uADA - Technical Report

TeddySwap

February 29, 2024

1 Introduction

See the medium article by TeddySwap for a longer explanation on the purpose of uADA.[1]

2 Functional Specifications

The uADA protocol is an approach to allow for users to exchange their ADA for a native token that is equivalent in value to ADA, but even when traded or exchanged still earns the holder the same staking rewards as the original ADA. ADA are locked in a spending contract together with a datum specifying the owner and with the owners stake key hash. The proper functioning of this protocol entails

- Ensuring that the amount of locked ADA in the spending contract is at all times equal to the amount of uADA in circulation.
- Ensuring that the owner of the uADA can at any time exchange their uADA for ADA at a 1:1 ratio.
- Ensuring that no third party can change the stake key of the locked ADA of another user or spend the locked ADA.
- The creation of a (ideally stableswap inspired) liquidity pool that allows for the exchange of ADA for the native token and vice versa to ensure the price pegging of the token.

As an additional feature, the spending of the locked ADA is controlled by the ownership of an NFT that is minted when the ADA is locked. This NFT can be used to perform actions on the locked ADA, such as exchanging it for uADA or moving it to another address. This allows selling the locked ADA to a third party without having to own the equivalent amount of uADA. The value of such an NFT is determined by the amount of locked ADA and the current price of uADA in the liquidity pool.

[1] `https://medium.com/@TeddySwapDEX/introducing-uada-a-unique-liquidity-provision-solution-e9f66834dd60`

2.0.1 Architecture

The uADA protocol is implemented as a smart contract on the Cardano blockchain. The contract is written in OpShin, a domain specific language for smart contracts on the Cardano blockchain. The contract supports being invoked by spending, minting and withdrawing transactions. The specific operations of each purpose are:

- Minting: The minting transaction controls the minting of uADA tokens.
- Spending: The spending transaction control that the ADA in the contract is only spent by the owner of the NFT.
- Withdrawing: The withdrawing transaction ensures the invariant that the amount of ADA in the contract is equal to the amount of uADA in circulation. It has to be present in every interaction (i.e. Spending and Minting) with the contract.

The liquidity pool is based on either the TeddySwap Decentralized Exchange Smart Contract [2] or the MinSwap StableSwap Smart Contract [3].

[2] https://github.com/teddy-swap/cardano-dex-contracts

[3] https://github.com/minswap/minswap-stableswap