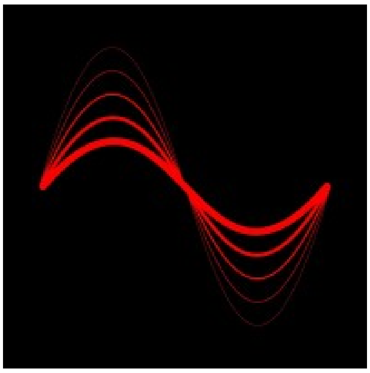
Cardano & Ouroboros (easy peazy) Summary

by

Harmonic Laboratories



Contents

Chapter 1

Cardano

Cardano is a proof-of-stake blockchain platform: the first to be founded on peer-reviewed research and developed through evidence-based methods. It combines pioneering technologies to provide unparalleled security and sustainability to decentralized applications, systems, and societies.

1.1 Development Phases

The five phases of Cardano represent a gradual and well-planned development path aimed at building a secure, scalable, and sustainable blockchain. Cardano's roadmap is unique in its methodical and research-based approach, making the project one of the most ambitious and promising platforms in the industry. As each phase progresses, Cardano moves closer to its goal of becoming a leading global blockchain platform capable of supporting a wide range of decentralized applications and services.

1.1.1 Byron (Foundation)

Main goals

- **Launch of the Mainnet**: the Byron phase marks the launch of Cardano's mainnet in September 2017, making Cardano available to the public;
- **Creation of the Daedalus Wallet**: during this phase, the official Cardano desktop wallet, Daedalus, was released. It was designed to be secure and user-friendly;
- **Implementation of the Blockchain**: this phase saw the creation and implementation of the blockchain based on Ouroboros, Cardano's Proof-of-Stake consensus protocol;
- **Support for ADA Cryptocurrency**: the Byron phase introduced ADA, Cardano's native cryptocurrency, which can be bought, sold, and stored in the Daedalus wallet.

Technical features

- **Proof-of-Stake**: introduction of the Proof-of-Stake (PoS) consensus mechanism through Ouroboros;
- **Blockchain Explorer**: a tool that allows users to check transactions on the Cardano network.

Outcomes

The Byron phase established the foundation of the Cardano blockchain, ensuring the network was secure, reliable, and capable of supporting further developments.

1.1.2 Shelley (Decentralization)

Main goals

- **Decentralization**: Shelley's primary objective was to decentralize the network. While Byron laid the groundwork, Shelley introduced mechanisms to transition to decentralized governance;
- **Staking and Stake Pools**: introduction of staking features, allowing users to participate in the network and earn rewards.

Technical features

- **Incentive System**: design of an incentive system to reward users for maintaining and securing the network;
- **Delegation**: ability for users to delegate their stake to staking pools to earn rewards;
- **Increase in Independent Nodes**: growth in the number of independent nodes, enhancing the network's security and resilience.

Outcomes

Shelley transitioned Cardano from a federated platform to a decentralized one, increasing community participation and establishing a distributed governance model.

1.1.3 Goguen (Smart Contracts)

Main goals

- **Smart Contracts**: the Goguen phase introduced support for smart contracts, enabling developers to build decentralized applications (DApps) on the Cardano platform;
- **Compatibility with other Blockchains**: improved interoperability with other blockchains and legacy systems.

Technical features

- **Plutus**: a new programming language for writing secure and reliable smart contracts. Plutus allows for the development of more complex applications on Cardano;
- **Marlowe**: another programming language specifically designed for financial contracts, enabling the creation of smart contracts even by users without programming experience;
- **Support for Native Tokens**: introduction of support for creating and managing native tokens on the Cardano blockchain, allowing for asset tokenization.

Outcomes

The Goguen phase made Cardano a versatile and competitive platform for developing DApps and smart contracts, expanding the network's use cases.

1.1.4 Basho (Scaling)

Main goals

- **Scalability**: improve the network's scalability to handle more transactions per second, making Cardano suitable for large-scale adoption;
- **Performance Optimization**: optimize network performance, reducing latency, and improving overall efficiency.

Technical features

- **Sidechains**: introduction of sidechains, which expand network capacity without compromising the security and integrity of the main blockchain;
- **Protocol Improvements**: updates and optimizations to the Ouroboros consensus protocol to enhance performance.

