Q2A- WHY THE MERKLE TREE IS BETTER THAN A SINGLE HASH

VICTOR NNADI

MAY 7, 2021

The Merkle tree is a hash based data structure. It is used to label data that is stored, transferred in and between computers because the structure allows a peer to verify that data blocks of a file received from other peers in a peer-to-peer network are received undamaged and unaltered, and to check that the other peers do not "lie" and send fake blocks. In the Merkle tree, every block has its own hash.

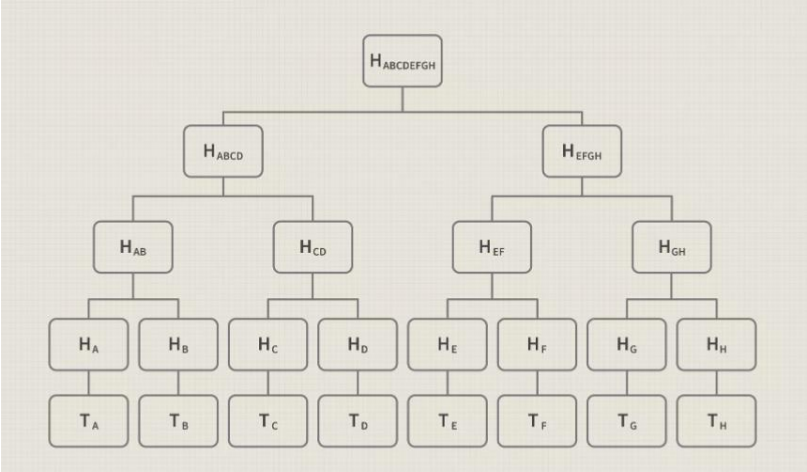

Image by Julie Bang © Investopedia 2020

They are better than a single hash of the entire file because in the case where a peer sends a file containing some damaged blocks, the receiving peer won't have to find another source of the entire file as you would with a single hash. The peer would only have to search for another source of the damaged blocks, using the hash of the blocks as reference, and replace them. Merkle tree structures increase data handling and verification efficiency by reducing the amount of data that is transferred in a network while still achieving the intended result.