PoS 常见问题回答

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

1. Decred PoS 系统是什么？

PoS 系统允许 Decred 持有人在管理货币的时候拥有话语权。它旨在给用户在矿工旁边提供一个声音。为了参与进来，用户可以购买票，进入到乐透池。每个区块从 PoS 票池中选 5 张票。如果有至少三张票验证了之前挖出的区块，那么新挖到的区块就会被加到链上，并且 PoW 矿工和 POS 股东都会收到回报。如果 PoS 股东没有验证区块，那么 PoW 矿工不会收到回报，但是 PoS 股东会收到。这是为了激励 PoW 矿工根据 PoS 股东的意愿来挖矿。

该 PoS 系统有几个可以解决纯 PoW 系统可能遇到的问题的优势。比如说，因为 PoS 股东必须验证 PoW 矿工挖出的区块，所以 PoW 矿工无法自己决定来改变网络规则（一次 51% 攻击）。或者，当 Decred 链硬分叉旧的、更小的链，那么链就会因为没有被链的 PoS 组件验证而快速地死去。

该 PoS 系统允许的另外一个有趣的特性是可以在一个 agenda 上进行投票的能力。因为区块验证可以被看做是一次投票，通过给票添加而额外的投票位（votebit）组件，系统可以在一系列的区块上跟踪并计数投票。这些投票可以是关于任何事情的。

在 Decred PoS 系统上，任何持有 DCR 的人都可以通过购买票来参与进来。

2. 票是什么？

一张票就是你买的一个用来参加进 PoS 系统的代币。你可以通过 dcrctl 的 CLI 或者通过一个像 Decredition[1]这样的 GUI 来购买票。只要你购买了票，你就要使用你的 DCR 来支付当前票价以及票费用。当一张票被购买，它会暂时进入“mempool”。每个区块可以包含 20 张票，票是否被挖取决于它们的每千字节费用。由于在一个给定价格（2880），可以被挖进区块的票的数量是有限的，所以在挖票之间就会产生一种竞争。在这种情况，你可以提高你愿意付的费用来使你的票被挖到。一旦你的票被挖到，它就会从当前的“allmempool”移到“immature”票池。在 256 个区块（大约 20 小时）之后，它会成熟（mature）并进入到使其有资格被选来投票的活跃票池（live ticket pool）中。

3. 我需要一直保持连接到网络来参与 PoS 吗？

一个钱包需要 24/7 保持在线来投票，如果你的一张票被选取了的话。主要有两种方式来实现这点；一个你设置好并且保持一直在线的单股钱包，或者你可以使用一个股份池。一个股份池基本上就是一个运行你指派你的票的投票权给的钱包的一个社区，并且该池会为了获取 PoS 奖励的一小部分而代表你来投票。

很重要的是要注意你只是把投票权交给了股份池，而不是你实际的资金。一个股份池在任何时间都不会有权限获取你的资金。

4. “票价”是什么？

票价是由一个旨在保持票池大小的算法来决定的，票池大小就是 PoS 系统票池中票数量的总和，大概 40960 张左右。票价会根据票的需求量以及当前票池中票的数量上涨或下跌。

每 144 个区块算法调整一次票价。这由一个购买窗来调用。每个区块可以包含 20 个新买的票。这就意味着在每个购买窗，最多 2880 张票可以加入到该 PoS 系统的票池中。

票价总会被返还，无论你的票是否已经投票了、错过了还是过期了。

[1] https://docs.decred.org/getting-started/user-guides/using-decrediton/#tickets

5. 费用有什么？

该 PoS 系统使用两种费用，一个交易费（txfee）（也被称为“split”费）和一个票费用（ticketfee）。

Txfee 是你支付给网络来处理你购买票的交易的。该费用默认设置为一个较低的数量（0.001 DCR/kB）并且无法改变。Ticketfe 是你的票被挖到的时候你支付的费用。这个费用是对 PoW 矿工的激励来挖你的票并添加到票池。

以免购买窗满了（也就意味着在那个购买窗，有更多的票被买但是有更少的票可以被挖），ticketfee 会被用来决定哪些票可以被放入票池中。有着更高 ticketfee 的票会被 PoW 矿工选取。

