百科 | 什么是委托权益证明 (DPoS)？

作者：Shailey Singh，CoinTelegraph；编译：白水，本站

## 一、什么是委托权益证明 (DPoS)？

DPoS 是权益证明 (PoS) 共识机制的演变，旨在提供增强的可扩展性、效率和民主治理。

区块链技术主要通过其去中心化性质和共识机制彻底改变了我们感知和处理数字交易的方式。这些去中心化机制的主要目的是确保在管理区块链交易和数据记录时没有中央把关。相反，共识机制依赖网络参与者来验证交易并将其添加为链上的新区块。

在各种共识算法中，一种备受关注的机制是委托股权证明。 DPoS 是经典权益证明共识机制的变体。

Daniel Larimer 在 2014 年提出了 DPoS 概念，作为传统 PoS 共识机制的增强，旨在提高效率和可扩展性。 Larimer 首先在 Bitcointalk 论坛帖子中分享了他的愿景，这导致了 DPoS 的实际实施以及 2015 年BitShares的推出。

这标志着 DPoS 在区块链技术中的开始，为其在 Steem 和 Eos 等其他项目中的采用奠定了基础。尤其是Eos，利用共识机制在2017年进行了加密货币行业最大的首次代币发行（ICO）之一，引起了对DPoS的高度关注，凸显了DPoS在实现高性能和去中心化治理方面的潜力。

## 二、DPoS 与 PoS 等其他共识机制有何不同？

DPoS 与传统 PoS 不同，它使用投票系统来选举代表进行区块验证，使过程更加民主和可扩展。

理解所有共识机制的关键在于如何达成共识。虽然比特币区块链引入了第一个通过工作量证明（PoW）在区块链上达成共识的机制，但区块链网络还有一些其他方法可以达成共识。 PoS是在2012年的一篇学术论文中引入的，它是由Sunny King和Scott Nadal撰写的，作为解决比特币挖矿高能耗问题的一种新的共识机制。

PoS 是最常见的共识机制之一，以太坊生态系统于 2022 年采用了它。逐渐地，PoS 的各种其他安全迭代开始出现，包括混合 PoS-PoW、纯 PoS 以及 2014 年的委托 PoS。

在 DPoS 系统中，网络用户投票将区块验证权委托给选定的一组见证人或区块生产者。这一过程旨在通过确保验证交易的权力分布在当选代表之间，而不是集中在少数富有的利益相关者手中，来解决标准 PoS 算法的一些民主限制。

这意味着，与利益相关者直接验证交易的传统 PoS 不同，DPoS 允许代币持有者选举负责验证区块的代表。

在 DPoS 系统中，网络用户投票将区块验证权委托给选定的一组见证人或区块生产者。这一过程旨在通过确保验证交易的权力分布在当选代表之间，而不是集中在少数富有的利益相关者手中，来解决标准 PoS 算法的一些民主限制。

这样，DPoS 简化了区块验证过程，从而缩短了交易确认时间。有限数量的当选代表也增强了网络的可扩展性。

## 三、DPoS 是如何运作的？

DPoS 的核心机制围绕投票、委托和验证。

DPoS 通过纳入选举机制来增强传统 PoS 系统，网络参与者投票选举负责验证和创建区块的代表。这个过程涉及四个关键参与者：投票者、见证者（或区块生产者）、代表和验证者。

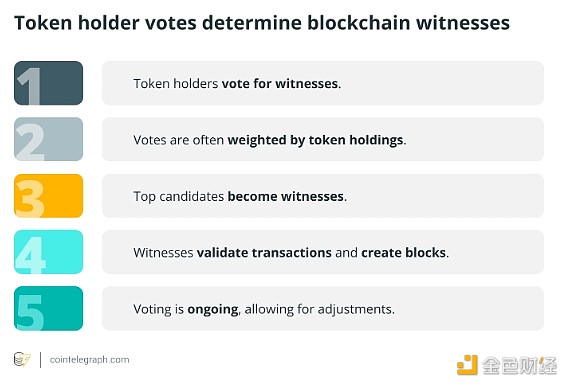
### 选民

在 DPoS 系统中，每个网络参与者即使持有最少量的原生代币也可以成为投票者，没有最低利益相关者代币参与要求。选民通过选举见证人和代表并通过治理提案参与决策过程，在网络治理中发挥着至关重要的作用。投票权与持有代币数量成正比，意味着拥有更多代币的用户拥有更大的影响力。

选民可以选择自己投票或将投票权委托给另一个人。他们的主要职责是选择见证人或区块生产者，因为这些实体直接参与区块生产过程。因此，选民有动力选择值得信赖且有能力的候选人，以确保网络的平稳运行和安全。

