MERKLE TREE在区块链中的应用

- 关于Merkle Tree的详细概念，请大家阅读以下文章：

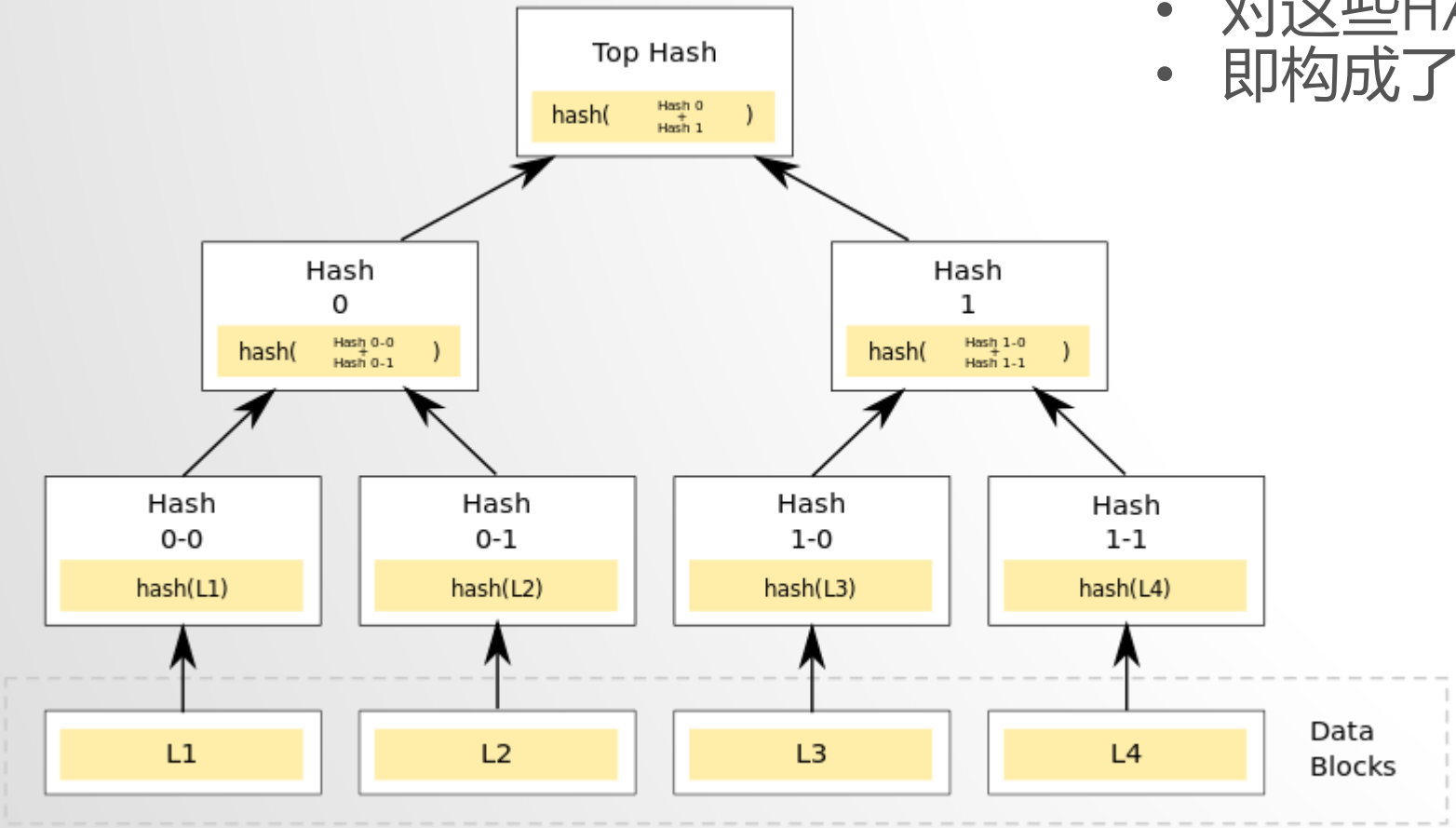
http://blog.csdn.net/wo541075754/article/details/54632929

