**权益证明机制下的奖励和惩罚**



上次编辑: [@DreamInMorning(opens in a new tab)](https://crowdin.com/profile/DreamInMorning), 2023年7月24日

查看贡献者

以太坊使用其原生加密货币以太币 (ETH) 来保证其安全。 那些希望参与验证区块和识别链头部的节点操作者，需要把以太币存入到以太坊的智能合约中。 他们运行验证者软件检查从点对点网络接收到的新区块的有效性，以及应用分叉选择算法来识别链头，然后收到用以太币支付的报酬。

对于验证者来说有两个主要角色：1) 检查新区块并且“证明”它们是否有效，2) 当从整个验证者池子被随机选中时，提议新的区块。 如果验证者无法完成其中任何一项的任务，将错过以太币的支付。 验证者有时也需要负责签名聚合以及参与同步委员会。

还有些操作很难无意为之，并且标志着一些恶意的意图，例如，为同一时隙提议多个区块和为同一时隙验证多个区块。 这些是“可被罚没的”行为，将导致验证者被移出网络之前有一些以太币（高达 1 ETH）被销毁，这个过程需要 36 天。 被罚没验证者的以太币将在退出期一点点耗尽，但到第 18 天，他们会收到一个“相关性惩罚”，即当更多的验证者都在大致相同的时间受罚时，惩罚将更重。 共识机制的激励结构会奖励诚实者和惩罚不良行为者。

所有的奖励和惩罚都在每个时段实施一次。

阅读了解更多详情...

**奖励和惩罚**

**奖励**

当验证者作出与大多数其他验证者一致的投票时，当验证者提议区块时，以及当验证者参与同步委员会时，他们会受到奖励。 每个时段奖励的数额是从 base\_reward 计算的。 这是计算其他奖励的基本单位。 base\_reward 代表了在每个时段的最佳条件下每个验证者的平均奖励。 这是根据验证者的有效余额以及活跃验证者的总数计算的，如下所示：

base\_reward = effective\_balance \* (base\_reward\_factor / (base\_rewards\_per\_epoch \* sqrt(sum(active\_balance))))

其中，base\_reward\_factor 是 64，base\_rewards\_per\_epoch 是 4，sum(active balance) 是所有活跃验证者的质押以太币总数。

这意味着基础奖励与验证者的有效余额成正比，与网络中的验证者数量成反比。 验证者越多，整体发行量越大（如 sqrt(N)），但每个验证者的 base\_reward 越小（如1/sqrt(N)）。 这些因素影响质押节点的年化利率。 在 [Vitalik 的笔记(opens in a new tab)](https://notes.ethereum.org/@vbuterin/rkhCgQteN?type=view#Base-rewards)阅读这方面的原理。

总奖励由五个部分之和组成，每个部分都有一个权重，决定每个部分在总奖励中的比重。 这些部分是：

1. 来源投票：验证者给正确的来源检查点进行了及时投票

2. 目标投票：验证者给正确的目标检查点进行了及时投票

3. 头部投票：验证者给正确的头部区块进行了及时投票

4. 同步委员会奖励：验证者参与了同步委员会

5. 提议者奖励：验证者在正确的时隙提议了区块

每个部分的权重如下所示：

TIMELY\_SOURCE\_WEIGHT uint64(14)

TIMELY\_TARGET\_WEIGHT uint64(26)

TIMELY\_HEAD\_WEIGHT uint64(14)

SYNC\_REWARD\_WEIGHT uint64(2)

PROPOSER\_WEIGHT uint64(8)

这些权重加起来等于 64。 奖励的计算方法是适用权重的总和除以 64。 如果验证者及时给来源、目标和头部投票，提议一个区块以及参与同步委员会，他们就能获取 64/64 \* base\_reward == base\_reward。 然而，验证者通常不是区块提议者，所以它们的最大奖励是 64-8 /64 \* base\_reward == 7/8 \* base\_reward。 既不是区块提议者，也不参与同步委员会的验证者能收到 64-8-2 / 64 \* base\_reward == 6.75/8 \* base\_reward。

