Deri

The Derivative Exchange Protocol

Version 0.0.9
2020 Dec

Abstract

In this paper we introduce a decentralized protocol allowing users to exchange risk exposures precisely and capital-efficiently. With this protocol, risk exposures are tokenized as non-fungible tokens so that they can be imported into other decentralized financial projects for their own financial purposes.

Table of Content

1. Introduction

1.1 What is derivative?

In finance, a derivative is a contract that derives its value from the performance of an underlying entity. This underlying entity can be an asset, index, or interest rate, and is often simply called the underlying or underlyer.

Derivatives can be used for a number of purposes, including insuring against price movements (hedging), increasing exposure to price movements for speculation, or getting access to otherwise hard-to-trade assets or markets.

Some of the more common derivatives include forwards, futures, options, swaps.

The economic essence of derivative is for the user to **acquire specific risk exposures precisely and capital-efficiently.**

1.2 Why a decentralized protocol for derivative?

Exchanging risk exposures is one of the core functions of finance, together with borrowing&lending, spot exchange, etc.. Blockchain as a financial infrastructure needs an on-chain mechanism to do that.

As a matter of fact, the centralized exchanges (CEXs) of crypto derivative have already been serving the purpose of exchanging risk exposures in the crypto world for a while. Nevertheless, since CEX is not organic within the blockchain, it cannot directly interact with other on-chain activities (i.e., transactions). Therefore, while CEXs can partially serve the purpose as a plug-in solution for the decentralized financial (DeFi) ecosystem, they cannot play the role of the on-chain (decentralized) exchanging mechanism. And for the same reason, while the hybrid solutions (partially on-chain, partially off-chain) do have added-values for specific scenarios, they cannot be the ultimate solution for DeFi either.

Simply speaking, the ultimate solution to exchanging risk exposures in the crypto world has to be something **original and organic within blockchain.**

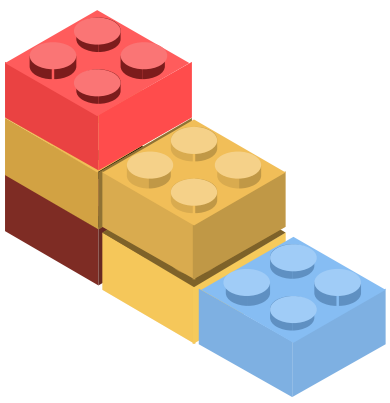
1.3. Derivative DEX vs CEX

Since the centralized exchanges (CEXs) of crypto derivative have already been partially serving the purpose, it helps understand the decentralized exchange (DEX) solution by comparing these two. Nevertheless, please note this is really a comparison between two different creatures: while DEX and CEX partially share the same purpose, they are fundamentally different in their natures.

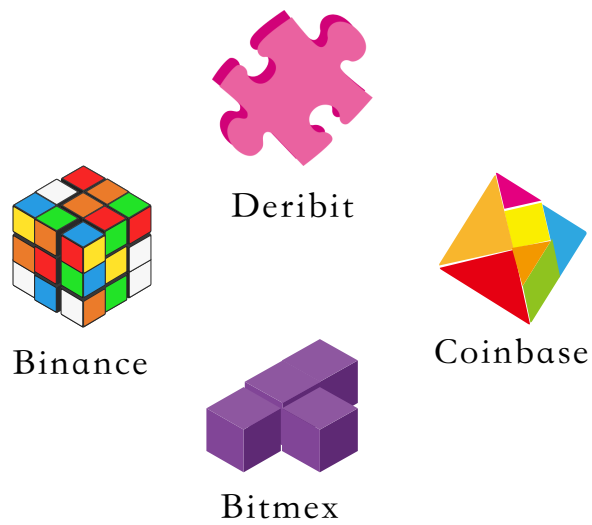
Table 1: DEX vs CEX

	DEX	CEX
What it really is?	A protocol (a group of smart contracts)	A physical platform run by an institute
Trading paradigm	Multiple paradigms: pool-based likely to dominate	Orderbook-driven
Composability	Designed to be composable: part of the whole DeFi “lego game”	Every CEX is a closed system of its own
Transparency	Trading process completely transparent	Partially transparent
Account type	Blockchain address	Website account
KYC/AML	An issue of chain/address, not of protocol	Controller's choice
Custodian & Capital security	Non-custodian;?as secure as ETH in wallet	Custodian; security depending on platform's tech level
Performance	TPS & latency depending on the chain's performance	High TPS & low latency
User-friendliness	crypto-friendly: extremely simple for people with wallets	Follow tranditional finance's UI

Among the many differences between DEX and CEX listed in the table 1, composability is a defining feature of DEX, which it inherits from the “superclass” DeFi.



