Ithil Finance

G. Casanova, S. M. Chiarello, M. Ugolotti

28/12/2021

Abstract

Ithil is a staking and investment protocol, where liquidity providers can earn passive income generated by the investment activity. Liquidity is protected thanks to various layers of decentralized liquidation and risk mitigation systems, for which external or internal liquidators are rewarded when they close positions which are incurring excessive loss. In every case, the traders have to post an adequate collateral to access the possible investments, in order to cover for possible losses. Modularity and upgradability make Ithil open to virtually any investment strategy, although for the first version it will only support margin trading, where the trading is done on a best-execution basis using external dexes or dex aggregators.

1 Introduction

Leveraged investments are an ancient and famous financial tool which allow traders to invest more than their available liquidity, thanks to a system called *leverage*. This makes it possible to profit from existent investment opportunity even if the immediate funds availability is relatively low. On the other hand, this comes with the risk of losing more than in the case of a classical, non-leveraged investment.

In this workflow, the trader posts a *collateral* on the platform, which serves as a warranty against possible losses, and obtains the possibility of investing a part of the platform's liquidity which is typically higher than the collateral he or she posted, under the payment of a fee. The ratio between the tradable amount and the margin is called the *leverage*: a leverage of 10x means that the trader can invest 10 times the posted collateral. The fees generated by such activity are then distributed between the *liquidity providers (LPs)*, i.e. investors who deposited their tokens to make the margin trading activity possible.

The main difference between Ithil's activities and undercollateralized loans, is that the borrowed funds are never transferred to the trader: they are just locked in an investment within the platform, which must be closed in order for the trader to withdraw any gain.

1.1 Comparison with other DeFi protocols

A few protocols, offering the possibility to perform margin trading, are already available in mainnet. Ithil stands out among them due to many significant differences, between which there are the following.

1. The usage of a single vault to collect liquidity allows LPs to deposit any ERC20 token on the platform without paying any gas beyond the transaction: as long as there is a trade on such token, the fees generated will be distributed to the LP, generating passive income.

2. Fees are generated in the tokens used to trade, therefore LPs are rewarded with the same token they provided, instead of with the platform governance token. This reduces exchange risk related to the market value of the platform's governance token.

3. An innovative, multilayer liquidation system, inspired by various liquidation systems already battle-tested on the market, protects the investors from adverse market movements, and opens interesting arbitrage opportunities for liquidators, which in turn creates a positive feedback system: the more liquidators act, the healthier the vault is.

4. Very flexible investment system which allows to open, close and modify the position in many different ways, thus offering the best-in-market user experience for traders.

5. Unused liquidity is staked using a gas-efficient automatic staking algorithm: this increments dramatically the APY of the protocol.

6. Ithil's architecture is a mixture of non-upgradable core contracts, which lock liquidity and assure a sound staking logic, and upgradable ancillary contracts, which implement the various investment strategies. This allows Ithil to always be up to date for the most popular investment strategies, which may change over the time as the DeFi world evolves and other external protocols become available.

Although Ithil's core contracts are not upgradable, some governance functions allow the community and the owners to change some of the state parameters (see further in this document), in order to calibrate them with the specific market conditions.

2 Ithil's vault

The leveraged investment activities cannot happen without a large protocol's liquidity, therefore Liquidity providers (LPs) are of greatest importance for Ithil. Investors can provide liquidity and profit from the trading fees: the greatest majority of the fees is indeed redistributed to the LPs themselves, while a smaller amount is distributed to Ithil's community (precise amounts to be decided by the community itself).

The *vault* is the core of the Ithil protocol. It consists of a non-upgradable contract which locks the LPs' tokens and make them available for Ithil's investment strategies. It is responsible for the following tasks:

1. Minting of wrapped tokens

2. Calculation of the interest rate applied when using its tokens to start an investment

3. Lending tokens to one of Ithil's supported strategies

4. Management of the traders' collaterals and investment power

5. Distribution of the fees to investors, community and insurance pool

2.1 Wrapped tokens

The fee redistribution process is conceived to respect a few core features:

- Absence of arbitrage opportunities.