Outcomes

The Basho phase laid the groundwork for a more efficient and scalable network, ensuring that Cardano can support a wide range of applications and an increasing number of users.

1.1.5 Voltaire (Governance)

Main goals

- **Decentralized Governance**: implement a decentralized governance system, allowing the community to make decisions regarding the network's future developments;
- **Sustainability**: create a sustainable funding system for the platform's maintenance and development.

Technical features

- **Treasury System**: introduction of a treasury system that collects funds to finance development projects proposed by the community;
- **Voting and Improvement Proposals**: implementation of a voting mechanism that enables stakeholders to propose and vote on improvements and changes to the network.

Outcomes

Voltaire transforms Cardano into a fully autonomous and self-governing platform, allowing the community to directly influence the network's future.

1.2 Ledger

The Cardano Ledger refers to the underlying structure and technology that supports Cardano's blockchain. It represents the complete system that records all transactions and smart contracts executed on the Cardano network, ensuring their security, transparency, and immutability.

1.2.1 Eras

There are several eras within the evolution of Cardano. Each era refers to the rules of the ledger. For example, what transaction types and what data is stored in the ledger, or the validity and meaning of the transactions.

DATE	PHASE	ERA	LEDGER PROTOCOL	PROTOCOL VERSION	CONSENSUM MECHANISM
2017/09	Byron	Byron	-	0.0	Ouroboros Classic
2020/02	Byron	Byron	-	1.0	Ouroboros BFT
2020/07	Shelley	Shelley	TPraos	2.0	Ouroboros Praos
2020/12	Goguen	Allegra	TPraos	3.0	Ouroboros Praos
2021/03	Goguen	Mary	TPraos	4.0	Ouroboros Praos
2021/09	Goguen	Alonzo	TPraos	5.0	Ouroboros Praos
2021/10	Goguen	Alonzo	TPraos	6.0	Ouroboros Praos
2022/09	Goguen	Babbage	Praos	7.0	Ouroboros Praos
2023/02	Goguen	Babbage	Praos	8.0	Ouroboros Praos

1.2.1.1 Byron and Shelley

The evolution of the Cardano mainnet began with the Byron ledger rules. The mainnet underwent a hard fork in late July 2020 to switch from the Byron rules to the Shelley ledger rules. It was a full reimplementation of Cardano, which enabled two fundamental changes: the support for multiple sets of ledger rules, and the management of the hard fork process of switching from one set of rules to the next. In other words, the new implementation could support both the Byron rules and the Shelley rules, which meant that, when deployed to the mainnet in early 2020, the implementation was fully compatible with the Byron rules. This allowed for a smooth transition from the old to the new implementation. Once all Cardano users had upgraded their nodes to the new implementation, it became possible to invoke the hard fork combinator event and switch to the Shelley rules.

1.2.1.2 Allegra, Mary and Alonzo

Allegra, Mary, and Alonzo eras are all part of the Goguen development phase.

Starting with Goguen, the ledger team introduced the notion of era into the ledger code. Shelley ledger rules then became 'the Shelley era'.

Because Goguen features were implemented in steps, each set of functionality was introduced with a different hard fork, hence there were several ledger eras:

- Allegra: introduced token locking support;

- Mary: brought native tokens and multi-asset functionality to Cardano
- Alonzo: introduced smart contract support.

1.2.1.3 Bubbage

The Babbage ledger era introduced such features as inline datums, reference scripts, and reference inputs.

1.3 Nodes

The Cardano node is the top-level component within the network. Network nodes connect to each other within the networking layer, which is the driving force for delivering information exchange requirements. This includes new block diffusion and transaction information for establishing a better data flow. Cardano nodes maintain connections with peers that have been chosen via a custom peer-selection process. By running a Cardano node, you are participating in and contributing to the network.

Stake pools use the Cardano node to validate how the pool interacts with the network and are responsible for transaction processing and block production. They act as reliable server nodes that hold and maintain the combined stake of various stakeholders in a single entity.

1.3.1 Stake Pools

A stake pool is a reliable server node that focuses on ledger maintenance and holds the combined resources - the 'stake' - of various stakeholders in a single entity. Stake pools are responsible for processing transactions that will be placed in the ledger, as well as producing new blocks. Stake pools are at the core of Ouroboros, Cardano's proof-of-stake protocol.