费用是用每千字节的 DCR 来计算的。由于一张票只有大概 300（单票）或者 540（池）字节的大小，你实际支付的费用将会比你设置的特定费用数量要低。

当一张票用来投票、过期或是错过之后，txfee 和 ticketfee 都不会被返还。

在一张票投票或是撤销之后资金返回到你的钱包，不会产生费用。

6. 股份池是什么？

股份池等同于矿池，但是是对于 PoS 系统来说的。通过你 Decred 钱包中的选项，你可以把你的投票权给一个股份池。如果你的票被选出来投票，股份池会替你投票并且你会获得 PoS 奖励减去股份池费用（通常是 4-5%）的回报。不像矿池，PoS 奖励不会在股份池的用户之间分割。所有奖励都会给票的拥有者。

一个股份池会允许你买票，但是不会要你自己的钱包解锁并一直在线。很重要的是要注意，你都资金永远不会离开你的钱包。你不会把任何东西发送给股份池，仅仅是给它替你投票的权利。一个股份池无权获取你的资金。

股份池通常会通过物理地全球分布钱包来实现多钱包冗余。这就意味着很少会因为一个钱包宕机而错过一次投票。它同样降低了钱包和网络之间的延迟，这也就降低了错过投票的几率。

7. 当我买了一张票之后，我的资金会发生什么变化？

用来购买票的资金会被锁住，直到这张票被选出来投票或是过期。它们不会离开你的钱包并且在你的钱包中的“lockedbytickets”分区出现。如果你的票被选出来投票，你会得你为这张票支付的全部费用以及 PoS 奖励。

使用这个系统所花费的只有你设置的费用。Txfee 会被网络作为你购票的交易而收取。Ticketfee 会被合并到票池而收取，并且付给 PoW 矿工。如果你的票没有被挖，因为这个交易永远没有在网络上进行，所以不会收取费用。

以免你的票在 40960 个区块之后（大约 4 个月）还没有被选出来投票，系统会撤销你的票并且你支付的 decred（减去费用）会被回退到你的钱包。

8. 我的票用来投票的机会有多大？

Decred 中使用的 PoS 系统使用一个泊松分布来决定一张票在任何给定的时间投票的机会。给定 40960 张票大小的目标池，任何一张票都有 50%的几率在 28 天内投票，和 99.5%的几率在过期之前投票。注意，这些值会根据池的大小而变化。

9. PoS 投票是什么？

因为由 PoS 系统执行的区块检验表现的就像是投票系统，所以它也可以用来投票其他问题。

当票被选出来验证一个区块时，它会投票是否批准之前挖的区块。这需要 5 张选出来的票中有 3 票投赞成（yes）。

通过给不干扰挖出的区块的批准的票添加另外一个参数，系统可以在大量区块上追踪使用那个参数的票的数量。你可以在你的钱包中在票投票之前，随时设置这个参数。

举个例子，你可以选择你票的颜色为红色或蓝色，设置那个选项，然后系统会数接下来的 100 个区块有多少红票有多少蓝票。也许会有 3000 张红票，1500 张蓝票，还有 500 张没选择颜色。

如果你用一个 yes 或 no 选项替换红票或蓝票选项，你就有了一个随时间计数投票的投票系统。通过使用 PoS 投票系统，任何持有 DCR 的人可以投票设置在一个 agenda 里的问题。

这个投票系统可以为任何管理问题所用。对于 Decred，最突出的用处将会是投票硬分叉，也就是货币工作的技术改变。一些例子如下：

- 增加区块的最大容量。
- 改变 PoS 使用的决定票价的算法。
- 为货币的主要新特性投票（比如，lightening network，增强的隐私）。
- 更改 PoW 算法。
- 社区决定的众多事情将会最优化货币的利息

目前，社区用来提交和主持投票 agenda 的一个平台正在开发中。

10. 硬分叉投票是什么？

像任何其他加密货币一样，Decred 可能需要在某些点上硬分叉。

为 PoS 投票系统设置的 agenda 问题之一可能是一个硬分叉。如果这样一个问题被设置新版本的 Decred 源代码将会包含硬分叉在其中，但是这个硬分叉直到 PoS 系统开始在上面投票了才会被激活。

要开始一个硬分叉投票需要满足两个重要的条件：

- 首先，75%的 PoW 矿工必须升级到当前网络区块的最新版本。这个检查在之前的 1000 个区块上运行。
- 其次，75%的 PoS 矿工必须升级到最新版本。这个检查在之前的 2016 个区块上运行。

一旦满足了这些检查，投票流程就开始了。票可以设置一个额外的参数 yes/no/abstain。在投票之前你要在你的钱包里做这件事。被标记为弃权（abstain）的票不会被计入总投票数中。

