

# SumSwap V3.0



Financial integrator of decentralation standing on the shoulders of giants

# Abstract

The emergence of Bitcoin (BTC) opens the gate of cryptocurrency world. Since the emergence of BTC, people have more demands for blockchain technology and cryptocurrency. Thanks to the efforts of many technological geeks, many excellent blockchain projects and better cryptocurrencies spring up. Originally, the value of 10,000 BTCs was equal to a pizza. But now, it is a huge cryptocurrency empire with value of thousands of billions of dollars.

According to statistics of professional organization, the market value of current cryptocurrency has almost reached USD 3000 billion which has exceeded the market value of many traditional world-level leading companies although their daily trading amounts vary within hundreds of billions of dollars. The remarkable development of cryptocurrency depends on the strong potentials of the blockchain and demands of new technology for cryptocurrency, as well as the development of various cryptocurrency exchanges.

The cryptocurrency exchange directly undertakes the responsibility of expanding the circulation and exchange of cryptocurrency. Definitely, it is impossible to see the current diversified cryptocurrency market without the cryptocurrency exchange.

The cryptocurrency and exchange benefit, promote and influence each other. As cryptocurrency is booming, a series of high-quality cryptocurrency exchanges have sprung up. The most famous exchange is Coinbase that is listed in the USA capital market. It means that the cryptocurrency has been accepted by the traditional capitalists. In addition, the global leading exchanges including Binance, Huobi, and OK can obtain considerable earnings per year.

Unfortunately, most decentralized trading can be made in the centralized exchange only, for example, the representative blockchain technology and cryptocurrency. Since the establishment of centralized exchange, many counterfeit events occur due to un mature regulation of the cryptocurrency market, which not only results in loss of assets for many users around the world, but also affects development of the whole industry. It can be predicted that such events cannot be avoided due to



centralized exchange.

With the continuous development of the industry, many technological geeks go toward the direction of decentralization. Until 2020, the whole decentralized financial market saw its booming development. Simply, Decentralised Finance (DeFi) is to realize various financial functions of cryptocurrency (e.g. trading, loan, derivatives, and stable coins) based on immutable and traceable features of various smart contracts on the public chain.

According to the data, since the early of 2020, the whole DeFi market has developed rapidly and DeFi locked position volume has increased for over 20 times from the original USD 500 million to the current thousands of billions of dollars. Besides, the total market value of DeFi related tokens also approximates to USD 70 billion. Although there is a large gap between the current DeFi market and centralized exchange due to threshold and experience, undoubtedly, DeFi will finally replace the traditional centralized exchange with the emergence and development of ETH2.0 and various Layer 2 technologies.



Fig. 1 Change of DeFi locked position since 2020

A group of technological geeks who have rich development experience in smart contract and pursue to develop the blockchain market believes that SumSwap V3.0 will have a wide prospect in the DeFi market. The well-known scientist Newton once said, “If I have seen further than others, it is by standing upon the shoulders of giants.” According to SumSwap V3.0, all great creations are not formed in a day, it is



by standing upon the shoulders of giants.

SumSwap V3.0 will update and develop continuously based on the decentralized exchange in the early stage and gradually expand the trading system of stable coins, loan system and algorithm arbitrage system in the later stage to create ideal digital finance of decentralization through smart contract.

## I. About SumSwap V3.0

All great creations are not formed in a day, it is by standing upon the shoulders of giants.

SumSwap V3.0 is a DeFi project that integrates current excellent smart contracts and realizes innovative upgrade. Deployed on the ETH L2 smart contract, SumSwap V3.0 originally focuses on cryptocurrency trading and realizing exchange between different ERC20 tokens. With continuous development and iteration in technology, it will be provided more functions, e.g. online and cross-chain trading, loan, and derivative trading.

In addition to the front-end flexibility for application of center codes, some functions of SumSwap V3.0 are created through the smart contract and audited by the global leading safety audit company Certik. SumSwap V3.0 is a completely open smart contract system where users can create trading pairs, add liquidity, and make cryptocurrency trading. The whole process is executed through smart contract to ensure safety, transparency, and traceability.

SumSwap V3.0 is especially created for smart contract, which allows front-end operation and even on-chain operation. It is the advantage of smart contract. The traditional centralized exchange cannot be used without maintenance by special staff. For SumSwap V3.0 specially created for the smart contract, users can execute on-chain operation without maintenance of centralization team. The assets are store on the chain completely and can be managed by users with private key.

From the view of trading design, SumSwap V3.0 has succeeded the common mathematical trading model of  $X*Y=K$  and AMM in current decentralization agreement. Differently, SumSwap V3.0 has innovated the traditional model and innovated trading design allows users to increase liquidity by zone to greatly improve the utilization rate of assets added to the liquidity pool. Besides, the limit order mode is also realized.

Moreover, SumSwap V3.0 is also provided with more interesting functions to



promote direct circulation of the whole ecology. In addition to the common bonus of service charge from addition of liquidity, addition of liquidity by zone, SUM mining through liquidity trading, SumSwap V3.0 is also provided with more functions, for example, sharing of service charge through inviting subordinates, mining through trading, and mining with Staking, which greatly improves the interestingness of SumSwap V3.0 ecology.

SumSwap V3.0 is deployed to the Arbitrum Layer2 solution with Optimistic Rollup technology. Layer2 is a general term of a series of off-chain expansion solutions. The expansion will not influence the public chain itself and can be improved by other methods. The current ETH Gas fee and trading speed have impeded development of the decentralized exchange. However, many users are tolerable to the Gas fees of dozens of dollars and even hundreds of dollars and the slow trading speed. When SumSwap V3.0 is deployed to the Arbitrum, it is possible to reduce 90% Gas fees and greatly improve trading speed.

At present, the sedimented assets of Arbitrum has reached dozens of billions of dollars. As time goes by, more projects are added to the Arbitrum ecology. It is noted that Arbitrum shows many advantages, but there are some disadvantages in assets withdrawal. It usually takes several days to withdraw assets in Arbitrum. Definitely, the deployment of SumSwap V3.0 is not limited to Arbitrum. If there is a better Layer2 solution, SumSwap V3.0 will select a better solution for deployment again.

