Ontoswap: The first cross-chain decentralized exchange built on the Ontology

OntoSwap Team

www.ontoswap.com

July 2020

Abstract

A variety of problems have plagued centralized exchanges since their inception, such as hacks, scams, and lost funds, together with issues including fake and manipulated trading data. Thus, decentralized exchanges have slowly but surely been gaining popularity over the past several years. Decentralized exchanges aim to address many of these issues by moving all accounts, transactions, and trading away from centralized databases to a blockchain-powered model. With a DEX, the user holds their private key, and all transactions are made directly on a blockchain, significantly reducing third-party risk and increasing transparency.

However, while DEXes do address some of the issues discussed above, they are not without their problems. Though liquidity issues can be solved with AMM (automatic market-making) mechanisms, user experience is often slower and more complex than that of centralized exchanges. The exchanges are limited by the blockchain technology they are built on, which is generally slower and less flexible than traditional relational databases. Another issue is how to trade assets from multiple blockchains on the same DEX.

Ontoswap, the first cross-chain decentralized exchange on the Ontology, aims to solve the existing issues in the DEX sector by providing instant transactions, lower fees, cross-chain asset exchange, improved user experience, and many other benefits. Moreover, the dual token economy model will incentivize users to provide liquidity and trading volume, thus facilitating the sustainable development of the OntoSwap ecosystem.

Contents

1 Background introduction

The release and development of hundreds of projects in the DeFi (decentralized finance) sector fostered an explosion in locked value which reached around 10 billion USD at its highest point. Though some DeFi projects show novel and well-designed interfaces, the underlying weaknesses remain, such as slow speed, low usability, centralization, lack of cross-chain support, absence of order books, imperfect DAO mechanisms, etc. Thus, if we want to expand the DeFi or DEX ecosystem and attract more users, it is necessary to improve the core features. These include:

1.1 Fast and cheap transactions

Above all else, DeFi is slow and expensive. It can cost dollars to complete a single trade, and minutes for it to clear. This is fine for some use cases – but many customers prefer the fast, cheap execution of centralized exchanges. It is hard to stare at your MetaMask or other cryptocurrency wallet, waiting for a trade to be confirmed, without missing centralized exchanges. Such underlying weaknesses are vital reasons why users cannot replicate centralized exchange experiences when trading on DEXes.

1.2 Order book

Though the automatic market-making (AMM) mechanism revolutionized the DEX space by allowing trading without order books, there are also many downsides to this model. For example, you cannot provide liquidity unless you offer equivalent assets to both sides; you cannot choose to only offer at a particular price; you cannot offer at a price other than the current market price.

AMM is a system where there are no limit orders, or even bids or offers. However, in an order book, you can decide the price, size, and direction you want to trade. Also, an order book system is indispensable for derivatives trading, which is extremely helpful for future DEX ecosystem development. Matching bids and offers with each other involves several operations, and the existing underlying technology, such as Ethereum, cannot handle these operations efficiently since blockchain transactions are slow and expensive.

1.3 Cross-chain swap

There have already been some attempts to solve the issue of how to trade assets from multiple chains on one DEX, and the current, most widely used approach is to trade wrapped versions of tokens from other chains on the DEX. This method is currently

live and in use on several Ethereum-based DEXes, but it has limitations. Perhaps most significantly, the process of converting back and forth from BTC to WBTC relies on trusted third-party gateways, including going through KYC/AML procedures.

1.4 Decentralized autonomous organization

Most DeFi projects are applying a decentralized autonomous organization (DAO) to foster their governance, but there are still many flaws in their models. For example, the project founder of SushiSwap kept 10% of rewards and sold them off for huge profits, which almost caused the project's demise. Thus, if a project wants to realize true decentralized organization, the governance token must follow 0 pre-mining, 0 private sales, and 0 initial circulation, so that it can guarantee fairness in the ecosystem and make the DAO sustainable.