The DeFi world



The CeFi world

1.4 What we need for derivative DEX?

Now we summarize the attributes that are essential for a decentralized exchanging mechanism of derivatives:

- Real DeFi: the core of the exchanging mechanism should becompletely on-chain;
- Real derivative: it should enable the users precisely and capital-efficiently get the risk exposures they want;
- Composability: the key component should be tokenized so it can be imported into other DeFi projects like lego blocks;
- Openness: the solution should adopt general tokens (e.g. stablecoins) as base token rather than using some “in-house chips”.

Additionally, while not a defining attribute, simplicity is also critical for a solution to work. A decentralized protocol of derivative should be as easy to use as spot exchange, e.g. Uniswap.

2 Deri Protocol

2.1 What is Deri?

Deri is short for derivative. As indicated by the name, Deri protocol facilitates people to trade derivatives. Essentially, Deri protocol is a decentralized protocol allowing users to exchange risk exposures **precisely and capital-efficiently**. As THE SOLUTION to decentralized derivative exchange, Deri protocol is designed with all the defining features of DeFi and financial derivatives in its nature.

Real DeFi: Deri Protocol is a group of smart contracts deployed on ethereum blockchain, where the exchange of risk exposures takes place completely on-chain.

Real derivative: The PnL's of the users' positions are calculated with mark price updated by oracle, which ensures the precision; positions are maintained by margin, which provides built-in leverage.

Composability: Positions are tokenized as non-fungible tokens (NFT), which can be held, transferred or imported into any other DeFi projects for their own financial purposes (as blocks in their own "lego game").

Openness: anybody can launch a pool with any base token (but usually with stablecoin, e.g. USDT or DAI). That is, the protocol does not enforce any specific "in-house chip".

Simplicity: Deri protocol adopts an extremely simple trading process.

2.2 The Greeks

In finance, the different kinds of risk exposures are denoted as a series of Greek letters (the Greeks). From a financial perspective, Deri is a decentralized protocol to exchange the “Greeks”, e.g. delta, gamma, vega. This is achieved by interacting with the liquidity pools. For the time being, Deri protocol provides liquidity pools of perpetual contracts, with which people can exchange Detla. Going forward, other types of pools will be launched to enable people to exchange other Greeks, e.g. Vega.

Among the Greeks, Delta, Δ, measures the rate of change of the derivative's value V with respect to changes in the underlying's price S.

$$\Delta = \frac{\partial V}{\partial S}$$

Most of the time when people trade/hold derivatives, they are really to acquire Delta, in order to increase/decrease their risk exposure to the underlying’s price change to an intended level. In less common scenarios, people trade/hold derivatives for other Greeks, such as Vega.

