共识机制

来源：网络

编辑：**xfli5**

推特：**@xfli5**

目录

区块链要成为一个难以攻破的、公开的、不可篡改数据记录的去中心化诚实可信系统，需要在尽可能短的时间内做到分布式数据记录的安全、明确及不可逆，提供一个最坚实且去中心化的系统。

区块链分布式记账的方式使得每个节点都有一本完整的账本，全网共有。而且随着节点的不断增多，数据越多，账本也越安全，难以摧毁。除此之外，任意一个或者部分节点的账本被篡改，都不可能被全网认同，除非你能控制 51%的节点，即 51%攻击，但是这耗能巨大，几乎是不可能的。

同时随着节点不断增加，**谁来记账，如何选择合适的节点来记账成为一个问题，而制定一个记账节点的选择方式以及规定，让所有节点来遵守这个规定，达成共识**，这就是区块链里面的共识机制。

共识机制是区块链节点就区块信息达成全网一致共识的机制，说得更直白一些就是对于如何选择记账的节点达成共识。共识机制可以保证最新区块被准确添加至区块链、节点存储的区块链信息一致不分叉甚至可以抵御恶意攻击。

比特币作为区块链的第一个应用，它的共识机制 PoW 共识机制曾经一枝独秀，但是随着区块链技术的不断发展，各类不同的共识机制开始不断涌现，各有千秋，各有拥趸。本节中我们介绍几种常见的共识机制：POW、POS 及 DPOS 等。

1POW 共识机制

1.1POW 的作用

2008 年 10 月，中本聪（Satoshi Nakamoto）发表了论文《Bitcoin: A Peer-to-Peer Electronic Cash System》，在论文中设计了区块链的 POW 的共识机制。那 POW 共识机制主要的作用是什么？仔细分析比特币的整体设计思路，使用非对称秘钥解决了电子货币的所有权问题，使用区块时间戳解决了交易的存在性问题，用分布式账本解决了剔除第三方机构后交易的验证问题。最后就剩下双重支付问题，在点对点的分布式系统中，要保障所有节点的数据一致性，就必须引入一种机制来保障。中本聪设计了 POW 共识机制，通过该机制消除双重支付，保证所有节点数据的一致性。

1.2 比特币 POW 实现方式

比特币采用哈希算法，逻辑上是对整个区块进行哈希运算，实际上是对区块头执行哈希运算。也就是说，所谓的区块的哈希值，更确切的表述为区块头的哈希值。区块头大小为 80byte，包含六个字段：version、timestamp、bits、nonce、hashpreblock 及 hashmerkleroot。如此设计首先带来的好处是方便哈希运算，每次运算只需要 80 字节的参数输入，而不是整个区块的数据，同时交易列表的任何变化又能体现在哈希运行结果上。

比特币采用 SHA256 哈希运算，且每次都是连续进行两次 SHA256 运算才能作为最终结果，前一次运算的结果作为后一次运算的输入，即 Double SHA256，一般简称 SHA256D，比特币合格区块判断依据如下：

SHA256D(Version,hashPreBlock,hashMerkleRoot,Timestamp,Bits,Nonce)<=MAXTARGET/Diff

比特币工作量证明（POW）的达成就是矿工计算出来的区块哈希值必须小于目标值。比特币工作量证明的过程，就是通过不停的变换区块头（即尝试不同的nouce 值）作为输入进行 SHA256 哈希运算，找出一个特定格式哈希值的过程（即要求有一定数量的前导 0）。而要求的前导 0 的个数越多，代表难度越大。我们可以把比特币矿工解这道工作量证明迷题的步骤大致归纳如下：

（1）生成用于发行新比特币奖励的 Coinbase 交易，并与当前时间戳的其他所有准备打包进区块的交易组成交易列表，通过 Merkle Tree 算法生成 Merkle Root Hash；

（2）把 Merkle Root Hash 及其他相关五个字段组装成区块头，其中 nonce 置零，将区块头的 80 字节数据（Block Header）作为工作量证明的输入；

（3）不停的变更区块头中的随机数即 nonce 的数值（nonce 初始置零，每次增 1），并对每次变更后的的区块头做双重 SHA256 运算（即 SHA256(SHA256(Block_Header))），将每次结果值与当前网络的目标值做对比，如果小于目标值，则成功搜索到合适的随机数 nonce 并获得该区块的记账权，工作量证明完成。

（4）如果在当前时间戳未成功，则更新时间戳，重复上述步骤，直到找到符合条件的 nonce。

（5）在节点成功找到**满足条件的哈希值**之后，会马上对全网进行广播打包区块。

（6）网络的其他节点收到广播打包区块，会立刻对区块的哈希值及交易数据的有效性进行验证。如果验证通过，则表明已经有节点成功解迷，自己就不再竞争当前区块打包，而是选择接受这个区块，记录到自己的账本中，然后进行下一个区块的竞争猜谜。

2POS 共识机制

2.1POS 共识机制

（1）POS 简介

PoS 最早出现在点点币的创始人 Sunny King 的白皮书中，它的目的就是**为了解决使用 PoW 挖矿出现大量资源浪费的问题**。PoS 共识机制一经提出就引起了广泛关注，Sunny King 也基于 PoW 的基础框架实现了第一代 PoS 区块链：点点币。

