Blockchain

What is Blockchain?

Lets Start with Bitcoin. In 2008 **Satoshi Nakamoto** invented Bitcoin with the BlockChain.So basically the technology behind the Bitcoin is BlockChain.

Bitcoin is basically a digital cryptocurrency which work on Peer-to-peer network.

It is also knows as distributed network that's mean no central Server.

Lets take a example In now a days we transfer the money by using central Server(system) which is bank which take fee for our transaction and maintain the security

But in Bitcoin there is no central System users directly do transaction to each other.

There are two issues arises when we talk about distributed System.

1:Security

2:Trust

How can you can trust this technology? And How can you Trust?

We can achieve Security by using Asymmetric Cryptography

Lets back towards to second issue which is Trust?

How can we make a system in distributed which solve this issue

How the Transaction will be verified and manageable?

Here comes the most important concept which is **Ledger.**

What is Ledger?

Ledger is simply a distributed database to every node in chain, once we saved the data in ledger no one can tempered or change the data that's the blockchain.

If someone try to change the data you know who is trying to change it but it cant be changed.

Lets explain with diagram

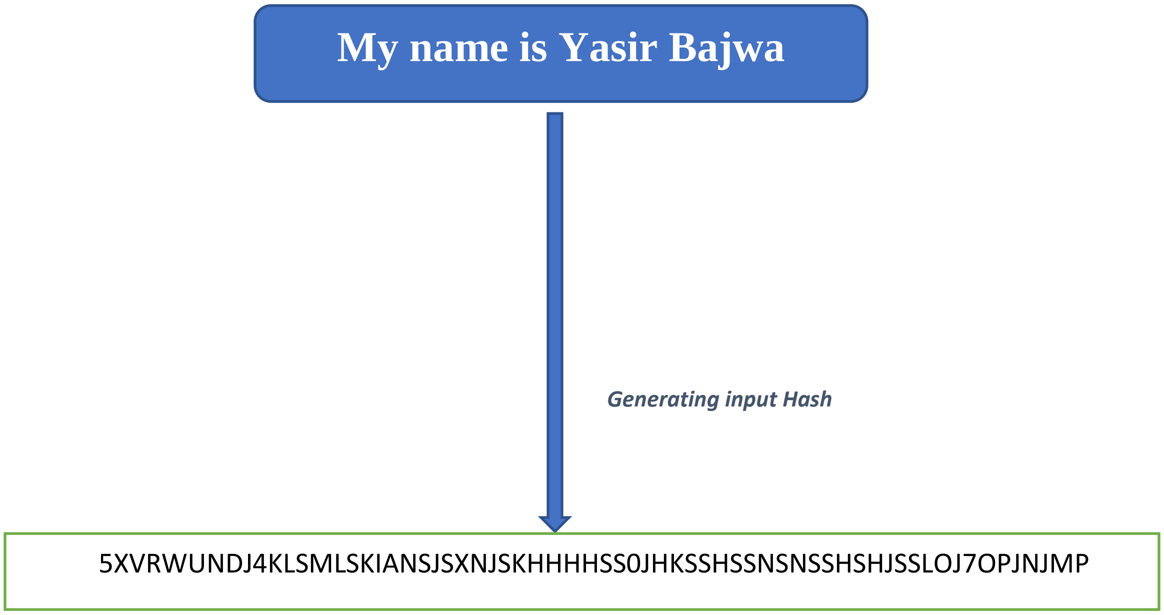
Block contain any data about personal info,fb data, Bitcoin and other types of data stored in database.

Bitcoin used the concept of Hashing

We can use different algorithms(MD5,SHA256,SHA512) to generate the hash key of block data

Lets under stand the concept of Hashing.

Assume we have an input i.e. my name is Yasir Bajwa and I applied a algorithm to generate its hash.



