**Blockchain**

Blockchain is a distributed software network that functions both as a digital ledger and a mechanism enabling the secure transfer of assets without an intermediary. Just as the internet is a technology that facilitates the digital flow of information, blockchain is a technology that facilitates the digital exchange of units of value.

Blockchain is the backbone Technology of Digital CryptoCurrency BitCoin. The blockchain is a distributed database of records of all transactions or digital event that have been executed and shared among participating parties. Each transaction verified by the majority of participants of the system. It contains every single record of each transaction. BitCoin is the most popular cryptocurrency an example of the blockchain. Blockchain Technology first came to light when a person or Group of individuals name ‘Satoshi Nakamoto’ published a white paper on “*BitCoin: A peer to peer electronic cash system*” in 2008. Blockchain Technology Records Transaction.

**What do you mean by block in blockchain?**

**Blocks** are files where data pertaining to the Bitcoin network are permanently recorded. A **block** records some or all of the most recent Bitcoin transactions that have not yet entered any prior **blocks**. Thus, a **block** is like a page of a ledger or record book.

**In other words Blockchain is a decentralized computation and information sharing platform that enables multiple authoritative domains, who do not trust each other , to cooperate, coordinate and collaborate in a rational decision making process.**

Bitcoin: (**₿**) is a [cryptocurrency](https://en.wikipedia.org/wiki/Cryptocurrency) invented in 2008 by an unknown person or group of people using the name [Satoshi Nakamoto](https://en.wikipedia.org/wiki/Satoshi_Nakamoto) and started in 2009 when its implementation was released as [open-source software](https://en.wikipedia.org/wiki/Open-source_software). It is a decentralized [digital currency](https://en.wikipedia.org/wiki/Digital_currency) without a [central bank](https://en.wikipedia.org/wiki/Central_bank) or single administrator that can be sent from user to user on the [peer-to-peer bitcoin network](https://en.wikipedia.org/wiki/Bitcoin_network) without the need for intermediaries. Transactions are verified by network [nodes](https://en.wikipedia.org/wiki/Node_(networking)) through [cryptography](https://en.wikipedia.org/wiki/Cryptography) and recorded in a public [distributed ledger](https://en.wikipedia.org/wiki/Distributed_ledger) called a [blockchain](https://en.wikipedia.org/wiki/Bitcoin#Blockchain). Bitcoins are created as a reward for a process known as [mining](https://en.wikipedia.org/wiki/Bitcoin#Mining). They can be exchanged for other currencies, products, and services.

20 november 2015 : 1 Bitcoin = 21,598 Indian rupees

25 november 2016 : 1 Bitcoin = 50,404 Indian rupees

24 november 2017: 1 Bitcoin = 5,67,706 Indian rupees

15 december 2017 : 1 Bitcoin = 12,59,035 Indian rupees

14 december 2018 : 1 Bitcoin = 2,28,890 Indian rupees

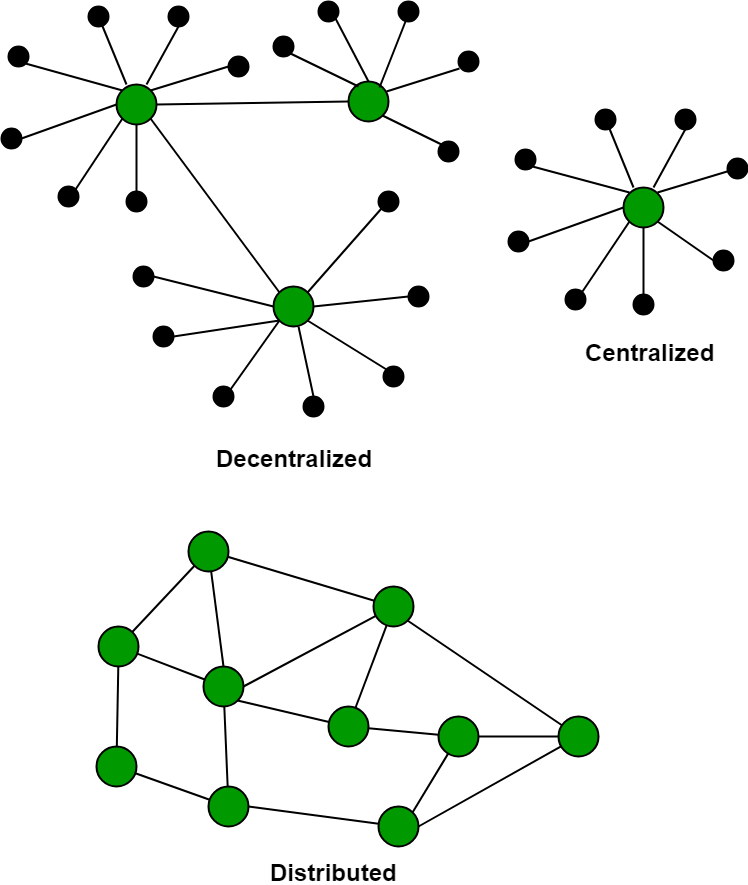
23 august 2019 : 1 Bitcoin = 7,25,701 Indian rupees

