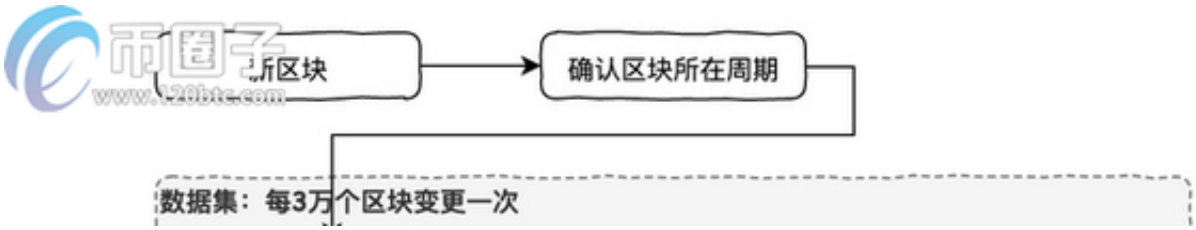
以太坊作为全球数字货币排行榜的第二名，相信大部分投资者对以太坊都有一定的了解，但这些了解大多是在最基础的层面，比如以太坊的价格、发展历史、创始人等。说到以太坊共识算法，可以说是一脸的默默无闻。目前常见的共识算法不多，以太坊属于哪一种？大多数投资者不会&#039；我不知道。那么，以太坊共识算法是什么？下面小编就来详细告诉你什么是以太坊共识算法？

以太坊共识算法是什么？

在以太坊中设计了一套基于POW的Ethash一致性算法。以太坊共识设计的主要思想是设计两个数据集，一大一小。初始大小为：小：16M缓存，大：1G数据集(DAG)

。

设计大数据集和小数据集的目的是大数据集由小缓存通过计算生成，挖掘者为了更快的挖掘只能保存大数据集，避免重复计算浪费时间，而轻节点只保存小缓存即可验证。



大小数据集的生成原理

1。小缓存：

初始大小为16M，以后每30000块改变一次容量大小。

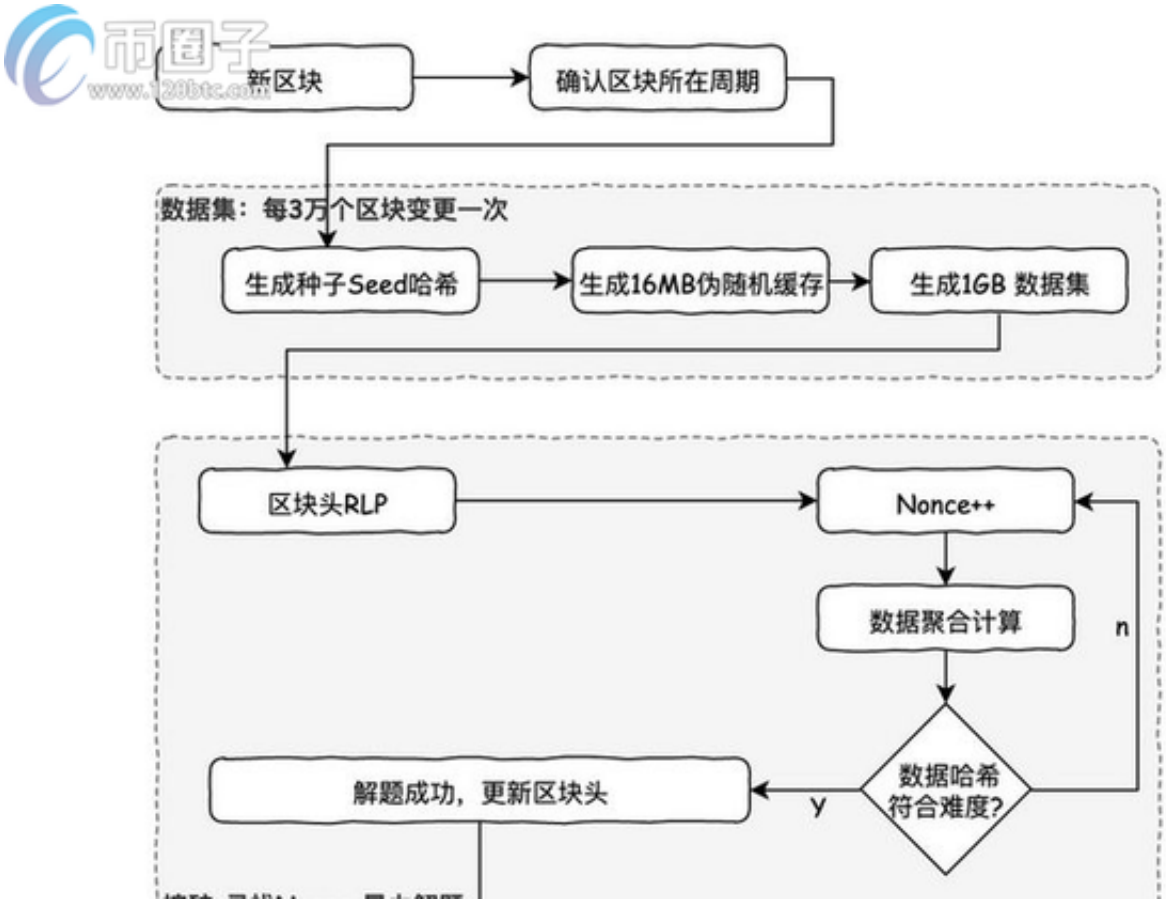
第一个数是通过Seedseed的一些运算得到的。之后，小缓存中的每个数字都是通过哈希前一个数字获得的。一般来说，轻型节点存储这种小型缓存。

