a unified standard for tracing, logging, and monitoring across different node implementations.

Programmable Assets

Expanding the capabilities of programmable assets will unlock new possibilities for decentralized applications.

Enhancing Cardano's programmable asset capabilities is crucial for unlocking the full potential of dApps. They expand on-chain asset functionality beyond simple transfers, enabling complex, programmable logic. These advancements will empower developers to build innovative dApps, exploring use cases like soul-bound tokens, or tokens that can never be transacted to another wallet, for decentralized identity, mechanisms for custodian regulated stablecoins, and royalty mechanisms to support creators.

- Develop frameworks that enable a new class of programmable assets beyond native tokens.
- UTxO intent signatures enhance decentralized exchange interactions by allowing users to signify their intent to spend UTxOs under specific conditions, facilitating swaps while maintaining user ownership of their funds.
- Explore the use of soul-bound tokens for decentralized identity and other applications.
- Implement royalty mechanisms to support creators and incentivize innovation.
- Enable the issuance of custodian regulated stablecoins on Cardano through policy-based mechanisms, such as USDC/USDT.

Multiple Node Implementations

The development and maintenance of multiple node implementations are absolutely crucial for Cardano's resilience and censorship resistance; however only if they adhere to a properly implemented and secure specification. This diversity strengthens security through a form of distributed peer review, as different teams scrutinize each codebase, increasing the likelihood of identifying and addressing potential flaws before they can be exploited. Furthermore, diverse implementations decentralize the development process itself, reducing the risk associated with relying on a single entity. This distributed development model fosters a more robust and adaptable ecosystem, as different teams bring unique perspectives and approaches to the ongoing evolution of the Cardano network Ultimately, the more high-quality, independent node implementations we have, the stronger, censorship resistant and more decentralized Cardano becomes, ensuring its long-term viability and success.

Ensuring node conformity in Cardano relies heavily on rigorous formal specifications. These specifications serve as the definitive guide for node implementation, detailing the precise behavior and functionality expected of every compliant node. They enable property tests to be automatically extracted, enabling node implementations to demonstrate full conformance to the specifications. By adhering to these meticulously crafted specifications, node developers can create implementations that are interoperable and compatible with the broader Cardano network. By providing concrete, actionable instructions and guidelines for building and configuring nodes, ensuring consistency and adherence to the established standards. This combination of precise specifications is essential for maintaining the integrity and stability of the Cardano network, guaranteeing that all participating nodes operate according to the agreed-upon rules and protocols.

SPO Incentive Improvements

The community has identified incentives can be improved for stake pool operators. This is a few suggestions of what can be assessed.

- Introduce min-margin parameter that can be voted on via governance to modify
- Modify pledge-benefit curve for a0

Note: This vision and roadmap represents a high-level overview and will be further refined and iterated upon based on ongoing research, community feedback, and technological advancements. It is based on the results of the TSC survey. The initial author of this roadmap is Sam Leathers, Chair for the Intersect Product Committee.