区块链基础及应用实验报告

H1

网络空间安全学院 信息安全专业

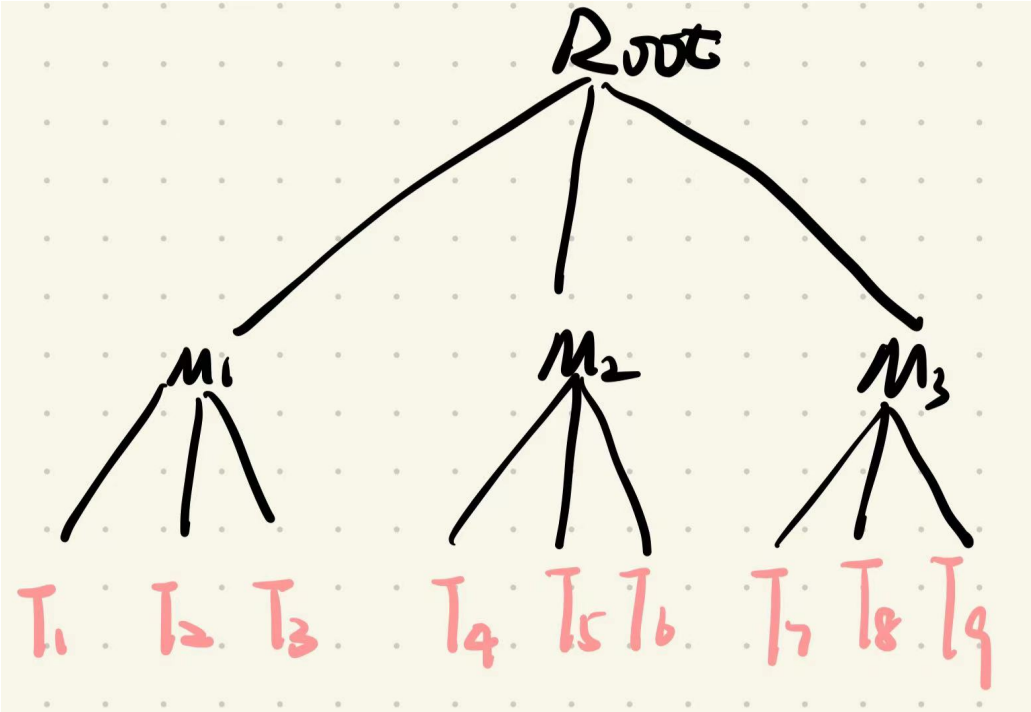
2112492 刘修铭 0939

https://github.com/lxmliu2002/Blockchain_Fundamentals_and_Applications

问题1：多元Merkle树

a

根据题目要求，构建Merkle Tree如下



- 计算对S的承诺，即计算Root的Hash。首先需要根据T_1、T_2、T_3的Hash计算出M_1的Hash，根据T_4、T_5、T_6计算出M_2，根据T_7、T_8、T_9计算出M_3，然后根据M_1、M_2、M_3再算出$Root$的Hash，即对S的承诺。
- 要证明T_4在S中，即需要T_5、T_6、M_1、M_3以及$Root$这5个值包含在证明中

b

经过计算可知，其证明长度为$[1+(k-1)\lceil \log_k n \rceil]$

c

当n较大时，分析b中得出的结果。因为对数函数中的底数 k 越大，对数增长的速度越快。故而当 n 较大时，随着 k 的增加，$[1+(k-1)\log_k n]$的增长速度也会增加。因此最好使用二叉Merkle树。

问题2：轻量级客户端

a

- 交易ID：Alice需要向Bob提供包含她支付给Bob的交易的交易ID。交易ID是一个唯一标识符，用于标识交易在区块链中的位置。
- 区块头：Alice需要向Bob提供包含她支付给Bob的交易的区块头。区块头包含了该区块的哈希值、交易Merkle树的根哈希值以及前一个区块的哈希值等信息。
- Merkle路径：Alice需要向Bob提供包含她支付给Bob的交易的Merkle路径。Merkle路径是从该交易所在的叶节点开始，一直到交易Merkle树的根节点的路径。路径中的每个节点都有一个哈希值。

b

首先考虑验证每个Merkle根的合法性。由前面可知，对于二叉Merkle Tree，需要$(1+\log_2 n)$的证明长度。

接着按照区块头保存的前一个区块的哈希查找前一个区块，以此循环k次。

而整个过程都使用SHA256作为哈希函数，故而每个哈希值为32字节。

故而这个证明过程需要$[(1+\log_2 n)\times k\times 32]$字节。

当$k=6,n=1024$时，上式等于2112，即需要2112字节。