Cardax DEX White Paper V2.0

May 2022

The Cardax Team

Abstract

Decentralised exchange systems where users can engage in transactions that take place in a secure environment without the need for intermediaries are an important manifestation of blockchain technology. This whitepaper describes Cardax DEX– a decentralised exchange (DEX) that will serve as an essential and powerful trading venue in the Cardano ecosystem, providing liquidity to projects that issue native tokens.

The first section of this work provides a brief technical description of the programming language we have built our protocol on. The following sections highlight the mechanism Cardax uses to get to a market price on each liquidity pool. Then, we describe our protocol that, we argue, creates a better trading experience for all users. We close the paper by highlighting the key features that make our Decentralised Exchange different from others and why we have decided to build it on Cardano rather than on Ethereum.

Contents

1. Introduction

Cardax DEX (version 1) is a fully decentralised Automated Market Maker (AMM) exchange (DEX) on the Cardano eUTXO blockchain. The first of its kind to be written in the novel Plutarch language, Cardax DEX utilises its proprietary Streaming Merge algorithm to negate the Cardano concurrency issue.

It provides a fair, deterministic and efficient platform for users to swap tokens and provide liquidity (future versions of the DEX will offer additional products). This whitepaper describes exactly how Cardax DEX works, highlighting its benefits over other DEXs in the Cardano ecosystem.

2. Decentralised Exchange (DEX) Background

2a. Automated Market Maker (AMM) DEXs

Unlike an exchange in traditional finance (an order book exchange), where buyers' orders are matched with those of sellers to complete the exchange/trade, an Automated Market Maker exchange uses algorithmically managed “liquidity pools”. The algorithm maintains the ratio of trading pairs to ensure liquidity is sufficient to allow trades to take place.

3. Cardax DEX V1

Cardax DEX is an AMM DEX on the Cardano blockchain. Version 1 (V1) of the DEX will allow token swaps and liquidity pools. Future versions will have yield farming, amongst other products, enabled.

4. Programming Languages on Cardano

4a. Plutus Tx

Plutus Tx is the native smart contract programming language for Cardano, it was developed by IOHK for use on Cardano. It is a Haskell based programming language and is used in the majority of Cardano smart contracts.

4b. Plutarch

Cardax DEX is built using the latest “Plutarch” programming language. Plutarch was developed in collaboration with MLabs to address the scalability and transaction throughput issue found by using the Plutus language (which the majority of other Cardano ecosystem projects use). Plutarch is a Haskell language but is 300% more **efficient** when it comes to both scalability and transaction throughput.

