区块链基础及应用 2024

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：混币交易隐私

请考虑下图中的交易图：矩形表示交易，空心圆表示新地址，实心圆表示由命名实体控制的地址（例如，A 代表 Alice，B 代表 Bob，C 代表 Carol）。标记为“change”的边表示终端是该交易的找零地址。注意，并不是每笔交易都有标识出的找零地址。

a. 你能否识别出在标记为(1)的交易中 Bob 支付的人是谁？请解释如何识别，或为什么不能确定识别。

b. 你能否识别出支付给 Carol 的人？解释如何识别，或为什么不能确定识别。