DaoSwap White Paper

DaoSwap Community

1, Abstract

More than a decade has passed since the introduction of what we know today as blockchain technology. Over that time,the promise of what the technology could offer businesses and industries has evolved from a cryptocurrency payment platform to something bigger, game-changing, and truly disruptive. In recent years, we have seen sentiment about blockchain's potential similarly evolving, along with companies directing actual investment dollars toward applications.
More and more organizations clearly view blockchain as a top priority, edging up to 55% of respondents (versus 53% in 2019 and 43% in 2018).
Two such industries reformed by the blockchain technology at the first place are investment and finance. Decentralized structures like blockchain will be the gold standard for investment and will undoubtedly bring revolutions in the traditional finance system existing in the market today. DeFi (Decentralized Finance) will make a game-changing impact on different economic dimensions of the world.
The most popular domain of DeFi is Decentralized Exchange (DEX), while the more advanced type of DEX is Automatic Market Maker (AMM).

2, Background

Goals and Vision

The ultimate goal of DaoSwap is to provide an efficiency AMM mode decentralized exchange platform.
DaoSwap envisions the huge growth of decentralized finance in the current market and in the near future. The goal is to serve people by outdating the drawbacks of centralized traditional finance ecosystems and provide ultimate liquidity for Token Ecosystems.

Tokenomics

As KK mentioned "The true value of a corporation in digital world is its digital asset". While digital asset is only valuable when it can be traded, to be able to be traded the asset has to be tokenized as a standard Token.
Token will be the infrastructure of new digital economy in Web 3.0.

Liquidity

In tradition centralized exchange or decentralized exchange which used order book mode, new projects and market is born lack of liquidity. It cost a lot of centralized effort to build the depth of the market, both for money and man effort.

DaoSwap

DaoSwap is the leading example of AMM mode to break this situation, optimized and upgraded Uniswap algorithm to a protocol for automated token exchange on Ethereum. It is designed around ease-of-use, gas efficiency, censorship resistance, and zero rent extraction. It is useful for traders and functions particularly well as a component of other smart contracts which require guaranteed on-chain liquidity.

Team

DaoSwap is a team of technical and finance experts who work together with the motive of offering the best possible services in the arena of AMM DEX.

3, Brief Introduction

DaoSwap is a protocol for automated token exchange on Ethereum. It is useful for traders and functions particularly well as a component of other smart contracts which require guaranteed on-chain liquidity.
Most exchanges maintain an order book and facilitate matches between buyers and sellers. DaoSwap smart contracts hold liquidity reserves of various tokens, and trades are executed directly against these reserves. Prices are set automatically using the constant product (x*y=k) market maker mechanism, which keeps overall reserves in relative equilibrium. Reserves are pooled between a network of liquidity providers who supply the system with tokens in exchange for a proportional share of transaction fees.
The decentralized applications (DApps) by DaoSwap are initialized or built on the Ethereum blockchain, a distributed ledger. This will lead to the exclusion of the influence of unauthorized persons. The copy of transaction details and investment data is available in every node on the blockchain that is present in the nooks and corners of the world. This will eliminate forced shutdown or censorship of the DaoSwap system. And also, an important thing to note is since investment details are distributed among thousands of users(nodes) there is no possible way to tamper your data. If anyone needs to modify, the data in every single node has to be overwritten which is practically impossible. This is why DaoSwap is secured over the traditional investment systems.

Decentralized and Open Source

All source code are open sourced, all smart contract on chain, there is no server, no data storage, no chance to perpetrate. DaoSwap is governance by community, no one has privilege.

Secure and no found trust

All core integration like order match and clear are all on chain, thre is no fund trust, no registration, all ETH wallet can trade from peer to peer. Complete safe, all rights are owned by end users. DaoSwap just provided a platform for them.

Liquidity mining

Provide liquidity to the pool is mining for the pool swap fees and DOI, this is designed to incent Liquidity Providers (LP) to keep providing liquidity to the

pool.

0 cost to start a project

Everyone can start a pool by providing a pair of ERC-20 token, no extra charge.

