Deri V2: The Derivative Exchange Protocol with Extreme Capital Efficiency

Version 0.1.0
2021 May

Abstract
In this paper, we introduce Deri Protocol V2, a decentralized protocol of derivative exchange upgraded from Deri Protocol V1. Deri V2 inherits all the features of V1 but supports several key new features, such as dynamic mixed margin and liquidity-providing. With such features of Deri V2, multiple tokens are supported as base tokens for liquidity providers to provide as liquidity as well as for traders to deposit as margin. Such a dynamic mixed margin and liquidity framework becomes feasible in the DeFi world because of the functionalities provided by other DeFi infrastructures. Within the framework of Deri V2, derivative trading can achieve an optimal capital efficiency, which is potentially higher than that of centralized exchanges.

Contents

1 Introduction

1.1 Summary of Deri V1

Several months ago, we introduced Deri Protocol V1, a decentralized protocol for users to exchange risk exposures precisely and capital-efficiently. Deri Protocol is the DeFi way to trade derivatives: to hedge risk, to speculate or to arbitrage, all on-chain. This is achieved by the so-called Automatic Market Maker (hereinafter referred to as AMM) mechanism: liquidity pools playing the roles of counterparties for traders. That is, the liquidity pools are standing by to always take the opposite side of traders' derivative positions. This is similar to how the AMM-based decentralized exchanges, e.g. Uniswap, accommodate the spot trading demands of traders. The only difference is between the respective trading natures of spot exchanges and derivative trading. The former is an exchange between token *X* and token *Y*. For such a business, a standing-by counterparty's job is to simultaneously hold a pair of reserves, one of *X* and the other of *Y,* and to swap *X* for *Y* (or *vice versa*) upon a trader's request. Whereas in the case of derivative trading, a standing-by counterparty's job is to always enter the opposite side when a trader is establishing some derivative position. For example, it is to enter the short position with the same volume when a trader is establishing a long position of futures contract. In this regard, Deri is playing the same role in the derivative trading business as that of the AMMs, e.g. Uniswap, in the spot exchange business.

In the case of spot AMM, the pair of reserves (*X* and *Y*) are contributed by the liquidity providers (hereinafter referred to as LP). Whereas in the case of derivative trading conducted as "cash settlement", there is no physical exchange of the trading objects (the underlyers) - the counterparties of a derivative only settle their profits and losses (hereinafter referred to as PnL) with "cash", i.e. the settlement currency/token. Thus for a derivative AMM to carry out the cash-settlement type of derivative trading, to which most of the crypto derivatives belong, only the settlement currency/token is needed to be held in the reserve. At the settlement with a trader, a derivative AMM pays out him/her on a realized profit while charges him/her on a realized loss, with settlement currency/token. Therefore, the LPs of a derivative AMM, e.g. Deri, only need to provide the settlement currency/token to the liquidity pools, to settle realized PnL of the traders.

And just like the LPs of an AMM are facing the issue of impermanent loss (IL), the LPs of the Deri pools are facing similar issues too, but in a different manner. Deri LPs are facing market risks. Nevertheless, it is important to point out that such market risks are different from the impermanent losses borne by the LPs of spot AMMs. The fact it is called "risk", instead of "loss", indicates that the result could be either positive or negative, whereas impermanent "loss" is a certain negative consequence. In regard to market risk, the ideal scenario for the liquidity pool accommodating traders' positions is that the long and short positions are equal so they cancel each other out. However, this would not happen spontaneously should there be no mechanism enforcing or inducing such states. While it is difficult to enforce a state of perfectly balanced long and short sides, the system could be induced to converge to such a state. Deri introduces the funding fee mechanism: the majority-side positions pay the minority-side positions a funding fee per block, proportional to the degree of imbalance (measured by the net position). When the funding fee rate is above some threshold, arbitragers would be induced to take the minority side. In reality, there would be more than one arbitrager competing for the funding fee, otherwise the only arbitrager would rather wait for the funding rate to grow big until it takes any action. Such arbitrage competitions ensure the funding rate cannot increase to a too high level, hence the long and short sides will not be too imbalanced. The arbitragers are motivated by profit but meanwhile help the traders and liquidity providers.

