PoW 算法

jask

2024-08-24

PoW 算法

什么是工作量证明（Proof Of Work，简称 PoW）呢？你可以这么理解：就是一份证明，用来确认你做过一定量的工作。比如，你的大学毕业证书就是一份工作量证明，证明你通过 4 年的努力完成了相关课程的学习。

区块链如何实现 PoW 算法

区块链也是通过 SHA256 来执行哈希运算的，通过计算出符合指定条件的哈希值，来证明工作量的。因为在区块链中，PoW 算法是基于区块链中的区块信息，进行哈希运算的，所以我先带你回顾一下区块链的相关知识。

区块链的区块，是由区块头、区块体 2 部分组成的，就像下图中的样子。

区块头（Block Head）：区块头主要由上一个区块的哈希值、区块体的哈希值、4 字节的随机数（nonce）等组成的。

区块体（Block Body）：区块包含的交易数据，其中的第一笔交易是 Coinbase 交易，这是一笔激励矿工的特殊交易。

拥有 80 字节固定长度的区块头，就是用于区块链工作量证明的哈希运算中输入字符串，而且通过双重 SHA256 哈希运算（也就是对 SHA256 哈希运算的结果，再执行一次哈希运算），计算出的哈希值，只有小于目标值（target），才是有效的，否则哈希值是无效的，必须重算。

计算出符合条件的哈希值后，矿工就会把这个信息广播给集群中所有其他节点，其他节点验证通过后，会将这个区块加入到自己的区块链中，最终形成一串区块链，就像下图的样子：

算力越强，系统大概率会越先计算出这个哈希值。这也就意味着，如果坏人们掌握了 51% 的算力，就可以发起 51% 攻击，比如，实现双花（Double Spending），也就是说，同一份钱花 2 次。

具体说的话，就是攻击者掌握了较多的算力，能挖掘一条比原链更长的攻击链，并将攻击链向全网广播，这时呢，按照约定，节点将接受更长的链，也就是攻击链，丢弃原链。就像下图的样子：

总结

在比特币的区块链中，PoW 算法，是通过 SHA256 进行哈希运算，计算出符合指定条件的哈希值，来证明工作量的。

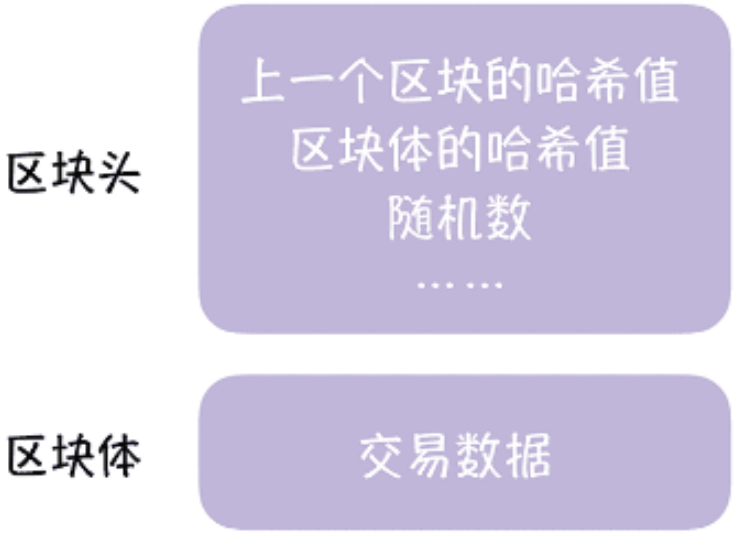

Figure 1: 结构

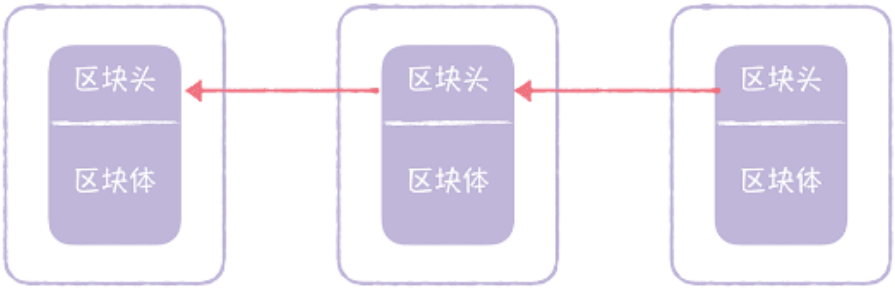

Figure 2: 区块链

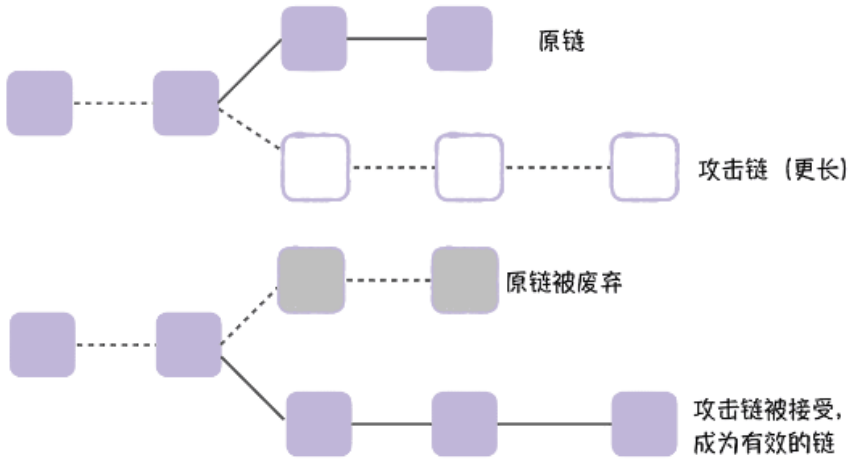

Figure 3: 区块链攻击

51% 攻击，本质是因为比特币的区块链约定了“最长链胜出，其它节点在这条链基础上扩展”，攻击者可以通过优势算力实现对最长链的争夺。

除了通过 PoW 算法，增加坏人作恶的成本，比特币还通过“挖矿得币”奖励好人，最终保持了整个系统的运行稳定。

在比特币中，我们采用了 Raft 算法实现共识，而不是基于 PoW 算法的区块链，那么，就会出现这样的情况，当恶意节点当选为领导者后，他可以不断地告诉其他节点，这些比特币都是我的，按照 Raft 的约定，其他节点也就只能接受这种情况，谁让恶意节点是领导者呢？最终就会出现，所有的比特币都被恶意节点盗走的情况，完全乱套了。