Chameleon Protocol 变色龙协议

新一代基于匿名隐私加密算法的多链 USDT 混币协议

一、产品介绍

Chameleon Protocol 变色龙协议是非常强大的匿名混币协议，支持多链 USDT 混币转移技术，让链上资产转移同样拥有隐私，并且不可追踪。平台早期支持的 USDT 的主链包括 ETH、TRON、BSC 等。Chameleon Protocol 完全基于智能合约和加密算法，从而保证用户的资产处于完全匿名隐私和安全的状态。Chameleon Protocol 有着如下的优势：

——影子匿名协议保证隐私
——加密算法保证资产安全
——流动性激励多资产规模
——融合多链 USDT 生态
——极短时间快速兑换

二、匿名智能合约实现分析

Chameleon Protocol 的智能合约设计是可组合性的，可以在技术上实现完全匿名。实现的原理如下所述。

用户存款流程如下：

取款地址：共 2 个，以加密的形式传给智能合约。

地址规则:只允许存款时约定的 2 个地址进行提币操作,第一次提币必须提取存款的本金(扣除手续费后的本金），第 2 次提款可以提取产生的利息部分，提取本金后停止计算利息。提取本金地址只用于提取本金，提取利息地址只用于提取利息。

质押存款到智能合约：用户质押存款与智能合约交互后，立刻扣除入池手续费(现默认设置的是 1%)，存款以 24 小时为一个周期，24 小时以内，不产生利息，24 小时以后，往后推算存满一个周期（即 24 小时）产生周期利息（利息也称为收益）。利率随机生成，利率算法：（取随机数%9+2）/100，其中 100 可以变动，会根据池子预计市场情况进行调节。举例，如果用户在池子里存款时间为 50 小时，那么计算利息的方式为：（50-24）/24=1 那么将计算一个周期的利息。

三、加密算法解析

Chameleon Protocol 由多个加密算法来进行平台资产的协议加密，保证用户的资产端的安全性。下面我们根据用户存款和用户取款来分别说明。

用户存款：用户存款时将传入三个加密后的取款 hash（GetcapitalHash）、GetinterestHash 以及 Callhash，并且保存在区块链中。取款 hash 由算法：sha256(sha256(address,privatekey),publickey,address)加密而来，最终加密形态为二层加密，sha256 加密为非对称加密，不可逆转。其中 privatekey 为用户前端生成的随机 64 位字符串，每一次生成的字符串都是随机并且唯一的。只有用户才掌握着取款的私钥（privatekey）。

用户取款：用户取款时把 sha256(address,privatekey) 加密以后的一层加密结果传给合约，合约拿到这个加密值以后，按照 sha256(hash 一层加密参数值,publickey,address)进行再次加密，如果加密结果与存款时保存的二层加密 Hash 的吻合，即验证通过。取款 hash 用完一次以后，就作废，查询 hash（即 callhash）可以重复使用。

四、平台质押奖励

用户在平台质押后，给予日收益 0.2%-1.1%的随机利息的奖励（奖励随着可能会随着项目升级而不断变动,质押需要超过一个质押周期以后才会计算利息),并且在项目上线初期有空投代币的奖励。

用户质押以后，默认是无法查看利率的，因为利率是个随机盲盒，如果用户需要查看利率，需要购买“利率窥视卡”，支付相应的代币以后，即可查看当前的利率。当用户觉得当前费率过低的时候，用户可以购买“利率重置卡”进行利率重置，但是，重置利率依然是随机盲盒，每个订单最多重置三次，重复越多次需要支付的代币数量越多。

五、Chameleon 影子匿名协议

Chameleon Protocol 可以通过影子匿名协议实现代币的匿名转移。实现的原理如下：

用户从 A 地址质押进来以后，可以允许从 B 地址进行提币，质押地址与提币地址无关联性。用户质押的金额是固定选择的金额（如 100USDT、1000USDT 如此类推），提取本金的金额也是扣除固定的费率的手续费以后的金额，质押与存币的每一个等级的金额都是一致的，可以起到混淆作用，即使查看链上合约交互记录，也无法知道，某地址的币最后是转到了哪个地址中。

利息（即收益）的产生：我们巧妙的设计了随机盲盒利率，并且把产生利息周期设置为 24 小时，也就是 24 小时以内可能会有很多订单起到混淆作用，并且因为利率的随机性，查看链上的提取利息记录，也无法猜测到到底是哪个地址产生的利息。并且利息提取地址也是单独的，脱离掉了与原存币地址的关联性。

我们在加密算法中，引入了独特的两层非对称算法，在进行提币的时候，提交给区块的信息是经过了非对称加密，同时，加密的私钥是掌握在用户自己的手中，且加密私钥是唯一的，这就有效的阻断了通过分析区块的数据进行猜解的可能性，保护了用户的数据隐私安全。

六、通证经济

Chameleon Protocol治理通证为CLP，发行总量 1 亿枚。CLP有着多个方面的权益：
——治理权益，通证持有者可进行参与平台治理
——收益权益，用户参与平台的存款/质押等可以获得平台通证的奖励

CLP通证80%用于挖矿奖励；10%用于技术激励；5%用于营销/运营等；5%用于生态合作。
挖矿激励 80% 8000万
Chameleon Protocol的挖矿方式分为流动性挖矿，交易挖矿，单币挖矿。三种挖矿产出的比例会在平台正式上线时说明。
技术激励 10% 1000万
我们是分布式的技术团队，技术团队来自于全球多个国家和地区。技术团队激励在平台上线后按12个月智能合约每日线性解锁。
营销/运营 5% 500万
该5%用于初始流动池的建立以及市场营销、运营、空投等。
生态合作 5% 500万
该5%用于生态合作，包括但不限于技术协议层合作对接、机构合作对接等。早期处于锁定状态，当进行生态合作时按比例解锁。