1.2 Why Deri V2 is needed?

Deri V1 has been working well for several months after its launch. A number of trading pools with trading symbols of different natures (both crypto and traditional financial) have been deployed on multiple blockchain networks (Ethereum, BSC, and HECO) to accommodate traders' speculating and hedging demands. Having been serving such demands correctly and smoothly for several months has generally proved that such a framework is effective and efficient for providing a way for users to trade derivatives on-chain. Nevertheless, it has not yet achieved the optimal capital efficiency that is possible in the DeFi world. That is, some of the major advantages of the DeFi system are yet to be taken. For example, in the DeFi world, most of the elements are tokenized (as fungible token like ERC20 or non-fungible token like ERC721), which are extremely easy to be swapped into other tokens ("cash-out") thanks to the spot AMM infrastructure. With such an infrastructure readily available, any tokens with a value realizable by the spot AMMs can serve the purpose of a "liquidity token".

Before diving into the discussion of the innovative liquidity-handling of DeFi, let's first look at the old-school ways. In the traditional finance or the pre-DeFi crypto world, usually only "cash" or "cash-equivalent" tokens could be adopted as "liquidity tokens". Typical "cash" or "cash-equivalent" tokens were Bitcoin or Ethereum in the pre-stablecoin era and gradually transited to the stablecoins, e.g. USDT or DAI, after the stablecoin infrastructure matured. This could be easily figured out by looking at what currencies/tokens the centralized derivative exchanges carry out their trading business based on: BitMEX adopts Bitcoin only while the Binance Futures adopts Bitcoin or other mainstream coins/tokens for its Coin-Margined Futures and USDT or BUSD for its USDⓈ-M Futures. The centralized exchanges limit their "liquidity tokens" to a very narrow range largely because converting tokens back-and-forth is somewhat of a burden. BitMEX, for example, is an exchange specialized for derivatives without built-in spot exchange functionality and thus has difficulties dealing with the non-cash types of tokens within the exchange. Binance, on the other hand, is in a better situation as it has its own spot exchange module and thus would be able to deal with non-cash types of tokens within the greater binance system should its spot and derivative modules interact seamlessly. But still, such dealing with non-cash types of tokens is within one single site. That is, the dealing is limited by the liquidity carried by the single site[1]. That is not the case for DeFi!

[1] One example of such centralized exchanges is FTX.

In the DeFi world, as of now, the whole blockchain is one unified financial system, in which every DeFi app is a module of the system and readily available for other apps to interact with. Moreover, such unification will be further enhanced upon the mature of cross-chain infrastructure. Thanks to the interactability and composability of DeFi applications, any token is just one swap away from another token as long as there is a spot AMM, e.g. Uniswap, providing liquidity for such a swap on this blockchain (or across blockchains in the future). Specifically, any token is just one swap away from the traditional "cash" or "cash-equivalent" tokens, e.g. USDT or DAI, given there is a spot AMM supporting the swap. Consequently, in theory we can extend the range of "liquidity token" to include any tokens that could be swapped into "cash" or "cash-equivalent" tokens. Of course, in practice there are some other factors to be taken into account, e.g. the volatility or the liquidity sufficiency, but the range of "liquidity token" would be substantially larger.

Such an enlargement of the "liquidity token" range leads to a significant enhancement of capital efficiency.

1.3. Capital efficiency

In finance, capital efficiency refers to the financial utility that one can achieve with a single unit of asset. Most of the financial tools in the modern financial system are designed to enhance the capital efficiency of economic activities.

