IPFS星际联盟 Lv2
2020年01月06日 阅读 44

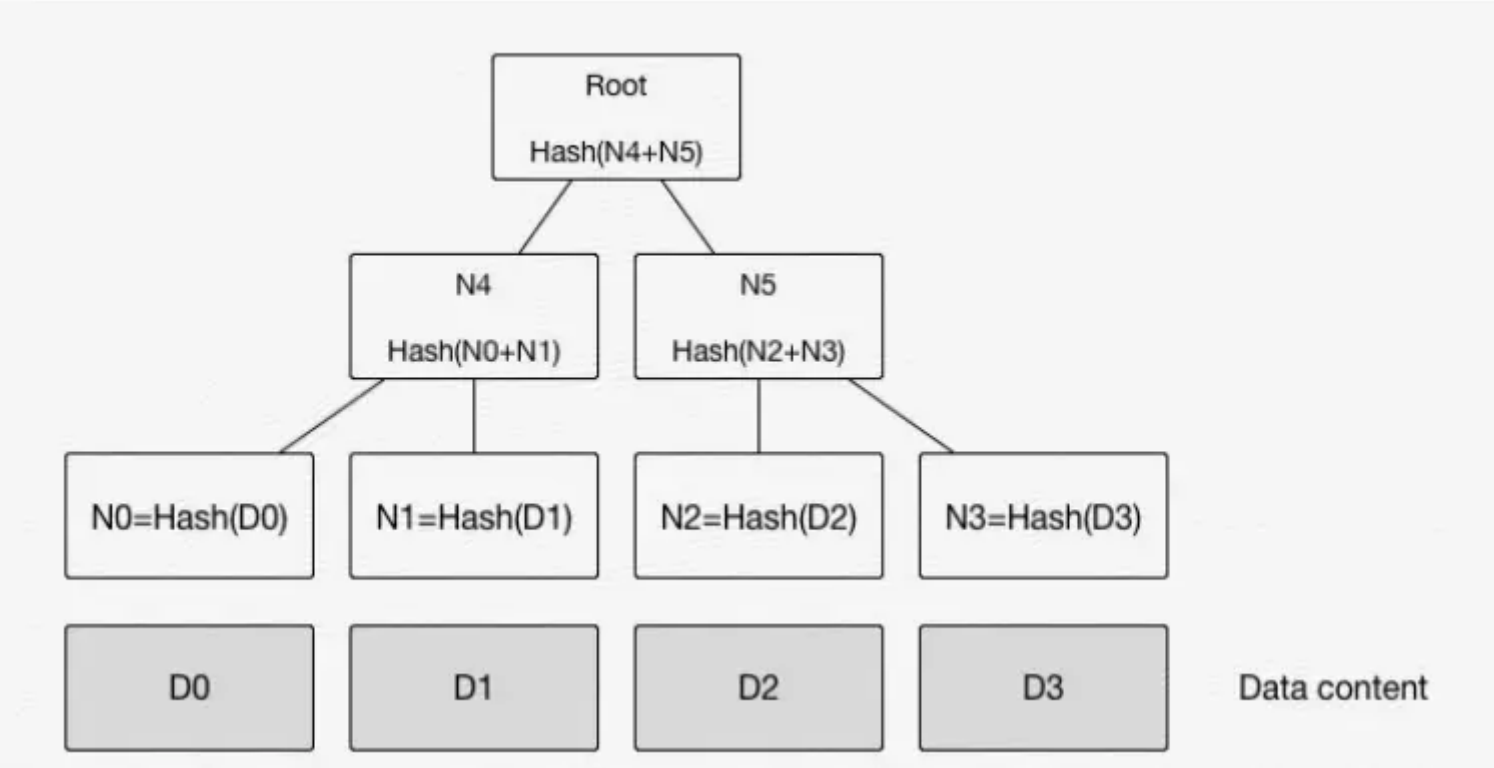
关注

# go-filecoin中的MerkleTree

*本文作者：星际联盟 原创作品，转载请注明出处*

## 什么是MerkleTree

MerkleTree是这样的一种二叉或多叉树，其数据被保存在各叶子节点中，其它节点则保存子节点们的Hash值，整树由下往上，依次对子节点取Hash并存入到父节点中，最后就能使用Root节点中的Hash代表整棵树的数据。 MerkleTree在区块链等分布式系统中有着广泛应用。




上图就是一个实现为二叉树的MerkleTree

## 使用默克尔树的意义

因为在MerkleTree中，每个父节点中保存的数据是对其所有子节点进行Hash运算得到的结果，而Root节点则相当于保存了整棵树的Hash值。所以如果树中任意一个节点的数据发生变化，必然会向上传递导致Root节点的数据发生变化。多数区块链都可以理解为一个透明的分布式账本，上面的数据只要产生，则不能发生改变，MerkleTree的特性正适合用于在区块链中验证区块中数据是否发生了改变，维护区块链的不可篡改性。

