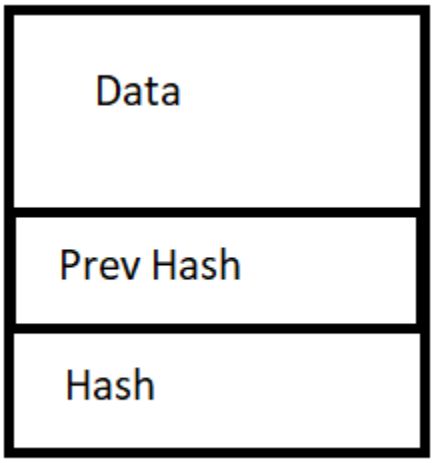
# Getting started with blockchain

- Table of contents.



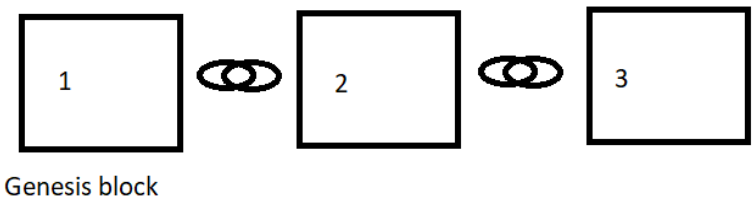
## 1. What is Blockchain?

In simple words, continuously growing list called blocks which are linked with other blocks using cryptographic algorithms is Blockchain.




Here is a simple block which is containing some data, this data could be anything depend on context of your blockchain.

*Hash is like a fingerprint of the blocks, which is unique and used to connect blocks.*



Genesis block is the first block which has Previous hash as ‘000000’. you can use any address as reference, it just denotes that it is the first block.

## 2. Hash SHA256 Algorithm:

Let’s understand this with an analog like any human fingerprint is unique which is used for identification of the person.

Same each block has a finger print which is nearly unique and Hash Algorithm sha256 which used hexadecimal characters determines the uniqueness of the blocks by providing a ramdom string.

Assume this like you are inserting data inside the algorithm and yoy are getting the hashed string.

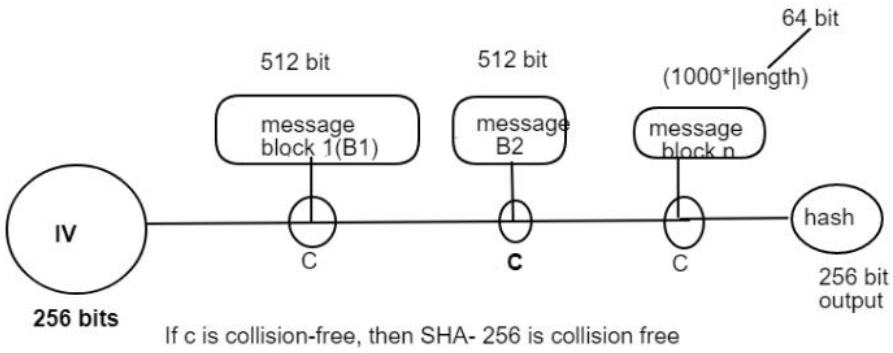
Properties of the sha256 algorithm:

1. It is one way once you encrypt the string you can’t reverse it back to original state.
2. Deterministic: For each set of input there should be a similar set of output
3. Fast computation: It should be comparatively fast.
4. Avalanche effect: Should be high, Small change in the input should change the hash significantly.
5. Must withstand collision:  Should be unique for each block.

Example: str = “abc”;

Hash: ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad

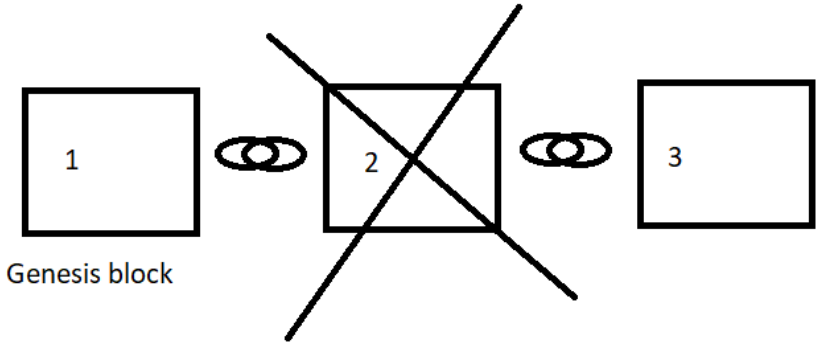
Computations takes place is: 3.8 milliseconds.



## 3. Immutable Ledger

This means that Once a data is recorded in the blockchain, it cannot be changed or altered.

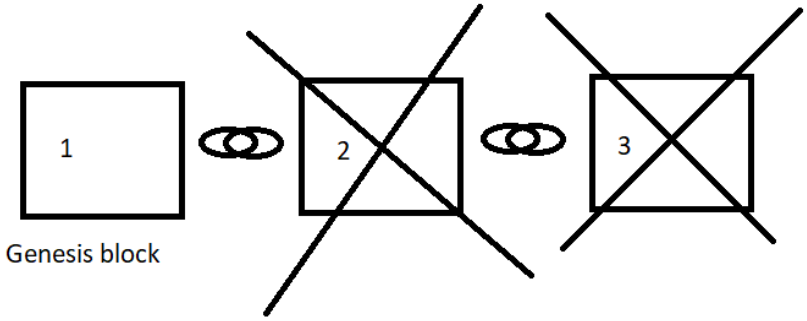
Example :




Attacker is trying to change the data

An Attacker is trying to change the data of Block no- 2, but changing block number 2 will change the Hash Remember we write in properties of the Avalanche effect.