Let's take an example to explain the concept. Suppose Alice would like to speculate on the price change of SP500 and she has a house with a market price of 1 million US dollars. Alice could take a loan with her house as collateral and long SP500 futures with the borrowed capital as margin. Two parameters are affecting the capital efficiency in this deal: the pledge-rate of the loan and the margin ratio of the futures. If the pledge-rate is 200% and the margin ratio is 10%, then she can borrow 500K USD cash with the house as collateral and long a future of 5M's notional value. Here the capital efficiency could be measured as the ratio of the financial position's notional value to the asset value being used. That is, with a collateralized loan and a derivative, Alice has achieved a financial position equal to 5 times her house value (i.e. a 5X leverage in the everyday words). The capital efficiency would be higher if she could have a lower pledge-rate or lower margin ratio.

While it is possible to adjust the risk management parameters, i.e. pledge-rate and margin ratio, to improve the capital efficiency of Alice's deal, in practice they are bound by other considerations. And the fundamental bottleneck constraining the capital efficiency here is the two-step procedure: Alice has to borrow the collateralized loan from a lender (usually a bank) and then posts the borrowed cash as margin to trade derivatives that she wants. That is, there has to be an intermediate step of cash in this deal, as the financial functionalities in the traditional finance are segmented thus the derivative trading business usually can only deal with cash or cash-equivalent for collateral. In other words, the liquidity is segmented into different financial functionalities and the whole financial system depends on cash or cash-equivalent to connect the segmented modules together. However, such an intermediate step of cash compromises capital efficiency.

1.4 The higher capital efficiency of Deri V2

One of the major motivations of upgrading Deri V1 to V2 is to improve the capital efficiency of derivative trading. One constraint of the capital efficiency of Deri V1 is that for derivative trading people have to deposit stablecoin as margin, just like Alice has to deposit cash as margin to trade equity index futures in traditional finance in the example in Section 1.3. If cash as an intermediate step could be skipped (e.g. directly deposit the house as collateral to trade futures), the capital efficiency would be substantially enhanced. While depositing house as collateral is rather difficult to execute in traditional finance (maybe only possible in some bespoke OTC deal), it's reasonably feasible to accept a wide range of non-cash-like tokens (assets) as collateral to trade derivatives in the DeFi world, simply because a lot of tokens or assets are just one swap away from the "cash" or "cash-equivalent" tokens, e.g. USDT or DAI, given there is a spot AMM supporting the swap. And thanks to the composability of the DeFi framework, this one-swap-away gap could be easily taken care of by just a function call to the spot AMM app. In short, with the swapping functionality provided by spot AMM, any DeFi app could treat a swappable non-cash-like token just almost like "cash". Please note it is "almost like" instead of "exactly like" because there is still one swap action to be carried out and price fluctuation (i.e. market risk) needs to be dealt with. Nevertheless, treating non-cash-like tokens just almost like cash could lead to extreme capital efficiency.

That is Deri V2's mission!

2 Architectural Changes

2.1 Dynamic mixed margin

Per discussion in Section 1, treating non-cash-like tokens just like cash could lead to extreme capital efficiency. Guided by this ideal, Deri V2 implements a margin system accepting multiple base tokens. With such a system, a trader could choose one or more from the supported range of base token to post as margin. And this no longer has to be stablecoin. Nevertheless, among all the base tokens, one has to be chosen as the settlement token (called Base0, or B_0, in the Deri terminology). The settlement token is playing the role of the "real cash" of the whole trading business. That is, all the fees and PnL are calculated and settled in this token. One can think of the settlement token as the base currency (e.g. USD the domestic currency) of an accounting system dealing with multiple currencies in traditional finance while the other base tokens as other types of assets that a financial system accepts as collateral (e.g. foreign currencies). Since the other base tokens' prices per the settlement token are generally in constant change, the balance of a trader's margin is constantly changing too. Hence it is called "dynamic" margin.

