

Dovish Finance

Protocol Whitepaper

Abstract

We introduce a decentralized protocol which enables users to seamlessly invest in factor-based quantitative strategies. This is accomplished by community-based rebalancing, where users initiate rebalances to oracle-computed portfolio weights. The protocol therefore enables them to access investments typically limited to accredited investors in traditional finance in an accessible and trustless manner.

1 Introduction

The emerging DeFi landscape is populated by a vibrant ecosystem of protocols that offer various opportunities to seek returns divorced from that of the broader cryptocurrency market. Users can engage in yield farming, lending, or speculating through derivatives (where perpetual futures are perhaps the most salient example). Unfortunately, despite the growing sophistication of decentralized financial markets, many of these protocols have failed to deliver on their promises. It is harder than ever to generate a productive return in DeFi without the use of advanced portfolio management tools, most of which are far outside the realm of the everyday user – especially when the user seeks optimized returns relative to fiat gains.

1.1 The Lack of Consistent Returns in DeFi

1.1.1 Yield Farming

Park [\(4\)](#) suggests that the deterministic liquidity invariance rule used by an automated market maker (AMM) for asset pricing allows for front-running-like sandwich attacks that increase trading costs – consequently reducing yield farming return. As such, yield farming is a suboptimal strategy for investors looking to maximize returns.

1.1.2 Lending

Lending in the decentralized finance (DeFi) space has emerged as a popular way for individuals to earn passive income through cryptocurrency. Despite its ease of access, the returns from crypto lending on platforms like AAVE and Compound Finance have recently been lower compared to traditional investment options such as US Treasury bonds. For example, as of February 3, 2023, the interest rates for supplying USD Coin (USDC) are 1.81% and 2.41% on AAVE [\(1\)](#) and Compound Finance [\(2\)](#) respectively. In contrast, the 12-month Treasury bill rate is at 4.72% [\(5\)](#).

This raises questions about the viability of lending in the DeFi space, particularly given the added risks associated with cryptocurrency.

1.1.3 Currency Risk

Currency or token risk can lead to a lack of consistent returns in DeFi. In the DeFi ecosystem, returns are often tied to the value of specific cryptocurrencies or tokens, such as Ethereum or USDC. If the value of these currencies or tokens decreases, it can result in lower returns or even losses for DeFi users who hold these assets.

This becomes a larger risk in combination with other DeFi mechanisms, e.g. staking, lending etc. This is because, in major market downturns, margin calls and rewards rates might cause actual portfolio values to sink significantly. The DeFi protocols users interact with might not be the issue, but the currency being transacted might lead to significant issues, e.g. LUNA after the Terra fiasco.

1.1.4 Derivatives — Options and Perpetual Futures

Crypto derivatives, such as options and perpetual futures, have become increasingly popular in the DeFi space. However, despite their growing popularity, they can lead to a lack of consistent returns for DeFi users.

Crypto derivatives, like options and perpetual futures, are analogous to picking individual stocks. The returns on these products are largely dependent on the performance of the underlying asset, and therefore, they carry similar risks and uncertainties as traditional stock investments. This can make it challenging for DeFi users to earn consistent returns from crypto derivatives.

Protocols like GMX have accumulated over \$100M USD (3) in token value over the past year providing decentralized perpetual futures from fees alone. For most users, generating sustainable alpha in this sector can be difficult.

1.2 The Problem

The problem that we aim to solve is the following.

Is it possible to enable users to invest in oracle-managed quantitative strategies typically limited to accredited investors in traditional finance in an accessible and trustless manner?

2 The Dovish Protocol

Dovish is an Ethereum Virtual Machine (EVM) compatible protocol that establishes different vaults, which are pools of assets which are rebalanced based on an oracle built around a backtested factor-based quantitative strategy. Users interact directly with the protocol, supplying a reserve asset in exchange for a proportionate share of each vault and triggering the vault's rebalances to oracle-determined portfolio weights at each timestep.

Because of the transparent nature of the blockchain, users will also be able to verify the rebalancing transactions and inspect the weights for them. This provides the users with a trustless way to invest in crypto and ensure that their funds will be invested for and only for their interests.

In other words, users will be able to benefit from the types of automated quantitative strategies that are typically reserved for high net-worth individuals in traditional finance.

