**以太共识算法**

一、Ethash简介

Ethash是以太坊1.0基于POW（工作量证明）的共识引擎，也叫以太的挖矿算法。其前身是Dagger算法和Hashimoto算法。

其思想是通过IO的限制来抵制专用矿机，实现挖矿设备平等，达到去中心化的目的。符合区块链的去中心化精神。

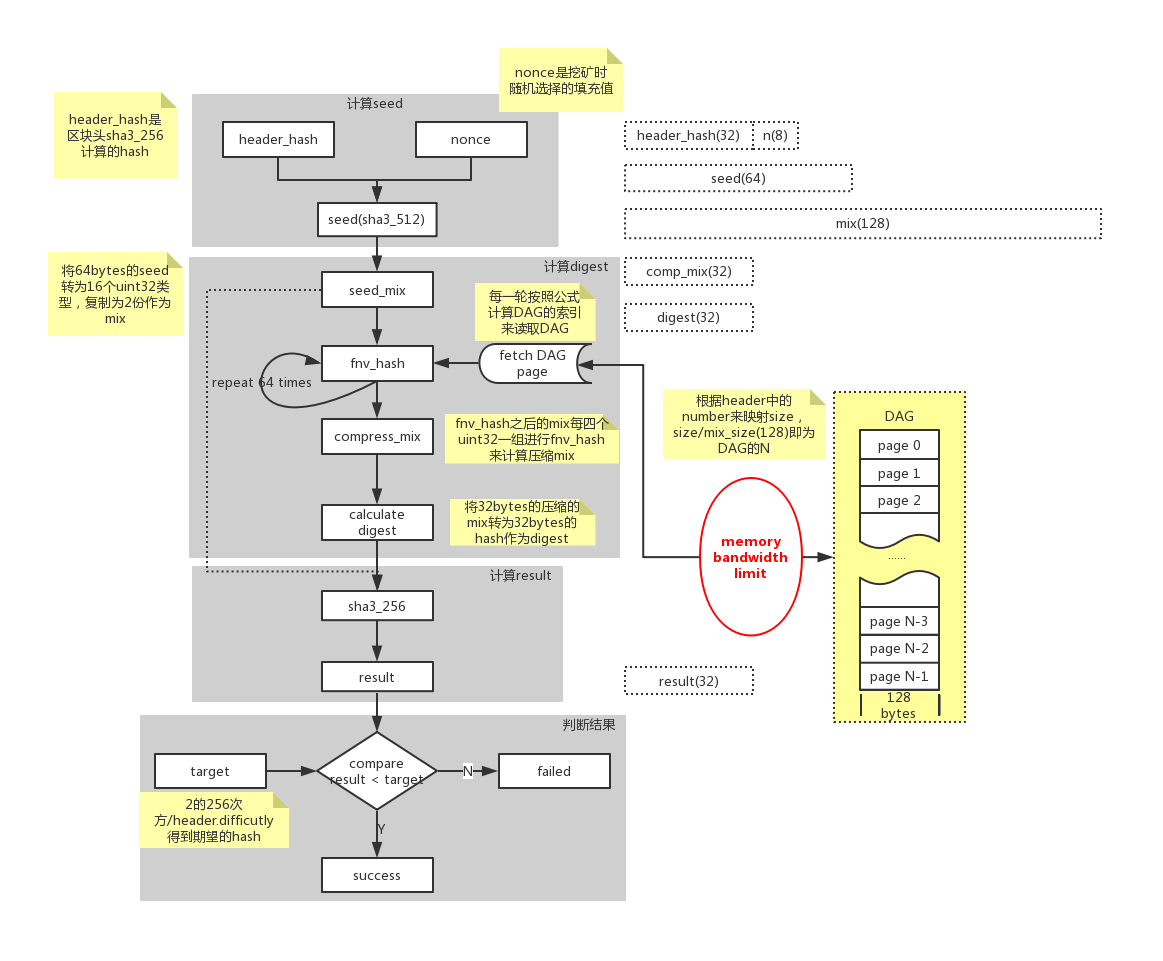
二、Epoch和DAG

在以太，每30000个块为一个epoch，其对应有一个DAG，DAG是一个大约1G大小的数据块，这个DAG需要几个小时的时间才能生成出来。

Ethash算法需要区块头和DAG，通过不停尝试不同的nonce，来计算满足难度值要求的hash。

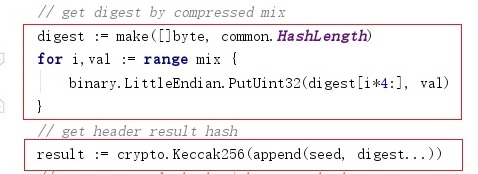
三、Ethash算法

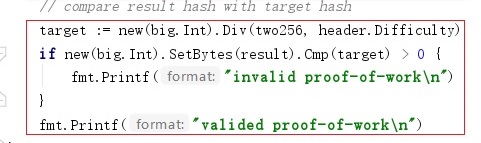
1. 算法流程



1. 区块头和nonce的hash作为seed
2. 按照公式计算一个DAG索引，根据索引从DAG中取数据，将取到的数据和seed进行fnv\_hash作为新的seed
3. 将第2步重复64轮
4. 压缩计算的seed作为digest
5. 将1步计算的seed和第四步计算的digest的hash作为该区块头的hash
6. 将区块头的hash和目标hash(2^256/difficulty)比较，如果小于目标hash则nonce值ok，否则更新nonce值重新开始。
7. 算法代码