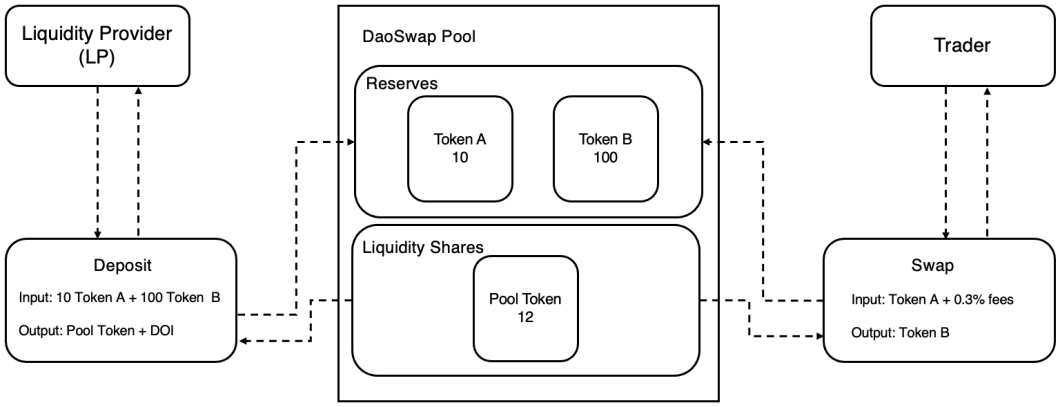
0 commission charge

DaoSwap does not charge any fees, all fees were rewarded to liquidity provider

AMM

Automatic Market Maker (AMM) mode automatically provide unlimited liquidity

4, How DaoSwap works



DaoSwap is an *automated liquidity protocol* powered by a constant product formula and implemented in a system of non-upgradeable smart contracts on the Ethereum blockchain. It obviates the need for trusted intermediaries, prioritizing **decentralization**, **censorship resistance**, and **security**. DaoSwap is **open-source software** licensed under the GPL.

Each DaoSwap smart contract, or pair, manages a liquidity pool made up of reserves of two ERC-20 tokens.

Anyone can become a liquidity provider for a pool by depositing an equivalent value of each underlying token in return for pool tokens. These tokens track pro-rata LP shares of the total reserves and can be redeemed for the underlying assets at any time.

Pairs act as automated market makers, standing ready to accept one token for the other as long as the “constant product” formula is preserved. This formula, most simply expressed as `x * y = k`, states that trades must not change the product (`k`) of a pair’s reserve balances (`x` and `y`). Because `k` remains unchanged from the reference frame of a trade, it is often referred to as the invariant. This formula has the desirable property that larger trades (relative to reserves) execute at exponentially worse rates than smaller ones.

In practice, DaoSwap applies a 0.30% fee to trades, which is added to reserves. As a result, each trade actually increases `k`. This functions as a payout to LPs, which is realized when they burn their pool tokens to withdraw their portion of total reserves. In the future, this fee may be reduced to 0.2%, with the remaining 0.1% withheld as a protocol-wide charge as further incentive.

Because the relative price of the two pair assets can only be changed through trading, divergences between the DaoSwap price and external prices create arbitrage opportunities. This mechanism ensures that DaoSwap prices always trend toward the market-clearing price.

5, Ecosystem Participants

The DaoSwap ecosystem is primarily comprised of three types of users: liquidity providers, traders, and developers. Liquidity providers are incentivized to contribute ERC-20 tokens to common liquidity pools. Traders can swap these tokens for one another for a fixed 0.30% fee (which goes to liquidity providers). Developers can integrate directly with DaoSwap smart contracts to power new and exciting interactions with tokens, trading interfaces, retail experiences, and more.

In total, interactions between these classes create a positive feedback loop, fueling digital economies by defining a common language through which tokens can be pooled, traded and used.

Liquidity Providers

Liquidity providers, or LPs, are not a homogenous group:

- Passive LPs are token holders who wish to passively invest their assets to accumulate trading fees.
- Professional LPs are focused on market making as their primary strategy. They usually develop custom tools and ways of tracking their liquidity positions across different DeFi projects.
- Token projects sometimes choose to become LPs to create a liquid marketplace for their token. This allows tokens to be bought and sold more easily and unlocks interoperability with other DeFi projects through DaoSwap.
- Finally, some DeFi pioneers are exploring complex liquidity provision interactions like incentivized liquidity, liquidity as collateral, and other experimental strategies. DaoSwap is the perfect protocol for projects to experiment with these kinds of ideas.

