Cardano and Smart Contracts

Sabina Săvescu, Tiberiu Bujor

# Abstract

Cardano is a blockchain-based platform (similar to Ethereum), which was created to scientifically research and solve all known, current difficulties of other blockchain currencies.

The intent of this report is to present details regarding Cardano’s most important features and how it aims to solve problems related to scalability, interoperability and sustainability. It offers an overview of the architecture, the concepts utilised and the improvements made in comparison to previous generations of cryptocurrencies. Future plans concerning the development of the project are also mentioned.

In the *Results* section, we showed how the Daedalus wallet is installed and used.

# Introduction

The development of Cardano was initiated in 2015 by Charles Hoskinson, one of the co-founders of Ethereum and is funded by three organisations: Input-Output Hong Kong (IOHK), Cardano Foundation and Emurgo. The purpose of this project is to redesign the development of cryptocurrencies in order to create a decentralized platform for complex value transfers that are guaranteed to be secure. It is based on peer-reviewed academic research, which means that all stages and concepts are reviewed and criticized by peers (researchers or developers). ADA is the internal cryptocurrency used by Cardano as payment for its transactions.

The main reason why this project was created was to solve the problems concerning the usability, security and scalability of previous blockchain-based cryptocurrencies, which are caused by weaknesses in the technical structures. The world of cryptocurrencies is constantly evolving. The first generation, in which static payments were made without contracts (Bitcoin) was followed by a generation in which dynamic contracts were possible (Ethereum). As a third generation blockchain, Cardano claims to improve scalability for mass usage, interoperability, and sustainability by implementing new technologies.

In order to increase interoperability with the legacy world, Cardano has the intention to focus on three obstacles which prevent the crypto world from being compatible with the legacy world: metadata (information related to transactions), attribution (identities of the people involved in transactions) and compliance (verification of the legitimacy of transactions).

# Concepts, implementation

## Architecture

Cardano is being developed in two layers: CSL and CCL. The separation of the two has the advantage that updates can be carried out separately and specifically. It also makes the platform safer because a hack on one layer does not affect the other. This allows developers of the platform to separately store and process metadata (information about the transaction, such as what the money is spent on, who it is given to and where it is spent).

1. *Cardano Settlement Layer (CSL)*

This is the fundamental layer that acts as a cryptocurrency - it manages the transfer of the native currency, ADA, under the proof-of-stake protocol, Ouroboros. It is meant as an improvement to Bitcoin.

1. *Cardano Control Layer (CCL)*

On this layer, account data is processed. This includes information (details about the way in which specific transactions occur), stored in a smart contract, for example, but also digital identities. The separation gives the user more control over the privacy and execution of smart contracts. Different users can create rules when validating transactions.

## Programming language

Cardano is a highly secure blockchain platform developed in Haskell, a functional programming language that uses complex mathematical logic for coding, and has a high fault tolerance degree. The reason why this is required is the fact that the protocols building Cardano (ADA) are meant to deliver the resilience necessary for mission-critical systems, in this case securing investment. The language used for defining smart contracts in Cardano is Plutus, a strictly typed pure functional programming language.

## Ouroboros

Ouroboros, a proof-of-stake protocol, was developed through the intensive collaboration of the Tokyo Institute of Technology, the University of Edinburgh, the University of Connecticut and IOHK. This solution is proven to be safe and more efficient and faster in comparison to other PoS systems.

The main reason behind choosing a proof-of-stake (PoS) algorithm over a proof-of-work (PoW) algorithm (used by Bitcoin), is that the energy consumption is reduced. In the case of proof-of-work, a solution to a computationally heavy problem needs to be found in order to choose a leader that generates a block, while the idea of proof-of-stake is to randomly select a node to generate a block based on probability (proportional to the size of the stake). ‘Proof’ refers to the legitimacy of the transactions, while ‘stake’ represents the total value held by addresses on a node divided by the total value in the CSL system.

