DIVA Protocol Whitepaper

A decentralized protocol for creating derivatives assets on anything

Date: 8 May 2021; Version: 1.0.0

Abstract

DIVA is a simple yet powerful decentralized protocol for creating derivative assets. By putting up collateral (which can be any ERC-20 token), users are issued tokenized ERC-20 long and short positions of the derivative contract. Traders can buy and sell those position tokens on the secondary market to place directional bets on the underlying asset, for the sake of speculation or hedging. In particular, shorting an asset is as simple as buying an ERC-20 token. Underlying assets are not limited to traditional or digital assets but may include any metric with a public data feed such as the TVL locked in DeFi, Ethereum gas price, Bitcoin hash rate or the total crypto market cap. Combined with a parametric payoff curve, this will allow the creation of new exotic products not yet available in the DeFi space. The solvency of each position token is guaranteed by the collateral locked in the smart contract, which eliminates counterparty risk and the need for margin calls. A protocol native oracle solution ensures that contracts are settled correctly using crypto economic incentives.

Table of Contents

1 Intro

The Decentralized Finance (DeFi) space built on Ethereum has been growing exponentially, with crypto assets locked in DeFi protocols surpassing $50bn in April 2021[1]. The excitement around DeFi protocols stems from the fact that financial transactions such as lending, borrowing, or trading can be conducted without a central intermediary. Anyone with an internet connection and an Ethereum wallet can access these financial services – no matter their location or social status. Ethereum enables the creation of a more inclusive financial system.

One crucial piece of infrastructure that plays a key role in the functioning of any efficient financial market are derivatives. Derivatives are financial instruments that derive their value from the movement of an underlying asset such as a stock, bond, commodity, interest rate or a market index. Derivatives can be used to speculate on the directional movement of an underlying asset, hedge a position against unfavorable price movements, or give leverage to holdings. Most common types of derivatives include futures, forwards, options, warrants and swaps.

With more than $500 trillion estimated market size as measured in notional value, the derivatives market is by far the largest market in the traditional financial world, 2x larger than the global debt market and 50x larger than the gold market.[2]

There is no doubt that derivatives will also become the largest market in DeFi. However, the DeFi space currently lacks a derivatives solution that is simple to understand for the average user, easy to use and offers highest flexibility in terms of underlying choice, payoff structure and leverage. Current solutions either require users to stake a native token as collateral or remargin positions which introduces unnecessary friction for users. Most of the solutions are also limited in the type of underlying assets, payoff structures that can be traded and the isolation of risk. DIVA protocol is addressing these limitations.

2 What is DIVA

DIVA is a simple yet highly flexible and powerful derivatives protocol built on Ethereum that allows everyone to create and trade derivatives on anything in a permissionless way. By putting up collateral (which can be any ERC-20 token such as DAI, USDC, BNB, BAT, LINK, WBTC or Uniswap v2 LP tokens), users are issued tokenized ERC-20 long and short positions of the derivative contract that track the positive and negative performance of the underlying asset.

By buying long or short position tokens, traders bet on the underlying asset to go up or down, for the sake of speculation or hedging. Users are speculating solely on the movement of the underlying asset, there is no delivery of the underlying asset. Profits and losses are settled at expiration date in the collateral asset based on the terminal value of the underlying asset and the contract specific payoff function. With DIVA, shorting an asset becomes as simple as buying an asset on the spot market. Position tokens are fully collateralized which eliminates margin calls, counterparty risk, and solvency risk for the holders of these tokens.

As opposed to many other platforms, underlying assets are not limited to traditional or crypto assets but may include any metric that has a public data feed such as the total value locked (TVL) in DeFi, Ethereum gas price, Bitcoin hash rate or the total crypto market cap. This will allow the creation of novel markets that will propel the entire DeFi space to the next level. For instance, users will be

---

[1] Source: defipulse.com

[2] Source: https://www.visualcapitalist.com/all-of-the-worlds-money-and-markets-in-one-visualization-2020/

able to create derivative contracts on the Ethereum gas price (or some variant of it). By buying the corresponding long position tokens, Ethereum users will be able to hedge themselves against rising gas prices. In the event of rising gas prices, the user's increasing transaction costs are fully or partially offset by the gains of their derivative position.

The payoff curves of the derivative contracts are highly customizable. Call/put option like payoff functions with any level of leverage (implied by the slope of the payoff curve) can be constructed. In particular, binary payoff functions (typical for prediction markets) are just a special class of derivatives in DIVA.

In DIVA, collateral is isolated per market. That means that traders only need to underwrite the risk of the market they are trading in.

3 How it works

In a first step, a user specifies the contract parameters including the underlying asset that is to be tracked, the collateral asset in which profits and losses are settled, the expiration date and additional parameters including strike, cap, and floor that govern the shape of the payoff curve of long and short positions. All required parameters are discussed in detail in the next section.

By pledging collateral (which can be any ERC-20 token), two virtual pools, one long and one short pool, are generated and funded according to the split provided by the user in the contract specification. In a next step, two ERC-20 position tokens are minted, one against each pool, and sent to the user. Each position token represents a fixed percentage claim on the provided collateral in the corresponding pool and entitles to redeem a portion of the remaining collateral in the pool after expiration.

At expiration, the collateral pools are rebalanced based on the prevailing underlying asset value and the contract specific profit and loss (PnL) function. If the underlying asset value is above a pre-defined threshold, the so-called strike, a portion of the collateral in the short pool is credited into the long pool, increasing the collateral amount that long position token holders can claim. If the underlying asset value is below the strike, a portion of the collateral in the long pool is credited into the short pool, increasing the amount of collateral that short position token holders can claim. If the underlying asset value is at the strike, the original collateral pool balances remain unchanged.

The two points around the strike at which 100% of the collateral in one pool is moved into the other define the tracking range of the derivative contract with the lower bound being referred to as the "floor" and the upper bound as the "cap".

The cap and floor together with the initial funding of the collateral pools determine the slope of the pool PnL curve and hence the rate at which collateral moves from one pool into the other relative to a change in the underlying value. The steeper the PnL curve, the larger the change in the collateral pool balance relative to a change in the underlying value. In an extreme case where cap and floor equal the strike, the payoff function turns into a step function resulting in an all-or-nothing pool rebalancing pattern.

The pool rebalancing and hence the token payoff is always zero-sum meaning that for every unit of collateral that the long position may gain, the short position will lose and vice versa. A holder of both long and short position tokens has no net exposure to the underlying asset, they are essentially perfectly hedged. In particular, the creator of the position tokens who receives both long and short position tokens is initially perfectly hedged. To get long or short exposure to the underlying asset, the contract creator has to sell the opposite side of the trade.

Once minted, position tokens can be traded on both decentralized and centralized exchanges, allowing traders to easily enter long or short positions to bet on the underlying asset to go up or down. In particular, short positions can be entered by simply buying a short position token, eliminating the need to engage in borrowing and being subject to margin calls. It is important to highlight that owning position tokens does not require participation in the derivative contract creation process.

During the lifetime of a DIVA derivative contract, anyone can send additional collateral to an existing derivative contract to mint long and short position tokens and sell them on the secondary market. The new collateral is split between the long and short pool proportional to initial pool funding.

At expiration, an oracle provides the settlement value for the underlying asset. Once the derivative contract enters a settled state, position token holders can call a function to claim their pro-rata share of the remaining collateral. There is no minimum period to redeem the position tokens and hence there is no risk of forgetting to exercise the derivatives.

A trader can unwind their position prior to expiration by simply selling their position tokens on an exchange or by purchasing an equivalent number of the opposite position tokens. For example, to close a long position, a trader can buy an equivalent amount of the corresponding short position tokens and redeem the set of tokens for a return of capital directly from the collateral pool at any point in time prior to expiration.

