Proof-of-Stake (PoS) Mining

（https://docs.decred.org/mining/proof-of-stake/）

综述

Decred 独特的 PoS 协议服务宗旨：

1. 允许股份持有人投票支持或反对对 Decred 区块链更改的提议。如果股份持有人赞成更改，则该链会硬分叉，而且新的特性会自动激活。关于投票的更多信息详见 Mainnet Voting Guide。
2. 为股份持有人提供一种机制来保持对不兼容的 PoW 矿工的检查。股份持有人可以投票使一个区块无效，即使他符合网络共识规则。这允许股份持有人抑制不利的挖矿行为，比如挖空的区块。
3. 允许 Decred 的长期持有人长时间锁定他们的资金来获得区块奖励产生的新币。

PoS 如何工作

为了参与到 PoS 挖矿，股份持有人锁定一部分 DCR 作为票（ticket）的回报。拥有的每张票都给股份持有人投一次票的权利。投票时，每张票会得到一个小小的奖励加上票的原始票价（Ticket Price）。每张票被随机选出来进行投票，获得一个 28 天的投票时间，但是可能最多需要 142 天，并有.5%的机会在被选中投票之前过期（过期返回原始票价但不含奖励）。每个挖出的区块必须包含 5 个投票（如果投票不足 5 个，矿工会遭到扣除奖励的惩罚）。每个挖到的区块也可以包含最多 20 张新票的购买。一张新票需要 256 个区块来使其成熟之后才能进入*票池（Tixket Pool）并有能力被用来投票。

有几个重要的变量你应该在分股的时候使自己熟悉。

每 144 个区块（~12 小时），股份难度算法就会计算一个新的票价（Ticket Price）来尝试保持票池（Ticket Pool）大小在在 40960 张票的目标池大小相近。这 144 个区块窗口被称为 StakeDiffWindowSize。

票价（Ticket Price）/股份难度（Stake Difficulty）就是你在一个 144 区块窗口必须付的票价。

票池（Ticket Pool）是在 Decred 网络中票的总数量。

票费用（Ticket Fee）（ticketfee）是必须包含在票的购买中来激励 PoW 矿工把那张票包含在一个新区块中要付的费率。票费用通常是指一次票购买交易的 DCR/kB 费率。因此，在一个更高的交易大小上，你应该付一个更高的绝对费用来结束。举个例子，单股（solo-staking）票购买大约 300 字节，这意味着一个.3 DCR/kB 的票费用会导致花费.1 DCR，当且仅当那张票被包含在一个区块中。

当票价在单个票窗口变得相对低的时候，你通常可以期望一个费用市场的形成，许多股份持有人尝试早窗口结束之前买票。当票价不是一个极其低并且有利可图的价格，0.001 DCR/kB 的默认票费用通常是足够高来包含到一个区块中的。

当一张票被调用投票的时候，有对那张票投票权利的钱包必须在线上。如果钱包没有在线投出它的票，那张票会被标记为 missed，并且你不会收到那张票的奖励。股份池（stakepool）被提出来作为那些不能 24/7 在线的投票钱包的一种解决方案。

股份池允许股份持有人生成给股份池投你的票的权利的票购买交易。它们代表你投票，通常需要一小部分费用来参与，这部分费用用来支付运行一个股份池所需的最少三个主机服务器的开销。这个费用被称作池费（Pool Fee），并且仅被从小的 PoS 奖励中取出。一张股份池的列表如下所示。

票生命周期

购买一张 PoS 的票是非常简单的（如下），但是在你买下它之后会发生声明？一张在主网（测试网使用不同参数）上的票会在其生命周期经过几个步骤：

1. 你使用 Decredition 或 dcrwallet 钱包购买一张票。每个单张票交易的总花费应该是票价+票费用（ticketfee）。
2. 你的票进入到 mempool。也就是你的票等待被 PoW 矿工挖的地方。每个区块只挖 20 张新票。
3. 被挖到区块里的票，具有更高票费用的交易就具有更高的优先级。注意，票费用是 DCR 每 KB 交易。一些普通的交易大小是 298 字节（一次单张票购买）和 539 字节（一次池票购买）。
4. A – 如果你的票被挖进一个区块中，它就会成为一张不成熟的票。这个状态持续 256 个区块（大约 20 个小时）。在此期间这张票不能进行投票。在此时，其票费用是不可退还的。

   B – 如果你的票没有被挖，票价和票费用都会退还到购买账户。
5. 在你的票成熟之后（256 个区块），它会进入票池并且具有了投票的资格。
6. 一张票的投票机会是基于泊松分布的，平均时间为 28 天。在 28 天之后一张票具有 50% 的可能已经投过票了。
7. 给定一个 40960 张票大小的票池，任何给定的票有 99.5%的机会在~142 天之内（大约 4.7 个月）投票。如果一张票在这个时间之后没有投票，它即过期。你会收到原始票价的退还金。
8. 如果投票钱包没有响应或者两个有效区块被发现彼此非常接近，一张票可能会错过其投票的调用。如果这种情况发生了，你会收到原始票价的退还金。
9. 当一张票已经投票、错过或是过期，资金（票价和补贴减去费用）会再次进入不成熟状态的 256 个区块，之后它们会被释放。如果一张票没错过或是过期，一个票撤回（revocation）交易就会由之后开发锁定票输出的钱包提交。注意：撤回只能为错过的票提交。你直到一张票过期了才能撤回它。