Umbrella Protocol

by YAM

Lite Paper v0.2

Updated 12/09/2020

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 NFT tokenized protection, 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 purchase coverage at a specific rate for a custom duration.

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 purchased 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. (Max 16)
>
> ***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.
>
> ***Interest Rate*** - The interest rate function used to determine what rate Protection Seekers pay for their protection.
>
> ***Rollover Rate –*** The percentage of premiums that are automatically deposited as additional coverage provided in a provider's account
>
> ***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.
>
> ***Max Protection Duration*** – The maximum duration a protection seeker can obtain coverage.
>
> ***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. 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 determined by the utilization rates of each contract pool. The pricing of these premiums is set according to the interest rate function of the MetaPool. Premiums for coverage are received when sweep() is called at the end of seeker's coverage period.

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 by purchasing coverage from the contract pools. Protection seekers receive an NFT representing their protection amount and duration of protection. Cost is determined by utilization levels according to the interest rate function of the MetaPool.

Claims Process

In the event of an exploit, it is up to the arbiter to initiate a payout. This is done via an on-chain governance vote. The arbiter submits a blocktime associated with the exploit validation, allowing all active coverage covering that blocktime to receive its specified payout. .

Pool Dissolution

If an arbiter no longer wishes to perform its arbitration duties on a pool, it may choose to dissolve the pool. In this case, existing protection will be carried out but no new providers or seekers may enter the pools.