第13讲 | 深入区块链技术（五）：PoS共识机制

2018-04-23 陈浩

第13讲 | 深入区块链技术（五）：PoS共识机制
朗读人：黄洲君　10′27″ | 4.79M

上一篇我们讲到了 PoW 共识机制，这一篇我们就来分享另外一种共识机制，PoS 共识机制。

PoS 全称是 Proof of Stake，中文翻译为权益证明。这一篇我们会将 PoS 与 PoW 对比讲解，帮助你加深理解。

PoS 的由来

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。

那到底是什么样的机制导致 PoS 具有这样的特性呢？让我们来看一看。

什么是 PoS?

在讲 PoS 之前，我先来讲一个叫做币龄的概念，币龄这个概念其实很好理解，它的英文是 CoinAge，字面意思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。

我们回过头来看看 PoS 究竟是什么， 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。这有点像公司的股权结构，股权占比大的合伙人话语权越重。

以上算是简述了 PoS 的概念，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。

PoW 早在比特币出现之前就已经应用了，而 PoS 是才是真正意义上为了区块链而创造出来的概念。

PoS 的实现原理

好了，现在我们开始讲解 PoS 的具体实现原理吧。这一部分公式较多，如果你在收听音频，可以点击文稿查看。

通过上一篇我们知道 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，这里就有意思了。

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。

具体代码分析这里就不讲解了，这里需要币龄作为输入，如果我们写示例代码也只是一个简单的参数，PoS 需要放到区块链的语境中才能运作。

PoS 的相关问题

通过上述的介绍我们知道：PoS 似乎完美地解决了 PoW 挖矿资源浪费的问题，甚至还顺带解决了 51% 攻击的问题，这里可以顺便讲一下 51% 攻击是什么，它是指 PoW 矿工如果积累了超过 51% 的算力，则可以一定程度篡改账本。

这里顺便科普一下，什么是 51% 攻击呢，我们发现，矿工挖矿的成本不再是物理设备和电费，而是虚拟代币，它的边际成本几乎为零，本质上 PoS 让挖矿者和使用者合二为一了。

这也意味着如果挖矿者发起 51% 攻击，就需要拥有全网 51% 的币或币龄，这几乎不可能办到，即使你成功地实施了 51% 攻击，那么也意味着作为全网最大的持币大户的你，损失也会最大。

PoS 看起来相当完美，其实并不然，PoS 有很多缺陷。

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，有的叫混合挖矿，其实，我并不同意混合挖矿这个说法，混合就意味着同时。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。

第二个问题是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。

第三个问题是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。

第四个问题是离线攻击，即使引入了时间上下限，时间仍然是自然流动的，也就是可以不需要求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。

这个问题叫做 Nothing at Stake，翻译过来叫做无成本 利益问题。大体的意思在 PoS 系统中做任何事几乎没有成本， 比如在 PoS 系统上挖矿几乎没有成本，这也就意味着分叉非常方便。

方便到什么程度呢，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。

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。

由于以太坊部分采用了 PoS 共识，它的名字叫做 Casper，它必须解决上述无成本 利益问题攻击。所以 Casper 协议要求 PoS 矿工需通过抵押保证金的方法对共识结果进行下注，具体实践结果我们还需要拭目以待。

总结

最后我们来总结一下 PoS 共识机制，PoS 的区块链系统无需外部物理输入，所以它相比 PoW 更为环保不费电，并且矿工就是使用者，这会在一定程度上抵御了 51% 攻击，所以基于 PoS 机制的数字货币属于理想状态的数字货币。

PoS 的缺点是缺乏 工业级的区块链应用，从逻辑上来看有点循环自证明的味道，就是用自己的币来维护系统的安全，而 币的安全性是由系统保证的，所以现阶段 PoS 共识机制往往不是独立运行的，而是混合了 PoW 一起运行，这就 可以弥补 PoS 的缺陷。

PoS 共识机制目前也出现了矿池，也可能会出现中心化挖矿的风险。

虽然 PoS 共识机制未来变数依然很多，但它的可塑性比 PoW 好，技术上的探索空间大，目前 PoS 币种相比较 PoW 币种风险也较高。

那么有哪些区块链项目使用了 PoS 共识机制呢？你可以给我留言，我们一起讨论，感谢你的收听，我们下期再见。

精选留言

陈南平　1
验证节点和账号是如何绑定的？如何将奖励给到节点账户？

您的回复：coinbase交易，由矿工自己填的。

老师，您好，有项目参考，或者资料吗？
我现在使用Tendermint+Ethermint，发现节点和账户是没有绑定的，所以区块奖励它给到了一个0x0000000000000000000000000000000000000000，也就是没有实现节点奖励，按照您的解释应该是它安装后会生成一个coinbase账户，所有的节点奖励会给到这个账户。
2018-04-26

作者回复
是不是没有指定etherbase?
2018-04-30

陈南平　1
验证节点和账号是如何绑定的？如何将奖励给到节点账户？
2018-04-25

作者回复
coinbase交易，由矿工自己填的。
2018-04-26

unite　1
讲的非常好，感谢老师！
2018-04-23

作者回复
谢谢支持呢
2018-04-23

吹牛老爹　0
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。 求解
2018-05-28

作者回复
因为PoS型的代币最开始集中在发行人手里，例如创始块产生100万的代币，那么接下来靠谁来挖呢，因为只有创始地址有币，只能自己挖。所以在1c0和erc20之前，PoS型代币都有一个短暂的PoW阶段，用于让其他人参与，主要目的就是把币分发出去。
2018-05-28

阿痕　0
对于文中提到的PoS节点离线问题的解决办法，如果把节点在线时长作为币龄，是不是可以解决这个问题呢？
2018-04-27

作者回复
区块链无法感知离线在线哦，这个可以作弊的。
2018-04-28

田大猫　0
"比如在 PoS 系统上挖矿几乎没有成本"，这个不太理解。因为币龄的存在，在pos上挖矿，不同的矿工难度不一样，但还是要耗电费的呀。
2018-04-24

作者回复
相比PoW而言，几乎就是零头。
2018-04-26

teletime　0
使用币数量有，无成本利益问题，使用币龄有没有呢？如果有，为什么不直接使用币数量，至少币数量方法，可以解决文中提到的二、三、四。如果没有，为什么币龄方式没有，它有什么内在的成本，拥有它一段时间需要什么成本？
2018-04-24

作者回复
都有无成本利益问题。
2018-04-26

duer　0
听完这两期节目，我最大的感受是，区块链技术对技术和算法的选型和使用I不仅仅是技术决策，更多的是商业逻辑和经济学原理，这在产品设计和技术管理的启发非常大，谢谢老师
2018-04-24

作者回复
谢谢支持呢，送赞\(≧▽≦)/
2018-04-26

栐哥　0
blk,
rdd
dcr是pow+pos
2018-04-24

四正　0
深入浅出！
2018-04-23

ytl　0
以太坊用pos
2018-04-23