So, the attacker has to change the all blocks.




Attacker is trying to change the data

So, an attacker has to have the System set up that can alter all blocks.

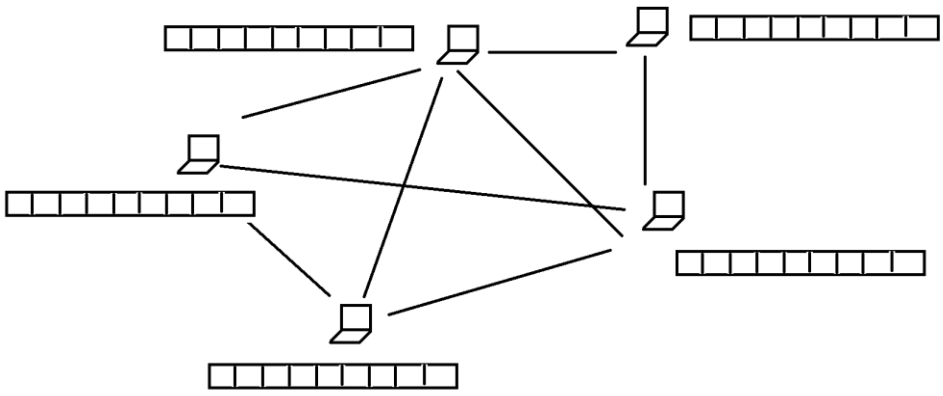
Later we will learn that It is practically impossible to alter even one block as there are various copy of these chains in the network and a communication is there. So, if one has to change one block in all system of network. We will see this later.

This is one of the properties of blockchain, Let's take an example of a bitcoin. In bitcoin it will build on the principle of blockchain and data is transactions done by the people. So if people started altering the transaction, it will not be a viable model.

## 4. Distributed P2P Network

In the above scenario, we learn as an attacker wants to change block, they have to change all blocks and that can solve their problem and they can successfully alter the block.

But Blockchain has added security level that is peer to peer network and that means copy of block chain in set of servers which is communicating so Practically an attacker has to change all blocks of all server. (Seems impossible)



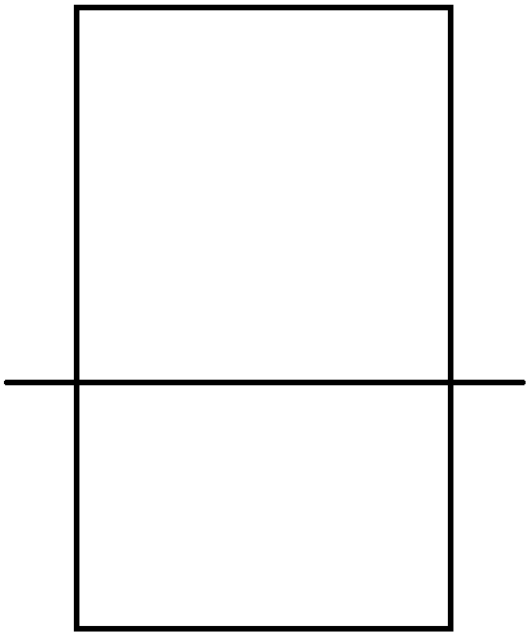
Servers across the network has copy of the blockchain and making difficult for the attacker to change the blocks.

**We will learn in later that how a block is added and shared across the networks.**

## 5 How mining the works, concept of nonce?

You learned the concept of blockchain, things are not so simple, there is concept of NONCE, which gives us extra power to determine the avalanche effect of the hash.

Nonce is a random number that determine your previous hash should be under certain target. No worry we will describe this in detail.




Our hash should lie below the target, which provide extra power to the determination of hash

When we determine the hash for our block it should lie below the target, so it takes extra computation (Trial and error) to calculate the hash and nonce.

When we find nonce that means we find hash, if it is below target It is called Golden Nonce.

## 6 Byzantine Fault Tolerance:

Described in 1982, it is one of the versions of two general problem with some catch. There are more than 2 teams that want to attach one castle but they can only attack if, consensus it reached as attack and there are more traitors that can change their decision.

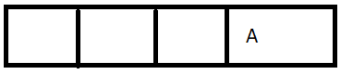
If is concluded that more than 2/3rd of teams are honest than we can reach to consensus. We will not go to much detail of the paper.

*How this is related to blockchain is – whenever a new block is to be added to one server of the network how other server will adapt I.e comes into a consensus of forwarding that packet to network or discard as it can be malicious.*

## 7 Consensus Protocol.

There are two problem that arrives till now what we have read

1. If one block is added to one server and another block is added to another server how a consensus should be there since each blockchain is same across the network.




Server A


Server B

Two server of same network has two different block trying to attach of same number? A big Problem

Solution: When there is two different blocks in the network so network which has more block of Type A wins the game and Type A will be attached to all server and then after Type A attached and all servers have same copy Type B will be attached and copied.

This is how consensus protocol work and achieved.

2. Another problem is How to determine a block is real and not malicious. It is very simple there is set of predefined rules that is checked before transaction/block is attached. If it obeys all rules it will be attached else discard and it is very unlikely to bypass this.

We will explain all rules in some later blog post/tutorial.