PoW共识机制原理及优缺点

PoW共识机制简介

区块链作为一种去中心化的网络，需要解决对各节点的信任问题，使得区块链在一个不可信的的分布式网络下可以不出错地运行，这就需要引入一个共识机制，当不同节点的信息不同时有一个机制来确定哪一个是有效的。目前所主要被使用的 PoW、PoS 等共识机制的本质都是在以证明各个节点提供信息所付出的经济代价或所拥有的经济基础作为限制恶意节点的方法。

中本聪在*Bitcoin: A Peer-to-Peer Electronic Cash System* 中提出了在比特币中 PoW 共识机制的运用，提到了与 Hashcash 的相似性。Hashcash 是一个有 Adam Back 提出的用于限制垃圾邮件和 DoS 攻击的 PoW 系统，其工作原理是查找一个进过哈希后前数个比特为0的值，然后将获得的哈希作为一个戳加入到发送信息的 header 中，以此来证明一个发送者的工作。这种方式的特点是查找的工作量大但是验证的方式简单。

在比特币中，每一个区块的时间戳哈希的产生需要在区块内容中不断加入一个临时值直到存在一个值使得区块的哈希前数位比特为0。每一个区块的时间戳包含前一个区块的时间戳哈希，因此，若要修改一个区块的内容，则需要重做该区块及其后面所有区块的工作。因此，最长的区块链可以被视为工作量累计最多的链。

通过这种方式，比特币的区块验证实质上就是累计算力的验证，当大多数算力由诚信的节点所控制时，它们所建立的链将会以更高的速度扩展。当攻击者想要修改一个区块时，不仅要重做那个区块后所有区块的工作，还必须以更高的速度使得其重新建立的链长于诚信节点的链。而且，比特币的 PoW 计算难度会随着每小时所产生的区块数目的上升而上升，以此来缓解硬件进步所带来的影响。

PoW 共识机制的问题

PoW 对限制恶意节点、保证区块链网络系统的正确性有着重要意义。然而，PoW 也存在着不少潜在的问题，这些问题对包括安全性、社会性以及对环保的考量，这些问题的解决对区块链技术未来的未来发展有着较大影响。具体的几个问题如下：

1. *"Proof-of-Work" Proves Not to Work* 一文中认为 Hashcash 所使用的 PoW 防垃圾邮件的方法并不够合理，反而可能会使正常邮件发送者活动减少。恶意发送者也可通过被骇入的机器进行工作量证明，对于 mailing list 类型的邮件分发PoW 也不太实用。
2. 在*Majority Is Not Enough: Bitcoin Mining Is Vulnerable* 一文中，分析了比特币矿工中 Selfish Mining 行为所带来的可能的问题，使得不诚信矿工可能可以不需要控制51%算力就对比特币网络进行破坏。Selfish Mining 行为指的是矿工在挖出一个区块后不马上将区块发布，而是在后续一定时间时将挖出的所有区块发布，从而使诚信矿工转向新发布的区块后进行挖矿，从而导致诚信矿工损失一定收获。

文中提出一种使得攻击者需要达到25%以上的算力才能使 Selfish Mining 有实际收获的方法。尽管当前比特币没有实体能达到25%以上算力，若最大的两个实体合谋，便可接近33%的算力集中，理论上可以对比特币造成实际损害。而且，也存在很多其他的使用 PoW 共识机制的区块链有着更为严重的算力几种情况，对于这些区块链而言 Selfish Mining 很可能成为一个实际的威胁。

3. PoW 共识机制可能造成大量的计算和能源资源浪费，对矿工而言拥有算力越高可以获得的利益越大，然而对于现实世界而言大量计算获得的符合条件的哈希值是没有实际意义的，耗费大量电力和计算芯片进行挖矿一类的哈希计算是一种资源浪费。
4. PoW 算力越高可能的获利越高的机制吸引大量矿工进行挖矿，可能导致算力的集中，从当前的矿池算力分布中就可以看到前6个最大的矿池就已经占据超过70%的算力，这样的矿池集中化给比特币造成了中心化的威胁。

PoS: 可能的替代方案

对于以上提到的一些 PoW 的问题，Vitalik 在 *Casper the Friendly Finality Gadget* 讲述了使用 Proof of Stake 共识机制来减轻 PoW 的负面外部问题的方法。Casper项目 是以太坊的一个 PoS 协议。在 Casper 中，验证者使用其所锁定的虚拟货币（如以太坊）作为其 stake 的证明，所持币越多的代理者对于新加入的区块的选择有着更大的影响。

对于恶意的节点， Casper 加入了惩罚机制，当某个认证者违反了协议规则，Casper 将会将违反者的全部锁定的 stake 用做惩罚。这是以太坊的实现与其他 PoS 的传统实现不同的地方，避免了恶意节点“Nothing at Stake”的行为。

相比于 PoW，PoS 有着如下的优势：

1. 大幅度减少电力资源消耗，因为 PoS 不再需要耗费大量算力进行大量哈希运算挖矿，可以显著减少算力和电力的浪费
2. 减少 Selfish Mining 一类的在 PoW 中出现的多个实体合谋以破坏区块链网络的情况出现，因为共识代理人与其对加密货币的投资联系更为紧密，违反规则造成的损失更大，遵守协议规则可以更好地获取利益。
3. 中心化效应可能可以得到缓减，PoW 下使用 ASIC 矿机进行专用的高速运算从而形成矿池中心化的方法不能再被利用于 PoS。

然而，PoS 相对 PoW 也有着一些问题：

1. “Rich Get Richer”，因为 PoS 系统根据认证者持有资金的比例分配新资金，少数更为富有的用户将可能获得更多的新资金，从而形成一种不公平的“经济模式”。然而，也有人认为对于 PoW 而言更富有的矿工可更容易地购入更多的矿机进行挖矿，所以同样存在着"Rich Get Richer"的问题。
2. 出现硬分叉时，当前的 stakeholder 都会在两条分叉上相同的币，从而容易默许分叉的存在，而不像 PoW 中硬分叉可以用大量的算力最终仅有一条链继续连接。这导致了纯 PoS 的区块链更容易出现分叉，从而使其可信任度降低。因此，Casper 在验证者对某一链存在争议时（即少于三分之二的验证者同意时）将会使用 PoW 进行操作，但是这样又会使得该系统对 PoW 具有一定依赖性。

总结

PoW 共识机制是区块链起始的时候解决双花、在多条链中选择等问题时的关键，然而 PoW 也存在着许多的局限，这些局限对整个区块链网络的发展，去中心化的维持等都有着影响。PoS 作为一个可能的替代方案解决了 PoW 存在的一些问题，并在一些方面有着更好的优势，但是单纯使用 PoS 的系统却面临着其他存在的问题，在一些时候仍需要使用 PoW 去解决。目前仍然没有一个可以称为对于区块链网络而言完美的共识机制，对于区块链应用而言需要根据实际面临的情况去对所使用的共识机制进行设计。