Position tokens are fully collateralized, meaning that the derivative contract has always enough collateral to pay back every position token holder. The maximum loss for the long and short pool is limited by the contributed collateral amount. This also implies that the maximum payout of long and short positions is capped by the overall collateral locked in the contract.

Before we make a concrete example with numbers, let us first define the parameters that govern DIVA contracts.

4 Contract specification

Each pair of long and short position tokens is governed by the following set of parameters:

- **Underlying asset** (or simply "underlying")**:** asset that the long and short position tokens of a derivative contract track. This can be the price of traditional stocks, bonds, digital assets, or any other metric that has a public data feed such as TVL in DeFi, Ethereum gas price, Bitcoin hash rate or the total crypto market cap.
- **Strike:** threshold underlying value for pool rebalancing. If, at expiration, the underlying value is above the strike, a portion of the short pool collateral will be credited into the long pool and vice versa if the underlying value is below the strike. If the terminal underlying value equals the strike, pool balances will remain unchanged relative to original funding.
- **Cap:** maximum underlying asset value that a position token can track. If, at maturity date, the underlying value is at or above the cap, the entire collateral in the short pool will be credited into the long pool.
- **Floor:** minimum underlying asset value that a position token can track. If, at maturity date, the underlying value is at or below the floor, the entire collateral in the long pool will be credited into the short pool.
- **Collateral asset:** asset that is deposited into the collateral pool at contract creation or during the lifetime of the contract to back the position tokens and in which profit and loss is

settled at maturity date. The collateral asset can be any ERC-20 token including DAI, USDC, BNB, BAT, LINK and WBTC.

- **Long pool balance:** collateral amount backing the long tokens at the strike.
- **Short pool balance:** collateral amount backing the short tokens at the strike.
- **Long token supply:** number of tokens to be minted for the long position.
- **Short token supply:** number of tokens to be minted for the short position.
- **Expiration/maturity date:** date at which the derivative contract expires and the payoff amount per long and short position tokens is determined.
- **Oracle address:** Ethereum address (externally owned account or a smart contract) of the data provider who is supposed to provide the underlying value at contract expiration (the "settlement value") to settle the market.

The specification of a combination of all the above parameters together creates a unique derivative contract. Given the number of parameters as well as the possible ranges each parameter can take, an infinite number of different derivatives can be created.

Equipped with the meaning of the parameters, we can now look at a concrete example of how DIVA protocol can be used.

5 Example

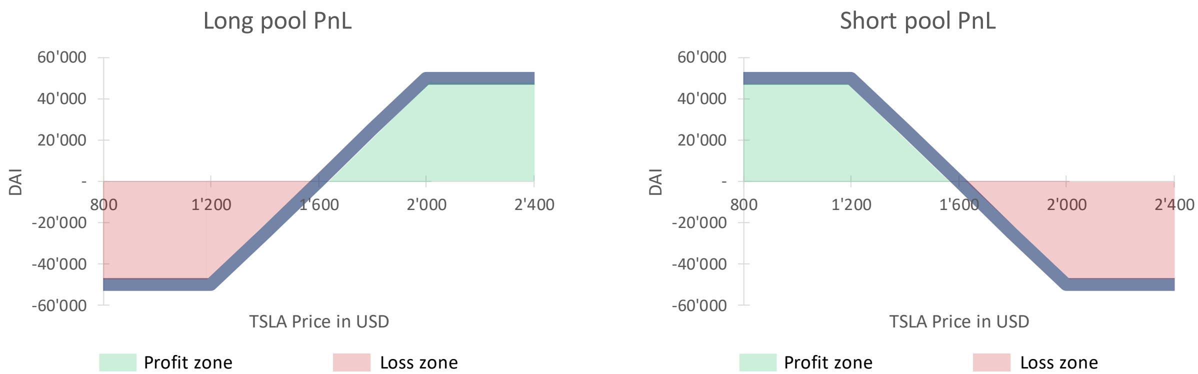
Chad is excited about electric cars and believes that the price of Tesla stock will go up from its current level of USD 1'600. Chad would like to bet on the Tesla stock price without owning the underlying asset. Chad uses the DIVA protocol to generate tokenized positions that will allow him to track the Tesla stock price.

5.1 Defining contract parameters

In a first step, Chad specifies the parameters that govern the PnL curves of the long and short pool and hence the payoff of long and short position tokens:

Contract parameter	Value
Underlying asset	TSLA/USD
Strike	USD 1'600
Cap	USD 2'000
Floor	USD 1'200
Collateral asset	DAI
Long pool balance	DAI 50'000
Short pool balance	DAI 50'000
Long token supply	100'000
Short token supply	100'000
Expiration date	2021-12-31
Oracle address	0x12345…

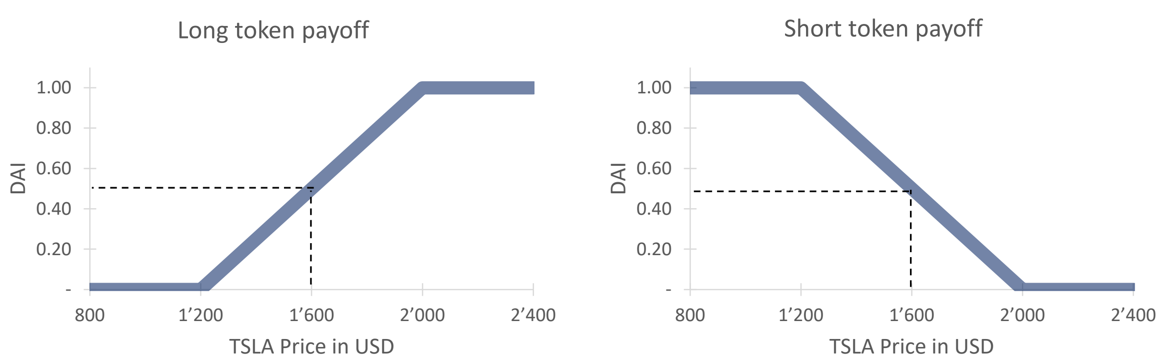
The implied PnL curves for the long and short pool are illustrated by the blue lines below. The green and red areas indicate the underlying price ranges in which the collateral pools gain or lose.



If, at expiration date, the Tesla price is above the strike of USD 1’600, a portion of the short pool collateral is credited into the long pool, hence increasing the capital that long position token holders can claim from the pool. If, at expiration date, the Tesla price is below the strike, a portion of the long pool collateral is credited into the short pool, hence increasing the capital that short position token holders can claim from the pool. If, at expiration date, the Tesla price equals the strike, the pool balances remain unchanged relative to initial funding (i.e., DAI 50’000 in long pool and DAI 50’000 in short pool).

The pool PnL curve, which is a function of the floor, cap and the initial collateral pool balances, implies that a 1% change in the underlying results in a 4% change in the pool collateral. This is equivalent to saying that the pool PnL curve has an implied leverage of 4x. In particular, if, at expiration date, the underlying price is at or below the floor price of USD 1’200 (equivalent to a drop of 25% or more in the underlying price), 100% of the long pool collateral will be credited into the short pool. Conversely, if, at expiration date, the underlying price is at or above the cap price of USD 2’000 (equivalent to an increase of 25% or more in the underlying price), 100% of the short pool collateral will be credited into the long pool.

The corresponding token payoff curves, which define the amount that long and short position token holders can claim per token from the collateral pool for any given underlying price, are illustrated below.



