# DIODE PROTOCOL

A PREPRINT

**Martin d'Hoffschmidt**
mdhoffschmidt@gmail.com

**Alexandre Collette**
alexcollette@hotmail.com

October 29, 2022

**ABSTRACT**

Yield harvesting in the Decentralized Finance has grown popular since 2020. Many protocols such as Aave[1] or Compound[5] introduces financial tools similar to TradFi in the DeFi space bringing numerous new product opportunities to traders. The present paper attempts to explore new opportunities to innovate on the financial products that can be offered to individuals and businesses in the DeFi space. We introduce the Diode Protocol in the present work. The use of the protocol is two fold. First, users willing to hedge themselves against the volatility of crypto assets while remaining exposed to market upsides will be able to do so, within a certain market downside range allowed by the available pool liquidity. Second, users willing to leverage their yield will be able to do so by taking over the rewards from the hedgers in case of upside. In case of downside, their rewards will be used to cover the positions of the hedgers. In both cases, no investors loses its collateral.

***Keywords*** Decentralized finance · Yield Harvesting · Financial options · Sommlier · Euler · ERC-721

## 1 Introduction

Two major DeFi innovations have enriched the ecosystem, namely lending and borrowing modules and stablecoins. On the one side, borrowing modules make it possible for traders to short an asset while lenders can earn yield by providing them the opportunity to do so. The dominant players here are Compound[5] and Aave [1]. Prior, traders were given no opportunities to short an asset in the decentralized way. On the other side, the volatility of crypto assets with respect to fiat currencies make it difficult for traders and organisations to manage the risk of their treasury. Stablecoins solve here an inherent problem of the DeFi space. Users can hedge their assets using decentralized stable coin protocols such as Angle Protocol [2].

These innovations have triggered other innovations in the Yield Harvesting space with Yearn[3], StakeDao, Euler[4] or Sommelier. These tools make it possible for liquidity providers to easily grow their assets by earning yield on the liquidity they provide to the pools. As many of such protocols improve and diversify their products, there is now opportunities to rely on them to build innovative financial products that can rely on future expected yield.

We want to introduce a novel way for crypto users or organisations to manage their treasury by giving traders two different trading opportunities. On one side, there are users willing to hedge themselves against the volatility of crypto assets. To do so they usually have to rely on stablecoins or remain exposed to the crypto market betting it will go up. Therefore, we want to give them the opportunity to hedge themselve against their assets's volatility within certain conditions to be defined while remaining exposed to potential market upsides. On the other side, the liquidity brought by the hedgers will generate rewards that traders willing to take risks can benefit from in case of market upside and in case of market downside, the rewards generated by their provided liquidity will be used to cover the positions of the hedgers. In both cases, no investors loses its initial deposit.

In the present work, we introduce a simplified version of the Diode Protocol that will be defined below.

## 2 Definitions

The investors are denoted by $k$. They range from $1$ to $n$ such that,

$$k \in [1, n] \tag{1}$$

The stake, or deposit, of the investors in the vault are denoted by $s_k$,

$$S = [s_1, s_2, \ldots, s_n] \tag{2}$$

where $S$ is the vector that stores all the deposits.

The long or short positions associated to each investor are denoted by $d_k$ values respectively equal to 1 and 0,

$$D = [d_1, d_2, \ldots, d_n] \quad \text{and} \quad d_k \in \{0, 1\} \tag{3}$$

The timestamp associated to each investor's deposit is denoted by $t_k$,

$$T = [t_1, t_2, \ldots, t_n] \tag{4}$$

The deposit price associated to the quote currency for each investor's is denoted by $p_k$,

$$P = [p_1, p_2, \ldots, p_n] \tag{5}$$

The reward associated to each investor is denoted by $r_k$,

$$R = [r_1, r_2, \ldots, r_n] \tag{6}$$

The total reward of the pool is denoted by $R_{tot}$ where the following holds,

$$\sum_{k=1}^{N} r_k = R_{tot} = R_{short} + R_{long} = \sum_{k=1}^{n} d_k r_k + \sum_{k=1}^{n} (1 - d_k) r_k \tag{7}$$

The end of the contract is characterized by timestamp $t_s$ with a strike price $p_s$. If the asset price is higher than the strike price, then the long positions are rewarded otherwise the short positions are rewarded. The reward is expressed as a share of the total reward of the vault generated during that period.

