OneSwap

On-chain One-stop Trading Service Platform

OneSwap Team
2020.09.06

Contents

Abstract

The liquidity of digital assets and value discovery of blockchain have always been enabled by centralized exchanges. However, amid the bloom of digital assets, the audit token listing system of centralized exchanges has failed to meet the trading needs of the long tail market.

Demands for trading and liquidity from long-tail tokens gave birth to the decentralized exchange (DEX) that later has embraced another boom with increasing automated market makers in the DeFi field. However, even under such prosperity, problems such as poor user experience and limited transaction methods remain unsolved.

OneSwap introduces limit orders on the basis of DEX's permission-less currency listing and automated market making, and improves user experiences via its own OneSwap Wallet. As a universal on-chain one-stop trading service platform, OneSwap can be deployed on any blockchain that supports smart contracts.

I. The value flow of digital assets

The blockchain industry, originating from Bitcoin, is essentially part of the financial industry, and the exchange serves as its fundamental infrastructure providing functions of liquidity and value discovery. After more than ten years of development, the blockchain industry has embraced explosive growth in both the type and quantity of digital assets: from Bitcoin in the beginning to tens of thousands of digital assets including digital currencies, stable coins, and application tokens.

The audit system for token listing, pursued by the centralized exchange (CEX) which has long been the main solution for exchanges, proves incapable amid the rise in digital assets. Moreover, centralized exchanges have also been criticized for their high default risk, security risks, and opaque rules. Such an audit system and its centralized trust mechanism run counter to such core concepts as decentralization and trustlessness of the blockchain industry.

There is an old Chinese saying that goes, “you should attack the enemy by exploiting his weakness.” Players in the blockchain industry have been working hard to solve the shortcomings of centralized exchanges via the blockchain way. They also turn to the decentralized exchange (DEX) built on blockchain that allows permissionless token listing and trading for solutions to satisfy the trading needs of the long tail market in response to the proliferation of digital assets.

One may easily come up with the idea of building DEX-dedicated public chains, such as BitShares and CoinEx Chain. Although CoinEx Chain is similar to centralized exchanges in terms of transaction processing speed and confirmation time, DEX public chains like CoinEx Chain cannot connect and aggregate with more digital assets in a decentralized and trustless manner before the cross-chain technology further matures. At the moment and in the foreseeable future, CEX will still be the best cross-chain transaction solution, and DEX and CEX will complement each other.

The concept of programmable assets originating from Ethereum’s smart contract technology has largely increased the types and quantities of digital assets, contributing to a strong demand for DEX. Smart contract technology also comes as a new source of solutions for constructing DEX to reconstruct the digital asset trading market and satisfy the trading needs of the long tail market. In addition, considering the current development status of Ethereum, which is subject to low transaction processing speed and high transaction fees, the DEX public chain represented by CoinEx Chain still has much room for development.

II. DEX platform based on smart contract

Restricted by Ethereum's transaction processing speed and transaction fees, most of the order book-based DEX contracts that have emerged on Ethereum, such as Dex.top and IDEX, adopt off-chain matching and on-chain settlement strategy. Due to issues such as poor user experience and limited liquidity of funds, DEX based on the order book, with a small transaction volume, cannot rival its centralized counterparts.

Recently, automated market makers (AMM), represented by Uniswap and Balancer, have sprung up, ushering in the upsurge of decentralized finance (DeFi) and offering new ideas on the construction of contract-based DEX platforms. On the one hand, these DeFi projects revitalize users' idle digital assets and improve liquidity via the capital pool; on the other hand, they quickly process users' transaction requests with simple logic through the constant function market maker (CFMM). Despite problems such as impermanent loss and low capital interest rates faced by AMM projects, the continuous rise in the total locked value in the capital pool and the daily transaction volume of digital assets have proved the feasibility of AMM and users' recognition for it. There are even projects, for example, Kyber and 1Inch.-Exchange, that provide automatically optimal transaction path discovery service for users in the prosperous DeFi world.

Although the daily trading volume of the star project Uniswap in the AMM model has exceeded 100 million US dollars, in the absence of order book in the current automatic market maker, users cannot perform limit orders in the AMM project as they used to in the centralized exchange. Instead, they can only trade according to the market price given by the AMM at the time of the transaction. Yet realities show that the trading volume of ordinary users in centralized exchanges is mainly settled with limit orders, or in other words, limit orders have become an indispensable part of users' trading activities. The lack of order book will also cause greater slippage in the CFMM model when processing large transactions, which will hinder users' enthusiasm for trading.