My name is Yasir Bajwa

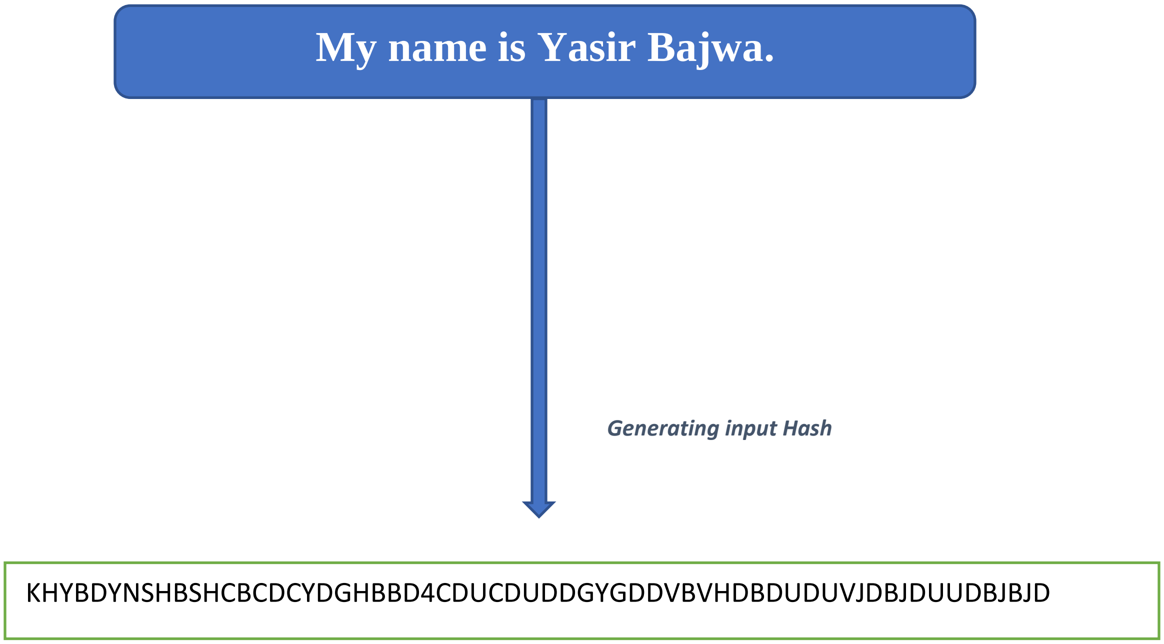
Generating input Hash

5XVRWUNDJ4KLSMLSKIANSJSXNJSKHHHHSS0JHKSSHSSNSNSSHSHJSSLOJ7OPJNJMP

Its does not matter how large the data hash key will be generated for all

Hash will be complete change if a single change OCCUR in input.

e.g a dot at the end of name is


My name is Yasir Bajwa.

Generating input Hash

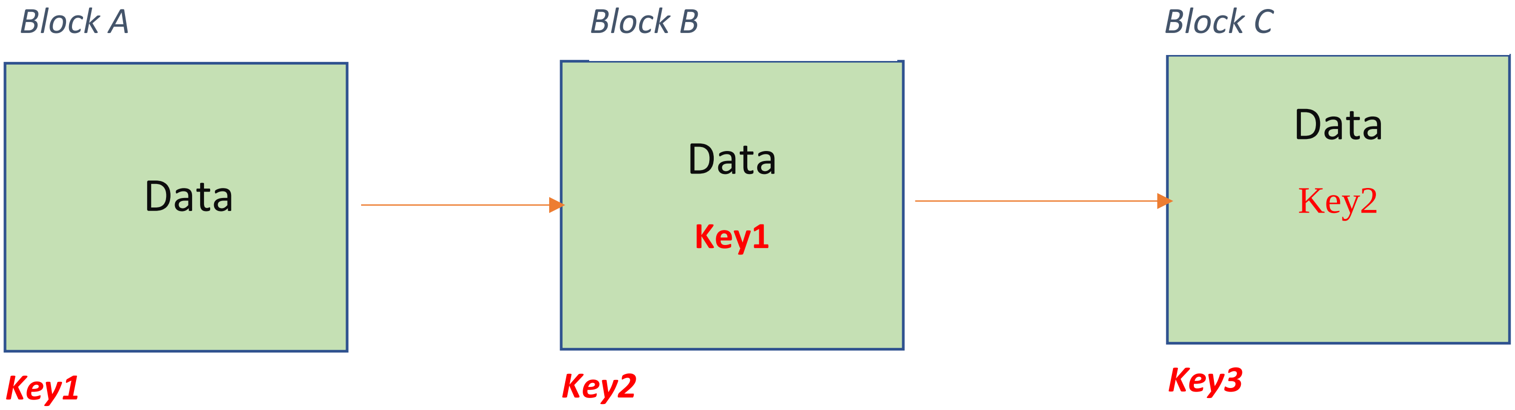
KHYBDYNSHBSHCBCDCYDGHBBD4CDUCDUDDGYGDDVBVHDBDUDUVJDBJDUUDBJBJD

We can call hash key is the digital Fingerprint of our data that data can only be modified through hash key.

How we know if someone has try to tempered our data?

Just take the key and compare with it

e.g like Linked List (second node know the position of first node)



If any block has change its data key will not match that’s why data cant be change.

So at the end it is the distributed ledger which cant be tempered .