Therefore, given the strike price $p_s$ if investor $k$ was right, he has coefficient $\delta_k$ of value 1 otherwise 0. More formally $\delta_k$ can be expressed as,

$$\delta_k = \begin{cases} 1, & P_{final} \geq P_s \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

Note also that we introduce a risk factor called $\Delta p$ that is set manually at the start of the contract. It's value is set to scale the reward of long of short investors for taking risk when the price is respectively lower or higher than the strike price.

## 3 Protocol

When the contract closes, the reward $r_k$ associated to investor $k$ is equal to,

$$r_k = \alpha_k \sum_{l=1}^{n} r_l \tag{9}$$

where $\alpha_k$ is coefficient that weights each investor's individual reward according to their contracted option, i.e. related to their time of deposit and risk taken on the price position. The following property must be true for $\alpha$ to be valid,

$$\sum_{k=1}^{n} \alpha_k = 1 \tag{10}$$

We introduce therefore the coefficients $\beta_k$ such that,

$$\alpha_k = \frac{\beta_k}{\sum_{l=1}^{n} \beta_l} \tag{11}$$

We want $\beta$ to be proportional to the deposit $s$ of the investor, the time it contributed to the vault with respect to others, denoted by $\tau$, and risk it took when depositing based on the current market price and the strike price, denoted by $\rho$, such that,

$$\beta_k = s_k \tau_k \rho_k \tag{12}$$

Let's first consider $\tau$, the coefficient that weights each investor's deposit time exposure with respect to others. If we consider there is a linear relationship between on the vault's exposure for each investor we can compute $\tau$ in the following way,

$$\tau_k = \frac{t_f - t_k}{t_f - t_1} \tag{13}$$

Now, let's consider $\rho$, the coefficient that weights the investor's deposit risk. We want to reward investors to take high risk based on the current market conditions with respect to others that take less risks when the outcome becomes obvious. Therefore, $\rho$ should be higher than 1 if reward should be granted and less than 1 when the outcome becomes obvious. Note $\rho$ should not be lower than 1. One way of expressing $\rho$ would be is the following,

$$\rho_k = \max\left(0, \frac{d_k(p_s - p_k) + (1 - d_k)(p_k - p_s)}{\Delta P}\right) + 1 \quad \text{and} \quad \rho_k \geq 1 \tag{14}$$

Finally, we can express the coefficient $\beta_k$ as,

$$\beta_k = \delta_k s_k \tau_k \rho_k \tag{15}$$

And $\alpha_k$ can then be easily computed by tracking each investors $\beta$ coefficient while tracking the sums on long and short positions respectively denoted by $\omega_{long}$ and $\omega_{short}$,

$$\alpha_k = \frac{\beta_k}{\sum_{l=1}^{n} \beta_l} = \frac{\beta_k}{\delta_k \sum_{l=1}^{n} \beta_l + (1 - \delta_k) \sum_{l=1}^{n} \beta_l} = \frac{\beta_k}{\delta_k \omega_{long} + (1 - \delta_k)\omega_{short}} \tag{16}$$

In other words, the investors have the incentive to deposit their funds early on to maximise their reward $k$ that is therefore expressed as,

$$w_k = \frac{\delta_k s_k \tau_k \rho_k}{\sum_{l=1}^{n} \delta_l s_l \tau_l \rho_l} \sum_{k=1}^{N} r_k \tag{17}$$