03 september 2020: 1 Bitcoin = 8,36,981 Indian rupees

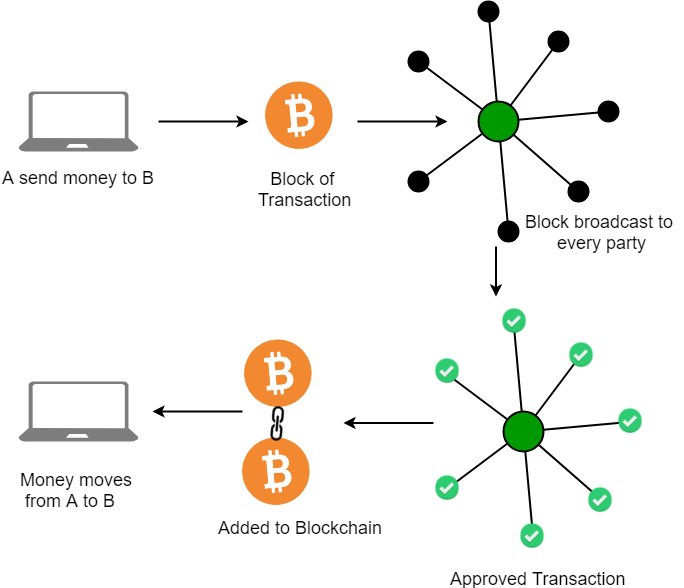
**Many people confuse and believe blockchain to be bitcoin. But, bitcoin is one application of the blockchain technology. There are many other applications and use cases that can be solved using blockchain other than just payment systems.**

**Peer to Peer Network –**  
A peer to peer network is a distributed application architecture that consists of computing devices connected to each other, without a central server.

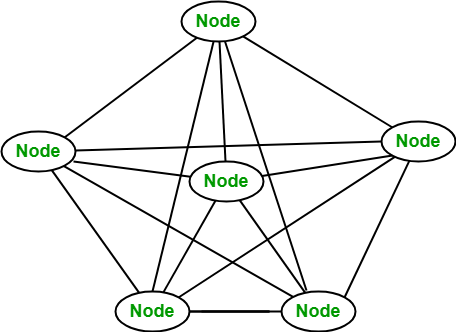
In centralised networks, the security is dependent on a single entity. If that central server is attacked, the security of the overall network is compromised. But a peer to peer network is more secure as there is no single point of failure.



**How Blockchain Technology works?**  
One of the famous use of Blockchain is Bitcoin. The bitcoin is a cryptocurrency and is used to exchange digital assets online. Bitcoin uses cryptographic proof instead of third-party trust for two parties to execute transactions over the internet. Each transaction protects through **digital signature (**A **digital signature** is a mathematical technique used to validate the authenticity and integrity of a message, software or **digital** document.).  
The data is distributed over Millions of Computers around the world which are connected with the Blockchain. This system allows Notarization of Data as it is present on every Node and is publicly verifiable.

****

**A network of nodes:** A node is a computer connected to the Blockchain Network. Node gets connected with Blockchain using the client. Client helps in validating and propagates transaction on to the Blockchain. When a computer connects to the Blockchain, a copy of the Blockchain data gets downloaded into the system and the node comes in sync with the latest block of data on Blockchain. The Node connected to the Blockchain which helps in the execution of a Transaction in return for an incentive is called Miners.