SumSwap V3.0 uses the mathematical integral signs (i.e. from zero to infinite) to integrate various excellent algorithms in the field of DeFi. SumSwap V3.0 considers that the current excellent DeFi project is innovated from the view of mathematics. The mathematics has greatly promoted development of current DeFi to a large extent. The mathematics is the language for human to communicate with the universe and God. Mathematics is law. The blockchain describes the mathematical law with codes and realizes the “code is law, mathematics is law, and code is law”. With the totem of integral and the vision of integrating excellent mathematical innovations in blockchain, SumSwap V3.0 realizes a true blockchain world of “mathematics is law and code is law”.



## II. Technical framework

The emergence of SumSwap V3.0 benefits from the development of various technologies, including rapid development of smart contract and Layer 2 technology and mathematical innovation of various DeFi products, for example, AMM,  $X*y=K$ , and other trading models. Based on the above technologies, SumSwap V3.0 has realized systematic optimization and experience upgrade to create a unique DeFi product that can be competitive with the centralized exchange.

### 2.1 Smart contract

The smart contract is the reusable code snippet (program) that is issued in EVM memory by developers. Everyone can request to execute the code of smart contract through making the trading request. The developers can write any executable applications in EVM (e.g. game, market, financial instrument) through issuing the smart contract, so that these apps are usually called “dapps” or “decentralized apps”.

ETH Smart Contract is a program that is running on ETH blockchain. It is the set of codes (functions) and data (states) of specific addresses on ETH blockchain. The smart contract is an ETH account. It means that they have balances and can send trading through network. However, they are deployed to the network and run by program, instead of being controlled by the user. Then the user account can interact with smart contract through submitting the trading of executing functions defined in the smart contract. Like common contract, the smart contract can define rules and automatically execute them through codes. The smart contract cannot be deleted by default and interaction with them is irreversible.

SumSwap V3.0 is deployed on ETH Layer 2 to provide decentralized foundation for SumSwap V3.0 through immutable and traceable feature of the smart contract. Generally speaking, SumSwap V3.0 is a section of program in ETH EVM, which can realize multiple functions in the trading.

### 2.2.AMM (Automated Market Maker)

AMM is the automated market maker strategy that is created with an algorithm combined with the constant product trading. It can simplify the process of traditional



market maker, avoid large Gas fees, and reduce the threshold of market maker.

### 2.2.1 Traditional financial market maker

It is difficult for a seller to find an appropriate buyer in the financial trading of traditional order book due to liquidity, vice versa. At this time, the market maker will make trading with the buyer or seller by appropriate price for arbitrage. Generally, there are more than one market maker in a qualified exchange where trading can be made successfully with the assistance of the market maker.

### 2.2.2 Traditional on-chain trading

If the order book is used for traditional on-chain trading, the market maker will spend more costs due to the on-chain Gas fees. Besides, if the traditional mode is used for on-chain trading, it cannot make ends meet because there is a small number of on-chain traders, resulting in the emergence of automated market maker (AMM).

### 2.2.3 Automated Market Maker (AMM)

Simply speaking, AMM (Automated Market Maker) is the position of replacing traditional centralized platform with an algorithm to provide liquidity for exchange in the market. Different from traditional market maker, AMM requires to add related assets to the liquidity pool as per the price ratio and then liquidity will be formed automatically. Besides, the more the added assets are, the larger the liquidity will be.

In addition, the traditional market maker requires large costs and high quantitative trading technology. However, there is not any requirement for AMM and it is enough to have assets for market making.

## 2.3 Constant product trading

The order book is a traditional trading mode, where both the buyer and seller can offer prices and make a trading when the price is consistent. The constant product is to replace the traditional order book through the trading formula  $X*y=K$ , where  $X$  is



the quantity of one digital assets,  $y$  is the quantity of another digital assets,  $K$  is constant,  $X/y$  is the price of  $X$  relative to  $y$ .

### 2.3.1 Trading rules of order book

Under the trading mode of order book, if the number of buyers is larger than the number of sellers, the price will rise; otherwise, the price will decrease. Both the buyer and seller wish to have a small sliding point, so that they can have a better experience. Actually, the ideal zero sliding point is a straight line.

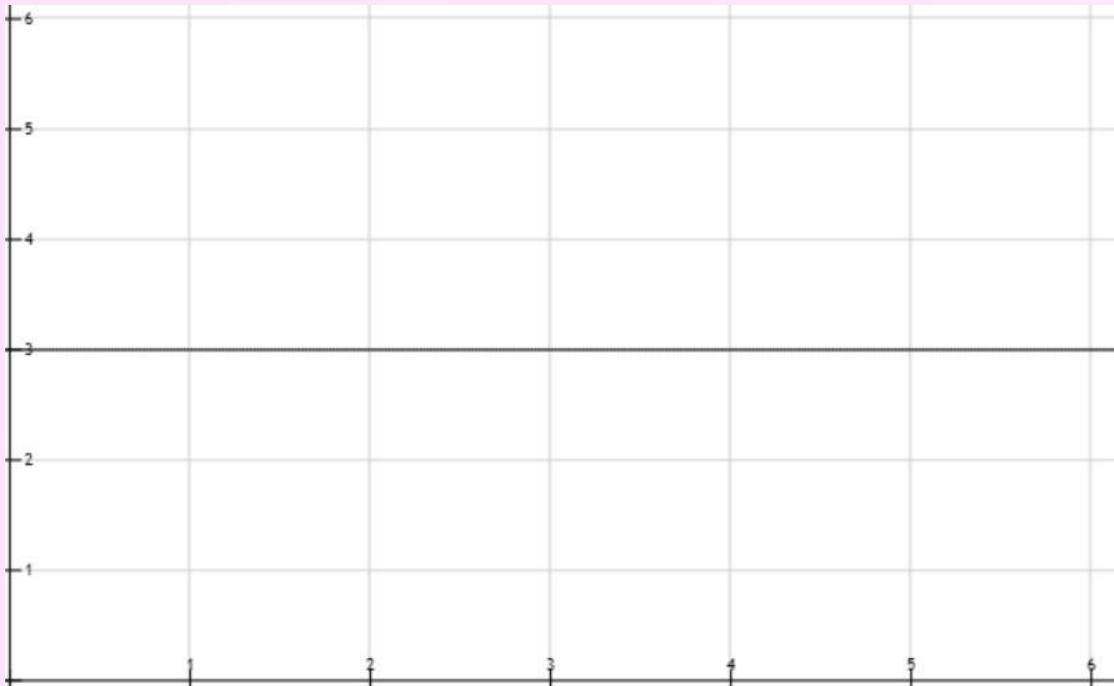


Fig. 2 The ideal zero sliding point is a straight line.

