dclex

Protocol Whitepaper

January 2025

Nicolas Martin
nicolas@dclex.com

Łukasz Wacławski
lukasz@dclex.com

Jelle Rijnink
jelle@dclex.com

Abstract

DCLEX is a non-custodial exchange that allows traders to swap tokenized stocks and/or cryptocurrencies at real-time market prices. The protocol contains multiple liquidity pools in which a stock is paired with the USDC. Operating as a peer-to-pool model, some participants first need to deposit both tokens in a pool to enable others to swap against this pool in both directions. Fees generated from swaps are distributed to liquidity providers and the protocol owner. Anyone can contribute liquidity to pools and earn a part of their swap fees.

Introduction

Finance is undergoing a profound shift as blockchain technology enables the tokenization of traditional assets like stocks, integrating them into the decentralized finance (DeFi) ecosystem. This breakthrough disrupts traditional finance (TradFi) by automating processes, reducing reliance on intermediaries, and granting individuals unprecedented control over their assets. This innovation shifts power back to individuals, opening opportunities that were previously reserved for a select class of investors.

This whitepaper introduces DCLEX, the first decentralized exchange that allows traders to seamlessly swap tokenized stocks and cryptocurrencies at real-time market prices, with instant settlement and without surrendering custody of their assets. With DCLEX, stock traders can now experience all the benefits of the blockchain and explore the DeFi with confidence for the first time. It represents a pivotal step in uniting TradFi with DeFi.

Overview

This paper describe DCLEX key components that ensure efficiency, transparency, and security:

- **Price Oracle:** Assets are priced according to the real-time market price of their underlying asset on traditional exchanges.
- **Liquidity Pools:** Each pool pairs a tokenized stock with USDC. Liquidity providers contribute both assets to these pools, earning a share of their swap fees.
- **Swaps:** Traders can swap assets with any trading pair, incurring a fee.
- **Dynamic Fees:** Swap fees adjust based on asset proportions in the pool, the size of the swap and its direction.
- **Protocol Fees:** A portion of swap fees is allocated to the protocol owner.
- **Permissioned Access:** Restricted to valid Digital Identity or Smart Contract Identity holders.

Price Oracle

The protocol is powered by the Pyth Network, an oracle solution delivering real-time financial price feeds aggregated from multiple trusted sources. DCLEX requires up-to-date data from Pyth to function, meaning tokenized stocks are not tradable outside of US market hours. Oracle fees are charged per update and are paid in the native currency of the blockchain, along with gas fees charged. Note that the USDC/USD price is an exception and is updated in a timely manner so that traders don't need to update it when they swap. Refer to the Pyth Network documentation for more information.

Liquidity Pools

The DCLEX protocol is composed of several liquidity pools that enable efficient and decentralized trading by acting as automated market makers (AMMs). Each pool pairs the USDC with a stock and is tied to the price feed of this stock (in USD). As a peer-to-pool system, liquidity pools require initial contributions from liquidity providers before trading can occur. Liquidity providers supply both assets to a pool, which then act as the counterparty for all trades.

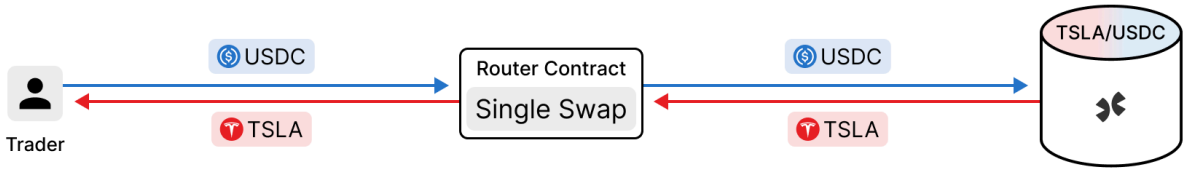
- **Adding Liquidity**: Liquidity providers deposit both assets in proportion to the pool's current composition and receive LP tokens representing their share of the pool.
- **Removing Liquidity**: Liquidity providers burn their LP tokens to withdraw both assets in the same proportion as the pool.

Swaps

The swap functionality represents the core value proposition of DCLEX, enabling efficient and seamless exchanges of tokenized stocks and cryptocurrencies. With a design focused on fair pricing, instant settlement and transparency, swaps ensure an intuitive and reliable trading experience.

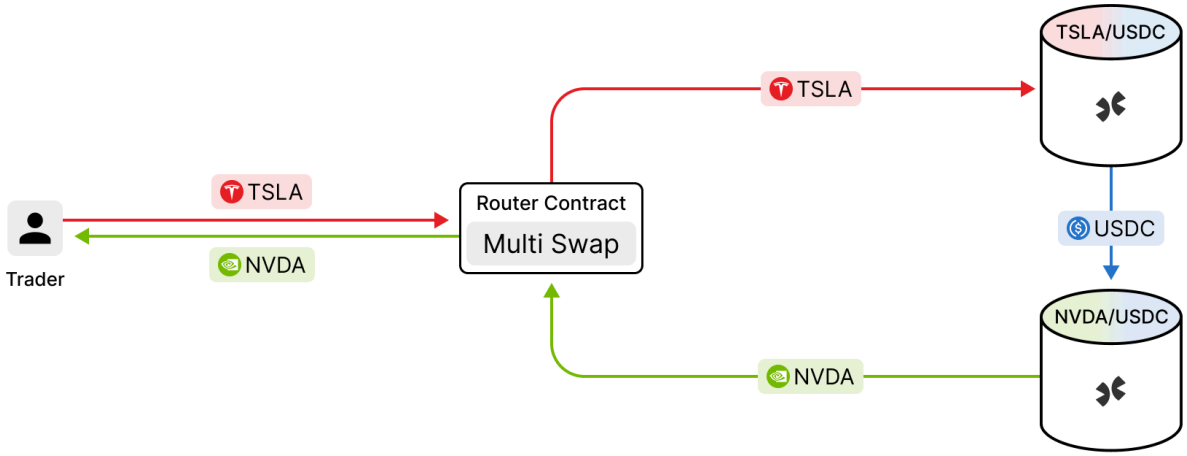
Single Swaps

Single swaps interact with a unique liquidity pool and, since every pool contains USDC, they always involve a direct exchange between a stock and USDC.



