Assignment 6 – 2019.10.29

Submission deadline: 2019.11.05

1. In cryptography, a **Merkle tree (Hash tree)** is a tree in which every leaf node is labelled with the hash of a data block, and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. It has been applied in various applications to prove membership in a very efficient way. Please read 8.9 (315-318) carefully, and answer the following questions:
   a) How does a Merkle tree work?
   b) Why is it efficient when using Merkle tree to prove membership?
   c) How to take advantage of a Merkle tree to prove non-membership?
   d) How does blockchain use Merkle tree to verify transactions? Please describe by concrete example.

P.S. Direct copy from the book is strictly forbidden. Students are required to summarize by their own language.