- Gas efficiency.

- Competitive APY.

- Very low risk of capital loss.

- High fungibility of the LP position.

In order to achieve this, Ithil mints fungible wrapped tokens which serve as a proxy of the deposited liquidity, and of the claiming rights of the particular token deposited. *These tokens have nothing to do with Ithil's governance token*. In particular, each liquidity provider is always rewarded *in the same token he or she has deposited*.

When a LP provides some amount of a particular token, a certain amount of wrapped tokens is minted by Ithil (for the precise amount, see section **??**) to reflect the amount deposited and the type of token deposited. Such tokens are then transfered to the LP's wallet and can be exchanged freely.

Such wrapped tokens can then be redeemed by making Ithil burn them and transfer (if immediately available, i.e. not locked in some investment) a corresponding amount of original tokens to the wrapped tokens' owner. Such amount is calculated in Section **??**, and it corresponds to the original deposited amount, plus a portion of the fees depending on the wrapped tokens burnt and the total supply. In this way, only fees generated *after* the minting can be taken by the LP who triggered the minting, thus allowing no arbitrage opportunity and a fair fee redistribution.

2.1.1 Unstaking

The fee distirbution is directly related to the amount of tokens minted and burned during the deposit and withdrawal process. At the moment of the deposit, Ithil will mint an amount of wrapped tokens calculated as follows:

$$\text{minted amount} = \frac{\text{total w-token supply}}{\text{total wealth}} \times \text{deposit} \tag{1}$$

By *total wealth* for a particular token, we mean the amount of that token which has been deposited or generated as fees. In particular, the liquidity posted as collateral or generated as a result of a swap is not considered. In equation (1), the total wealth and the total wrapped token supply are as of *before* the deposit. In the case the total wealth is 0 (i.e. no investor has deposited that particular token yet), then we adopt a $1:1$ rate of minted token to deposited token:

$$\text{minted amount} = \text{deposit}, \quad \text{if total wealth} = 0. \tag{2}$$

Similarly, when the wrapped tokens are burned through Ithil, an amount of original tokens is transferred to the burner, following this equation:

$$\text{transferred amount} = \frac{\text{total wealth}}{\text{total w-token supply}} \times \text{burned amount} \tag{3}$$

where the total wealth and total w-token supply are as of *before* the transfer.

This assures a fair fee distribution in a gas efficient way: a LP will only benefit of the fees generated *after* the deposit occurs, thus preventing arbitrage, and the entitlement is only calculated at the moment of the withdraw, without performing any unnecessary transfer.

2.2 Interest rates and fees

When the tokens leave the vault to start an investment, the vault calculates the fixed fees and the interest rate applied for this loan. The *fixed fees* are token-specific, community-based percentages of the amount which goes out of the vault, and are the direct compensation to LP for providing their liquidity to Ithil's investment activities. The *interest rate* is investment specific, and captures the riskiness of the investment as seen from the vault's perspective.

Both the interest rate and the fixed fee applied are returned as a parameter from the dedicate vault's functions, while the repayment and the logic for the calculation of risk is included in the implementation of the investment strategies. The riskiness is captured in an integer called *risk factor* which is passed to the vault `borrow` function as a parameter. The interest rate is then computed as

$$\text{IR} = \text{IR}_{\text{base}} + \text{risk factor} \times \text{leverage} \times \frac{\text{uncovered liquidity}}{\text{free liquidity}}. \tag{4}$$

Here the free liquidity is the available liquidity in the vault for trading, in that particular token, while the uncovered liquidity is the amount of free liquidity which is not covered by the vault's insurance pool. The base interest rate IR_{base} is the minimum interest rate and is governance-based.

2.3 Lending procedure

In order to make the leveraged investments possible, the vault must lend tokens to verified strategies, which belong to Ithil as well and whose addresses are whitelisted in the vault's state. The vault cannot transfer tokens to any other address, except for the normal staking/unstaking procedure and for posting and withdrawing the trader's collateral.

At the moment the strategy is launched, the tokens are borrowed from the vault by calling the `borrow` function and passing the risk factor as an input; the vault's state is then updated accordingly. When an investment is closed, the same strategy calls the `repay` function, which cancels the debt opened by the position and distributes the generated fees between the investors and the insurance pool.