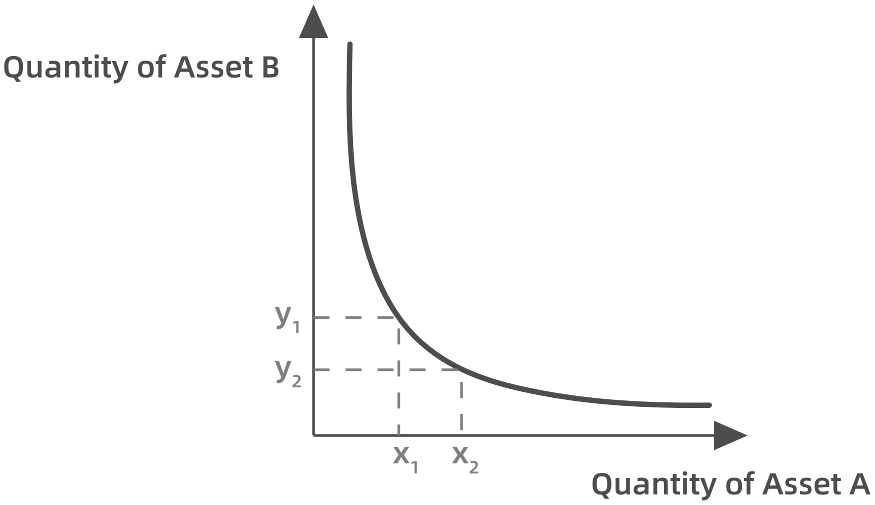
III. OneSwap, an on-chain one-stop trading service platform

Based on the permissionless listing of DEX, OneSwap, an on-chain one-stop trading service platform, draws on good practices of the AMM projects, and introduces the on-chain order book on the basis of the CFMM model to improve the trading experience for AMM users. The combination of the CFMM model and the on-chain order book not only provides users with a familiar way of trading limit orders, but also enhances the liquidity of digital assets. OneSwap is committed to solving the transaction and liquidity issues of long-tail tokens while ensuring security and decentralization using DEX. In addition, with the help of the well-designed interactive interface and one-click currency issuance tools in the OneSwap Wallet that comes with the platform, it provides users with a one-stop trading experience.

Having fully examined the various CFMM models in current AMM projects, OneSwap adopts the Constant Product Market Maker (CPMM) model in the Uniswap project. In a transaction scenario involving only two tokens, CPMM is more concise and versatile than models such as Constant Sum Market Maker (CSMM) and Constant Mean Market Maker (CMMM).

OneSwap supports all transactions between tokens that meet specific standards. It requires no permission to create a market or charges any fees for token listing. Under the CPMM model, it can be expected that when each rational liquidity provider creates a capital pool of two assets, he or she will inject into the pool an appropriate amount of the two assets following the current market price. For example, when the exchange rate between ETH and USDT is 350 USDT per ETH, the injections into the capital pool will be subject to that ratio, say, 10 ETH versus 3500 USDT. OneSwap users can inject liquidity into OneSwap's trading pair capital pool with their idle digital assets and earn transaction fees as liquidity providers. Each fund pool in OneSwap has a corresponding equity token, and users who inject liquidity into the pool will receive the corresponding equity token as proof of equity to withdraw funds.

In every response to the exchange transaction request, the capital pool will maintain the product of the two token quantities, x and y, in the pool as a constant: $x* y = k$. Assume the number of the two tokens in the pool before and after an exchange transaction are x1, y1 and x2, y2, respectively, then CPMM guarantees: $x1 * y1 = x2 * y2$. It is worth mentioning that such equality only occurs when no transaction fee is charged. With a transaction fee, k in the CPMM model will continue to increase as the fee accumulates. In addition, the absolute value of k will keep changing with the injection and outflow of liquidity.

