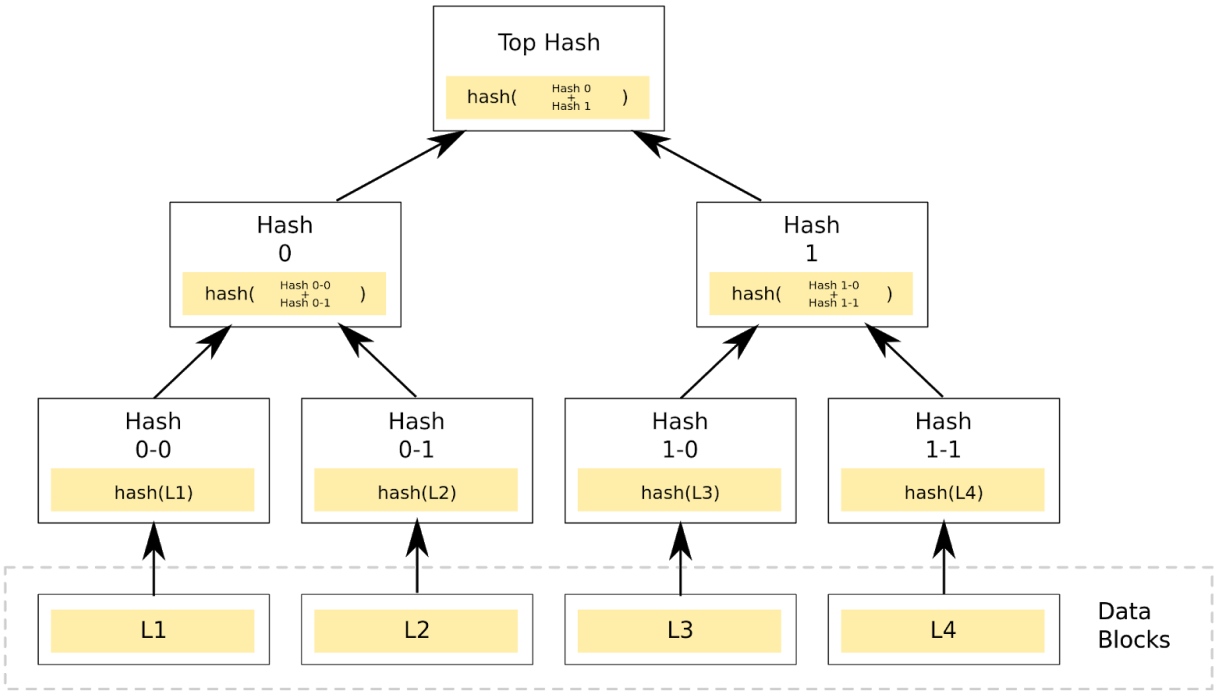
Merkle Tree

A Merkle tree is a relatively simple data structure that is used to check data integrity.

It's a binary tree where each node contains a cryptographic hash of its two children.

$H_{parent} = hash(H_{left} + H_{right})$



If a node has only one child, its hash is the same as its child's.

The hash of the root node of the tree is called the *Merkle root*. The leaves of the tree contain the hashes of the input data.

Part 1 - Merkle tree implementation

With the coding language of your choice, write a module allowing the creation of a Merkle tree from an array of data (in the illustration, that would be L1, L2, L3, et L4).

For instance:

```
createMerkleTree([string1, string2, string3, ...]) =>
MerkleTree
```

The Merkle tree should have the following function:

```
// Returns the Merkle root of the tree

MerkleTree#root()

// Returns the number of levels of the tree

MerkleTree#height()

// Returns an Array containing the hashes of the given level

MerkleTree#level(index)
```

Hashes are computed using the cryptographic function SHA256.

Bonus : writing a test suite

Part 2 - Questions

1) In the illustration, let's imagine I know the whole Merkle tree. Someone gives me L2 data block but I don't trust him. How can I check if L2 data is valid?

2) I know only the L3 block and the Merkle root. What minimum information do I need to check that the L3 block and the Merkle root belong to the same Merkle tree?

3) What are some Merkle tree use cases?