还增加一个额外奖励来激励快速认证。 这就是 inclusion\_delay\_reward。 这个值等于 base\_reward 乘以 1/delay，其中 delay 是分隔区块提议和认证的时隙数。 例如，如果在区块提议的一个时隙内提交认证，那么认证者将获得 base\_reward \* 1/1 == base\_reward。 如果认证在下一个时隙到达，认证者将收到 base\_reward \* 1/2，以此类推。

包含在区块中的**每一个有效认证**都能让区块提议者获得 8 / 64 \* base\_reward，所以奖励的实际值与证明验证者的数量成比例。 通过在所提议区块中包含其他验证者的不良行为证据，区块提议者也能增加奖励。 这些奖励是鼓励验证者诚实的“胡萝卜”。 一个包含罚没的区块提议者将被奖励 slashed\_validators\_effective\_balance / 512。

**惩罚**

到目前为止，我们已经考虑了行为良好的验证者，但对于那些没有及时作出头部、来源和目标投票或者投票非常慢的验证者呢？

错失目标和来源投票的惩罚等于认证者提交这些投票时获取到的奖励。 这意味着没有奖励会添加到他们的余额中，反而会从余额中移除同等价值。 错失头部投票没有惩罚（即，头部投票只有奖励，没有惩罚）。 也没有与 inclusion\_delay 值相关的惩罚 - 只是不会把奖励添加到验证者余额。 区块提议失败也没有惩罚。

在[共识规范(opens in a new tab)](https://github.com/ethereum/consensus-specs/blob/dev/specs/altair/beacon-chain.md)中阅读更多关于奖励和惩罚的内容。 Bellatrix 升级调整了奖励和惩罚 - 观看 Danny Ryan 和 Vitalik 在[“以太坊改进提案解读”视频(opens in a new tab)](https://www.youtube.com/watch?v=iaAEGs1DMgQ)中对此的讨论。

**罚没**

罚没是一种更加严重的行为，将导致验证者被强制移出网络并且他们质押的以太币会损失。 有三种方式会让验证者被罚没，所有这些都相当于不诚实地提议或认证区块：

* 在同一时隙提议或签名两个不同的区块
* 认证一个“包围”另一个区块的区块（有效地更改历史）
* 通过证明同一个区块的两名候选人进行“双重投票”

如果这些行为被检测到，验证者就会被罚没。 这意味着 1/32 的质押以太币（最多是 1 个以太币）将被立即销毁，然后一个为期 36 天的移除期开始。 在移除期内，验证者的质押将逐渐流失。 在中间点（第 18 天），会有一个额外的惩罚，其幅度与罚没事件前 36 天内所有罚没验证者的质押以太币总数成比例。 这意味着被罚没的验证者越多，罚没的幅度就会增加。 最大的罚没幅度是所有罚没验证者的全部有效余额（即，如果有很多的验证者被罚没，那么他们将失去全部的质押）。 另一方面，一次单独的罚没事件只会销毁一小部分的验证者质押。 这个与罚没验证者的数量成比例的中间点惩罚被称为“相关性惩罚”。

**怠惰惩罚**

如果共识层超过四个时段都还没有最终确定，则会激活称为“怠惰惩罚”的紧急协议。 怠惰惩罚的最终目的是给该链恢复最终确定性创建必要条件。 正如上文所解释的那样，最终确定性需要 2/3 多数的总质押以太币来同意来源和目标检查点。 如果超过 1/3 验证者总数的验证者离线或者提交正确认证失败，那么就不可能有超过 2/3 的绝对多数来最终确定检查点。 怠惰惩罚会让非活跃验证者的质押逐渐流失，直到他们控制的总质押少于 1/3，这就允许了其余的活跃验证者可以最终确定该链。 不管非活跃验证者的池子有多大，其余的活跃验证者最终都会控制超过 2/3 的质押。 质押损失对于非活跃验证者尽快重新激活有着强大的激励！ 在 Medalla 测试网曾遇到过一个怠惰惩罚的场景，少于 66% 的活跃验证者能够在当前区块链头部达成共识。 怠惰惩罚被激活，最终重新获得最终确定性！

共识机制的奖励、惩罚和罚没的设计，可鼓励个人验证者做出正确行为。 然而，从这些设计选择中催生了一个这样一个系统：它强烈激励在多个客户端平均分配验证者，并应强烈抑制单一客户端的主导地位。