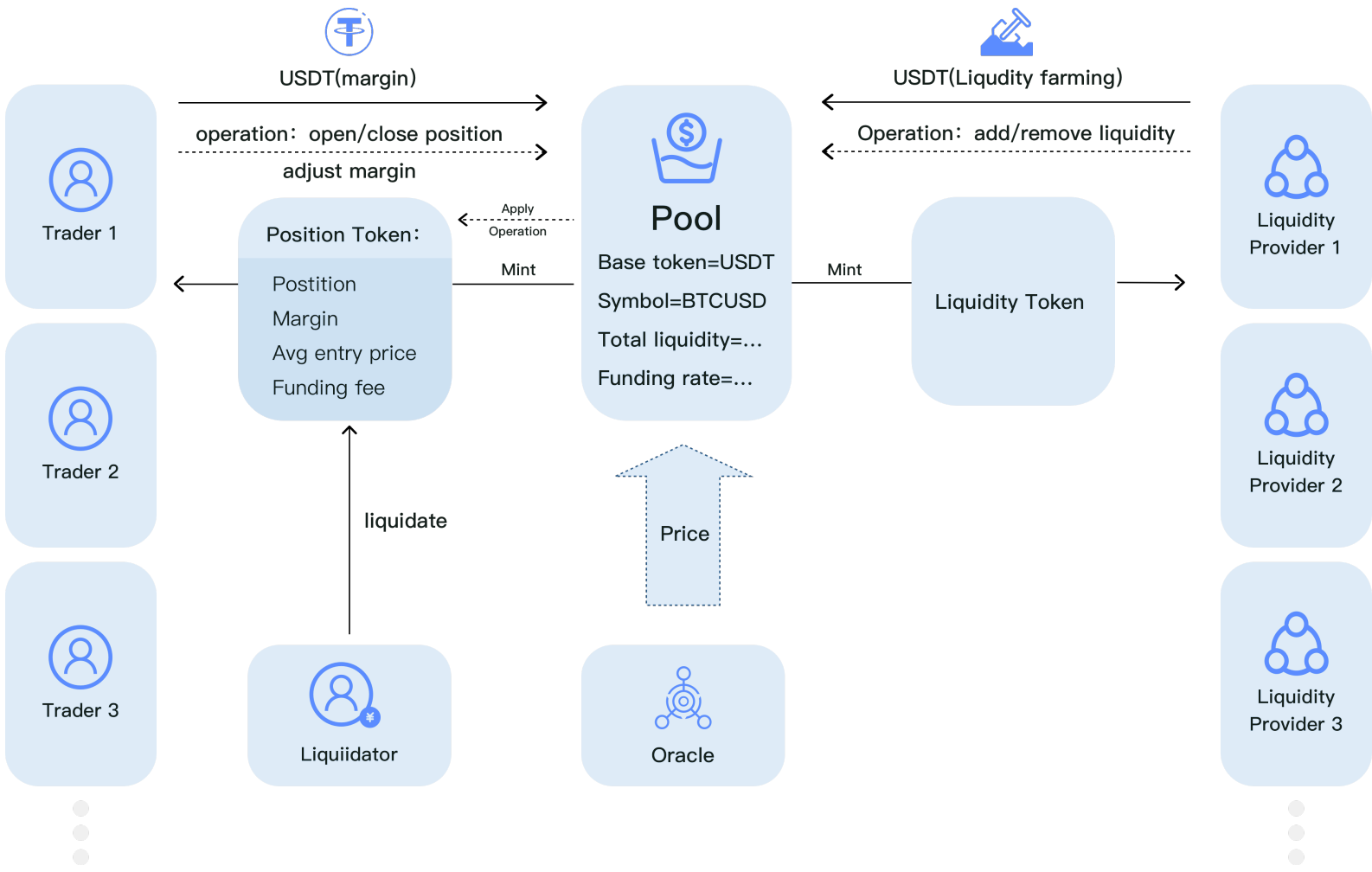
Derivatives' primary purpose is to let people **acquire the correct delta at minimal cost**. The minimal cost (optimal capital efficiency) is achieved by leverage. A 10 times leverage enables one to obtain an exposure of 1 million USD with only 100K USD capital being held as margin. Therefore, an derivative without a leverage greater than 1 is almost useless, because one would rather hold the underlyer itself instead of the derivative.

2.3 How Deri Protocol works?

2.3.1 Fundamental

The mechanism of Deri protocol is somewhat like that of Uniswap, where the pools play the role of traders' counterparties. In the case of Uniswap, where spot exchange takes place, each pool holds a pair of tokens and is ready to exchange one for the other upon traders' requests. Whereas in the case of Deri, the pools play the role of the counterparties of derivatives. In financial industry, such a role in derivative trading business is called dealer. Typical derivative dealers are the derivative trading desks in the investment banks. Essentially, the liquidity pools of Deri protocol are the "derivative trading desks" in the DeFi world. They enter derivative contracts as counterparties of their clients. That is, they take the opposite positions against their clients' trading positions. In traditional financial industry, the trading desks hedge their net positions to manage their market risk. In the case of Deri protocol, the pools carry out such hedges in a decentralized way, which will be explained later.

The architecture chart below illustrates how the different characters interact with each other under Deri protocol. The liquidity pool works as liquidity medium and makes base token transactions with traders and liquidity providers. Position tokens and liquidity tokens are minted to represent the traders' positions and liquidity providers' liquidity shares.



