问题 1：

(1)参见课上讲解的三叉 Merkel tree 示例。

(2)采用 Merkle tree 的方法，可以知道成员证明需要 Sibling 的集合，因此假设是 k 叉树，那么所需要的 Hash 数目是 $1 + (k-1)\lceil log_k(n) \rceil$; （包括根节点）

(3) n 在渐进意义下，成员证明大小正比于 (k-1)/log(k)。可以知道

1/log(2)< 2/log(3) (也就是 log(3)<2log(2))，因此还是二叉 Merkle 树更好。

问题 2：

(1) $\sigma = \sigma_1\sigma_2\sigma_3$.

(2) 签名数据中需要包含的内容：

$\sigma_{9,i} = \mathrm{H(m)}^{x_{9,i}}, i = 1,2,3,$ pk9, 以及 Merkle tree 的 pk9 成员证明，也就是 Sibling 包括 $\lceil \log 2(10) \rceil$=4 个哈希。 所以一共是 3*48+48+4×32 字节;

大于原来 Multisig 方法中需要提供的 3 个签名大小，也就是 3×64 字节； 还有 OP_0(1 字节).

(3)现在考虑 t-n 一般情形，我们需要比较不同方法所消耗字节数：

Multisig 方法： t*64+1;

该方法： $t*48+48+\left\lceil \log 2\left(\binom{n}{t}\right)\right\rceil * 32;$

即比较 t?> $2*\left\lceil \log 2\left(\binom{n}{t}\right)\right\rceil + 3^{-}$.

比如 t=11, n=12,就有 $11>2*\left\lceil \log 2\left(\binom{12}{11}\right)\right\rceil + 3^{-}$，也就是这种情况下，所提方案消耗空间更少。

但是，该方法在 n, t 很大的时候不具备实用性，因为计算 Merkle tree 也需要耗费不少算力; 此外 Paring 的计算代价也高于 ECDSA。