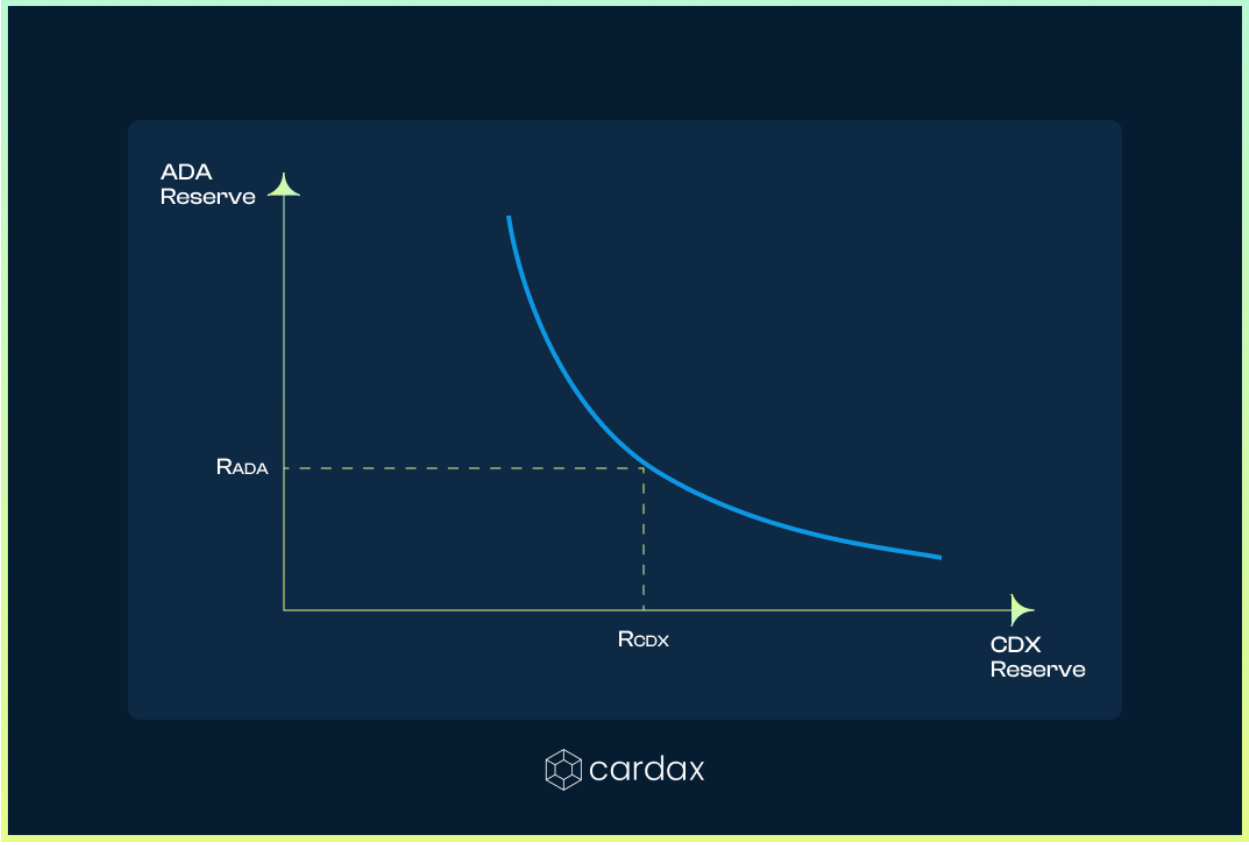
Cardax DEX is the first DEX on the Cardano blockchain to use only Plutarch (to date only one other DEX has used it for a very small part of their build).
By using Plutarch, we have future-proofed the Cardax DEX, meaning we will be able to scale much easier than other Cardano DEXs.

5. Constant Product Market Maker

Cardax DEX uses the Constant Product Market Maker for our liquidity pools. As with all liquidity pools, they consist of a token pair (e.g. ADA:CDX) held in a constant ratio.
This is expressed as x * y = k. Where x and y represent each token's reserve, and k is a constant (that must be maintained).

In the example given above, ADA and CDX have an inverse correlation in terms of reserve size. When the ADA reserve increases, the CDX reserve must decrease, and vice versa. Their reserves can be found anywhere along the curve in the diagram below.

ADA/CDX Inverse correlation within a liquidity pool



6. How Token Prices are Established in a Cardax Pool

A token's exchange price is determined by the reserve ratio.
When someone sells CDX tokens to the liquidity pool, he gets ADA tokens from the pool.
CDX's price to ADA is thus ADA/CDX.

The x * y = k should be respected, so $CDX \times ADA = (CDX + \Delta CDX) \times (ADA - \Delta ADA)$.
From the calculation, we get the price of CDX and ADA in each trade.

The liquidity pool's token reserve reflects market supply and demand, and the relation between supply and demand decides a token's value.

In simple terms, the higher a token's reserve volume, the lower the token’s price, and vice versa.

7. Cardax DEX Objective

By utilising our Streaming Merge algorithm Cardax DEX aims to provide fast and reliable transactions, whilst adhering to our three primary pillars:

