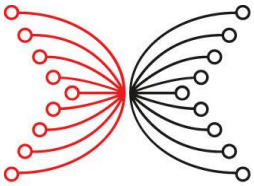
The Cardano Roadmap

Input | Output's perspective on the Cardano roadmap



INPUT | OUTPUT

Table of contents

Delivering across the eras

Cardano aimed to do for economic, political, and social systems what Bitcoin did for finance – providing a foundation for creating alternative structures that are decentralized and transparent. The project was motivated by a vision of empowering individuals and communities, challenging centralized structures, and giving participants true ownership and autonomy within the system.

Cardano was built to embrace formal methods and a peer-reviewed academic approach, aiming for a platform with high security, reliability, and scalability. Cardano celebrates the accomplishments of the prior development phases: Byron (foundation), Shelley (decentralization), Goguen (smart contracts), Basho (scaling), and the most recent phase – Voltaire (governance).

The age of Voltaire brings a number of opportunities to expand on the prior development themes while building on that solid foundation for a new generation of capabilities. This document captures the view of Input | Output (IO) on where Cardano should focus to build on its technology leadership and to capture a wider audience with new use cases to drive the impact originally envisioned. This document encapsulates a presentation by Charles Hoskinson: ‘After Voltaire, The Next Evolution of Cardano’. It represents IO’s view on the future of Cardano and is offered as input to the community process to establish a solid roadmap.

From eras to aeons

The world needs a digital revolution, akin to the revolutions that deposed kings and put the broad populace as the rulers, but for the digital realm and deposing the technology kings that rule in this era. Blockchain technology offers a shift from ‘don't be evil’ to ‘can't be evil’, fostering trust through transparent infrastructures that can restore faith in institutions.

This revolution must attract users from established platforms. To achieve this, it's essential to create legacy-friendly systems that can accommodate billions of existing users. To get to this next era, Cardano’s capabilities in key areas such as privacy, identity, and automated regulation must be extended.

To ensure the community continues to be principle-driven, there must be guiding principles for Cardano. These fundamental rights – essential for maintaining integrity within decentralized systems – for Cardano’s users are proposed within a set of tenets (shared principles). Cardano’s roadmap is inspired by these tenets outlined in the earlier blog post (and discussed in a recent X Space). Ultimately, it will be driven by the tenets outlined in the Cardano constitution as ratified by community vote on-chain.

From Byron to Voltaire, Cardano’s development phases have delivered foundational elements for a blockchain platform and driven it to success as one of the major networks.

Now, the focus for Cardano shifts to three main areas to drive innovation:

1. Scalability
2. Usability and utility
3. Interoperability and extensibility.

These areas are focused on ensuring Cardano's infrastructure will support artificial intelligence (AI) and exponential technologies, adapting to a world increasingly influenced by AI mistrust of institutions and political decentralization.

Maintaining momentum as a community is vital. Much of what must be achieved is in progress today and are continuity items that keep Cardano moving forward. However, some areas are more forward-looking and require research on how to best achieve them.

Scalability

Cardano aims to support billions of users by 2030, addressing limitations in affordability and ease of access. This will achieve massive scalability while maintaining decentralization, affordability, and security. The network will incorporate advanced scaling solutions that enable high transaction volumes and maintain security. Cardano developers will achieve near-term scaling goals through complementary approaches:

- Layer 2 Hydra state channels
- Layer 2 rollups (ZK and optimistic)
- Ouroboros Leios and Peras
- Mithril certificates
- Data API services
- Local node services and Daedalus
- Catalyst voting platform
- Core node improvements.

Many blockchains are striving to incorporate essential features for scale but often through centralization, which simplifies processes and reduces costs. The principle of decentralization is a word that everyone uses, but this is a core principle of Cardano which is the first project to measure this with the Edinburgh Decentralisation Index (EDI). Historical failures such as Mt.
Gox, Luna, BitConnect, and FTX highlight the risks associated with centralized structures in the cryptocurrency field.

These technologies collectively represent a multi-layered approach to scalability, allowing Cardano to support both high-throughput applications like gaming and micropayments and large-scale infrastructure DePIN projects like mobile networks on a global level. The focus on decentralization, even in scalability, aims to protect the network's integrity and keep it accessible to a wide user base.

Layer 2 Hydra state channels

Hydra is an off-chain scalability solution for Cardano, designed to handle high transaction volumes by using state channels. In a recent demonstration, the Hydra protocol ran the video game *Doom* on Hydra channels, achieving up to 90 million transactions in a day, far beyond what most blockchains can handle.