2 OntoSwap - a swap based on Ontology

The current situation of the cryptocurrency market is that centralized exchanges have become the gateway to most traffic, and thus command the power of discourse in the blockchain world. The goal of a decentralized trading platform is to solve the problems of centralized architecture by establishing a peer-to-peer market directly on the blockchain. Decentralized exchanges allow users to continue to monitor their funds with a unique transaction technology. Users can implement cryptocurrency transactions without exposing their crypto assets from the security of their private wallets.

The most popular decentralized exchange applications currently focus on token transactions only on one chain, which significantly reduces the potential application scenarios and the richness of the user experience. OSWAP, the decentralized exchange based on Ontology, will unveil a fully functional decentralized exchange. Thanks to the high-performance underlying technology of the Ontology, OntoSwap will provide its users with trustless cross-chain trading, all at the best speed and price.

- **OSWAP**: the OntoSwap token is the utility token of the OntoSwap ecosystem; it will be fully integrated with OntoSwap and will benefit from buyback and burn with part of the net profits.
- **OntoSwap DAO (YFO)**: the YFO token is the governance token of the OntoSwap ecosystem, and it will be used for the DAO governance by the community. Also, YFO has no pre-mining, no team reserve, no initial circulation, and it can only be mined. This way, YFO will preserve fairness in the governance system.

- **Cross-chain swap:** Thanks to Ontology's robust infrastructure, in contrast to most current protocols that rely on trusted parties to administer swaps, OntoSwap will support cross-chain swaps to exchange assets trustlessly between chains. This will also allow easy margin positions in DeFi on synthetic assets.
- **Order book:** OntoSwap will be equipped with a decentralized automated full limit order book, which not only gives traders complete control over their orders unlike automated market-making but also automatically executes on-chain order matching. The order book will allow users to submit orders with directions, prices, sizes, etc., which gives users control over their trading. OntoSwap includes lots of optimization in the order book system to make it simpler and more efficient for users.
- **High scalability:** Ontology's unique infrastructure will provide OntoSwap with enhanced Layer 2 scalability to undertake more transactions than existing decentralized exchanges, offering users a much smoother experience.
- **Decentralized identity:** Ontology's decentralized identity system will help OntoSwap establish a decentralized and trustless credit system for all financial actions in the ecosystem.
- **Dividends and buybacks:** 50% of net profits will be used to buyback and burn OSWAP, while the other 50% will be distributed to OntoSwap holders.
- **Referral program:** OntoSwap will give rewards to those who refer new users.

- To summarize, below is a comparison between OntoSwap and other DEXes:

	OSWAP	Uniswap	SushiSwap	Serum
Fast and cheap	Yes	No	No	Yes
Stablecoin mining	Yes	No	No	No
Order book	Yes	No	No	Yes
Cross-chain	Yes	No	No	Yes
Derivatives	Yes	No	No	No
Buyback	Yes	No	Yes	Yes
Dividends	Yes	No	Yes	No
Completely fair DAO governance	Yes	Yes	No	No
Referral program	Yes	No	No	No
Transaction mining rewards	Yes	No	No	No

3 Why Ontology?

The Ontology has proved to be a high-performance public blockchain infrastructure which can be customized for different applications. It has significantly higher speeds and lower costs than older blockchains. Also, Ontology supports collaboration among chain networks with its various protocol groups through cross-chain technology. The robust and efficient underlying technology and cross-chain features match the demands of DEXes quite well. The Ontology-based OntoSwap DEX will have the speed, cost, and UX that users expect from a centralized exchange, but it is trustless and non-custodial. Moreover, due to Ontology's full cross-chain integration, users will be able to trade BTC, ERC-20 tokens, NEP-5 tokens, Ontology-based tokens, and more. Eventually, this will give DeFiers a fully decentralized exchange that offers the same experience they have come to expect from CeFi.

