《区块链原理与技术》Hw2

16340041　陈亚楠

POW 是一种抵御分布式账本中女巫攻击的有效手段。它可以理解为：区块链中的节点花费自己的算力资源来进行“挖矿”，先完成“挖矿”任务的节点可以将自己的工作量证明连同已经整理好的区块一起广播给链中的其他节点。其他节点接收到消息后，首先验证该工作的有效性，如果工作有效并且区块信息也验证无误，则该节点就可以将此区块加入链中，收到奖励并开始下一轮的算力竞赛。如果验证失败，则继续进行当轮的“挖矿”工作。因此，POW 的成功运行需要配合两条约定：将最长的链条视为正确的链条，找到正确的区块后有奖励收益。

除此，“挖矿”过程应具有工作量可以被度量并且结果易于验证的特点，因此 POW 采用了哈希运算的方式，对于特定输入，哈希的结果每次都一样，容易被其他节点进行验证；反之，要生成一个特定的哈希值，只能不断变化输入即“试错”，这也就要求了节点的高算力。

POW 的具体实现方式是对比特币采用哈希算法。逻辑上比特币是对整个区块进行哈希，而真正实现的时候是将区块头中的参数作为哈希函数的部分参数输入。比特币采用 SHA256D 哈希运算，即每次连续进行两次 SHA256 运算作为最终结果，前一次运算的结果作为后一次运算的输入。“挖矿”所做的工作就是不断的尝试一个随机值，直至找到一个哈希结果小于目标值的随机数，一旦该随机数被找到，该节点即竞争到了记账权，可以将自己的区块广播给他人进行验证接收。

POW 共识算法引入了竞争挖矿和分叉处理的机制，降低了达成共识的难度，而且其逻辑简单，容易实现，其安全也有严格的数学论证，保证了各个节点在生成区块并获得报酬的可能性上的公平。

由上面的介绍我们可以很明显的看到，POW 的核心要义为算力越大，挖到“矿”的概率越大，在风险和收益的博弈中必然会导致联合挖矿，大算力矿池可能会对系统的去中心化构成威胁。除此之外，POW 机制也存在严重的效率问题，每个区块的产生需要耗费时间，同时新产生的区块去要后续区块的确认才能保证有效，这需要更长的时间，严重影响了系统的效率。而且矿机日夜运转消耗大量的计算资源、电力资源、人力资源，造成了巨大的浪费。

POW 的威胁主要来自于拥有高算力的矿池，因此我们的解决关键应该是保证挖矿权的足够分散，增加恶意节点掌握大部分竞争力的难度，减少其改写区块链的可能性。目前也已经出现了许多的共识算法，我们可否根据每个算法的特点，实现证明方式的混合化，即将 POW 机制与其他机制进行混合，比如 POS 机制。POS 的安全隐患是活跃的大股东，它与 POW 的共同特点都是决定挖矿的算力或权益可以被少部分人控制。若将他们进行混合，则恶意节点如果想要进行攻击，则必须同时掌握大部分的算力与大部分的股权，这一点的实现还是相对有难度的。而且即使可以被实现，整个区块链系统也会由于过高的中心化而失去了其原本的意义。