PoW 的具体实现有很多版本，但它们大多只是在挖矿算法上有所改进，主体逻辑并没有发生质的变化。PoS 包含了多个变种实现，每个变种往往会涉及区块链代币经济模型的改动，可以说是牵一发而动全身。这些实现有点点币、黑币、未来币、瑞迪币，它们都推动了 PoS 机制的发展，PoS 研究前沿还有以太坊的

Casper ，以及 Cardano 的 Ouroboros。

在 PoS 中有一个叫做**币龄（coinage）**的概念，**币龄就是币数量乘以天数**。比如你有 100 个币，在某个地址上 9 天没有动，那么产生的币龄就是 900，如果你把这个地址上这 100 币转移到任意地址，包括你自己的地址，那么 900 个币龄就在转移过程中被花费了，你的币数量虽然还是 100 个，但是币龄变更为 0。币龄在数据链上就可以取到，任何人都可以验证。

区块链共识机制的第一步就是随机筛选一个记账者，PoW 是通过计算能力来获得记账权，计算能力越强，获得记账权的概率越大。PoS 则将此处的**计算能力更换为财产证明**，就是节点所拥有的币龄越多，获得的记账的概率就越大。

POS 机制就是一个根据你持有某种数字币的量和时间，给你发利息的一个制度。**这其中仍然存在算力挖矿，需要算力解决一个数学难题**。但数学难题的难度和持币者的“币龄”相关。简单来说，持币者持有币的时间越长，难题越简单，挖到币的概率越大。举个例子：在权益证明 POS 模式下，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(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，这下就很有意思了，持币有利息，非常好!(需要注意的是，5%的年利率仅仅是举例，并非每个 POS 模式的币种都是 5%，比如点点币 PPCoin 就是 1%年利率)

POS 机制最核心的逻辑就是——谁持币，谁就有网络的控制权。我们通常说的挖矿，一般都值得是 PoW 的矿机挖矿。当提到 PoS 币的挖矿时候，大家通常使用“**利息**”这个词语来表示。PoS 挖矿让持币者（任何在其区块链钱包里有余额的人），可以用通过持有区块链的证明来进行 PoS 挖矿。其实，PoS 币的挖矿和利息有很大不同，PoS 挖矿的时候，我们的币是还在自己手里的。而我们在银行拿利息的时候，我们已经把钱出借个银行。PoS 模式比银行安全！当然，PoS 挖矿和 PoW 矿机挖矿一样，都可以维护区块链的增长和安全。

实际上，PoS 的发展经历了三个版本，第一个版本是以点点币为代币的 **PoS1.0** 版本，这个版本中使用的是币龄；第二个版本为代表的是黑币（blackcoin），它使用的为 **PoS2.0** 版本，对应这个版本使用的是币数量，相当于是财产证明，后面黑币又升级**到 PoS3.0**，这个版本又回到了币龄。

（2）POS 实现原理

我们知道 PoW 挖矿的基本逻辑和步骤，我们先寻求一个 nonce 小于目标值，这一步用公式可表示为：

Hash (block_header) < Target

从公式中我们可以看到，PoW 下所有矿工的目标值是一样的，只要计算结果哈希小于目标值即可，简化来看就是前导 0 的个数。

而在 PoS 系统中，这个公式变更为：

Hash (block_header) < Target * CoinAge

我们可以看出多引入了一个变量叫做 CoinAge，也就是币龄。这个变量为会造成每个矿工看到的目标值不一样，如果你的币龄越大，也就意味着你的获得答案越容易。这里的 Target 与 PoW 一致，与全网难度成反比，用来控制出块速度的。

例如当前全网的目标是 4369，A 矿工的输入的币龄是 15，那么 A 矿工的目标值为 65535，换算成十六进制就是 0xFFFF，完整的哈希长度假设是 8 位，也就

是 0x0000FFFF。而 B 矿工比较有钱，他输入的币龄是 240，那么 B 矿工的目标值就是 0x000FFFFF。你如果仔细观察肯定会发现，相比 A 矿工的目标值，B 直接少了一个零。即如下：

A 矿工 Hash(block_header) < 0x0000FFFF

B 矿工 Hash(block_header) < 0x000FFFFF

所以 B 矿工获得记账权的概率肯定要比 A 高。

2.2 点点币的 PoS 共识机制

（1）点点币的 PoS 实现原理

点点币 PPCoin 前期采用 PoW 挖矿开采和分配货币，以保证公平。后期采用 PoS 机制，保障网络安全，即拥有 51%货币难度更大，从而防止 51%攻击。PoS 核心概念为币龄，即币数量*持有天数。例如有 10 个币、持有 90 天，即拥有 900 币龄。另外使用币，即意味着币龄的销毁。

点点币的 PoS 证明计算公式为：

proofhash < 币龄 x 目标值

其中 proofhash，对应一组数据的哈希值，即 hash(nStakeModifier + txPrev.block.nTime + txPrev.offset + txPrev.nTime + txPrev.vout.n + nTime)。

币龄即 bnCoinDayWeight，即持有的币数乘以持有币的天数，此处天数最大值为 90 天。目标值，即 bnTarget，用于衡量 PoS 挖矿难度。目标值与难度成反比，目标值越大、难度越小；反之亦然。由公式可见，持有的币龄越大，挖到区块的机会越大。

