Hotpot Fund

White Paper

1/2/2021

+++

Contents

1. Summary

This document is the technical white paper of the Hotpot Fund V1. It comprehensively demonstrates the design ideas behind Hotpot Fund smart contracts.

This document covers all key designs of Hotpot Fund, includes: the way of fund deposit and withdraw; the calculation method of fund profit and loss; fund share calculation and transfer mechanism; the design of investment portfolio, the investment pairs must contain the fund's local currency; the range of investment operations that can be done by the fund manager, the restrictions that are placed on the fund manager's investment operations, based on security considerations; the fund may mine UNI using their liquidity pool share, and how to manage and distribute UNI assets; the basic information about HPT token, and how can HPT token holders capture fund profits.

2. Introduction

The Hotpot Fund is a transparent fund project on the public blockchain, consisting of a set of smart contracts deployed on the Ethereum blockchain.

Here, the term "transparency" refers to the Hotpot Fund contracts are all open source and with security audit and verification, the operations of the fund manager are transparent, the fund's investment choices and proportion are transparent, the user is anonymous and anticensorship. This is determined by its own characteristics of the Ethereum blockchain, not the exclusive characteristics of the Hotpot Fund.

3

Hotpot Fund V1 is all founded by the fund of Uniswap V2 liquidity pool. Uniswap is a decentralized exchange on the Ethereum blockchain, well-known for its constant product and automated market making. It is currently the largest decentralized exchange by volume and number of users. Since Uniswap liquidity pool providers can share the 3‰ fee charged by the exchange, they can create certain returns for investors, but the price fluctuation of crypto currency could also bring unpredictable losses for investors who hold coins. Therefore, investing in Uniswap liquidity pool requires professional knowledge and in-depth analysis. To this end, Hotpot Fund was born.

Through Hotpot Fund, crypto currency investors can easily obtain the profits of investing in the Defi project.

Investors can deposit in the fund smart contract at any time, and withdraw from the fund contract at any time, deposit and withdraw are all calculated in the local currency of the fund. For example, the deposit and withdraw of DAI fund are all made in DAI tokens. Investors deposit in the fund and the fund manager carries out rollup investment operation. The fund manager can only make investment portfolio strategy within a limited scope and has no right to transfer any assets in the smart contract.

When investors withdraw from the fund contract, 20% of their profits will be paid to HPT token holders. If the user has a loss, they must first make up previous loss, then pay the share of the fund.

3. Characteristic

3.1 Deposit and Withdraw

In Hotpot Fund, investors deposit and withdraw are all operated in the local currency of the fund. For example, DAI fund, the investors deposit DAI, also when they withdraw from DAI. The same goes for ETH, USDT, USDC funds.

Since the assets held by the Fund are Uniswap liquidity pool share, when investor withdraw, the fund completes the operation by swapping corresponding proportion of assets from the Uniswap liquidity pool into the fund's local currency and transfer them to the investor in one transaction. Swap on Dex inevitably occurs a slippage, therefore in reality investors obtain slightly less currency than they display. For large investors, they should consider withdrawing in batches.

If the investor make a profit, 20% of the profit is paid to the HPT token holder when the investor withdraws it. If the investor does not make a profit, there is no fee applied withdrawing, and the investor's subsequent investment income will cover the previous loss, and the share will not be paid until the total profit is made.

UNI is the only exception on access currency: if UNI mining is restarted, the Hotpot Fund mined UNI tokens will not to be swapped to the fund's local currency, but return UNI directly to the investor.

3.2 Fund Share

3.2.1 Calculation

Hotpot funds use ERC20 token to calculate users' fund share. When investor deposit, share tokens are minted; When investor withdraw, the share tokens are burned.

The token amount deposited by the user in the Hotpot Fund is denoted as

Amount, the total issued share of the fund is denoted as Total Supply, and the current total value of the fund is denoted as Total Assets.The number of fund share tokens obtained by the first investor is:

$$Share = Amount$$

The calculation formula for the number of fund share tokens obtained by subsequent investor is as follows:

