HotPot Fund V2 White Paper

- HotPot Fund V2–White Paper

Contents

1. Summary

This document is the technical white paper of the Hotpot Fund V2. It comprehensively demonstrates the design ideas behind Hotpot Fund smart contracts. With the release of Uniswap V3, the Hotpot Fund has also been upgraded accordingly. Hotpot Fund V1 is all invested in Uniswap V2 liquidity pool; similar to V1, V2 is all invested in Uniswap V3 liquidity pool. Meanwhile, Hotpot Fund V2 has made some upgrades: Anyone with liquidity pool investment experience can create a fund through the Hotpot fund platform; fund investment is no longer restricted by the fund's local token, and can invest in any trading pairs of Verified Token. The burn mechanism of the fund governance token HPT is more flexible.

2. Introduction

In the field of Defi (Decentralized Finance), a decentralized exchange (DEX) driven by an automated market-making protocol (AMM) can provide services for traders to complete transactions by converging liquidity and algorithms. Presently, the decentralized exchange represented by Uniswap has become one of the most important use case of blockchain technology.

Decentralized exchanges provide services for transactions by converging liquidity. In theory, anyone can become a Liquidity Provider, but in fact, to provide liquidity efficiently requires professional knowledge, in-depth data analysis and corresponding automation tools. The original intention

of the Hotpot fund is to create valuable liquidity gains by merging user's fund, managed by a professional fund team; to create valuable liquidity gain under the prerequisites of open source code, transparent operation, and user funds security.

Firstly, let's briefly review the Hotpot Fund V1. We have implemented the following feature in V1:

1. Through a set of smart contracts on the Ethereum blockchain, gather user funds to invest in the Uniswap V2 liquidity pool;
2. Each fund is settled by a fund's local token, user deposits and withdrawals, and asset accounting are all based on the fund's local token;
3. User can deposit and withdraw at any time, and the user's funds are always controlled by the user's own wallet;
4. Fund manager completes investment operations in a unified approach, and he or she can invest, remove from liquidity pool, and adjust trading pairs. Fund manager's investment operations are restricted: he or she can only invest in trading pairs that include the fund's local token, and the other token in the trading pair must be a verified token. Fund manager can invest in multiple trading pairs, but he has no right to transfer funds for any other purpose.
5. 20% of user's income is used to purchase and burn project governance tokens in Uniswap to reflect the value of governance tokens.

With the release of Uniswap V3, it has significantly upgraded the Automated Market Making Agreement (AMM). The core is to introduce the concept of Concentrated Liquidity, which prominently optimizes the

efficiency of funds and made big changes in the provision of liquidity. We can interpret the concentrated liquidity of Uniswap V3 can as one modification made to the inverse function of x*y=k , which is similar to calculus transformation. Meanwhile, using the logarithm of the price as price ticks (geometric average price) can distribute prices more evenly.

At the same time, Uniswap V3 increases the difficulty of liquidity provision. In order to obtain higher capital utilization, liquidity providers need to frequently adjust their investment positions. For investors of small amount, liquidity gains may not be enough to cover the gas cost of their investments. Also, for retail investors, their weaknesses of lacking of in-depth data analysis and corresponding automated tools are especially obvious.

In this document, we comprehensively introduced Hotpot Fund V2, a fund that invest in Uniswap V3 liquidity pool. It enables fund managers with professional knowledge and tools to efficiently employee user funds to create liquidity income through funds gathering.

V2 provides some new features, while maintaining the same key features of Hotpot Fund V1:

1. Position management: Uniswap V3's concentrated liquidity has changed the way of liquidity investment. As a fund that invest in Uniswap liquidity pools, in addition to managing trading pairs, Hotpot funds need to further manage investment positions. Unlike Hotpot Fund V1, which only needs to manage trading pairs, fund managers need to

manage investment positions more meticulously inV2, and adjust investment positions in a timely manner based on price fluctuations in order to improve capital efficiency.

2. Factorization: Every fund is created through a factory contract. Anyone can use the factory contract of the Hotpot Fund to create a fund that invest in Uniswap V3 liquidity.

3. Investment is no longer restricted by the fund's local token: Hotpot Fund V1 is restricted to only invest in trading pairs containing the fund's local token, but V2 no longer contains this restriction. Hence, except for the fund's local token, the fund manager needs to set swap pathes for each token in the investment trading pair, and each token in the pair must be verified.

4. 20% of user income is still used for fund sharing, but the method has changed: 10% of the income is paid to the fund manager in the form of the fund's local token, to cover the cost of the fund manager; 10% of the income is used to purchase and burn the project governance tokens to reflect the value of governance token. The path of purchase and burn can be set by the governance account to realize the purchase and burn operations of various fund's local token to HPT, thus having a more flexible burning mechanism. All purchase paths need to go through the Uniswap V3 WETH9/HPT (fee rate 0.3%) trading pair.