5.2 Collateral deposit

After Chad has confirmed the contract specification, he sends a total of DAI 100’000 as collateral to the DIVA factory smart contract. The collateral is split between the virtual long and short pool according to the proportions defined in the contract specifications. After the collateral has been deposited, 100’000 long and the same amount of short position tokens, each representing a claim of 1/100’000 or 0.001% on the collateral in the respective pool, are minted and sent to Chad.

At this point in time, Chad is owning all long and short position tokens, hence he has no net exposure to the Tesla price. That means that every increase in the long token value is offset by a decrease in the short token value making him perfectly hedged against price fluctuations.

5.3 Trading

As Chad is interested in the long side of the trade only, he needs to find someone who is willing to buy his short position tokens. Chad puts the short position tokens for sale on a decentralized exchange.

Karen who has seen the Tesla price rallying over the last couple of weeks believes that there will be a pullback. She sees the offering on the decentralized exchange and buys the short position tokens. By holding the short position tokens, she can now benefit from a declining Tesla price. The price that Karen is paying for the short tokens is referred to as the premium and is immediate revenue for Chad.

5.4 Settlement

At expiration date, the Tesla stock price is at USD 1'800, 12.5% above the strike and half-way to the price cap of USD 2'000. As a result, 50% of the short pool is credited into the long pool, reducing the short pool balance from DAI 50'000 to DAI 25'000 and increasing the long pool balance from DAI 50'000 to DAI 75'000.

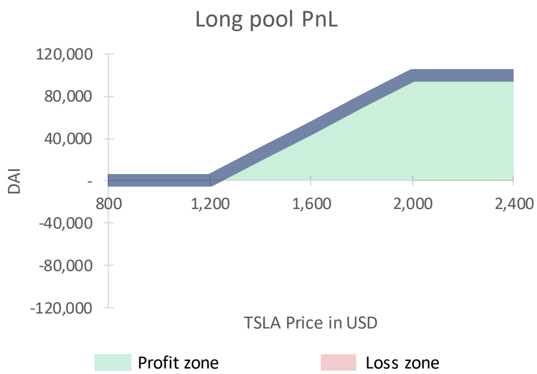
To claim the collateral, Chad and Karen send back their tokens to the DIVA factory smart contract to receive DAI 0.75 and DAI 0.25 per long and short token, respectively, in return.

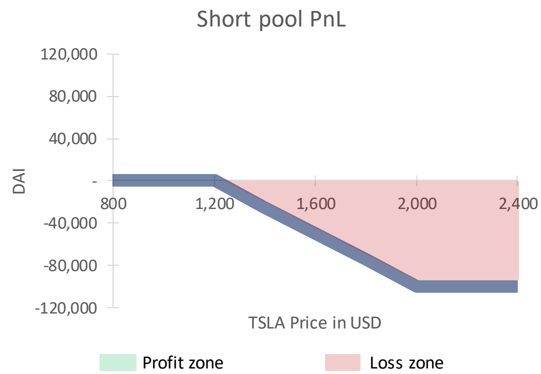
6 Payoff curves

A reader familiar with options will recognize the payoffs of the two positions as capped variants of a long call and a long put option, with the floor taking the role of the call option strike and the cap that of the put option strike. Technically, the long position is a combination of a long call and a covered short put option with the same strike. Similarly, the short position is a combination of a long put and a covered short call option with the same strike. More precisely, minting position tokens on DIVA is equivalent to issuing a long call and a long put option, pre-funding the maximum loss of the corresponding short positions and tokenizing the combination of the long call and the covered short put for the long position and the long put and the covered short call for the short position.

6.1 One-sided collateral pools

The same payoff curves as in our previous example can be replicated by allocating all collateral (DAI 100'000) to the short pool and setting the strike to USD 1'200. The pool PnL curves are illustrated below.





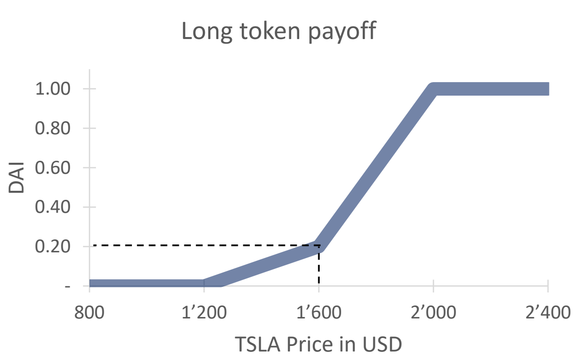
In that case, the short pool cannot gain new funds. Collateral can only flow in one direction, from the short into the long pool. This setup is equivalent to writing a call option and pre-funding the maximum loss for the short call position. In a scenario where the underlying stays below the strike, the option writer can redeem all the collateral from the short pool, leaving them with a net gain equal to the premium earned from selling the long position tokens / call option. Similarly, funding the long side of the pool will issue a long put and its covered short lag.

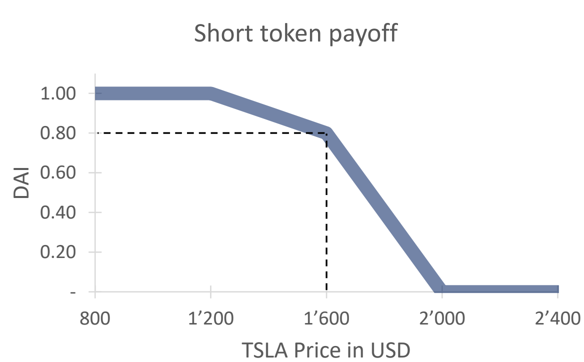
Note that if the long pool remains unfunded, the floor is irrelevant. If the short pool remains unfunded, the cap is irrelevant. In both cases, the strike of the position tokens equals the strike of the pool PnL curves.

6.2 Benefits of two-sided collateral pools

The flexibility to fund both pools at the same time has the following benefits:

- The issuance of a long call and put option, their packaging and tokenization can be conducted in one single transaction instead of four when replicated individually with one-sided collateral pools.
- Enables the creation of exotic payoff patterns by funding the pools in different proportions and/or choosing the floor and cap at different distances from the strike. Below an example with DAI 80’000 short pool size and DAI 20’000 long pool size which results in two different slopes left and right of the strike creating a kink at the strike.





6.3 Implied leverage

Leverage refers to the use of debt to turn relatively small amounts of capital into significant profits. With many financial instruments, such as stocks, the only way to take advantage of leverage is to borrow funds to take a position which is not always possible for everyone. One of DIVA's benefits is that leverage is possible without the need to borrow funds.

Visually, leverage is represented by the slope of the payoff curves. The steeper the curve, the larger the change in the collateral pool balance per unit of change in the underlying asset.

The slope depends on the initial allocation of the collateral between the long and short pool and the distance of the cap/floor from the strike. The collateral allocated to the short pool represents the maximum gain for the long pool which is realized at the cap. The collateral allocated to the long pool represents the maximum gain for the short pool which is realized at the floor.