Hydra allows many transactions to be processed off-chain and then brings them back on-chain as necessary. Each 'Hydra head' can run parallel to the main chain, effectively multiplying the network's throughput. This is especially useful for applications like gaming or high-frequency transactions, where high speed and low latency are essential. Hydra carries the same safety guarantees as the mainnet as it requires all participants to agree to close out the head.

Projects such as Gummiworm are showing how Hydra can bridge the gap between the security guarantees of on-chain transactions and the speed and cost of centralized exchanges. Hydra will incorporate the thinking behind Gummiworm and projects like Hydrozoa to unlock this sweet spot for DeFi on Cardano. In the near future, innovations are coming to Hydra to increase its utility, including community projects such as the proposal to connect Hydra heads to other layer 2s.

Following the successful delivery of Hydra heads, IO will follow the originally envisioned roadmap. The Hydra scalability architecture can be divided into four components: the head protocol, the tail protocol, the cross-head-and-tail communication protocol, and a set of supporting protocols for routing, reconfiguration, and virtualization. The centerpiece is the 'head' protocol, which enables a set of high-performance and high-availability participants (such as stake pools) to very quickly process large numbers of transactions with minimal storage requirements by way of a multiparty state channel – a concept that generalizes two-party payment channels as implemented in the context of the Lightning network. Some work remains on heads to enable it to handle a larger set of users and security over funds:

- Disaster recovery (ensure funds are recoverable)
- Incremental commits (adding funds to a running head)
- Partial fanout (ability to bring portions of the final state to mainnet).

It is complemented by the 'tail' protocol, which enables those high-performance participants to provide scalability for large numbers of end-users who may use the system from low-power devices, such as mobile phones, and who may be offline for extended periods of time. While heads and tails can already communicate via the Cardano main chain, the cross-head-and-tail communication protocol provides an efficient off-chain variant of this functionality. All this is tied together by routing and configuration management, while virtualization facilitates faster communication, generalizing head and tail communication. Tails remain a roadmap feature.

Layer 2 rollups (ZK and optimistic)

The industry has settled on two distinct approaches to rollups: optimistic and zero-knowledge (ZK) proofs. Cardano is pursuing both approaches to rollup scalability. Cardano plans to support rollups that can batch large numbers of transactions, including cross-chain transactions and micropayments. Rollups aggregate multiple transactions into a netted transaction that can be validated by the network, reducing computational load while maintaining security. This allows for considerable scale without burdening the main network, as participants process transactions off the mainnet and utilize the network for settlement. This aligns with the original CSL vision for Cardano. Cardano's recent introduction of cryptographic primitives in PlutusV3 unlocks these possibilities.

With optimistic rollups, the layer 2 network submits a summary of transactions (the rollup). No proof is provided for the validity of these transactions. Instead, users are able to challenge the validity of the summary through an on-chain challenge process. This means users are unable to

withdraw their funds during the challenge period. The community is pursuing optimistic rollups for Cardano with the Midgard project.

With ZK proof-based rollups, the rollup is final and contains a zero-knowledge proof of the validity of the transactions. The proof is validated as a part of the consensus process. This allows for the instant withdrawal of funds from the layer 2 bridge. PlutusV3 introduced new cryptographic primitives such as BLS which enable it to support ZK proof based rollups. There is already success in rollup-based layer 2 networks such as zkFold, which will leverage the new Plutus primitives and unlock layer 2 scaling with fast withdrawals.

Ouroboros Leios and Peras protocols

All blockchains battle the 'trilemma' in the trade-offs between decentralization, security, and scalability. Users expect secure decentralized systems but also demand fast finality and throughput from the blockchain.

The next generation of consensus protocols that will address these needs is Leios. It delivers a high-speed consensus protocol that represents a significant upgrade over previous Ouroboros versions. This innovation aims to make Cardano one of the fastest blockchain systems, increasing throughput without sacrificing security. Leios enables parallel block creation by allowing multiple execution threads to process transactions simultaneously, achieving speeds that approach theoretical maximums ('one minus delta'). Cardano's goals for 2025 include:

- AGDA formal and executable specification
- Multi-node simulations
- Analysis and visualization tools to quantify behavior and performance
- Conformance tests
- SRL-6 prototype release.