### 见证人（区块生产者）

见证人，也称为区块生产者，是代币持有者青睐的验证交易和创建新区块的节点。这些实体对于区块链的运行至关重要，因为它们确保交易数据的完整性和准确性。在验证区块中的所有交易后，见证人会收到区块奖励，通常与支持他们的选民分享。



如果见证人未能在规定的时间内验证交易，他们就会错过该区块并丧失奖励。这种错过的奖励通常会传递给下一个成功验证该区块的见证人。该系统激励选民和见证人诚实行事：选民的目标是选出可靠的见证人以最大化他们的回报，而见证人则努力保持自己的诚信和声誉以吸引选票。

### 代表们

选民选举代表来监督 DPoS 中的治理职能。与专注于区块生产的见证人不同，代表负责对网络提出改进和更改建议。这些建议的范围从修改区块大小到调整区块奖励。

一旦代表提出提案，必须经过网络参与者投票才能实施。代表本身无权直接将变更应用于系统；他们的作用是促进并提出改进建议，然后得到社区的批准。这种职责分离有助于维持平衡和去中心化的治理结构。

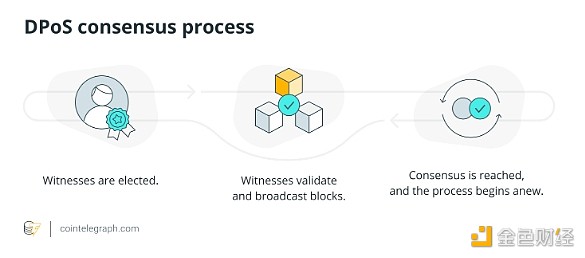
### 验证者

验证者是完整的节点，用于验证见证人创建的区块是否遵守共识规则。与见证人不同，任何用户都可以成为验证者，并且通常没有直接的经济激励来执行此角色。验证者通过确保所有区块都遵守既定的规则和协议，在维护区块链的完整性方面发挥着关键作用。

## 四、DPoS 的激励和治理机制

DPoS机制协调所有参与者的激励，以促进安全高效的网络。选民被激励选择有能力的见证人和代表，以最大化他们的回报并确保网络的完整性。反过来，见证人和代表也有动力维护自己的声誉，并按照网络的最佳利益行事，以保留自己的职位并继续获得奖励。

整个过程看起来很简单：



持续的投票过程以及替换表现不佳或恶意行为者的能力有助于建立动态且有弹性的治理模型。该系统促进了高水平的社区参与，并确保决策权仍然分配给利益相关者。

## 五、DPoS的优点

与其他共识机制相比，DPoS 具有多种优势，使其成为某些区块链项目的首选。

DPoS 提供了几个显著的优势，可以增强区块链网络的性能和治理。主要好处之一是它的可访问性。与需要大量计算能力和专用设备的 PoW 系统不同，DPoS 允许任何拥有原生代币的人参与投票过程并成为代表。这种低准入门槛促进了更具包容性的网络，让更广泛的参与者可以参与共识机制。

DPoS 的另一个显著优势是其可扩展性。通过限制负责区块生产的代表数量，DPoS 可以实现更快的共识，从而提高交易吞吐量并提高网络性能。此外，DPoS 是环保的，因为它不需要与 PoW 系统相关的大量能源消耗。这种可持续性方面符合对绿色技术不断增长的需求。

此外，DPoS 的民主本质促进了更加去中心化的治理模式。持续的投票过程确保代表们对社区负责，利益相关者可以积极参与决策过程。这种动态治理结构可以快速适应和实施网络改进，从而增强区块链的整体弹性和发展。

## 六、DPoS 的局限性

尽管 DPoS 有许多优点，但它也有其局限性和挑战。

主要关注点之一是中心化的可能性。虽然 DPoS 旨在分散决策权，但该系统可能会无意中将权力集中在少数代表手中。

由于当选代表的数量有限，因此存在一小群代表可能主导网络的风险，从而导致类似于传统 PoS 系统中出现的中心化问题。这种权力的集中可能使网络面临共谋和恶意活动的危险。

此外，DPoS 需要高水平的选民参与和意识。为了使系统有效运作，选民必须充分了解候选人及其表现。然而，较小的利益相关者可能会觉得自己的投票微不足道，而选择不参与，从而降低了共识机制的整体稳健性。

此外，对有限代表数量的依赖引发了安全问题。如果大多数代表串通或恶意行为，他们可能会执行 51% 攻击，从而损害网络的安全性和稳定性。此漏洞需要社区保持警惕和积极主动，以确保不断选举出诚实且有能力的代表。

DPoS 代表了区块链共识机制的演变。随着区块链技术的发展，DPoS 旨在提供一个实现去中心化治理和高效区块验证的框架。