With that, we can derive the following general formulas to calculate the leverage ratios λ^L and λ^S for long and short positions:

$$\lambda^L = -\frac{C_0^S}{C_0^L} \Big/ \left(\frac{p^c - K}{K} - 1\right)$$

and

$$\lambda^S = -\frac{C_0^L}{C_0^S} \Big/ \left(\frac{p^f - K}{K} - 1\right),$$

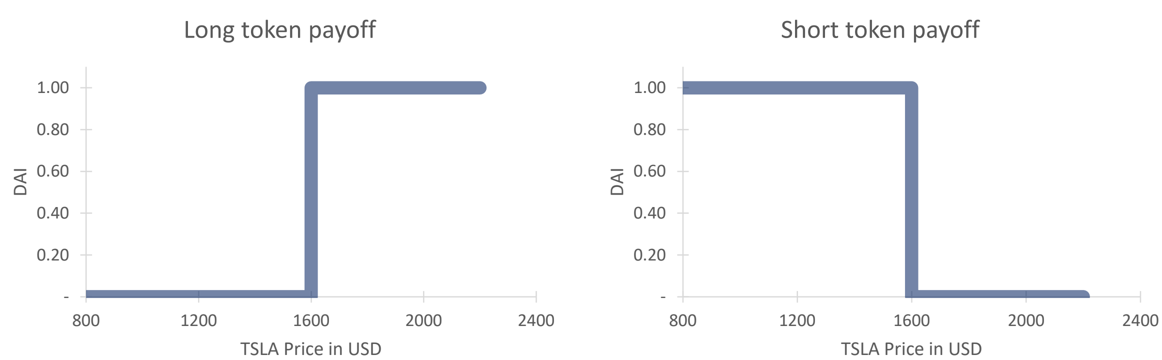
where C_0^S and C_0^L is the collateral amount deposited into the short and long pool at the time of creation, p^c is the cap, p^f the floor and K the strike. All else equal, the narrower the range between cap/floor and strike, the higher the implied leverage.

6.4 Example payoff functions

By choosing different combinations of contract parameters or by combining a series of position tokens, users will be able to replicate many different payoff structures and risk profiles. Below are a few examples.

6.4.1 Binary options

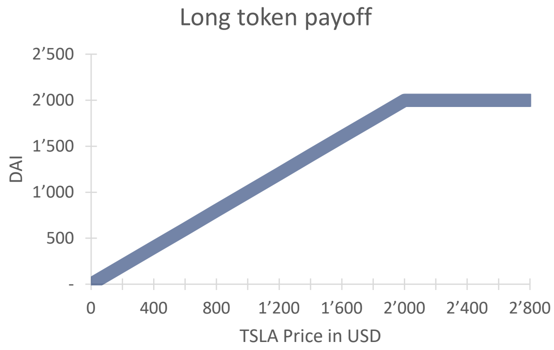
One popular type of derivatives are binary options in which the payoff is either some fixed monetary amount or nothing at all. In DIVA, a binary call/put option can be replicated by funding one side of the pools and setting the floor/cap very close to the strike. For instance, a call contract with strike USD 1'600, cap USD 1'600.01 would yield the following payoff curves for long and short position token holders:

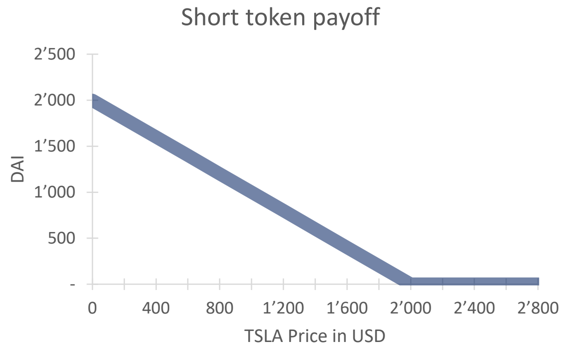


Prediction markets are essentially binary options. In DIVA, prediction markets are just one specific class of derivative contracts out of many.

6.4.2 Synthetic assets

DIVA allows to construct synthetic assets that track the price movements in the underlying asset 1:1. By setting the strike to zero, allocating 100% of the collateral to the short pool, and setting the long token supply equal to the ratio between the short pool size and the cap (we assume the same short token supply for simplicity), the following payoff structures for long and short position tokens result:





Since the strike is zero, the long position's payoff at expiration equals the value of the underlying asset.[3] As holding the long position token generates the same payoff as holding the underlying asset, arbitrage considerations imply that the long position token should trade very closely to the price of the underlying asset[4], hence representing a synthetic version of the underlying asset.[5]

As the short pool is pre-funding the maximum gain of the long token, the payoff increases if the underlying price decreases, hence forming a put like payoff structure for the short tokens.

Synthetic assets are particularly attractive for market makers as they can hedge their positions by simply buying the underlying asset using the proceeds from the long token sale. We expect these type of derivatives to dominate in the early phase of the protocol.

6.4.3 Straddle

Traders can create customized payoff structures by combining a series of position tokens. One popular example is the straddle, a V-shaped payoff structure which is used when a trader believes that the underlying asset will experience significant volatility in the near term. The strategy is profitable only when the underlying asset either rises or falls from the strike by more than the total premium paid for the tokens.

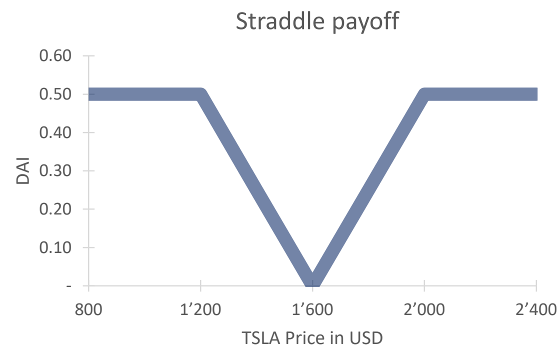
A straddle can be constructed by purchasing a put and a call like payout with the same underlying asset, strike and expiration date. For strike USD 1'600, floor USD 1'200 and cap USD 2'000, the payoff structure looks as follows.

---

[3] At least up to the cap which can be chosen high enough to render it unlikely to be reached.

[4] As holders of synthetic assets do not receive dividends or have voting rights, the value of synthetic assets is typically lower than that of the underlying assets.

[5] Arbitrage considerations only apply if the underlying asset can be traded in the market and the long position can be hedged. Zero-strike derivatives on non-tradeable underlyings (e.g., Bitcoin hash rate) do not need to trade close to their underlying value.



6.4.4 Derivative parameters

The relatively large number of parameters required to create a DIVA contract can be a major challenge for using the protocol. To abstract away the complexity, the web interface will offer pre-configured payoff curves such as a plain vanilla call/put option, binary option and trackers (i.e., options with strike zero) with a default position token supply. Users will always be able to switch to advanced mode to modify the parameters to create custom derivatives.

Another challenge of giving users too much flexibility in creating derivatives is that it would fragment liquidity, preventing a liquid market from forming around any particular set of position tokens. To address this problem, the expiry dates in the web interface could be limited to end of quarter and strikes to discrete steps.

7 Use cases

7.1 Trade anything

With DIVA, users can get exposure to assets that are not native on Ethereum. This includes traditional assets such as stocks, bonds, commodities or market indices as well as other crypto assets such as Bitcoin, Litecoin or Monero.

7.2 Short selling

Currently, there are limited options available in DeFi to short crypto assets to profit from declining asset prices. With DIVA Protocol, shorting becomes as easy as buying a token. For instance, by buying a short position token on Tesla stock, your position will gain in value as the stock price declines. Shorting an asset using DIVA position tokens does not require borrowing funds or dealing with margin calls and liquidations.

7.3 Hedging

Besides speculation, derivatives in traditional finance are primarily used as a risk management tool to protect against adverse price movements in an asset, also referred to as hedging. For instance, airlines hedge against rising jet fuel prices, banks hedge against changes in interest rates. This is achieved by taking a position in a derivative instrument that will gain in value when the underlying asset loses in value and vice versa.

To give an example, imagine that Bob holds BTC which is currently trading at USD 10’000. Bob is worried that it can go below USD 8’000. Bob buys short position tokens with strike USD 8’000. If BTC falls below USD 8’000, the short token will gain in value offsetting the loss he incurred on the underlying asset. The hedging position limits his losses to USD 2’000.

With DIVA Protocol, hedging is no longer exclusive to large institutions. Anyone can hedge their price exposure using position tokens. In particular, by acquiring short position tokens, traders can limit the downside of their holdings.

