

原文作者：Stakin 编译：SHOU 原文链接：<https://medium.com/stakin/proof-of-stake-guide-dpos-vs-lpos-vs-bpos-vs-hybrid-1393a33e849c>

对于权益证明 (PoS) 大家已经很熟悉了，这篇文章中我们就来了解一下 PoS 都有哪些变体。

第一部分 — Proof-of-Stake

对于那些不太熟悉权益证明 (PoS) 的人，我们先来简单了解一下。

PoS 通常被拿来与工作量证明 (PoW) 作比较，PoS 根据网络验证器拥有的代币数量来进行激励。

PoS 于 2012 年由 Sunny King 首次提出。该机制选择利益相关者来验证交易。在 PoS 中，通过抽签过程选择下一个区块的创建者。创建新块并添加到网络中将获得数字资产的奖励。在 PoS 中，staked 代币的数量决定了网络的安全保障，而在 PoW 中，是靠算力保护网络。我们非常看好权益证明 (PoS) 加密货币的未来，因为我们相信它具有以下优点：

1. 与 PoW 相比消耗更少：我们在各种 PoS 协议上运行几个 staking 节点，只需要几个安全的 VPS 就可以做到这一点，而 PoW 矿工的挖矿设备却需要好多。
2. 代币持有者可以根据通货膨胀率赚取奖励/利息；这有助于建立社区，激励人们持有代币。
3. 去中心化：根据协议采用的 PoS 类型，网络有可能达到完全去中心化，这是创建加密货币的初心。

接下来，将向您介绍各种 PoS 变体，详细介绍它们的工作原理，然后为您提供一个简单的概括表。为了简化起见，验证器指用于保护和验证网络上交易的节点，以赚取代币报酬。根据协议的不同，也可以称其为区块生产者、见证人或面包师。

第二部分——不同的 PoS 差异

Delegated Proof-of-Stake (DPoS)

DPoS 通常通过选举系统工作，在选举系统中会授权固定数量的验证器来保护网络安全。作为代币持有者，您可以投票决定谁将验证网络上的交易，投票权取决于您的质押份额 > 。得票最多的验证器可以成为委托人，验证交易并获得奖励。

DPoS 已经在 Lisk、Tron、Steem、Bitshares 甚至 EOS 等协议上实现，EOS 是 Daniel Larimer 创建的一个可扩展的区块链 Dapp 平台，因为其创纪录的 40 亿美元 ICO 而出名。根据协议的不同，DPoS 可能需要验证器具有强大的计算能力。

Delegated Proof of Contribution Protocol(DPoC)

一些人可能会熟悉 ICON 网络，PoS 区块链引入了一种新协议，该协议直接用加密货币奖励节点和委托人，被称为委托贡献证明。在许多方面，它类似于 DPoS，但是激励机制的设置方式使得社区成员真正有兴趣为协议的发展做出贡献

在 DPoC 中，委托（称为投票）是可选的和非托管的。此外，可以在不给节点运营商投票的情况下质押代币。

DPoC 是一个去中心化的民主的治理协议，在该协议中，代币持有者通过将代币质押委托给那些直接对网络作出贡献的人：公众代表（P-Rep）来行使其治理权。共有 22 名当选的主要 P-Rep，不限制副 P-Rep 的数量，他们也受到激励做出贡献。此外，还向其他类型的生态系统参与者和 Dapp 建设者提供奖励。

如果出现严重的宕机，P-Rep 及其选民将面临削减惩罚的风险，目前是可能会受到 6% 的罚款。

DPoC 仍在快速发展并不断改进。stakin 作为一名 P-Rep 参与了协议下一次迭代的开发，并支持 IISS3.0，这可以使 DPoC 更接近 LPoS（符合债券要求），同时去中心化激励参与者建设者！

Liquid Proof-of-Stake (LPoS)

在 LPoS 中，委托是可选的。代币持有人可以将验证权委托给其他代币持有人，而无需托管代币，这意味着代币仍保留在代币持有人的钱包中。此外，只有验证器在出现安全故障时才会受到惩罚（例如双重认可）。LPoS 也具有投票权，作为代币持有者，如果你作为自己的节点，你可以在协议修正案中直接投票。

LPoS 最初是由 Tezos 引入的。Tezos 是由 Kathleen 和 Arthur Breitman 创建的链上治理协议，自 2018 年 9 月以来一直在主网上平稳运行。Tezos 的 LPoS 已经证明是非常成功的，目前的质押比例约为 80%，分布在 450 个验证器和 10000 多个委托人中。从技术上讲，委托人的数量受到债券规模最低要求的限制，目前可能已经高达 10 万人左右，去中心化程度很高。