https://en.wikipedia.org/wiki/Merkle_tree

http://www.jianshu.com/p/458e5890662f

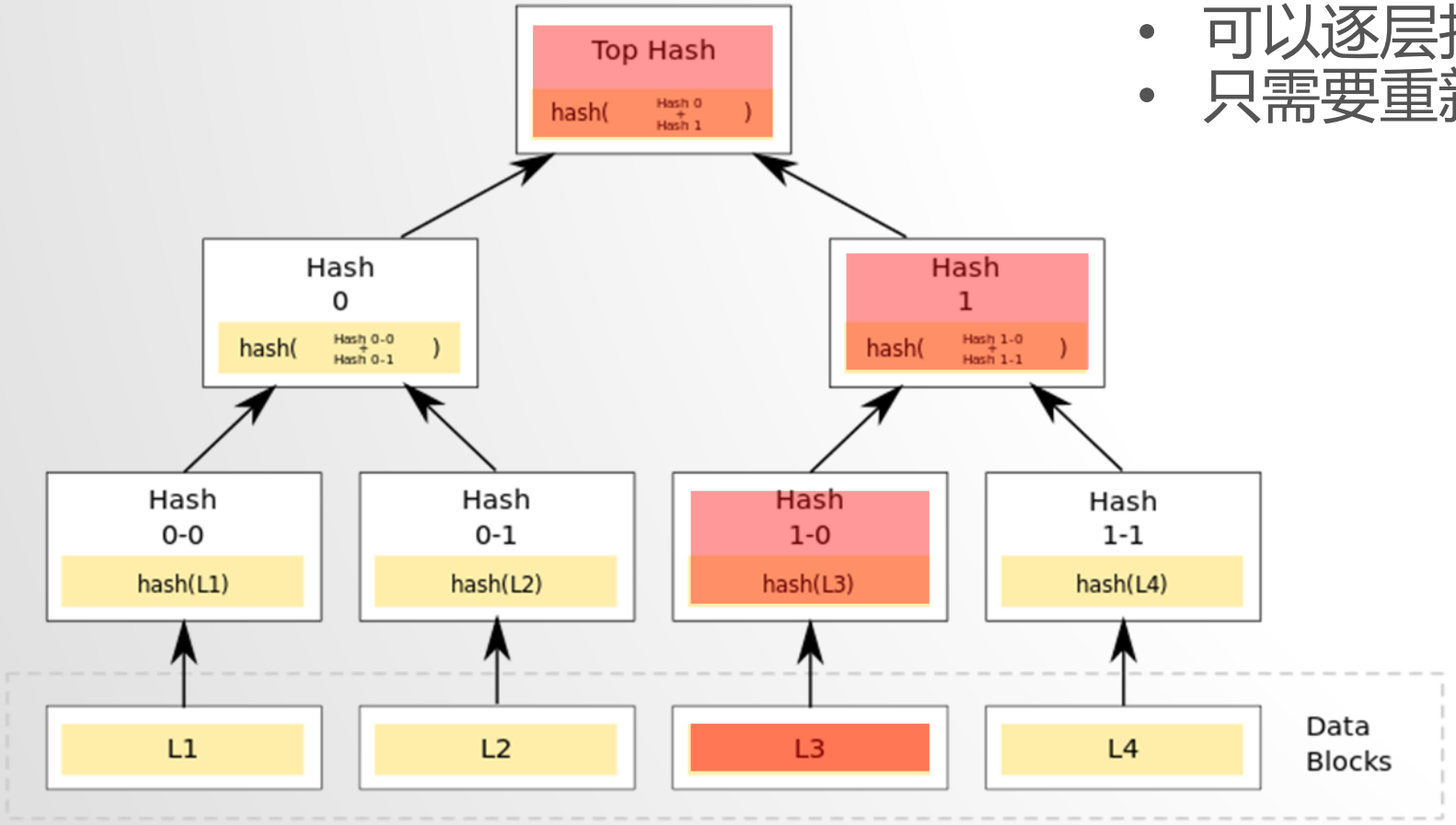
- 本文仅用于帮助大家理解Merkle Tree，
  以及Merkle Tree在区块链中的应用