7.4 Exotic products

DIVA's use case goes beyond tracking traditional or digital assets. Any metric that has a public data feed, such as TVL in DeFi[6], Bitcoin hash rate[7], Ethereum gas price[8], or the total crypto market cap[9], can be used as the underlying asset. Even binary events such as the outcome of a sport event or election can be fit into the framework. This will allow for the creation of novel, exotic markets.

For example, Ethereum users will be able to hedge themselves against rising Ethereum gas prices by holding long position tokens linked to the Ethereum gas price.

8 Collateral

DIVA position tokens are fully backed by the collateral contributed to the contract. The collateral amount allocated to the long/short pool determines the maximum loss that the corresponding pool can take. This has several benefits which are outlined below.

8.1 No margin calls

Existing derivatives solutions require traders or network participants to constantly manage their positions to ensure that they are sufficiently collateralized to avoid forced liquidations or other forms of "punishment". For the average trader, this is impossible to do and discourages them to participate at the cost of liquidity.

With DIVA, traders do not need to worry about margin calls or forced liquidations. They can simply hold and forget about their positions without constantly monitoring it. We believe that this is essential to onboard new users to the derivatives space in DeFi.

8.2 No counterparty risk

The collateral asset is held by a smart contract. Hence, a position token holder does not need to worry about the other side of the trade not being able to fund its obligations. Traders can always be assured to be repaid.

8.3 Supported collateral assets

DIVA supports all ERC-20 tokens as collateral including DAI, USDC, BNB, BAT, LINK, WBTC and Uniswap v2 LP tokens. This has the benefit that traders can more easily create derivative contracts without the friction of having to acquire new assets as collateral. In particular, users can deposit interest bearing instruments such as cUSDC or aUSDC from lending platforms such as Compound or Aave to maximize capital efficiency.

As opposed to existing derivatives solutions, in DIVA, collateral is isolated per market. That means that traders only need to underwrite the risk of the market they are trading in.

[6] www.defipulse.com
[7] www.blockchain.com
[8] www.ethgasstation.info
[9] www.coingecko.com

9 Liquidity providers

Users that provide collateral to DIVA derivative contracts are referred to as liquidity providers and are essential to the protocol. The creator of a derivative contract is the first liquidity provider in any given contract.

9.1 Adding liquidity

At any point in time during the lifetime of a contract, users can add funds to the collateral pool to mint new long and short position tokens. The new funds added to the collateral pool are split between the long and the short pool proportional to the initial funding. The number of new position tokens issued is directly proportional to the collateral added to the respective pool.

Example: Let’s assume that Alice discovers the Tesla derivative contract that Chad has created in section 5 and decides to mint additional position tokens. She contributes a total of DAI 50’000 to the contract which is then split 50/50 between the long and short pool resulting in a new long and short pool balance of DAI 75’000. As her stake represents 1/3 of the long and short pool, Alice is issued 50’000 long and 50’000 short position tokens in return. This ensures that the payoff functions of the newly issued position tokens are exactly the same as the ones of the originally issued tokens. Existing position token holders will not be impacted in any way.

Alice can offer the newly issued position tokens for sale on an exchange, hence increasing the liquidity of the market.

9.2 Removing liquidity

At any point in time during the lifetime of a contract, position token holders can withdraw liquidity from the pool by submitting an equivalent amount of long and short tokens to the derivative contract. This is particularly useful when liquidity providers do not manage to sell all their position tokens on the market or want to preempt the settlement process (which is described in more detail in the next section).

Example: Let’s assume that Alice didn’t manage to sell 50% of her newly minted position tokens. By submitting the remaining position tokens in equivalent proportions, i.e., 25’000 long and 25’000 short position tokens in our example, the DIVA smart contract will return DAI 25’000 to Alice and burn the submitted position tokens forever.

A trader who wishes to withdraw liquidity from the pool prior to expiration but holds long position tokens only would need to acquire short position tokens and vice versa.

10 Settlement

This section outlines the details around derivative contract settlement at expiration.

10.1 Time of settlement

All DIVA derivatives are European-style, meaning that formal settlement happens only at expiry. To close a position prior to expiration, a trader can either sell a portion of their position tokens or neutralize their position by acquiring an equivalent amount of the opposite tokens and remove liquidity from the pool.

The fact that traders have to trade the position tokens if they want to settle before expiration allows for more liquid markets to develop, as opposed to their American counterparts that allow for early settlement.

10.2 Collateral based settlement

All profits and losses of derivative positions are settled in the collateral asset which is locked in the contract. Once the terminal value of the underlying asset has been provided by an oracle, the long and short pools are rebalanced based on the underlying PnL curves. Anyone who is in possession of long or short position tokens will be able to redeem their pro-rata share of the collateral in the respective pool.

Users can collect their payoffs at any time post expiration. There is no minimum period to redeem the position tokens and hence there is no risk of forgetting to exercise the derivatives.

10.3 Oracles

As opposed to other derivative protocols, the value of DIVA position tokens is not reliant on an Oracle providing constant data updates. Given the European nature of the contracts, only one single update is required, namely at the time of expiration. During the lifetime of the contract, the "oracle" is a trader's off-chain observation of the prevailing price. As the underlying price changes and arbitrage opportunities arise, traders will be financially incentivized to "submit" their off-chain observations by means of arbitrage trading. This will greatly benefit the liquidity of the derivatives markets.

The reporting of the settlement value at expiration is the most critical part of the DIVA protocol as it directly determines the payoff of each position token. The oracle solution of choice should give users the confidence and trust that derivative contracts will settle correctly.

In the following sections, we describe the key requirements for an oracle in DIVA and present a protocol native solution that satisfies all of them.

10.3.1 Oracle requirements

The following criteria have been identified to be crucial for a robust oracle solution for DIVA protocol:

- **Prevention of invalid markets:** derivative contract creators should be discouraged from choosing oracles that cannot or are not willing to provide the data (e.g., in case of unethical markets).
- **Buyer protection:** buyers of position tokens should have an easy way to check whether a specified data provider is considered trustworthy or not.
- **Alignment of incentives:** data providers are sufficiently incentivized to provide correct data and incentives are aligned with DIVA token holders.
- **Special events:** data providers are able to report correct settlement values in the event of stock splits, hard forks, changes in index calculation methodology, flash crashes, etc.
- **No single point of failure:** contracts should settle even if the data provider fails to provide their input.
- **Dispute mechanism:** position token holders should be able to request a review of the submitted settlement value.
- **Simple:** under normal circumstances, derivative and DIVA token holders should not get involved in the settlement process.
- **Flexible:** the oracle solution should allow for a rich set of data feeds.

Existing oracle solutions such as Chainlink or Band protocol are not able to meet all our criteria (e.g., set of data feeds is limited, no dispute mechanism available, incentives are not necessarily aligned with DIVA token holders, uncertainty about special event handling). While users will retain the freedom to integrate existing oracle solutions in DIVA's settlement process, DIVA will offer users their own protocol native oracle for highest settlement security, which is described in more detail in the next section.

10.3.2 DIVA's protocol native oracle solution

At contract creation, the user has to provide the address of a data provider that is supposed to report the terminal value of the underlying asset following contract expiration. Theoretically, any Ethereum account (externally owned account or a smart contract) can be assigned to provide the settlement value. While this gives contract creators maximum flexibility to configure the contract settlement to their individual setup, malicious actors may abuse it in an untrusted environment with anonymous market participants to create markets that will settle incorrectly.

To protect traders from malicious markets, DIVA token holders will maintain a whitelist of credible and trustworthy data providers which contract creators can reference at contract creation. While contract creators will retain the freedom to deviate from the whitelist, the incentive to do so will be significantly reduced for the following two reasons:

i) Users and liquidity are expected to concentrate around markets with a trusted and reputable data provider and
ii) DIVA token holders will step in and vote on the settlement value in the event that a whitelisted data provider fails to provide a settlement value within the pre-defined time interval, offering additional settlement security.