****

**Disadvantages of current transaction system:**

* Cash can only be used in low amount transaction locally.
* Huge waiting time in the processing of transactions.
* Need to third party for verification and execution of Transaction make the process complex.
* If the Central Server like Banks is compromised, whole System is affected including the participants.
* Organization doing validation charge high process thus making the process expensive.

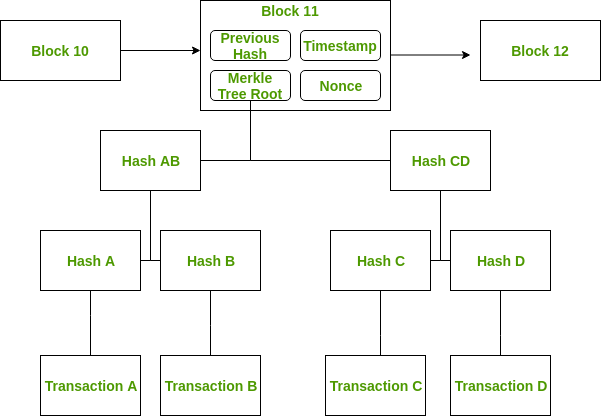
**Benefits of Blockchain Technology:**

* **Time-saving:** No central Authority verification needed for settlements making the process faster and cheaper.
* **Cost-saving:** A Blockchain network reduces expenses in several ways. No need for third-party verification. Participants can share assets directly. Intermediaries are reduced. Transaction efforts are minimized as every participant has a copy of shared ledger.
* **Tighter security:** No one can temper with Blockchain Data as it shared among millions of Participant. The system is safe against cybercrimes and Fraud.

**What is inside a blockchain?**

A blockchain is a chain of blocks connected to each other. A block consists of four parts:

* Previous Hash
* The timestamp
* Nonce
* Merkle tree root



**Figure –** A block in a blockchain

Each block contains a cryptographic hash of the data of the previous block. The nonce is calculated by the miners by solving a cryptographic puzzle to propose the next block in the chain. It is known as proof of work. The blockchain is said to be immutable because of its cryptographic properties. But this does not mean that changing the data is impossible. It means that it is extremely hard to change the data and any change can be easily detected. A merkle tree is a binary tree with hash pointers. A merkle tree is a structure that allows for efficient and secure verification of content in a large body of data. The advantage of using merkle trees is that proving membership requires O(logn) steps. Also, in a sorted merkle tree, non-membership can also be proved in O(logn) steps. The first block is known as the genesis block.

**Advantages of Blockchain**  
1. Blockchains are expected to be implemented by most businesses because of the several benefits it provides.

2.The blockchain eliminates the need of a third party between two entities that are willing to exchange something.

3.This saves time as exchanges can be done without any outside interference. It saves money as it reduces overhead and cost of intermediaries.

4. It reduces risk of tampering, fraud and cyber crime due to its immutable nature.

5. There is no need to trust a third party now as the records are stored in distributed ledgers.

**Types of Blockchain**  
There are different types of blockchains possible in the ecosystem.

1. **Public –**  
   A public blockchain is also known as permission-less blockchain. Here, everyone can be a part of this blockchain and can participate by running as a node, by mining a block or by making transactions in the blockchain. Bitcoin and Litecoin are examples of public blockchains.
2. **Private –**  
   A private blockchain is also known as permissioned blockchain. Here, there are restrictions on the participation as only selected individuals or member of an organisation can be a part of the blockchain. Multichain and Hyperledger projects (Fabric, Sawtooth) are examples of private blockchain.
3. **Consortium (an association)–**  
   A consortium blockchain are said to be partially-decentralised or semi-decentralised. It is controlled by a group of organisations unlike one organisation as in private blockchain. The member organisations has the authority to participate by running as a full node, by mining etc. R3 and EWF (Energy Web Foundation) are examples of consortium blockchain.

**Blockchain architecture:**

Mostly people think that Blockchain is Bitcoin and vice-versa. But it’s not the case. In fact, [Bitcoin](https://www.geeksforgeeks.org/what-is-bitcoin/) is a digital currency or cryptocurrency that works on [Blockchain Technology](https://www.geeksforgeeks.org/blockchain-technology-introduction/).