- 对一些数据进行分片
- 每段数据取HASH
- 对这些HASH进行两两取HASH
- 即构成了一个MerkleTree



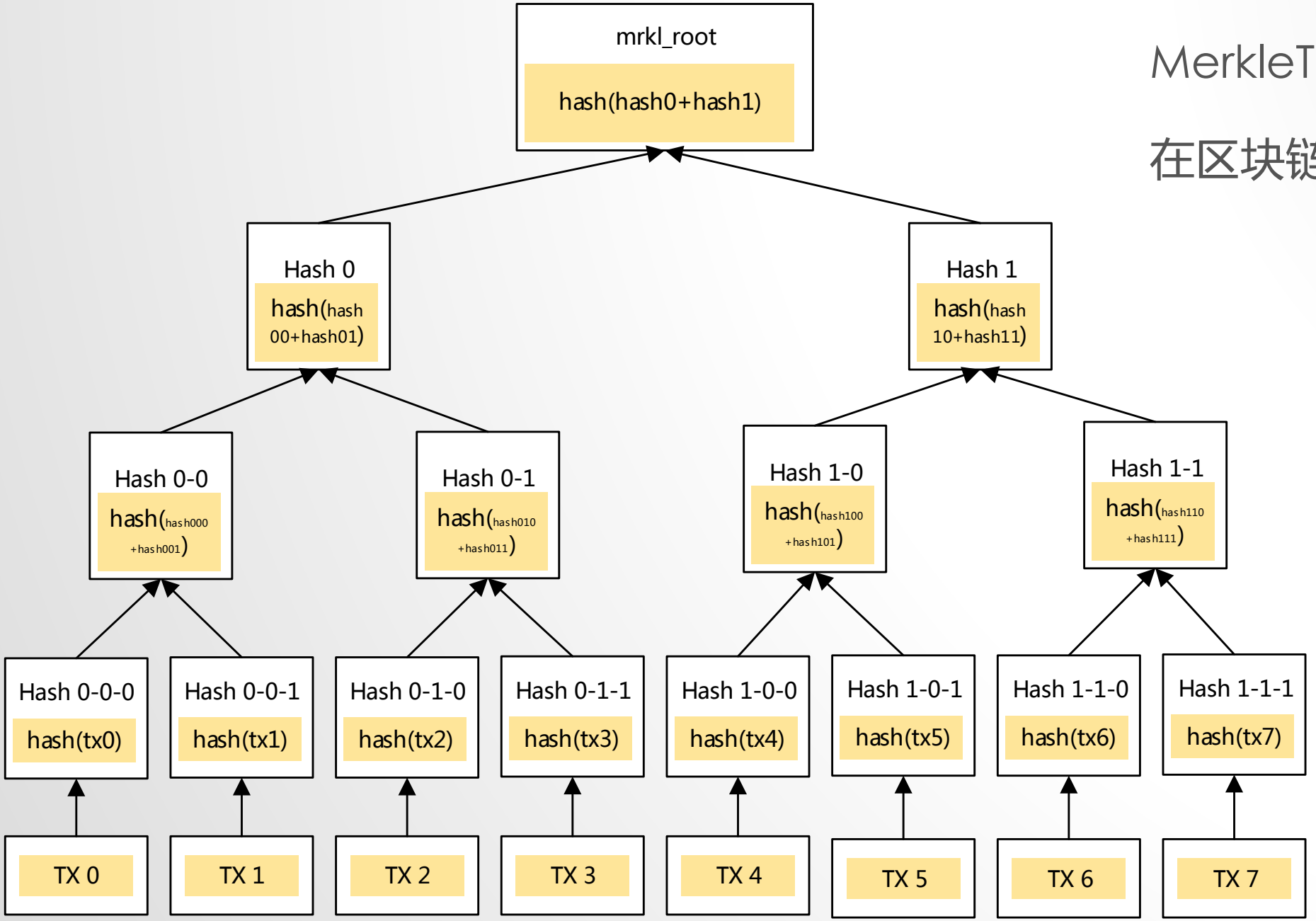
如果有一段数据不一致：