Finality times in particular are a barrier to greater adoption. While Leios will address much of this challenge, it will be a major engineering undertaking. In the interim period, Cardano needs to move to a much faster finality period. The current 12-hour period for finality is holding back not only faster on-chain settlement but also the ability to integrate with other chains. Ouroboros Peras is the solution to this near-term dilemma.

Peras is the protocol designed to fill this need and to achieve it quickly. Peras is already at an evolved stage with a proof-of-concept implementation along with an underlying research paper and a formal methods implementation with an AGDA-literate CIP. 2025 is about taking this to the final step of engineering and mainnet deployment. The impact of Peras is a fast win taking finality time from 12 hours to 2 minutes in most cases.

Mithril certificates

Mithril is named after the precious metal in J.R.R. Tolkien's Middle-Earth – lightweight and

amazingly strong. Cardano's Mithril is a unique technology in the blockchain field allowing nodes to quickly bootstrap or obtain data from central parties but with the ability to verify its authenticity. It has the ability to empower off-chain users, or even other chains, to efficiently obtain subsets of data that are trustless but don't require visibility into the node itself for this assurance. The initial use case for Mithril is fast bootstrapping of a node but many other use cases have been conceived. For example, Mithril can provide secure and efficient access for light clients such as light wallets and mobile apps, and support for enhanced layer 2 protocols such as Hydra, partner chains, and bridges. The work on Mithril's signature scheme and network layer will also enable Cardano scaling protocols such as Peras and Leios.

For 2025 the Mithril team has put forward the following objectives:

- Decentralized signature diffusion
- Decentralized signer registration
- An incentive model.

Future work includes ZK recursive certificates linking certificates. The current signatures are not suitable for ZK proof, but the signatures for ALBA will be. However, ALBA is still at the research stage and the primitives will need to be implemented into the crypto core library. With community consent, at the current cadence, Mithril v1 can be live on mainnet in Q1 of 2026.

Data API services

Applications that interact with a blockchain often must obtain information from the ledger to build transactions or present information to users. Additionally, to put a transaction into the mempool of the network for execution, users must have access to a node connected to the mainnet peers. To achieve this, users must either operate a full node and an indexing server such as DB Sync or rely on server infrastructure operated by external entities that provide this service.

API providers such as Blockfrost offer easy access to blockchain networks, allowing developers to interact with the network without needing to run a full node themselves. They provide functionalities such as:

- HTTP-based data retrieval (eg, account balances, transaction histories)
- Transaction submission (sending transactions to the network).

However, reliance on these types of operators violates the decentralization principles of blockchains. The operators are able to act as gatekeepers to the network, are subject to surveillance or censorship or may be a single point of failure. In the Ethereum network, it is estimated that Infura can account for over 50% of all transactions. In the Cardano ecosystem, the primary gateway is Blockfrost who have noted they often submit over 50% of all transactions within an epoch.

The Blockfrost team is working to remedy this through a phased decentralization of their

services. In the end, state data providers will be stake pool operators (SPOs). SPOs will be able to service a request by a user for data and be compensated for that service with ada. This helps the SPOs gain additional revenue. More importantly, it ensures Cardano remains the most decentralized blockchain network. The vision includes not only operators but individuals whose desktop clients can provide the same services furthering the decentralization of this layer.

Local node services and Daedalus

The Daedalus wallet was the original Cardano wallet launched on mainnet in 2017. It is a full node wallet enabling a user to have a fully trustless interaction with Cardano as the wallet acts as a peer on the network. This allows the wallet to obtain information from their local server directly and not rely on a third party such as Blockfrost. It also allows them to propagate their transactions directly in the mempool across the network as their wallet connects to network peers.

Daedalus is now seven years old. It was built on an old framework and needs to be retired. However, IO wants to ensure we maintain the ability for a user to operate in a completely trustless way locally. To achieve this, IO is building a local desktop node that will operate as a full node connecting to peers on mainnet. It will also provide a local indexing service that provides only the relevant data for the user, ensuring the memory and storage requirements are kept to a minimum.

With this local node running as a service, users can connect any wallet directly to the node. This expands the possible number of wallets, as any existing wallet that leverages the Blockfrost APIs will be able to connect by simply changing the connection parameters.

The development of the local node is achieved by building on the same effort as the decentralization work being led by Blockfrost. The local node will be able not only to provide data locally, but to potentially act as a data provider to the network and optionally a full node. The Blockfrost services will run locally ensuring there are no external dependencies.

Following the release of the desktop node service, the Daedalus wallet will be deprecated. The IO team will ensure Lace is ready to support the local node during this deprecation period.