# 4 Implementation

At the contract level, we must be able to track all investors reward at any time. We therefore introduce the variables $\alpha_{long}$ and $\alpha_{short}$ that denotes respectively the sum of the investors reward contribution for the long side and short side,

$$\omega_{long} = \sum_{k}^{n} d_k \alpha_k \tag{18}$$

$$\omega_{short} = \sum_{k}^{n} (1 - d_k) \alpha_k \tag{19}$$

The detail of the implementation is given here 1,

**Algorithm 1:** Long Short Yield Harvesting Protocol

**Contract** *LongShortYieldHarvesting*($p_{strike}, t_{start}, t_{final}, \Delta_p$) **contains**

$\omega_{long} \leftarrow 0$
$\omega_{short} \leftarrow 0$

**Struct** *Investor* **contains**
  *t, s, d, α ;*
**end**

**Function** *ComputeTimeContrib(timestamp t)* **contains**
  $\tau \leftarrow (t_f - investor.t)/(t_f - t_s)$
  **return** $\tau$;
**end**

**Function** *ComputePriceRisk(price p, position d)* **contains**
  **if** *position is long* **then**
    $\rho \leftarrow 1 + \max(0, (p_{strike} - p)/\Delta_p)$
  **else**
    $\rho \leftarrow 1 + \max(0, (p - p_{strike})/\Delta_p)$
  **end**
  **return** $\rho$;
**end**

**Function** *ComputeAlpha(s, t, p, d)* **contains**
  $\tau \leftarrow computeTimeContrib(t)$
  $\rho \leftarrow computePriceRisk(p, d)$
  $\alpha \leftarrow s\tau\rho$
  **return** $\alpha$
**end**

**Function** *getReward(int k)* **contains**
  $r \leftarrow 0.0$
  **if** $now \geq t_{final}$ **then**
    $\alpha \leftarrow investors[k].\alpha$
    $d \leftarrow investors[k].d$
    **if** *d is long* **then**
      $r = \frac{\alpha}{\omega_{long}} * totalAssets()$
    **else**
      $r = \frac{\alpha}{\omega_{short}} * totalAssets()$
    **end**
  **return** $r$
**end**

**Function** *Deposit(amount s, position d)* **contains**
  $t \leftarrow now$
  $p \leftarrow OraclePrice$
  $\alpha \leftarrow computeAlpha(s, \tau, \rho, d)$
  $investors \leftarrow investors + Investor(t, s, d, \alpha)$
  **if** *position is long* **then**
    $\omega long \leftarrow \omega long + \alpha$
  **else**
    $\omega short \leftarrow \omega short + \alpha$
  **end**
**end**
**end**

## 5 Simulation

The figure 1 shows the evolution of the Ethereum price over the year 2022. The figure also shows the positions taken by investors. The red dots represent the short positions and the black dotes the long positions. Two different simulations will be carried out. The first one will reward the short investors and the second ones the long investors. The goal of each of them is two fold. First, it is useful to prove that the math are valid. Second, it gives the reader a clearer understanding of the working principles of the protocol.

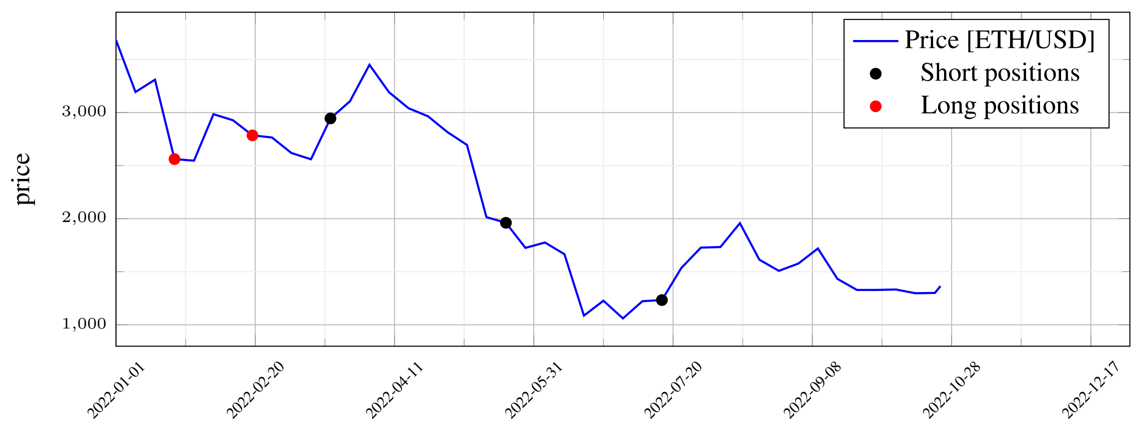


Figure 1: Price evolution

In order to carry out the simulation, the parameters of the contract must be set. We assume that the contract start first day of this year and ends on the last day of the same year. In addition to that, the strike price $p_{strike}$ is set to 2000 [DOL/ETH]. We assume the risk on the asset $\Delta_p$ to be equal to $1000$. The table 1 shows the parameters chosen for the simulation.