For example, if the price of a coin is 3, then the trading price of the coin will change slightly under the sufficient liquidity.

### 2.3.2 $X*y=K$ trading rules

Given that  $X*y=3$ , Fig.3 shows the coordinates graph of the function. It can be seen that  $y$  will decrease if  $x$  increases and  $x$  will decrease if  $y$  increases. It completely simulates that the price will rise when the number of buyers is larger than the number

of sellers and the price will decrease when the number of buyers is smaller than the number of sellers.

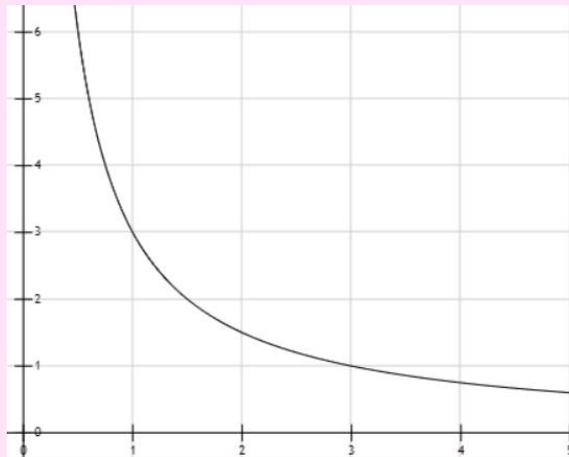


Fig. 3  $X*y=3$

It can be seen that  $X*y=K$  can completely simulate the order book mode.

If the user liquidity is increased, for example,  $X*y=6$ , the graph will be changed into:



Fig. 4  $X*y=6$

If the liquidity continues to increase, for example,  $X^*y=30$ , the following graph can be obtained.



Fig. 5  $X^*y=30$

It can be seen clearly that the slope of a fixed point on the curve will decrease gradually with an increase of liquidity. That is to say, with the increase of liquidity, the trading of a certain range is close to a straight line to achieve the same effect with the order book mode.

### III. Concentrated liquidity and limit order

#### 3.1 Concentrated liquidity

It can be seen clearly from the above model that  $X*y=K$  can perfectly simulate the condition under the order book mode, i.e. when the number of buyers is larger than the number of sellers, the price will rise; when the number of buyers is smaller than the number of buyers, the price will decrease. When the liquidity increases, the sliding point can also decrease.

Although it is only necessary to increase liquidity of the order book mode under a certain price range, the liquidity of mathematical model  $X*y=K$  is scattered to the whole range of  $(0, \infty)$ , which greatly decreases the utilization rate of assets.

SumSwap V3.0 upgrades the original function, so that users can directly add liquidity for a price range to greatly improve the utilization rate of assets.

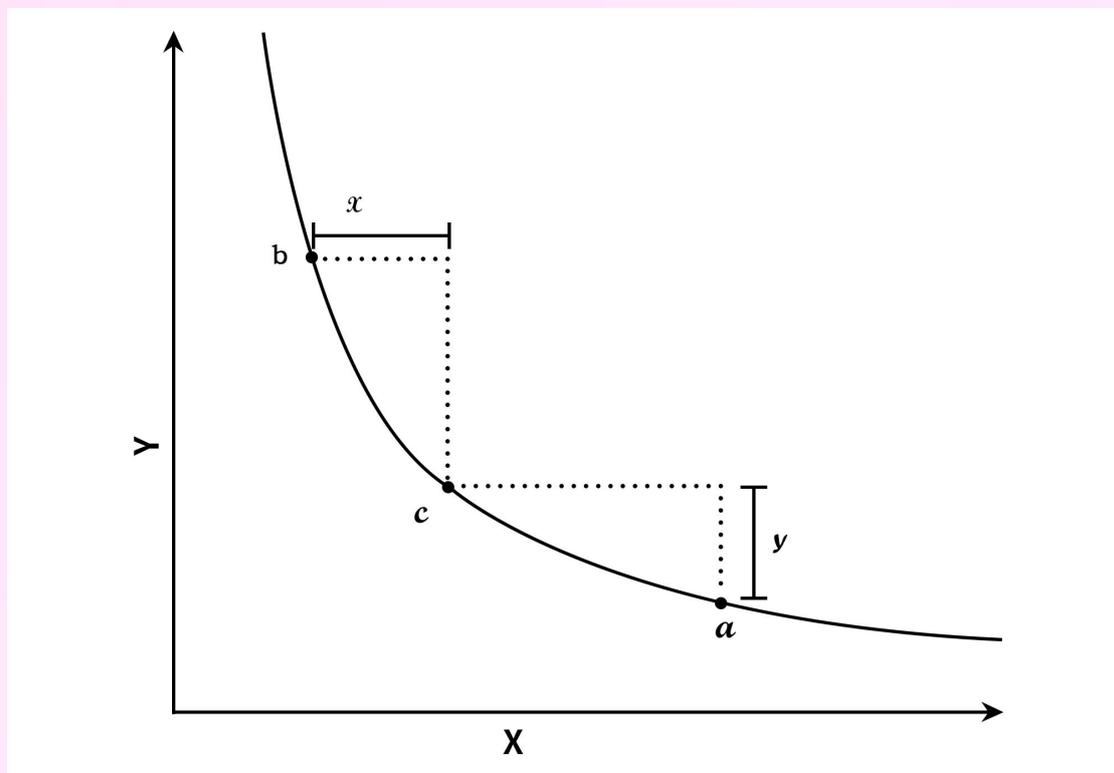


Fig. 6 Add liquidity in the range of limit price

### 3.2 Limit order

SumSwap V3.0 enables users to unilaterally provide liquidity. The limit order mode can be realized through adding liquidity to range and unilaterally adding liquidity.

