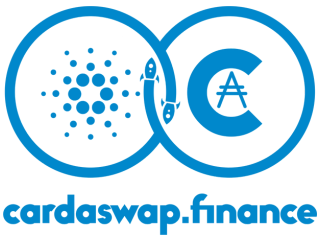


CardaSwap Finance

Abstract

This technical whitepaper clarifies some of the design decisions behind Cardaswap Protocol and the functionality of Its contracts.

CardaSwap is an automated market maker (AMM) / Decentralized exchange built for the Cardano blockchain.

Cardaswap Exchange allows participants of the blockchain to add liquidity and create a market pair for other users to exchange their native Cardano tokens. In return, traders pay a small fee and the liquidity providers earn a percentage of their deposit.

This whitepaper describes the mechanics of Cardaswap contracts including the token pair contract that stores liquidity providers' assets.

Introduction

The term “Decentralized Exchange” or DEX refers to an application that is accessible through a series of smart contracts running on a blockchain, which enables financial services where trustless parties can participate in a financial market, relying solely on the smart contracts to secure the transactions.

Each Cardaswap pair stores pooled reserves of two assets and provides liquidity for those two assets while maintaining the invariant that the product of the reserves cannot decrease.

Traders pay a fee on trades, which goes to liquidity providers. The contracts are non-upgradeable.

In addition to decentralizing access to financial services, a DEX also typically decentralizes profits from those services. Participants who provide the liquidity to create the market collect a small fee, creating a vehicle for passive income at returns usually reserved for large institutions and unheard of for the individual investor. Several successful DEXs have been built on existing blockchains like Uniswap and Curve on Ethereum and also PancakeSwap on the Binance Smart Chain.

CardaSwap is a DEX being built for a new blockchain, the Cardano blockchain.

The Cardano ecosystem is a new generation POS blockchain that is primarily focused on, among other things, proof of stake for throughput and energy efficiency which is estimated to be 1.6 million times more efficient than Bitcoin.

As this new ecosystem opens up and gets upgraded with more features, the users and projects that choose to build on the Cardano blockchain will have a great and pressing need for the financial services described above.

There’s however a major difference between Cardano Ecosystem and other blockchains that is worthy of mention in this paper.

The accounting model and virtual machine are dramatically different from those on other smart-contract enabled blockchains. Tokens are tracked as bundles of unspent outputs from previous transactions and can be locked with a validation script that determines under what conditions they can be spent.

Outline

The remainder of this paper is organized as follows:

- Section 2 gives an introduction to the principles of an “Automated Market Maker.”
- We describe a naive implementation of this scheme on the Cardano blockchain in Section 3.
- We detail a plan for enabling long-term protocol upgrades in Section 4.
- We discuss some promising opportunities for additional improvements in Section 5.
- Finally, Section 6 summarizes the work.

AMMS & Liquidity Pools

In a centralized exchange setting, an exchange like Binance acts as a central authority, maintaining an order book and matching buyers with sellers to facilitate the exchange of tokens or Crypto Assets. Because of the incredible potential, this entity has for manipulating the market for further profit, there is an immense amount of existing regulation in place to forestall the above-mentioned problems.

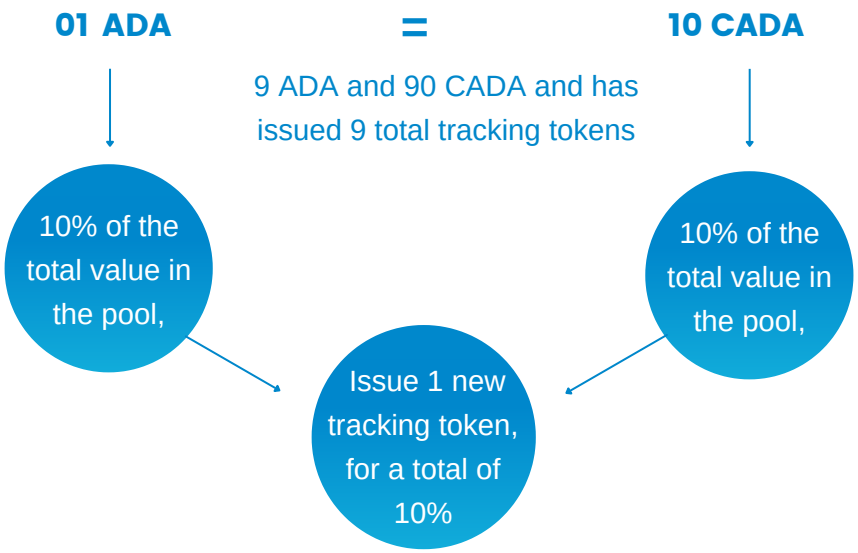
Initially, CardaSwap will provide an automated market maker that is an adaptation of the model popularized by Uniswap.

In such a model, the pricing and distribution of assets are satisfied by a mathematical formula or algorithm.

This section, then, will take some time to describe the Uniswap model.