Catalyst voting platform

The Catalyst fund is an on-chain fund that helps bootstrap the development of new projects (including decentralized applications (DApps) and other technical solutions) for Cardano. It has one of the most successful track records in the blockchain industry with 3 million votes cast by Cardano Catalyst community members to allocate 223m ada in grants and rewards allocated to over 2,000 projects by EOY 2024. Over 1,000 projects have already been completed, establishing a cornerstone in the Cardano ecosystem and a leader in decentralized ecosystem

funding allocation across the blockchain industry.

To facilitate this, Catalyst must have a set of tools for managing proposals, privacy-preserving voting, milestone tracking and the management of the funds. Currently, Catalyst achieves this with a set of Web2 tools such as IdeaScale for proposal management, a small network of deprecated Jormungandr servers, proprietary iOS and Android voting applications, and a milestone administration interface for a community-driven process that verifies grantee deliverables are achieved, and an industry-leading compliance process for the distribution of funds.

Catalyst put forward a proposal in 2023 to solve known issues with a decentralized solution for the proposals, voting, and management activities. These are codenamed projects Hermes and Voices. Hermes is intended to replace the current sidechain environment and demonstrate decentralizing the end-to-end backend processes. The upgraded Catalyst UX, currently termed 'Voices' will replace IdeaScale, the SaaS commercial application that is used to manage proposals, and features will enable liquid democracy within Catalyst voting, akin to the original treasury paper.

These tools not only facilitate a decentralized voting platform for Catalyst, but represent a novel approach to decentralized applications that do not require a blockchain except for posting the final rollups, such as tallied votes. This project was funded by the Catalyst community and plans to deliver in 2025, demonstrating part of the new UX in the next fund slated for Q1, alongside commercial experiments For 2025, Catalyst objectives are to:

- Launch Fund14-ready IdeaScale replacement
- Manage three Funding rounds
- Upgrade auditability, payments, and billing automation tooling
- Develop a native mobile app for community participation.

Core node improvements

A number of improvements have been proposed for the core node with the aim of ensuring it remains the most stable blockchain platform in the market and drives down the operating cost. The initiatives include:

- LSM
- Revised stake pool incentive scheme
- Anti-grinding measures
- Tiered pricing.

LSM

LSM is a memory management module that helps address a problem where SPO node

memory use exceeds available resources or increases SPO and other operator costs to unacceptable levels. LSM will move the UTXO set and other data structures on disk to reduce the memory required to run a node. When implemented, it will enable Cardano to reach the Bitcoin scale in terms of the number of users and wallets and the size of the UTXO set. At the same time, SPO nodes and full node wallets will be able to function on commodity hardware, including cheap cloud instances.

The implementation is broken into three phases. Phase 1 will move UTXO on-disk using LMDB which is currently in progress. This phase cannot be used on relays or block-producing nodes. Phase 2 is to migrate LMDB to the custom LSM library developed by Well-Typed. Phase 3 is to identify other parts of the ledger state that can be migrated to reduce memory further.

Revised stake pool incentive scheme

Smaller stake pool operators, especially those with single pools, are unable to compete with larger, especially multi-pool operations. This reduces diversity and choice, making it harder for new pools to enter the Cardano ecosystem.

Several proposals have been made to adjust the current stake pool incentives scheme. A particular concern is that of providing smoother incentives for smaller pools. This project will investigate this important issue, considering the merits of existing proposals, identifying possible improvements to the current scheme with costs/benefits, and outlining a development plan if successful. The community will benefit from greater diversity in the stake pool offering, with healthier small pools. Stake pools will benefit from fairer treatment.

Anti-grinding measures

A grinding attack occurs when network leaders manipulate block additions to improve their chances of re-election as future leaders. The Ouroboros protocol includes anti-grinding measures, but these protections often impact settlement times and finality. Furthermore, grinding attacks are CPU-based, meaning their effectiveness escalates as CPU power becomes more accessible and affordable. This prompts the question: can we enhance settlement times and finality while maintaining robust defenses against the evolving threat of grinding attacks?

This initiative focuses on enhancing the Ouroboros consensus layer by increasing the difficulty for adversaries to execute grinding attacks, while imposing minimal overhead on honest participants in the Praos leader election process. Specifically, the project will explore cryptographic alternatives for the η-nonce computation and provide updated recommendations for the security parameter K, currently set to 2160 blocks (approximately 12 hours). It addresses two CPSs: CPS-0017 (Settlement Speed) and a new CPS (Countermeasures for CPU-Based Attacks).