The listing (or de-listing) of a strategy is governance-based. More details of the only strategy supported so far, margin trading, are given in Section 3.

2.4 Collaterals

In order to be able to open a position in any strategy, a trader has to post a *collateral* to cover for potential losses caused by unfavorable market movements. The collateral can be posted in any token, and potentially gives the right to use any token type of the ones within the vault. The maximum loan size is determined by imposing that the interest rate, as of Equation (4), should not exceed a maximum interest rate fixed by the governance. For example, in the scenario of a very risky investment (high risk factor), or when most of the vault is uncovered (insurance pool amount too low), the allowed leverage is lower.

2.5 Fee distribution

As anticipated in Section 2.1, the fees are not distributed to LPs every time they are generated. Instead, they contribute into increasing the total wealth of the vault, which will then be used to calculate how many tokens an investor is entitled to. Once the fees are generated, they are split into:

- Investors' yield

- Protocol fees

- Insurance pool

The precise percentages to allocate these three slices are yet to be defined, although the greatest majority of the fees will go to the investors' yield: this defines the vault's APY for a given token. The protocol fees are distributed to the governance tokens' owners, while the insurance pool is constantly maintained in order to cover the LPs against unexpected adverse events.

3 Margin trading

The Margin Trading Strategy (MTS) is the core business of the platform, and the first strategy available when the project will be launched. Traders can use the platform's liquidity to perform any supported token, and to gather high profits thanks to the leverage.

Since margin trading is, in particular, an investment strategy, it has the duty of passing the risk factor of every trade to the vault, and to manage accountability of the open and closed positions. Moreover, *liquidation* (see 3.5) will call the MTS, which therefore also manages the liquidators' compensations and allowed strategies.

3.1 Margin

The *margin* is a lump sum of tokens, which the trader deposits (*locks*) into the position in order to fund the trading activity. Traders can post margin in any token, also more than one at the same time. However, any order (see further) needs to have a unique token to be locked as margin in the forthcoming position.

We will consider the example of Tracy, a trader, which posts 1000 `DAI` as collateral in the vault (see Subsection 2.4). At the beginning, Tracy can open any position locking up to 1000 `DAI` as its margin.

3.2 Orders

An *order* is the implementation of an investment decision by the trader. It is a Solidity struct with the following members.

- `address srcToken` the token swapped from the vault.

- `address dstToken` the token to obtain from the dex.

- `uint256 collateral` the amount of margin to be locked.

- `bool collateralIsSrcToken` whether the collateral is posted in the same token as `srcToken`.

- `uint256 minAmount` the minimum amount of `dstToken` to be obtained from the dex.

- `uint256 maxAmount` the maximum amount of `srcToken` to be swapped from the vault.

- `uint256 deadline` the deadline of the order.

For example, Tracy might want to go long `WETH`, thus betting on an increase of the `WETH` token value with respect to `DAI`. She then decides to buy 5000 `DAI` worth of `WETH`, locking 500 `DAI` as a margin. Slippage is managed by adjusting `maxAmount` and/or `minAmount`. Tracy is thus performing an investment with a 10x leverage, and if the order will not revert, her free collateral will become 500 `DAI`, while the rest of her collateral will be locked as a margin in the position that will be created after submitting the order. The obtained `WETH` will be then locked in the MTS.

Conversely, if Tracy wanted to go *short* on `WETH`, she would sell 5000 `DAI` worth of `WETH` from the vault, thus obtaining 5000 `DAI` to be locked in the MTS contract.

3.3 Positions

A *position* is the registration of one or several orders whose submission completes successfully. It is a Solidity struct with the following members.

- `address owner` the position's owner.

- `address owedToken` the token borrowed from the vault for the swap.

- `address heldToken` the token locked in the MTS as result of the swap.

- `address collateralToken` the token used as collateral (in the first version, we only allow it to be either `owedToken` or `heldToken`).

- `uint256 collateral` the amount of tokens locked as margin.

- `uint256 principal` the amount of borrowed tokens.

