**权益证明机制(POS)**



上次编辑: [@jackson21182(opens in a new tab)](https://crowdin.com/profile/jackson21182), 2023年7月24日

查看贡献者

权益证明 (PoS) 是支撑以太坊[共识机制](https://ethereum.org/zh/developers/docs/consensus-mechanisms/)的基础。 以太坊于 2022 年启动了权益证明机制，这是因为和原先的[工作量证明](https://ethereum.org/zh/developers/docs/consensus-mechanisms/pow/)架构相比，以太坊更安全、能耗更低并且更利于实现新的扩容解决方案。

**前提条件**

为了更好地理解本文，我们建议你首先阅读以下内容 [共识机制](https://ethereum.org/zh/developers/docs/consensus-mechanisms/)。

**什么是权益证明？**

权益证明是构成[共识机制](https://ethereum.org/zh/developers/docs/consensus-mechanisms/)的基础，区块链使用这些机制来实现分布式共识。 在工作量证明共识机制中，矿工通过消耗能源来证明他们拥有资本以应对风险。 以太坊采用权益证明机制，在该机制下，验证者明确地通过以太币将资本质押到以太坊上的智能合约中。 这些质押的以太币充当抵押品，如果验证者有失信行为或者消极怠工，那么可以销毁抵押品。 之后，验证者负责检查在网络上传播的新区块是否有效，并偶尔自己也创建和传播新区块。

与工作量证明体系相比，权益证明有许多改进：

* 能效更高 – 无需在工作量证明计算中使用大量能源
* 门槛更低、硬件要求下降 – 无需购买高性能硬件以便获得创建新区块的机会
* 中心化风险降低 – 权益证明应该可以增加保护网络安全的节点
* 由于能源需求低，发行较少的以太币就可以激励大家参与
* 与工作量证明相比，对不当行为的经济处罚让 51% 攻击的代价呈指数级增加。
* 如果 51% 攻击是为了攻破加密经济的防御，那么社区可以求助于诚实链的社会恢复。

**验证者**

要想作为验证者参与，用户必须向存款合约存入 32 个以太币并运行三种独立的软件：执行客户端、共识客户端和验证者。 存入以太币时，用户会进入一个激活队列，限制新验证者加入网络的速度。 激活后，验证者将从以太坊网络上的对等节点接收新区块。 区块中交付的交易会被重新执行，并且对区块签名进行检查以确保区块是有效的。 然后验证者在整个网络上发送支持该区块的投票（称为认证）。

在工作量证明中，生成区块的时间是由挖矿难度决定的，而在权益证明中，节奏是固定的。 权益证明以太坊中的时间分为时隙（12 秒）和时段（32 个时隙）。 在每个时隙中随机选择一位验证者作为区块提议者。 该验证者负责创建新区块并发送给网络上的其他节点。 另外在每个时隙中，都会随机选择一个验证者委员会，通过他们的投票确定所提议区块的有效性。