### 3.3 Different trading rate

SumSwap V3.0 provides three different trading rates for users (i.e. stable coin rate 0.05%, common trading pair rate 0.3%, non-common trading rate 1%) to accommodate demands of different traders and optimize the trading experience better.

### 3.4 Better trading pairs of stable coins

Different from exchange between different currencies, the trading demands for stable coins include smaller sliding point and lower trading fee. SumSwap V3.0 can meet the above demands well because it adds liquidity to fixed range, and then decrease the sliding point to a lower level than the centralized exchange.

## IV. Contract framework

SumSwap V3.0 consists of more than ten contracts as a whole. Each contract has its specific functions, and all these contracts constitute SumSwap V3.0 through specific framework.

As a whole, the business logic looks like a complex automobile plant, and each contract represents a production process. Some contracts act as materials import and detection department, some contracts act as automobile framework department, some contracts act as automobile energy department, and some contracts act as the assembly department.

To sum up, SumSwap V3.0 is a complex structure that is constituted by multiple contracts. It is impossible for only one contract to constitute such structure.

The contracts of SumSwap V3.0 include liquidity manager that is used for managing addition and deletion of global liquidity and withdrawal of service charge; contract plant that is used for deploying new trading pair contract and service charge; liquidity management contract that is used for calculating addition of liquidity and trading fee. Besides, the contract of producing ERC721 tokens for users, non-homogenous token management contract, and trading switch management contract are also included.

All contracts are linked by certain functional sequence and function to constitute a complex decentralized system.

Depending on these complex contract frameworks, SumSwap V3.0 can create trading pairs, add liquidity, directly exchange various ERC20 tokens, and realize other functions.

In addition to these basic functions, the contracts of SumSwap V3.0 have also realized trading and mining and recommended to subordinates to get service charge. The function of getting service charge through recommendation is especially applicable to users with cryptocurrency community. It is legal and appropriate because only one-level service charge is shared. Only if the subordinate traders make

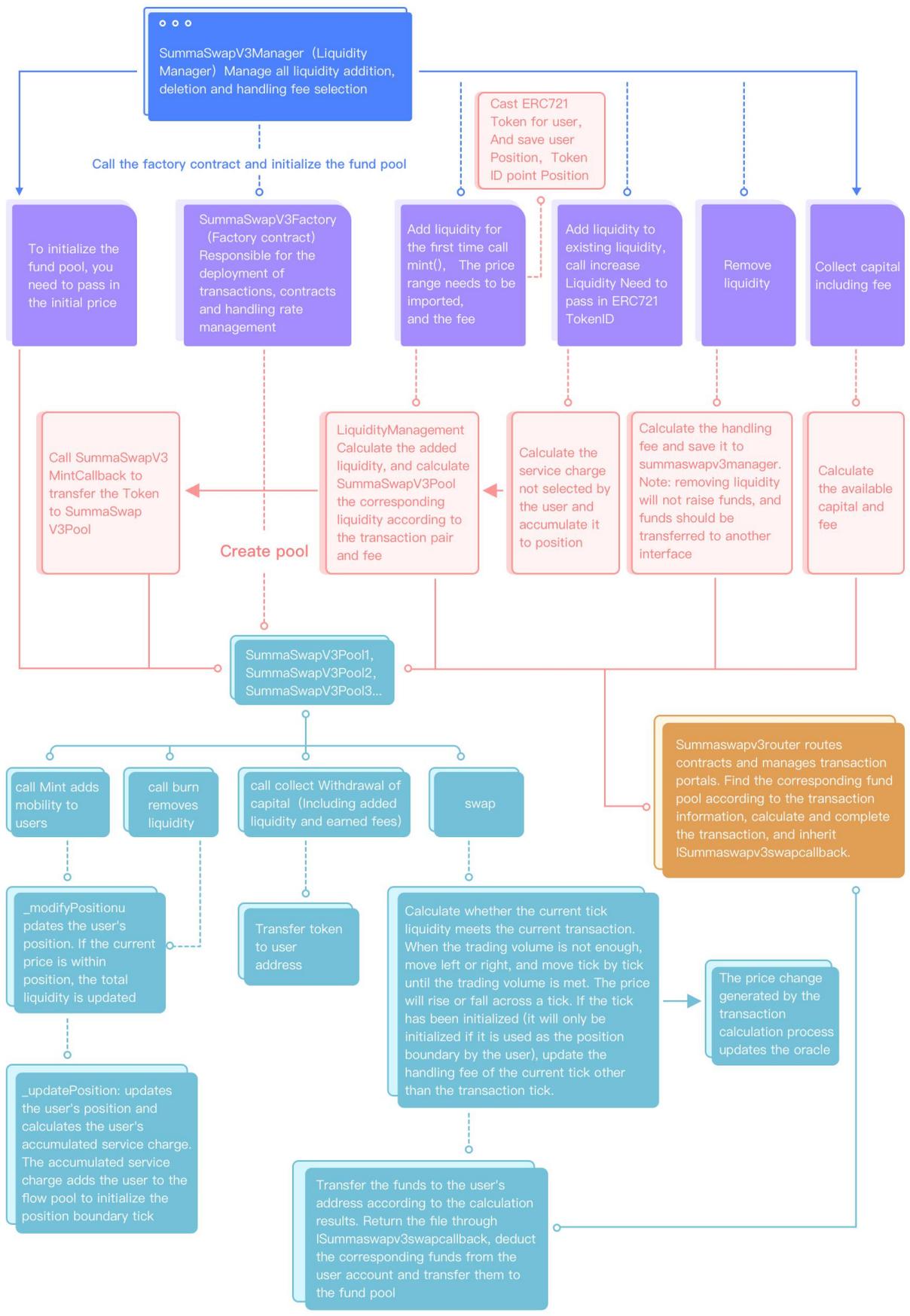


a trading successfully, the service charge will be returned to the recommender through the smart contract.

