Umbrella Protocol

by YAM

Lite Paper v0.1

Table of Contents

Introduction

Throughout DeFi's history, smart contract exploits have been a constant threat to the ecosystem and its users. From low level language exploits like the DAO hack to economic attacks resulting from flash loans, the risk vectors are numerous and unforgiving. It's become clear that audits are in no way a guarantee, and risk management solutions must be created.

We believe these solutions should also be DeFi native, leveraging Ethereum's unique capabilities, operating as open and permissionless, and balancing decentralized governance and immutability.

The Umbrella Protection Protocol is designed with these factors in mind, featuring perpetual ERC20 streaming coverage, immutable coverage pools, and a permissionless pool creation process that allows for customization and iteration over time.

Overview

The Umbrella Protection Protocol is designed to enable Protection Providers to earn premium fees in return for staking funds to be paid out in the event of an exploit to Protection Seekers, who stake and pay a funding rate to earn protection in such an event.

There are two pool types in the protocol, one accessed by Protection Providers and one by Protection Seekers. The first pool type are the MetaPools, which are funded by Protection Providers and provide coverage on the second pool type, the Coverage Pools, which are accessed individually by the Protection Seekers.

Each MetaPool is made up of Coverage Pools, which provide protection on specific protocols or contracts. An example of a MetaPool could be "Lending Protocols" while the Coverage Pools that Seekers could access would be "Compound", "Aave", "Cream." If any of those protocols experienced an exploit deemed valid by the arbiter of the MetaPool, a portion of the Provider's stake would be used in a payout to Seekers who had staked for coverage in the affected protocol's Coverage Pool.

Pool Creation and Functionality

Anyone is able to create and submit a MetaPool for approval by the arbiter of their choice. These pools are immutable once created, and if updates are desired, a new pool will need to be created. When creating a MetaPool, there are a number of inputs to consider:

Coverage Pools - A list of protocols or contracts that will be covered by the MetaPool. Protection Seekers will stake for coverage in these pools individually, while the Protection Providers are willing to stake protection in the aggregate.

Arbiter - The address of the chosen arbiter for the MetaPool, which will determine the validity of claims.

Protection Description - A description of the coverage rules the creator request the arbiter abides by. The arbiter has final say in the interpretation of this description.

Arbiter Rate - The arbiter rate is the percentage of all premiums that are allocated to the arbiter in return for their services.

Creator Rate - The creator rate is the percentage of all premiums that are allocated to the creator of the MetaPool.

Funding Rate - The funding rate function used to determine what rate Protection Seekers pay on their protection stake.

Bonding Curve - The bonding curve function is used to determine how many protection tokens are minted or burned during staking and withdrawal of Protection Seekers.

Provider Withdrawal Period - The amount of time a Protection Provider's withdrawal is held to prevent a bank run in the event of an exploit.

Seeker Purchase Period - The amount of time before a Protection Seeker receives coverage to prevent excess minting in the event of an exploit.

Protection Asset - The protection asset is the asset both protection buyers and seekers deposit into the contracts.

MetaPools and their coverage pools act as a self-contained unit, meaning a "Compound" Coverage Pool in MetaPool A and a "Compound" Coverage Pool in MetaPool B are completely unrelated to one another in terms of pricing, utillization, and claims processing.

Protection Providing

Protection providers receive cashflows in the form of premiums in return for staking capital in the protection MetaPools, as well as an ERC20 representation of their position. The protection MetaPools cover multiple contract pools, and if any underlying contract pool has a valid exploit, a portion of the seller's stake is paid out to the affected contract pool's protection seekers.

In return for this risk, protection providers receive premiums via a funding rate determined by the utilization rates of each contract pool. The funding rate function is set at MetaPool creation.

Providers are able to withdraw their stake at any time, but the withdrawal is subject to a holding period specified at MetaPool creation. Utilization cannot exceed 100%, so Providers may only withdraw up to that point.

Protection Seeking

Protection seekers receive protection in return for staking capital in the contract pools, where a funding rate is applied to pay for the protection. Protection seekers receive perpetual ERC20 representations of their staked deposits, which operate similarly to cTokens, decreasing the balanceOfUnderlying as the funding rate is applied to the staked deposits. The amount of protection corresponds to the amount staked, meaning the amount of coverage decays over time.

When depositing funds for protection, there is a delay in receiving coverage to ensure users do not mint excess coverage in the event of an exploit.

Claims Process

In the event of an exploit, anyone can submit a claim to the arbiter on behalf of a Coverage Pool. If a claim is ruled to be invalid, then the system continues unaffected. If a claim is determined to be a valid exploit according to the agreed upon "protection description", then a payout is performed.

The amount of a payout is equivalent to the amount staked in the affected Coverage Pool, plus any unutilized funds in the MetaPool. As an example, if a MetaPool has 1000 DAI and 3 pools each with 100 DAI, and a covered protocol is hacked, the payout would be (Amount Staked) + (Total MetaPool Funds - Total Coverage Pool Staked) = 100 DAI + 700 DAI = 800 DAI. If there were 6 pools, each with 100 DAI, the calculation would be 100 DAI + 400 DAI = 500 DAI. This allows each Coverage Pool to always return at least 100% on staked capital in the event of an exploit, while also allowing Protection Providers to calculate their maximum drawdown in the event of a single hack.

A MetaPool will continue to function after a valid claim, with a new Coverage Pool for the affected protocol being automatically created when a claim is deemed valid.

Pool Dissolution

If an arbiter no longer wishes to perform its arbitration duties on a pool, it may choose to dissolve the pool, setting funding rate to zero, allowing immediate withdrawals by all parties, and disabling additional deposits.