2.3.2 Trading process

With Deri protocol, users trade with an Uniswap-style pool as the counterparty in simple steps:

1.Go to the website, connect to wallet (e.g. MetaMask)

2.Choose the underlyer to trade (i.e. choose the pool)

3.Specify the direction (long/short), volume and leverage (margin to post)

4.Place order and confirm on the wallet

If the margin requirement is met, the pool will process the order and mint a Position token for the trader.

2.3.3 Position token

Upon processing an order, the pool will mint a Position token (an NFT) to record the following parameters of the position and send this Position token to the trader's address.

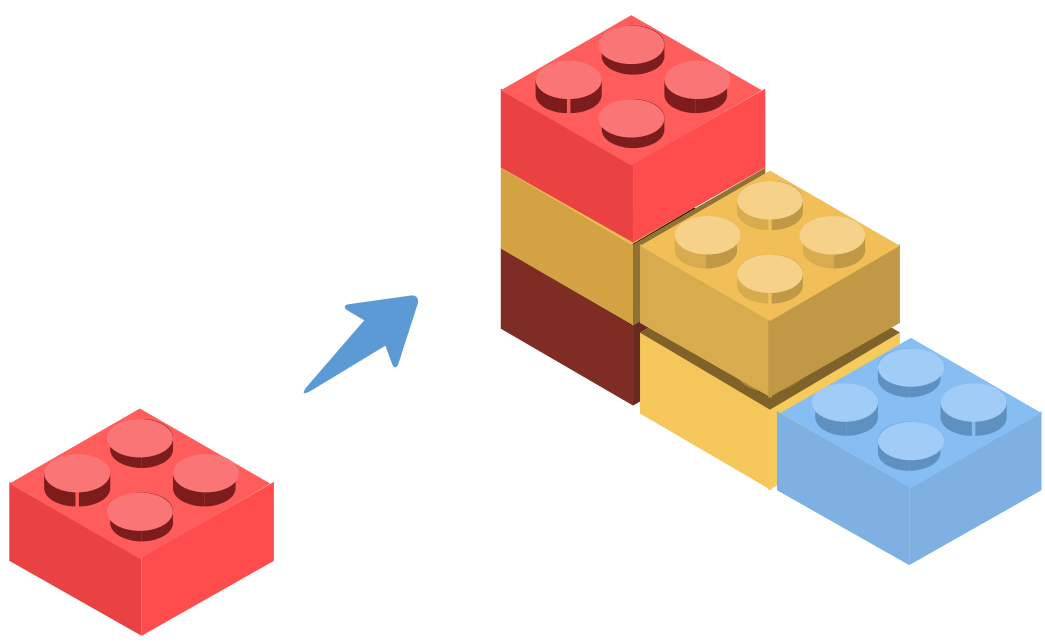
- direction & volume
- entry price
- margin held

The trader can come back to the pool to carry out the following operations to the position token:

- Close the position: the pool will calculate the PnL and the fees, refund the base token (if position value > 0) to the position holder's address and burn the position token
- Adjust position: increase or decrease
- Adjust margin: deposit more or withdraw

The position token can be used in any scenarios where such risk exposure is needed.

For example, when someone holds a portfolio of tokens and would like to adjust its risk exposure to some specific underlyer, he/she can add such a position token to the portfolio.



Deri Position A DeFi porfolio

2.3.4 Mark price and PnL

For any liquidity pool, its underlyer's mark price is updated by an "oracle". This could be either an off-chain oracle server or an on-chain oracle smart contract (see 2.4 for the more details). Every time some operation takes place (e.g. a trader operates on the position or a liquidity provider adds/removes liquidity), the pool will obtain the latest price from the oracle and use it as the mark price to update the position or calculate liquidity share values.

2.3.5 Funding fee

Per the Deri protocol, each pool charges the majority-side positions funding fees and reimburse the minority-side positions. This is to balance the long and short sides of the positions.