（2）点点币的 PoS 挖矿难度

点点币使用目标值来衡量挖矿难度，目标值与难度成反比，目标值越大、难度越小；反之亦然。当前区块的目标值与前一个区块目标值、前两个区块的时间间隔有关。计算公式如下：

当前区块目标值 = 前一个区块目标值 x (1007x10x60 + 2x 前两个区块时间间隔) / (1009x10x60)

由公式可见，两个区块目标间隔时间即为 10 分钟。如果前两个区块时间间隔大于 10 分钟，目标值会提高，即当前区块难度会降低。反之，如果前两个区块时间间隔小于 10 分钟，目标值会降低，即当前区块难度会提高。

2.3 黑币的 POS2.0 共识机制

为了进一步巩固 PoS 的安全，2014 年 rat4（Pavel Vasin）提出了 PoS 2.0，并发布了黑币。黑币前 5000 个块，为纯 PoW 阶段；第 5001 个块到第 10000 个块为 PoW 与 PoS 并存阶段，从第 10001 个块及以后为纯 PoS 阶段。黑币首创快速挖矿+低股息发行模式，发行阶段采用 POW 方式，通过算法改进在短时间内无法制造出专用的 GPU 和 AISC 矿机，解决分配不公平的问题。

PoS2.0 相比 PoS 的改进：

1）将币龄从等式中拿掉。新系统采用如下公式计算权益证明：

proofhash < 币数 x 目标值

点点币中，部分节点平时保持离线，只在积累了可观的币龄以后才连线获取利息，然后再次离线。 PoS 2.0 中拿掉币龄，使得积攒币龄的方法不再有效，所有节点必须更多的保持在线，以进行权益累积。越多的节点在线进行权益累积，系统遭遇 51%攻击的可能性就越低。

2）为了防范预先计算攻击，权益修正因子每次均改变。

3）改变时间戳规则，以及哈希算法改用 SHA256。

黑币的 PoS 实现原理

黑币的 PoS 证明计算公式为：

proofhash < 币数 x 目标值

hash(nStakeModifier + txPrev.block.nTime + txPrev.nTime + txPrev.vout.hash + txPrev.vout.n + nTime) < bnTarget * nWeight

其中 proofhash，对应一组数据的哈希值，即 hash(nStakeModifier + txPrev.block.nTime + txPrev.nTime + txPrev.vout.hash + txPrev.vout.n + nTime)。币数即 nWeight，目标值即 bnTarget。

2.4POS 共识机制的问题

（1）币发行问题

PoS 遇到的第一个问题就是币发行的问题。一开始的时候，只有创始区块上有币，意味着只有这一个节点可以挖矿，所以让币分散出去才能让整个网络壮大，那么如何分散出去又是另外一个难题了。

所以早期 PoS 币种基本都采用了分阶段挖矿，很多币种其实是分了阶段的，即第一阶段是 PoW 挖矿，到第二阶段才是 PoS 挖矿。

随着 ERC20 类型的标准合约代币的出现，这个问题被解决了，不再需要第一阶段改成 PoW，也可以将代币分散出去。

（2）币龄问题

由于币龄是与时间挂钩的，这也意味着用户可以无限囤积一定的币，等过了很久再一次性挖矿发起攻击；所以解决方案是：PoS 机制需要引入一个时间上限来控制时间因素的自然增长。

（3）币囤积问题

虽然引入了时间上下限，用户还是倾向于囤积代币，这会造成币流通的不充分；基于此，所以瑞迪币引入了币龄按时间衰减，构造了权益速度证明，鼓励用户流动代币，而不是倾向于囤积代币。

（4）离线攻击

即使引入了时间上下限，时间仍然是自然流动的，也就是可以不需要挖矿节点长时间在线。挖矿是可以离线的，这简直是灾难，所以任意一个 PoS 机制的实践形式都必须避免这个问题，因为网络节点数量的多少直接关系到区块链网络的健壮性。

当然这些问题都不是致命问题，还记得我们一开始提到了 PoS 经历了三个版本，而第二个版本 PoS 2.0 使用的不是币龄，而直接是币的数量。这会造成完全不同的结果，上述第二、三、四问题都不存在了，似乎看起来直接使用币的数量会更好一些，但却出现了整个 PoS 机制的致命问题。

（5）Nothing at Stake

Nothing At Stake, a situation where someone loses nothing when behaving

badly, but stands to gain everything.

Nothing At Stake 问题的本质是“作恶无成本，好处无限多”。具体来讲，是当在 PoS 共识系统出现分叉 (fork) 的情况时，出块节点可以在”不受任何损失“的前提下，同时为多条链出块，从而有可能获得“所有收益”

POS 机制特别容易产生分叉，每个诚实矿工在产生孤块的时候都可以继续挖下去，反正也没什么成本，反正分叉链和主链都可以同时挖，也就是任何持币较少的用户都可以尝试分叉，并且把分叉链广播出去。