4 Token economy

In the market, different DEXes are coming up with their incentive mechanisms, such as SushiSwap, which offers SUSHI as an additional reward for liquidity providers. However, after analyzing SushiSwap's token economy, several common flaws of DEXes arise:

- Team reserve: SushiSwap's founder keeps 10% of each SUSHI distribution, a time bomb for the sustainable development of the ecosystem;
- Staking risk: The protocols require users to stake LP tokens and earn profits;
- Token economy: Existing protocols mess up the DAO and utility tokens, which could destroy the entire ecosystem;
- Single asset swap: Since most of the protocols are based on Ethereum, meaning they only support ERC-20 swaps;
- Low speed and high costs: Due to Ethereum's underlying technology, transactions on the swap protocols are relatively slow and expensive.

To solve this dilemma, OntoSwap creatively applies a dual token model (OSWAP and YFO). OSWAP is the utility token in the ecosystem, while YFO is the governance token in the decentralized autonomous organization. This way, OntoSwap solves the problems with the following solutions:

- The OntoSwap DAO token has no team reserve, no VC allocation, and no pre-mining;
- OntoSwap provides a stablecoin trading pair mining option to help users offset risks;
- OntoSwap applies a dual token mechanism to separate governance and utility

tokens, so that ecosystem members can enjoy the development of OntoSwap while guaranteeing unbiased DAO governance.

● OntoSwap provides a high-performance and low-cost transaction experience, as well as a cross-chain swap based on Ontology infrastructure.

To elaborate, OntoSwap and YFO have the following features:

4.1 OntoSwap token (OSWAP)

OntoSwap is expected to have the following features:

● 50% net profits will go to OSWAP buyback and burn;
● 50% net profits will be rewarded to OSWAP holders;
● Holding OSWAP gives one privilege to enjoy a 50% discount off all fees;
● Users can enjoy double rewards when mining YFO with OSWAP;
● Users can enjoy OSWAP rewards while providing trading volume to Ontoswap.

The OSWAP token has a fixed supply of one billion, and the distribution is projected to be as follows:

● 10%: Team and advisors;
● 10%: Locked seed purchasers;
● 80%: Ecosystem incentive fund.

The distribution above is anticipated and may be subject to modification.

Token Distribution

■ Team and Advisors ■ Locked Seed Purchasers; ■ Ecosystem Incentive Fund
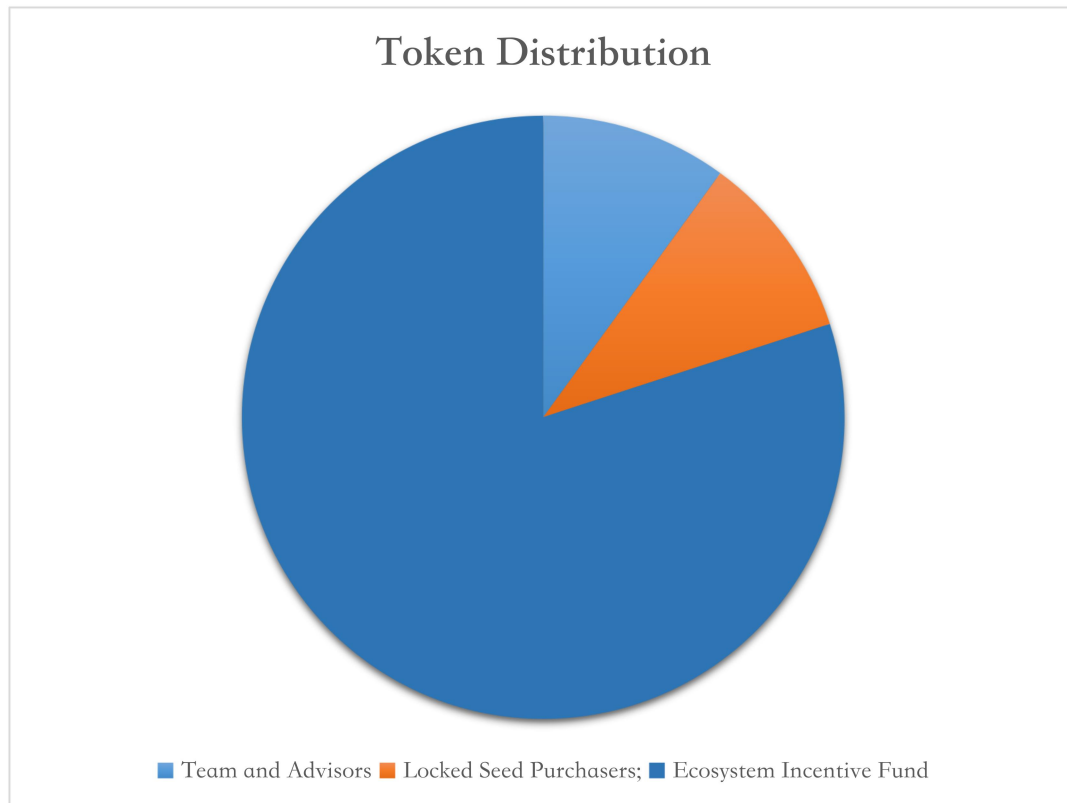
4.2 OntoSwap DAO token (YFO)