Tiered pricing

The Cardano network faces congestion issues during peak times, leading to unpredictable transaction delays. Approximately 20% of the time, users experience delays that disrupt critical, time-sensitive transactions, often causing frustration and financial risk.

The tiered pricing model introduces a prioritization mechanism for Cardano transactions. Users can select from three transaction channels – Standard, Priority, and Assured – each offering different fee levels and block inclusion expectations. This flexible system, powered by AI-based congestion predictions, allows users to choose the urgency and cost of their transactions to meet their specific needs. This will lead to predictable timing and costs. Users can better anticipate both transaction times and fees, enhancing reliability. It will enable flexible prioritization as higher fees for urgent transactions ensure timely inclusion. Ultimately this results in an improved UX as users avoid delays and unexpected costs during congestion.

Usability and utility

Blockchain has a usability gap. Simplifying the user experience is key, targeting broader adoption. It is important to learn from the mistakes of PGP, a disruptive innovation with little uptake due to its usability issues. Many in the industry are attempting to solve usability problems through centralization of services. This core tenet of Cardano is something that IO will not sacrifice.

To achieve the ultimate aim of reconstructing the systems of the world requires new ingredients: identity, privacy and the ability to conform to regulatory requirements. A framework for identity is required to ensure counterparties in transactions are known or meet regulatory requirements, among other practical uses such as blockchain governance. It is necessary to recognize the need for privacy and understand that privacy is defined across a spectrum and scale. Finally, current regulatory frameworks are highly fragmented; thus, integrating regulation into blockchain systems poses significant challenges. IO will achieve these aims through:

- Developer productivity
- Identity via Hyperledger Identus
- Privacy via Midnight
- Babel fees.

Developer productivity

Cardano has evolved from a single language platform (Plutus) with a reputation for being challenging for developers to build on, to one of many languages supported by a fertile ecosystem of tools and supporting infrastructure, such as the addition of BLS. This has greatly reduced the cost of development and maintenance for building Cardano applications. This momentum will continue with a number of initiatives across Plinth (formerly known as Plutus Tx) and Plutus HA as well as alternative languages such as Aiken and Plu-TS. Much of the proposed work spans these languages. IO's proposals include:

- **Static analyzer**. Identifies vulnerabilities and issues in smart contracts by analyzing code without execution.
- **Property-based testing**. Generates diverse inputs to validate smart contract behavior and identify edge cases.
- **Formal verification tools**. Ensures smart contracts meet predefined specifications through mathematical proofs.
- **Container-based development environment**. Provides a streamlined and isolated environment for efficient contract development and verification.
- **Code profiler**. Offers performance insights by measuring execution time, memory use, transaction costs, and bottlenecks in smart contracts.
- **Load testing tool**. Simulates high-traffic scenarios to test DApp performance under stress, such as stress testing, spike testing, volume testing, soak testing, scalability testing, endurance testing, load testing, etc.

- **Universal annotation language**. Provides a common language across all smart contract programming languages to formally specify the business logic and security properties of a DApp. It will be used in the formal verification tool as the specification language.

Plinth and Plutus Core

The Plutus team has rebranded Plutus Tx as Plinth, a decision made to clarify terminology within the ecosystem. This change aims to distinguish between Plutus Tx and Plutus Core more effectively. ‘Plutus’ has often been confusingly used for both modules.

Plutus HA

Plutus High Assurance is an upgraded version of the Plutus language to apply the principles of formal methods and certification tooling. It aims to bring the highest level of security in contracts by providing developers with access to easy-to-use formal methods and a suite of certification tools to test their applications. A more detailed roadmap can be found here.

- Finalize a high assurance CIP
- VSCode extension for integrated testing
- Automatic formal verification.

Aiken, PluTS, and alternative languages

The Cardano community has rallied around Aiken due to its approachability and familiarity. This has helped Cardano overcome one of its perceived weaknesses with the requirement to use a Haskell-based language which is unfamiliar to many and challenging to learn. IO views this as a critical area to ensure a superior developer experience for Cardano, but we are only contributors rather than leaders in this area. IO has been actively contributing to the Aiken project with dedicated engineers and will continue to do so in 2025. The PluTS language offers an even simpler alternative leveraging a TypeScript syntax. IO is contributing to the engineering work on this language with full-time resources.