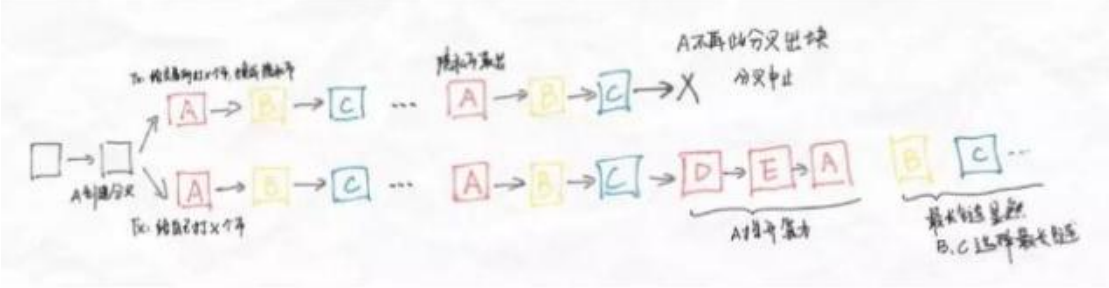
这个时候如果其他诚实矿工看到了，第一反应也是没有成本，那么咱们也来挖吧，说不定什么时候就值钱了，意思就是说任何逐利的矿工并不会使这个系统变得更强壮稳定，而是更加的混乱。**无成本利益问题无论以币龄还是币数量作为 PoS 的参数，都无法避免**。

举个小例子：

这就好比有个窗口，排队既可领钱，当只有一个窗口时，大家会乖乖的排队，每人都有，其乐融融 。但是当第二个窗口出现时。大家知道最终这两个窗口有可能只有一个领到的是“真钱”，另外一个的钱会变成废纸。但排队的你不知道哪个窗口会是发“ 真钱” 的窗口。所以你会怎么做呢？ 你可能会下个跑腿订单帮你分身同时去另外一个窗口排队。但是，在实际 PoS 出块节点时，此时的分身无成本，只是计算机做一个运算而已。

聪明的出块节点会有动力产生新的分叉，支持或发起不合法交易，其他逐利的出块节点会同时在多条链（窗口）上排队出块支持新的分叉。随着时间的推移，分叉越来越多，非法交易，作恶猖狂。区块链将不再是唯一链，所有出块节点没有办法达成共识。

Nothing At Stake 让双花变得更容易。假设 A、B、C 三个出块节点，假如 A 是攻击节点，它在产生分叉时创造两笔交易。一笔将 X 个币发给自己的一个钱包地址，同时在另外一个分叉上将 X 个币发到交易所。B、C 出块节点因 Nothing At Stake 所以同时会在两条分叉链上出块。当交易被交易所确认后， A 将 X 个币出售兑换成隐私币种，移出交易所。之后 A 通过增加质押币量，或创建多个其他出块节点的方式提升出块权重，只在分叉链继续出块。此时最长链很明显，且逐渐拉开差距，会最终成为最长链，A 成功将 X 个币双花。



而 PoW 则没有这样的问题，我们回到 PoW 系统中来看，因为任何的分叉都会造成挖矿成本直接变成负收益，所以这会抵抗分叉的产生，矿工倾向于跟随“最长”的链。

2.5POS 对比 POW

（1）首先，算力的来源不同

在 PoW 挖矿中，决定谁更能挖到矿的是矿机(CPU、显卡、ASIC 等)的运算速度，而在 PoS 中则不同。PoS 挖矿并不需要你去购买额外的挖矿设备，也不会占用大量的运算资源。在 PoS 中，决定谁更可能挖到币的是“币龄”。

（2）其次，出币的数量不同

在 PoW 中，一个块出的币和你所持有的币无关，但在 PoS 中，你用来挖矿的币越多，你这些币的天数越长，你挖到的币也就越多。比如说你有 1000 个币，这些币有 183 天没动用过了，该币的年华利率为 15%，那么你挖到的币数量如下：1000(币数)* 183(天数)* 15%(利率)/365= 74.17(个币)

3DPOS 共识机制

3.1DPOS 由来

我们聊 DPoS 时，为什么要从 BM 聊起呢，其实，这和聊比特币绕不开中本聪一样，DPoS 是 BM 一手创造的。DPoS 不是独立提出的共识算法，而是直接被 BM 应用到比特股项目中，在稳定运行了 3 年多后，又接着被 BM 构造成可复用的区块链工具箱：石墨烯。

虽然应用得很早，但 DPoS 算法直到 2017 年才被 BM 单独拎出来作了一篇“DPoS 技术白皮书”，这期间伴随着比特股、Steemit、EOS 三个项目的依次发布。那么到底 BM 是谁，市场上对这个人的评价为什么富有争议呢？或许我们从了解 BM 开始，才能体会到 DPoS 的精髓。

BM 的本名是 Daniel Larimer，由于他的 GitHub 昵称是 ByteMaster，所以才被称作 BM。BM 是比特股、Steemit、EOS 项目的创始人，与年少成名 V 神的辍学经历不同，BM 2003 年毕业于弗吉尼亚理工学院，获得计算机学士学位，算是正经的科班出身。

BM 曾直言不讳地说到：“我的人生目标就是找到自由市场的方案来保护生命、自由和财产”。他认为要达成这个目标，就必须要从货币开始。2009 年，他怀揣梦想开始了数字货币的事业，他先发现了比特币，于是不遗余力地推广着这个项目。然而在 2010 年，BM 指出中本聪 10 分钟一次的交易确认时间太长了，这样的话，性能会是一个瓶颈，然而这样的想法却遭到了中本聪的暴击：看不懂就算了，我没时间搭理你。

于是，BM 觉得比特币不是希望，便着手开发第一个项目——比特股，同时创造出 DPoS，把自己的高性能共识算法想法形成了实践。在这里，我们可以看出 DPoS 与其他共识机制的第一个区别，就是交易确认时间短。