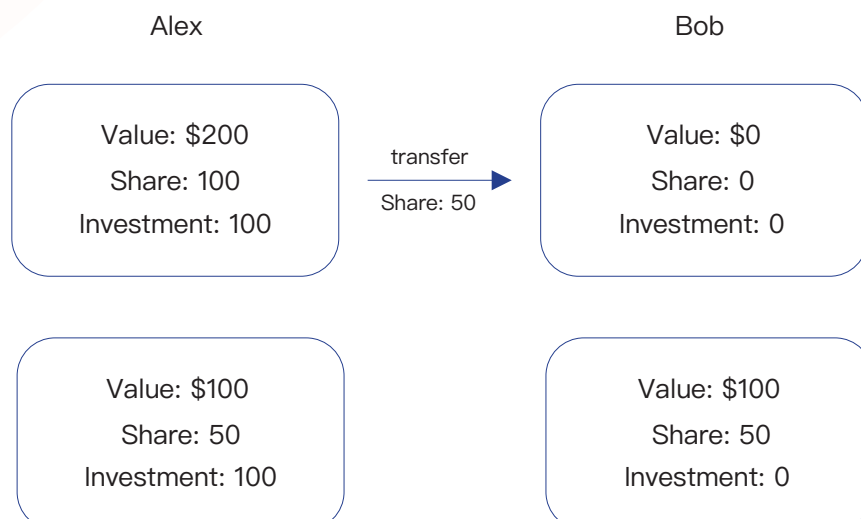$$Share = Amount * \frac{Total\ Supply}{Total\ Assets}$$

3.2.2 Transfer

Since the fund shares themselves is ERC20 token, investor's fund shares can be transfer to other account and can also be traded. When investor transfer fund shares, their investment will not be transferred, which means:

1. For the investor who transfer out, due to the amount of investment does not decrease, when he/she withdraw the remaining fund share, the calculated profit is less than the real situation, so less share is paid to the fund.

2. For the investor which transfer in, due to the amount of investment is not increased, the profits calculated more than the real situation at the time of withdraw, so the investor pay more share to the fund.

As shown in figure:

Alex   Bob

Value: $200		Value: $0
Share: 100	transfer →	Share: 0
Investment: 100	Share: 50	Investment: 0

| Value: $100 | | Value: $100 |
| Share: 50 | | Share: 50 |
| Investment: 100 | | Investment: 0 |

The consideration for this design is: we assume that when the investor transfer the fund share, he/she has already obtained the income from the recipient through other means, and the way to obtain the income is accomplished outside the fund system, not within the scope of the fund management. As shown in the figure above, Alex's nominal earning is 0 (Value $100, Investment also is $100), but the share of the fund sent to Bob should have earned a profit; Bob should have known his fund shares does not have any investment so when he withdraws he will have to pay shares to the fund in full.

3.3 Investment Portfolio

Hotpot Fund V1 are all invested into the Uniswap V2 liquidity pool. Each fund can invest in one or more Uniswap trading pairs, and the trading pairs must contain the fund's local currency. Investing in multiple trading pairs means Hotpot funds hold a portfolio rather than a single asset. The assets held by the Hotpot fund include the local currency assets of the fund, as well as certain Uniswap V2 liquidity pool assets (which it invests in). Portfolio position matching and subsequent investment allocation are adjustable, so that the fund manager's operation has limited flexibility.

As shown in figure:
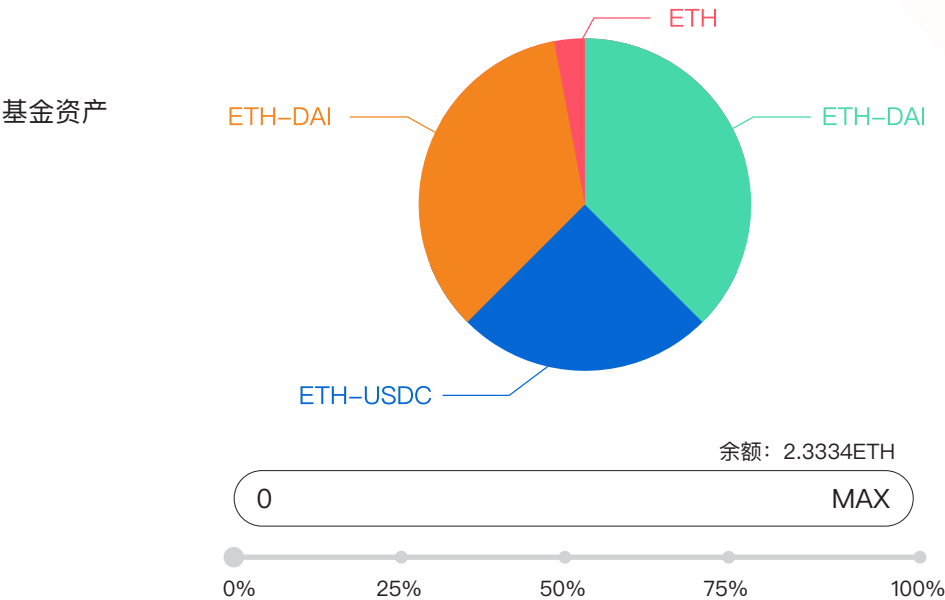
This is the testing investment portfolio of Hotpot Fund and ETH Fund on ropsten, which holds 4 assets: the fund's local currency ETH and the liquidity pools of 3 trading pairs –– ETH–USDT, ETHUSDC, and ETH–DAI.