**如何在以太坊权益证明中执行交易**

以下提供了关于如何在以太坊权益证明中执行交易的端到端解释。

1. 用户使用他们的私钥创建并签署[交易](https://ethereum.org/zh/developers/docs/transactions/)。 这通常由钱包或库处理，例如 [ether.js(opens in a new tab)](https://docs.ethers.io/v5/)、[web3js(opens in a new tab)](https://web3js.readthedocs.io/en/v1.8.1/" \t "_blank)、[web3py(opens in a new tab)](https://web3py.readthedocs.io/en/v5/" \t "_blank) 等，但本质上是用户在使用以太坊 [JSON-RPC 应用程序接口](https://ethereum.org/zh/developers/docs/apis/json-rpc/)向节点发出请求。 用户定义他们准备支付一定量的燃料作为给验证者的小费，以鼓励他们将交易纳入在一个区块中。 [小费](https://ethereum.org/zh/developers/docs/gas/#priority-fee)支付给验证者，而[基础费](https://ethereum.org/zh/developers/docs/gas/#base-fee)被销毁。
2. 交易被提交给以太坊[执行客户端](https://ethereum.org/zh/developers/docs/nodes-and-clients/" \l "execution-client)验证有效性。 这意味着确保发送人有足够的以太币来完成交易，并且他们已经使用正确的密钥来签名交易。
3. 如果交易有效，执行客户端将其添加到其本地内存池（待处理交易列表），并通过执行层广播网络将其广播到其他节点。 当其他节点听到关于交易的消息时，它们也将其添加到本地内存池中。 高级用户可能会避免广播他们的交易，而是将其转发给专门的区块构建器，例如 [Flashbots Auction(opens in a new tab)](https://docs.flashbots.net/flashbots-auction/overview" \t "_blank)。 这使他们能够在即将到来的区块中组织交易以获得最大利润（[最大可提取价值](https://ethereum.org/zh/developers/docs/mev/#mev-extraction)）。
4. 网络上的节点之一是当前时隙的区块提议者，之前使用 RANDAO 伪随机地进行了选择。 该节点负责构建和广播下一个要添加到以太坊区块链的区块并更新全局状态。 该节点由三部分组成：执行客户端、共识客户端和验证者客户端。 执行客户端将来自本地内存池的交易捆绑到“执行负载”中，并在本地执行它们以生成状态更改。 此信息被传递到共识客户端。在该客户端，执行有效载荷被包装为“信标区块”的一部分。该信标区块还包含有关奖励、惩罚、罚没、认证等的信息，从而使网络能够就链头的区块顺序达成一致。 [连接共识客户端和执行客户端](https://ethereum.org/zh/developers/docs/networking-layer/#connecting-clients)中更详细地描述了执行客户端和共识客户端之间的通信。
5. 其他节点在共识层广播网络上接收新的信标区块， 并将其传递给它们的执行客户端。在执行客户端上，交易在本地重新执行以确保提议的状态更改有效。 然后，验证者客户端证明该区块是有效的，并且根据他们对链的看法，这是逻辑上的下一个区块（这意味着它建立在具有最大认证权重的链上，如[分叉选择规则](https://ethereum.org/zh/developers/docs/consensus-mechanisms/pos/" \l "fork-choice)所定义）。 该块被添加到证明它的每个节点的本地数据库中。
6. 交易可以被认为是“最终确定的”，即，如果它已经成为两个检查点之间具有“绝大多数链接”的链的一部分，则它不能被恢复。 检查点出现在每个时段的开始，并且要拥有绝对多数链接，它们都必须得到网络上总质押以太币 66% 的证明。

有关最终确定性的更多详细信息，请参见下文。

**最终确定性**

交易在分布式网络具有“最终确定性”是指，该交易是区块的一部分，而且除非销毁大量以太币，否则便无法改变。 在权益证明以太坊上，通过“检查点”区块来管理确定性。 每个时段中的第一个区块是检查点。 验证者为他们认为有效的“检查点对”投票。 如果一对检查点获得了质押以太币总数中三分之二以上的投票，那么这对检查点将被升级。 这两个（目标）中较新的一个会变成“合理”状态。 较旧的一个检查点已经是合理状态，因为它是上一个时段中的“目标”。 现在，这个检查点会升级为“最终确定”状态。 要回滚最终确定的区块，攻击者将承担至少相当于质押以太币总数三分之一的损失。 此[以太坊基金会博文(opens in a new tab)](https://blog.ethereum.org/2016/05/09/on-settlement-finality/" \t "_blank)解释了其确切原因。 因为最终确定性需要获得三分之二多数投票，攻击者可以用质押以太币总数的三分之一投票来阻止网络实现最终确定性。 有一种可以防御这种攻击行为的机制：[怠惰惩罚(opens in a new tab)](https://eth2book.info/bellatrix/part2/incentives/inactivity" \t "_blank)。 当链超过四个时段无法最终确定时，这项机制会触发。 怠惰惩罚逐渐消耗与大多数投票相反的验证者的质押以太币，使得大多数验证者重新获得三分之二多数投票并最终确定链。

**加密经济的安全性**

运行验证者是一种承诺。 验证者应当保持足够的硬件和连接，来参与区块的验证和提出。 作为回报，验证者将获得以太币（他们的质押余额增加）。 另一方面，作为验证者参与，也为用户为了个人利益或破坏而攻击网络开辟了新的渠道。 为了防止这种情况，如果验证者在被调用时未能参与，他们就会错过以太币奖励；如果他们有不诚实行为，他们现有的质押可能会被销毁。 主要有两种行为被视为不诚实：在一个时隙中提出多个区块（模棱两可）和提交相互矛盾的认证。 被罚没以太币的金额取决于大致同一时间受到罚没的验证者数量。 这称为[“相关性惩罚”(opens in a new tab)](https://eth2book.info/bellatrix/part2/incentives/slashing" \l "the-correlation-penalty" \t "_blank)，相关性惩罚可以是轻微的（单个验证者被罚没质押以太币的 1%），也可以是导致验证者质押的以太币全部被销毁（大额罚没事件）。 这种惩罚在强制退出期执行，首先是第 1 天的立即处罚（最多 0.5 个以太币），接着是第 18 天的相关性惩罚，最后是第 36 天的逐出网络。 如果验证者在网络上但不提交投票，他们每天都会受到轻微的认证惩罚。 对于攻击者来说，这些措施都意味着协同攻击的代价将极其高昂。