2014 年，当 V 神还在到处奔走，开始发起以太坊项目的众筹时，当很多项目还是基于比特币的微创新时，比特股就已经横空出世了。所以比特股一跃成为了当时的明星项目，它的口号是“Beyond Bitcoin”，在这里我们可以感受到极强的攻击性和目的性，也正因为如此，日益强大的比特币社区被树在了它的对立面。

比特股一共有 2 个版本，比特股在 1.0 版本之前，某些版本甚至都没有提供向下兼容。虽然后来正式发布了 1.0 版本，似乎并没有改善多少。糟糕的使用体验，庞大的系统资源开销，还是让尝鲜的用户逐渐流失了。这时候 BM 利用了自己手里超过 1/3 的记账节点，在没有达成社区共识的情况下，强行增发了比特股总量。这一招几乎就是比特股项目的灭顶之灾，社区人就此纷纷退出。虽然社区萎靡，BM 还是继续了开发工作，将比特股升级到了 2.0，它的易用性和稳定性勉强可以满足正常使用。随着比特股 2.0 的发布，BM 也同时发布了石墨烯工具箱。尽管在技术上提供了改进，但比特股社区最终选择让 BM 离开比特股项目，比特股回到了另一位币圈大佬——巨蟹的手里。随后比特股的发展陷入了长期的低迷，长期在 2 分，最多到 2 角钱左右，直到去年的牛市，比特股涨到过 2 元人民币。

虽然最终离开了比特股，但是 BM 依然会参与 BTS 紧急 Bug 修复工作。与此同时，BM 又开发了一款旨在颠覆传统互联网媒体行业的项目——Steemit，这也是开辟了基于区块链 Token 内容社区的先例。Steemit 也是基于石墨烯技术的，它非常流行。

2017 年，随着 Steemit 的成熟，BM 宣布退出了 Steemit，开展了下一个项目 EOS。EOS 的目的是要做出区块链行业的操作系统，为开发者提供底层功能，包括并行运算、数据库、账户系统等等。EOS 一经发布，就广受关注，短短五天内，EOS 便筹集到了数亿美金，它的代币销售规模在目前为止是最大的。现阶段的 EOS 超级节点竞选也体现出了 BM 强大的影响力。 EOS 项目影响力也越来越大，BM 因为与 V 神在区块链上的理念不合，也经常互怼，他们争论的重点是二人对于去中心化的前提假设不同，这也造就了两个不同的设计逻辑，所以，两人的争论过程可以说是非常地吸引眼球了。我们从 BM 的个人经历、项目经验、影响力都可以看出 BM 是一个很懂金融的天才式程序员，同时也是一个有点刚愎自用导致与社区矛盾不断的意见领袖。

3.2DPOS 详解

（1）DPOS 基本原理

DPoS 是由**社区选举的可信帐户**（代理人，得票数排行**前 101 位或者 21 位，也可以是其他数字，具体由区块链项目方决定**）来创建区块。为了成为正式代理人，用户要去社区拉票，获得足够多用户的信任。**用户根据自己持有的加密货币数量占总量的百分比来投票**。DPoS 机制类似于股份制公司，普通股民进不了董事会，要投票选举代表代他们做决策。

这 101 个代理人可以理解为 101 个矿池，而**这 101 个矿池彼此的权利是完全相等的**。那些握着加密货币的用户可以随时通过投票更换这些代表（矿池），只要他们提供的算力不稳定，计算机宕机、或者试图利用手中的权力作恶，他们将会立刻被愤怒的选民门踢出整个系统，而后备代表可以随时顶上去。

（2）DPOS 运行机制

DPoS 共识机制引入了“受托人（代理人）”的角色。

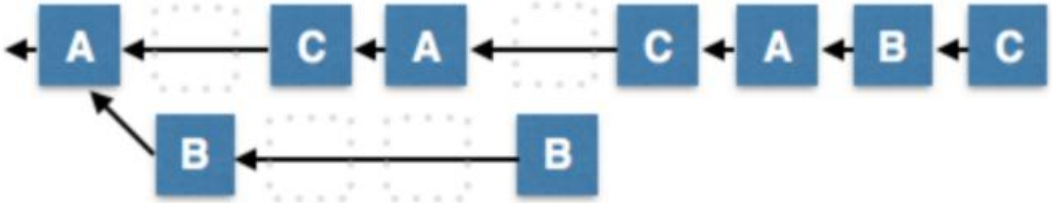
DPoS 的运作机制如下：

1）所有持币者先选出**代理人**负责签署区块：选举过程比较类似由股东会选举出董事会（101 人代表），代替股东会做出日常营运决策。授权董事会后，决策会更有效率 （相较于 PoW 每 10 分钟产生一个区块，DPoS 每 3 秒钟即可产生

