

区块链从2009年发展至今，已经演变出多种共识。其中，大部分的共识都来自于“BFT家族”和“Proof of X家族”，而“Proof of X家族”是目前公链领域内应用较多的一类共识。

说到“Proof of X”，一般想起来的自然就是目前圈内著名的PoW、PoS和PoC这三大共识——当然目前而言2014年诞生的PoC的影响力还远远不如他的两位老大哥。本篇文章就在此聊一聊这三大共识，究竟孰优孰劣？

- 01 -

PoW，最早的王者

PoW(Proof of Work)作为最早被应用的共识机制，在比特币上获得了巨大成功——它支撑了比特币系统超过10年无重大故障的平稳运行；同时它身上也寄托着中本聪的最初设想——人人皆可挖矿、按劳分配、公平。

尽管在设计之初，PoW的意图是通过代码搭建一套人人参与、权利均等、少数服从多数的制度，但是随着资本的进入和ASIC芯片的面世，号称“人人都可参与”的PoW也已经拔高了准入门槛，而人人权利平等更是无从谈起。除此之外，PoW还存在着一些明显问题：

资源浪费：

PoW共识过程高度依赖区块链网络节点贡献的算力。同时，加密数字货币生态圈已经在资本和设备方面呈现出明显的“军备竞赛”态势，逐渐成为高能耗的资本密集型行业，进一步凸显了资源消耗问题。

算力集中：

根据btc.com数据显示，在资本大量进入的情况下，过去一年矿池算力份额排名前五位的矿池占据了比特币总算力份额的65%，马太效应逐渐显现，而算力过度集中还存在着51%攻击的风险。

性能低：由于需要通过设置一定的工作量来达成共识，PoW的区块链通常处理交易业务的性能非常低，比如比特币TPS理论上最多只有7笔/秒，这也就是说PoW天然受到区块链不可能三角的限制。

为了解决以上弊端，各种各样的共识机制开始走上了台面，其中最有力的挑战者自然就是PoS了。

- 02-

PoS，最有力的挑战者

正因为PoW的势微，主流算法里面，PoS (Proof of Stake) 顺利成章成为了最有力的挑战者。近些年来，基于PoS共识打造的区块链逐渐增多，就连市值长期保持第二的以太坊也计划从PoW转到PoS，而随着Tezos、Cosmos等公链的出现，“Staking经济”一度成为了2019年热词，也受到了交易所和钱包的大力追捧。

客观来说，PoS机制的诞生确实解决了PoW的部分弊端：

1. 以PoS机制开发新区块在一定程度上避免了资源浪费，同时系统区块的自动产出缓解了由于数字资源有限性而产生的通货紧缩；
2. PoS共识机制弱化了中心矿池规模经济的需求，算力集中垄断的情形也得到了缓解，个体竞争力差别相对减小；
3. 就51%攻击而言，PoS共识机制发起一小时攻击的成本远大于PoW共识机制。

然而，PoS也不是万能的，一般而言，它存在着以下问题：

无权益问题 (Nothing at Stake)

：用户在PoS中可以同时在两个分叉上面下注；无论哪一个分叉后面被公认为主链，该用户都可以获得奖励而没有机会成本的损失。这样也在事实上会干扰共识的形成。

被动形成中心化

：PoS主网上线伊始，创世块中分配的Token绝大多数属于数量有限的项目方和早期投资人。因此PoS的区块链很容易被早期用户垄断和支配。

记账节点选择问题：

很多PoS依赖于BFT类算法，但是许多BFT类共识需要确定节点后才能进行下去。记

账节点的不确定还会增大网络分区的概率。

于是，追求完美的人们又推出了许多混合类共识，比如PoW+PoS、DPoS+BFT等。同时出现的当然还有本文即将介绍的第三种共识机制——PoC。

- 03-

PoC，世界上最大的受众群体？

其实早在2014年，PoC就存在了，只是一直没火。这种通过普通硬盘就能挖矿的共识机制，可以说拥有着世界上天然的最大受众群体，门槛也比PoW的ASIC矿机和PoS的硬件要求低得多——

假如每台电脑都可以锁定筹码挖矿获得收益，市场会有多大？

而随着以PoC共识机制为代表的BHD的价格的走高、BHD算力本身的疯涨以及虫哥、Alex等PoC布道者在各地的布道，沉寂已久的PoC共识协议终于又开始火了起来。在经历了逐渐搭建起行业高壁垒、让新矿工望而生畏的四年后，没人知道以“人人挖矿”“节能环保”“重返2012年”口号宣称的PoC挖矿是不是一次新的机会。

那么，PoC到底有哪些优势呢？

1. 相比于POW，POC挖矿将算力替换成硬盘空间，在很大程度的杜绝了POW挖矿造成的资源浪费以及对环境不友好等问题，让矿工从挖矿中赚取更多的利润。
2. PoC只需电脑硬盘即可挖矿。相比于使用其他数字货币使用矿机、显卡、ASIC芯片等挖矿，PoC挖矿投入的成本更低。
3. POC硬盘挖矿，虽然在挖矿的概念上和POW相似，但在设计之初加入了一个抵押机制，抵押机制使得超级矿工出现的概率变得极低，即便有超级矿工出现，得益的也是普通散户，也就是杜绝了超级矿工垄断挖矿的局面。
4. PoC硬盘挖矿，只对硬盘容量有需求，对数据的吞吐并无要求，因此天然杜绝ASIC化。

反过来讲，PoC又有哪些劣势呢？

1.
激励机制可能存在问题。
不谈利益的挖矿和共识机制对用户来说并没有什么吸引力。并且目前的PoC中的Plot文件除了用来挖矿外，并不能用做其他用途。

2.
PoC并没有实现真正的平等。
尽管人人都可挖矿，但是在资本方的加持下，PoC也改变不了越有钱的人挖得越多的命运——当然除非共识完全是根据时间参数来的，不然实现完全平等只能是一句空话。

当然了，这三大共识机制并不能完全代表现有区块链行业，孰优孰劣之争也远未定局，但是对于投资者而言，选择赛道进行站队已经是当务之急，你能看得准吗？

参考文章：火币研究院《共识机制的“权力的游戏”》