Cardano and Smart Contracts

Sabina Săvescu, Tiberiu Bujor

# Abstract

Cardano is a blockchain-based cryptocurrency project (similar to Ethereum), that was created to scientifically research and solve all known, current difficulties of past 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

Cardano was developed by Charles Hoskinson, one of the co-founders of Ethereum, and its development is funded by Input-Output Hong Kong. The project, which started in 2015, aims to completely redesign the way cryptocurrencies have been developed at different levels, ultimately creating a decentralized platform for complex, programmable value transfers from a scalability and security perspective. Cardano uses the internal cryptocurrency ADA as payment for its transactions.

From the perspective of the founders of the project, all previous blockchain-based cryptocurrencies inevitably encounter a number of serious problems concerning the practical usability, security, scalability and social and economic integration of cryptocurrencies. These problems arise from the inherent weaknesses in the technical structures of established cryptocurrencies. Thus, the world of cryptocurrencies has moved from a first generation, in which static payments were made without contracts (Bitcoin), to a second generation, in which dynamic contracts were possible (Ethereum). As a 3rd generation blockchain, Cardano would introduce arbitrary scalability for mass usage, interoperability, and sustainability by learning from the mistakes of previous generations and by implementing new technologies.

Cardano aims to solve the three most important problems in this area for any scalability to a mass use: the number of transactions per second, the necessary bandwidth of the network and the accumulating amount of data for the storage of the effected transaction information. To solve these problems, Cardano is working on a new, secure proof-of-stake protocol called Ouroboros. This algorithm was jointly developed on a scientific basis through the intensive collaboration of the Tokyo Institute of Technology, the University of Edinburgh, the University of Connecticut and Input Output Hong Kong. As with Cardano itself, every developmental step has been scientifically reviewed several times before it has finally been integrated into the protocol. In the future, Ouroboros should allow parallel, partitioned blockchains and implement a quantum-proof encryption. In doing so, the formation of a block in the blockchain will cause a fraction of the cost of the current blockchain implementations.

Cardano works on a platform that wants to allow the interaction of protocols of various kinds from the world of cryptocurrencies to interact with each other and protocols of the external financial world. In the future, the aim is to store encrypted metadata for each transaction that stores the source and other master data of a cash flow and can be disclosed to confidential bodies for verification. Cardano would like to take a middle ground between openness to the public sector and protection of privacy for the participant in the network and decentralization. In addition, the tokens of other crypto currencies can be used within the Cardano sidechains.

# Methods, implementation

## Layers

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 of personal data.

1. *Cardano Settlement Layer (CSL)*

Information such as Bitcoin is transferred via transactions. This includes details on the amount, the transferor, the recipient and the transfer date. The token of the platform, ADA, is also transferred on this layer.

1. *Cardano Control Layer (CCL)*

On this layer, account data is processed. This includes information stored in a smart contract, for example, but also digital identities.

## Programming language

Cardano is a highly secure blockchain platform developed in Haskell, a 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.

## Ouroboros

Cardano uses a proof-of-stake protocol. Basically, such protocols have the advantage of giving developers the ability to precisely control the conditions under which a user can become a stakeholder. Stakeholders have a defined amount of coins. This amount of coins entitles them to verify transactions within the decentralized network.

If a stakeholder behaves merely to his advantage, for example, by attempting to manipulate transactions in his own favour, the protocol recognizes this behaviour and excludes that stakeholder directly from the network. This also includes the complete loss of the held coins. Under certain circumstances, this can be very expensive for a stakeholder.

If a stakeholder behaves according to the rules, he is part of a decentralized network with other stakeholders. All stakeholders have the function of verifying transactions and verifying them against the relevant protocol. The more stakeholders confirm a transaction, the more likely it is that it was done correctly. For the operation of a node, stakeholders receive a reward per verification of a transaction block.

The platform uses a form of proof-of-stake algorithm that allows nodes to be selected and chosen by themselves. The Delegated Proof-of-Stake algorithm allows stakeholders to choose so-called consensus nodes. These nodes perform a special form of task, confirming the correctness of transaction blocks that are integrated into the blockchain. Each stakeholder has the option of being able to operate a consensus node himself, if elected. In addition, each stakeholder can choose any other stakeholder.

Ouroboros works with so-called time epochs. In each epoch there are different time intervals, so-called slots, which represent potential blocks. An algorithm provides for the random selection of a consensus node that can select a slot and fill it with transaction information. After a block has been created, the block is forwarded to other nodes for review. In each epoch, all newly created tokens are pooled and then distributed to individual nodes, depending on their involvement.

The highlight of the Delegated Proof of Stake algorithm is that consensus nodes can handle multiple slots on many different blockchains at the same time. This solves the scaling problem. The platform makes use of the sharding[[1]](#footnote-1) concept, which is currently being implemented by Ethereum.

## Daedalus Wallet

Daedalus Wallet is a multi-currency wallet in 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.

## Roadmap

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

# *Byron* – includes the initial development of the main net 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 Echange 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 7. NTP not synced error |

# Conclusion

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

1. It is based on peer-viewed academic research, which means that all stages and concepts are reviewed and criticized by peers(researchers or developers).
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.

# 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. 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-1)