In an unlikely scenario where both the data provider and DIVA token holders fail to provide a value within the given timeframe, the settlement value will default to the strike.

10.3.2.1 Data provider

Anyone who wants to become a data provider for the DIVA protocol has to submit a formal application to DIVA governance including a list of data feeds that they are able to provide. After careful review and due diligence, DIVA token holders will vote whether to accept or reject the applicant.

Example applicants may include:

- Crypto exchanges like Binance, Kraken, Coinbase or Gemini to provide price data for crypto asset such as BTC, ETH, or DIVA
- defipulse.com to provide the total value locked (TVL) in DeFi
- ethgasstation.info to provide the Ethereum gas price
- Individuals for publicly available data such as the end of day prices of traditional assets on Yahoo

Data providers (including those that are not whitelisted) will be incentivized to report the correct value in three different ways:

1) **Settlement fee:** a data provider receives 0.05% of the overall collateral locked in the contract for every successful settlement. For example, providing one data point to settle a contract with DAI 1 million collateral locked will earn the data provider DAI 500.
2) **Reputation score:** every successful and failed data feed will be recorded on the blockchain, visible to all users of the protocol at any time. Any misconduct will result in reduced user trust and lower revenues for the data provider in the future
3) **DIVA token staking:** each whitelisted data provider will be required to stake a certain amount of DIVA tokens to ensure alignment of incentives between the data provider and the DIVA token holders. Any failure to provide data will be penalized by slashing a portion of their staked DIVA tokens.

In the early phase of the project, a small group of project supporters and team members will be the only whitelisted data provider. Available data feeds will include assets that have a publicly available and easily verifiable data source such as Yahoo Finance or coingecko.com. Over time more data feed providers will be onboarded to offer users a wide range of data feeds.

10.3.2.2 Dispute mechanism

Despite users delegating the reporting to one of the trusted third parties, they will be able to intervene by requesting a review of the submitted settlement value if they believe the value is incorrect. It is important to highlight that the dispute mechanism was designed to correct human error such as a typo in the settlement value or failure to account for a denomination in the underlying asset (e.g., stock split). It was not designed to protect against malicious data providers. The dispute mechanism is available for all DIVA contracts, including those with non-whitelisted data providers.

Following a 48 hours window after contract expiration (“submission period”) during which the data provider can submit the settlement value, position token holders will have 24 hours (“challenge period”) to request a review.

If no request for review is submitted during the challenge period, the provided settlement value is considered confirmed and position token holders will be able to withdraw their implied share of the collateral, earliest 72 hours / 3 days after contract expiration (fast settlement is discussed in the next section).

If a request for review is submitted during the challenge period, the data provider has 24 hours to either confirm the previous value or provide a new value. If the data provider submits the same value as before, the settlement value is considered confirmed and position token holder can immediately withdraw the collateral. If the data provider submits a new value, position token holders will have 24 hours to request a review of the new settlement value. This continues until the data provider submits the same value twice in a row. This is a deliberate design choice to prevent position token holders (especially those whose positions become worthless) from deliberately delaying the settlement process until infinity by triggering requests for review.

All time windows are absolute meaning that they are independent of when a settlement value is submitted or a review is requested. This removes the need to constantly watch the blockchain and provides better planning security for all settlement participants.

10.3.2.2.1 Discussion

In the base case, position token holders will not be involved in the settlement process. Once the data provider submitted the correct settlement value and the challenge period expired without a request for review, position token holders will be able withdraw their collateral, earliest 72 hours after contract expiration.

To reduce the likelihood of disputes and hence the involvement of position token holders, whitelisted data providers will be encouraged to use data sources that are public and hence easily verifiable for position token holders (e.g., Yahoo Finance, coingecko.com, etc.).

To support position token holders in monitoring the settlement process of their contracts and triggering requests for review if needed, a notification service will be implemented.

Whitelisted data providers that fail to report a settlement value within the given time period, submit and confirm wrong values or add uncertainty to the settlement process by adjusting the value multiple times following review requests run the risk of losing their whitelisted status and hence future revenues. At any point in time, DIVA token holders can trigger a vote to remove a data provider from the whitelist. If a whitelisted data provider is removed from the whitelist, DIVA token holder will step in as data providers for all open contracts where this data provider is assigned as the oracle.

We acknowledge that the proposed oracle involves human interaction and may be less efficient than receiving inputs from one of the existing oracle solution (e.g., Chainlink or Band Protocol). However, we believe that the benefit of involving human judgement in non-standard situations (e.g., a change in the index calculation methodology or stock split during the lifetime of the contract) and having full flexibility in terms of underlying choice will outweigh the extra cost.

Existing oracles solutions may be considered at a later stage to offer users that are willing to take the risk of purely automated settlement an alternative.

10.3.2.3 Fast settlement

While giving position token holders the possibility to challenge the submitted settlement value increases the trust in correct settlement, long settlement periods are a bad user experience. Position token holders have to wait at least 72 hours / 3 days post expiration until they can withdraw their funds.

We do not consider this to be a problem though. Due to this potentially large settlement delay, we expect market makers to jump in and offer faster settlement services against a small discount, especially when the chosen data provider is deemed trustworthy. In particular, the data provider themselves may step in as a market maker to benefit from an additional revenue stream.

Example: Let's assume the following two actors:

- Alice: has 1 long position token worth 1 ETH and wants fast settlement
- Bob: has 0.95 ETH and is willing to accept the settlement delay and the settlement risk

Right after expiration date, Bob offers Alice to buy back her long position token for 0.95 ETH. If Alice accepts the offer, Bob will pay Alice 0.95 ETH in exchange for her long position token which he can then redeem for 1 ETH at the end of the settlement period. We expect the fees paid to these market makers to compress over time, if there's demand for this service, making the procedure completely invisible to users eventually.

10.3.2.4 Reputation score

Every settlement process and the length of the dispute mechanism is recorded on the blockchain and is visible to everyone. We will use this data to derive a reputation rating for each data feed provider. In particular, any failure to provide a settlement price within the given time period as well as more than one correction of the value following review requests will negatively contribute to the rating.

11 Trading

Since DIVA position tokens follow the ERC-20 standard, they can be easily integrated and traded on any ERC-20 compliant decentralized exchange (e.g., Uniswap, Loopring, Matcha) or centralized exchanges.

Larger OTC trades can be agreed upon through traditional means, then made formally-binding using the protocol.

12 Valuing position tokens

A long/short position token gives the holder the right to claim the remaining collateral in the respective pool at expiration date. That right comes with a price, also referred to as the *premium*, which rests on the probability that claiming collateral will end up being profitable at expiration.

The premium is essentially a probability-weighted average of future payoffs. The more likely a payoff is to occur, the more expensive the position token. For instance, the value of a long position token goes up as the underlying asset goes up.

The premium can be broken down into two components, the intrinsic value and the time value which we will explore in greater detail below.

12.1 Intrinsic value

The first component that impacts the premium is the intrinsic value. The intrinsic value of a position token is the value that a position token holder would be able to claim if the contract expired today. For long position tokens, the intrinsic value is positive as long as the underlying value stays *above the floor*; otherwise it's zero. For short position tokens, the intrinsic value is positive as long as the underlying value stays *below the cap*; otherwise it's zero. The intrinsic value is derived from the payoff curve of the respective position token.

Given the capped nature of the payoff curves, the intrinsic value has a maximum value. For both long and short position tokens, the maximum intrinsic value is given by the overall collateral deposited into the pool divided by the respective token supply. For long position tokens, this maximum is reached if the underlying value is at or above the cap. For short position tokens, this maximum is reached if the underlying value is at or below the floor.