3.Asset Accounting

Hotpot Fund V2 still uses the fund's local token for asset accounting; user deposits and withdrawals also in the form of fund's local token.

Hotpot Fund V2 still uses ERC20 tokens to calculate and manage users' fund shares. When the user deposits, the share token is minted; when the user withdraws, the share token is burned. Fund shares can be transferred and sold. For details about the calculation and transfer of fund shares, please refer to the V1 white paper.

Hotpot Fund V2 no longer manages airdrop or mining UNI assets.

3.1 Total assets

The assets of Hotpot Fund V1 are composed of multiple investment trading pairs, and the asset accounting method of each trading pair is very simple:
the liquidity's corresponding amount of fund's local tokens * 2.

This is determined by the characteristics of Hotpot Fund V1 and Uniswap V2: V1 fund must contain the fund's local token, and the values of two tokens in Uniswap V2 trading pair are equal.

The assets of Hotpot Fund V2 are composed of multiple positions of multiple trading pairs, and the total assets of the fund are derived from the sum of all position assets:

$$Total\ Assets = \sum_{i=0}^{n} Assets_i$$

Because total asset accounting needs to iterate over the array , the Hotpot Fund smart contract uses a two-dimensional dynamic array to manage positions.

3.2 Position assets

The fee of Uniswap V3 is no longer automatically accumulated to liquidity assets, but is stored separately in the form of tokens. Therefore, the assets of each position are composed of liquidity assets and the fee.

3.2.1 Liquidity assets

Liquidity assets are no longer the equivalent distribution as Uniswap V2, but are related to the position's liquidity quantity, its price ticks interval, and the current price of pool:

◦When the pool's current price is below the price ticks range($i_c < i_l$),all assets are token 0 (denoted as X);
◦When the pool's current price is above the price ticks range ($i_c \geq i_u$), all assets are token1 (denoted as Y);
◦When the pool's current price is within the price ticks range ($i_l \leq i_c < i_u$), liquidity assets are composed of X and Y. Its calculation rules can be understood as: the price rises from the current price to the upper tick, how many X can be sold (after the upper price tick has been crossed, all assets are replaced by Y); and the price falls from the current price to the

lower tick, how many Y can be sold (after lower price tick has been crossed, all assets are replaced by X).

The following calculation formula comes from the Uniswap V3 white paper:

$$\Delta Y = \begin{cases} 0 & i_c < i_l \\ \Delta L \cdot (\sqrt{P} - \sqrt{p(i_l)}) & i_l \le i_c < i_u \\ \Delta L \cdot (\sqrt{p(i_u)} - \sqrt{p(i_l)}) & i_c \ge i_u \end{cases} \tag{3.1}$$

$$\Delta X = \begin{cases} \Delta L \cdot (\frac{1}{\sqrt{p(i_l)}} - \frac{1}{\sqrt{p(i_u)}}) & i_c < i_l \\ \Delta L \cdot (\frac{1}{\sqrt{P}} - \frac{1}{\sqrt{p(i_u)}}) & i_l \le i_c < i_u \\ 0 & i_c \ge i_u \end{cases} \tag{3.2}$$

3.2.2 Fee

The fee of Uniswap V3 is stored separately in the form of token and is no longer added to the liquidity automatically. Each position records its settled Tokens Owed; but since this variable only records the transaction fee that has been settled, which does not fully reflect the position assets. For position assets, settlement will only be performed when the position withdrawing the commission (burn or collect function is triggered).

So, in addition to the settled commission, it is necessary to calculate the already incurred but not yet been settled handling fees during the transaction. In other words, in addition to the settled fee for each position, there is also a part of the fee that has been incurred during the transaction but has not yet been settled for the position. Funds are not

the same as ordinary liquidity providers, complete assets need to be taken in to calculation, so they need to take into account the unsettled fees.

The calculation of the fees involves the following variables. Since the fees of token0 and token1 need to be stored separately, there are actually two figures for each of variables. Since all fees stored are fee of per unit liquidity, its value is a floating-point number, therefore the actual storage and calculation are all done with 128-bit left shift process.

- feeGrowthGlobal: It saves the total amount of fee per unit of virtual liquidity (L) in the entire contract life cycle, and it is a progressive value.
- feeGrowthOutside variable on the price ticks: It is used to save the accumulated fee in a given price tick and is updated when the price tick is crossed.
- Current price: this determines whether the price ticks range of the position can receive fee income.
- feeGrowthInsideLast: used to save the fee of the position's last settlement, as the basis for the calculation of the next settlement. Update will be done when the position's fee is settled.
- tokensOwed: Update will be done when the position's fee is settled or collected.