As the name suggests, blockchain is a chain of blocks that contains information. Each block consists of a number of transactions and each transaction is recorded in the form of Hash. Hash is a unique address assigned to each block during its creation and any further modification in the block will lead to a change in its hash.

A block has mainly 3 parts:

1. Data/Information part- contain the information of the transaction incurred
2. Hash- Unique ID of block
3. Previous Hash- Hash of previous block

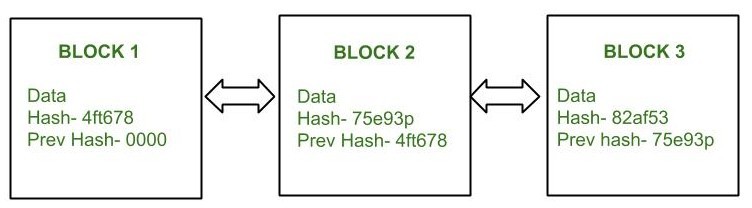


Figure – Blockchain architecture

Blockchain vs Bitcoin

Bitcoin is a crypto-currency (a kind of digital currency), mainly created to simplify a transaction without having third-party intermediaries. It all started when this mysterious man under the name of**Satoshi Nakamoto**(whose actual identity is still unknown) published a white-paper named **Bitcoin: A Peer-to-Peer Electronic Cash System** in 2009. **A Satoshi is the smallest unit of Bitcoin. A unit of Satoshi is equal to 0.00000001 bitcoin.**

**The most interesting part here is that these Bitcoins are not issued by any centralised banks or authorities. They are ‘mined’ by a group of people called as ‘miners’**. They solve complex mathematical problems/puzzles and are issued a certain number of Bitcoins in exchange.

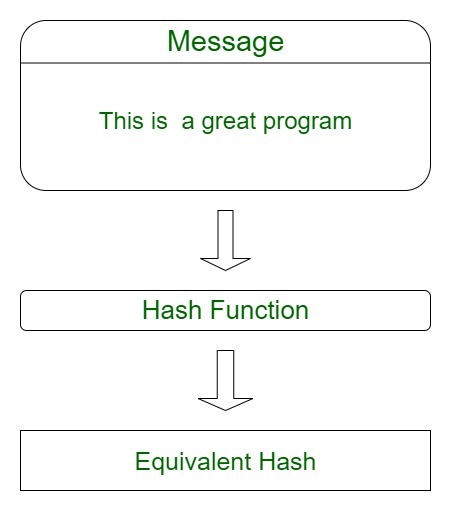
[**Blockchain**](https://www.geeksforgeeks.org/blockchain-technology-introduction/)  
Blockchain is a data structure or ledger that stores information about any transactions that occurs(not just bitcoin). Anything that is stored once can’t be changed or modified. This feature of Blockchain makes it the most secure. It is **decentralized** and establishes a **peer to peer** network thus eliminating any middle-men.

Blockchain is made up of blocks that are stored in a chronological order. Each block has a capacity of around 500 transactions on an average. Thanks to the cryptography involved, these blocks are extremely secure. Each block will a unique ‘hash’ value attached to it which is calculated based on the data stored in the block. Every-time a new block is added to the chain, the new block contains the hash of the previous block as well. So modifying the contents of any previous block is practically impossible(and would destroy the whole chain). This makes Block-chain **immutable**.

**Blockchain Hash Function**

[Blockchain](https://www.geeksforgeeks.org/blockchain-technology-introduction/) is a constantly growing ledger that keeps a permanent record of all the transactions that have taken place, in a secure, chronological and immutable way. To make the data secure blockchain uses hash function.

**Hashing:**  
In simple terms, hashing means taking an input string of any length and giving out an output of a fixed length. The fixed-length output is called an equivalent hash or simply hash.

