FINAL

IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2018

MEng Honours Degree in Mathematics and Computer Science Part IV
MEng Honours Degrees in Computing Part IV
MSc in Advanced Computing
MSc in Computing Science (Specialist)
for Internal Students of the Imperial College of Science, Technology and Medicine

This paper is also taken for the relevant examinations for the Associateship of the City and Guilds of London Institute

PAPER C467H

PRINCIPLES OF DECENTRALISED LEDGERS

Thursday 22 March 2018, 10:00
Duration: 70 minutes

Answer ALL TWO questions

Paper contains 2 questions
Calculators not required

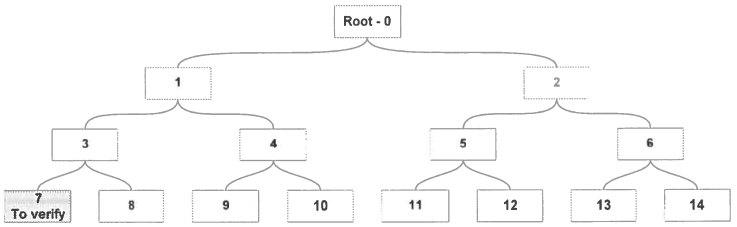

Fig. 1: Merkle Tree as seen by Alice.

1 The following questions address basic knowledge about decentralized blockchains (e.g. Bitcoin/Ethereum).

a Open and decentralized blockchains are also referred to as cryptocurrencies. This name stems from their significant use of cryptography, in particular of elliptic curve cryptography, such as ECDSA.

i) What is encrypted in Bitcoin/Ethereum?

ii) What is cryptographically signed in Bitcoin/Ethereum? Why is a signature necessary?

b A Merkle Tree is a hash tree, culminating in a Merkle root hash. Describe how a Merkle Tree in the Bitcoin block header is used to prove that a transaction is included in a block.

c How much data is required to demonstrate that a leaf node is part of a given hash tree?

d Given the Merkle Tree in Figure 1, assume Alice (full node) wants to prove to Bob (SPV client) that transaction 7 has been included in the respective block. What information must Alice provide to Bob?

e For what other purposes could a Merkle Tree be used? Feel free to be creative in your suggestions.

The five parts carry, respectively, 30%, 25%, 15%, 15%, and 15% of the marks.

2a i) Given a hash function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^{256}$, Alice's computer requires on average 16 minutes to find a hash with at least 24 leading zeros. What is her hashrate?

ii) How long does she need on average to compute a hash with 25 leading zeros?

iii) How long does she need on average to compute a hash with 30 zeros at the end?

iv) Consider the hash function $\mathcal{H}' : \{0,...,9\}^* \to \{0,...,9\}$, which is calculated by taking the digital root (i.e. repeatedly taking the digit sum until the result is one digit) of the input. Find a second preimage to the input $x = (1,4,7,3,9,0,1,4)$.

b i) Given transaction 1 and its output with the script OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG, and transaction 2 with its input with the script <Sig> <PubKey>, please verify if the transaction 2 is allowed to spend the output of transaction 1. We assume here that the signature of the input of transaction 2 is valid. We expect you to draw the execution stack and the execution code for each instruction of the Script.

ii) What happens if two transactions use the same previous transaction output as input? Please provide a detailed answer about different outcomes and consequences.

The two parts carry, respectively, 60% and 40% of the marks.