The logic for calculating all fees for a position is:

- Step 1: Calculate the unsettled feeGrowthInside (f_{i_l,i_u}) for the position.
- Step 2: Subtract the feeGrowthInsideLast for the last update of the

position.

- Step 3: Add the settled fees tokensOwed for the position.

Depending on whether the current price is within or outside the ticks range---that is, the current tick index i_c is greater than or equal to i, the following formula can be used to calculate the liquidity perunit, fees received above the tick i (f_a) and below the tick i(f_b):

$$f_a(i) = \begin{cases} f_g - f_o(i) & i_c \geq i \\ f_o(i) & i_c < i \end{cases}$$

$$f_b(i) = \begin{cases} f_o(i) & i_c \geq i \\ f_g - f_o(i) & i_c < i \end{cases}$$

Then use the following formula to calculate the unsettled fee feeGrowthInside (f_{i_l,i_u}), between the two ticks(the lower boundary of the range i_l and the upper boundary of the range i_u), the total amount of accumulated fees:

$$f_{i_l,i_u} = f_g - f_b(i_l) - f_a(i_u)$$

For the derivation process of the above formula, please refer to the Uniswap V3 white paper.

3.2.3 Convert into fund local token assets

The calculated result of fees and liquidity assets is the quantity of token0

and token1, which need to be converted into assets measured in the fund's local token. According to the set token swap path, the current exchange rate between each token and the fund's local token can be obtained, and then token0 and token1 assets can be converted into fund's local token assets.

Because the price can be changed, any scenario that needs to rely on the exchange price for asset accounting; must carefully consider the way the price is acquired. In the Defi field, there are numerous security incidents due to price manipulation. Especially through flash loans, an attacker can lend a large amount of assets in a transaction to manipulate the price, which significantly reduces the cost of the attack. Presently, Using flash loans to manipulate prices and attack Defi projects is a common attack method.

Hotpot Fund V2 uses price oracle machine of Uniswap V3, which has been upgraded compared to V2's oracle machine mechanism. The V2 oracle mechanism requires the external caller to record the data of the two observation points to obtain the oracle price, so it cannot be used by other smart contracts that require instant accounting; after the upgrade, other smart contracts can obtain the price of the oracle between two or more observation points from the V3 oracle. For more details, please refer to the Uniswap V3 white paper.

After using the Uniswap V3 oracle machine, the exchange price of the hot pot fund for asset accounting is the price of the most recent transaction before the block of this exchange. Even if an attacker

manipulates the current price through a flash loan, it cannot change the result of the current asset calculation, therefore increases the difficulty of the attack significantly.

The calculation process of asset accounting did not take into consideration of the impact of slippage and fees in actual swap process. However, this is reasonable, since the current fund assets should not consider the slippage and fees in the swap process.

3.2.4 Uniswap V3 peripheral position management contract is not used

The Uniswap V3's core contract does not realize the tokenization of position assets, but is realized in peripheral contracts. Unlike Uniswap V2, which uses ERC20 token to represent liquidity shares, in peripheral contracts of Uniswap V3, ERC721 (ie: NFT) token are used to represent each position.

The position management contract in the peripheral contract does not realize the accounting for unsettled fees. Therefore, the Hotpot fund does not use peripheral contracts to manage positions. Not using peripheral contracts to manage positions, that means the Uniswap V3 position assets held by the Hotpot fund are not visible in Uniswap V3 Graph queries.

4. Fund Manager

Modification of factorization has been done to Hotpot Fund V2's smart contract. Now, any person or institution with liquidity pool investment experience can create and manage funds on Hotpot Fund and act as a fund manager.

4.1 Create Fund

Only need to specify a fund's local token, give a name of the fund, and give a brief introduction (the length of the name cannot exceed 8 bytes, and the length of the introduction cannot exceed 24 bytes) to create a fund.

4.2 Set Swap Path

Firstly, The fund manager needs to set the swap path for the two tokens in the trading pair which he intends to invested, unless the token is the fund's local token. The swap path of each token includes a Buy Path and a Sell Path.

The swap path of Hotpot Fund V1 also includes the Curve liquidity pool, especially for swap between stable coins. The slippage of Curve is lower than that Uniswap V2. Since Uniswap V3 greatly optimizes capital efficiency. its swap slippage is also been optimized; all built-in swaps of Hotpot Fund V2 are completed in Uniswap V3 and no longer rely on other projects.

The fund manager cannot modify the trading path at his pleases. If the trading path is to be modified, all liquidity pools containing the target token must first be cleared of all positions. This is to prevent fund managers from stealing users' assets by modifying the transaction path.

4.3 Investment Operations

There are 4 kinds of investment operations for fund manager: init (initialize a position), add (investment), sub (withdrawal), and move (adjustment).