The funding rate is calculated by

$$\text{FundingRate} = \frac{r \times (L - S) \times \text{CurrentMarkPrice} \times \text{ContractSize}}{\text{PoolLiquidity}}$$

From a perspective of financial market, funding fee is essentially the cost of liquidity to executing a trade. In a traditional orderbook-based exchange ,such cost is paid in the forms of fixed liquidity taker fees and variable market impact cost (depending on the orderbook depth). Deri protocol adopts a pool-based paradigm of trading, where the majority-side positions (the liquidity takers) pay the minority-side positions (the liquidity makers) the funding fee to compensate for the liquidity they consume. Note that the funding rate is inversely proportional to the pool's total liquidity. That is, the more liquidity the pool contains, the less funding fee the majority-side positions will be charged. This is consistent with that in the traditional orderbook-based exchanges: the better liquidity, the lesser trading cost.

2.3.6 Position liquidation

Determined by the entry price, maintenance margin requirement, the margin posted and funding fee applied, every position token has a liquidating price.

A position token can be liquidated when the mark price breaches its liquidating price. The liquidation is triggered by the liquidating function of the token. When the liquidating condition is satisfied, this function can be called by anybody (as a liquidator). The liquidator pays the gas and share part of the position’s remaining margin as award.

When liquidation is triggered, a position's remaining margin will be distributed to the liquidator and the pool. The position token will be burned and exist no more.

2.4 Oracle

The pools of Deri protocol adopt two types of oracles: off-chain oracle server or on-chain oracle smart contract.

2.4.1 Off-chain Oracle server

An oracle server reads prices from one or several sources (compiles the multiple sources if more than one) and feeds the (compiled) prices into the associated pool(s). This is executed as follows:

1. every time when some operation takes place (a trader operates on the position or a liquidity provider adds/removes liquidity),

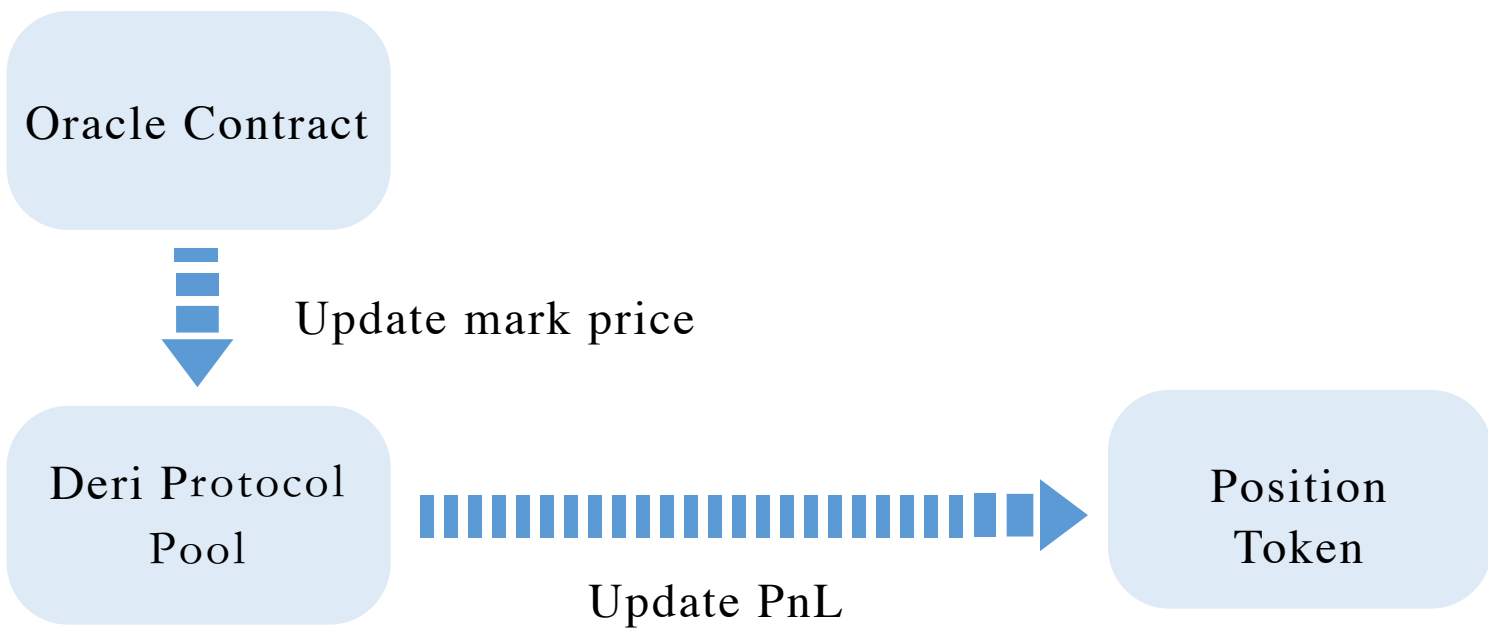
2. the interface query the oracle server regarding the price of the pool's underlyer

3. the oracle send the latest price together with its timestamp and the oracle's signature

4. the pool receives and accepts the price, then proceeds to the following steps.

