区块链基础及应用 2023

问题 1：多元 Merkle 树。Alice 可以使用二叉 Merkle 树来提交的一组元素 S = （T_1, ..., T_n），之后她可以向 Bob 证明 S [i] = T_i，每个证明最多包含$\lceil \log_2 n \rceil$ 个哈希值。对 S 的承诺是单一的哈希值。在这个问题中，请你解释如何使用 k 叉树来做同样的事情，也就是说，每个非叶节点最多可以有 k 个子节点。每个非叶节点的哈希值是其所有子结点的值的哈希值。

a.假设 S ＝（T_1,...，T_9）。解释 Alice 如何使用三叉 Merkle 树计算对 S 的承诺（即 k = 3）。Alice 如何向 Bob 证明 T_4 在 S 中，即哪些值被包含在证明中？

b.假设 S 包含 n 个元素。S [i] = T_i 的证明长度是多大？用 n 和 k 的函数表示。

c.对于较大的 n 值，如果我们想最小化证明的大小，最好使用二叉 Merkle 树还是三叉 Merkle 树？为什么？

问题 2：

轻量级客户端：假设 Bob 运行一个超轻量级的比特币客户端，该客户端从一个可信赖的源获取区块链的当前头部。这个客户端的内存非常有限，所以它只存储链中最近的区块头（链的头部），并删除任何之前的区块头。

a. 考虑当前的区块链设计，每个区块头包含（i）所有交易的 Merkle 根，和（ii）前一个区块头的哈希。假设 Alice 在链上发布了一个给 Bob 支付的交易。一段时间后，Alice 想向 Bob 证明她已经支付给他。Bob 运行一个超轻量级的客户端，只有最新的区块头。为了证明她给 Bob 的付款已经被包含在链上的一个区块中，Alice 应该发送什么信息给 Bob？

b. 假设 Alice 的支付包含在当前头部之前的第 k 个区块中，并且每个区块恰好有 n 笔交易。估计这个证明需要多少字节，用 n 和 k 表示。计算 k=6 和 n=1024 时的证明大小，假设整个过程中都使用 SHA256 作为哈希函数。