**Introduction:**

The **term blockchain** was first **described** back **in 1991**. A group of researchers wanted to create a tool to **timestamp digital documents** so that they **could not be backdated or changed**. Further, the technique was adapted and **reinvented by Satoshi Nakamoto**. **In 2008**, Nakamoto created the **first cryptocurrency**, the blockchain-based project **called Bitcoin**.

Logically, a blockchain is a **chain of blocks** which contain specific information (database), but **in a secure and genuine way** that is **grouped together** **in a network** (peer-to-peer).

In other words, blockchain is a combination of computers linked to each other instead of a central server, **meaning that the whole network is decentralized**.

**The core characteristics:**

* Decentralization – meaning no central server maintained
* Accountability,
* Security.

**Benefits of Blockchain:**

* This technique can **improve operational efficiency** and **save costs** significantly.
* The blockchain technique allows digital information to be distributed, rather than copied. This distributed ledger provides **transparency, trust, and data security.**

**Distributed Ledger:**

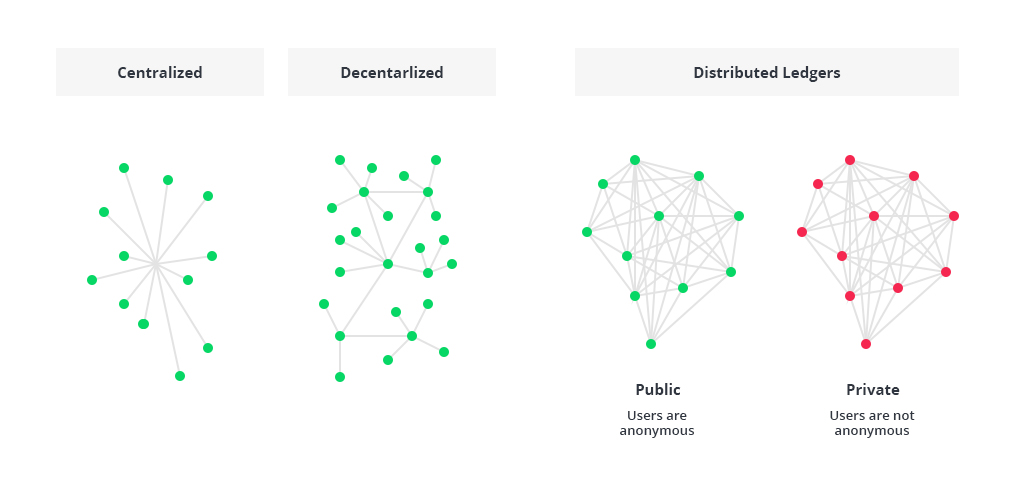
A distributed ledger is a database **held and updated** independently **by each participant** (or node) **in a large network**.

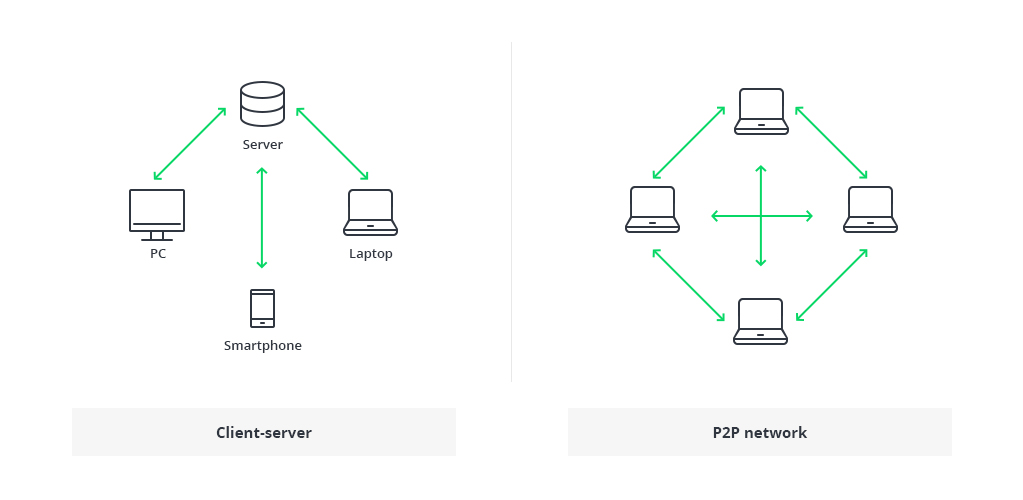
**P2P network:**

Peer-to-Peer (P2P) technology is **based on the decentralization concept**, which lets **network participants conduct transactions without needing any middleman**, intermediaries **or central server.**

**Blockchain Structure:**

The blockchain is organized as a series of “blocks” that are “chained” together.