12.2 Time value

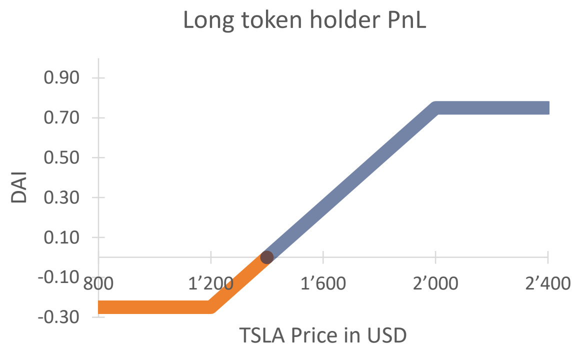
The second component that impacts the premium is the time value. In general, the time value is positive and is based on the underlying's expected volatility and time until position token's expiration. All else equal, the less time there is until expiry, the lower the uncertainty about the outcome and hence the lower the value of the position token. As the contract approaches expiration, the time value converges to zero and the position token's value converges to its intrinsic value.

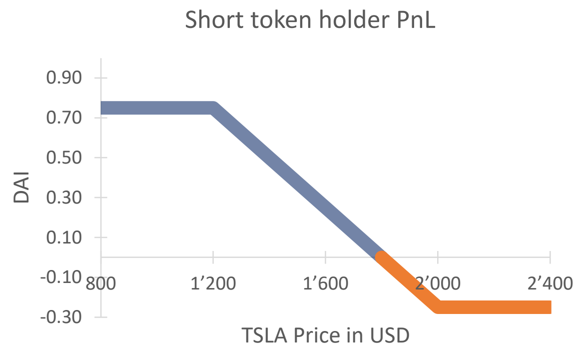
Similarly, all else equal, the higher the expected volatility of the underlying asset, the higher the probability of extreme payoffs due to substantial moves up or down and hence the higher the value of the position token. Given the high volatility of crypto assets, it is very likely that position tokens issued on these assets will have a significant time value component included in the premium. In contrast, for stablecoin pairs (e.g., DAI/USDC), the volatility is close to zero and hence the time value is expected to be close to zero. Latter will make protective short positions against a black swan event that causes the DAI peg to break an attractive investment opportunity.

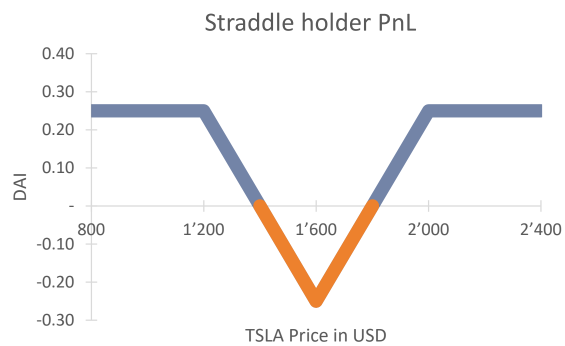
Position tokens are similar to traditional options in that they offer a chance to receive a positive payoff in the future against a premium paid today. There exist several option pricing models to determine the fair market value of an option. Of these, Black-Scholes model is the best-known options pricing model and could also be applied to price DIVA position tokens.

12.3 Trader PnL

The net gain of a position at expiry will be the amount claimable per token minus the premium paid. This is illustrated below for three different payoff functions.







12.4 Arbitrage bounds

Similar to the put-call parity relationship in options pricing, there is a tight relationship between the value of a long and a short position token. At any point in time, the combined market value of long and short position tokens should equal the overall collateral locked in the pool:

$$p_t^S * M_t^S + p_t^L * M_t^L = C_t^S + C_t^L$$

where p_t^L / p_t^S is the long/short position token price, M_t^L / M_t^S the corresponding token supply and C_t^L / C_t^S the corresponding pool balance at time t. Any deviation from that relationship will open up arbitrage opportunities which traders will exploit until it disappears and position tokens converge to their fair value.

Example: Let’s assume that the long position token of Chad’s Tesla derivative contract (see section 5) was traded at DAI 0.7 and the short position tokens at DAI 0.5. At a token supply of 100’000 each, this implies a combined market value of DAI 120’000 which exceeds the maximum collateral that can be redeemed from the contract by DAI 20’000. An arbitrage trader can exploit this situation by sending, say, DAI 10 to the contract in order to mint ten long and ten short position tokens and sell them on the market for DAI 12, pocketing in an immediate risk-free gain of DAI 2. Similarly, if the tokens were traded at, say, DAI 0.4 each, a trader could purchase one long and one short position token on the market for a total of DAI 0.8 and redeem it immediately from the contract for a total return of DAI 1.0.

Assuming that the relationship can be enforced, a quoted price for one position token would imply a quoted price for the opposite position token. In other words, liquidity has to develop only on one side of the trade, the liquidity on the other side is automatically derived.

DIVA will use that relationship to build a dedicated decentralized exchange for position token trading.

13 Scalability

Gas prices on Ethereum have exploded in recent times which makes contract execution very expensive. Layer 2 solutions such as zkRollups, Optimistic Roll-ups or Matic will be explored in the early phase of the project.

14 DIVA Tokenomics

A good token design is critical to any decentralized project's success. The introduction of a token serves three main goals:

- Incentivize developers and the community to contribute to the development of the protocol
- Align incentives of all stakeholders to act in the best interests of the protocol
- Encourage market participants to use the protocol

To achieve these goals, it is critical that the token captures value and is closely linked to the growth of the platform. At the same time, it is important to enable all DIVA users a frictionless experience by eliminating unnecessary frictions including staking or holding the token to interact with the protocol (such as paying protocol fees in DIVA token for example).

We believe that we can achieve these goals with the following tokenomics:

1. **Max supply:** 100 million will be the max supply. No more tokens will be minted.
2. **Protocol fees:** At expiry, a protocol fee of 0.25% is charged on the collateral locked in the pool and transferred to the DIVA treasury. The fee is paid in units of the deposited collateral by short/long position token holders at redemption and converted into DIVA tokens. This ensures that demand for DIVA tokens will increase as the platform grows.
3. **Governance:** Each DIVA token represents one vote and will entitle holders to vote on binding governance initiatives related to DIVA protocol upgrades and how to spend the DIVA treasury.
4. **Fee discount:** A 50% fee discount is granted when DIVA token is used as the collateral asset.

To incentivize the usage of the protocol in the early phase, protocol fees will be waived at the beginning. As the usage and liquidity of the platform grows, market makers will extract a large part of their revenue from trading position tokens which allows to redirect a portion of the fees towards the DIVA treasury.

14.1 Token distribution

DIVA tokens will be earned by using the DIVA protocol. By depositing collateral into derivative contracts (either at contract creation or during the lifetime of a contract), liquidity providers will continuously and automatically receive freshly minted DIVA tokens, up to a total maximum token supply of 100 million.

More precisely, 70 million DIVA tokens will be placed into a Reservoir contract, which transfers 3.0 DIVA tokens per Ethereum block (~19'500 per day, ~7'000'000 per year) into the protocol for distribution over a period of roughly 10 years based on the following split:

- 50% Liquidity providers (35% of overall token supply)
- 22% DIVA treasury (15% of overall token supply)
- 28% DIVA protocol team (20% of overall token supply)

The amount distributed to liquidity providers is proportional to the liquidity provided within eligible markets. DIVA token holders will decide which markets are eligible for the DIVA token drop (e.g., markets using WETH, WBTC, DAI, USDC, or DIVA as collateral) and the allocation between them.