When initializing a position, you can invest or not. While invest, you needs to specify the amount of local token. While sub or move, it is not refer to the quantity of liquidity, but the proportion of liquidity to be subbed or moved. Since the fee of Uniswap V3 is not automatically reinvested, an option is given in add function, you can choose whether to reinvest the incurred and settled fees.

4.3.1 Calculating Investment Distribution

When invest (add) or adjust (move), it is necessary to calculate the distribution of these two tokens.

When investing, there are three types of tokens: the fund's local token, the collected fee of token 0 and token1.

When calculating the investment distribution, we first convert the fund's local token and token1 into the equivalent amount of token0 with the

current price, denoted as A .

Then, use the total quantity of token0 (A), combined with the price range of the position and current price of the pool, to calculate the distribution of token0 and token1.

Knowing the total quantity of token0 (A), the current price is $P = \frac{y}{x}$, the upper boundary of position's price is P_l ,and the upper boundary of the position's price is P_u .
we needs to calculate the quantity of token0 Δx And the quantity of token1 Δy .

When the current price is below the position's price range, all invested assets are token0:

$$\begin{cases} \Delta x = A & (P \le P_l) \\ \Delta y = 0 & (P \le P_l) \end{cases} \tag{4.1}$$

When the current price is above the position's price range, all invested assets are token1:

$$\begin{cases} \Delta x = 0 & (P \ge P_u) \\ \Delta y = A & (P \ge P_u) \end{cases} \tag{4.2}$$

When the current price is within the price range of the position, the invested asset is partly token0 and partly token1. We assume that the exchange between token0 and token1 can be completed at the current price, and also does not consider swap slippage and fees. The following formula can be obtained:

$$\Delta x + \frac{\Delta y}{P} = A \tag{4.3}$$

According to formulas (3.1) and (3.2), we can get:

$$\frac{\Delta x}{\Delta y} = \frac{\frac{1}{\sqrt{P}} - \frac{1}{\sqrt{P_u}}}{\sqrt{P} - \sqrt{P_l}} \tag{4.4}$$

From formulas (4.3) and (4.4), the required quantity of token0 can be obtained. The quantity of token1 can be calculated from the quantity of token0. The calculated formula is:

$$\Delta x = \frac{A}{1 + \frac{\sqrt{P_u} \cdot (\sqrt{P} - \sqrt{P_l})}{\sqrt{P} \cdot (\sqrt{P_u} - \sqrt{P})}} \qquad (P_l < P < P_u) \tag{4.5}$$

$$\Delta y = (A - \Delta x) \cdot P \qquad (P_l < P < P_u) \tag{4.6}$$

After obtaining the quantity of token0 and token1 of the investment distribution, the fund's local token and fee are exchanged to the corresponding number of token0 and token1 respectively. The current price conversion method does not consider the slippage and fee during the actual exchange, so some token0 or token1’s dust may incurre, and lastly the remaining token0 or token1 needs to be swaped back to the fund's token.

The fund manager only needs to specify the amount of investment in the local token, and Hotpot Fund V2 completes the corresponding calculation, swap and investment in a transaction, which can save the fund manager's gas consumption efficiently.

4.4 Profit

When the user withdraws, 10% of his income will be paid to the fund manager in the form of the fund's local token to cover the cost of the fund manager.

Special treatment has been made to WETH9 fund: when the user withdraws from the WETH9 fund, he will receive ETH; and the share received by the fund manager is WETH9, which is not converted into ETH.

5. Governance

Hotpot Fund V2 still has a governance account, and the governance account has only two permissions: set verified tokens and set burning pathes.

At the beginning phase, the governance account is controlled by the project team, and should be considered to hand over power to the community in future.

5.1 Set Verified Tokens

The investment scope of fund manager is limited to verified tokens to avoid potential security risks.

5.2 Set Burn Path

When the user withdraws, 10% of his income is paid to the controller

contract in the form of the fund's local token, and this part of the share belongs to the HPT token holders. The controller contract provides a public harvest function. Anyone can use this function to purchase and burn HPT tokens from Uniswap V3.

Hotpot Fund V1 has established multiple trading pairs in Uniswap V2 for purchase and burn of HPT tokens. In Hotpot Fund V2, only one trading pair is established in Uniswap V3: WETH-HPT, with a fee rate of 0.3%. All fund local tokens need to set up a burning path to reflect the fund's profit in the value of HPT tokens.

6. Disclaimer

This document is a technical white paper, used for general purposes only. This document does not constitute any recommendation for investment, nor does it contain any recommendation for purchase or sale. It should not be used as a reference for making any investment decisions. This document describes the current technical design ideas of the hot pot fund team. If these design ideas change, we will not notify you otherwise.

Reference

- Hotpot Fund V1 White Paper (EN / CN)
- Uniswap V3 White Paper (EN / CN)
- HotpotFunds V2 code
- Uniswap V3 code (core / pheriphery)

HotPot Fund

Let the professionals handle professional issues.