保护伞协议

（Umbrella Protocol）

YAM出品

简明文档 v0.1

简介

在DeFi的发展历程中，恶意利用智能合约漏洞的行为，无论是对整个生态还是用户来说都是一个持续存在的风险。从利用底层语言漏洞进行DAO攻击，再到借用闪电贷发起的金融攻击，其中的风险向量众多且令各方都无法承受。很显然，仅执行协议或合约的代码审计不是万能的保障，建立一个风险管理解决方案是绝对必要的补充。

我们也相信，这些相关的保护性解决方案应该是根植于DeFi生态，同时可以有效利用以太坊的特性的，譬如开放的运行环境并且无需许可，可平衡的去中心化治理同时无法篡改。

我们因此开发了雨伞保护协议（The Umbrella Protection Protocol），又名保护伞协议，并在协议的设计上充分考虑了以上因素。恒定的产品险池，无需许可的定制化创建方式，无期ERC20代币凭证，随时间推移迭代更新，这些都将作为保护伞协议的特色而存在。

综述

雨伞保护协议旨在使投保人和承保人双方均可以受益。投保人在存入一定数量的投保金额并支付保费后，可以在投资产品遭受漏洞攻击事件时，获得赔付以降低风险；而承保人则在投入承保资金并承担风险后，可以获得相应的保费收益。

保护伞协议中设有两种不同的类型池：第一种是由承保人注入承保资金并设立的**承保池**，也叫**元池（MetaPools）**，承保人具有元池的访问权限。第二种是针对不同产品（协议或合约）提供保险服务，并由投保人将一定数量的投保金额存入其中的**投保池**，又称**险池（Coverage Pools）**，投保人具有险池的访问权限。同时，元池会为险池提供赔付保障支持。

每个元池会同时覆盖多个险池，并为其涵盖的多个险池提供赔付资金保障。例如，一个元池用于为“借贷协议”产品提供保障，它就可以同时覆盖并保障多个为借贷产品提供保险服务的险池。如Compoud险池、Aave险池和Cream险池。如果其中任何一个产品（协议或合约）遭遇了漏洞攻击事件，并被仲裁人裁定为有效，那么就会使用一定比例的该元池承保资金，作为赔付资金支付给那些参与并投保了受影响产品的投保人。

类型池的设立和功用

任何人都可以创建和提交一个**元池**，即**承保池**，并通过自己选择的仲裁人进行理赔审核。元池一旦被创建便不可再进行修改，任何更新需求，都必须重新创建一个新的元池作为替代。因此，创建元池时，需要考虑诸多的设定参数：

险池（Coverage Pools）
即**投保池**，每个元池都会覆盖一系列的产品（协议或合约）险池，投保人会根据投保标的将一定数量的投保金额存入相应的产品险池。另一方面，承保人则会在总承保资金额度范围内，为这些险池提供赔付保障支持。

仲裁人（Arbiter）
被选取作为元池仲裁人的以太坊地址所有者，将负责确认索赔申请是否真实有效。

保障说明（Protection Description）
元池创建人规定仲裁人所要履行的保障责任说明，仲裁人拥有此说明解释的最终决定权。

仲裁费率（Arbiter Rate）
保费中用于支付给仲裁人提供仲裁服务的费用，仲裁费与保费总额的比值即为仲裁费率。

创建人费率（Creator Rate）
保费中分配给元池创建人的费用，此费用与保费总额的比值即为创建人费率。

资金费率（Funding Rate）
资金费率函数用来确定投保人支付保费的费率水平。

绑定曲线（Bonding Curve）
绑定曲线函数用于确定投保人存入和取回其投保金额时，所需铸造或销毁的保险代币数量。

承保人撤回锁定期（Provider Withdrawal Period）
承保人撤回锁定期用于预防漏洞攻击事件出现时的挤兑行为，是承保人申请撤回承保资金到收到款项所需经历的时间周期。

投保人购买生效期（Seeker Purchase Period）
投保人购买生效期用于预防漏洞攻击事件出现时的超额铸造行为，是从投保人购买保险到该保险生效所需经历的时间周期。

保护资产（Protection Asset）
保护资产是指投保人存放于其它产品（协议或合约）中的资产，因规避风险需要而对其进行投保。

每个元池（承保池）和其所涵盖的险池（投保池）都会构成一个自给自足的独立单元。也就是说，【元池A】中的【Compound险池】与【元池B】中的【Compound险池】，在投保价格、赔付比率和索赔处理等方面，都是完全独立且没有任何关联的。

承保

承保人在元池中投入的承保资金将会获得保费现金流回报，同时，会生成一种ERC20代币作为承保人投入资产情况的证明。该元池覆盖的多个不同产品（协议或合约）险池中，任何一个产品遭遇漏洞攻击事件并出险，元池都会分配一定份额的承保资金用于赔付并支付给受影响产品险池内的投保人。

承保人会以收取保费的形式作为投入资金并承担风险的回报，收取保费的资金费率由每个产品险池的承保金使用率来确定，而资金费率函数是随同元池创建一并设定的。

承保人可以随时撤回其承保资金，撤回操作必须满足该元池创建时所设定的撤回锁定期限。因为元池内的承保资金使用率不会超过100%，因此承保人撤回的承保资金数量，取决于撤回时该元池内承保资金的使用率。

投保

投保人在产品（协议或合约）险池内存入一定数量的投保金额以换取保险服务，并按照资金费率支付保费。同时，投保人会获得一种无期ERC20代币作为其投保情况的证明。在操作上，这种无期ERC20代币与Compound项目的质押凭证（cToken）相类似，标的资产余额（balanceOfUnderlying）会随保费的支付累计而逐渐递减。因可供赔付的金额应与存入的投保金额相一致，故投保人可获得的赔付金额也会随时间推移逐渐衰减。

当投保人存入一定数量的投保金额换取保险服务时，需要经过一段延迟期后，该保险方可生效。这样做的目的是确保出现漏洞攻击事件时，投保人不会借机进行超额铸造以不道德的方式进行牟利。

索赔处理

任何遭受漏洞攻击事件的投保人都可以代表相关险池，向仲裁人提交索赔申请。依据已获同意的保障说明，如果该索赔申请被裁定为无效，则雨伞保护协议的运行不会做出任何变动；而一旦该索赔申请被认定为有效，则会进入赔付处理程序。

赔付金额等于受影响险池内的投保金额与元池内未使用承保资金的总和。例如，某个元池目前存有1000枚DAI，同时此元池所覆盖的3个险池内各存有100枚DAI。此时，其中一个险池内的产品协议遭遇了漏洞攻击，则该险池的相应赔付金额应该是800枚DAI。计算方法如下：

受影响险池投保金额 + (元池承保资金总额 − 所有险池投保资金总额) = 100DAI + (1000DAI − 300DAI) = 800DAI。

同样的算法，如果该元池覆盖6个险池，且每个险池内各存有100枚DAI，某一个险池出险时的赔付金额则变为500枚DAI。这样便可以保证每个险池在出险时都可以获得不低于投保金额的赔付额度。同时，承保人也可以计算出赔付后的最大资金回撤。

每当索赔申请被裁定为有效时，相关受影响的产品（协议或合约）险池都会被自动重新建立，元池则会在赔付处理完成后继续保持运作。

解散类型池

如果仲裁人无意继续履行仲裁职务，可以选择解散元池。此时，资金费率设置为零，并允许参与各方即时撤回款项，同时禁止款项存入。