Computer Science: Problems and Solutions

Doyinsolami Samuel Olaoye

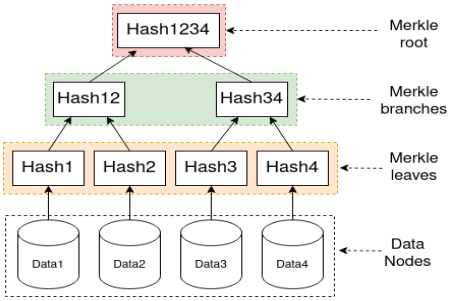
May 9, 2021

Question 1

The Merkle Tree is a central data structure to most cryptocurrency implementations, why is it better than a single hash?.

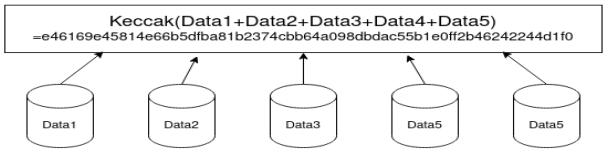
Solution:.

A Merkle tree is fundamentally just a hierarchical set of hash values, building from a set of actual data (Merkle leaf) to intermediate hashes (Merkle branches) and up to the Merkle root that summarizes all the data in one hash value.



In the figure above, the bottom nodes (Data1-Data4) are the actual data processed by the application. Each of these is summarized by their respective hash value (Hash1-Hash4), as a Merkle leaf. From these, the Merkle tree builds a hierarchy, combining hashes together until only one is left. The nodes combining other hash nodes are called Merkle branches (here Hash12 and Hash34). When there is only one left (here Hash1234), this is called the Merkle root. In the event where there is an uneven (odd) number of leaf (data) nodes, the extra hash is duplicated to pair with itself. Note that any change in any transaction data changes the Merkle root, and it no longer matches the one stored in the blockchain for that block (in block header).
Bitcoin and similar cryptocurrencies make use of Merkle trees to summarize and validate the transactions in a block, and embed the Merkle root into their block header as a summary of it all.

In the single hash system, one could just concatenate all the transaction data together and build a single root hash. Here also, changing just one data value will have the same effect of invalidating the summary hash



However, the real benefit of using a Merkle tree over a single hash is that it gives you more granularity in the hash verification, and enables other clever tricks to process the blockchain more efficiently. While also providing the transaction integrity assurance / verification.