BLOCKCHAIN :

It is a decentralised network in which all the nodes in the network are connected with each other without a central server, thereby reducing the possibilities of cyber attacks and making the data immutable. Implication of Blockchain will avoid the most feared problem “Double spending”. In blockchain all transactions are hashed and is visible on a public ledger, this maintains the trustworthiness of blockchain even without an external Trusted authority.

Implementation :

Initially a genesis block is created, this genesis block forms the origin the blockchain. Succeeding blocks are linked with this genesis block and the chain grows. When a transaction takes place it is pushed to the block and a hash is generated. When a node mines the block, the transaction completes. Followed an acknowledgement send to the public ledger, So that the status of transaction is visible publicly.

Client server architecture :

If the server is malicious or hacked or attacked the network becomes non-functional whereas in blockchain as there is no central server, this is not possible. This stands as gigantic advantage when compared with centralised system.

Merkel tree :

Merkel tree is a tree structure where the data is present only in the leaf nodes and the intermediate nodes are hashed. In order to access the data the user needs to traverse several levels of hashes from root to leaf node.

Hashing :

Hashing is a technique in which the data are mapped with their corresponding hash value. This hash value is generated by means of hash function.

How hashing works in blockchain :

* The hash of the contents of the new block is taken.
* A nonce (random string) is appended to the hash.
* The new string is hashed again.
* The final hash is then compared to the difficulty level and seen whether it’s actually less than that or not.
* If not, then the nonce is changed and the process repeats again.
* If yes, then the block is added to the chain and the public ledger is updated and alerted of the addition.
* The miners responsible for this are rewarded with bitcoins.

Public key & Private key Encryption :

Every user will have their own unique private and public key, encryption is done by the sender by using the public key of the receiver, which is visible globally. And the receiver decrypts the message using his private key that is known only the user himself.