2.1 Use cases

2.1.1 Maximizing Fiat Gains

Dovish Vault returns are issued in terms of stablecoins, not a native token with a fluctuating value. After placing assets into the vault, the vault ensures that users will be able to withdraw their investment to obtain USDC at any time.

While the vault may take positions in risky assets in the form of various tokens, the vault's portfolio value is marked-to-market with fiat as the benchmark, and deposits and withdrawals are settled in the specified reserve asset (usually a stablecoin).

This is unlike the common scenario where a user stakes a token in exchange for rewards in the form of the protocol's native token, exposing the user to currency risk in the form of the staked token's value relative to fiat and the staking reward token's value relative to fiat.

Another common situation is when the protocol requires the user to be invested for an extensive period of time, which reduces the liquidity of the user's investment and exposes them to additional risks (e.g. inability to withdraw when the protocol's performance is poor).

2.1.2 Systematic Strategies

With Dovish Protocol, users will be able to leverage our quantitative strategy to receive superior risk-adjusted returns, no matter what the current market regime is. Compared to simply holding their crypto assets, Dovish Protocol enables users to reduce their exposure to the volatile crypto markets. Dovish Protocol provides users with a new risk-managed way to invest their crypto assets.

3 Implementation and Architecture

At its core, Dovish consists of vaults holding assets connected to oracles that determine which assets to hold in what quantity through a quantitative strategy. The vaults themselves are constructed using Set Protocol smart contracts and architecture, while the signal oracles are a novel Dovish invention. Dovish's architecture has been designed to be extensible, which enables users with different risk appetites to invest in vaults with different risk levels and exposure. Currently, we are beginning with a risk-on risk-off strategy focused on WETH called the ETH Stability Vault.

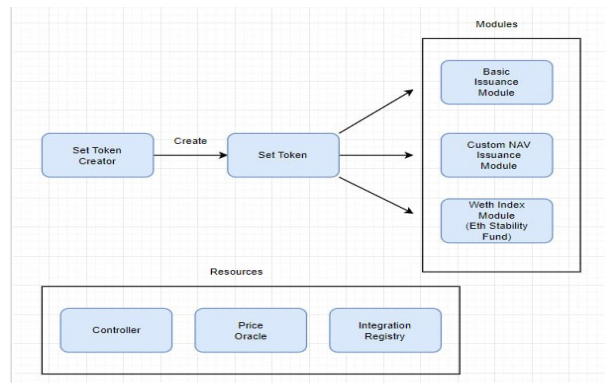


Figure 1: Overall Dovish architecture.

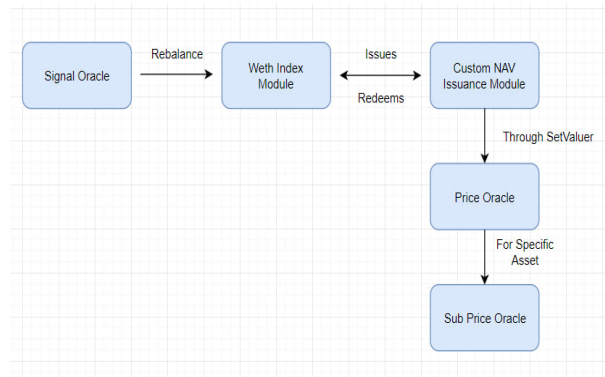


Figure 2: Architecture of oracles used to determine the vault's portfolio weights.

4 Key contract functions

Taking the ETH Stability Vault as an example, the core functions of any Dovish Vault will be the following:

4.0.1 Issuing

A user who wishes to place assets into a vault may call

```
issue(ISetToken setToken, address reserveAsset, uint256 reserveAssetQuantity,  
      uint256 minSetTokenReceiveQuantity, address to)
```

in the CustomNavIssuanceModule with the relevant vault. This function call checks the user's balance of the specific reserveAsset, transfers the specified amount of assets to the vault, and mints correct number of vault tokens to the user based on the vault's NAV.

The Custom NAV Issuance module has a small issuance premium around oracle prices paid by the user to avoid arbitrage and front-running issues.