Bonded Proof-of-Stake (BPOS)

BPOS 与 LPoS 非常相似：授权是可选的、非托管的，代币持有者从协议修正案的投票权中受益。尽管如此，它之所以被称为 BPOS 是有原因的：在出现安全或宕机的情况下，验证器和委托人的一部分质押将被削减。在 LPoS 中，只有验证器有被削减惩罚的风险，而授权者唯一的风险是错过一些奖励。通过这种方式来防止验证器不诚实或效率低下。

这种 BPOS 机制的优势在于，它可以为一些 LPoS 协议上的验证者提供一个清晰的解决质押比率（类似于资本要求）问题的方案，他们需要尽量维持该比率以防止过度委托。在样也意味着授权人需要在授权前要进行额外的尽职调查，并对验证器的情况保持关注。

BPOS 最早是由 Cosmos 和 IRISnet（基于 Cosmos SDK/Tendermint）等项目引入的。两者都是非常有趣的跨链协议。在 Cosmos 和 IRISnet 等 BPOS 协议中，验证器的数量是有限的，根据它们的总质押量（自有质押+委托）的大小来决定有效验证器。

Nominated Proof-of-Stake

波卡生态系统引入了提名权益明机制（NPOS）。现在许多基于 Substrate 的链都在使用，如 Polkadot、Kusama 以及 Edgeware。在这个系统中，验证器每天自动选择几次。这些验证器运行代价昂贵，例如要确保高通信响应度、建立长期的可靠性信誉并质押代币。这样做是为了保持良好的行为，当他们偏离协议时，他们的利益就会被削减。而且，从最近 Edgeware 验证器的故障我们可以看到，在 NPOS 上可以非常快地执行削减操作。

在 NPOS 中，委托者被称为提名者。提名者在候选列表中提名验证器，并锁定一定数量的代币来支持它们。在 NPOS 中，验证程序的数量受治理的限制，并且这些验证器是根据它们在网络中的总质押量来选择的。与验证器不同，提名者可以有无数的参与者。提名者被激励不断寻找可靠的新候选人。有了这两个角色，NPOS 可以让所有代币持有者持续参与网络。因此，它保持有限验证器数量的同时，保持了高级别的安全性。

Hybrid Proof-of-Stake (HPoS)

混合 PoS/PoW 通常被称为工作量证明和权益证明之间的混合。它使用两种方法一起来保护网络：PoS 与 PoW

系统一起工作，以进一步保护区块链。通常，在这种方法中，矿工通过 PoW 生成新的块，然后 PoS 验证器对这些块的有效性进行投票。HPoS 通过哈希的力量，避免了更多的攻击。

在 HPoS 项目中，我们可以看到 Decred 和 Hcash。以太坊也正在进行 Casper 升级成为 HPoS。在 Decred 中，代币持有者有能力检查矿工挖出的区块，并对共识规则的变更进行投票。

Pure Proof-of-Stake

Algorand 引入的另一个共识算法是 PPoS，它是一种具有开放参与性、可扩展性、安全性和交易终结性的协议。在这个算法中，网络将其安全性与大多数人的诚实联系在一起。

这个算法的不同之处在于，与前面提到的 DPoS，LPoS 或 BPOS 不同，对于实体行为不当的情况，没有制裁机制。网络宁愿让少数人不能作弊，允许大多数人作弊，也不会进行削减。该协议的发展方式是，只要网络中 75% 的大多数人是诚实的，它就可以继续正常工作。

Leased Proof-of-Stake

租赁权益证明 (LPoS) 是 PoS 的直接变体。当使用这个共识协议时，领导者可以参与生成新的块。因为在网络节点内租用的数量越大，选择它创建下一个块的机会就越高。

LPoS 的工作方式如下：为了能够开始租赁，代币持有者需要创建一个租赁事务，并指定地址以及要租赁的代币数量。Waves 平台是采用 LPoS 网络。

其他可以归类为 PoS 的项目

本文的目标是为您提供一个全面的概述，了解各种 PoS 协议的核心。随着 PoS 在整个区块链行业中越来越受关注，我们还想提及一些其他项目，这些项目也提供质押：

Tomochain: Proof-of-Stake Voting (PoSV) 权益证明投票

达世币 Dash: 主节点质押

本体 Ontology: ONG “红利” 委托拜占庭容错

Neo: GAS “红利” 委托拜占庭容错

总结