18 以太坊中的GHOST协议

以太坊的平均出块时间是15s，但是底层的网络原理没有考虑实际的拓扑结构，所以实际上的传播速度是非常慢的。导致共识协议有很多的挑战，出现分叉的可能性越来越高了。如果直接和比特币的处理方式一样，把冲突的分叉但没有最后在最长合法链上的区块直接作废，那么以太坊中的矿工挖到作废的区块的可能性就很高，这样就不会有人愿意挖矿了。正常来说，挖矿的期望收益应该是和算力本身成正比的。所以如果以太坊直接作废短的链上的区块的话，对于个体矿工是非常不友好的，因为大的矿池一定可以把自己的链延展成最长合法链。 这个时候就会出现centralization bias，因为零散的矿工也会愿意沿着大矿池的区块继续往下挖，要不然可能就白挖了。

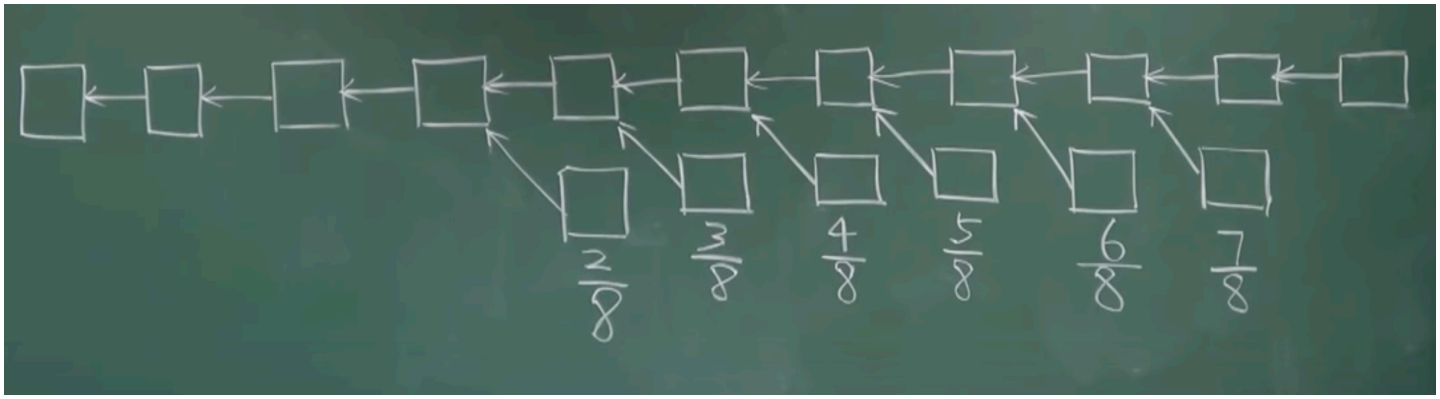
以太坊是基于GHOST协议的共识机制，GHOST协议是出现在以太坊之前的。GHOST机制的核心就是即使挖到的区块最后被放弃了，但是会得到一些安慰和奖励。被放弃的区块我们称之为uncle block（而不是比特币中的orphan block），叔父区块uncle block会得到7/8的出块奖励，当前新发布的这个区块每包含一个叔父区块就可以多得到1/32的出块奖励，每个新发布的区块可以最多包含两个叔父区块。这就是最初版本的GHOST协议。

一个问题是一次只能包含两个叔父区块，如果多于两个叔父区块的话，可能就会有的分支不愿意合并，

还有就是大的矿池可以故意不包含一些叔父区块，这样叔父区块就没有办法得到7/8的出块奖励了，损人不利己。但是因为大型矿池之间往往存在商业竞争，所以可能会这么干。

在以太坊当中，区块是不进行论资排辈的，所以叔父区块不仅仅可以包含叔父级别的区块，祖父或者曾祖父，只要是过往的没有在最长合法链上的区块都可以。这样上述的两个问题都可以得到解决。首先就是即使每个新发布的区块只能包含两个叔父区块，但是后面的新区块可以一直包含过往的区块，所以就可以解决这个问题。第二就是即使大型矿池故意不包含一些叔父区块，但是因为后续的区块也可以继续包含过往的叔父区块，所以问题不大。

但是叔父区块也不能无限制的多少辈都可以，而是只有这下面的六个辈分的叔父区块才可以，而且越久远的叔父区块收获的收益越是少。这样的机制是为了限制大家为了躲避挖矿难度都直接去挖叔父区块，而不是挖正常的区块。而且如果不限制辈分的数量，那么全节点维护所有的区块就太麻烦了。递减的叔父区块的出块奖励是为了鼓励出现分叉之后尽早的进行合并，如果合并的晚了，得到的奖励就会衰减，如果太晚了的话就完全没有出块奖励了。但是这种叔父区块的机制没有办法合并硬分叉（比如说更新一些版本这样的）



在以太坊中，每个区块可以得到一个出块奖励block reward，还有另外一个奖励就是执行智能合约得到的汽油费gas fee。

新发布的区块在包含叔父区块的时候，需要检查这个叔父区块是否满足挖矿难度即可，而不需要检查叔父区块内包含的交易是否合法（因为可能和当前区块或者主链上的交易冲突）。因为新发布的主链上的区块不会执行叔父区块内的交易。

只有分叉后的第一个区块，合并之后才可以得到叔父区块的奖励，分叉上后面的区块是没有叔父区块奖励的。原因在于如果后面的区块都有奖励，会使得分叉攻击的成本降低。我就每次都发动分叉攻击，如果攻击成功了的话，我就可以回滚交易，如果攻击不成功，我还可以得到一些叔父区块的奖励，也不亏。