POW共识机制相关论文读书报告

学号：16340023

姓名：陈明亮

1. POW共识机制的工作原理

- POW共识机制，是区块链体系中用于证明比特币区块记账合法性的机制，全称为`Proof Of Work`。与其余的中心化体系截然不同的是，比特币为去中心化架构，那么应该由谁来决定每一笔交易的合理性和有效性呢？针对此关键问题，POW共识机制的引入，实现通过消耗一定量计算资源，采用算力运算数学哈希求解问题，若运算成功即可达到对某个交易的合法性证明。

- 工作量证明系统(POW-System)通过采用POW共识机制，在去中心化交易结构(如比特币交易系统)上存在着很大的优势。它通过要求交易双方中的客户端运算解答一个具有难度的问题获得结果，同时接收方却可以很容易地验证结果的正确性的相关结构，采取非对称性方案实现对工作结果的验证。

- 可以将POW共识过程概括为以下五步：

  1. 客户端接收POW难题
  2. 客户端消耗算力计算难题
  3. 客户端得出结果
  4. 客户端发送结果给接收方
  5. 接收方验证结果，给出证明。

  一般情况下，POW问题通常借助非碰撞，不可穷举的目标哈希散列结果，要求客户端通过某种加密哈希算法(一般为SHA256)获取到期望值，实际上可以得知该种问题的解决时间符合随机概率分布，平均计算时间分布在数学期望值附近。

- 在比特币中，这种POW机制算法叫做哈希现金，它被应用在其交易链上，通过赋予交易链上的每一个区块散列值，版本号，时间戳，难度值等等头信息，标识了每一个不同交易列表的特殊性。对应于每一个区块的第一个交易，被称为`CoinBase`，实际上就是*矿工*通过解决特定难题，产生合法区块的过程。可以把其过程大致描述为：

  1. 矿工请求进行`CoinBase`交易，将其他准备打包进此区块的交易组成交易列表，使用MerkleTree算法生成对应的Root哈希值
  2. 将生成的Merkle Root 哈希值作为初始字段装入Block Header，作为POW的输入
  3. 不停地使用算力变更随机数nonce，并且对每一变更后的结果进行加密哈希运算(一般为SHA256)，若结果值与目标条件对应，则解题成功，POW工作完成。

2. POW共识机制存在的优缺点

- POW工作自由度高，只要客户拥有足够的算力资源，都可以参与到工作过程中，解答对应问题即获得货币奖励，充分调动参与者的热度；去中心化的特点也正是POW机制的好处之一。

- POW机制面向工作结果进行验证，不采取监视工作过程的行为，实际上好处是节省时间与空间资源，使整个区块链内部体系简单化，很大程度上也避免了伪造攻击的常见问题，随着内部链网络算力的增强，伪造区块攻击变得更加困难。

- POW实际上单纯地只依靠解决一些毫无意义的数学问题来验证对方工作是否有效，这很大程度上是在消耗全球的资源(可回收率，价值均为0)，每次达成共识需要全链上的每一个节点参与更新，性能效率上无疑是很低的。此外，比特币、以太坊等大型区块链系统已经吸引了大部分的网络算力，这使得其余使用POW机制的区块链系统无法得到充足的算力保证自身安全。

3. POW共识机制问题及相应解决思路

1. POW机制难题不应该只是毫无意义消耗电力资源的随机求解问题，更应该发挥计算过程的价值性，并非把珍贵的电力资源转换成无实体的事物，这是不符合可持续发展环保价值观念的。相应的解决方法为：将难题与实际问题相挂钩，如建筑参数的计算，城市规划方面的困扰等，充分发挥计算资源的有价值性。同时，或许可以开放相应矿工服务器，与其签订另外一种长期协议：Bouns-For-Opening(BFO)，签订期间矿工服务器负责计算某些大型工程的数学问题，或者是其他系统所需要的庞大算力，根据矿工们的算力总和给予奖励。

2. POW共识的完成需要全网的每一个节点上的所有信息进行更新，这无疑会导致交易延时问题。实际上可以通过对节点活跃度进行排序，每一次共识的完成只需要更新那些较为活跃的，排名在前51%上的节点信息，对于其余的节点，当且仅当他们索取相关交易信息时(或者其他可以证明其活跃值到达一定程度的操作)，才主动地去更新他们的节点信息。