The dynamic nature of the margin actually causes an extra burden for risk management. In a static margin system where only the settlement currency/token is accepted as collateral, the risk management system only needs to compare a position's dynamic balance (changing due to the realized PnL) with its static margin value. Whereas in the case of dynamic margin, the risk management system needs to compare two things both dynamic in real time: the balance and the margin value. The latter is way more complicated than the former. For a centralized derivative exchange, such comparisons are usually carried out in real time by the (centralized) risk management engine, which puts a bottleneck on the processing capacity of the order-matching engine. Whereas in the trading system of Deri, such comparisons (and any subsequent action-taking) are handled in a decentralized way[2]. Therefore the extra burden introduced by the dynamic mixed margin is handled in a way with a much larger capacity. That said, the decentralized liquidators do need to upgrade their algorithms of monitoring the margin ratios of the trading positions to correctly handle the compare-dynamic-to-dynamic situation.

One extra procedure is involved when a position is closed in loss (including the case of enforced closing, i.e. liquidation) while the position's margin token B_x is not the settlement token B_0: since everything is settled in B_0 the pool needs to convert part or all of the position margin in B_x into B_0 to settle the loss. This is handled by swapping B_x into B_0 via an external spot AMM, e.g. Uniswap. Please note a position could hold multiple base tokens simultaneously and when a position has B_0 and non-B_0 tokens as margin at the same time, B_0 will always be used to settle loss first. A conversion of non-B_0 tokens into B_0 for settlement only takes place when there is no sufficient B_0. Please also note that profit is always paid in B_0.

2.2 Dynamic liquidity providing

Just like on the trader side, Deri V2 also allows liquidity providers to choose one or more from the supported range of base token to provide liquidity. Also just like the margin value, the provided liquidity provided is dynamic too, in general. Consequently, the total value locked (hereinafter referred to as TVL) in a liquidity pool is also dynamic. The liquidity pool is playing the role of the counterparty for the traders. Essentially, the pool itself is a passive trader and its TVL is its margin balance (excluding unrealized PnL). From this perspective, the dynamic TVL of a pool is essentially similar to the dynamic margin of a trader's position. Hence it is handled in a similar way.

On the pool side, there is one additional procedure involved. Since all the liquidity providers share the pool income (including transaction fee, funding fee, trader's loss and the remaining value of liquidated positions)[3] per their respective liquidity contributions, the pool income needs to be distributed in a dynamic manner too. Specifically, this is done by distributing pool profit (or loss), whenever it is generated, to the base tokens per their respective weights calculated by real-time prices. This procedure could be thought of as every base token has its virtual account within the pool. Every time there is a PnL generated, it is distributed by the real-time weights of the base tokens and credited into the virtual accounts. When some LP withdraws his/her liquidity of some base token (denoted as B_x), he/she will take out his/her share of the profit in B_x if B_x has

[2] Refer to Section 2.3.6 of the Deri V1 whitepaper for details.

[3] Please note this income could be negative as all the traders together could have a positive net profit, corresponding to a loss of the pool.

accumulated a positive PnL during his/her liquidity mining period, or he/she will pay out his/her share of the loss in B_x if B_x has accumulated a negative PnL during his/her liquidity mining period. While the pool accumulates PnL continuously, every LP takes the profit or pays the loss for the period he/she has been participating in the liquidity contribution (i.e. liquidity mining). To implement such a PnL sharing mechanism, the LP token (called LToken in Deri terminology) is designed to be a non-fungible token to record the information at the starting and end points of the mining period, which is specific to each LP (hence non-fungible).

Similar to the loss-settlement process of non-B_0 margin token, one extra procedure is involved in the PnL sharing mechanism when B_x is not B_0: since the PnL is always in B_0 and the LP is mining with B_x, the pool needs to convert the PnL in B_0 into B_x to settle the LP's share of PnL. This is handled by swapping B_x into B_0 for a negative PnL or *vice versa* for a positive PnL.