Traders

There are a several categories of traders in the protocol ecosystem:

- Speculators use a variety of community-built tools and products to swap tokens using liquidity pulled from the DaoSwap protocol.
- Arbitrage bots seek profits by comparing prices across different platforms to find an edge. (Though it might seem extractive, these bots actually help equalize prices across broader Ethereum markets and keep things fair.)
- DAPP users buy tokens on DaoSwap for use in other applications on Ethereum.
- Smart contracts that execute trades on the protocol by implementing swap functionality (from products like DEX aggregators to custom Solidity scripts).

In all cases, trades are subject to the same flat fee for trading on the protocol. Each is important for increasing the accuracy of prices and incentivizing liquidity.

DaoSwap Team and Community

The DaoSwap team along with the broader DaoSwap community drives development of the protocol and ecosystem.

6, Swaps

Token swaps in DaoSwap are a simple way to trade one ERC-20 token for another.

For end-users, swapping is intuitive: a user picks an input token and an output token. They specify an input amount, and the protocol calculates how much of the output token they'll receive. They then execute the swap with one click, receiving the output token in their wallet immediately.

In this guide, we'll look at what happens during a swap at the protocol level in order to gain a deeper understanding of how DaoSwap works.

Swaps in DaoSwap are different from trades on traditional platforms. DaoSwap does not use an order book to represent liquidity or determine prices. DaoSwap uses an automated market maker mechanism to provide instant feedback on rates and slippage.

As we learned in Protocol Overview, each pair on DaoSwap is actually underpinned by a liquidity pool. Liquidity pools are smart contracts that hold

balances of two unique tokens and enforces rules around depositing and withdrawing them.

This rule is the constant product formula. When either token is withdrawn (purchased), a proportional amount of the other must be deposited (sold), in order to maintain the constant.

7, Pools

Each DaoSwap liquidity pool is a trading venue for a pair of ERC20 tokens. When a pool contract is created, its balances of each token are 0; in order for the pool to begin facilitating trades, someone must seed it with an initial deposit of each token. This first liquidity provider is the one who sets the initial price of the pool. They are incentivized to deposit an equal *value* of both tokens into the pool. To see why, consider the case where the first liquidity provider deposits tokens at a ratio different from the current market rate. This immediately creates a profitable arbitrage opportunity, which is likely to be taken by an external party.

When other liquidity providers add to an existing pool, they must deposit pair tokens proportional to the current price. If they don't, the liquidity they added is at risk of being arbitraged as well. If they believe the current price is not correct, they may arbitrage it to the level they desire, and add liquidity at that price.

Pool tokens

Whenever liquidity is deposited into a pool, special tokens known as *liquidity tokens* are minted to the provider's address, in proportion to how much liquidity they contributed to the pool. These tokens are a representation of a liquidity provider's contribution to a pool. Whenever a trade occurs, the 0.3% fee which is levied is distributed *pro-rata* to all LPs in the pool at the moment of the trade. To receive the underlying liquidity back, plus any fees that were accrued while their liquidity was locked, LPs must burn their liquidity tokens.

Liquidity providers can also choose to sell, transfer, or otherwise use their liquidity tokens in any way they see fit.

Why pools?

DaoSwap is unique in that it doesn't use an order book to derive the price of an asset or to match buyers and sellers of tokens. Instead, DaoSwap uses what are called Liquidity Pools.

Liquidity is typically represented by discrete orders placed by individuals onto a centrally operated order book. A participant looking to provide liquidity or make markets must actively manage their orders, continuously updating them in response to the activity of others in the marketplace.