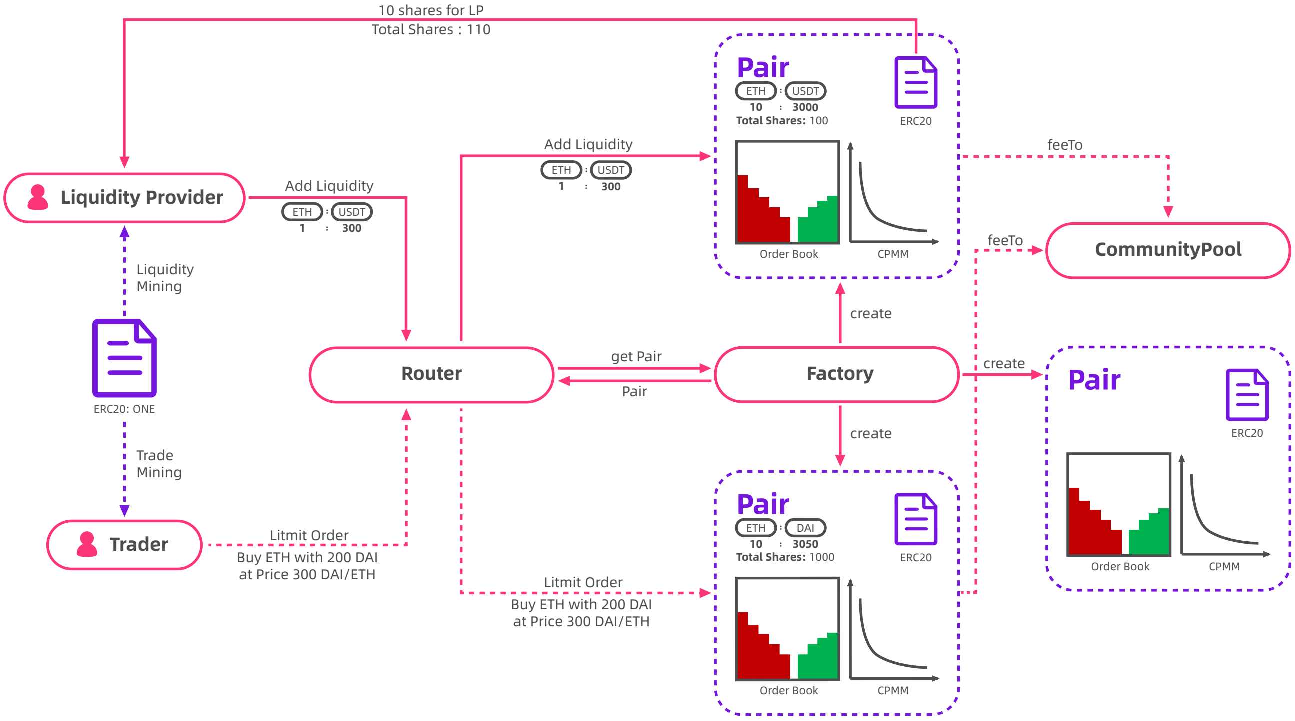


OneSwap users can either initiate market order transactions or limit order transactions. When processing a market order, the Pair contract will compare the optimal price in the order book with the AMM price, and try to fulfill the transaction request at the optimal price. The market order that cannot be traded is further processed in time through the CPMM model, and the qualified limit order is processed in time upon the price fluctuation of CPMM. The unfilled order is temporarily saved to the on-chain order book and will be processed later.

OneSwap is a universal on-chain one-stop trading service platform that can be implemented and deployed on any blockchain that supports smart contracts. The OneSwap team plans to implement and deploy the trading platform on Ethereum first. To facilitate on-chain governance and encourage community development, OneSwap on Ethereum will issue governance tokens for liquidity mining, transaction mining, and on-chain governance voting.

