

1 分红

可分红资金池将包含万分之 X 的一部分，可用于分红分配。对于可分红资金池中的总金额 T 以及当前 DARC 协议内各个代币级别的分红权重之和，我们可以按照以下方式确定每个分红单位的分红金额：

$$u = \frac{XT}{10000W}$$

这里， u 代表每个分红单位的分红金额， T 是可分红资金池中的总金额， W 代表当前 DARC 协议内所有可分红代币跨不同代币级别的分红权重之和。

对于每个用户，假设用户 i 持有的各个代币级别的分红权重之和为 D_i ，那么用户 i 在本轮中可以接收的总分红金额 U_i 为：

$$U_i = \frac{D_i}{10000}u$$

对于 DARC 协议，可以采用三种分红分配方法：

基于交易的分红分配：第一种方法是基于可分红交易的数量分配分红。这通过设置分红交易周期计数器， N ，到一个合理的值来实现。一旦接收到至少 N 个可分红交易，指令 `OFFER_DIVIDENDS` 就变得可执行。执行后，可分红资金池和可分红交易周期计数器被重置为零，开始新的计数。这个过程重复，等待下一个 N 交易和随后的分红分配操作。

基于时间的分红分配：第二种方法是基于时间分配分红。将 N 设置为 1，可以引入一个额外的插件，允许在整个 DARC 实例中，`OFFER_DIVIDENDS` 被调用的时间不少于上一次调用后的 S 秒。以这种方式，分红可以每 2 周、4 周、3 个月、6 个月或 1 年安排一次。这种方法更接近传统公司的分红。

基于资金池的分红分配：第三种方法涉及根据可分红资金池中的总金额分配分红。将 N 设置为 1，一个额外的插件使得一旦可分红资金池中的金额超过一个指定的阈值，就可以执行 `OFFER_DIVIDENDS`。根据这种设计，分红分配可以在获得 Y 个可分红本币代币后触发。

用户可以选择上述任何一种方法，或者设计插件来创建基于不同 DARC 组织结构和方法的替代、实用和合理的分红分配模式。

需要注意的是，对于每个收到的可分红交易执行 `OFFER_DIVIDENDS` 可能会导致大量的 Gas 费用浪费。这是由于潜在的时间复杂度为 $O(MNP)$ ，其中 M 代表代币级别的数量， N 是每个级别中的代币数量， P 是代币持有者的总数。因此，实现一个高效的分红分配机制以节省 Gas 费用是必要的。

此外，可分红资金池中的资金不会被 DARC 协议锁定在智能合约中。协议不保障现金分红，`OFFER_DIVIDENDS` 只执行计算，将每个代币持有者即将获得的分红存储在可提取的分红余额中。当操作者提取分红时，如果 DARC 协议没有足够数量的本币代币，这是不可能的。为了保护特定或所有代币持有者的分红权利，必须设计额外的插件。