2。BigDag:[XY002][XY001]大数据集中的元素都是由一个小cahe计算出来的。在小缓存中，通过伪随机序列获得一个位置的元素A的值，然后通过计算A的hash获得位置B的值，经过256次迭代获得大数据集中的第一个元素，以此类推，直到获得所有DAG元素。

3。采矿过程

以太坊挖矿成功的条件和比特币一样。要找到一个nonce值，需要满足H(header)

当尝试一个随机数nonce时，它在一个大DAG中。，由header和nonce计算出一个初始散列值，并映射到初始位置A，然后是位置A的元素和位置A的元素&#039；与之相邻的是阅读，然后是立场(BandB&#039；)是由(A和A&#039)，以此类推，经过64次迭代。，一共读出128个数字，最后计算这128个数字的哈希值并与目标值进行比较。如果符合



整个挖掘过程如下图所示：

4。验证过程

验证过程类似于比特币，给定一个nonce值，只需要验证一次。

验证过程类似于挖掘过程。对于整个节点，一个大的DAG被保存在存储器中。将64次循环计算后得到的最终哈希值与目标值进行比较；对于轻节点，先通过小缓存计算大DAG再计算，后期过程和整个节点一样。

eth使用的共识协议介绍

以太坊的共识机制有四个阶段，即边疆、家园、大都市、宁静。以太坊前三个阶段用的是力量共识机。。在第四阶段，我们将采用自己的POS机制，命名为Casper投注共识，该机制增加了惩罚机制，并基于POS的思想在记账节点选择验证者。

POW是工作负载证明，这是比特币系统采用的共识机制。。(本文主要讲解以太坊的共识机制)

说到Casper投注共识，首先要说说POS。POS是权益的证明。主要特点是用权益证明代替工作量证明，权益最高的节点实现新增区块，获得激励收益。。POS共识是解决POW共识机制资源浪费和安全缺陷的替代方案。其本质是用权益证明代替POW中基于哈希计算能力的工作量证明，系统中权益最高而非计算能力最高的节点获得块记账权。。股权体现在一个节点对特定金额货币的所有权上，这个节点被称为货币年龄或货币天数。

币龄是特定数量的币和最后一次交易时长的乘积，每一次交易都会消耗特定数量的币龄。。例如，如果某人在一次交易中收到10个硬币，并持有10天，他们将获得100个硬币。然后，在消费5个硬币后，它会消费50个硬币。显然，采用POS共识机制的系统在特定时间点的硬币总数是有限的，长期的硬币持有者倾向于拥有更多的硬币。因此，币龄可以视为其在POS系统中的权益。

投注共识是以太坊下一代共识机制Casper推出的全新概念，属于POS。卡斯帕&#039；美国的共识是逐块达成的。，而不是像POS那样按链。

为了防止验证者在不同的世界提供不同的赌注，还有一个简单而严格的条款：如果你的赌注序列号两次相同，或者你提交了一个Casper无法根据合同处理的赌注。你会失去所有的存款。从这个角度来看，Casper与传统POS的不同之处在于Casper有惩罚机制，让非法节点不仅可以&#039；t通过网络恶意攻击获取交易费用，还要面临押金被没收的风险。

Casper协议下的验证者需要完成两个活动，即封锁和下注。具体如下：

阻塞是一个独立于所有其他时间发生的过程。验证者收集交易，当轮到他们阻止时，他们制作一个阻止并签名。，然后将其发送到网络。下注的过程比较复杂。目前

，卡斯帕&#039；的默认验证者策略旨在模仿传统的拜占庭容错共识：观察其他验证者如何下注，取33%的值并进一步移动到0或1。

确认客户端当前状态的过程如下：首先下载所有的区块和投注，然后利用上述算法形成自己的观点，但不要发表；它只是按顺序在每个高度观察，如果一个块的概率高于0.5，就处理它。，还是跳过吧。在处理完所有块之后，获得的状态可以显示为区块链的当前状态。"

那个&#039；以太坊共识算法是什么。总之，ethash的基本思想类似于比特币的pow。nonce获得的值不断与难度进行比较。如果满足条件，则挖掘成功，否则继续尝试。不同于比特币&#039；ethash通过生成庞大的数据集和限制内存来防止计算能力强的ASIC矿机垄断。