Hotpot Fund investment income is calculated in terms of the fund's local currency; in order to calculate the value of the investment, the trading pair must contain the fund's local currency.
As shown in figure:

DAI funds

> ETH: 100
> DAI: 50,000
> (WETH–DAI)
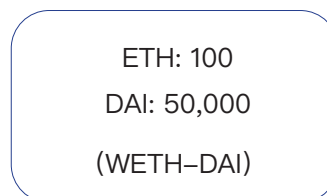
DAI Fund holds 100 ETH + 50,000 DAI in the WETH–DAI trading pair, which is simple when calculating the value of the fund:

$$50,000 \ DAI * 2 = 100,000 DAI$$

The result is obvious. This is determined by the characteristics of Uniswap: the value of the two tokens equals in the trading pair. But if the trading pair does not include the fund's local currency, there is no price anchor while calculating the fund's value. If the off–chain price oracle is introduced to obtain the price of the substitute currency, it will inevitably introduce additional complexity, and brings security risks. Therefore, we sacrifice flexibility here, the trading pair must contain the fund's local currency, which limits the fund manager's operation and prevent him from invest in any random trading pair.

3.4 Investment Operations

When the investor deposit in, the currency is not immediately invested in

Uniswap liquidity pool, but it is invested under the fund manager's concentrated operation.

3.4.1 Save Gas

Suppose DAI Fund invests in two Uniswap V2 trading pairs. To complete the investment actions of these two trading pairs, investors need to perform two swaps and two Add Liquidity operations, and the amount of Gas consumed is about 600,000. Take the Gas Price of 50 GWei as an example, it is 0.03 ETH. The Gas consumption deposit in the hotpot fund is about 150,000, which is 0.0075 ETH, saving 0.0225 ETH Gas consumption, which is $13.5 calculated at the ETH price of $600. It's important to save Gas for investors when they don't have much money to invest. If the hotpot fund investors make a lot of small investments, the accumulated Gas consumption saved will be a meaningful saving.

The fund manager will invest after the funds have accumulated to a certain amount, thus saving Gas consumption per unit investment.

3.4.2 Only Invest the Trusted Tokens

Trusted tokens are set by the governance account, and fund managers can only invest portfolios within trusted tokens. Fund manager account is the account that should perform daily investment operations, and governance account is low frequency operation account, the separating design of governance account and fund manager account avoided the potential safety risk of fund manager's account. Meanwhile, reserving the extensibility of the fund governance power when handling to Autonomous community.

3.4.3 Operation Types

The types of the fund manager's investment operations include: set the proportion of each trade pair and invest, add and remove liquidity of trading pairs, and adjust the invested liquidity pool.