Identity via Identus and Lace

Bringing identity to Cardano will unlock a whole new set of use cases and set Cardano for success if regulation demands stronger identity checks. Self-sovereign identity (SSI) has long been viewed by the industry as the technology to do this, as it preserves the principles of decentralization and empowers individuals to control their own identity.

IO has delivered on this vision with Identus, now a full Linux Decentralized Trust Foundation (FKA Hyperledger) project. Identus provides a rich set of services that enable the issuance, revocation, and verification of credentials. Those credentials are held by individuals in a local wallet allowing them to manage their own identities.

Identus brings decentralized identifier (DID) and credential management to Cardano. By ensuring Cardano is the first platform supported by Identus, IO is helping to ensure Cardano leads in the inevitable need for strong identity management on blockchains. Cardano brings a resilient and long-lived platform for DID management.

The power of SSI is allowing users to manage their credentials. IO will be bringing this capability to users via our wallet solution, Lace. Lace will enable users to interact with any claims, and generate and manage their own DIDs putting users in control of their identity. It will enable any DApp to straight through process claims made by a user over their identity, even on-chain.

In 2025, IO will be laying out a longer-term roadmap for Identus. IO is working on a number of near-term capabilities to continue its evolution including:

- Simplification of deployment, making multi-tenancy and SaaS capabilities optional
- Ability to add VDRs with open driver architecture
- Improvements of the JWT VC data model including SD-JWT revocation.

Privacy via Midnight

Privacy is expected by users of most systems and in many cases is a regulatory requirement. Bringing privacy to blockchains unlocks many new use cases that will bring the next wave of transactions and users. IO is bringing privacy not only to Cardano but to any network via Midnight. Midnight is the first partner chain, discussed later in this document.

The Midnight blockchain provides privacy through its ZK proof-based smart contracts. Leveraging a simple Typescript-based syntax known as Compact, developers can create powerful contracts that allow them to control the level of privacy they require selecting private or public fields. They can also select whether data is stored on-chain or off-chain leaving only the proofs on-chain. Midnight operates as a partner chain allowing it to provide privacy services to any network it has connected to.

As a partner chain, Midnight is secured by Cardano's SPOs. Cardano SPOs can register to become validators of the Midnight network and gain block rewards for securing the network. The SPOs leverage their stake for security enabling them to have additional gains for ada staking and pass a share of those gains to their stakers.

Midnight has a unique dual token structure. The primary token is a Cardano native token, issued and governed by a Cardano-based contract. This enables Midnight to leverage the proven security of Cardano in its bootstrap phase. Users can pre-purchase blockspace allowing them to have predictable pricing and avoid the dynamic price spikes that have made other platforms unviable for enterprise use cases.

Midnight is currently in its testnet phase and will be launching the mainnet in late 2025.

Babel fees

Users who do not hold ada are not able to easily interact with the Cardano blockchain because they cannot pay transaction fees, supply min-UTXO ada for each UTXO, or provide collateral for engagement with scripts. Support is needed to allow such users to seamlessly use non-ada tokens for those purposes not only for usability for native Cardano users but also for users on other networks that may be unaware they are leveraging Cardano.

Babel fees was a research paper that aimed to allow users to pay their fees in any token rather than just ada while still allowing the SPOs to be rewarded in ada. The transaction for this swap would occur as a part of the transaction the user has submitted and appear seamless to them. This enables users to work with Cardano without having to go through the extra steps of acquiring ada. This not only enables convenience but also unlocks possibilities for bridging to other networks such as Midnight. Those networks will be able to use Cardano settlement while still retaining value in their native token. This is explained further in a brief example here.

IO undertook a project to move the proposal from the white paper to a mature software readiness level. In this process, we developed a CIP that allows for the outcomes of Babel fees through a more flexible intent-based transaction type known as nested transactions. Nested transactions are a change to the current ledger design to support a specific kind of transaction batching. By allowing individual transactions in a batch to be unbalanced, but the full batch itself must be balanced, this design supports swap intents. Intents allow users to submit transactions with an intended outcome but without the need to know all the steps toward that outcome.

IO has brought this work to SRL5 and has delivered not only a CIP for the nested transactions. In 2025 we aim to:

- Production-ready AGDA formal specification with completed proofs
- Ledger implementation of the CIP
- Integration to the node put it into production on mainnet.

The implementation of this CIP unlocks not only Babel Fees but new transaction types uses of which we have not yet envisioned.