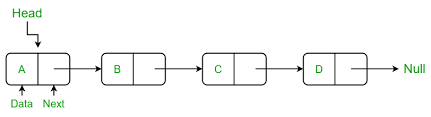
The **traditional architectur**e of the World Wide Web **uses a client-server network**. In this case, the server keeps all the required information in one place so that it is easy to update, due to the server **being a centralized database controlled by several administrators with permissions**.

In the case of the distributed **network of blockchain** architecture, each participant within the network maintains, approves, and updates new entries. The system is **controlled** not only byseparate individuals, but **by everyone within the blockchain network**.

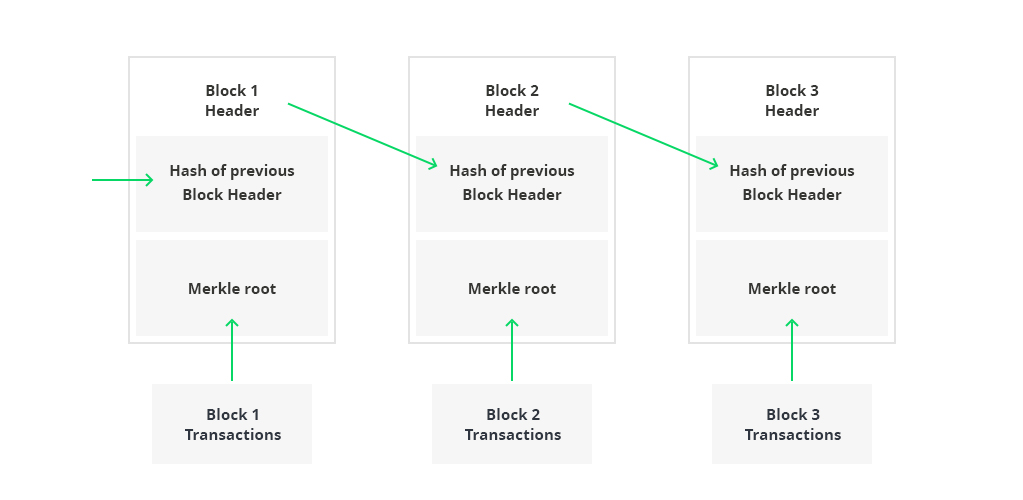
Each member **ensures that all records and procedures are in order**, which **results in data validity and security**. Thus, parties that do not necessarily trust each other are able to reach a common consensus.

The structure of blockchain technology is represented by a list of blocks with transactions in a particular order. These lists can be **stored as a flat file** (txt. format) or **in the form of a simple database**. Two vital data structures used in blockchain include:

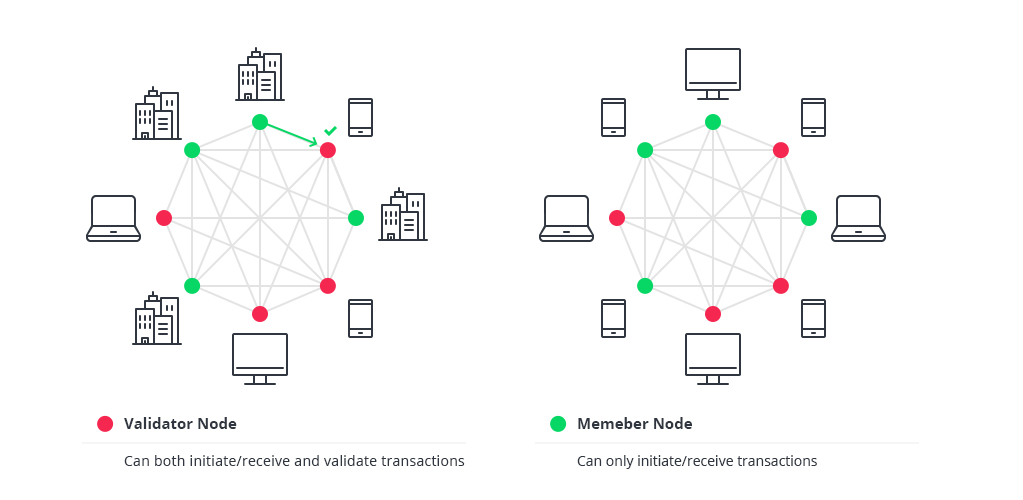
* **Pointers** - variables that **keep information about the location** of another variable. Specifically, this is pointing to the position of another variable.
* **Linked lists** - a sequence of blocks where **each block has specific data and links to the following block with the help of a pointer.**