2.3 Multiple trading symbols in one pool

Another new feature introduced in Deri V2 is that multiple trading symbols (i.e. underlyers) could be traded in one pool. This is to further enhance the capital efficiency since the trades of different symbols are sharing the same liquidity hub. The correlation between the price movements of the trading symbols determines the degree of capital efficiency improvement. The less correlated the price movements are, the higher capital efficiency the pool can achieve. Please note this is something unimaginable in the traditional orderbook-based trading paradigm, since an orderbook is always for one specific trading symbol and there is no way two or more symbols can share liquidity.

Trading multiple symbols in one pool is one of the liquidity-enhancing mechanisms that make the pool-based trading paradigm more capital-efficient than the orderbook-based one, which is the dominant paradigm of centralized exchanges.

2.4 Other changes

Deri V2 also upgrades the algorithm of funding fee so it is more suitable for the volatile market of cryptocurrencies. Specifically, the funding fee that one long contract pays one short contract per block is:

$$F_{block} = R \cdot N$$

where *R* is the funding rate and *N* the notional value of one contract, calculated as follows:

$$R = \frac{r(l-s)Pm}{L},$$

$$N = Pm$$

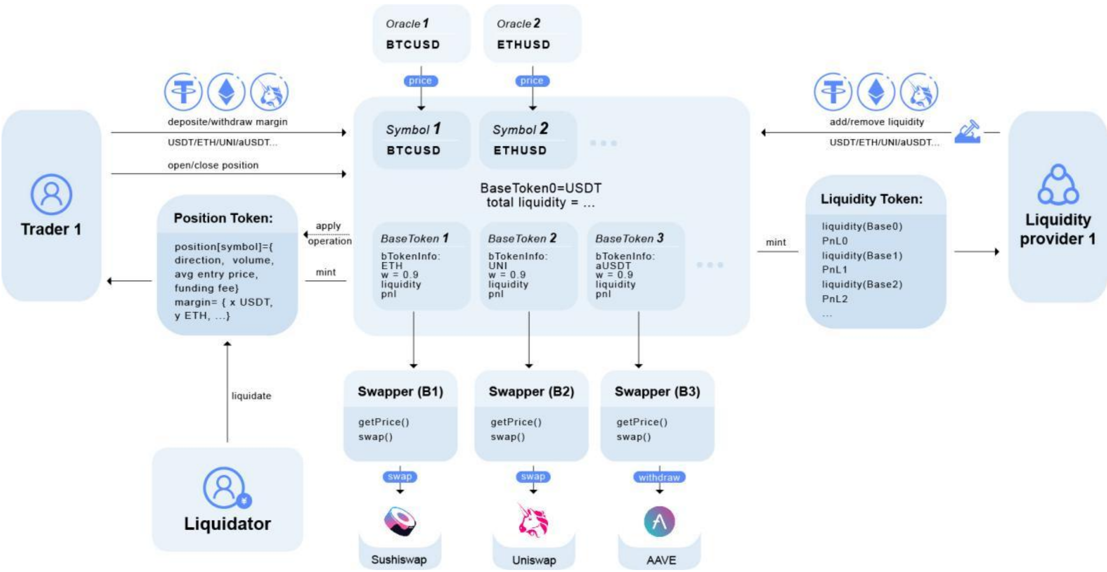
Where *r* is the funding rate coefficient; *l* and *s* the numbers of long and short contracts; *P* the trading symbol price; *m* the contract multiplier and *L* the pool liquidity.

3 Implementation

3.1 The architecture

The architecture of Deri V2 is largely similar to that of V1: the liquidity pool on one hand accepts liquidity from liquidity providers and on the other hand establishes positions for traders' long or short orders. Essentially, the liquidity pool plays the role of liquidity medium and makes transactions of base tokens between traders and liquidity providers to reflect trading PnLs. Compared with that of Deri V1, one additional job for the pool of Deri V2 is to deal with non-Base0 tokens. When necessary, it calls the corresponding functions in external DeFi applications to swap between B_0 and other B_x tokens. This is handled by a module called swapper, explained in Section 3.3.

