POW 共识机制原理及优缺点

16340209 唐育涛

工作量证明（Proof-of-Work，PoW）最早被用于阻止拒绝服务攻击（DDOS）、反垃圾邮件等一些服务滥用的经济对策。后来逐渐发展为一种对应服务与资源滥用、或是阻断服务攻击的经济对策。一般是要求用户进行一些耗时适当的复杂运算，并且答案能被服务方快速验算，以此耗用的时间、设备与能源做为担保成本，以确保服务与资源是被真正的需求所使用。此一概念最早由 Cynthia Dwork 和 Moni Naor 于 1993 年的学术论文提出，而工作量证明一词则是在 1999 年由 Markus Jakobsson 与 Ari Juels.所发表。现时此一技术成为了加密货币的主流共识机制之一。

在了解 POW 共识机制之前，我想先介绍一下为什么要有这种机制，这种机制又用来做什么。这不可避免的要谈到区块链比特币中的一个经典安全问题（Sybil Attack 多重身份攻击/女巫攻击），我们知道区块链的记账是通过各个节投票来决定一个行为是否被认可和记录的。因为在区块链节点中创建多重身份代价极低，但是假设每一个身份都拥有记账权和投票权，那么恶意犯罪将可以通过一个结点创建很多个身份来投票赞成自己的双花行为从而导致双花行为被认可。但这显然是不符合我们想要的结果的，也是威胁着我们账户安全的问题。因此，如何解决女巫攻击问题是我们一定要思考面对的问题，在这种情况下，我们的前辈提出了 POW 机制---通过消耗资源解决一个问题获得投票资格。也就是说并不是每个被创建的身份都能够拥有投票权，只有你消耗资源，通过复杂的运算解决了问题才能获得投票权，并且单个的投票权只能被单个节点所拥有，所以这样的话通过创造多个身份并不会获得多个投票权，你解决了一个问题就只会获得一个

投票权，从而有效的遏制了女巫攻击问题。

接下来我们来介绍一下这个机制，pow 共识机制原理上较为简单，就是一个人出示一个计算结果证明自己，而且这个计算结果在网络中被认为是需要通过一定难度的计算才能得到，但是出示的计算结果却可以很容易进行验证。在 bitcoin 中，使用 pow 机制来生成区块，矿工生成区块后，所有其余节点验证计算结果，更新本地副本。注意，两个特点：1.一定程度的复杂运算 2.易于被验证。这就好比说你要得到某个奖项得到某个证明，你是需要付出大量的时间，花费很大努力才能获得奖项，但是一旦你获得奖项，别人可以通过你的奖杯奖状轻易的知道你是不是真的获奖了，这就是这种机制的重要两个特点，当然还有要求工作过程相对公平，解题答案具有随机公平分布等特点。这种机制需要一定程度的复杂运算来能获得记账权或者投票权，这样就有效的保障了每一个记账权和投票权都是辛苦得来的，并不是同一个结点创建多个伪造身份就能实现的，保障了参与投票的结点的安全性。第二，要易于被验证，是真是假要很容易被验证，如果能够以假乱真，或者真假不分，或者需要大量的运算才能鉴别真假， 那这种机制将变得没有作用，因为每发起一个投票各个结点就需要复杂的运算来验证这个记录是否应该被接受，这将耗费大量的算力和资源，显然不合适。具体到比特币中，矿工被要求综合上一个区块的 Hash 值，上一个区块生成之后的新的验证过的交易内容的 Markle Root 值，再加上猜测的一个随机数 Nonce，一起打包到一个候选新区块，让新区块的 Hash 值小于比特币网络中给定的一个数。这是一道面向全体矿工的“计算题”，这个数越小，计算出来就越难。而只要你解答出来了这个问题并且处于最长链上，那么你将获得一定的比特币和这个区块的记账权，也就是前面所说的投票权。利用 hash 满足了一定的计算量但又容易验证，不易反

推保障了安全性。

我们承认这样的一种极致有效的解决了区块链中的一些问题，而且有它本身的优点：1.容易实现，PoW 在算法复杂度足够高的前提下，基本不需要太多的节点间互相通讯和确认，对代码的实现要求极低，编程的实现是很简单的。2.安全可靠，由于需要通过一定程度的计算才能获得记账权，保障了参与投票的每一个结点不可能是女巫伪造的多重身份，有效避免了女巫攻击问题。

但是这个算法也有自己本身的缺陷问题：1.极大的电量消耗，比特币中大量的矿工进行挖矿从而获得一个区块的记账权，但只有第一个计算出来的矿工的计算是有用的，也就是一个区块被发现的过程中是很多矿工通过蛮力计算的，消耗了大量的重复资源，并且随着区块链结点的增长，维护这些结点的电费将进一步提升。举个例子，2017 年全球矿工用于比特币挖矿的电力已经超过 159 个国家的年度电费输出。显然是极其浪费资源的。2.矿池集中或者说算力集中，51%的攻击问题是区块链中不得不担心的安全问题，矿池或者算力的大程度集中并不是一件好的事情，在矿池集中的情况下，假设 A 巨头具有 31%的算力，B 有 21%的算力，如果他们联合起来造假从而允许双花问题的发生，这对区块链的安全是有极大威胁的。3.自私挖矿，在工作量证明机制下，矿工收益与投入算力成正比；自私挖矿策略的提出被认为是工作量证明机制的重要缺陷，在一定条件下，执行自私策略的矿工可以获取超额利润，造成其他诚实矿工的工作作废。

针对上述问题，我个人也是觉得 PoW+PoS 混合共识。现有的 PoW 机制纯粹依靠算力，导致专业从事挖矿的矿工群体似乎已经和比特币社区完全分离，某些矿池巨大的算力俨然成为个“中心”。严重威胁着区块链的数据安全。现在我们将风险不仅仅控制在 POW 机制上，引入了 POS 机制，POS 的耗能相对减

少了很多，并且在这种情况下要发动51%的攻击，攻击者需要至少接近1/3的PoW 算力 + 1/3 的 PoS 持票量才能发起 51% 算力攻击。大大的提高了51%的难度,削弱了矿池集中产生的威胁,DCR已经用数学计算证实了这一点:在DCR所采取的PoW+PoS混合共识下发动双花攻击的代价,是纯PoW机制下发动双花攻击的25倍！很明显提高了造假成本，提高了安全性。

以上，就是我的个人见解，谢谢！

16340209 唐育涛