While order books are foundational to finance and work great for certain use cases, they suffer from a few important limitations that are especially magnified when applied to a decentralized or blockchain-native setting. Order books require intermediary infrastructure to host the orderbook and match orders. This creates points of control and adds additional layers of complexity. They also require active participation and management from market makers who usually use sophisticated infrastructure and algorithms, limiting participation to advanced traders. Order books were invented in a world with relatively few assets being traded, so it is not surprising they aren't ideal for an ecosystem where anyone can create their own token and those tokens usually have low liquidity. In sum, with the infrastructural trade-offs presented by a platform like Ethereum, order books are not the native architecture for implementing a liquidity protocol on a blockchain.

DaoSwap focuses on the strengths of Ethereum to reimagine token swaps from first principles.

A blockchain-native liquidity protocol should take advantage of the trusted code execution environment, the autonomous and perpetually running virtual machine, and an open, permission less, and inclusive access model that produces an exponentially growing ecosystem of virtual assets.

It is important to reiterate that a Pool is just a smart contract, operated by users calling functions on it. Swapping tokens is calling `swap` on a Pool contract instance, while providing liquidity is calling `deposit`.

Just how end-users can interact with the DaoSwap protocol through the Interface (which in turn interacts with the underlying contracts), developers can interact directly with the smart contracts and integrate DaoSwap functionality into their own applications without relying on intermediaries or needing permission.

8, Fees

Liquidity provider fees

There is a 0.3% fee for swapping tokens. 0.2% is split by liquidity providers proportional to their contribution to liquidity reserves. 0.1% is split by all TOI holders according to the number of tokens they hold.

Swapping fees are immediately deposited into liquidity reserves. This increases the value of liquidity tokens, functioning as a payout to all liquidity providers proportional to their share of the pool. Fees are collected by burning liquidity tokens to remove a proportional share of the underlying reserves.

Since fees are added to liquidity pools, the invariant increases at the end of every trade. Within a single transaction, the invariant represents `token0_pool / token1_pool` at the end of the previous transaction.

9, Pricing

How are prices determined?

As we learned in Protocol Overview, each pair on DaoSwap is actually underpinned by a liquidity pool. Liquidity pools are smart contracts that hold balances of two unique tokens and enforces rules around depositing and withdrawing them. The primary rule is the constant product formula. When a token is withdrawn (bought), a proportional amount must be deposited (sold) to maintain the constant. The ratio of tokens in the pool, in combination with the constant product formula, ultimately determine the price that a swap executes at.

How DaoSwap handles prices

In DaoSwap V1, trades are always executed at the “best possible” price, calculated at execution time. Somewhat confusingly, this calculation is actually accomplished with one of two different formulas, depending on whether the trade specifies an exact *input* or *output* amount. Functionally, the difference between these two functions is miniscule, but the very existence of a difference increases conceptual complexity. Initial attempts to support both functions in V2 proved inelegant, and the decision was made to **not provide**

any pricing functions in the core. Instead, pairs directly check whether the invariant was satisfied (accounting for fees) after every trade. This means that rather than relying on a pricing function to *also* enforce the invariant, V2 pairs simply and transparently ensure their own safety, a nice separation of concerns. One downstream benefit is that V2 pairs will more naturally support other flavors of trades which may emerge, (e.g. trading to a specific price at execution time).

At a high level, in DaoSwap V2, *trades must be priced in the periphery*. The good news is that the library provides a variety of functions designed to make this quite simple, and all swapping functions in the router are designed with this in mind.

Pricing Trades

When swapping tokens on DaoSwap, it's common to want to receive as many output tokens as possible for an *exact input amount*, or to pay as few input tokens as possible for an *exact output amount*. In order to calculate these amounts, a contract must look up the *current reserves* of a pair, in order to understand what the current price is. However, it is *not safe to perform this lookup and rely on the results without access to an external price*.

Say a smart contract naively wants to send 10 DAI to the DAI/WETH pair and receive as much WETH as it can get, given the current reserve ratio. If, when called, the naive smart contract simply looks up the current price and executes the trade, it is *vulnerable to front-running and will likely suffer an economic loss*. To see why, consider a malicious actor who sees this transaction before it is confirmed. They could execute a swap which dramatically changes the DAI/WETH price immediately before the naive swap goes through, wait for the naive swap to execute at a bad rate, and then swap to change the price back to what it was before the naive swap. This attack is fairly cheap and low-risk, and can typically be performed for a profit.

