# Cardax

A decentralized exchange, powered by the EAMM protocol, that aims to provide liquidity to projects that issue native tokens on Cardano.


Version 1.0.0

Author: Ryan Morrison

# Abstract

Decentralized 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 – a decentralized 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 Cardax system. The following section highlights the main advantages and disadvantages of the order book and automated market maker (AMM) – the two approaches used by DEXs to provide market prices. Then, we describe our protocol – the Extended Automated Market Maker (EAMM) – that, we argue, takes the best features from book orders and AMM to create a better trading experience for all users. We close the paper by highlighting the key features that make Cardax different from other DEXs, outline the system's development roadmap, and discuss some of the implications of a Cardano-based DEX.

# Content

# Introduction

Cardano does not yet have a decentralized exchange (DEX), which means tokens built on the Cardano network don't have a native exchange list. This will soon no longer be the case, as Cardax will be the native exchange that Cardano needs to provide liquidity to projects that create native assets. The Mary hard fork, completed on March 1st 2021, allowed anyone to build native assets on Cardano. This brings multi-asset support to Cardano, allowing users to create custom tokens and carry out transactions directly on the Cardano blockchain.

Cardano offers several tokenization options. The Mary hard fork allows the ledger's account infrastructure to provide transactions that carry several asset types simultaneously. Native support is an important advantage for developers, as they no longer need to use smart contracts for custom token creation or transactions. As such, the ownership and transfer of assets is tracked by the accounting ledger, removing extra complexity and potential for manual errors in a cost-efficient manner. More specifically, native tokens do not require smart contracts to transfer their value, which means users can send, receive, and burn their tokens without having to pay for smart contract transaction fees or adding event-handling logic to track transactions.

Applications of general purpose (fungible) or specialized (non-fungible) tokens include the creation of custom payment tokens, rewards for decentralized applications (DApps), stablecoins pegged to other currencies, and assets to represent intellectual property, among others. These assets can be traded, exchanged, and used as payment. On Cardano, tokens can be created, distributed, and exchanged in three ways: 1) Cardano command line interface (CLI); 2) token builder graphical user interface (GUI); and 3) the Daedalus wallet. The native token lifecycle consists of five phases: minting, issuing, using, redeeming, and burning. [1]

Using CLI requires familiarity with setting up and operating the Cardano node and experience in working with transactions and managing addresses and values. The GUI token builder makes token creation easier and allows creating tokens for DApps, tokenizing a property, creating NFT collector cards represented as specialized assets, and creating a stablecoin pegged to the value of other currencies. Finally, Daedalus and Yoroi wallets allow users to use existing tokens for payments and purchases or exchanges.

Teams can build DApps on Cardano by taking advantage of the features provided by the Mary hard fork along Goguen - smart contract on Plutus[2]. Plutus is a purpose-built smart contract development language and execution platform that uses the Haskell programming language. Plutus enables the use of Alonzo update -the final phase of Goguen in Cardano's roadmap.

[1] https://iohk.io/en/blog/posts/2021/02/18/building-native-tokens-on-cardano-for-pleasure-and-profit/
[2] https://developers.cardano.org/

The Alonzo hard fork brings native smart language to the Cardano blockchain. Alonzo adds many new opportunities for businesses and developers by allowing the development of DApps and smart contracts for decentralized finance (DeFi). Alonzo extends the simple multi-signature scripting language (multi-sig) used in Cardano Shelley by applying a systematic approach focused on formal methods and verification. With an update to the Plutus Core language, Multisig provides more efficient and stable scripting options.

The Alonzo ledger provides powerful scripting by implementing the extended unspent transaction output (EUTXO) accounting model. This implementation is made possible by using the hard fork combiner technology of IOHK and leads to smart contracts that allow efficient automated trading applications and large cash movements. Furthermore, developers have Cardano transactions validation experimentation tools to customize them. The APIs library will be expanded, allowing Plutus Core code to be deployed and operated while communicating with wallets and the ledger.

The Alonzo upgrade was preceded by the Daedalus update, which allows users to use their wallet as a single unified interface to receive both ADA and several other native tokens on the Cardano blockchain. The introduction of Daedalus marked the point from which all of the platform's stake pools are operated by community-led stake pool operators. [3]

[3] https://cointelegraph.com/news/cardano-s-upcoming-alonzo-smart-contract-update-takes-ada-to-new-highs

# Order Book vs Automated Market Maker (AMM)

Crypto exchanges usually provide market prices by relying on Order Book or Automated Market Maker (AMM)[4]. One cannot determine which of the two approaches is better without taking into consideration the type of tokens that will be served on the exchange.

