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

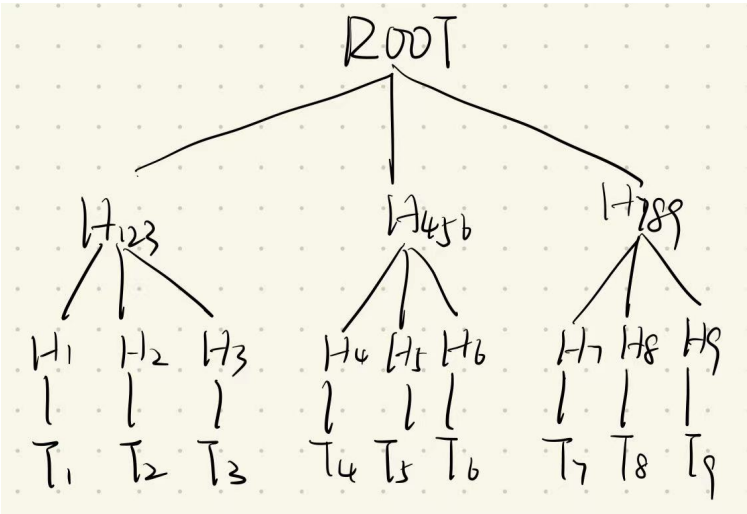
2112492 刘修铭 0939

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 H_1、H_2、H_3 计算出 H_{123}，根据T_4、T_5、T_6 的 Hash H_4、H_5、H_6 计算出 H_{456}，根据 T_7、T_8、T_9 的 Hash H_7、H_8、H_9 计算出 H_{789}，然后根据 H_{123}、H_{456}、H_{789} 再算出 $Root$，即对 S 的承诺。
- 要证明 T_4 在 S 中，即需要 H_5、H_6、H_{123}、H_{789} 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（Hash）：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$(1+\lceil \log_2 n \rceil)$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，向前找 k 个。

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 $[(1+\lceil \log_2 n \rceil + k) \times 32]$ 字节。

当 $k=6, n=1024$ 时，上式等于 544，即需要 544 字节。