**分叉选择**

当网络以最佳状态诚信运行时，链头始终只会有一个新区块并且所有验证者都会证明它。 然而，由于网络延迟或因为区块提议者提议多个区块（模棱两可），验证者可能看到不同的链头视图。 因此，共识客户端需要一种算法来确定支持哪一个区块。 权益证明以太坊中使用的算法称为 [LMD-GHOST(opens in a new tab)](https://arxiv.org/pdf/2003.03052.pdf)。它的工作原理是确定其历史记录中具有最大证明权重的分叉。

**权益证明和安全性**

正如在工作量证明中一样，权益证明中仍然存在 [51% 攻击(opens in a new tab)](https://www.investopedia.com/terms/1/51-attack.asp)的威胁，但对于攻击者来说风险却更大。 攻击者需要获得 51% 的质押以太币。 然后他们可以通过自己的认证确保他们首选的分叉拥有最多累积认证。 共识客户端使用累积认证的“权重”确定正确的链，所以攻击者能够使他们的分叉成为规范区块。 然而与工作量证明相比，权益证明的优势在于，社区能够灵活地发动反击。 例如，诚实的验证者可以决定继续在非主流链上构建并忽略攻击者的分叉，同时鼓励应用程序、交易所和池也这样做。 他们还可以决定强行将攻击者从网络中移除并销毁攻击者质押的以太币。 这些都是对 51% 攻击的强有力的经济防御措施。

51% 攻击只是其中一种恶意行为。 不良行为者可能会尝试长程攻击（尽管最终确定性小工具抵消了这种攻击向量）、短程“重组”（尽管提议者权重提升和认证期限可以缓解这种情况）、弹跳攻击和平衡攻击（也可以通过提议者权重提升来缓解，并且这些攻击只能在理想化的网络条件下演示）或雪崩攻击（被只考虑最新消息的分叉选择算法规则抵消）。

总的来说，已经证实以太坊实施的权益证明在经济方面比工作量证明更安全。

**优点和缺点**

| **优点** | **缺点** |
| --- | --- |
| 质押使个人更容易参与其中保障网络的安全，促进去中心化。 验证者节点可以在普通笔记本电脑上运行。 质押池让用户可以在没有 32 个以太币的情况下质押。 | 与工作量证明相比，权益证明仍处于起步阶段，并且经过的实践检验较少。 |
| 权益质押更加去中心化。 规模经济不像适用于工作量证明挖矿那样适用于权益证明。 | 实现权益证明比实现工作量证明更加复杂。 |
| 权益证明的加密经济安全性高于工作量证明 | 用户需要运行三种软件才能参与以太坊的权益证明。 |
| 需要发行较少的新以太币就可以激励网络参与者 |  |

**更愿意通过视频学习？**

**延伸阅读**

* [Proof of Stake FAQ(opens in a new tab)](https://vitalik.ca/general/2017/12/31/pos_faq.html) *Vitalik Buterin*
* [What is Proof of Stake(opens in a new tab)](https://consensys.net/blog/blockchain-explained/what-is-proof-of-stake/) *ConsenSys*
* [What Proof of Stake Is And Why It Matters(opens in a new tab)](https://bitcoinmagazine.com/culture/what-proof-of-stake-is-and-why-it-matters-1377531463) *Vitalik Buterin*
* [以太坊 2.0 信标链：一篇需要优先阅读的解读文章(opens in a new tab)](https://ethos.dev/beacon-chain) *Ethos.dev*
* [Why Proof of Stake (Nov 2020)(opens in a new tab)](https://vitalik.ca/general/2020/11/06/pos2020.html) *Vitalik Buterin*
* [Proof of Stake: How I Learned to Love Weak Subjectivity(opens in a new tab)](https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/) *Vitalik Buterin*
* [权益证明以太坊的攻击和防御(opens in a new tab)](https://mirror.xyz/jmcook.eth/YqHargbVWVNRQqQpVpzrqEQ8IqwNUJDIpwRP7SS5FXs)
* [权益证明设计理念(opens in a new tab)](https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51) *Vitalik Buterin*