With an order book, traders set buy and sell orders for an asset and then the order book organizes them by their prices, meaning assets can be traded as long as there is a supply and demand for it. The order book model works best when the exchange offers trading pairs that have high liquidity (e.g., BTC/ETH, ADA/USDT, BTC/BUSD). The majority of centralized exchanges use order books, including the biggest ones such as Binance, Bittrex or Coinbase. IDEX, a decentralized exchange for ERC-20 tokens, uses the order book model as well.

Order books work less effectively in an illiquid market, as finding a match for an order takes more time, which sometimes means one cannot escape volatility and large spread occur. Order books also allow market manipulation. For instance, speculators may be able to determine the direction in which an asset's price is moving from clues from the order book. For example, if a book hits a buy or sell wall, this suggests that traders are looking to buy or sell an asset, respectively). Some users provide false clues for the market and cause traders to make a wrong decision.

Switcheo is another example of an order book style DEX. After 4 years of launching, it has only 25,000 USD in daily volume and can be regarded as a bad experience for users who want to trade their assets. Because of low liquidity, users sometimes wait weeks for an order to be completed. At times, orders cannot be completed at all, as orders do not find a counterparty to trade with and remain open.

On the other hand, an AMM model, such as the one that Uniswap uses, suits better if the exchange offers mainly pairs with low liquidity. AMMs use a mathematical formula that takes into account the current level of liquidity of a trading pair and gives an instant quote to traders. In other words, while in the previously described model prices are provided by order books, in an AMM system the price is provided by an algorithm – which implies AMM markets act as uninformed.

The main advantage of an AMM system is that there will always be liquidity for otherwise illiquid markets — at least while there are enough people to invest in a liquidity pool. However, if there isn't enough liquidity around the desired price to fill a large market order, there could

[4] Capponi, A., & Jia, R. (2021). The Adoption of Blockchain-based Decentralized Exchanges: A Market Microstructure Analysis of the Automated Market Maker. *Available at SSRN 3805095*.

be a big difference between the price that you expect your order to fill and the price that it fills at – a difference referred to as slippage. This, together with impermanent loss- are the main disadvantages of an AMM system.

Slippage refers to the extent to which an order's size affects the price at which a token is bought or sold. Slippage will be low when the orders are small but rise exponentially with order size. For instance, an order taking up half of the liquidity pool will lead to a huge slippage that would double the token price. To prevent such events, the average order should take less than 1% of the liquidity pool, which is not always possible when using an AMM system.[5]

Projects that issue their own token come to a DEX to find liquidity. Although an AMM system allows them to create a new pair (e.g.Bobtoken/ADA), it also means they need to have enough capital to create a liquidity pool that is liquid enough so that they don't end up with a high slippage if a large order is executed. The bigger the collateral, the more liquid the pool becomes and lower slippage happens when bigger orders are executed.

Impermanent loss refers to the situations where users who provide liquidity to AMMs see their staked tokens lose value compared to simply holding the tokens on their wallets and occurs when the price of tokens inside an AMM diverge, with the size of the divergence being proportional to the size of the impermanent loss. While the loss is not permanent when the relative prices of tokens in the AMM return to their original state, it is more often the case that this does not occur and the loss is permanent.

Impermanent loss occurs because AMMs do not automatically adjust prices based on changes in the external market but require an arbitrageur to buy the underpriced asset or sell the overpriced asset in order to match the external markets. The profit extracted by the arbitrageur is taken from liquidity providers, which results in impermanent loss.

[5] https://thecontrol.co/a-comparison-of-decentralized-exchange-designs-1deef249f56a

## Getting the Best of the Two Worlds

The order Book model works best with highly liquid trading pairs while the AMM model works better for illiquid pairs as long as there is enough liquidity around a price to fill a large market order. We propose a system that gets the best of the two worlds, namely one that:

1. Allows anyone to become a market maker by either starting a liquidity pool or participating in an existing one.
2. Minimizes slippage.
3. Minimizes the risk of impermanent loss.
4. Provides more price transparency.
5. Allows token issuers to create a new pair without the need for a big amount of capital to serve as collateral.

## Extended Automated Market Maker (EAMM) Protocol

Cardax's EAMM protocol aims to be an improved version of the existing AMM protocols.

One of the problems of AMM is the relatively high barrier to entry. As an illustrative example, let's assume you are building a Cardano native token called Patiencetoken (PTT) and you want to create a market to be able to trade it against ADA. In order to create the pair ADA/PTT, you will have to provide both ADA and PTT.