To be secure, Ouroboros requires a good number of stakeholders to be online and maintain sufficiently good network connectivity at any given time. This is why Ouroboros relies on stake pools, entities that are committed to running the protocol 24/7, on behalf of the contributing stakeholders that hold ADA. The idea is that these resource holders can bring their resources (their stake) together and form a pool, where typically one holder is the operator of the pool and the rest are delegators.

1.4 Blocks

The goal of blockchain technology is the production of an independently-verifiable and cryptographically-linked chain of records (blocks). A network of block producers works to collectively advance the blockchain. A consensus protocol (Ouroboros) provides transparency and decides which candidate blocks should be used to extend the chain.

Submitted valid transactions might be included in any new block. A block is cryptographically signed by its producer and linked to the previous block in the chain. This makes it impossible to delete transactions from a block, alter the order of the blocks, remove a block from the chain or insert a new block into the chain without alerting all the network participants. This ensures the integrity and transparency of the blockchain expansion.

1.4.1 Slots and Transactions

The Cardano blockchain uses the Ouroboros Praos protocol to facilitate consensus on the chain. Ouroboros Praos divides time into epochs. Each Cardano epoch consists of a number of slots, where each slot lasts for one second. A Cardano epoch currently includes 432,000 slots (5 days). In any slot, zero or more block-producing nodes might be nominated to be the slot leader. On average, one node is expected to be nominated every 20 seconds, for a total of 21,600 nominations per epoch. If randomly elected slot leaders produce blocks, one of them will be added to the chain. Other candidate blocks will be discarded.

1.4.1.1 Slot leader election

The Cardano network consists of a number of stake pools that control the aggregated stake of their owners and other stakeholders, also known as delegators. Slot leaders are randomly elected from among the stake pools. The more stake a pool controls, the greater the chance it has of being elected as a slot leader to produce a new block that is accepted into the blockchain. This is the basic concept of proof of stake (PoS). To maintain a level playing field, and prevent a situation where a small number of very large pools control the majority of stake, Cardano has an incentive system that discourages delegation to pools that already control a large portion of the total stake.

1.4.1.2 Transaction validation

When validating a transaction, a slot leader needs to ensure that the sender has included enough funds to pay for that transaction and must also ensure that the transaction's parameters are met. Assuming that the transaction meets all these requirements, the slot leader will record it as a part of a new block, which will then be connected to other blocks in the chain.

Chapter 2

Consensus

Consensus is the process of reaching a majority opinion by everyone involved in running the blockchain. An agreement must be made on which blocks to produce, which chain to adopt and to determine the single state of the network. The consensus protocol determines how individual nodes assess the current state of the ledger system and reach a consensus.

Blockchains create consensus by allowing participants to bundle transactions that others have submitted to the system in blocks, and add them to their chain (sequence of blocks). Determining who is allowed to produce a block when, and what to do in case of conflicts, (such as two participants adding different blocks at the same point of the chain), is the purpose of the different consensus protocols.

The protocol has three main responsibilities:

- perform a leader check and decide if a block should be produced;
- handle chain selection;
- verify produced blocks.

2.1 Ouroboros

Cardano runs on the Ouroboros proof-of-stake consensus protocol.

Ouroboros divides time on Cardano into epochs where each epoch is divided into slots. A slot is a short period of time in which a block can be created. Grouping slots into epochs is central to adjusting the leader election process to the dynamically changing stake distribution.

A slot leader is elected for each slot, who is responsible for adding a block to the chain and passing it to the next slot leader. To protect against adversarial attempts to subvert the protocol, each new slot leader is required to consider the last few blocks of the received chain as transient: only the chain that precedes the prespecified number of transient blocks is considered settled. This is also referred to as the settlement delay. Among other things, this means that a stakeholder can go offline and still be synced to the blockchain, so long as it's not for more than the settlement delay.

Within the Ouroboros protocol, each network node stores a copy of the transaction mempool (where transactions are added if they are consistent with existing transactions) and the blockchain. The locally stored blockchain is replaced when the node becomes aware of an alternative, longer valid chain.