- 则顶层HASH必然不一致
- 可以逐层找到不一致的数据段
- 只需要重新下载该段数据

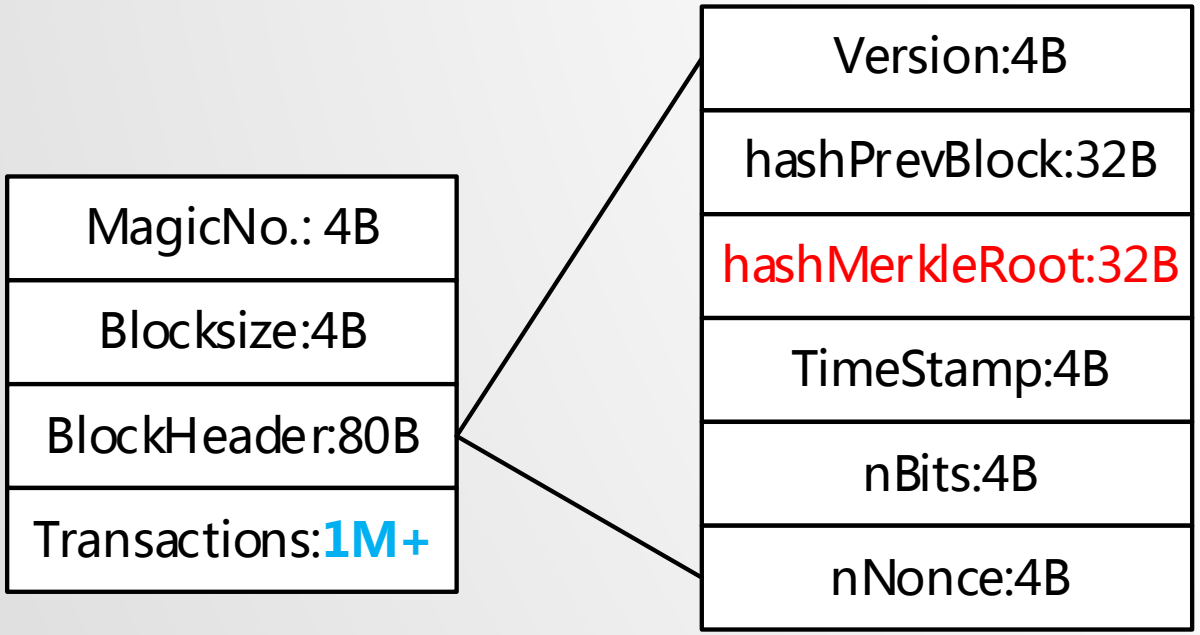


MerkleTree

在区块链中索引交易



比特币区块结构