Logically, the **first block does not contain the pointer** since this one is the first in a chain. At the same time, there is potentially going to be a final block within the blockchain database that has a pointer with no value.



### **Types of Blockchain Architecture Explained**



**Validator node:**

A [validator node](https://www.zeeve.io/validator-nodes/) is a participant in the network that has the role of **validating and relaying transactions**. Validators are fundamental to the functioning and security of a [blockchain network](https://www.zeeve.io/platform/).

**Member node:**

It is also a participant in the network that can **only initiate or receive transactions**.

All blockchain structures fall into **three categories**:

* Public blockchain architecture
* Private blockchain architecture
* Consortium blockchain architecture

**Public blockchain architecture**

A public blockchain architecture means that the **data and access** to the system is available **to anyone** who is willing to participate (e.g. Bitcoin, Ethereum, and Litecoin blockchain systems are public).

**Private blockchain architecture**

As opposed to public blockchain architecture, the private system is **controlled only by** users from a specific organization or **authorized users** who have an invitation for participation.

**Consortium blockchain architecture**

This blockchain structure can consist of a few organizations. In a consortium, procedures are set up and **controlled by the preliminary assigned users.**

The following table provides a detailed comparison among these three blockchain systems:

|  |  |  |  |
| --- | --- | --- | --- |
| Property | Public blockchain | Consortium blockchain | Private blockchain |
| Consensus determination | All miners | Selected set of nodes | Within one organization |
| Read permission | Public | Public or restricted | Public or restricted |
| Immutability level | Almost impossible to tamper | Could be tampered | Could be tampered |
| Efficiency (use of resources) | Low | High | High |
| Centralization | No | Partial | Yes |
| Consensus process | Permissionless | Needs permission | Needs permission |

A private blockchain is considered more centralized since it is controlled by a particular group with increased privacy. On the contrary, a public blockchain is open-ended and thus decentralized.

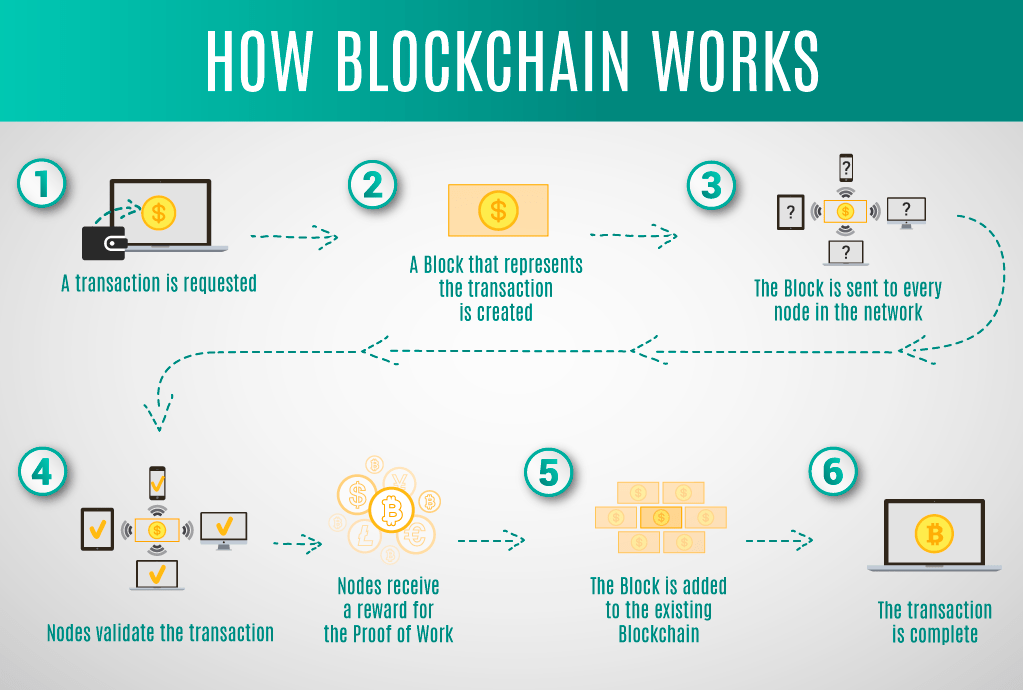
In a public blockchain, all records are visible to the public and anyone could take part in the agreement process. On the other hand, this is less efficient since it takes a considerable amount of time to accept each new record into the blockchain architecture.