- Deterministic
- Fair
- Efficient

8. Cardax DEX Protocol

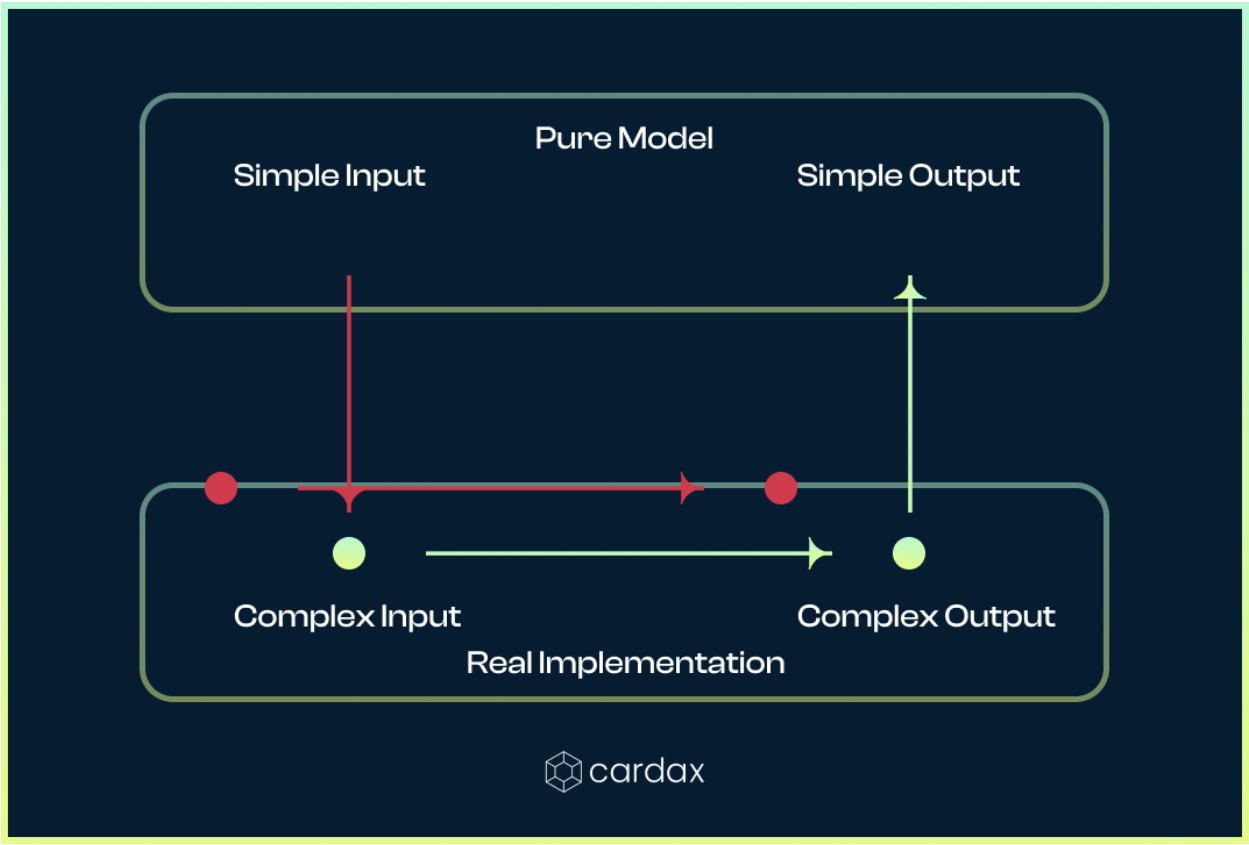
8a. Pure Model

Before the real implementation, we decided to implement a Pure Model of our new Streaming Merge protocol.

The Pure Model of our Streaming Merge algorithm is a simplified version of the real implementation: The simplified model focuses on the algorithm and protocol itself and leaves out the complexity which needs to be introduced because of the blockchain or any other external context (e.g. wallet) in a real implementation.

Our Streaming Merge Pure Model allows us to verify that the overall protocol design is correct and, on top of this, to write tests for invariants for the algorithm. The advantage, then, is that these invariants must also hold for the real implementation and therefore the tests for the Pure Model can be reused for the real implementation.

For applying the tests to the real model, the process is very well described by Duncan Coutts of Well-Typed in his "*Cardano Development Techniques*"[1] video: First, a simple input for the Pure Model is mapped to (is analogous to) a complex input for the complex model (the real implementation). Then both models process their input. The output of the complex model is mapped back to a simple model and compared with the result of the pure model. If the two outcomes are the same, the models are assumed to behave in the same way.



In essence, the Pure Model was extra work upfront, but has provided us with, not only an easy to access and clean version of the protocol, but will also pay off easily at a later stage when the already developed test suite can be re-used to verify the real implementation.