In this model, liquidity providers (LP) deposit equal values of two crypto assets in a smart contract, and receive tracking tokens (LP Tokens) each representing their portion of the pool of assets.

ADA/CADA liquidity pool



For example, suppose an ADA/CADA liquidity pool has 9 ADA and 90 CADA and has issued 9 total tracking tokens to previous liquidity providers.

If a user deposits 1 ADA and 10 CADA, since those represent 10% of the total value in the pool, the smart contract issues 1 new tracking token, for a total of 10. That 1 token out of 10 entitles the liquidity provider to 10% of the pool's total assets, which equals 1 ADA and 10 CADA, as expected. The pool also allows "swaps" to happen: someone deposits one asset, and receives the other, according to the exchange rate of the pool. In the above example, if I deposit 0.1 ADA, I might expect to withdraw 1 CADA.

One useful analogy from classical finance to wrap your head around the notion of a liquidity pool is to think of it as an automatic ETF: A collection of securities traded and balanced against the market, of which you have small ownership.

How Do We Implement This On The Cardano Blockchain

Unlike the Ethereum Virtual Machine (EVM), The Cardano Blockchain, however, uses a novel approach to its accounting and execution model that is known as “Extended Unspent Transaction Outputs” (eUTXOs) which makes it not as straightforward as you might expect.

The Extended Unspent Transaction Outputs model implements smart contracts more “passively” than an explicit function call, which heavily discourages the use of the global state.

The Cardano Blockchain Model extends this in the following ways:

- The UTXO is equipped with an arbitrary datum
- The script/Contract locking the funds has access to input data which is also known as the “redeemer,” as well as the entire transaction

To Implement this, we will be utilizing a global “Cardaswap Pool Factory” with unique tokens which will be locked via a script that allows users to create specific “Asset Pair Liquidity Pool” unique tokens, ensuring that the asset pairs stay unique. Then, these unique tokens are always locked in an eUTXO alongside the liquidity stored in the pool, using a validator script that enforces the constraints of the pool:

How Do We Make This Work?

It will be made possible by a minting policy that allows tracking tokens to be minted so long as the appropriate liquidity is deposited.

The same minting policy will also allow tracking tokens to be burned so long as the appropriate liquidity is removed.

The validator script allows swaps to occur, so long as they respect the pricing function and Script fee structure.

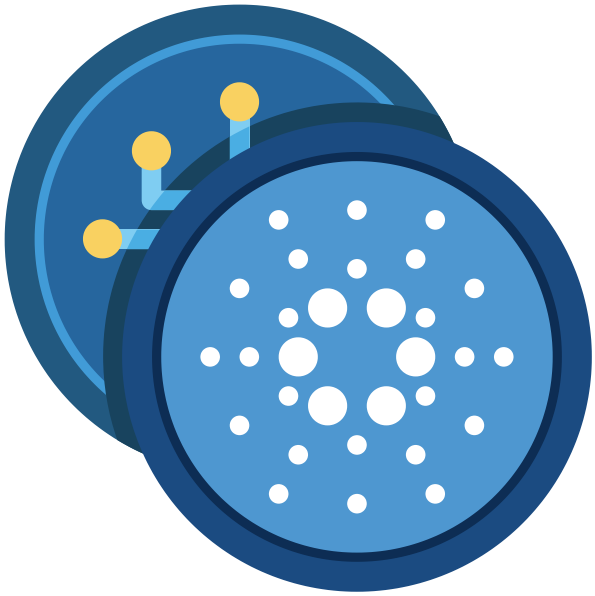
This model however is flawed greatly because any given eUTXO can only be spent once and as part of one transaction which makes it appear as only one swap can happen per block.

On the Cardano blockchain, there is roughly one block every 20 seconds. This would be appalling throughput for a decentralized exchange.

We will discuss our scaling solution in a subsequent whitepaper.

Future Upgrades

Given that the Cardano Blockchain is evolving quickly, There are a number of upgrades and extensions to the Cardaswap protocol that will be discussed in future whitepapers



Future Work

There are a number of extensions to the protocol above that we are finalizing the details on, and which will be discussed in future whitepapers

.

For example:

- The role of the CADA token
- A mechanism to increase throughput dramatically
- A mechanism to provide concentrated liquidity for more efficient market leverage
- A mechanism to provide secondary derivative markets
- A mechanism to further decentralize the role of the liquidity pool

Ending Notes

The Cardano blockchain is evolving at a fast pace with new and exciting improvements in terms of throughput, fees, energy efficiency.

The planned Alonzo Hard Fork which will be the advent launch of Smart Contracts later this year will bring about a huge surge in economic activity and utility of the Cardano Blockchain as more and more native tokens will be created to track and satisfy real-world value.

There will be an ever-increasing need to have decentralized markets to trade and acquire these tokens. The above model provides a simple, scalable solution to meet these early needs, well suited for the Cardano blockchain, and positions Cardaswap to expand into more efficient and more sophisticated protocols and instruments in the future.