3.5 Built-in Swap Using Uniswap or Curve

When users withdraw and fund managers invest and adjust the liquidity pool, the Hotpot Fund contract needs to carry out the swap operation. Swap on DEX will inevitably occurs slippage, so it is necessary to choose the optimal swap path.
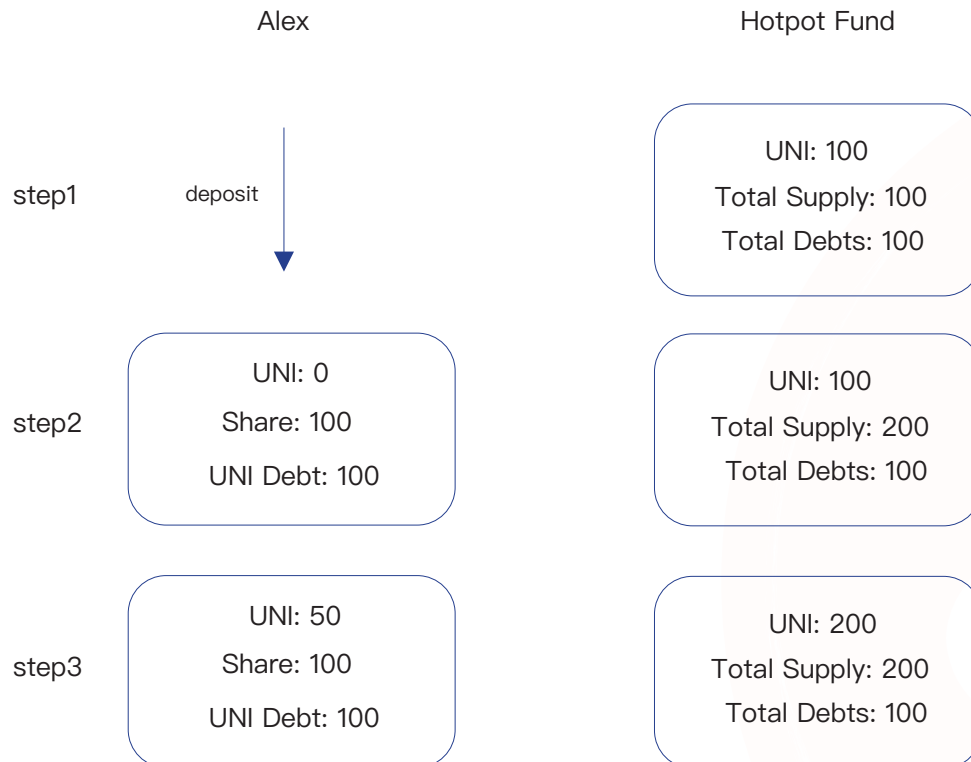
Two paths are designed for In-fund swaps, using Uniswap by default or Curve. If a trading pair has set an address to Curve pool, the pool address is preferred. Otherwise, the default path is Uniswap. Since the slippage of Curve is lower when swap between several stable coins, the swap path of several stable coins will be set to Curve. As there is no unified entry such as the Uniswap Router contract in Curve, the Curve pool address needs to be set. The Curve pool address is set by governance account, not the fund manager, to avoid potential security risks in the fund manager account.

3.6 UNI Mining

Uniswap has issued its own UNI token, as funds to invest in the Uniswap liquidity pool, the Hotpot Fund supports staking the LP held to mine UNI, to generate more profits for investors. All UNI earned from mining are distributed to the investors and the fund itself does not have any share in UNI assets. Whether Uniswap continues to use mining or airdrops in the future, Hotpot will be able to fairly distribute the UNI it acquired to the fund's investors.

3.6.1 UNI Debt

Since UNI is an additional asset to the fund, independent of the fund's local currency and trading pair, a new system is needed to design for it. The Hotpot Fund introduces a concept of UNI debt to calculate UNI assets. As shown in figure:

Alex   Hotpot Fund

		UNI: 100 Total Supply: 100 Total Debts: 100
step1	deposit	

step2	UNI: 0 Share: 100 UNI Debt: 100	UNI: 100 Total Supply: 200 Total Debts: 100

step3	UNI: 50 Share: 100 UNI Debt: 100	UNI: 200 Total Supply: 200 Total Debts: 100

step1) When Alex deposit in the fund, the fund has held 100 UNI already.

step2) Alex deposit in and receive 100 fund share, since Alex did not invest the corresponding amount of 100 UNI (of course, he don't need to invest), Alex's UNI debt is recorded as 100.

$$(Total\ UNI\ +\ Total\ Debts) * \frac{Share}{Total\ Supply} - debt = 50UNI$$

In conclusion, by introducing the concept of UNI debt, Hotpot Fund has skillfully solved the issue of how to calculate UNI assets.

3.6.2 UNI Mining Contract

The first phase of UNI mining consists of four trading pair LPs, one contract for each trading pair LP, which may or may not be extended. In the mining mechanism of UNI, each trading pair corresponds to a mining contract. The trading pair invested by the Hotpot Fund is variable, so it is necessary to set the address of UNI mining contract, which is also completed by governance account, for the same reasons as mentioned above.

3.7 HPT Token

Hotpot Fund project have it's own token: Hotpot Funds (Symbol: HPT). The share of the Hotpot Fund profits will all captured by HPT tokens holders.

3.7.1 Token Information

- Token Symbol: HPT
- Token Name: Hotpot Funds
- Initial Supply: 1million
- Mining: No less than 40% of the tokens will be mined by staking the fund share. The specific mining details will be notified in other ways.
- Features: Can be burned, cannot be minted, pure deflationary token.