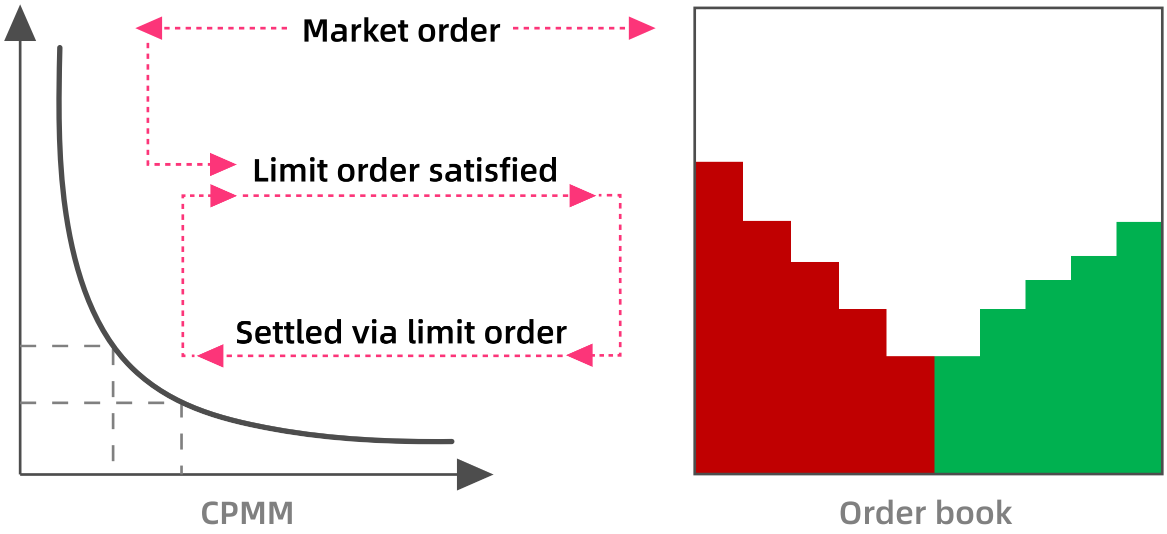
IV. OneSwap architecture design

OneSwap deployed on each blockchain platform contains a series of capital pools that are referred to with the transaction pair contract. Each Pair contract consists of three parts: 1) On-chain order book, which stores limit orders that cannot be fulfilled in time; 2) CPMM model: constant product market maker, which provides liquidity for the Pair contract; and 3) equity tokens that record a liquidity provider's privileges. The OneSwap architecture on Ethereum is shown in the figure below, where equity tokens are tokens that comply with the ERC20 standard.



When the liquidity provider injects digital assets into the capital pool of the Pair contract, the Pair contract will mint new equity tokens for the liquidity provider based on the current size of the pool, the total amount of equity tokens that have been issued, and the current injections. When the liquidity provider wants to retrieve his or her funds, the Pair contract will return to the liquidity provider the funds according to the corresponding proportion of the equity tokens in the total, and burn those equity tokens.

Each Pair contract is created on-demand by the Factory contract. For users' convenience, OneSwap also provides a Router contract, which receives all transactions, as a communication bridge between users and the Pair contract. Every time a user injects funds for a new trading pair, the Router contract will instruct the Factory contract to create a new Pair contract for the trading pair. OneSwap allows the user to specify the exchange path of the transaction. The user sends the exchange path to the Router contract, and the Router will complete the exchange following the path provided by the user according to the Pair contract address stored in the Factory contract.



As mentioned earlier, each Pair contract supports both market orders and limit orders. When processing a market order, the Pair contract will compare the optimal price in the order book with the AMM price, and try to fulfill the transaction request at the optimal price. Since each transaction will cause the price of CPMM to fluctuate, whenever the price fluctuates to the price of the pending limit order, the Pair contract will try to process the limit order in the order book. Limit orders that cannot be executed immediately are temporarily stored in the order book of the Pair contract.

The on-chain order book always raises concerns about excessive gas consumption, especially under the premise that gas prices remain high due to the current congestion of the Ethereum network. Through the in-depth optimization of the Pair contract, OneSwap manages to control the gas consumption of the transaction at the same level as in Uniswap V2, and may cost even less in certain circumstances. This is partly due to the data structure carefully organized by the OneSwap development team and partly because it fails to provide flash swap and on-chain price oracle provided by Uniswap V2. These functions consume more gas besides enhancing the functions of Uniswap.

V. OneSwap incentives and governance

To facilitate on-chain governance, OneSwap deployed on Ethereum will issue an ERC20 governance token called ONES which enables ownership transfer and a blacklist mechanism. Its total amount is constant at 100 million, and 11% is for initial circulation. All these tokens are to be distributed and circulated as follows.

