区块链常见的三种共识机制

PoW

“工作量证明机制（PoW）”最早由比特币采用，用工作量结果来证明贡献大小，再根据贡献大小来确定记账权与奖励。

从这个角度看，“工作量证明机制”也可以看作是比特币系统的激励机制。

工作量证明机制（PoW）的运行原理是这样的：全网想要达成共识，需要通过解答“哈希函数”的方式来证明自己完成了一定的工作量，谁能够快准狠地完成工作，解答正确哈希值，谁就会获得记录交易（记账）的权力，进而获得比特币奖励。

优点

1. 算法简单，容易实现；

2. 节点间无需交换额外的信息即可达成共识；

3. 破坏系统需要投入极大的成本，允许全网 50%节点出错。

缺点

1. 浪费能源，依赖机器进行数学运算来获取记账权，资源消耗相比其他共识机制高、可监管性弱，同时每次达成共识需要全网共同参与运算，性能效率比较低；

2.区块的确认时间难以缩短；

3.容易产生分叉，需要等待多个确认；

4.永远没有最终性，需要检查点机制来弥补最终性；

PoS

权益证明（Proof of Stake，POS）要求用户证明拥有某些数量的货币（即拥有对货币的权益）。

POS 最早在 2012 年 8 月，由点点币（PPCoin，简称 PPC）首次实现。

PPC 在 SHA-256 哈希运算的难度方面引入了币龄（每个币每天产生 1 币龄）的概念，使得难度与交易输入的币龄成反比。在 PPC 中，币龄被定义为币的数量与币所拥有的天数的乘积，这使得币龄能够反映交易时刻用户所拥有的货币权益。

POS 机制简单来说，就是根据你持有货币的量和时间，给你发利息的一个制度。

POW 以算力竞争记账权利；POS 以权益竞争记账权利。

POW 机制是干的越多，得到越多；POS 机制是持有越多，获得越多。

优点：

1.耗能少，不需要像工作量证明机制一样，耗费大量的能源。

2.作恶成本高昂，想要攻击网络的话，必须要有 51%的币龄。

3.达成共识的时间短，网络环境好的话，可实现毫秒级速度。

缺点：

1.持币趋于集中化，因为持有的币越多，时间越长，分配的收益越大，获得的币越多，使币过于集中；

2.流动性变差，持币有收益分配，就没有动力去套现，会屯币不动，开启躺赚模式，导致币的流动性变差。

DPOS

DPoS 委托权益证明机制，是在 PoS 基础上优化而来的。DPOS 与 POS 原理相同，主要区别在于节点选举若干代理人，由代理人验证和记账。

其合规监管、性能、资源消耗和容错性与 PoS 相似。类似于董事会投票，持币者投出一定数量的节点，代理他们进行验证和记账。

DPOS 机制遵从如下几条基本原则：

1. 持股人依据所持股份行使表决权，而不是依赖挖矿竞争记账权。

2. 最大化持股人的盈利。

3. 最小化维护网络安全的费用。

4. 最大化网络的效能。

5. 最小化运行网络的成本（带宽、CPU 等）。

优点：

1. DPOS 机制相比于 POS 大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证。

2. 在一定程度上解决拒绝服务攻击和潜在作恶节点联合作恶问题。

缺点：减弱了去中心化的程度，由选出的代表进行记账，存在一定的中心化控制。

最后我们再来通过一张图，对这三种机制进行一个总结：

最后值得一提的是，没有一种共识机制是完美无缺的，每种共识机制都有其优缺点。这些共识机制都是为解决一些特定的问题而生的，未来说不定也会出现更好的机制来取代现有的共识机制。