4.0.2 Redeeming

A user who wishes to redeem assets from a vault may call

```
redeem(ISetToken setToken, address reserveAsset, uint256 setTokenQuantity,  
       uint256 minReserveReceiveQuantity, address to)
```

in the CustomNavIssuanceModule with the relevant vault. This function call checks the user's balance of the specific vault token, converts the value of those tokens into the specified reserve asset, transfers them to the user and burns the specified number of vault tokens from the user.

4.0.3 Price Oracles

A master price oracle is called by SetValue whenever the value of any vault token is needed. The master price oracle maintains a list of Sub Price Oracles for each supported asset relative to each accepted reserve asset. Each Sub Price Oracle can return either the spot price or the average price of a specific asset over a period of time using Chainlink data feeds.

4.0.4 Rebalancing

startRebalance() in WethIndexModule can only be called by the manager of the Dovish Vault (in this case the ETH Stability Vault). It sets the new target units for the specified vault (the ETH Stability Vault) in accordance with the signal oracle.

4.0.5 Trading

A user who wishes to trigger a trade in the vault may call trade(address component) for each component of the vault. Several restrictions apply: each vault component has a specified cooloff period between trades as well as a size limitation for each trade in order to avoid moving markets. Trades may also only occur after a rebalance has been started. In the context of the ETH Stability Vault, this would only occur during a change between risk-off and risk-on signals or vice versa.

5 Strategy Construction

Any strategy deployed on the oracle is constructed with a parsimonious yet comprehensive and carefully selected range of quantitative signals. These signals are transformed, normalized, and combined to determine the portfolio weights computed by the oracle.

Each quantitative strategy is backtested on historical data during development, with appropriate measures taken to mitigate backtest overfitting, data-snooping, multiple-testing bias, look-ahead bias, survivorship bias, and the like. After development, another independent backtest is performed by another member of the team on a hold-out test set of data. The strategy is then paper-traded for a validation period before deployment.

We strive to make the performance of the strategies deployed as transparent as possible. Consequently, the mark-to-market portfolio value and strategy performance metrics are available daily on Dovish Protocol and can be verified by users.

5.1 Example: ETH Stability Vault

The ETH Stability Vault is a risk-on, risk-off systematic strategy that enters a position in ETH when a proprietary signal $s_t, t = 1, \dots, T$ is above a threshold τ , and exits that position in favor of USDC when the signal is below the threshold.

Consequently, the trading strategy is bang-bang, with portfolio weights determined by $w_t^{ETH} = \rho \cdot \mathbb{1}(s_t > \tau)$ and $w_t^{USDC} = \rho \cdot \mathbb{1}(s_t \leq \tau)$ where ρ is a user-defined constant representing the percentage of the user's investment in the risky asset at each timestep.

Given the boom-bust cyclical nature of the price of ETH, with $\rho = 0.2$, this trading strategy outperforms a naive 20% (equivalently, $\rho \cdot 100\%$) allocation to ETH (33.63% v.s. 29.68% CAGR, 1.71 v.s. 1.21 Sharpe ratio, 18.38% v.s. 39.57% max drawdown from 6 August 2015 to 29 January 2023).

6 Value to the DeFi Ecosystem

6.1 Greater Accessibility

To make the ETH Stability Vault more accessible, the protocol only charges a minimal management fee and exit fee. Dovish does not charge any entry fees. The protocol does not penalize—but rather encourages—users to frequently invest and dollar-cost average into the vault. Dovish does not charge any performance fees either.

6.2 Public Indicators

In the interest of contributing to the greater crypto community, Dovish makes some indicators available completely free on Dovish Protocol. These indicators are derived from some signals used for the systematic trading strategies, but are smoothed and de-noised for a human to better interpret them.

References

- [1] AAVE (2023). Aave - markets. <https://app.aave.com/markets/>. Accessed: 2023-02-03.
- [2] Compound Finance (2023). Compound finance - markets. <https://compound.finance/markets>. Accessed: 2023-02-03.
- [3] GMX (2023). Gmx analytics. <https://stats.gmx.io/>. Accessed: 2023-02-03.
- [4] Park, A. (2022). Conceptual flaws of decentralized automated market making.
- [5] U.S. Department of the Treasury (2023). Resource center | u.s. department of the treasury. <https://home.treasury.gov/resource-center/data-chart-center/interest-rates/>. Accessed: 2023-02-03.