Distributed to	Percentage	Main Usage	Initial Circulation	Unlocking Method and Cycle
Rewards for initial mining	5%	For miners participating in the initial mining	5%	Wholly unlocked
Rewards for forward mining	45%	Mainly for the new liquidity mining schemes to be launched in the future, community construction and promotion, project partnership, etc. Details in the release of forward mining rewards are decided by the community voting, including the time of release, mining market, and shares released.	0%	Unlocked on demand by community voting
Project operation and maintenance	25%	To keep the network secure and maintain project functions	2.5%	Unlocked in 9 times in four and a half years, with 2.5% unlocked every half a year
Strategic investment institutions	15%	Distributed to long-term strategic investment institutions of the project	1.5%	Unlocked in 9 times in four and a half year, with 1.5% unlocked every half a year
Team incentives	5%	For the core team and future employees	1%	Unlocked in four times in 2 years, with 1% unlocked every half a year
Early investors	5%	For early investors and early liquidity providers	1%	Unlocked in 4 times in 2 years, with 1% unlocked every half a year

The forward mining rewards are mainly set to support liquidity mining, transaction mining, community construction and development, promotion and publicity events, project partnership, etc. These rewards are governed on chain; rewards for project operation and maintenance are used for the development, testing, security audit, and network maintenance of OneSwap Contracts, Dapps, wallets and other applications; rewards for the initial mining are set to encourage users to join in liquidity mining and transaction mining in the initial stage of OneSwap launch, and all users who have injected liquidity into or trade with the fund pool will have the opportunity to be rewarded with ONES.

Users can initiate proposals and vote on the proposals in the community as a way of on-chain governance. Those with a sufficient number of ONES (more than 1% of the total tokens) can initiate proposals, and any user holding ONES can vote for or against a proposal. The voting lasts for three days, with one token for one vote. After the voting, the proposals receiving more positive votes than the negative are passed.

The voting process is uniformly managed by the governance contract. For proposals passed by voting, the governance contract automatically performs corresponding operations on the chain. Currently, OneSwap supports four types of proposals: plain-text proposals, proposals on community fund spending, proposals on transaction fee rate modification, and proposals on Pair contract upgrade. The plain-text proposals are for initiating community opinion surveys only.

To make the OneSwap project more transparent and credible, the ONES as part of the forward mining rewards are in custody of the governance contract, while the ONES that need to be linearly unlocked on time are managed by the lock-up agreement. After ONES are created, 11% for initial circulation will be transferred to the specific address by the aforementioned proportions, 45% to the governance contract, and 44% to the lock-up agreement.

A proposal on community construction spending is required to apply for financial support, in which the number of tokens applied should be specified. ONES holders vote for or against the proposal according to the fund usage stated by the applicant. If the proposal is voted to be passed, the applicant can obtain ONES from the governance contract.

OneSwap charges the Taker a fixed percentage of transaction fees based on the transaction amount, while Maker does not need to pay. The transaction fees generated in the Pair contract are divided into two parts: 60% that directly goes to the liquidity provider, and 40% to repurchase and burn ONES. ONES is a deflationary token in that it is repurchased and burned automatically by the token repurchase contract.

To follow market dynamics, OneSwap allows the modification of transaction fee rates within a certain range. To change it, users should initiate a proposal in which the value should be specified. After the proposal is voted to be passed, the governance contract updates OneSwap's transaction fee rate based thereupon.

The agency model adopted in OneSwap contracts not only saves a lot of gas when OneSwap trading pairs are created, but also makes it possible to upgrade the logic of the Pair contract. After a proposal is voted to be passed through the on-chain governance process, the governance contract can upgrade the logic of the Pair contract.

VI. OneSwap development plan

The OneSwap team plans to take the lead in implementing and deploying OneSwap on Ethereum, and then deploy it on TRON. It will keep an eye on the development of public chains of smart contracts and deploy OneSwap on mature ones in due course.

All OneSwap contract codes will be reviewed by top security agencies to ensure the security. In addition to considerate mechanism design and secure contracts implementation, a good user experience also matters for the operation of any DeFi project. In order to improve the user experience, the OneSwap team has worked hard on wallet support, interaction design, token management, and transaction services.

To make itself more accessible, OneSwap comes with a wallet. Through OneSwap Wallet, users can quickly access OneSwap without relying on any third-party tools. With abundant market data and the simple and clear trading interface design, OneSwap Wallet is committed to providing users with a better trading experience. It also supports C2C transactions of fiat money, making it a platform of one-stop transaction services.

To further lower the technical barrier of token issuance, OneSwap Wallet has a built-in one-click token issuance tool. With its help, users only need to fill in the name of the token to be issued, the total amount, whether to support additional issuance, burning, freezing, and other options to create a token contract on the chain.

In addition to the basic features, OneSwap Team will closely stir its attention on the DeFi development and support extra DeFi protocol in OneSwap Wallet in time. Based on the Wallet, OneSwap aims to become the entry of the future DeFi world.