- `uint256 allowance` the amount of heldToken obtained from the swap.

- `uint256 interestRate` the interest rate calculated at the opening of the position.

- `uint256 fees` the fees generated by the position so far.

- `uint256 createdAt` the time in unix epoch when the position was opened (used for interest calculations).

Getting back to our example, assume the market exchange rate at the moment Tracy is performing the swap is 2500 `DAI` per `WETH`. Assuming the trade incurs no slippage, the position will have an `allowance` of 2 (`WETH`) and a `principal` of 5000 (`DAI`), while we recall from 3.2 that the `collateral` locked by the trader is 500 (`DAI`). In particular, `collateralToken` is `DAI`.

Let us assume that, after some time, the market price of `WETH` has raised by 20% reaching 3000 `DAI` per `WETH`. At this point, Tracy may decide to *close* the position She opened, exchanging her allowance of 2 `WETH` to the dex, which will return (assuming no slippage) 6000 `DAI`. At this point, Tracy must repay the position's `principal` to the vault, thus getting $1000 DAI$ of gain from this swap, assuming no time fees and no fixed fees (see 3.4). Such gain is transferred to Tracy's posted collateral, and the margin locked in the position is unlocked: after the position has been closed, Tracy has 20000 `DAI` worth of free collateral, which she can either withdraw or use for other investments.

Open positions can be modified at any time, either performing an additional swap in one direction or the other, allowing to increase or decrease the allowance or the principal, or by locking some more margin in it, or again withdrawing part of the position margin, to adjust the trader's risk appetite towards a possible liquidation (see 3.5). In all cases, a position allowance and principal cannot exceed the maximum set up for the margin locked in (see 2.4).

3.4 Fees

Fees in the event of a swap are always paid in the token borrowed from the vault to perform a swap; in particular, it changes if the order is long or short.

As mentioned in Section 2.2, it is MTS's task to provide the vault with a risk factor which captures the trade's riskiness. In the case of MTS, the major risk is caused by each token's volatility, due to the fact that a high volatility has a negative impact on the liquidation efficiency (see 3.5). Therefore, a mapping `mapping(address => uint256) riskFactors` is stored in MTS and managed by governance, and the risk factor of the particular swap is defined as the arithmetic mean of the risk factors of the two tokens.

The interest rate and fees are then computed via Equation (4). The fees coming from the interest rate are calculated at the position's closure or at liquidation time, and are applied with no compounding.

In 3.3, we saw how a swap of 5000 `DAI` was performed. Assuming a fixed fee of 0.2% for the `DAI` token, and an interest rate of 0.01% daily, and assuming the position has been kept for 10 days, Tracy must pay in total 0.3% of the swapped amount, i.e. 15 `DAI`, at the closure of the position. This is simply subtracted from Tracy's free margin, which will be 1985 `DAI` when the position is closed (rather than 2000 `DAI`).

If a position is modified, the time fees generated so far go to populate the `fees` member of the position, and the `createdAt` member of the position is refreshed. In this way, only the debt effectively locked in a position generates time fees, and we avoid double-counting.

3.5 Liquidation and risk mitigation

Since the amount of tokens swapped from the vault is greater than the amount provided by the trader in the form of margin, the protocol would be exposed to an exchange risk if there were no liquidation system. This system will close the positions which are incurring a loss which is dangerously close to attacking the protocol's liquidity, thus protecting the LPs and at the same time putting a stop loss for the traders. Liquidation can therefore be thought of as a maintenance process to assure the health of the platform.

In line with the DeFi philosophy, Ithil outsorces liquidation to the public. Liquidating an open position means closing it, which in turn amounts to performing a swap in the opposite direction with respect to the one used to open that position.

