# 区块链第一次书面作业

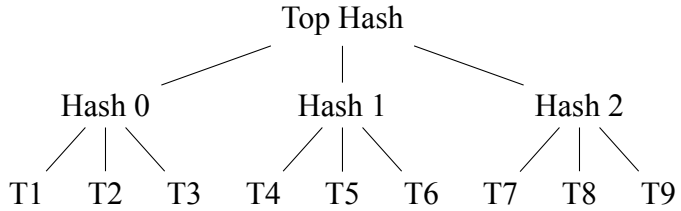
朱浩泽 1911530 计算机科学与技术

November 15, 2021

## 1 多元 Merkle 树问题

### 1.1 问题 a

画出其 Merkle 树如下图所示：




通过上图可以看出，如果 Alice 想向 Bob 证明 T4 在 S 中，则先需要 T5 和 T6 的值，通过 Hash 函数算出 Hash 1 的值，再利用 Hash 0 和 Hash 2 的值同算出的计算出的 Hash 1 的值通过 Hash 函数计算出 Top Hash 的值，与获得的可行的 Top Hash 值进行对比，便可检验出 T4 在 S 中。其中我们利用了 T5、T6、Hash 0、Hash 1 的值。

### 1.2 问题 b

记一共有 $n$ 个元素，每个非叶节点最多可以有 $k$ 个子节点，则此 Merkle 树有 $\lceil \log_k n \rceil + 1$ 层，除去 Top Hash，每一层的证明需要 $(k-1)$ 个元素，所以其证明长度为 $(k-1) \times (\lceil \log_k n \rceil + 1 - 1) = (k-1) \times \lceil \log_k n \rceil$。

### 1.3 问题 c

$$
\begin{aligned}
&\lim_{n\to\infty} \frac{(3-1)\times \log_3 n}{(2-1)\times \log_2 n} \\
=&\lim_{n\to\infty} 2 \times \frac{\log_3 n}{\log_2 n} \\
=&\lim_{n\to\infty} 2 \times \frac{\log_n 2}{\log_n 3} \\
=&2 \times \log_3 2 \\
=&1.2619 > 1
\end{aligned}
$$

由此可见，最好使用二叉默克尔树。

## 2 分层确定性钱包

如果将 $H(k||i)$ 换成 $k+i$，第 $i$ 个公钥为 $g^{x_i} = g^{k+i}g^y$, 则第 $i+1$ 个公钥为 $g^{x_{i+1}} = g^{k+i+1}g^y = g^{x_i}g$
于此同时，第 $i$ 个私钥为 $x_i = y + k + i$, 则第 $i+1$ 个私钥为 $x_{i+1} = y + k + i + 1 = x_i + 1$
由此可见，知道一个公钥的来源后，通过简单的乘法计算，可以轻松判定这些公钥来自同一个钱包。与此同时，如果某一天有人猜出来了 g 的值，通过第 $i$ 个公钥和 g 的值推算出了 $x_i$ 的值，那么如果我们使用的是 $H(k||i)$ 函数的话，也无法通过这个泄漏的私钥匙推算出其他的私钥；但如果使用的是 $k+i$ 函数的话，只需要简单进行 +1 计算，便可得知所有的公钥和私钥对，从而盗走所有比特币。所以这种算法也可能会影响安全性。