In terms of efficiency, the time for each transaction in a public blockchain is less eco-friendly since it requires a huge amount of computation power compared to private blockchain architecture.

These are the core blockchain **architecture components**:

* **Node** - **user or computer** within the blockchain architecture (each has an independent copy of the whole blockchain ledger)
* **Transaction** - **smallest building block** of a blockchain system (records, information, etc.) that **serves as the purpose of blockchain**
* **Block** - a data structure used for **keeping a set of transactions** which is distributed to all nodes in the network
* **Chain** - a **sequence of blocks** in a specific order
* **Miners** - specific nodes which **perform the block verification** process before adding anything to the blockchain structure
* **Consensus (consensus protocol)** - a **set of rules and arrangements** to carry out blockchain operations

Any new record or transaction within the blockchain implies the building of a new block. Each record is then proven and digitally signed to ensure its genuineness. Before this block is added to the network, it should be verified by the majority of nodes in the system.



Each blockchain block consists of:

* certain data
* the hash of the block
* the hash from the previous block

The **data** stored **inside each block depends on the type of blockchain**. For instance, in the Bitcoin blockchain structure, the block maintains data about the receiver, sender, and the amount of coins.

A hash is **like a fingerprint** (long record consisting of some digits and letters). Each block hash is **generated with the help of a cryptographic hash algorithm** (SHA 256). Consequently, this helps to **identify each block** in a blockchain structure easily. The moment a block is created, it **automatically attaches a hash**, while any **changes made in a block affect the change of a hash** too. Simply stated, **hashes help to detect any changes in blocks.**

The final element within the block is the **hash from a previous block**. This creates a chain of blocks and is the main element behind blockchain architecture’s security. As an example, block 45 points to block 46. The very first block in a chain is a bit special - all confirmed and validated blocks are derived from the genesis block.

Any corrupt attempts provoke the blocks to change. All the following blocks then carry incorrect information and render the whole blockchain system invalid.

On the other hand, in theory, it could be possible to adjust all the blocks with the help of strong computer processors. However, there is a solution that eliminates this possibility called **proof-of-work**. This allows a user to **slow down the process of creation of new blocks**. **In Bitcoin** blockchain architecture, it takes around **10 minutes** **to** determine the necessary proof-of-work and **add a new block to the chain**. This work is done by miners - special nodes within the Bitcoin blockchain structure. Miners get to keep the transaction fees from the block that they verified as a reward.

Each new user (node) joining the peer-to-peer network of blockchain receives a full copy of the system. Once a new block is created, it is sent to each node within the blockchain system. Then, each node verifies the block and checks whether the information stated there is correct. If everything is alright, the block is added to the local blockchain in each node.

All the nodes inside a blockchain architecture create a consensus protocol. A consensus system is a set of network rules, and if everyone abides by them, they become self-enforced inside the blockchain.

For example, the Bitcoin blockchain has a consensus rule stating that a transaction amount must be cut in half after every 200,000 blocks. This means that if a block produces a verification reward of 10 BTC, this value must be halved after every 200,000 blocks.

As well, there can only be 4 million BTC left to be mined, since there is a **maximum of 21 million BTC** laid down in the Bitcoin blockchain system by the protocol. **Once the miners unlock this many, the supply of Bitcoins ends unless the protocol is changed.**