## 区块链共识算法（POW、POS、DPOS）

**1、POW：Proof of Work，工作证明**

比特币在Block的生成过程中使用了POW机制，一个符合要求的Block Hash由N个前导零构成，零的个数取决于网络的难度值。要得到合理的Block Hash需要经过大量尝试计算，计算时间取决于机器的哈希运算速度。当某个节点提供出一个合理的Block Hash值，说明该节点确实经过了大量的尝试计算，当然，并不能得出计算次数的绝对值，因为寻找合理hash是一个概率事件。当节点拥有占全网n%的算力时，该节点即有n/100的概率找到Block Hash。

1. **POS：Proof of Stake，股权证明**

POS：也称股权证明，类似于财产储存在银行，这种模式会根据你持有数字货币的量和时间，分配给你相应的利息。

简单来说，就是一个根据你持有货币的量和时间，给你发利息的一个制度，在股权证明POS模式下，有一个名词叫币龄，每个币每天产生1币龄，比如你持有100个币，总共持有了30天，那么，此时你的币龄就为3000，这个时候，如果你发现了一个POS区块，你的币龄就会被清空为0。你每被清空365币龄，你将会从区块中获得0.05个币的利息(假定利息可理解为年利率5%)，那么在这个案例中，利息 = 3000 \* 5% / 365 = 0.41个币。

1. **DPOS：Delegated Proof of Stake，委任权益证明**

比特股的DPoS机制，中文名叫做股份授权证明机制（又称受托人机制），它的原理是让每一个持有比特股的人进行投票，由此产生101位代表 , 我们可以将其理解为101个超级节点或者矿池，而这101个超级节点彼此的权利是完全相等的。从某种角度来看，DPOS有点像是议会制度或人民代表大会制度。如果代表不能履行他们的职责（当轮到他们时，没能生成区块），他们会被除名，网络会选出新的超级节点来取代他们。DPOS的出现最主要还是因为矿机的产生，大量的算力在不了解也不关心比特币的人身上，类似演唱会的黄牛，大量囤票而丝毫不关心演唱会的内容。

以上主要是目前主流的共识算法。

从时间上来看，这个顺序也是按该共识算法从诞生到热门的顺序来定。

对于POW，直接让比特币成为了现实，并投入使用。而POS的存在主要是从经济学上的考虑和创新。而最终由于专业矿工和矿机的存在，让社区对这个标榜去中心化的算法有了实质性的中心化担忧，即传闻60％～70%的算力集中在中国。因此后来又出现DPOS，这种不需要消耗太多额外的算力来进行矿池产出物的分配权益方式。但要说能起到替代作用，DPOS来单独替代POW，POS或者POW＋POS也不太可能，毕竟存在即合理。每种算法都在特定的时间段中有各自的考虑和意义，无论是技术上，还是业务上。

共识最好的设计是模块化,例如Notary，共识算法的选择与应用场景高度相关，可信环境使用paxos 或者raft，带许可的联盟可使用pbft ，非许可链可以是pow，pos，ripple共识等，根据对手方信任度分级，自由选择共识机制，这样才是真的最优。