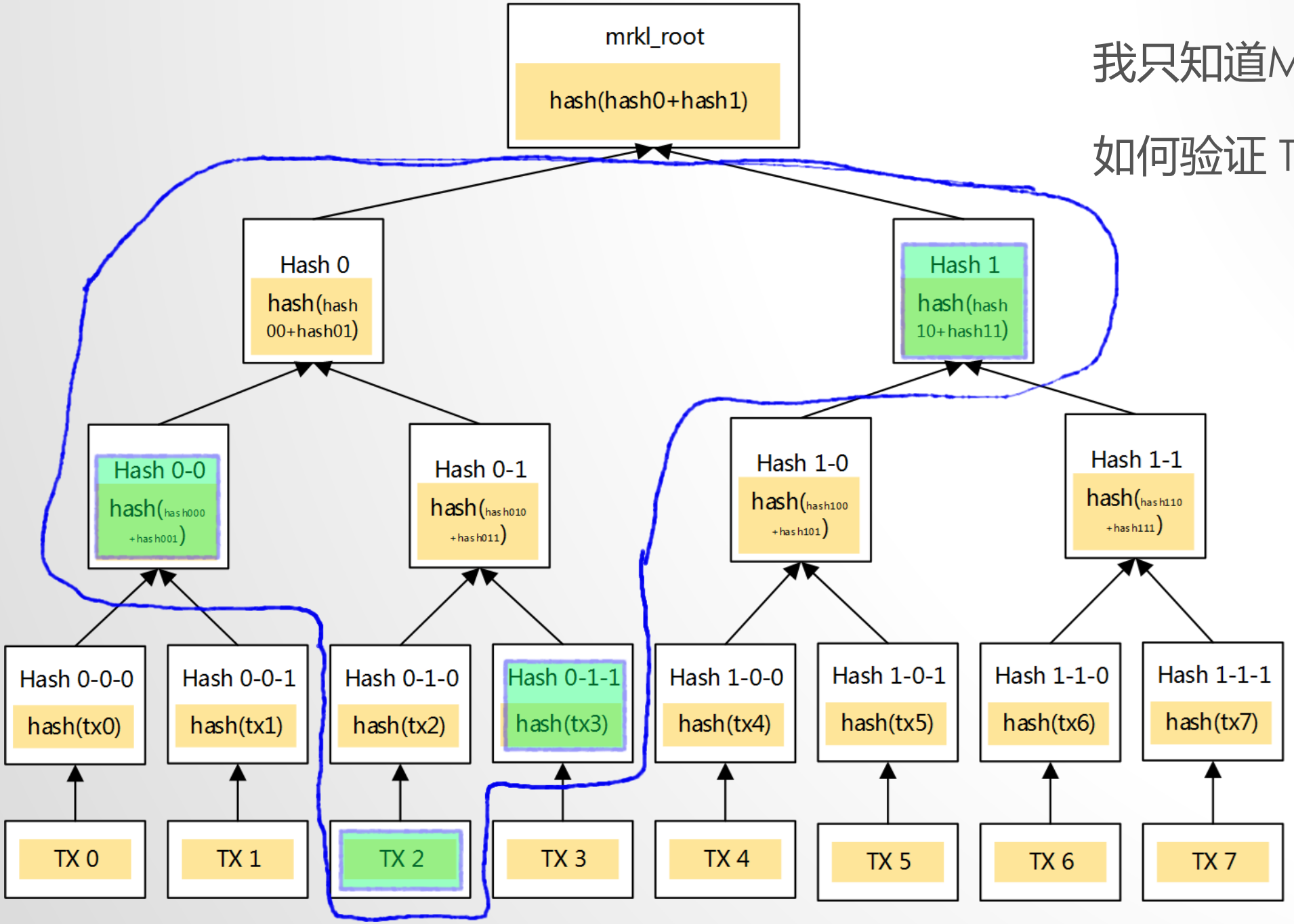
- 比特币区块体积很大
- 比特币区块头中包含了MerkleRoot
- MerkleRoot保证交易一致性
- 只要同步区块头，可保证不可篡改