Ouroboros is a consensus mechanism. In cryptocurrencies, a ledger[[1]](#footnote-1) is generated by digitally signing and sending transactions to the network and receiving blocks of verified transactions. The cryptocurrency is decentralized which means that many people from all around the world are involved in the generation of the ledger. Therefore, a consensus about the state of the ledger is required, which is the reason why such a mechanism is implemented.

The algorithm offers developers the ability to precisely control the conditions under which a user can become a stakeholder. In case a stakeholder attempts to manipulate transactions in his own favour, the protocol recognizes this behaviour and excludes that stakeholder from the network, which results in them also losing all their coins.

If a stakeholder behaves according to the rules, they are part of a decentralized network and have the function of validating transaction blocks that are integrated into the blockchain. After a block is created it is forwarded to other nodes for review. As more stakeholders confirm a transaction, it is ensured that it was done correctly. Stakeholders receive a reward per verification of a block.

Ouroboros works with time epochs (that last for ~20 seconds), each having different time intervals called slots, which represent potential blocks. Each slot has a leader who can choose a block to be added. The condition for a stakeholder to have the chance to be elected as a slot leader is to own 2% stake, the chance increasing the more stake they own. If order for it to be unbiased, the election is made through a multiparty computation (MPC) which consists of three phases:

1. *Commitment*

An elector generates a message (commitment) which contains encrypted shares and a secret and has the epoch number and public key attached. Each elector sends their own commitment and receives all the other electors’ messages, which then become part of the blockchain.

1. *Reveal*

Each elector sends a special value called opening, used to unlock the commitment, which is also put into the blockchain.

1. *Recovery*

The secrets from the commitments are extracted by verifying their match with the openings and form a randomly generated byte string (seed).

The FTS (Follow the Satoshi) is a simple algorithm that selects a coin from the stake randomly, so the owner of it becomes the slot leader.

An important aspect related to Ouroboros is that consensus nodes can handle multiple slots on many different blockchains at the same time. This solves the scaling problem. The platform utilises the sharding[[2]](#footnote-2) concept, which is currently being implemented by Ethereum.

In the future, Ouroboros is supposed to allow parallel, partitioned blockchains and implement a quantum-proof encryption. This way, the formation of a block in the blockchain will cost less than the current implementations.

## Sidechains

An ecosystem in which Ada can flow into Ethereum, for example, without the need of middlemen can be achieved through sidechains, which are parallel chains running along with the main one. The idea of sidechains comes from the need to create a compressed version of a blockchain and interoperability between chains.

## Treasury

The most difficult problem is that of sustainability, which refers to the way in which the platform is supposed to pay for its future development. A solution is the creation of a treasury, which works by collecting a part of the reward every time a block is added to the chain and is proportional to the size of the network.

In case someone wants to bring changes to the system, they can ask for other stakeholders to vote secretly in order to receive grants. Some aspects that must be taken into consideration are related to the implementation of a fair voting system and making the process decentralized.

## Daedalus Wallet

Daedalus Wallet is a multi-currency wallet which allows free exchange between the supported currencies. Although it currently stores only native Cardano coins (ADA), it is planning to offer support with Bitcoin and Ethereum Classic. The new technology it uses provides a high level of protection from vulnerabilities. A more detailed description is found in the *Results* section.

## Roadmap

## The project has a constantly evolving roadmap and should be released in 5 stages:

# *Byron* – includes the initial development of the main network and enables users to trade and transfer ADA

# *Shelley (the current stage)* – ensures that the network becomes fully decentralized

# *Goguen* – introduces a virtual machine, called IELE, similar to the Ethereum Virtual Machine (EVM) and develops a universal language framework for future blockchain technology

# *Basho* – aims to improve scalability, security, and performance

# *Voltaire* – implements the Treasury model, providing a self-sustaining ecosystem for the network

# Results

Our test environment consists of a fresh snapshot of Ubuntu 18.04 ran in VirtualBox on Windows 10. The software installed on the Ubuntu VM: VBox GuestAdditions & network time protocol software (ntp / ntpdate).

The first step was to install the specific version of the TESTNET (give execute permissions to the binary) and do not close the terminal even if it looks like it’s not working.