| Parameters | value |
|---|---|
| $t_{start}$ | 2022-01-01 |
| $t_{final}$ | 2022-12-31 |
| $p_{strike}$ | 2000 |
| $\Delta_p$ | 1000 |

Table 1: Parameters for the simulation

Two simulations are then performed. The first one, referenced by 2 shows the results of the simulation for a price end of the year below the strike price at $1800$ EUR. The first one, referenced by 3 shows the results of the simulation for a price end of the year above the strike price at $2200$ EUR.

| timestamp | s | p | d | $\tau$ | $\rho$ | $\alpha$ | $\omega$ | reward | rate |
|---|---|---|---|---|---|---|---|---|---|
| 2022-01-25 00:00:00 | 1.5 | 2177.17 | 0 | 0.9341 | 1.1772 | 1.6493 | 0.5766 | 0.3286 | 0.2191 |
| 2022-02-17 00:00:00 | 0.9 | 2545.38 | 0 | 0.8709 | 1.5454 | 1.2113 | 0.4234 | 0.2414 | 0.2682 |
| 2022-03-20 00:00:00 | 2.0 | 2592.38 | 1 | 0.7857 | 1.0 | 1.5714 | 0.6081 | 0 | 0.0 |
| 2022-05-23 00:00:00 | 0.5 | 1845.02 | 1 | 0.61 | 1.155 | 0.3523 | 0.1363 | 0 | 0.0 |
| 2022-07-15 00:00:00 | 0.8 | 1222.26 | 1 | 0.4644 | 1.7777 | 0.6605 | 0.2556 | 0 | 0.0 |

Table 2: Simulation if the asset price is equal to $1800$ EUR

| timestamp | s | p | d | $\tau$ | $\rho$ | $\alpha$ | $\omega$ | reward | rate |
|---|---|---|---|---|---|---|---|---|---|
| 2022-01-25 00:00:00 | 1.5 | 2177.17 | 0 | 0.9341 | 1.1772 | 1.6493 | 0.5766 | 0 | 0.0 |
| 2022-02-17 00:00:00 | 0.9 | 2545.38 | 0 | 0.8709 | 1.5454 | 1.2113 | 0.4234 | 0 | 0.0 |
| 2022-03-20 00:00:00 | 2.0 | 2592.38 | 1 | 0.7857 | 1.0 | 1.5714 | 0.6081 | 0.3466 | 0.1733 |
| 2022-05-23 00:00:00 | 0.5 | 1845.02 | 1 | 0.61 | 1.155 | 0.3523 | 0.1363 | 0.0777 | 0.1554 |
| 2022-07-15 00:00:00 | 0.8 | 1222.26 | 1 | 0.4644 | 1.7777 | 0.6605 | 0.2556 | 0.1457 | 0.1821 |

Table 3: Simulation if the asset price is equal to 2200 EUR

# 6 Conclusion

We have introduced the Long-Short Future Yield Harvesting Protocol. The contract was deployed at address xxx on the Ethereum mainet. The simulation shows that the math behind the protocol is working fine. As a next step, the contracts should be audited.

# References

[1] T. Aave. Protocol whitepaper. *aave*, 2020.

[2] T. Angle. A decentralized, over-collateralized and capital efficient stablecoin protocol. *angle*, 2021.

[3] Y. Finance.

[4] B. Michael and H. Doug. Euler protocol. *euler*, 2021.

[5] L. Robert and H. Geoffrey. Compound: The money market protocol. *compound.finance*, 2019.