# 共识算法

## POW:(Proof of Work)：工作量证明机制。

基本原理：第一代共识机制，比特币的基础。理解起来，很简单，就是“按劳取酬”，你付出多少工作量，就会获得多少报酬（比特币等加密货币）。在网络世界里，这里的劳动就是你为网络提供的计算服务（算力x时长），提供这种服务的过程就是“挖矿”。假如是真的矿场，显然在均匀分布的前提下，人们“挖矿”所得的比重与各自提供的算力成正比，通俗一点就是，能力越强获得越多。

优点：

机制本身当然很复杂，有很多细节，比如：挖矿难度自动调整、区块奖励逐步减半等，这些因素都是基于经济学原理，能吸引和鼓励更多人参与。

理想状态，这种机制，可以吸引很多用户参与其中，特别是越先参与的获得越多，会促使加密货币的初始阶段发展迅速，节点网络迅速扩大。在CPU挖矿的时代，比特币吸引了很多人参与“挖矿”，就是很好的证明。

通过“挖矿”的方式发行新币，把比特币分散给个人，实现了相对公平。

缺点：

算力是计算机硬件（CPU、GPU等）提供的，要耗费电力，是对能源的直接消耗，与人类追求节能、清洁、环保的理念相悖。不过，如果非要给“加密货币”找寻“货币价值”的意义，那么这个方面，应该是最有力的证据。

这种机制发展到今天，算力的提供已经不再是单纯的CPU了，而是逐步发展到GPU、FPGA，乃至ASIC矿机。用户也从个人挖矿发展到大的矿池、矿场，算力集中越来越明显。这与去中心化的方向背道而驰，渐行渐远，网络的安全逐渐受到威胁。有证据证明Ghash（一个矿池）就曾经对赌博网站实施了双花攻击（简单的说就是一笔钱花两次）。

比特币区块奖励每４年将减半，当挖矿的成本高于挖矿收益时，人们挖矿的积极性降低，会有大量算力减少，比特币网络的安全性进一步堪忧。

## POS(Proof of Stake):股权证明机制。

基本原理

这是点点币（PPC）的创新。没有挖矿过程，在创世区块内写明了股权分配比例，之后通过转让、交易的方式（通常就是IPO），逐渐分散到用户手里，并通过“利息”的方式新增货币，实现对节点的奖励。以太坊是POW跟pos结合。

简单来说，就是一个根据用户持有货币的多少和时间（币龄），发放利息的一个制度。现实中最典型的例子就是股票，或者是银行存款。如果用户想获得更多的货币，那么就打开客户端，让它保持在线，就能通过获得“利息”获益，同时保证网络的安全。

**优点：**

节能。不用挖矿，不需要大量耗费电力和能源。

更去中心化。首先说，去中心化是相对的。相对于比特币等PoW类型的加密货币，PoS机制的加密货币对计算机硬件基本上没有过高要求，人人可挖矿（获得利息），不用担心算力集中导致中心化的出现（单用户通过购买获得51%的货币量，成本更高），网络更加安全有保障。

避免紧缩。PoW机制的加密货币，因为用户丢失等各种原因，可能导致通货紧缩，但是PoS机制的加密货币按一定的年利率新增货币，可以有效避免紧缩出现，保持基本稳定。比特币之后，很多新币采用PoS机制，很多采用工作量证明机制的老币，也纷纷修改协议，“硬分叉”升级为PoS机制。

**缺点：**

纯PoS机制的加密货币，只能通过IPO的方式发行，这就导致“少数人”（通常是开发者）获得大量成本极低的加密货币，在利益面前，很难保证他们不会大量抛售。PoS机制的加密货币，信用基础不够牢固。为解决这个问题，很多采用PoW+PoS的双重机制，通过PoW挖矿发行加密货币，使用PoS维护网络稳定。或者采用DPoS机制，通过社区选举的方式，增强信任。

## DPOS（Delegated Proof of Stake）：授权股权证明机制

基本原理

无人控制的公司发行股份，产生利润，并将利润分配给股东。实现这一切不需要信任任何人，因为每件事都是被硬编码到软件中的。通俗点讲就是：公司股份制，股东持有这些公司的股份，公司为股东产生回报，无需挖矿。

**优点：**

能耗更低。DPoS机制将节点数量进一步减少到101个，在保证网络安全的前提下，整个网络的能耗进一步降低，网络运行成本最低。

更加去中心化。目前，对于比特币而言，个人挖矿已经不现实了，比特币的算力都集中在几个大的矿池手里，每个矿池都是中心化的，就像DPoS的一个受托人，因此DPoS机制的加密货币更加去中心化。PoS机制的加密货币（比如未来币），要求用户开着客户端，事实上用户并不会天天开着电脑，因此真正的网络节点是由几个股东保持的，去中心化程度也不能与DPoS机制的加密货币相比。

更快的确认速度。每个块的时间为10秒，一笔交易（在得到6-10个确认后）大概1分钟，一个完整的101个块的周期大概仅仅需要16分钟。而比特币（PoW机制）产生一个区块需要10分钟，一笔交易完成（6个区块确认后）需要1个小时。点点币（PoS机制）确认一笔交易大概也需要1小时。

**缺点：**

投票的积极性并不高。绝大多数持股人（90％+）从未参与投票。这是因为投票需要时间、精力以及技能，而这恰恰是大多数投资者所缺乏的。

对于坏节点的处理存在诸多困难。社区选举不能及时有效的阻止一些破坏节点的出现，给网络造成安全隐患。

关于DPOS

现实生活中有更多的类似于DPOS的制度.。比如中国的人名代表大会制度，美国的两会制度。

就以人民代表大会制度为例，每个省市通过选举选择出自己的代表， 然后由这些代表参加人名代表大会, 这样会更有效率， 也能组织起更多的人。