2.4.2 On-chain Oracle contract

When an oracle contract is adopted, the procedures are similar to that of the off-chain oracle server set-up. The underlyer's mark price is updated as follows:



Please note that, no matter the pool adopts an off-chain oracle server or an on-chain oracle smart contract, the mechanism of obtaining mark price is decoupled into the oracle's responsibility. The oracle can adopt whatever source and method it deems to be reasonable and suitable for the underlying. Therefore the underlyer universe that Deri Protocol can deal with is defined by the range of objects that oracle contracts can correctly handle the marking of. Theoretically, this covers any financial prices/indices, crypto or traditional.

As an simple and straightforward example of on-chain oracle contract, an oracle can read the price of BTCUSDT from Uniswap so that a derivative with BTCUSDT as underlyer can be a traded. Please note that using Uniswap as oracle should adopt some special techniques to prove from price manipulation, e.g. flashloan attacks. Uniswap has some detailed documents for this topic.

As another example, an oracle server can read SP500 index from exchanges, brokers or some oracle services, e.g. ChainLink. This provides users of Deri protocol access to risk exposures in traditional finance.

2.5 Liquidity Farming

Pools play the role of counterparties to the traders. Liquidity providers (LPs) provide liquidity (base token) to the pools so that the pools will have adequate liquidity (small funding rate).

In return, LPs gain two parts of yields: base token profit (possibly) and DERI token award:

- **Base token profit**:this comes from transaction fee, position remaining value at liquidation, funding fee, possible traders' loss;
- **DERI award:**DERI tokens will be awarded to the liquidity providers additional to the base token profit.

Please note that the liquidity farming for Deri protocol is not riskless. There is a possibility of **impermanent loss**: LPs face market risk - the possibility of losing base token due to the net position it holds. Nevertheless, this is protected by the arbitragers. The following sector explains this in details.

2.6 Arbitrage

The arbitragers are key players of the Deri Protocol ecosystem.

Arbitragers are induced by funding rate to always be on the minority side. The arbitrage is implemented by holding a position on the minority side of the pool to earn the funding fee while hedging this position somewhere else (e.g. with a spot position or on some CEX of derivative). In reality, there will be more than one arbitragers 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. The arbitragers are motivated by profit but meanwhile help the traders and liquidity providers:

- The arbitragers reduce the funding rate so that the regular traders on the majority side do not pay too much to hold their positions.

- The arbitragers are always to reduce long-short imbalance (all liquidity providers' total net position) and thus shelter the liquidity providers from market risk.

3 Governance and protocol token

3.1 Governance

There are two levels of governance: the governance of a single pool and that of the protocol.