YFO is the governance token in the OntoSwap ecosystem. YFO has no pre-mining, no founder shares, and no VC interests – it has completely equal opportunities for staking distribution to attract a broad and likeminded community to steward the future of the protocol and token. There will be six mining pools at inception, of which different amounts of YFO will be allocated to the pools, halved every seven days. On the first day of mining, only the OSWAP-USDT pool will be available, and other pools will be open the following day. If the community wants to amend the pools, they can follow the DAO governance rules found in section 4.3.

The initial set of mining pools are as following:

● OSWAP-USDT (2x reward) - initial YFO is 20,000, and the total will be 40,000;
● YFO-USDT (1.5x reward) - initial YFO is 15,000, and the total will be 30,000;
● DAI-USDT - initial YFO is 10,000, and the total will be 20,000;

Mining models for different pools are as follows:

● **The OSWAP-USDT liquidity mining model:**

Week_OSWAP/USDT_Pool	YFO mined	Total YFO mined
1	20000	20000
2	10000	30000
3	5000	35000
4	2500	37500
5	1250	38750
6	625	39375
7	312.5	39687.5
8	156.25	39843.75
9	78.125	39921.875
10	78.125	40000

`

● **The YFO-USDT mining model:**

Week_YFO/USDT_Pool	YFO mined	Total YFO mined
1	15000	15000
2	7500	22500
3	3750	26250
4	1875	28125
5	937.5	29062.5
6	468.75	29531.25
7	234.375	29765.625
8	117.1875	29882.8125
9	58.59375	29941.40625
10	58.59375	30000

● **The DAI-USDT mining model:**

Week_DAI/USDT_Pool	YFO mined	Total YFO mined
1	10000	10000
2	5000	15000
3	2500	17500
4	1250	18750
5	625	19375
6	312.5	19687.5
7	156.25	19843.75
8	78.125	19921.875
9	39.0625	19960.9375
10	39.0625	20000

YFO is expected to have the following features:

- Only be earned through providing liquidity to the pools;
- Voting rights in the OntoSwap ecosystem to determine project development;
- Can be used to mine YFO;
- Governance frameworks;
- Fee allocations;
- Value-added incentives;
- Pool additions and amendments;
- Protocol economics.

4.3 DAO governance

With the development of the OntoSwap ecosystem, YFO will be the hub of the community. If more projects want to list in the mining pools, they need to follow these steps to create a community vote:

- Spend 10% of the designated number of YFO to apply for a community vote. For example, project A wants to list on OntoSwap with 1,000 YFO to mine. Therefore, they need to buy 100 YFO tokens to create a vote. This fee is non-refundable, which means, if the vote fails, project A will not receive the 100 YFO back;
- If the community approves, the project owner has to buy the remaining 90% of its pool amount. In the previous example, this would mean project A needs to buy another 900 YFO tokens;
- On approval, the project owner can pay another 10% of the pool fee to the community to create a vote to increase the token supply, but with a maximum amount of the project's buying amount.