For those users who are recommended, some service charges can be reduced only when they contact their superiors for activation. Therefore, subordinates are willing to complete activation by their recommenders. Combined with other functions of SumSwap V3.0, the whole system can form an interesting and valuable ecology.

About the complete contract framework of SumSwap V3.0, please see the following contract framework diagram of SumSwap V3.0.





## V. Advanced Oracle

As one of the important branches of DeFi, Oracle can provide out-chain data for various on-chain apps and therefore has become one of the fundamental apps at present and even in the future.

SumSwap V3.0 can realize trading service of digital assets and Oracle functions to provide Oracle offer service for various apps.

For example, if you want to determine the possible USD price of given ERC-20 token through getting DAI price feed, you can complete it with SumSwap V3.0, but you shall pay attention to some problems as below:

First, is there any problem if the final trading price is extracted from SumSwap V3.0 liquidity pool only?

Although it seems to be a feasible strategy, it will be controlled easily and then hacker event will occur inevitably. How to control the final trading price?

Simply, you only need to make trading on SumSwap V3.0. As above mentioned, “if users are selling TOKEN1, its price will be decreased”. Most importantly, it is not necessary to spend more assets. You only need to sell TOKEN1 and exchange it into TOKEN2 with the controlled price, and then sell TOKEN2 immediately. It looks like the flash loan, where attack cost is almost 0, except the service charge.

SumSwap V3.0 v3 uses the time weighted average price. First, SumSwap V3.0 v3 calculates the price only when one block is ended. That is to say, if you want to control the price, you must purchase the token and wait for the next block, and then you can sell it successfully. This provides more arbitrage opportunities for other traders, which increases the risk/cost of price controller. Second, SumSwap V3.0 v3 is provided with the function of time weighted average price. Although it seems too complex, its basic functions are very simple:

Two new methods are added to each liquidity pool:



price0CumulativeLast()

price1CumulativeLast()

It is not enough only depending on the above two methods. After all, we are interested in the average price in a certain time, but there are no historical prices of priceCumulativeLast.

For example, if we want to get the time weighted average price of token0 within 24 hours, we need to store price0CumulativeLast() and corresponding timestamp (block.timestamp) and wait for 24 hours. The average price within 24 hours is calculated as  $(\text{price0CumulativeLast}() - \text{price0CumulativeOld}) / (\text{block.timestamp} - \text{timestampOld})$ .

In some cases, it is enough to have price0 only. However, different results can be obtained if the time weighted average of token0 or token1 is used, so that SumSwap V3.0 provides the above two weighted values.

SumSwap V3.0 is integrated into the contract as Oracle. But the problem is historical data. It means that it cannot be integrated into your contract only. Based on requirements and complexity of implementation, the simple, medium, or complex Oracle integration method can be selected.

## 5.1 Simple method: manually fix time window

You can regularly call the update function in manual settings. For example, the function shall be called for once per day for the 24-hour weighted average, and the average price is calculated with the above formula.

Price weighted difference/time lapse.

FixedPoint.uq112x112 is not important from the view of concept. The result is just expressed as a fixed point with 112 bits on both sides.

```
function update() external {
```



```

        (uint price0Cumulative, , uint32 blockTimestamp) = SumSwap
V3.0V2OracleLibrary.currentCumulativePrices(pairAddress);
        uint32 timeElapsed = blockTimestamp - blockTimestampLast;

        require(timeElapsed >= TIME_PERIOD, 'UniOracle: Time period not yet
elapsed');

        price0Average = FixedPoint.uq112x112(uint224((price0Cumulative -
price0CumulativeLast) / timeElapsed));
        price0CumulativeLast = price0Cumulative;
        blockTimestampLast = blockTimestamp;
    }

```

Now we have obtained the average price. The amountIn with unit token0 can be used for calculating amountOut with unit token1.

```

function convertToken0UsingTimeWeightedPrice(uint amountIn) external view
returns (uint amountOut) {
    return price0Average.mul(amountIn).decode144();
}

```

We have not calculated price1Average. If you want to get more accurate value, you can calculate with price1CumulativeLast. Besides, you can also directly take the reciprocal of price0Average:

```

function convertToken1UsingTimeWeightedPrice(uint amountIn) external view
returns (uint amountOut) {
    uint256 price1Average = price0Average.reciprocal();
    return price1Average.mul(amountIn).decode144();
}

```

For this method, you have to call the contract through manual timing. In addition, the average price in fixed window reacts slowly to the recent price change, and there are same weights for historical price and the recent price (actually, it is better to have



a larger weight for closer price).

## 5.2 Medium method: manual sliding window

The window size can be defined through moving the window. Then you can designate the particle count that means the number of measurement points in the window, e.g. set value.

Window size: 2 months; Particle count: 3. Fig.7 shows the results.