3.5.1 Risk factor

A position is *liquidable* if the quoted value of its entitlement, plus the margin, minus de quoted value of its debt, all expressed as an amount of margin tokens, is lower than a certain fraction, called the *risk factor*, of the position's margin. Therefore, assuming we are having a long position, calling P the price of a unit of investment token expressed as amount of margin tokens, and r the risk factor for the investment token, then the position is liquidable if

$$\text{entitlement} \times P + \text{margin} - \text{debt} - \text{fees} < r \times \text{margin} \qquad (5)$$

where "fees" are all the fees generated so far, except liquidation fees. Risk factors, as explained in 3.4, are token-pair pased: the more volatile the token pair, the higher the risk factor. The main purpose of a high risk factor is to protect the protocol's liquidity from further adverse market movements occurring before the actual liquidation occurs, or during the closure of the position, since the very action of performing a swap on any dex causes a price impact on the swapped pair.

3.5.2 Reverse swapping

The first layer of liquidation is reverse swapping, which can be thought of as a decentralized stop-loss mechanism.

External liquidators can trigger the liquidation process after posting a margin on the platform corresponding to a percentage of the tokens to be liquidated (the precise percentage is yet to be decided). The liquidator passes an array of position ids as a parameter to the liquidation contract, which then checks for the liquidability of each one. The allowance of all such liquidatable positions is then summed, although it cannot exceed a maximum amount given by the liquidator and capped depending on the liquidator's margin. This is done to avoid excessive price impact which can weaken the effectiveness of the liquidation process.

Once the loop is finished, a single swap of the entire allowance calculated in the loop is performed, and all liquidatable positions are closed; this avoids the high gas costs of performing many swaps to liquidate many positions. Because of Equation (5), if the price does not change abruptly during the liquidation process, each of such position will have a positive residual margin once closed. A percentage of such residual margin is then transfered to the liquidator's one: this is the *liquidation premium*, while the rest of the margin is freed up and transferred to the trader's free margin.

3.5.3 Principal coverage

The second layer of risk mitigation is principal coverage.

A liquidator can, in any moment, cover totally or partially an open position or a batch of positions by staking the corresponding `principal` in the vault: in this way, the coverer earns part of the interest rate fees (but *not* of the fixed fees, which are considered a payment to the LP to provide liquidity and are in all cases directed to the vault) and can have the entire staked amount back in the case the position is closed or liquidated successfully. In the case the liquidation procedure fails to repay entirely the position's principal, the purchaser's staking is eroded in order to cover the vault's loss.

The effect of purchasing a position is the minting of an NFT representing such position and giving entitlement to the interest rate fees: such NFT can, of course, be exchanged freely, but it can only be burnt when the position is closed: to rephrase this principle, once the position is covered, it cannot be un-covered.

3.5.4 Margin call

The third layer of liquidation is margin call. When a position becomes liquidatable, a liquidator can obtain it (i.e. become the `owner` of the position) by posting a collateral which is high enough to make the position not liquidatable again. The previous collateral is then eroded by the *liquidation premium*, and the remaining part, if any, is transferred back to the trader, which will have no more entitlement on the position. The liquidator will then be able to close the position and immediately realize the premium, or to keep it open to speculate on further market movements.

3.5.5 Further development

In general, the MTS is agnostic on the liquidation procedures, which are stored in seperate contracts and whitelisted inside the MTS. Other liquidation strategies, based on internal logics or external contracts, can be implemented by the governance and linked to the MTS.

4 Modularity and further investment strategies

Ithil's philosophy is to always adapt to the changing DeFi world, and provide the best-to-knowledge investment strategies as time goes. In order to achieve this, the vault, which is the core contract and the only one containing LPs' tokens (except the ones locked in a given investment) is completely agnostic on the particular investment strategy such as the MTS. The transfers and movements relative to each investment are implemented and managed on the particular strategy, which must simply be whitelisted by the vault in order to accept calls from it.

One of the requirements for a strategy to be whitelisted, is the implementation of at least one adequate risk mitigation system, which should be totally decentralized and tailored on the particular investment strategy. Further guidelines for the minimal requirements in order for a strategy to be whitelisted will be available in a future document.

Further details on the code's architecture and design principles will be available in the developer's guide.

Although at the moment of the launch margin trading only will be supported, the community is actively working towards implementing other investment strategies (such as leveraged staking, options, synthetic assets...) and improving the existing ones, following a continuous improvement philosophy for the ultimate benefit of Ithil's community, investors and stakeholders.