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

Faris Hijazi s201578750

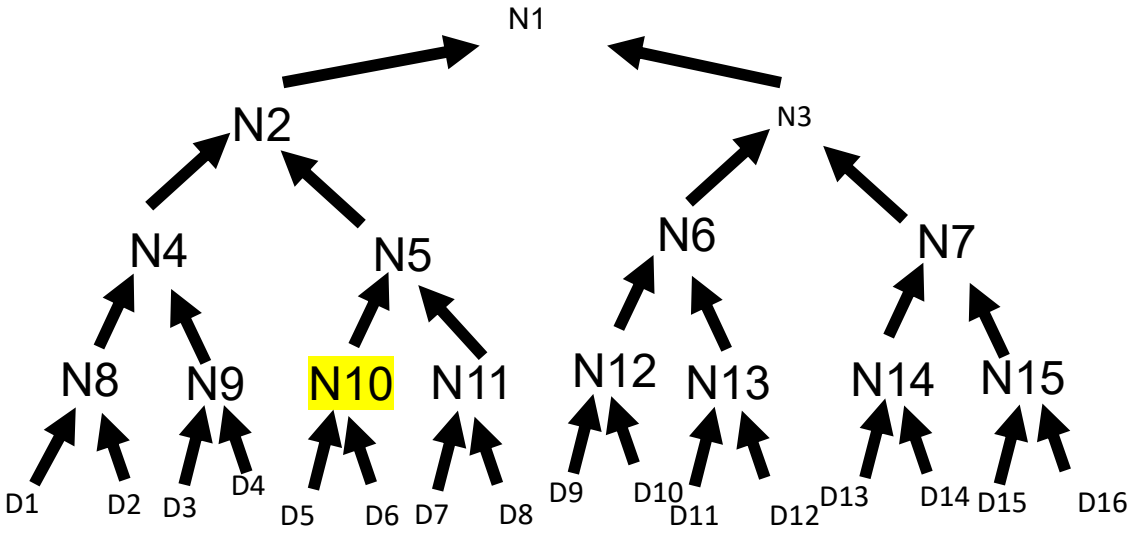
Fall 2019 (191)

Assignment 4: Due date Tuesday 17/12/2019

1.1 Question1: Merkle Hash Tree (20 pts)

(a) Construct a binary Merkle tree for data blocks $D_i \forall i \in [1,16]$. In your tree, represent the hash of each block with $Hash(D_i)$. Similarly, represent the hash of each node with $Hash(N_i)$, where N_i is the i^{th} 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.



N1 = H(N2||N3)

N2 = H(N4||N5)
…..
N8 = H(H(D1)||H(D2))
….

(b) 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

1.2 QUESTION2: BITCOIN FUNDAMENTALS (40 PTS)

Read the Bitcoin white paper [1] and answer each of the following questions in your own words.

(a) 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).

(b) Explain how Bitcoin incentivizes nodes to mine on the network

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

(c) 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