This way, YFO will be used to create a positive cycle that serves useful projects on Ontology, while protecting the rights of YFO token holders.

5 Ecosystem incentives

5.1 Liquidity mining

Traditionally, liquidity providers can only share a small portion of the pool's trading fees when they are actively providing liquidity. Once they have withdrawn their portion of the pool, they no longer have any rights in the ecosystem. With OSWAP, one cannot only earn their share of the trading fees but also earn rewards in the form of OSWAP tokens. Moreover, as an early provider of liquidity, you become a significant stakeholder of the protocol and enjoy governance rights through YFO tokens.

The additional earnings that you will receive from staking will be proportional to your share size versus the total amount of shares in the pool. Both OSWAP and YFO tokens can be used to mine YFO, which could integrate the value of these two tokens and foster the sustainable development of the ecosystem.

5.2 Transaction mining

In addition to liquidity mining, users can also enjoy OSWAP rewards by providing transaction volume in different pools. The transaction fees you pay will be paid back in the form of OSWAP. The more you trade, the more rewards you will get. Also, half of all net profits in the OntoSwap ecosystem will be proportionately distributed to the OSWAP holders.

5.3 Buyback & burn

The remaining half of net profits will get converted back to OSWAP through OntoSwap and will be burned as part of the OntoSwap deflation scheme.

5.4 Referral program

OntoSwap will be the first decentralized exchange with a complete referral program.

6 Product development

OntoSwap will follow three versions to accomplish a stable, high liquidity, fast, and low-cost cross-chain decentralized exchange which will provide our global users with the best user experience.
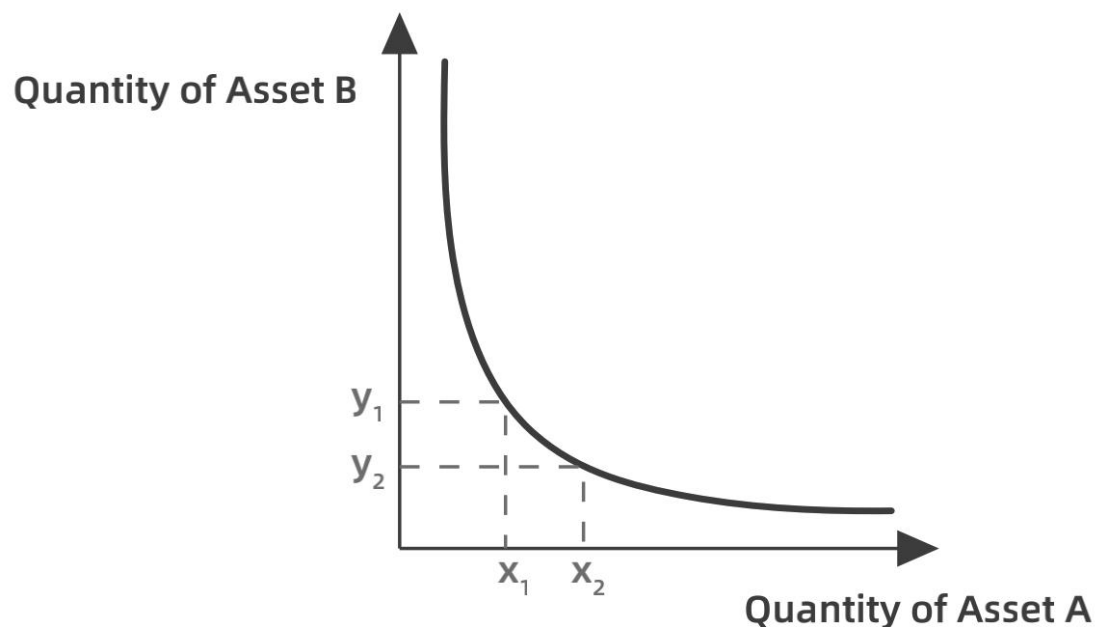
6.1 OntoSwap v1.0