3.7.2 How to Capture the Value

HPT token holders capture the Hotpot fund profits not by distributing the fund profits directly to token holders, but by using the fund harvest function to swap and burn the HPT tokens on the Uniswap exchange. All swap and burn operations are driven by smart contracts, anyone can call the harvest function of the controller contract to complete the swap and burn of HPT.

The details are as follows:

1. The profits of the fund are all collected in the controller contract.

2. On Uniswap, a trading pair is established for each fund, and there will establish four trading pairs, namely HPT/ETH, HPT/DAI, HPT/USDT, and HPT/USDC.

3. The controller contract provides a harvest function entry to swap the collected fund profits into HPT on Uniswap and burn HPT concurrently.

4. When the fund profits are collected into the controller contract, anyone can call the harvest function to complete the operations of token swap and burn.

As shown in figure:
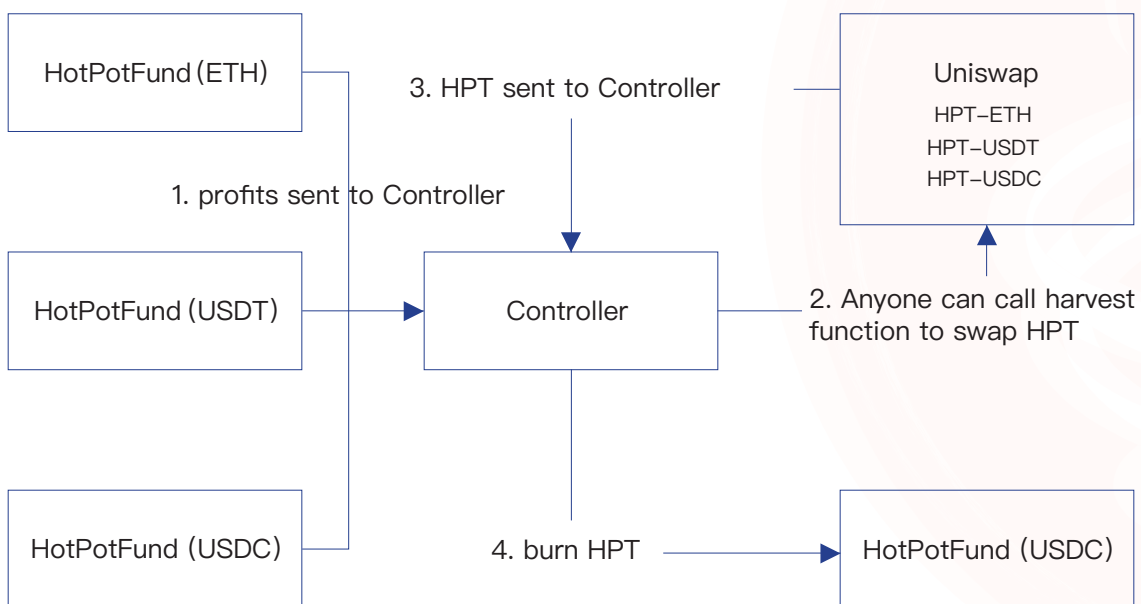
HPT token is a pure deflationary token, which makes the price of HPT have rich imagination space and can enhance its value.

Since there are multiple currency funds, HPT tokens have multiple trading pairs on the Uniswap exchange, which raises some interesting opportunities for arbitragers:

Since the profits of each fund must be unequal, that means some funds will have higher profits and others lower. For funds with high profits, when someone calls the harvest function to swap and burn HPT tokens, it will cause the price of the HPT tokens in the trade pair to rise, thus bring arbitrage opportunities for arbitragers. Arbitrage between different trading pairs will in turn smooth out the HPT price difference caused by the imbalance of fund profits. The arbitrage operation of arbitrageurs ensures that HPT tokens always have good liquidity, without worrying about liquidity dries up.

4. Disclaimer

This document is a technical white paper and is intended for general purposes only. This document does not constitute any recommendation to invest, nor does it contain any recommendation to buy or sell, and it should not be used as a reference to make any investment decision. This document describes the current technical design ideas of the Hotpot Fund team. If these design ideas changed, we are subject to change without prior notice.

参考资料

1. *uniswap-v2-core*

2. *uniswap-v2-periphery*

3. *Uniswap v2 Core White Paper*

4. *curve-contract*

参考资料

Hotpot Fund

The first decentralized investment fund in the world