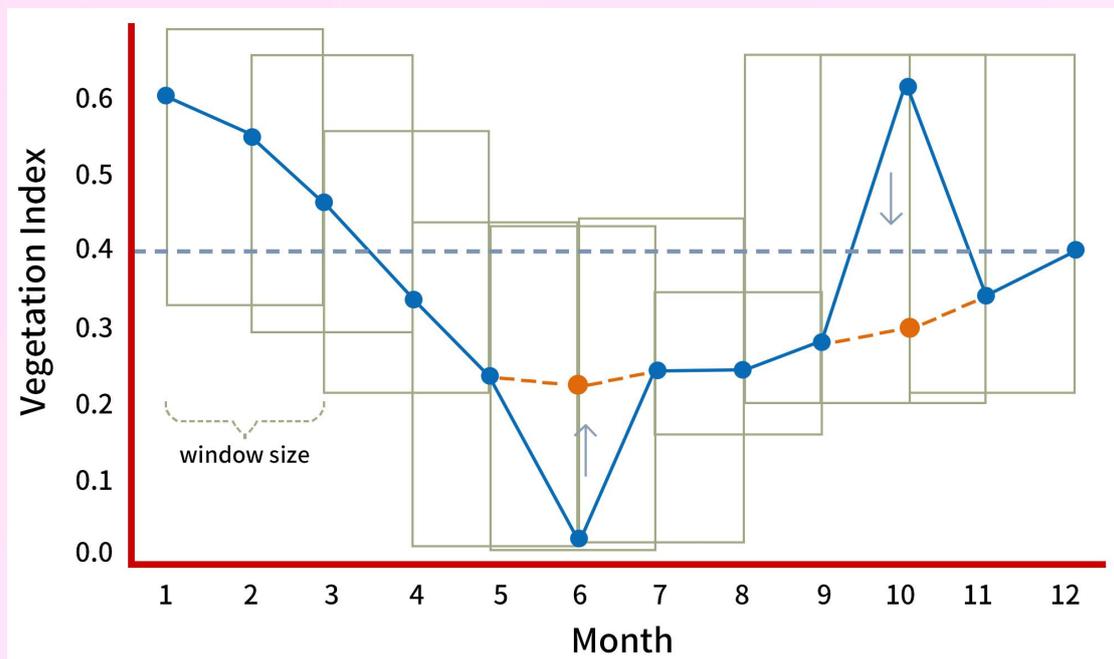


Fig. 7 Oracle of average data

The average value of current window is calculated. The higher the particle count is, the more accurate the average value will be, and the large the times of calling update() will be.

Complete Remix example: You can see a complete example in Remix. After modification, you can use DAI and WETH pair in Kovan test network. Before reading the results, you shall call “update” and consider particle count and time window.

Otherwise, SlidingWindowOracle: MISSING\_HISTORICAL\_OBSERVATION

cannot be called successfully. Besides, you can see a common “reverted” only because Remix does not display any detail about “return” and “view” function. The simplest test method is to use the minimum particle count (=2) and appropriate window size (e.g. 30 s).

### 5.3 Complex method: automatic sliding window

Finally, there is a cool project which realizes a solution, without calling any automatic update().

How does it work?

Remember, we need to have the historical value of “price0CumulativeLast()”. The historical value cannot be read from the contract memory directly because it is not on-chain. But there are some other on-chain objects related to the value.

At least for the last 256 blocks, we can still read hash value of block from EVM.  
blockhash(uint blockNumber) returns (bytes32)

There is a tip here. The resultant hash of block is the root of Merkle Tree. Let me tell you how it works through a high-level concept.

### 5.4 Merkle Tree

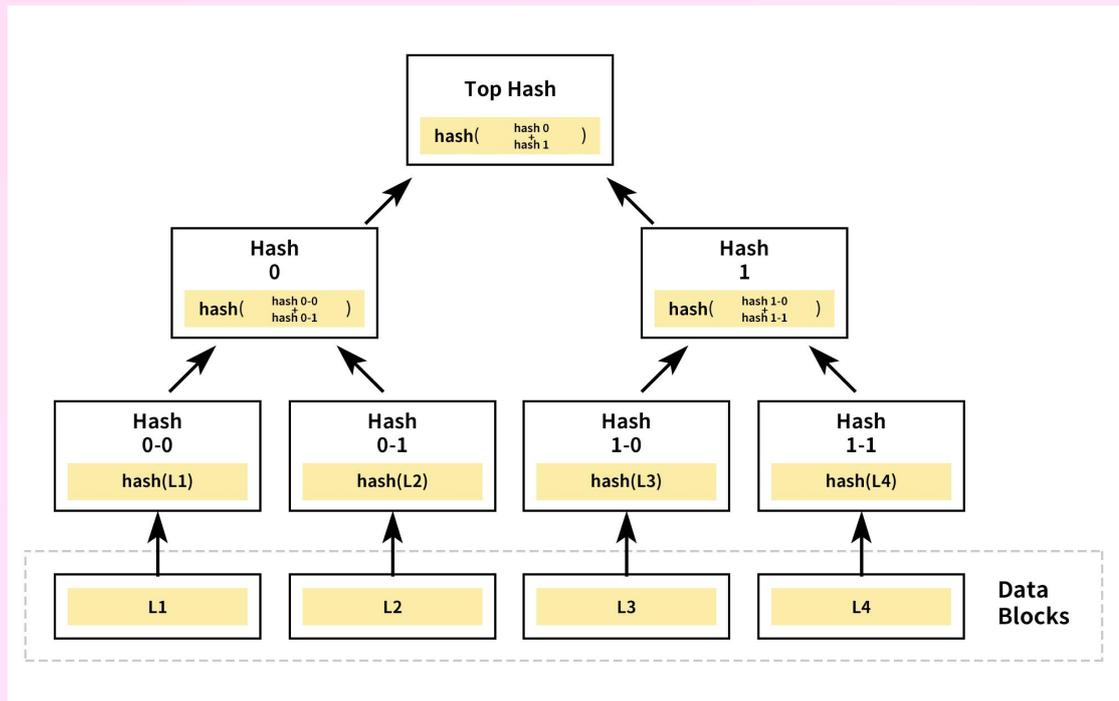


Fig. 8 Merkle Tree

The root of Merkle Tree is the root hash which is obtained with `blockhash(uint blockNumber)`. It is created through hash processing for each data block and storage as leaf node. The two leaves are combined together through hash to form new hash and then recombine together, until a tree with only one root hash is created.

Merkle demonstration is to prove that L3 block definitely includes one given value. It is necessary to provide Hash 0, Hash 1-1 and L3 block only to complete the demonstration. You can calculate hash value of L3 firstly, then calculate hash1 and finally calculate the root hash. Then we can compare the root hash with the given root hash. Merkle demonstration can be explained here well.