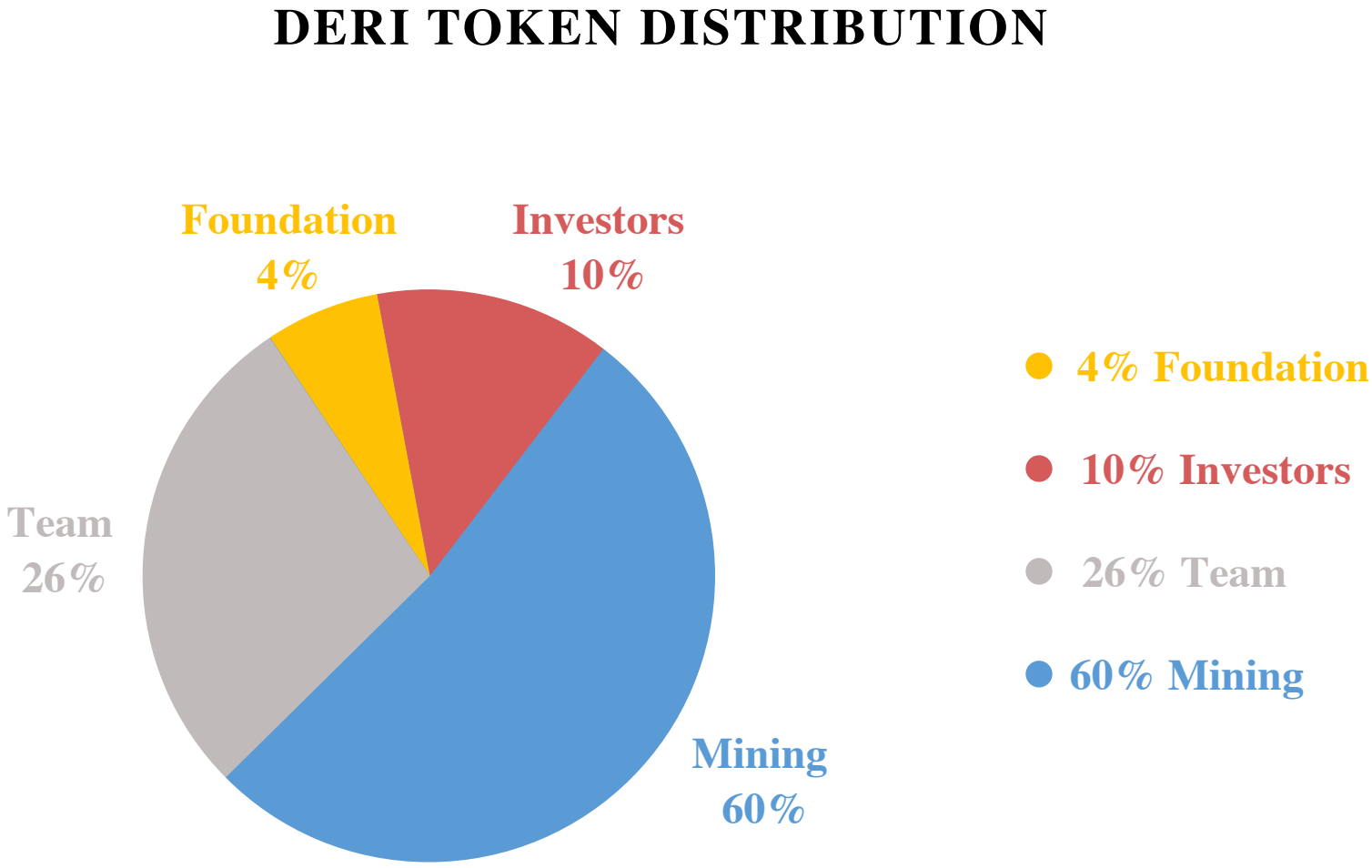
At the pool level, each pool is a self-managed group of smart contracts. That is, pools are autonomous themselves.

The Deri protocol is maintained and updated by the development team in the launching stage. Once having proven product-market fit for highly decentralized financial infrastructure, the governance will be transferred to a community-based governance system, based on the protocol token DERI.

3.2 DERI: the Deri Protocol token

The Deri Protocol token, DERI, will be rolled out to enable a shared community ownership and a prosperous, diverse, and dedicated governance system, which will actively guide the protocol towards the ultimate decentralized financial world. Within the ecosystem of Deri protocol, the token will be used as governance token as well as fee token.

The DERI token will have a total supply of 1 billion, 60% of which will be minted through liquidity mining and the rest will be awarded to the team, the investors and the foundation. The non-mining part will be locked in a vesting plan and released linearly in 2 years. The chart below illustrates how the 1 billion DERI will be distributed among mining and non-mining allocations.



4 Summary

Deri protocol provides an on-chain solution for users to gain specific risk exposures precisely and capital-efficiently.

With Deri protocol, the targeted risk exposures are tokenized as position non-fungible tokens. Such position tokens' values are updated by their associated pools to exactly follow the underlying price changes.

The position tokens minted with Deri protocol can be imported into other DeFi projects to serve their own financial purposes.

Reference

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

[2] How To DeFi: https://landing.coingecko.com/how-to-defi/

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

[4] Greeks (finance): https://en.wikipedia.org/wiki/Greeks_(finance)