8b. Cardax Streaming Merge

The Streaming Merge algorithm is Cardax's solution to concurrency. By using the time at which an order was placed and random sorting of simultaneous orders, it enables the Cardax DEX to provide true decentralisation by being deterministic, fair and efficient.

When a user books their slot in a pool (*more on this below)*, they are given their own designated "lane", after which they can place an order.
Once the lane is booked, the user can place orders without waiting. The DEX will provide an estimated waiting time on the Web-App.

Their order details are then packaged as “sealed and opaque”; the only information that is available to the algorithm is the time the order was submitted, the rest is hidden (thus excluding any form of bias from the process).

The Streaming Merge algorithm then sorts the orders by time initiated.

However, when there are multiple orders submitted at a very similar time, blockchain limits make it difficult to determine the order they were placed (we refer to these as simultaneous orders), the Streaming Merge algorithm has to work out in what order the orders are processed.

The Streaming Merge algorithm randomly sorts the simultaneous orders. This keeps the whole process fair, as no user can predict the position of their order in the queue.

At this point, the DEX now knows the order in which all orders should be processed, and the lanes are then merged together into the correct order and executed.

Cardax DEX does not require third-party involvement (such as elected operators or batching bots*), merging will happen automatically when a user submits their order.
As no third party is financially incentivised and the order of transactions is known before orders are executed, Streaming Merge operates deterministically.

8c. Booking a Slot

Booking a slot simply means that a user submits their intention to make transactions in a liquidity pool. The Streaming Merge protocol gives each user an exclusive lane to make transactions in a liquidity pool without interruptions and contentions.
Once a slot is booked, the user has an exclusive lane to the pool and can place different orders: swap, add liquidity and withdraw liquidity.

8d. Cardax DEX Reduces Slippage

Slippage is the difference in a token's price between what the trader initially requested and the execution price. It is due to the price change between the time the order is submitted and the time when the order gets executed.

Cardax allows you to customize the slippage tolerance.

When the price is outside your slippage tolerance, your order will be rejected, and you will get your money back.

On Cardax DEX, slippage is even more contained than on other AMM DEXs because:

- **A pool can handle a greater number of parallel orders in a merge transaction,**
- **The merge transaction is executed within a limited duration of time.**

In essence, when a user submits an order, only a limited number of other orders may impact the token's price. It is more probable to have the executed price close to your requested price than in an open system.

8e. Tokenomics and Fees

Total supply: 1,000,000,000
Circulating supply: 30,000,000

Cardax B.V. currently holds the remaining supply of CDX tokens. Cardax will progressively put more CDX tokens in circulation. How much and when exactly is not disclosed. This token injection process will be done in a way that does not impact the price of the token negatively.

Traders pay fees to make a token swap on Cardax DEX. Each order has:

- **2 ADA flat fee. It goes to the Cardax B.V.**
- **0.3% trading fee on the swapped token. It goes to the liquidity providers.**
- **Cardano network fee for the transaction.**

Cardax B.V. is the company behind Cardax DEX. The funds collected will have multiple uses, including giving rewards, increasing liquidity on the DEX, DeFi education, community growth, marketing and future development.

9. Cardax DEX V1 - Key Features

- Pre-registration (Streaming Merge algorithm)
- Swap any Cardano Native token (CNT) for another CNT
- Create a liquidity pool
- Add liquidity to an existing pool
- Remove liquidity from a pool

Version 2 (coming in late 2022) of the Cardax DEX will provide yield farming and governance.

10. Why have we built Cardax on Cardano?

The choice to build our DEX on Cardano was for reasons threefold. Firstly, the research-first approach Cardano was very appealing as it fits very well with our own ethos of launching a product that works securely and efficiently straight out of the box.

Secondly, the Cardano community genuinely wants to make a difference in the world, especially for those who don't have access to traditional banking. This gives us the opportunity to work with lots of amazing projects who are making a real difference to those most in need.

Also, the fact that Cardano offers low transaction fees (compared to Ethereum) is crucial if we want to bring DeFi to those who are not currently part of the cryptocurrency ecosystem. After all, we are still very early and our ecosystem, while growing rapidly, is still extremely small compared with that of the traditional, fiat-based financial system.

References

1. **IOHK | Cardano development techniques, with Duncan Coutts, PhD**