# KFUPM College of Computer Science and Engineering Computer Engineering Department COE 449: Privacy Enhancing Technologies

Faris Hijazi s201578750

Fall 2019 (191)

Assignment 4: Due date Tuesday 17/12/2019

## Question1: Merkle Hash Tree (20 pts)

1. Construct a binary Merkle tree for data blocks *Di* ∀*i* ∈ [1*,*16]. In your tree, represent the hash of each block with *Hash*(*Di*). Similarly, represent the hash of each node with *Hash*(*Ni*), where *Ni* is the *ith* node in the tree.

Since we need 1-16, we’re gonna need the following layer sizes: 16, 8, 4, 2, 1.

So we’re gonna need a 5 layer deep tree.

N9

N11

N15

N14

N13

N12

N10

N8

N1

N2

N3

N4

N5

N6

N7

D15 D16

D13 D14

D9 D10

D7 D8

D3

D1

D2

D4

D11 D12

D5 D6

N1 = H(N2||N3)

N2 = H(N4||N5)

…..

N8 = H(H(D1)||H(D2))

….

1. Given block *D*6, list the set of hash values needed to validate the integrity of *D*6.

You need to have all the blocks that are affected/dependant on D6, and those would be: D5, N5, N4, N3

## Question2: Bitcoin Fundamentals (40 pts)

Read the Bitcoin white paper [[[1]](#footnote-1)](https://bitcoin.org/bitcoin.pdf)and answer each of the following questions in your own words.

1. Explain how Bitcoin addresses the double-spending problem

The transaction must be agreed upon by the peers, and Explain how Bitcoin deters denial of service attacks or other service abusers

There is a challenge, the miners have to find a Nonce that results in a hash value less than C (usually meaning that there are a certain number of leading zeros).

1. Explain how Bitcoin incentivizes nodes to mine on the network

There is a reward given to the miners, (Longest chain for consensus)

1. Explain how does Bitcoin deal with fork chains

When there is a disagreement (fork), the transactions branch, and the first to reach 6 blocks is the one that is agreed upon. (that’s why transactions take some time).

1. <https://bitcoin.org/bitcoin.pdf> [↑](#footnote-ref-1)