Merkle Trees are data structures designed for provable immutability and computationally efficient consistency verification. A n'ary Merkle Tree, like a search tree, is a directed acyclic graph with one root node and a branching factor of *n*. Data is stored in the leaf nodes. Every parent node holds the hash of the concatenation of the strings stored by their children.

With the help of a cryptographic hash function, a fingerprint of boundless amount of data can be represented in the root node alone, as the hash of the root depend upon the overall structure of the tree. The Bitcoin blockchain uses this data structure to store all the transactions that are being included within a certain block.

The consensus algorithm of a blockchain system is the process through which the individual nodes of the distributed network reach an agreement on how to update the data as new information is to be added to the ledger. In the Bitcoin blockchain this is achieved through a process called Proof-of-Work, in which only those computers that has solved a cryptographic puzzle is allowed to create new blocks and propagate them through the network.

The Proof-of-Work algorithm is designed in such a way that it achieves several goals simultaneously. Every time a new block is created, a new Bitcoin is minted out of thin air and given as a reward to the miner – thus creating an economical incentive to contribute to the maintenance and integrity of the blockchain.

Since solving the cryptographic puzzle is a computationally heavy task, this ensures that tampering with the information stored in the blockchain becomes practically infeasible.

However, using Proof-of-Work as consensus algorithm is far for optimal with respect to the aggregated energy consumption associated with mining, and hence more energy-efficient consensus algorithms have been proposed and adopted by competing blockchains.