然后 PoS 系统开始在事先决定的数量的区块上计数含有这些参数设置的票。如果在这个间隔上“yes”的票大于等于 75%，那么投票通过。一个在设置好数量的区块时间段上的锁将会在硬分叉启动之前开始，这样每个人都有一次机会来升级并且不会被硬分叉淘汰出网络。

因为硬分叉的代码已经准备好看，在之后的 Decred 的当前版本中，就不需要开发人员干预或者大多数的 PoW 矿工和 PoS 矿工在一个决定到达之后升级。如果硬分叉的投票通过了，它会在上锁期间之后自动实现。

硬分叉投票可能在多个点上失败。如果 PoW 矿工或者 PoS 矿工不升级的话，投票可能根本不会开始。在那之后， 也可能达不到 75%的投票这个阈值。

以免投票失败，一个新的回合将会在流程的初始阶段开始。这意味着如果 PoS 矿工已经升级，则检查 PoW 矿工是否升级，然后开始另一个投票计数阶段。这会持续一定数量的回合，在那之后，如果投票未通过，那个 agenda 问题就会被搁置。

11. PoS 易受使用其客户的 decred 大型交易所的影响吗？

个人（或交易所）拥有的 decred 的数量对于 PoS 来说毫无意义。它就是你拥有的票的数

量。用来买票的资金直到他们买的票投票之后才会被解锁。这就意味着 PoS 涉及到的 decred 实际上是不可交易的。对于交易所要使用他们的客户的 decred 来投票，他们必须把 decred 从钱包中转出并上锁多至 5 个月。人们会注意到他们的余额变化（锁在 PoS 上的 decred 会显示不可花费）并且他们不能取出任何资金，所以交易所会承受很大的资金流失。

而且有一个每区块加 20 张票的强限制，所以交易所不能比这个速度更快地涌入池中。

最后，池中有一个对于票的总数的软上限。每 144 个区块（2880 张票）票价要基于池中票数和上一窗口新票加入的比率调整一次。最终票价会变得非常高即使一个交易所也无法买入很多的票。并且要记住，即使他们那样做了，他们的 DCR 会被锁住所以票价再次降下来的时候他们也不能买入更多。

12. PoS 易受像最初开发者这样的大余额持有人的影响吗？

上述的池大小限制适用于此。这阻止了个人/团队用其自己大量的票涌入 PoS 池。即使他们买光了整个池（以大量的费用）他们最多可能获得大约 4000 张票（基于之前的窗口，通常会在下一个窗口由大约 30 DCR 涨至 100，然后下一个的最大值通常超过 300）。所以一个拥有大量余额的持有人可能买光两个窗口。30 的窗口会是 85400 DCR，然后下一个 100 的会是 288000 DCR。所以那将会花费 374400 DCR 来买 5760 张票。随着 40960 张票大小的目标池，374400 DCR 会给你带来大约所有票的 14%。

现在持有人可能等待几天票价下跌然后重新买光票。除了那些大部分的资金会在之前买的那些被锁住（尽管有些可能已经投过票了），所以他们在新窗口的购买力会被大幅度削弱。但是让我们假设他们拥有大量的资金并且在所有交易所买下了所有的 decred。所以他们有能力再买两个窗口并替换那些已经投票了的票并且成功买下了所有的票（以非常高的费用和/或价格）。让我们假设那花费了他们大约 25%的票。

一个区块的票是随机分布选取的。强制一个投票以特定的方式进行你将需要一个给定的区块 5 票中的 3 票也就是 60%。甚至以那样大量的资金支出，他们也少于一半。由于一个投票不会在一个单独的区块上被决定，所以你需要投票阶段的 75%的区块的 60%。

然后，你仍然需要 PoW 矿工来确认投票。如果他们认为某些人正在尝试超控系统他们可以选择使区块无效。

所以基本上，这接近于不可能，即使一个人拥有大量比例的 DCR。

但是我们然后来说股份池。股份池，没有权限获取任何用户的资金，却拥有改变分配给他们的票的投票的能力。这就是为什么当加入一个股份池的时候建议人们不要只是简单的去最大的股份池。Decred 是“去中心化信用（decentralised credit）”的缩写，所以 PoS 的部分灵感是为了确保 PoS 股份池不会相比于其他变得非常大。然而，即使是近乎 20%的最大的股份池也只能获得平均每个区块一次投票。

所以 Decred 是特定设计用来最小化来自大 PoW 和 PoS 池和拥有大量存货个人的影响的。