一个区块。）

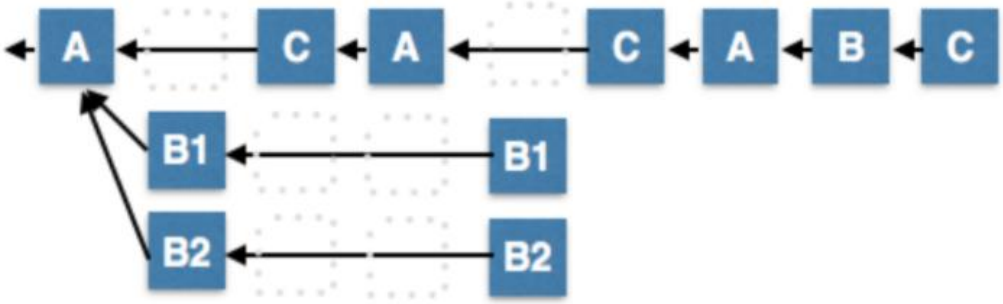
2）与 PoW 相同，**DPoS 的规则也是最长链胜出**。其中每个代理人（共 101 个）必须按照生产排程，轮流产生区块。拿一间工厂作为比方，假设排程排定 A、B、C 分别轮早、中、晚班生产，A 在晚上是无法刷门禁卡进入厂房生产的，同样地，C 在早班时段也是无法进厂房的。

3）今天有一些恶意的节点生产了分叉区块，假设 A、C 都是诚实的节点，只有 B 节点是恶意的，由于 B 产生区块的速度（每 9 秒只能产生 1 个）慢于 A、C 合力产生区块的速度（每 9 秒产生 2 个），根据最长链胜出的规则，诚实的节点还是会胜出。

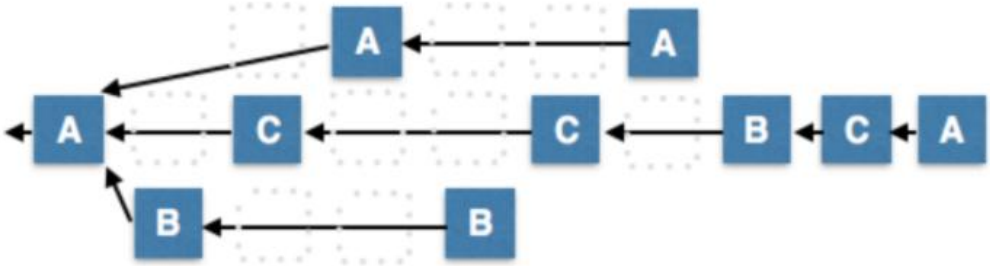


4）同理，因为一个节点要产生重复两个区块的速度必定慢于诚实区块产生的速度，所以根据最长链胜出的规则，诚实的节点还是会胜出。

5）如果今天 A、B、C 三个代理人的网络有段时间是碎片化、各自为政的



呢？在短期内的确有可能三链并行，但一旦网络连结恢复，短链自然会向最长的链回归。



因为受托可签署人数为奇数 101，所以两大派系势均力敌僵持不下的情况不会维持太久，最终势必会有其中一方的链更长。

（3）恶意节点的惩罚机制

注册成为候选代理人需要支付一笔保证金，就像是参与民意代表选举前缴纳的保证金一样，一般来说担任受托人约两周后才可达到损益平衡，这促进了受托人的稳定性，确保至少会挖满两周的矿。

惩罚机制为：不按排程产生区块的节点将在下一轮被投票剔除，也会被没收之前缴纳的保证金。

DPoS 是效率较 PoW 和 PoS 更高、产生区块的速度更快；

虽然恶意的节点将在下一轮投票被踢出，但单个恶意区块在短期仍有可能是有效的状态。短期虽然可能存在恶意区块，但长期下来，可以透过受托人的自主选择来回归链条的有效性

假定现在总共有 4 个受托人 A、B、C，D 加入排程后，只要确认之前的区块中，有 2/3 以上个受托人遵循的链是哪条就可以了。

（4）DPOS 优缺点

优点：

1）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。

2）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。

3）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：

1）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。

2）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。

4BFT-DPOS 共识机制

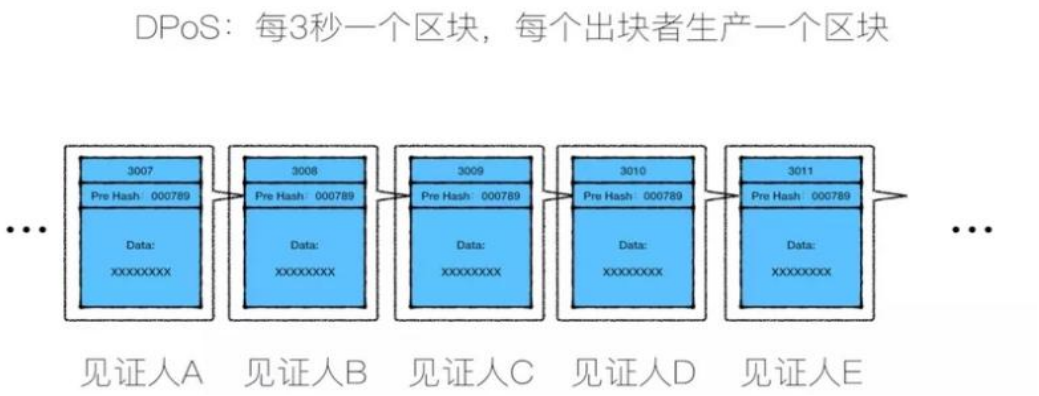
（1）EOS 项目初期采用 DPOS

EOS 项目刚刚发布的时候的共识机制是 DPoS，DPoS（Delegated Proof of Stake），意思是代理权益证明共识机制。相比于比特币的 PoW 机制，DPoS 不用浪费算力资源争夺记账权，其通过赋予 EOS 通证持有人投票权，选出 21 个“超级节点”来担任记账人的角色，保证整个网络的正常运行。21 个超级节点轮流负责记账，每一个区块产生后，会按照顺序传递到下一个超级节点中，第二个超级节

