Question 1:

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

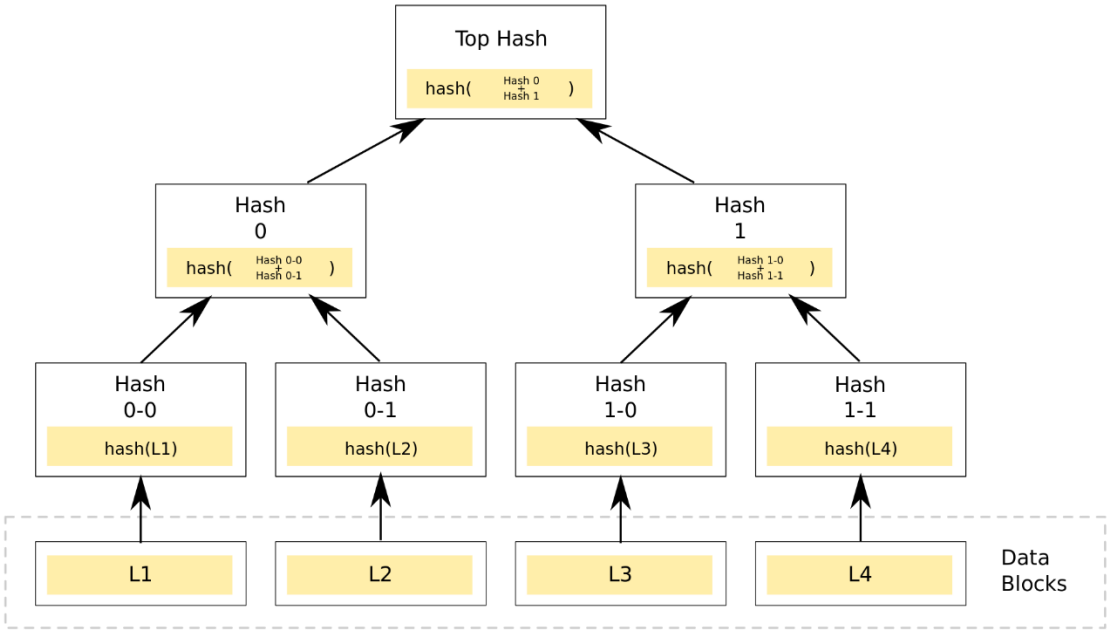
Solution:

The Single Hash: A **Single hash** function, also known as a message digest, fingerprint or compression function, is a mathematical function which takes a variable-length input string and converts it into a fixed-length combination of words and numbers.

The Merkle Tree:

Merkle tree is a data structure that is used in computer science applications. In bitcoin and other cryptocurrencies, **Merkle trees** serve to encode blockchain data more efficiently and securely.

A Merkle tree is a hash-based data structure that is a generalization of the hash list. It is a tree structure in which each leaf node is a hash of a block of data, and each non-leaf node is a hash of its children. Typically, Merkle trees have a branching factor of 2, meaning that each node has up to 2 children.



Benefit over a single hash:

Merkle trees are used in distributed systems for efficient data verification. They are efficient because they use hashes instead of full files. Hashes are ways of encoding files that are much smaller than the actual file itself. Currently, their main uses are in peer-to-peer networks such as Tor, Bitcoin, and Git. Data verification is used to make sure data is the same everywhere. If there is an error, you can easily trace the error to the roots if using a Merkle tree hash, but if its just a single hash, the error becomes untraceable.