Interoperability and extensibility

Interoperability with other networks, as well as extending the capabilities of the Cardano network, is critical to the ability to capture the benefits of the promise of blockchain and help Cardano grow. To succeed in the third generation of blockchain technology, embracing interoperability is essential, even outside blockchains by acknowledging existing legacy services that underpin vast financial systems.

Cardano today has few bridges to other networks but there has been great progress on this with work on IBC or other bridges in progress. However, bridges suffer from attacks, wrapped tokens, and other deficiencies. IO believes interoperability has much broader requirements than what bridging brings today.

Partner chains is IO's solution to the shortcomings of bridges and isolated blockchain networks. Partner chains brings three novel approaches to interoperability and extensibility:

- **Service layers**. Partner chains act as service layers providing services to other networks, enabling developers to call on services from many different networks.
- **Hybrid apps**. Partner chains enable atomic cross-chain transactions allowing users to create complex multi-chain transactions in a trustless manner.
- **Multi-resource consensus**. Minotaur is the multi-resource consensus technology that allows a partner chain to be validated by native layer 1 validators.

Achieving the stated aims for Cardano's future requires a node architecture that allows development to move quickly, create alternate clients, and place Cardano as the settlement layer as originally envisioned. This is discussed in the first section on proposed microservices architecture in a polyglot node.

The ultimate outcome of interoperability is a native integration with Bitcoin. Bitcoin not only represents a natural network for integration at a technology level but also at the level of shared beliefs. Bitcoin integration will bring the power of Cardano's smart contracts to the $1.7 trillion of value held by its users today.

This section discusses our interoperability and extensibility through:

- Cardano: layered node architecture with microservices
- Partner chains: multi-resource consensus via Minotaur
- Partner chains: extensibility via partner chains service layers
- Partner chains: cross-chain transactions via hybrid DApps
- Cardano as the smart contract layer for Bitcoin.

Cardano: layered network architecture and microservices

Haskell was originally chosen as Cardano's primary language because of its strong emphasis on formal methods, mathematical rigor, and safety, which aligned well with Cardano's goals of creating a secure, reliable blockchain. However, any single language platform makes it difficult to move fast or create alternate clients. Additionally, the community has not found Haskell to be accessible which has led to node development being overly central inside IO. A shift to a revised architecture is essential to enhancing scalability, developer accessibility, extensibility, and system flexibility.

A polyglot approach to the architecture combined with a microservices architecture will lead to higher quality in addition to faster development. A microservices architecture allows a large application to be separated into smaller independent parts, with each part having its own realm of responsibility. Cardano will gain the ability to add new features without the core upgrade. This also means developers can work with languages like Rust, Go, TypeScript, and Haskell on the core node, expanding the potential base of contributors for Cardano.

Scalable systems like those used by Netflix or Google can handle growth dynamically largely due to their microservices architecture. Cardano's move to an event-driven architecture with microservices aims to increase flexibility and scalability across different applications. By splitting Cardano's services into modular components such as consensus, staking, and indexing, developers can plug in various functionalities tailored to their needs. This structure enables more efficient scaling of specific services without overloading the entire system.

Existing code and functionalities will be 'wrapped' and integrated with new developments in a polyglot system. This lets the old Cardano codebase coexist with new components, enabling a phased upgrade to more advanced architecture without needing a complete rewrite. This layered compatibility helps Cardano evolve without disrupting current projects and allows the gradual implementation of complex protocols like Ouroboros Leios.

This also enables those same components to be used in partner chains or the Pragma Rust node (Amaru). In fact, IO is already working with TxPipe and Globant to build the Cardano networking stack in Rust for use in both the Pragma node and the Substrate stack used by partner chains. Mithril is written in Rust and is a good candidate for an early polyglot integration step. Another early proof of concept will be demonstrating that a microservice architecture with disk storage can meet the required block validation time.

Partner chains: multi-resource consensus via Minotaur

Minotaur is a research paper from IO that showed how the use of mixed resources to secure a network leads to a higher security level than either one alone can provide. In the first version of this paper, we evaluated proof of work (PoW) mixed with proof of stake (PoS). However, we quickly recognized the multi-resource concept of Minotaur brings more than increased security to blockchains: it provides the ability to integrate those networks and the economic incentives for those networks to cooperate on the shared network.

IO is evolving the Minotaur roadmap to capture this new reality and to create a new means of

interoperability between networks. We'll be landing Minotaur's capabilities in partner chains as a unique consensus mechanism.