点要负责打包新的区块，同时确认上一区块的内容，当某一区块被至少 2/3 的**其他超级节点（不低于 14 个其他节点）**确认后，该区块将被确认为不可逆区块。

这种共识机制出块速度为 3 秒，交易不可逆需要至少 45 秒（从区块生成到确认）。为什么需要 45 秒呢？因为 DPoS 下，见证人生产一个新区块，才表示他对之前的整条区块链进行了确认，表明这个见证人认可目前的整条链。而一个交易要达到不可逆状态，需要至少 2/3 的其他见证人确认，在 EOS 里就是 14 个见证人。我们假设一个交易被包含在 1000 号区块中，需要其他 14 个见证人轮流出块至 1014 号区块，这样才能“收集”到 15 个见证人（包括区块生成者和其他 14 个见证人）对此交易的确认。至少 2/3 的其他见证人确认的交易，就是不可逆的交易了，这就是 45 秒确认时间的由来。

（2）BFT（Byzantine Fault Tolerance，拜占庭容错算法）



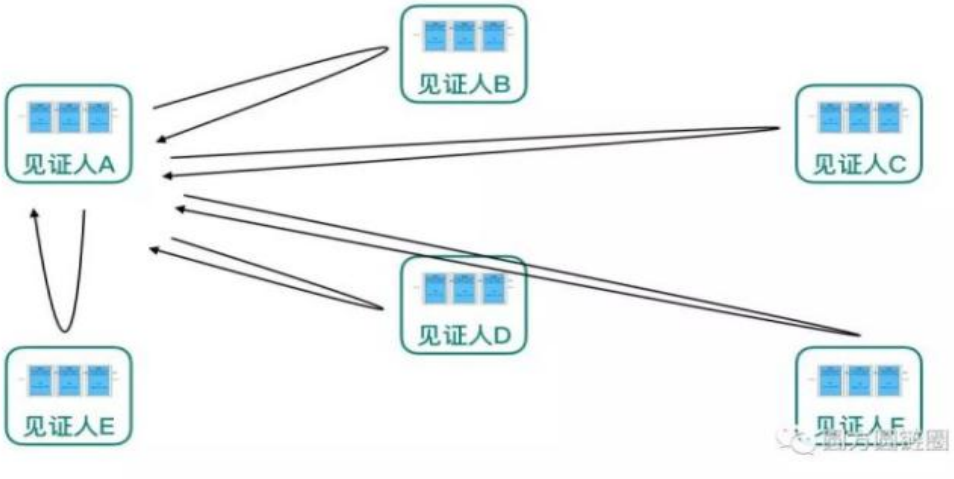
Lamport 对该问题的研究指出“对于拜占庭问题来说，假如节点总数为 N，叛变将军数为 F，则当 N>=3F+1 时，问题才有解。”也就是说当一群节点中恶意节点的数量少于总数量的三分之一时，这群节点便可通过某种协议达成对某一状态的共识，而这种协议就是 BFT 协议。

为了改进传统的 DPoS 算法，我们可以借鉴 BFT（Byzantine Fault Tolerance，拜占庭容错算法）的机制。在传统 DPoS 共识机制中，我们让每个见证人在出块时向全网广播这个区块，但即使其他见证人收到了目前的新区块，也无法对新区块进行确认，需要等待轮到自己出块时，才能通过生产区块来确认之前的区块。

在新的机制下，每个见证人出块时依然全网广播，其他见证人收到新区块后，立即对此区块进行验证，并将验证信息立即反馈出块见证人，不需等待其他见证人自己出块时再确认。

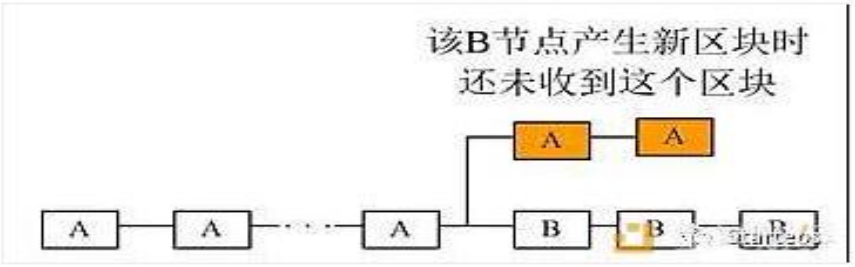
从当前的出块见证人看来，他生产了一个区块，并全网广播，然后陆续收到了其他见证人对此区块的确认，在收到至少 2/3 的其他见证人确认的瞬间，区块（包括其中的交易）就不可逆了。交易确认时间大大缩短，从 45 秒缩短至 3 秒左右（主要为等待生产区块的时间）。这种机制可以称为初级版的 BFT-DPoS 共识机制。