Providing PTT is not a problem because you are the issuer (you can issue as many tokens as you want). A problem does occur when you have limited ADA, as this means you will end with a small, illiquid pool. Many small projects face this exact problem on Uniswap currently.

The EAMM protocol aims to solve problems of this nature by providing pricing power to takers when new pairs are created. In this scenario, makers no longer have any control over the price and the discovery mechanism relies solely on the takers. This is an option the protocol will give to people that create a new pair and don't want to put a large amount of capital. Ultimately, it is the new pair creator who decides if they want to take this option or not.

The EAMM protocol will allow anyone to create a liquidity pool. Liquidity Providers will be able to create a liquidity pool and/or to add liquidity to an existing pool.

There will be a 0.35% fee for swapping tokens, 0.30% will be split by liquidity providers proportional to their contribution to liquidity reserves. The remaining 0.05% will go to Cardax's

treasury. The protocol will distribute fees among liquidity providers and Cardax treasury. Liquidity providers will be paid in Cardax utility token, CDX.

## Governance

Cardax will manage a treasury based on IOG's paper: "A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence"[6], through its own Governance Tokens (CDX) in the same way they currently do with ADA. The Cardax DAO structure will be live from Day 1 on mainnet to ensure the future voting power within the protocol is effectively distributed amongst CDX token holders. This allows CDX token holders to vote and decide collectively on how the funds in the Cardax treasury should be allocated.

## Governance Distribution

The distribution of CDX tokens has been carefully designed to create a decentralized, community-driven DeFi protocol that is not controlled by a small group of actors.

---

6 https://iohk.io/en/research/library/papers/a-treasury-system-for-cryptocurrenciesenabling-better-collaborative-intelligence/

# Token economics & Vesting

The Cardax team has agreed upon a vesting schedule that will release CDX governance tokens to the core team and advisors after 2 years.

The tokens allocated for the Team (20%) and Advisors (5%) are locked in a smart contract that releases the tokens after a two-year period. The vesting period starts with the launch of Cardax Dex on mainnet.

- Total amount of CDX tokens: 1,000,000,000
- Percent of CDX tokens allocated to Team (+ future hires): 20%
- Percent of CDX tokens allocated to Advisors: 5%
- Total amount of CDX tokens vested: 250,000,000
- Length of vesting: 2 years

# What Makes Cardax Different to other DEXs?

DEXs typically rely on either order books or AMMs to provide market prices. Our team has been researching how to leverage the two models to provide the best trading experience on tokens that will be served on Cardax. By combining the best features of order books and AMM, we believe to have achieved a system that:

1. Allows users to become market makers by starting a liquidity pool or participating in an existing pool

2. Minimizes slippage

3. Minimizes the risk of impermanent loss

4. Provides more price transparency

5. Allows token issuers to create a new pair without the need of huge capital as collateral.

We end this section with a list of the key features of Cardax along with our road map, which should provide a global picture of what we are trying to accomplish with our decentralized system.

## Features

- Add support for any Cardano native token
- Join liquidity pools to collect fees on ADA - Cardano Native Tokens pairs
- Liquidity-sensitive automated pricing using EAMM protocol
- Trade ADA for any Cardano Native Token
- Trade any Cardano Native Token for any Cardano Native Token in a single transaction
- Trade and transfer to a different address in a single transaction
- Buy ADA or any Cardano Native Token from Yoroi wallet

# Roadmap

Our project consists of 6 phases, outlined below.

**1. Architecture + User Interface/ User Experience:**

- Developing system logic and the ‘must have’ features
- Creation of wireframes for each feature and page
- Designing the look and feel of the complete project
- Creating a functional demo of the front end

**2. EAMM Protocol**

**3. Backend Development**

**4. Security:**

- Documentation of potential security risks and prevention/mitigation approaches
- Implementation of Google Authentication, SMS authentication, anti-phishing system, and cloudflare to prevent DDoS attacks.

**5. Smart Contracts**

**6. Testing and Going Live**

# Conclusion

One of the main premises of blockchain technology is to develop decentralized systems where information and governance are shared. Decentralized 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. With the increasing adoption of Cardano and ongoing initiatives to support DeFi, a Cardano-based DEX will serve as an essential and powerful trading venue in the ecosystem.

Cardax is set to provide a secure way of connecting stakeholders while promoting equitable governance and involvement in the Cardano community. Cardax's use of the EAMM protocol highlights our belief that the best way to overcome the limits of order books and AMM is by using the best feature of the two systems within a new one while removing the limitations of each. As with other decentralized platforms, DEXs are still in their early years and will need further development of infrastructure, refinement of user experience, and improved scaling mechanisms to ensure future adoption.