In the two years since its launch, Uniswap has solidified its position as one of the mainstays in DeFi. The exact exchange rate between two assets is set by the initial provider and fluctuates depending on the supply and demand of these assets on the open market. This process occurs automatically as a result of its "constant product" mechanism, and is derived from the following mathematical formula:

$$X * Y = K$$

X = Quantity of ETH;
Y = Quantity of ERC-20 tokens;
*K = Constant value.*

Thus, in OntoSwap version 1.0, we would like to adopt Uniswap's elegant core design. Still, we have added community-oriented features that we believe improve the design of the protocol, as well as provide further benefits to participants. Like existing protocols such as SushiSwap, OntoSwap has a dual token model: OSWAP

and YFO, and the YFO will not be pre-mined, have no team reserve, and no VC interests. By staking the OSWAP/USDT LP token in liquidity, users can enjoy YFO rewards.

6.2 OntoSwap v2.0

Around two weeks after the protocol's inception, OntoSwap will conduct a liquidity migration. We will be migrating all the liquidity tokens staked OntoSwap contracts. This migration will involve taking all of the Uniswap LP tokens staked on SushiSwap, redeeming them on Uniswap for the respective token pairs, and initializing new liquidity pools from these tokens. For DEXes, Uniswap has over 60% of the market share by volume as shown in the graph below, which means it will bring huge amount of traffic to us. Once the migration is complete, the liquidity converted will be fueling the first sets of OntoSwap pools and will bring the protocol into operation immediately. The stakers do not need to do anything. They will continue to receive YFO token rewards from providing liquidity going forward, as well as receive OSWAP token rewards by joining the transaction mining. Meanwhile, we will launch the first complete referral program in the market to facilitate the development of the OntoSwap ecosystem.
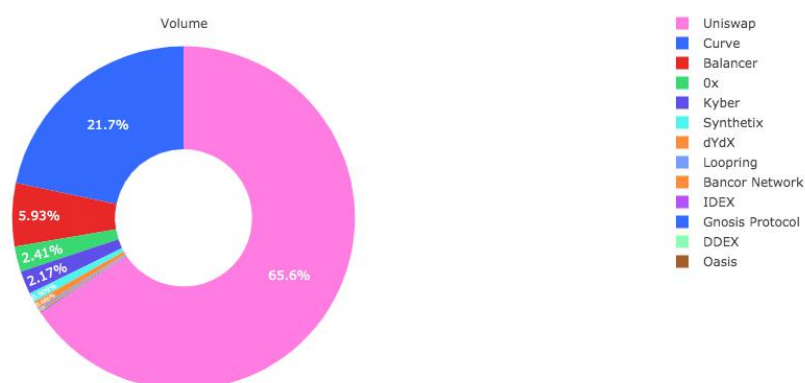
6.3 OntoSwap v3.0

OntoSwap v3.0 will be a fully cross-chain decentralized exchange built on Ontology. Empowered by Ontology's underlying technology, OntoSwap will integrate cross-chain swaps, providing users with the most convenient trading experience. Digital assets on different chains joining OntoSwap for swaps will significantly support OSWAP's development. Meanwhile, OntoSwap will build more financial products, including decentralized futures, options, etc., to meet with diversified demands.

- **Perpetual swap**

OntoSwap implements a synthetic trading market on the Ontology that allows for exposure to arbitrary liquid assets using tokens on different chains as collateral. Similar to existing perpetual contracts, the price of the contract is tethered to the price of the underlying asset by a dynamic interest rate called the "funding rate." The funding amount paid or received by an account over time length T is calculated according to this formula:

$$F = (-1) * R * (T / A \text{ hours}) * B * X$$

F = the change in account balance over the given period;
R = funding rate as an A-hour rate;
B = position balance of the account;
X = on-chain index price.