（3）BFT-DPOS



在最早的 EOS 技术白皮书中，EOS 主要采用上述的 DPoS 机制每 3 秒来产生一个区块，而在最新版的 EOS Dwan 3.0 中为使区块链系统有更快的出块速度，EOS 采用了 BFT-DPoS 共识机制从而达到了 0.5 秒的出块间隔。**该机制的具体过程是**：EOS 的持有者通过投票系统对各个超级节点竞选者进行投票，选出 21 个节点为超级节点。然后这 21 个超级节点以自身的网络资源状况商议出一个出块权拥有顺序，在每个超级节点拥有出块权时，以间隔为 0.5 秒(0.5 秒是 EOS 团队通过大量实验测试得出的当前网络状态下可达到的最小的稳定状态下的出块间隔)连续产生 6 个新区块，然后切换到下一个超级节点连续产生之后的 6 个区块。

该方式可以保证一个超级节点可以连续以 0.5 秒的间隔产生区块，因为在同一超级节点产生新区块时不受当前网络状况的影响，但由于网络的延迟很难使得其他节点对已经产生的区块进行确认，使其成为不可逆区块。因此 EOS 引入了 BFT 协议，当超级节点 A 产生第一个新区块后，A 将该区块进行签名并广播给其他超级节点，其他超级节点对该区块进行验证后对其进行签名并返回给 A 节点，当 A 节点收到来自 14 个不同节点签名的区块后，该区块就成为不可逆区块串联到之前的区块链中(以 0.5 秒产生新区块的过程和对区块进行 BFT 协议共识的过程在超级节点中是同时进行的，即确认过程不影响超级节点产生新的区块)。EOS 团队通过大量实验测试，在当前的网络状况下，一个超级节点广播一个新区块并确认的过程可在 1 秒的时间内完成。因此，**每个新区块的产生到成为不可逆区块最多需要 1.5 秒的时间**，这就使得跨链通信的时延大大缩小。因为一个区块链在引入另一条区块链的交易状态时必须等待其成为不可逆交易，所以两个基于 EOS 的区块链在 3 秒钟以内就可以进行一次来回的通信，而以太坊进行类似的通信需要 9 分钟，比特币需要 3 小时以上。



上述过程虽然可以保证同一超级节点产生新区块时可以达到 0.5 秒的间隔，但当切换超级节点产生区块时，由于网络延迟使得上一节点产生的最后几个新区块有可能被该超级节点忽略。为解决此问题，EOS 选用了确定顺序的超级节点轮流出块，比如以纽约(美国东海岸)、芝加哥(美国中部)、洛杉矶(美国西海岸)、日本东京、中国上海这样的顺序，该顺序使得上一节点产生的最后区块传播到下一节点时有最小的延迟，从而避免下一个超级节点忽略上一节点产生的区块。如果是随机定义出块权的超级节点，那么在现有的网络条件下，出块间隔只有控制在 3 秒时才可保证下一节点较大概率上不会忽略上一节点产生的区块。

为了挖掘 EOS 系统的性能，Daniel Larimer 在以上基础上又进行了修改。首先，他将出块速度由 3 秒缩短至 0.5 秒，理论上这样可以极大提升系统性能，但带来了网络延迟问题：0.5 秒的确认时间会导致下一个出块者还没有收到上一个出块者的区块，就该生产下一个区块了，那么下一个出块者会忽略上一个区块，导致区块链分叉（相同区块高度有两个区块）。

比如：中国见证人后面可能就是美国见证人，中美网络延迟有时高达 300ms，很有可能到时美国见证人没有收到中国见证人的区块时，就该出块了，那么中国见证人的区块就会被略过。

为解决这个问题，Daniel Larimer 将**原先的随机出块顺序改为由见证人商议后确定的出块顺序**，这样网络连接延迟较低的见证人之间就可以相邻出块。

比如：日本的见证人后面是中国的见证人，再后面是俄罗斯的见证人，再后面是英国的见证人，再后面是美国的见证人。这样可以大大降低见证人之间的网络延迟。使得 0.5 秒的出块速度有了理论上的可能。

为了保证万无一失，不让任何一个见证人因为网络延迟的意外而被跳过，Daniel Larimer 让每个见证人连续生产 6 个区块，也就是每个见证人还是负责 3 秒的区块生产，但是由最初的只生产 1 个变成生产 6 个。最恶劣的情况下，6 个区块中，最后一个或两个有可能因为网络延迟或其他意外被下一个见证人略过，但 6 个区块中的前几个会有足够的时间传递给下一个见证人。

BFT-DPOS 共识机制总结

（1）21 个超级节点（见证人节点） + 100 个备选见证人节点；

（2）0.5 秒出块时间 + 1 秒全网确认；

（3）每个见证人节点通过协商方式确定各自出块顺序，并且每轮产生 12 个区块以减少网络延时的影响，见证人间按顺序处理交易，可尽量减少地理影响；

（4）当 21 个见证人的 15 个确认交易后，交易即不可逆转；

（5）当达到不可逆转状态后，就无法分叉。

BFT-DPOS 共识机制缺点

（1）不是完全去中心化，可能会有多个中心之间共同串通而损害整个社区利益的行为。

（2）依赖于投票机制.

投票制度其实有以下问题，首先有可能最后投票的参与度会很低，影响投票结果。其次也会可能有这种情况，例如用户把币都存在了交易所，交易所有可能会代替他们去投票，但是用户并不是很在意到底交易所会把票投向何处。也就是说有时候代币持有者的兴趣点和用户的是可能不完全一样的。