In Ethereum (ETH), there is a Merkle Tree that is state tree. It includes all states (e.g. balance) and contract storage. It means that it also includes `price0CumulativeLast` value. Therefore, we make the above Merkle demonstration for the historical price value. EIP-1186 introduces `eth_getProofRPC` invocation which can automatically get required demonstration data from the running ETH nodes. We can convey the demonstration data to oracle contract and verify the demonstration in the smart contract.

In the future, the realization of automatic sliding window is only applicable to the last 256 blocks (about 1h), because only these blocks can access their hash values from the contract. However, this may be changed in the future as Vitalik proposed EIP-2935. It is scheduled to provide an independent contract in EIP-2935 to ensure hash values of all historical blocks. As a result, SumSwap V3.0 Oracle with Merkle demonstration will be stronger.

## VI. Token design

### 6.1 SUM issue

The quantity of SUM tokens and issuing method are not changed. A total of 320 million SUM tokens will be issued in 10 years through the base index method, of which 90% tokens are produced through mining. (The following shows the issuing quantity of SUM tokens in each stage. The 54000 ETH blocks are considered as one day and the duration in each stage may be different due to different running speeds of ETH block.)

Detailed algorithm:

The increased original base value per month in the first issuing stage is 6%. The monthly issuing quantity is calculated with the formula Y (monthly issuing quantity), X (month). If  $x = 1, 2, 3, \dots$ , then:

$$y = 32 \text{ million} \times 1.06^{(x-1)} \times 6\%$$

$$y_1 = 32 \text{ million} \times 1.06^{(1-1)} \times 6\% = 1,920,000$$

$$y_2 = 32 \text{ million} \times 1.06^{(2-1)} \times 6\% = 2,035,200$$

$$y_3 = 32 \text{ million} \times 1.06^{(3-1)} \times 6\% = 2,157,312$$

and so on, then the daily issuing quantity in the first month is  $1.92 \text{ million} / 30 = 64000 \text{ SUM}$

It can be calculated that 64000 SUM tokens can be issued per day in the first month. According to the time schedule, it is now the 4<sup>th</sup> month for issuing SUM tokens.



Fig. 9 Issuing cycle of SUM

## 6.2 Effect of SUM token

As the fuel and governance certificate of the whole system, Sum token can maintain stability of the whole system, and expand the system.

### 6.2.1 DAO governance

The user who holds SUM tokens can vote for decentralized governance for the project.

### 6.2.2 Buy-back with service charges

The platform will regularly repurchase SUM tokens with profits of the service charge.

### 6.2.3 Voting for mining right

The user who holds SUM token can determine participation of new online trading pair in SUM mining.

### 6.2.4 Various preferential rights

The user who holds SUM token can enjoy platform activities and preferential experience.

## VII. Mining design

### 7.1 Staking

Earnings of SUM-holding Staking (3/10 of daily tokens)

Earnings of ecological Staking (3/10 of daily tokens, only two-level for ecological hash rate)

Settlement for once every 5400 blocks

#### 7.1.1 SUM-holding Staking

The inverted jump ranking weighted algorithm is used for SUM-holding Staking.

Earnings of SUM-holding Staking for A:

$$A_i = M_i / (M_1 + M_2 + M_3 + \dots + M_n) \times W \times 30\%$$

( $M_i$ : jump ranking for individual holding SUM;  $W$ : total number of SUM tokens of the day;  $A_i$ : earnings of SUM-holding Staking for the player of the day.  $M_1, M_2, M_3, \dots, M_n$ : jump ranking for holding different SUM tokens)

Example: If there are total 12 users in the whole system, then the quantity of SUM tokens and ranking are listed as below:

Number of SUM tokens	300	300	300	300	300	300	300	300	301	302	999,000	9 million
Ranking	1	1	1	1	1	1	1	1	9	9	11	12
Zone	Common zone for users holding SUM tokens								The best zone for holding SUM tokens	The worst zone for holding SUM tokens		

The following graph of earnings can be obtained based on calculation results. The earnings rate is not ideal for users who hold a small number of SUM tokens and users who hold a large number of SUM tokens, but the earnings rate is ideal for users who hold a medium number of SUM tokens.

The design can effectively balance the number of SUM tokens in the whole systems, promote sound development of SumSwap V3.0, and encourage users to hold an appropriate number of SUM tokens.



Fig. 10 Ranking of earnings for holding SUM

### 7.1.2 Earnings of ecological Staking

The two-level hash rate of activated users is used for calculating the hash rate of ecological Staking, for example, A invites C, B invites C, and C continues such invitation, but the hash rate of A can be used for calculating hash rate of B and C only, except C and below.

In addition, the ecological earnings are changed from 4/10 of original daily SUM tokens into 3/10 of daily SUM tokens.

Other algorithms are not changed as below:

Calculation formula for earnings of ecological Staking

$$A = \frac{A_i \text{ (Hashrate of A)}}{A_i + B_i + C_i + \dots + N_i \text{ (Total hashrate of the network)}} \times W \times 40\%$$

$$A_i = \sqrt[3]{P_{\max} + P_1 + P_2 + P_3 + \dots + P_n}$$

( $A_i$ : hash rate of A;  $W$ : total number of SUM tokens of the day)

( $P$  is SUM capacity of each zone;  $P_{\max}$  is the number of SUM tokens for the zone the maximum capacity)

If  $P = P_{\max}$ , the cube root is extracted directly;

If  $P > 10000$ , the value  $10000 \times 10 + (P - 10000)$  is taken;

If  $P \leq 10000$ , the value  $P \times 10$  is taken.

#### Summary of rules

Clearly, it is not true that the larger the number of SUM tokens for activated user is, the more the earnings of inviter will be in the design of ecological Staking. Instead, if there are more user accounts are activated and these users hold an appropriate number of SUM tokens, then the earnings of inviter will be larger.

It means that more users shall be invited and activated users shall hold appropriate number of SUM tokens to get more earnings of ecological Staking.

## 7.2 Proportion of mining with Earning

The proportion of mining with Earning is 40% of daily SUM output, including mining through addition of liquidity and mining through trading. The mining through addition of liquidity is 2/3 of the total earnings, while the mining through trading is



1/3 of the total earnings.