An on-chain price oracle is used for liquidation purposes, and secondarily, to calculate funding payments. The order book for the market can remain off-chain, allowing for faster price movements and better liquidity. Moreover, the contract's underlying asset does not have to already exist as a token. For each account trading the perpetual, profits and losses are exchanged using the margin token.

- **Options:**

Though derivatives markets comprise of some of the most liquid markets in all of traditional finance, options markets are missing in DeFi. Moreover, liquid options markets provide market participants with access to hedging, leverage, and financial insurance, making the development of such markets a prerequisite to DeFi's maturation.

As in all options markets, the two key actors in the protocol are those who want to sell options and those who wish to buy options. Anyone can buy options to protect themselves against DeFi risks. Users can also deposit collateral in a vault to mint and sell options, earning premiums for protecting others.

In addition to perceptual swaps and options, OntoSwap will explore more opportunities to develop derivatives products on the Ontology.

7 Risk warning & disclaimer

7.1 Risk warning

There are risks in the development, maintenance, and operation of the OntoSwap ecosystem, many of which are beyond the control of the OntoSwap ecosystem developers. In addition to the content described in this white paper, participants should also be fully aware of and agree to accept the following risks:

Market risks

The price of a token is inseparable from the overall situation of the digital currency market. If the overall market situation is inactive, or there are other uncontrollable factors, it may lower the value of token despite it having favourable prospects.

Regulatory risks

Since the development of blockchain is still at an early stage, there are no relevant regulatory documents related to prerequirements, transaction requirements, information disclosure requirements, locking requirements, and other requirements in the recruitment process. It is also unclear how existing policies will be implemented. These factors may have an uncertain impact on the development and liquidity of the project.

Blockchain technology has become a primary target of supervision in all major countries in the world. OntoSwap may be affected by regulatory policies, such as restrictions on the circulation of tokens. Tokens may be restricted, or the development of the OntoSwap ecosystem may even be terminated unexpectedly.

Competition risks

At present, there are many projects in the field of blockchain, and the competition is intense. Whether OntoSwap can breakthrough among the many other excellent projects and receive wide recognition, is not only concerned with its management capabilities and vision planning but also influenced by different actors in the market, including existing competitors and the potential entry of internet giants. There will always be a possibility of fierce market competition.

Organizational structure change risks

OntoSwap brings together a talented team with both vitality and strength. The team attracts senior practitioners in the blockchain field and technical developers with

rich experience. In future development, the organizational structure may change, which may have an impact on OSWAP.

7.2 Disclaimer

This document is only for the purpose of conveying information; the content is for reference only and does not constitute any trading advice, abetting, or invitation to sell or buy stocks or securities on OntoSwap or its related products. This document is not constituted nor understood as providing any trading behavior, nor any form of contract or commitment. Given unpredictable circumstances, the goals listed in this white paper may change. Although the team will try to achieve all the goals of this white paper, all individuals and groups holding tokens will be at their own risk. Part of the content of the document may be adjusted accordingly in a new version of the white paper as the project progresses. The team will announce the updated content to the public by posting announcements or a new version of the white paper on the website.

OntoSwap clearly states that it will not bear the direct or indirect losses incurred by participants, including the team, who are fully committed and will strive to achieve the goals laid out in this document. However, certain events, beyond the control of the parties, may inhibit the parties from fulfilling their duties and obligations under the project agreements. In such settings, the team cannot be held liable for any force majeure events. A token is a digital token for the value circulation and application; we cannot completely guarantee that it will increase in value. To the maximum extent permitted by applicable law, OntoSwap shall not be liable for damages and risks arising from participation, including but not limited to direct or indirect personal damage, loss of commercial profit, loss of business information, or any other economic loss. The platform communicates possible risks to participants. Once participants participate in token mining or secondary market purchases, they have confirmed that they understand and recognize the terms and conditions in the rules and accept the potential risks and consequences of this platform.