Multi Swaps

Multi swaps refer to the mechanism that enables the exchange of one asset for another, using USDC as an intermediary. The system first swaps the input asset for USDC and then swaps USDC for the desired output asset. Note that non-stock swaps are executed via Uniswap V4, ensuring deep liquidity and better pricing for traders. The multi swap process does not change the user experience; traders interact with the router contract as they would for single swaps. This ensures seamless exchanges between assets, even when no direct trading pair exists.

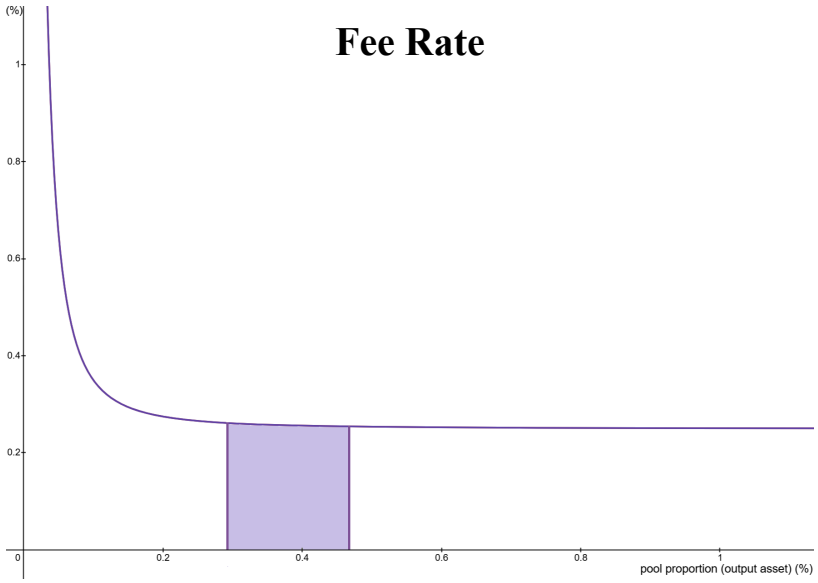


Dynamic Fees

In constant product AMMs like Uniswap, the price of each asset in the liquidity pool is the primary unknown variable. These algorithms rely on the ratio of tokens in the pool to determine asset prices, leaving pools vulnerable to arbitrage. This inefficiency forces liquidity providers to indirectly pay arbitrageurs to align pool prices with the market price, eroding their profits.

By integrating oracle price feeds into its core, DCLEX eliminates this inefficiency. It allows the protocol to accurately reflect the market prices of the underlying assets within the pool. This not only protects liquidity providers but also ensures fair pricing for traders. The fees associated with maintaining price feeds are a small cost compared to the cumulative losses LPs face in traditional AMM designs.

In DCLEX, prices are given by the oracle and the AMM is implemented in the dynamic fees structure. Each pool applies swap fees which are computed using the fee rate curve below and deducted from the transaction output:



Graphically, swap fees can be seen as the area under the curve between the pool proportions before and after the swap. Note that traders always swap toward the left as the *x-axis* represents the proportion of the asset leaving the pool.

Mathematically, swap fees are computed as the integral of the fee rate curve, evaluated between the pool proportions $before$ and $after$ the swap:

$$fee(\theta_{before}, \theta_{after}) = \int_{\theta_{before}}^{\theta_{after}} \left(\frac{0.001}{\theta^2} + 0.25 \right) \mathrm{d}\theta$$, where θ is the proportion of the output asset.

The unique shape of the curve is specially designed to provide nearly flat fees except when the pool is about to run out of liquidity in which case the curve increases sharply to infinity, thus preventing the pool from being drained from one asset. And, since they are computed as the integral of the curve, swap fees vary not only depending on the proportion of each asset in the pool but also on the size and direction of the swap.

Protocol Fees

Initially, 15% of swap fees is allocated to the protocol owner as compensation for facilitating swaps. This allocation incentivizes the ongoing development and maintenance of the protocol's infrastructure. The protocol owner can update the protocol fee rate by using the `setProtocolFeeRate` function and claim accumulated protocol fees by calling the `withdrawCollectedProtocolFees` function.

Permissioned Access

Tokenized stocks can only be transferred if the sender and the receiver hold a valid Digital Identity or Smart Contract Identity which are non-transferable NFTs that can only be minted by verified users and smart contracts, respectively. These NFTs act as permissions to use the protocol and its tokenized stocks. This permissioned framework not only enhances security by mitigating risks associated with anonymous usage but also ensures compliance with regulatory requirements. By implementing this system, DCLEX fosters a safe environment for all participants, while maintaining a user-friendly experience. Refer to the DCLEX Mint documentation for more information on tokenized stocks.