

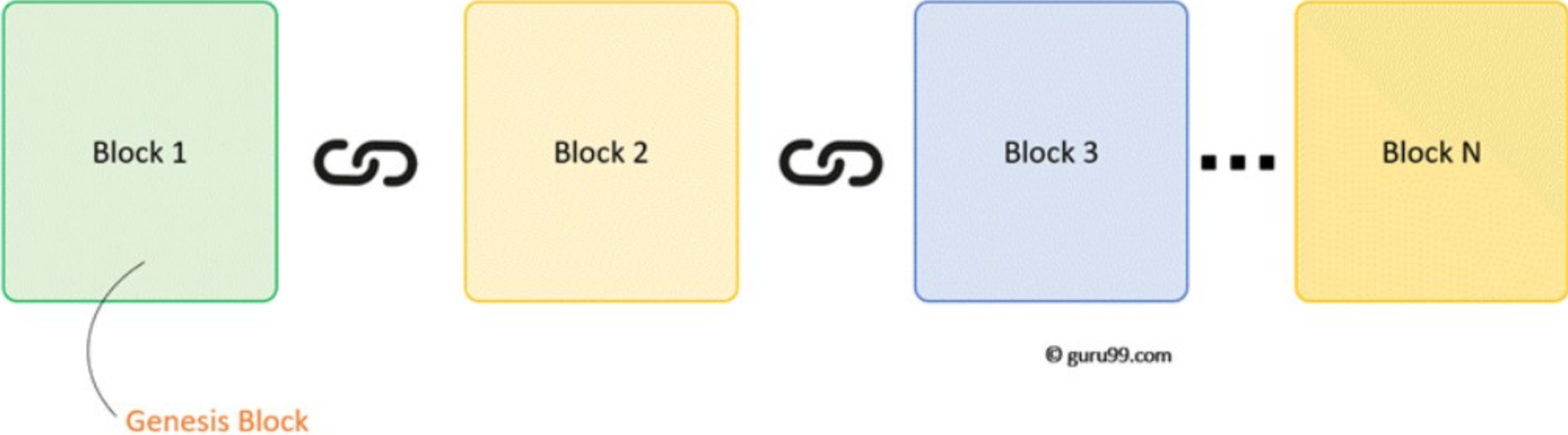
Summary

- A Blockchain is a chain of blocks that contain information
- The blockchain is not Bitcoin, but it is the technology behind Bitcoin
- Every block contains hash.
- Each block has a hash of the previous block
- Blockchain require Proof of Work before a new block is added
- The blockchain database is disturbed amongst multiple peers and is not centralized.
- Block chain technology is Resilience, Decentralize, Time reducing, reliable and its offers unalterable transitions
- The blockchain is Available in three different variants 1) Public 2) Private 3) Consortium
- Higher cost, slower transactions, small ledger, the risk of error are some disadvantage of using this technology

Blockchain Architecture

Now in this Blockchain Technology tutorial, let's study the Blockchain architecture by understanding its various components:

Blockchain is chain of Blocks that contains Data



Understanding Block- Hash

A block also has a hash. A can be understood as a fingerprint which is unique to each block. It identifies a block and all of its contents, and it's always unique, just like a fingerprint. So once a block is created, any change inside the block will cause the hash to change.

Therefore, the hash is very useful when you want to detect changes to intersections. If the fingerprint of a block changes, it does not remain the same block.

HASH:

7E0CE566ED2900D81508C7
768A05A4A50CCBC3632E72
EE8D32DE69636B663362



**Hash acts as a Unique
Fingerprint of the Block**

Each Block has

- 1.Data
- 2.Hash
- 3.Hash of the previous block

Consider following example, where we have a chain of 3 blocks. The 1st block has no predecessor. Hence, it does not contain has the previous block. Block 2 contains a hash of block 1. While block 3 contains Hash of block 2.

Therefore, changing a single block can quickly make all following blocks invalid.



Hence, all blocks are containing hashes of previous blocks. This is the technique that makes a blockchain so secure. Let's see how it works -

Assume an attacker is able to change the data present in the Block 2. Correspondingly, the Hash of the Block also changes. But, Block 3 still contains the old Hash of the Block 2. This makes Block 3, and all succeeding blocks invalid as they do not have correct hash the previous block.



Proof of Work

Hashes are an excellent mechanism to prevent tempering but computers these days are high-speed and can calculate hundreds of thousands of hashes per second. In a matter of few minutes, an attacker can tamper with a block, and then recalculate all the hashes of other blocks to make the blockchain valid again.

To avoid the issue, blockchains use the concept of Proof-of-Work. It is a mechanism which slows down the creation of the new blocks.

A proof-of-work is a computational problem that takes certain to effort to solve. But the time required to verify the results of the computational problem is very less compared to the effort it takes to solve the computational problem itself.

In case of Bitcoin, it takes almost 10 minutes to calculate the required proof-of-work to add a new block to the chain. Considering our example, if a hacker would to change data in Block 2, he would need to perform proof of work (which would take 10 minutes) and only then make changes in Block 3 and all the succeeding blocks.

This kind of mechanism makes it quite tough to tamper with the blocks so even if you tamper with even a single block, you will need to recalculate the proof-of-work for all the following blocks. Thus, hashing and proof-of-work mechanism make a blockchain secure.



However, there is one more method which is used by blockchains to secure themselves, and that's by being distributed.

Instead of using a central entity to manage the chain, Blockchains use a distributed peer-peer network, and everyone is allowed to join. When someone enters this network, he will get the full copy of the blockchain. Each computer is called a node

when any user creates a new block. This new block is sent to all the users on the network. Each node needs to verify the block to make sure that it hasn't been altered. After complete checking, each node adds this block to their blockchain.

All these nodes in this network create a **consensus**. They agree about what blocks are valid and which are not. Nodes in the network will reject blocks that are tampered with.

So, to successfully tamper with a blockchain

1. You will need to tamper with all blocks on the chain
2. Redo the proof-of-work for each block
3. Take control of greater than 50% of the peer-to-peer network.

After doing all these, your tampered block become accepted by everyone else. This is next to impossible task. Hence, Blockchains are so secure. Next in this beginners Blockchain development tutorial, we will learn how a Blockchain transaction works?

Blockchain Variants

Public:

In this type of blockchains, ledgers are visible to everyone on the internet. It allows anyone to verify and add a block of transactions to the blockchain. Public networks have incentives for people to join and free for use. Anyone can use a public blockchain network.

Private:

The private blockchain is within a single organization. It allows only specific people of the organization to verify and add transaction blocks. However, everyone on the internet is generally allowed to view.

Consortium:

In this Blockchain variant, only a group of organizations can verify and add transactions. Here, the ledger can be open or restricted to select groups. Consortium blockchain is used cross-organizations. It is only controlled by pre-authorized nodes.