The proposed distribution mechanism will benefit early adopters disproportionally as they will have to share the DIVA reward with less participants in the early phase of the protocol.

The remaining 30 million DIVA tokens will be allocated to the team (10 million) and DIVA treasury (20 million) at launch of the protocol.

14.2 DIVA governance

The DIVA protocol is maintained and upgraded through a community governance system in which DIVA token holders and their delegates debate, propose, and vote on all changes to the protocol. The governance mechanism will fork the Compound DAO, which is well established and understood within the DeFi ecosystem. Governance has control over the following actions:

- Adjust settlement parameters (e.g., challenge period, review period)
- Adjust protocol fees for settlement and redemption
- Adjust governance parameters (e.g., quorum threshold, proposal threshold)
- Adjust whitelist of data feed provider
- Decide on the markets that are eligible for the DIVA token drop

In addition to protocol level governance, DIVA token holders will be able to vote on how to spend the DIVA treasury. This can include protocol developments, marketing, partnership incentives, hiring, security audits, token buyback and burn, etc.

15 Conclusion

With DIVA, we are bringing a simple yet powerful derivatives solution to DeFi. DIVA will be the easiest and most efficient way to express long and short views on any asset in the world. Uniswap has demonstrated that successful products do not need to be complicated.

16 Appendix

16.1 Payoff function

Given the terminal value of the underlying asset, the payoff function determines the collateral amount that long and short token holders can claim from the respective pool following contract expiration. In particular, the payoff function can be used to calculate a position token's intrinsic value at any point in time during the lifetime of a contract.

The payoff function is a shifted version of the pool PnL function expressed per token. Hence, to derive the payoff function, we will first derive the pool PnL function.

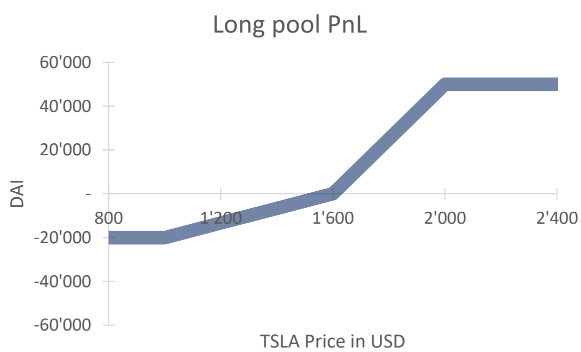
16.1.1 Pool PnL function derivation

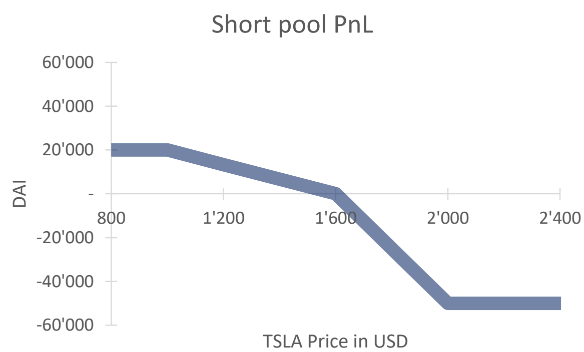
We define the following variables:

- C_t^L Collateral amount in the long pool at time t
- C_t^S Collateral amount in the short pool at time t
- p^c Cap
- p^f Floor
- K Strike
- M_t^L Long token supply at time t
- M_t^S Short token supply at time t
- p_t Underlying value at time t

A generalized example of pool PnL curves is shown below using the following contract configuration:

$C_t^L = DAI\ 20'000,\ C_t^S = DAI\ 50'000,\ p^c = USD\ 2'000,\ p^f = USD\ 1'000,\ K = USD\ 1'600,\ M_t^S = M_t^L = 100'000$





As can be seen from the charts, the slope of the PnL curves changes at the strike. Let β_t^L denote the slope of the long pool PnL curve. Then β_t^L is formally given by

$$\beta_t^L = \begin{cases} \dfrac{C_t^S}{p^c - K}, & p_t \geq K \\ \dfrac{C_t^L}{K - p^f}, & p_t < K \end{cases}$$

The intercept parameter of the implied linear function is given by

$$\alpha_t^L = -K * \beta_t^L.$$

As the maximum loss of the long pool is capped by C_t^L and the maximum gain by C_t^S, we can derive the long pool PnL function V_t^L:

$$V_t^L(p_t) = \min\{C_t^S; \max\{-C_t^L; \alpha_t^L + \beta_t^L * p_t\}\}.$$

Similarly, the short pool PnL function is given by

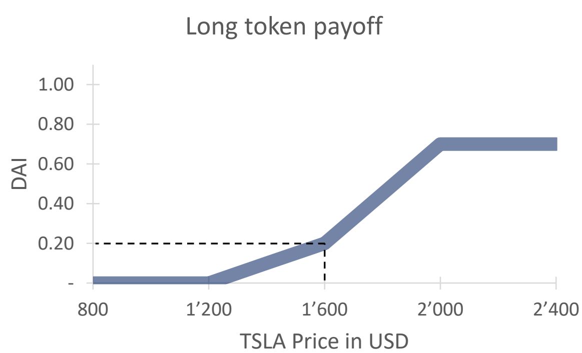
$$V_t^S(p_t) = \min\{C_t^L; \max\{-C_t^S; \alpha_t^S + \beta_t^S * p_t\}\},$$

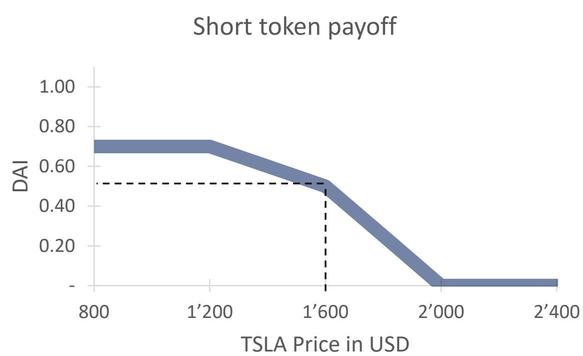
where $\beta_t^S = -\beta_t^L$ and $\alpha_t^S = -\alpha_t^L$. Given the zero-sum relationship between the long and the short pool, V_t^S can also be written as

$$V_t^S(p_t) = -V_t^L(p_t).$$

16.1.2 Payoff function derivation

The payoff per long and short position token is obtained by shifting the pool PnL curves by the collateral amount deposited in the respective pool and dividing by the corresponding token supply. The payoff per token resulting from above pool PnL curves are illustrated below:





Formally, the long and short token payoff functions are given by

$$\hat{V}_t^L(p_t) = (V_t^L(p_t) + C_t^L)/M_t^L \;= \min\{C_t^S + C_t^L; \max\{0; \alpha_t^L + \beta_t^L * p_t + C_t^L\}\}/M_t^L$$

and

$$\hat{V}_t^S(p_t) = (V_t^S(p_t) + C_t^S)/M_t^S = \min\{C_t^L + C_t^S; \max\{0; \alpha_t^S + \beta_t^S * p_t + C_t^S\}\}/M_t^S.$$

Latter can also be written as

$$\hat{V}_t^S(p_t) = (C_t^S + C_t^L - \hat{V}_t^L(p_t) * M_t^L)/M_t^S.$$

The formulas show that for both long and short positions gains are capped by $C_t^L + C_t^S$ divided by the respective token supply.

16.1.3 Symmetric case

In a scenario where the long and short pool are equally funded (i.e, $C_t^S = C_t^L$) and the cap/floor are equidistant from the strike (i.e., $p^c - K = K - p^f$), β_t^L does no longer depend on the position of the underlying value p_t relative to the strike:

$$\beta_t^L = \frac{C_t^S}{p^c - K}.$$