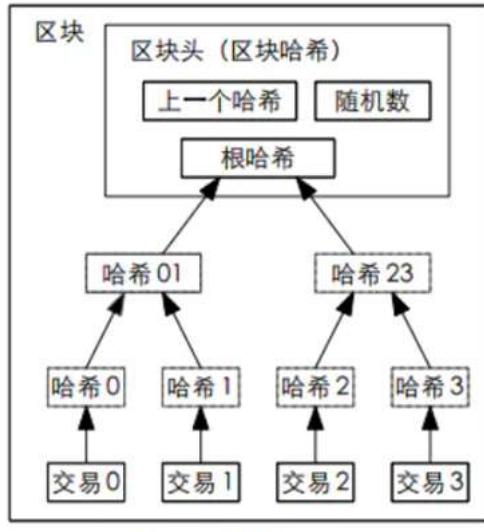


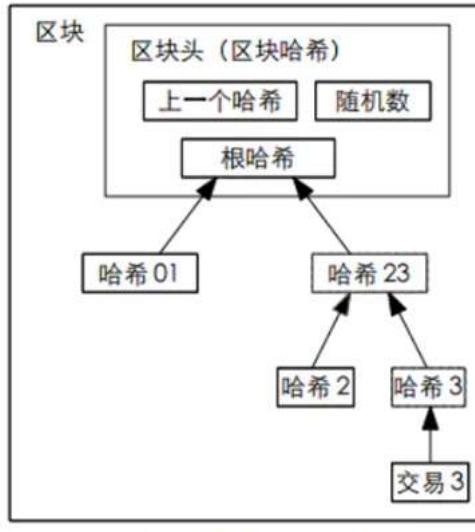
Merkle树

白皮书引入

Merkle树是一种数据结构



交易被哈希进默克尔树



从区块中剪除交易 0-2

CSDN @LEVI_104

图1-1：比特币白皮书插图

生成一个Merkel树

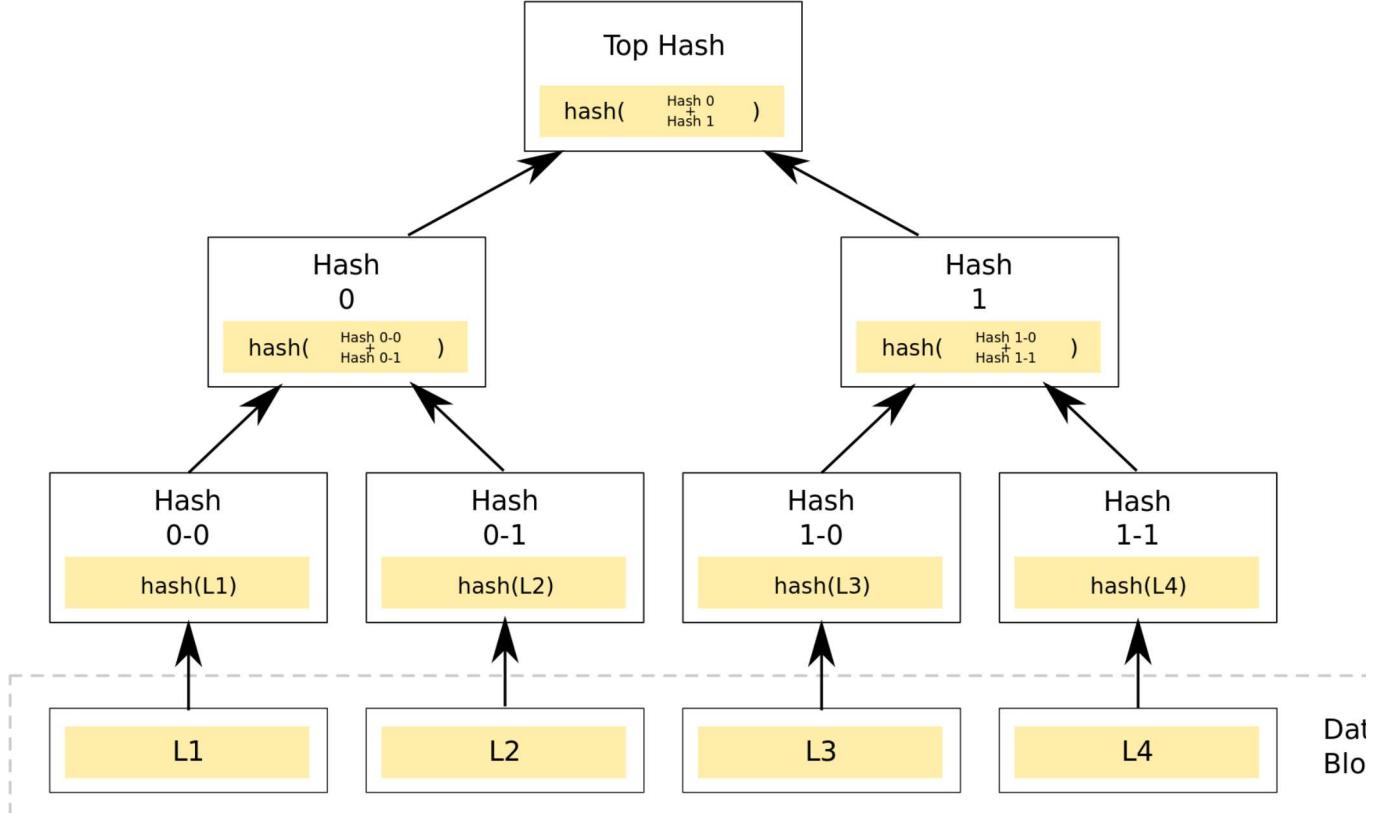


图1-2：来自维基百科插图

分析：自下而上



LEVI_104

1 0 1 0 1 0

1. 我们有四个文件（比特币系统的话就是交易，这个数据结构可以用在各种方面）：L1、L2、L3、L4
2. 四个文件通过hash算法（两个哈希值并起来）得到各自的块：0-0、0-1、1-0、1-1
3. 块之间两两进行hash算法得到新的块：0-0于0-1生成0、1-0于1-1生成1
4. 重复步骤3，得到最终的根节点