The architectural chart below illustrates how the pool interacts with liquidity providers and traders under Deri protocol.



3.2 The new LP token as NFT

LP token in Deri is denoted as LToken. Since a liquidity provider can choose from one or more of the supported base tokens as liquidity to provide to the pools of Deri V2, all LPs' contributions are heterogeneous and thus can no longer be represented by fungible tokens. Instead, non-fungible tokens (hereinafter referred to as NFT) are adopted to implement LToken. An LToken of Deri V2 records the liquidity an LP has contributed with each base token (denoted as an "asset" in the code). This is implemented by a table mapping base token ID to asset recording the LP's contribution and PnL on each base token. PnL is calculated with a cumulative methodology so that the LP is only sharing the accumulated PnL in his/her participating period.

3.3 The swappers

The pool deploys one swapper for each non-Base0 token. The swappers are responsible for swapping B_x into B_0 or *vice versa*. This takes place in the following scenarios:

- When a trader closes a position in loss (including enforced closing, i.e. liquidation) and the margin account does not have sufficient B_0 token to settle the loss, then the swappers would kick in to swap part or all of the non-Base0 tokens in the margin account for the loss settlement.
- When an LP withdraws his/her non-Base0 (B_x) liquidity from the pool with a positive PnL, the corresponding swapper swaps some of the pool's B_0 into B_x to pay his/her profit.
- When an LP withdraws his/her non-Base0 (B_x) liquidity from the pool with a negative PnL, the corresponding swapper swaps some of the LP's B_x into B_0 to settle his/her loss.

Please note that no swapping is involved when trading or liquidity providing is handled with Base0. Also please note that the verb "swap" is a general term: for example, in the case B_x is the "yield token" of B_0, e.g. aUSDT corresponding to USDT deposited in AAVE, the action of swapping B_x into B_0 means *redeeming* B_x (aUSDT) to *withdraw* B_0 (USDT) from the AAVE staking pool.

4 Summary

Since its launch, Deri V1 has been working well for several months with various trading pools deployed on multiple blockchain networks to accommodate traders' speculating and hedging demands. It has proved that such a framework is generally effective and efficient for users to exchange risk exposures. Nevertheless, some of the major advantages of the whole DeFi ecosystem are yet to be taken advantage of to further improve the protocol, especially on the capital efficiency part.

In order to provide an optimal capital efficiency for the users, we have upgraded Deri Protocol from V1 to V2 with a number of changes:

- Accepts traders to choose one or more from the supported base tokens to post as margin;
- Accepts liquidity providers to choose one or more from the supported base tokens to provide as liquidity;
- Supports multiple trading symbols within one single pool

With these defining features of Deri V2, users can enjoy capital efficiency beyond most of the other existing derivative trading exchanges or platforms. Such optimal capital efficiency is made possible mainly thanks to the interactability and composability of the DeFi applications. That is, the DeFi applications on the same blockchain can interact with each other just like calling internal functions.

References

[1] The Deri V1 whiterpaper:
https://github.com/deri-finance/whitepaper/blob/master/deri_whitepaper.pdf

[2] The Uniswap whitepaper: https://uniswap.org/whitepaper.pdf

[3] Financial derivatives: https://en.wikipedia.org/wiki/Derivative_(finance)

[4] Bitmex Perpetual Contracts Guide: https://www.bitmex.com/app/perpetualContractsGuide

[5] Binance Contract Specifications of USDⓈ-M Futures:
https://www.binance.com/en/support/faq/360033161972

[6] Binance Coin-Margined Futures Contracts and Contract Specifications:
https://www.binance.com/en/support/faq/a4470430e3164c13932be8967961aede