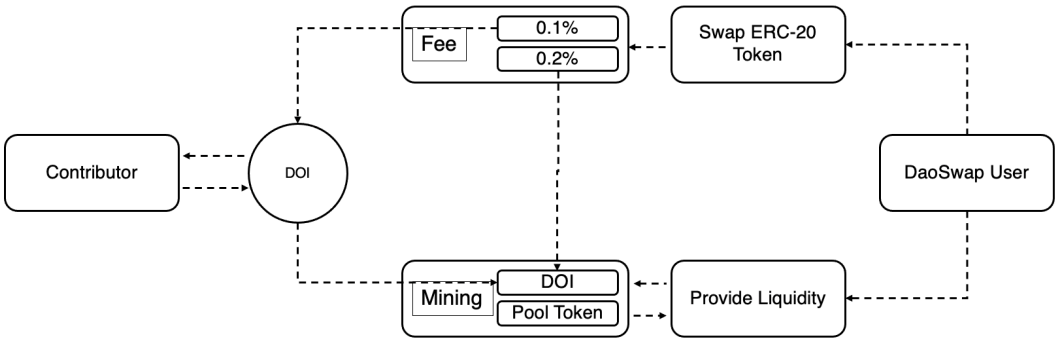
To prevent these types of attacks, it's vital to submit swaps *that have access to knowledge about the "fair" price their swap should execute at*. In other words, swaps need access to an *oracle*, to be sure that the best execution they can get from DaoSwap is close enough to what the oracle considers the "true" price. While this may sound complicated, the oracle can be as simple as an *off-chain observation of the current market price of a pair*. Because of arbitrage, it's typically the case that the ratio of the intra-block reserves of a pair is close to the "true" market price. So, if a user submits a trade with this knowledge in mind, they can ensure that the losses due to front-running are tightly bounded. This is how, for example, the DaoSwap frontend ensure trade safety. It calculates the optimal input/output amounts given observed intra-

block prices, and uses the router to perform the swap, which guarantees the swap will execute at a rate no less that `x`% worse than the observed intra-block rate, where `x` is a user-specified slippage tolerance (0.5% by default).

10, Tokenomics

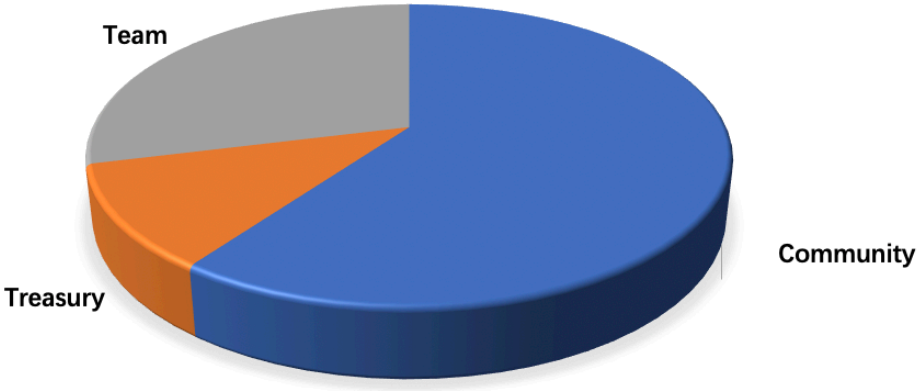
DOI

DaoSwap minted DOI to server the purpose for community-led growth, development, and self-sustainability, enabling shared community ownership and a vibrant, diverse, and dedicated governance system, which will actively guide the protocol towards the future.



DOI Allocation

- 1 billion in total
- 60% to DaoSwap community members
- 11.12% to community treasury
- 28.88% to team and linear release 7.5% every 3 month



DOI holders will have immediate ownership of:

- DaoSwap governance
- DOI community treasury
- The protocol fee share

11, Disclaimer

This material should not be taken as the basis for making investment decisions, nor be construed as a recommendation to engage in investment transactions. Trading digital assets involves significant risk and can result in the loss of your invested capital. You should ensure that you fully understand the risk involved and take into consideration your level of experience, investment objectives and seek independent financial advice if necessary.


DAOSWAP