注意：hash函数将任意长度的任意类型的数据映射到固定大小的输出。默克尔树汇总一个区块中的所有交易，并生成整个块的哈希验证值，允许用是否包含在该区块中

hash算法

Hash是一个把任意长度的数据映射成固定长度数据的函数。

例如，对于数据完整性校验，最简单的方法是对整个数据做Hash运算得到固定长度的Hash值，然后把得到的Hash值公布在网上，这样用户下载到楼对数据再次进行Hash运算，比较运算结果和网上公布的Hash值进行比较，如果两个Hash值相等，说明下载的数据没有损坏。可以这样做是因为输入微改变就会引起Hash运算结果的面目全非，而且根据Hash值反推原始输入数据的特征是困难的。

hash list

适用于点对点网络数据传输：

在点对点网络中作数据传输的时候，会同时从多个机器上下载数据，而且很多机器可以认为是不稳定或者不可信的。为了校验数据的完整性，更好的文件分割成小的数据块。这样的好处是，如果小块数据在传输过程中损坏了，那么只要重新下载这一快数据就行了，不用重新下载整个文件。如何的数据块是错误的？查看“Merkel树的检索”

Merkel tree和hash list的区别

Merkel tree可以直接下载并立即验证Merkle Tree的一个分支。因为可以将文件切分成小的数据块，这样如果有一块数据损坏，仅仅重新下载这个数了。如果文件非常大，那么Merkle tree和Hash list差不多，但是Merkle tree可以一次下载一个分支，然后立即验证这个分支，如果分支验证通过，就据了。而Hash list只有下载整个hash list才能验证。

Merkel树的检索

为了更好理解，我们假设有A和B两台机器，A需要与B相同目录下有8个文件。这个时候我们就可以通过Merkle Tree来进行快速比较。假设我们在文候每个机器都构建了一个Merkle Tree。具体如下图

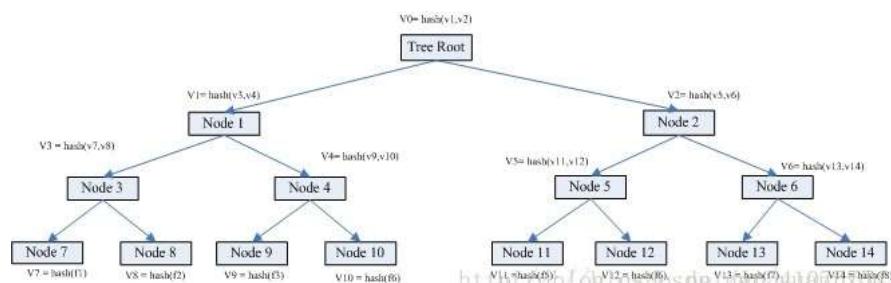


图1-3：网图引用

从上图可得知，叶子节点node7的value = hash(f1)，是f1文件的HASH；而其父节点node3的value = hash(v7, v8)，也就是其子节点node7 node8的值。就是这样表示一个层级运算关系。root节点的value其实是所有叶子节点的value的唯一特征。

假如A上的文件5与B上的不一样。我们怎么通过两个机器的merkle treee信息找到不相同的文件？这个比较检索过程如下：

Step1. 首先比较v0是否相同，如果不相同，检索其孩子node1和node2。

Step2. v1相同，v2不同。检索node2的孩子node5 node6；

Step3. v5不同，v6相同，检索比较node5的孩子node 11 和node 12

Step4. v11不同，v12相同。node 11为叶子节点，获取其目录信息。

Step5. 检索比较完毕。

Merkel树的不可篡改性

在p2p网络下载网络之前，先从可信的源获得文件的Merkle Tree树根。一旦获得了树根，就可以从其他从不可信的源获取Merkle tree。通过可信的树受到的Merkle Tree。如果Merkle Tree是损坏的或者虚假的，就从其他源获得另一个Merkle Tree，直到获得一个与可信树根匹配的Merkle Tree。

修改了树中任意数据，都会导致根节点的值发生改变

Merkel树的高效性

检索理论复杂度是 $\log(N)$

文章知识点与官方知识档案匹配，可进一步学习相关知识

算法技能树 leetcode-树 95-不同的二叉搜索树 II 11465 人正在系统学习中

“相关推荐”对你有帮助么？



关于我们 招贤纳士 商务合作 寻求报道 ☎ 400-660-0108 📩 kefu@csdn.net 💬 在线客服 工作时间 8:30-22:00

公安备案号11010502030143 京ICP备19004658号 京网文〔2020〕1039-165号 经营性网站备案信息 北京互联网违法和不良信息举报中心
家长监护 网络110报警服务 中国互联网举报中心 Chrome商店下载 ©1999-2022北京创新乐知网络技术有限公司 版权与免责声明 版权申诉
出版物许可证 营业执照