比特币轻钱包

- 比特币全节点体积很大：140GB
- 轻钱包只收录区块头
- 轻钱包如何验证交易：提供交易以及“沿途”Hash，与MerkleRoot比较验证

我只知道MERKLE TREE ROOT

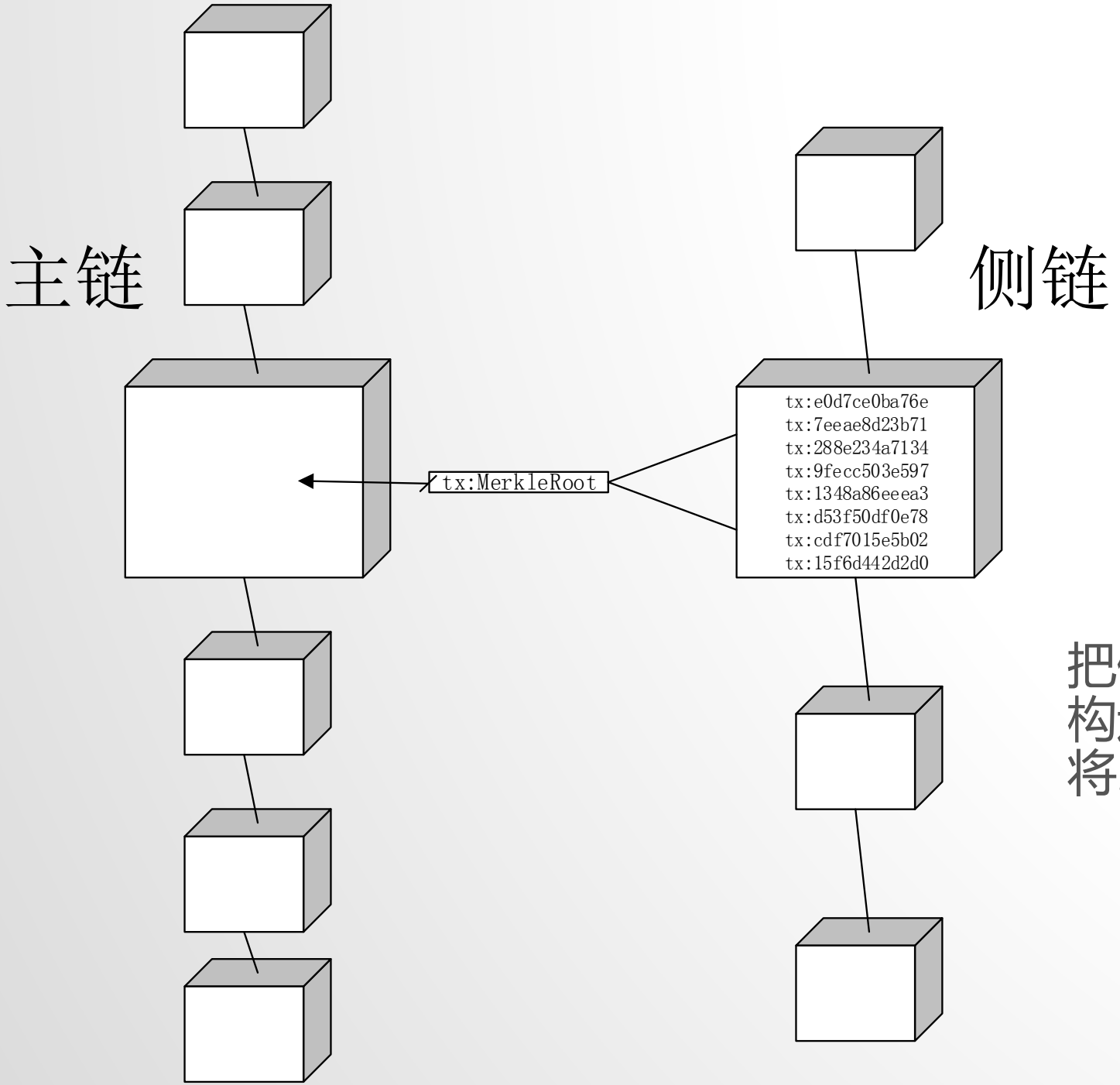
如何验证其中一笔交易的有效性？



我只知道MerkleTreeRoot

如何验证 TX2的有效性？

如何利用MERKLE TREE实现跨链收录？



把侧链上一个区块内的所有交易，
构造一个Merkle Tree。
将MerkleRoot插入到主链中