19 ETH 挖矿算法

Bug bounty，对找到bug的人进行悬赏。比特币是天然的bug bounty，你能找到bug就可以轻松获得比特币。

但比特币饱受争议的点就是必须用ASIC矿机才能挖到矿，这样和比特币最初的设计理念-去中心化是背道而驰的。理想状态下应该是one cpu，one vote（出自于中本聪最早的论文）。

所以ETH在设计挖矿算法的时候是考虑ASIC resistance。一个办法就是使用memory hard mining puzzle。增加需要对内存进行的访问。ASIC芯片相对于普通计算机的优势就是计算能力强，但是在内存访问的性能差距是很小的。所以如果我们能设计一个对内存访问要求很高的mining puzzle，就可以限制ASIC矿机。这个时候可以参考莱特币，LiteCoin。它的哈希函数采用scrpyt，是一个密码学里的哈希函数。

初始一个数组，和一个种子数，然后对种子数取哈希。然后填入数组的第一个位置。然后第二个位置填入第一个位置数的哈希值，然后以此类推，最后得到一个伪随机数数组。解puzzle的时候，先读取第一个起始位置A（数组内任何一个可能的位置），然后经过一系列运算，得到下一个读取的位置B，然后依次往后算。这样做的好处就是如果这个数组开的足够大的话，这个数据就是memory hard，因为如果不保存这个数据，那么计算的复杂度就是非常大的。因为如果不存数组，每次都需要把数据里的哈希值从头到尾算一遍。当然也可以只保存奇数位置，碰到偶数位置就重新算一下。时间复杂度会提高一点，但是所需要的内存就比较少。这就是time-memory trade off。

这个设计的好处是对于矿工而言，这个puzzle是memory hard。但是不好的是，对于轻节点来说，也是memory hard。莱特币在实际使用的过程中，为了照顾轻节点（手机之类的），这个数组只有128KB。但是实际检验，莱特币的设计并没有抵抗GPU和ASIC矿机。但是莱特币解决了冷启动的问题，早期的宣传有cpu就可以挖矿，吸引了很大一批人来挖矿。挖矿的人越多，货币价值越高，也越安全。而且莱特币的出块时间是两分半。比比特币快四倍。

以太坊用的数据集和莱特币很不一样，用了两个数据集。一个是只有16M的cache，还有一个是1G的dataset，DAG。轻节点只需要保存16M的cache就可以了，只有挖矿的矿工才需要保存1G的dataset。这个cache和dataset需要定期增长，现在dataset已经2.5GB了。cache的生成与莱特币类似。初始一个数组，和一个种子数seed，然后对种子数取哈希。然后填入数组的第一个位置。然后第二个位置填入第一个位置数的哈希值，然后以此类推，最后得到一个伪随机数数组。大的dataset是通过小的cache得到的。生成大dateset的时候，先读取第一个起始位置A（数组内任何一个可能的位置），然后经过一系列运算，得到下一个读取的位置B，然后依次往后算。算256次后，将得到的数字填到大dataset的第一个。按照这样的方法将整个大dataset全部填满。求解puzzle的时候不用cache，只用生成出来的大dataset。解puzzle的时候，先读取第一个起始位置A（将block header和nonce取哈希）和它右边的数，然后经过一系列运算，得到下一个读取的位置B和它右边的数，然后依次往后算。循环64次后，得到128个数。最后算出来一个哈希值，和我们挖矿难度的目标阈值比较一下，如果满足就是挖到了。如果不满足，就替换nonce值，然后重新开始计算。

每隔30000个区块会重新生成seed（对原来的seed取哈希），并且利用新的seed生成新的cache。cache的初始大小为16M，每隔30000个区块重新生成时增大初始大小的1/128 -- 128k。DAG的初始大小为1G，每隔30000个区块重新生成时增大初始大小的1/128 -- 8M。

轻节点在验证的时候，需要通过cache来生成dataset中指定index的数。最后验证这个nonce是否能够满足target即可。

如果矿工不保存大数据集的话，那么每次尝试一个新的nonce，就需要重新计算一遍大数据集，时间上非常久。这个算法被称之为ethash。目前来说挖矿还是以GPU为主，ASIC矿机用的十分的少，所以目前来说还是ASIC resistance的。

除此之外，以太坊一直在计划从Proof of Work 转换成Proof of Stake。权益证明是不用挖矿，类似于股份制公司按照股份多少来投票。这对于ASIC芯片的厂商来说是非常致命的，因为ASIC芯片的设计生产是非常费钱的。如果转成proof of stake，那么ASIC芯片就没用了。这样就一直吓唬大家，不断告诉大家我们马上就要转换成proof of stake，就没有人愿意去设计ASIC芯片了。

以太坊中采用了pre-mining的机制，早期预留一些以太坊。就是当以太坊成功之后，把这些预留的币分给早期的创始人和开发者。还有一个是pre-sale，把pre-mining预留的币当成资产进行出售，然后进行后续的开发。如果你非常看好一个加密货币，可以在早期pre-sale的时候进行买入。

也有人认为让普通设备参与挖矿石不安全的，只有像比特币那种用ASIC挖矿才是比较安全的。如果要对比特币的系统发动攻击，必须要投入大量的资金购买ASIC矿机。而且ASIC矿机只能挖一种币。而且一旦攻击成功，大家对于比特币的信心就会大跌，比特币的价格就会下跌。这个时候买矿机的钱就收不回来了。但是如果让普通的计算机都可以挖矿，那么发动攻击的成本就会非常低。因为不需要购买ASIC矿机了。比如说一些大的互联网公司，可以临时把自己的所有服务器全部用来挖矿发动攻击，攻击完了这些服务器还能接着用。这样攻击的成本就非常低了。所以有一部分人认为只有ASIC矿机一统天下才是最安全的。