Cycle:

The withdrawal can be executed for once for mining with Earning every 5400 ETH blocks. It requires that there is a certain number of SUM tokens in the account address. In a cycle:

Withdrawal conditions:

It stipulates that “at least 100SUM shall be kept at the user address” and “number of SUM tokens at the user address is larger than and equal to 1/10 of mined SUM tokens at the user address”.

You can access the “earnings” page and click “extract” button to extract SUM tokens mined with Earning.

Training pairs for mining:

The mining of SUM/USDT liquidity pool is 60% of the total output;

The mining of DAI/SUM liquidity pool is 20% of the total output;

The mining of ETH/USDT liquidity pool is 10% of the total output;

The mining of ETH/DAI liquidity pool is 5% of the total output;

The mining of ETH/USDC liquidity pool is 5% of the total output.

The above are common trading pairs with rate 0.3%. Users can mine SUM tokens through adding liquidity to the above liquidity pool or being involved in the trading of the above trading pairs. SumSwap V3.0 adds liquidity by zone in the mining of liquidity pool, so that the number of SUM tokens in each cycle (every 5400 blocks) of each trading pair is calculated by the proportion of service charge from user



assets in the total service charges of current trading pair in current cycle, and the same method is also used for the mining through trading.

It is noted that the above trading pairs for mining and mining proportion will be adjusted based on future development of SumSwap V3.0.

### 7.3 Design of service charge

The 1/10 service charges are exempted for trading of activated account;

The project party can get 1/6 service charges of trading each time for project development and operation;

The inviter can get 1/10 service charges of activated account;

The liquidity is added in the limit price range to get the service charge of trading.

## VIII. Future prospect

### 8.1 Current situations of CeFi market

CeFi (centralized finance) mainly focuses on the centralized exchange which also provides loan and financial products in addition to its own trading. For CeFi, there are many risks, for example, non-transparent operation, black box operation, and market control. Besides, if CeFi assets are kept in the centralized exchange, it is easily to see that the exchange is attacked or bankrupted, resulting in loss of users' assets.

In addition, the centralized exchange may easily monopolize the industry development after being stronger, which will influence industrial development. Moreover, the centralized exchange manages almost the majority of digital assets in the market.

### 8.2 Gradual development of DeFi

Since the early of 2020, DeFi has been accepted and recognized. Due to trading transparency, assets safety, monopoly and other problems, more and more users focus more on decentralized exchange. The uniswap is taken for an example. Since its emergence, the total trading volume has reached hundreds of billions of dollars.

It is the result of innovation. Many technological geeks have made various innovations in exchange, for example, constant product trading and market making and mining through AMM liquidity, so that various decentralized exchanges are widely accepted.

### 8.3 Diversified DeFi ecology

According to statistics of professional organization, the market value of DeFi locked position or total market value of DeFi token has exceeded USD 20 billion.

The diversified DeFi ecology includes decentralized trading, decentralized loan, decentralized synthetic assets, and algorithm stable coins, etc.

The decentralized trading includes the most famous SumSwap V3.0 and Sushiswap; top decentralized loan Aave, Compound and Maker; decentralized synthetic asset Synthetix; and other assets such as renbtc.

#### 8.4 Characteristics of SumSwap V3.0 project

Safe, transparent, and decentralized. All trading will be made on the ETH chain. After safety audit by system, the trading data will be transmitted to the chain to realize safety and transparency of the whole system.

Strong expansion and Staking mechanism. Based on the SUM-holding staking and ecological Staking, users can get earnings through holding and sharing SUM tokens. The rules can be expanded strongly. The flexible earnings design and mining design with Earning allow the addition of liquidity and trading of digital assets to have SUM earnings. The service charge can be exempted through activating account and users can get bonus of service charge from the subordinate trading.

Safe assets and independent management for assets. Different from the centralized exchange, SumSwap V3.0 will not touch any asset of users. In the whole process, assets are always kept and managed by users with private key.

SumSwap V3.0 ecology. SumSwap V3.0 is an integrated product of DeFi ecology, which will depend on the decentralized exchange in the early stage and gradually expand the trading system of stable coins, loan system, and algorithm arbitrage system in the later stage.

SumSwap V3.0 target. The daily trading amount of top 6 centralized exchanges reached over USD 10 billion, but the daily trading amount of top 5 decentralized exchanges was less than USD 10 billion, and the trading amount of following decentralized exchanges was lower. Standing on the shoulders of giants, SumSwap V3.0 hopes to create a decentralized exchange that is comparable with centralized exchange through integrating mathematical algorithms. In the future, more decentralized businesses will be expanded based on the decentralized exchange.



Since the emergence of ETH in 2014, the smart contract has created infinite possibilities for various decentralized apps. Since then, many technological geeks have been researching and developing many decentralized apps.

Depending on innovative experiments and technical development for many years by many technological geeks, various smart contracts sprung up in 2020, of which the most famous contract was DeFi app. In addition, other apps such as Oracle, DAO, and NFT also develop gradually. Undoubtedly, some decentralized apps that can change the industrial pattern will come soon!

The decentralized market has been mature gradually and epochal products will come soon! SumSwap V3.0 will grasp the opportunity to expand DeFi market and become the leader of the domain.

## IX. Risk and disclaimer

The document is used for providing related information only, instead of constituting any comment and suggestion about the digital asset trading. The above information or analysis will not constitute investment decision or specific suggestion.

The document will not constitute investment, legal, tax, regulatory, financial, and accounting suggestions and the like. Before participating in the SumSwap V3.0 project, potential participants shall consult their own legal, investment, tax, accounting consultant or other consultants in advance to determine potential benefits and risks of such trading and undertake related consequences.

The schedule in the document is not constant but will be adjusted based on the market environment.

The project team will try their best to do everything. As an innovative asset, the cryptocurrency is risky to a certain extent, so that participants shall make decisions cautiously and the project party will not make any guarantee for the return on investment.