# 区块链中五种常见共识算法　　你知道几个？

区块链是一种去中心化的分布式账本系统，可以用于登记和发行数字化资产、产权凭证、积分等，并以点对点的方式进行转账、支付和交易。区块链系统与传统中心化系统相比，具有公开透明、不可篡改、防止多重支付等优点，并且不依赖于任何的可信第三方。

由于点对点网络下存在较高的网络延迟，各个节点所观察到的事务先后顺序不可能完全一致。因此，区块链系统需要设计一种机制对在差不多时间内发生的事务的先后顺序进行共识。这种对一个时间窗口内的事务的先后顺序达成共识的算法被称为“ 共识机制 ”。

在区块链这样的分布式账本系统中，保障整个系统的安全性和适应性十分重要，这也是共识算法出现的根本原因。

那么，区块链中常见的共识算法都有哪些呢？


1、POW ：Proof of Work ，工作量证明

POW 是比特币在 Block 的生成过程中使用的一种共识算法， 也可以说是最原始的区块链共识算法了。 POW 工作量证明，简单地理解就是，通过一份证明来确认做过一定量的工作。

在比特币系统中， 得到合理的 Block Hash 需要经过大量尝试计算。 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。

这种工作量证明的形式，在我们日常生活中也十分常见。比如驾照，能拿到驾照，说明你已经进行过为期几个月甚至几年的练车和考试；再比如现在很火的吃鸡和王者荣耀游戏中的 K/D（Kill/Death ）和胜率，

分值越高证明你越厉害，同时也说明你进行了大量的游戏练习和技巧学习。

2、POS：Proof of Stake ，权益证明

由于 POW 机制存在消耗算力巨大、交易确认时间较长，挖矿活动集中容易形成中心化等缺点， 便演进出了 POS 权益证明。POS 简单来说，就是一个根据持有数字货币数量和时间来分配相应利息的制度，类似平时我们在银行中存款。

基于权益证明共识的区块链系统中，参与者的角色是验证者 Validator ，只需要投资系统的数字货币并在特定时间内验证自己是否为下一区块创造者，即可完成下一区块的创建。下一区块创造者是以某种确定的方式来选择，验证者被选中为下一区块创造者的概率与其所拥有的系统中数字货币的数量成正比例，即拥有 300 个币的验证者被选中的概率是拥有 100 个币验证者的 3 倍。

在 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，如果你验证了一个 POS 区块，你的币龄就会被清空为 0，同时从区块中获得相对应的数字货币利息。

这下就很有意思了，持币有利息。并且由于 POS 是在一个有限的空间里完成，不是像 POW 那样在无限空间里寻找，因此无需大量能源消耗。

3、DPOS ：Delegated Proof of Stake ，授权权益证明

DPOS 最早出现在比特股中，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完全相等。

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数字货币的人身上，类似演唱会的黄牛，大量囤票而丝毫不关心演唱会的内容。

DPOS 通过其选择区块生产者和验证节点质量的算法确保了安全性，同时消除了交易需要等待一定数量区块被非信任节点验证的时间消耗。通过减少确认的要求， DPOS 算法大大提高了交易的速度。通过信任少量的诚信节点，可以去除区块签名过程中不必要的步骤。

4、PBFT：Practical Byzantine FaultTolerance，实用拜占庭容错

PBFT 意为实用拜占庭容错算法，该算法由 Miguel Castro（卡斯特罗）和 Barbara Liskov （利斯科夫）在 1999 年提出来，解决了原始拜占庭容错算法效率不高的问题，将算法复杂度由指数级降低到多项式级，使得拜占庭容错算法在实际系统应用中变得可行。

PBFT 是一种状态机副本复制算法，即服务作为状态机进行建模，状态机在分布式系统的不同节点进行副本复制。每个状态机的副本都保存了服务的状态，同时也实现了服务的操作。

将所有的副本组成的集合使用大写字母 R 表示，使用 0 到|R|-1 的整数表示每一个副本。为了描述方便，假设 |R|=3f+1 ，这里 f 是有可能失效的副本的最大个数。 尽管可以存在多于 3f+1 个副本，但是额外的副本除了降低性能之外不能提高可靠性。

5、RAFT，一致性共识算法

RAFT 算法包含三种角色，分别是：跟随者（ follower ），候选人（candidate ）和领导者（ leader ）。集群中的一个节点在某一时刻只能是这三种状态的其中一种，这三种角色可以随着时间和条件的变化而互相转换。

RAFT 算法主要有两个过程： 一个过程是领导者选举， 另一个过程是日志复制，其中日志复制过程会分记录日志和提交数据两个阶段。 RAFT 算法支持最大的容错故障节点是（ N-1 ）/2，其中 N 为集群中总的节点数量。

国外有一个动画介绍 RAFT 算法介绍的很透彻，有兴趣的朋友可以结合动画更好的理解下 RAFT 算法，这里不再做过多介绍。动画链接地址：thesecretlivesofdata.com

上述是目前主要的区块链共识算法，当然还有其他算法，比如 POET：Proof of Elapsed Time 流逝时间量证明， Ripple Consensus 瑞波共识机制等。

每种算法，各有千秋，在特定环境下和时间段上被采用都有各自的考虑和意义。对不同的区块链应用场景而言，适合的算法即为最好的算法。