## 详说MerkleTree的特性

上面简述了在区块链系统中MerkleTree存在的必要性。接下来我们详细列举一下MerkleTree的特性

- **防篡改**

> 正如上一节所说，任意一个叶子节点的细微变动，都会导致根节点随之改变，可以用来判断保存的数据是否被篡改

- **快速检测修改**

> 只是可以检测数据是否发生了变动，我们有很多其它的方法。最简单地比如，直接对数据进行Hash运算，把得到的值与之前计算的值进行比较，不一样就说明数据必然被修改。但这样就会导致算法效率低下，因为这样会产生O(n)的复杂度，即保存的数据越多，要运行的Hash次数也越多。 而在MerkleTree中，如果节点D1中数据被修改，父节点P1的值就会发生变化，P1的父节点G1也会改变，最后Root节点变动，沿着D0 - > N0 - > N4->Root这条路径即可快速定位到实际发生改变的数据块D9，算法复杂度为O(logn)，效率会高很多。

- **零知识证明**

> 零知识证明指证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。比如上图中若要证明某个数据（D0.....D3）中包括给定内容 D0，构造一个MerkleTree，公布 N0，N1，N4，Root，D0拥有者就可以很容易检测 D0 的存在，但不需要知道其它内容。

go-filecoin中区块是保存在MerkleDAG中，将MerkleDAG抽象为一种接口，定义如下

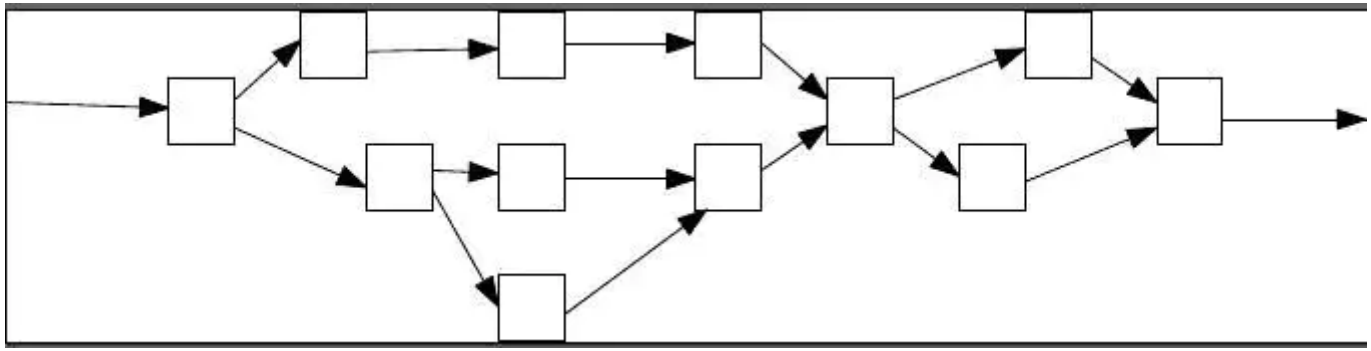
```
// DAGService is an IPFS Merkle DAG service.
type DAGService interface {
    NodeGetter
    NodeAdder

    // Remove removes a node from this DAG.
    //
    // Remove returns no error if the requested node is not present in this DAG.
    Remove(context.Context, cid.Cid) error

    // RemoveMany removes many nodes from this DAG.
    //
    // It returns success even if the nodes were not present in the DAG.
    RemoveMany(context.Context, []cid.Cid) error
}
```

DAGService提供了获取、添加、删除节点的功能。

MerkleDAG跟MerkleTree的主要区别包括：MerkleDAG不需要进行树的平衡操作，非叶子节点允许包含数据等；MerkleTree主要用于验证，如验证数字签名，以及比特币Merkle Proof。

MerkleDAG拥有如下的功能： • 内容寻址：使用多重哈希来唯一识别一个数据块的内容 • 防篡改：可以方便的检查哈希值来确认数据是否被篡改 • 去重：由于内容相同的数据块哈希是相同的，可以很容去掉重复的数据，节省存储空间

下图显示了一个保存区块的DAG：



**关注下面的标签，发现更多相似文章**

区块链

**IPFS星际联盟** Lv2 星驰（上海）网络科技有限公司
发布了 27 篇专栏 · 获得点赞 87 · 获得阅读 3,074

关注



评论

输入评论...

专栏 · 起个帅的名 · 3天前 · 区块链

## 以太坊智能合约开发实战

1

专栏 · flydean · 9天前 · 区块链

## 区块链从入门到放弃系列教程-涵盖密码学,超级账本,以太坊,Libra,比特币等持续更新

7 2

专栏 · 十壹 · 25天前 · 区块链

## 前端er应该知道的区块链技术

7

专栏 · 林冠宏_指尖下的幽灵 · 7月前 · 前端 / 区块链

## 从区块链技术研发者的角度，说说我的区块链从业经历和对它的理解

64 54

专栏 · 胡七筒 · 1年前 · Node.js / Go

## 程序猿生存指南-25 逃离帝都

106 72

专栏 · flydean · 1月前 · 区块链

稀土君 · 1年前 · 区块链

## PRS Dapp 线上征集评选活动

专栏 · 胡七筒 · 1年前 · MySQL / Redis

## 程序猿生存指南-14 钱迷心窍

103 82