2.1.1 Versions

2.1.1.1 Classic

The first implementation of Ouroboros achieved three major milestones:

- the foundation for an energy-efficient protocol to rival proof of work;
- the introduction of the mathematical framework to analyze proof of stake;
- the implementation of a novel incentive mechanism to reward participants in a proof-of-stake setting.

But what really set Ouroboros apart from other blockchain protocols (specifically, proof-of-stake protocols), was its ability to generate unbiased randomness in the protocol's leader selection algorithm, and the subsequent security assurances that provided. Randomness prevents the formation of patterns, which is critical for maintaining the protocol's security. Ouroboros was the first blockchain protocol developed with this type of rigorous security analysis.

2.1.1.2 BFT

Ouroboros Byzantine Fault Tolerance (BFT) was the protocol's second implementation, used during the Byron update (transition from the old Cardano codebase to the new). The second instance of the protocol prepared Cardano for the decentralization that came with the Shelley release.

Ouroboros BFT enabled synchronous communication between a network of federated servers (the blockchain) providing ledger consensus in a simpler and more deterministic manner.

2.1.1.3 Praos

Ouroboros Praos introduced substantial security and scalability improvements to the Ouroboros Classic implementation. Praos processes transaction blocks by dividing chains into slots, which are aggregated into epochs. But unlike Ouroboros Classic, Praos is analyzed in a semi-synchronous setting and is secure against adaptive attackers, using private-leader selection and forward-secure, key-evolving signatures to ensure that a strong adversary cannot predict the next slot leader and launch a focused attack (such as a DDoS attack).

2.1.1.4 Genesis

The fourth iteration of Ouroboros, Genesis, further improves upon Ouroboros Praos by adding a novel chain selection rule that enables parties to bootstrap from a genesis block without the need for trusted checkpoints or assumptions about past availability. The Genesis paper also provides proof of the protocol's Universal Composability, which demonstrates that the protocol can be composed with other protocols in arbitrary configurations in a real-world setting, without losing its security properties.

2.1.1.5 Crypsinous

Ouroboros Crypsinous equips Genesis with privacy-preserving properties. It is the first formally analyzed privacy-preserving proof-of-stake blockchain protocol, which achieves security against adaptive attacks while maintaining strong privacy guarantees by introducing a new coin evolution technique relying on Snarks and key-private forward-secure encryption. Crypsinous isn't currently planned to be implemented on Cardano, but it can be used by other chains for increased privacy-preserving settings.

2.1.1.6 Chronos

Chronos achieves two goals:

- it shows how blockchain protocols can synchronize clocks securely via a novel time synchronization mechanism and thereby become independent of external time services;
- it provides a cryptographically secure source of time to other protocols.

In short, Chronos makes the ledger more resistant to attacks that target time information.

From an application point of view, Chronos can dramatically boost the resilience of critical telecommunications, transport, and other IT infrastructures that require the synchronization of local time to a unified network clock that has no single point of failure.

Glossary

hard fork Hard Forks are small and focused semantic changes to the ledger. . 4

proof-of-stake Proof-of-Stake (PoS) is a consensus mechanism used in blockchain networks to validate transactions and secure the network. Unlike Proof-of-Work (PoW), which requires computational power to solve cryptographic puzzles, PoS selects validators based on the number of coins they hold and are willing to ”stake” as collateral. The probability of being chosen as a validator is proportional to the amount of cryptocurrency staked. This approach significantly reduces energy consumption, increases efficiency, and enhances security against certain types of attacks. PoS also incentivizes participants to act honestly, as malicious behavior can lead to the loss of their staked coins. . 1, 7

smart contracts Smart contracts are a revolutionary concept in the blockchain and cryptocurrency space. They are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. . 2

Bibliography

[1] *Cardano Basics*. URL: https://cardano.org/.

[2] *Cardano Phases and Eras table*. URL: https://github.com/cardano-foundation/CIPs/blob/master/CIP-0059/feature-table.md.

[3] *Cardano Roadmap*. URL: https://roadmap.cardano.org/.

[4] *Consensus Overview*. URL: https://docs.cardano.org/about-cardano/learn/consensus-explained/.

[5] *Ouroboros Overview*. URL: https://docs.cardano.org/about-cardano/learn/ouroboros-overview/.