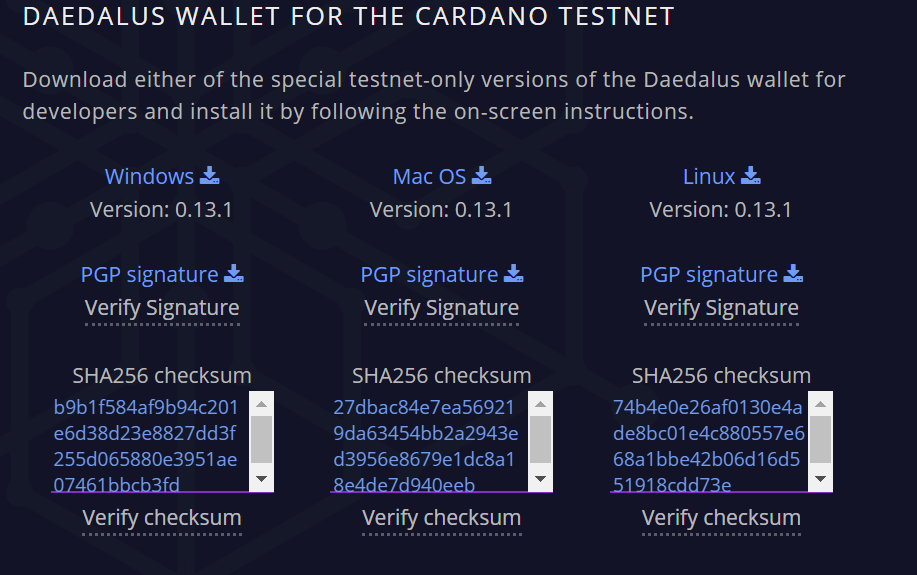


Fig. 1 Cardano TESTNET versioning

Second step is to sync the time of the machine with the correct server using ntp and ntpdate to make the software capable of syncing blocks.

|  |
| --- |
| Fig. 2 Syncing blocks |
|  |

The third step is to create a virtual wallet with NAME / PASSWORD and secret key-phase.

|  |
| --- |
| Fig. 3 Secret key-phase |
|  |

Fourth step consists of filling the virtual wallet by generating a unique wallet address in the receive tab and using the faucet API to add virtual coins (ADA).

|  |
| --- |
| Fig. 4 Wallet addresses |
|  |
| Fig. 5 Empty wallet |
|  |

|  |
| --- |
| Fig. 6 Faucet API Request |
|  |

Using the virtual coins received we can now create more wallets and exchange them.

|  |
| --- |
| Fig. 7 Coin exchange |
|  |

In Fig. 7 we are sending 2 ADA coins + fees from wallet homework5 to wallet Exchange by using the generated wallet address.

The coin transfer can only be done when the software is completely synced and does not function properly when the network time is not exact by 15 seconds.

|  |
| --- |
| Fig. 8 NTP not synced error |
|  |

# Conclusion

Cardano is a long-term project with a lot of potential and has many advantages:

1. It claims to be a tested platform which brings innovations related to consensus, governance and interoperability.
2. It offers security through a layered architecture; its transactional processes work based on smart contracts which are layered, a property which makes them more secure than those of other cryptocurrencies.
3. Its aim is to be decentralized, and not reside with restricted individuals.
4. It offers higher speed and lower transaction costs, by increasing the number of transactions per second.

# 

# References

1. <https://www.cardano.org/en/what-is-cardano/>
2. <https://coinswitch.co/info/cardano/what-is-cardano>
3. <https://coincentral.com/cardano-beginner-guide/>
4. <https://whycardano.com/>
5. <https://cardanodocs.com/introduction/>
6. <https://confionacompra.com/en/what-is-cardano-ada-project/>
7. <https://medium.com/prysmatic-labs/how-to-scale-ethereum-sharding-explained-ba2e283b7fce>
8. <https://blockgeeks.com/guides/what-is-cardano/>

1. Database which contains information about the amount of money each address has [↑](#footnote-ref-1)
2. The entire state of the network is split into a set of partitions called **shards** which contain an independent piece of state and transaction history [↑](#footnote-ref-2)