The first release of Minotaur is out now and allows a new partner chain to leverage the security of the Cardano SPOs. By leveraging Cardano as the root of trust, a new partner chain can securely bootstrap its security. With Minotaur, the network is able to slowly migrate to local validators as they demand. This uniquely means they are not locked into any network or security model.

The following release will enable the network to leverage two layer 1 PoS network validators, further enhancing the security but also unlocking a new mode of trustless interoperability. The next network to be added will be Ethereum, building trustless interoperability between Cardano and Ethereum.

By opening up connections and enhancing capabilities, these developments will draw more users to the Cardano platform, similar to establishing an airport or cruise line for tourism. This will create pathways for Bitcoin and Ethereum communities to engage with Cardano's offerings without needing deep technical knowledge about its underlying structure.

Partner chains: extensibility via service layers

Multi-chain interoperability is crucial for the evolution of blockchain technology, allowing different systems to communicate effectively. This would allow networks to specialize in capability, asset types, or other ways similar to how traditional systems work today. Yet, as deterministic systems, blockchains have evolved to be closed networks unable to interact with each other. This leads to an all-or-nothing compromise for users who must accept the trilemma tradeoffs made by the network. Bridges fail to solve this, as they largely are only capable of wrapping tokens on other networks, not cross-chain transactions.

Blockchains can learn from cloud architectures where different systems are optimized for a specific purpose but can still provide services to other systems. IO envisions a similar approach for the blockchain ecosystem called a service layer. The service layer enables networks to operate with their own optimizations while providing services to other blockchain networks.

These services retain their decentralization. This is the vision being delivered through partner chains.

Partner chain networks enable transactions across blockchains without requiring the bridging of tokens or migration of contracts between those blockchains. This unlocks new possibilities for blockchain. It allows blockchain networks to specialize and differentiate while not requiring them to bridge and move tokens for liquidity, recreate DApps and onboard new users. As the

first partner chain, Midnight is showing how it can provide privacy services to Cardano and other networks. For example, a contract on Cardano can reach out to Midnight to request ‘know your customer’ (KYC) related confirmation data. Midnight can ensure the data is kept private but provide a result back to the Cardano DApp.

Partner chains: cross-chain transactions via hybrid DApps

Service layers enable blockchains to communicate via contracts but IO also aims to enable users to create their own transactions across blockchains without requiring developers to have implemented this. Users should be able to build complex, multistep transactions that span multiple chains but execute in a near-atomic manner without any bridging. This concept is called hybrid DApps.

Hybrid DApps build on the concept of chain abstraction, moving toward a world where users are leveraging blockchains and may not even be aware. This is how to bring Web3 capabilities to Web2. With hybrid DApps, users will be able to perform transactions across any chains the partner chain is validated by. A user will view blockchains, DApps, and liquidity as if it were a single platform and be able to transact across them. The cross-chain capability is facilitated at the consensus layer ensuring it remains a trustless solution.

To achieve this, IO is leveraging Minotaur. With Minotaur, a partner chain’s validators are the same validators as those of the layer 1 the partner chain integrates with. These validators not only observe other networks but can participate by submitting transactions on behalf of their users. Using threshold signatures (TSS) the validators can ensure a complex, multi-chain transaction will occur in an atomic manner while allowing the tokens to stay on their native chains. TSS allows the network validators to take control of the assets on the native chains on behalf of the users for the duration of the contract. As an MPC mechanism, TSS ensures any action requires consensus by the network validators, including those from multiple networks.

This work is in the early stages of development but has exciting potential to enable users to move past the boundaries of the existing networks.

Cardano as the smart contract layer for Bitcoin

The premiere example of partner chains in action will be the integration of Bitcoin and Cardano. In many ways, Cardano is the natural complement to Bitcoin. It builds on the original principles and design decisions such as UTXO and carries forward the principles of decentralization.

Cardano builds on Bitcoin’s notion of a decentralized payment system bringing smart contracts, and governance among many other capabilities. We wish to join these communities and allow Cardano to act as the natural DeFi and smart contract layer for Bitcoin.

2025 is the year IO will take meaningful steps into this integration. We are exploring how to

bring Bitcoin miners into the fold by evaluating merged mining to allow the Bitcoin miners to help secure a Partner Chain. This work is in research today but will unlock a new execution layer for Bitcoin users and unleash the liquidity of Bitcoin into Cardano. The partner chains world will enable composability at the network level. Bitcoin users will be able to execute private transactions leveraging Midnight with their value in DeFi contracts on Cardano. This is only the beginning of the possibilities partner chains will bring.