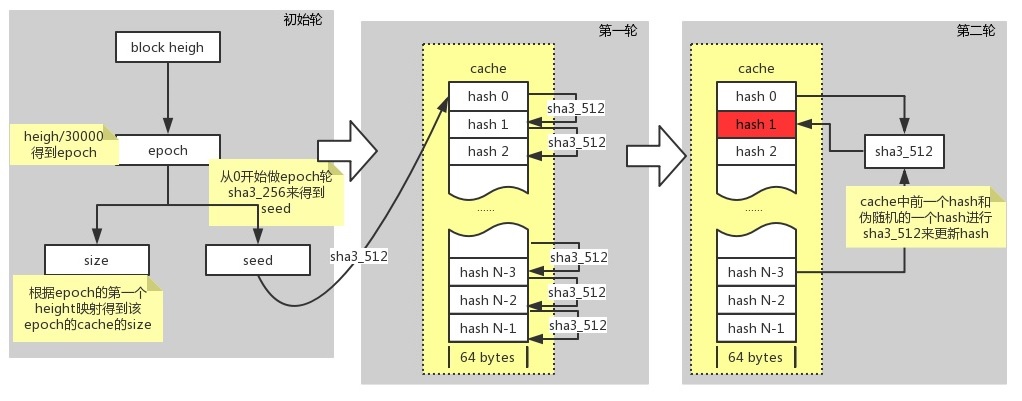




四、DAG的生成

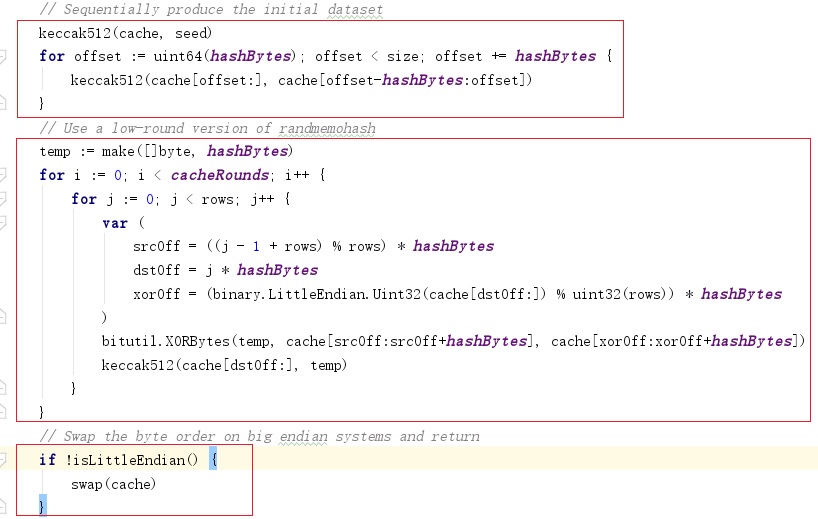
要生成DAG需要先生成一个Cache，再基于Cache生成DAG。

1. DAG Cache的生成

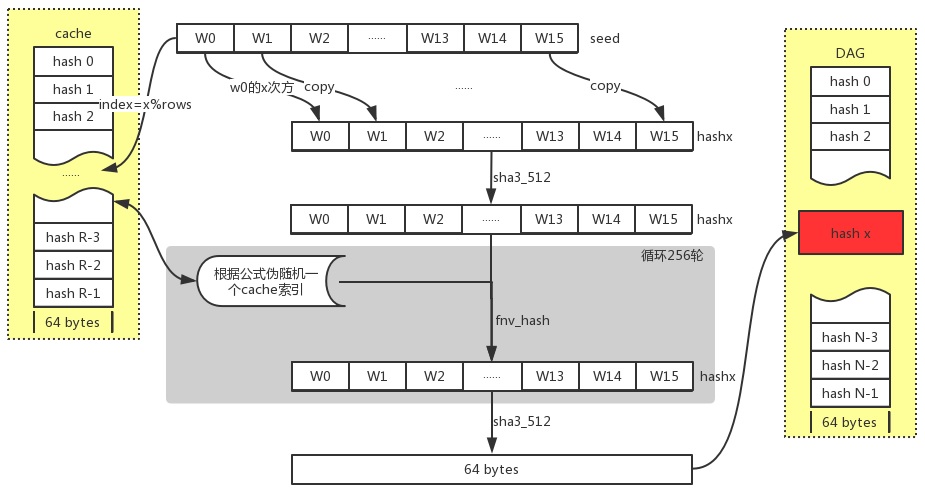


1. 根据当前block的height映射到对应的epoch
2. 生成epoch的seed
3. 将seed的hash为cache中第一个hash，cache中后续每个hash均为前一个hash的hash
4. 将cache中的一个hash更新为其前一个hash和cache中伪随机索引的一个hash的hash
5. 将第4步重复3轮
6. DAG Cache生成代码





1. DAG生成



以计算DAG索引x处的hash（记为hashx）为例：

1. 从Cache中取x/rows(rows为Cache中hash的总个数)的hash作为seed，共16个W（W为一个uint32的整数）
2. 取seed hash的W0计算W0^x（W0的x次方）作为hashx的W0，将seed hash的其他W拷贝到hashx对应的W
3. 计算hashx的hash作为新的hashx
4. 根据公式在Cache中伪随机索引一个hash和hashx计算fnv\_hash作为新的hashx，这步重复256轮
5. 将hashx进行hash得到新的hashx即为DAG索引x处的hash

按照上面的方法计算DAG所有索引位置的hash。

1. DAG生成代码