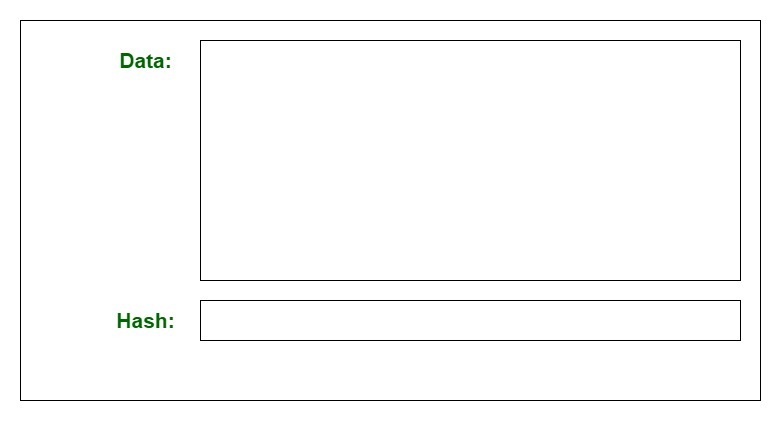


**Types of cryptographic hash functions:**

* Secure Hashing Algorithm (SHA-2 and SHA-3)
* RACE Integrity Primitives Evaluation Message Digest (RIPEMD)
* Message Digest Algorithm 5 (MD5)
* BLAKE2

**SHA-256:**  
SHA-256 is the most famous of all cryptographic hash functions because it’s used extensively in blockchain technology. SHA-256 Hashing algorithm was developed by the National Security Agency (NSA) in 2001.

**Hashing process:**  
For this hash function we can use [Anders Brownworth Hash Program](https://andersbrownworth.com/blockchain/hash), a program developed by Anders Brownworth.



If we type any character in the data section, we will observe its corresponding cryptographic hash in the hash section.



**Small Changes In The Input Changes the Hash:**  
If we make a small change in the input, the equivalent hash produced will be entirely different.



Changing the capital “T” to small “t” completely changed the equivalent hash.

It is very difficult to determine the original string from the equivalent hash but its not impossible. The only method to determine the original string from its hash is by using “brute-force”. Brute-force basically means that we have to take random inputs, hash them and compare them with the target hash.

There can be basically three scenarios:

1. **Best case scenario:**  
   We get our answer on the first try. The odds of this happening are astronomical.
2. **Average case scenario:**  
   In case of SHA-256 we get our answer after 2^256/2 = 2^255 times. In other words, its a huge number.
3. **Worst case scenario:**  
   We get our answer at the end of data.

Attention reader! Don’t stop learning now. Get hold of all the important DSA concepts with the [**DSA Self Paced Course**](https://practice.geeksforgeeks.org/courses/dsa-self-paced?utm_source=geeksforgeeks&utm_medium=article&utm_campaign=gfg_article_dsa_content_bottom) at a student-friendly price and become industry ready.

Distributed ledger

A **distributed ledger** (also called a **shared ledger** or **distributed ledger technology** or **DLT**) is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions. Unlike with a [distributed database](https://en.wikipedia.org/wiki/Distributed_database), there is no central administrator.

A [peer-to-peer](https://en.wikipedia.org/wiki/Peer-to-peer) network is required as well as [consensus](https://en.wikipedia.org/wiki/Consensus_(computer_science)) algorithms to ensure replication across nodes is undertaken. One form of distributed ledger design is the [blockchain](https://en.wikipedia.org/wiki/Blockchain) system, which can be either public or private.

**Digital Money to Distributed Ledgers**

Underlying **distributed ledgers** is the same technology that is used by **blockchain**, which bitcoin uses as its **distributed ledger**. A **distributed ledger** can be described as a **ledger** of any transactions or contracts maintained in decentralized form across different locations and people.

Is distributed ledger technology the same as Blockchain?

The most important difference to remember is that **blockchain** is just one type of **distributed ledger**. Although **blockchain** is a sequence of blocks, **distributed ledgers** do not require such a chain. Furthermore, **distributed ledgers** do not need proof of work and offer – theoretically – better scaling options.

**Protocols used in blockchain**

Enterprise blockchain protocol or blockchain protocols are designed to maintain different aspects of blockchain. This means that there are blockchain security protocols, **network protocols**, and blockchain consensus protocols. All these protocols, when combined, mainly combine into becoming a blockchain framework.

**What is distributed ledger technology and how does it work?**

Distributed ledger technology (DLT) is a digital system for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time. Unlike traditional **databases**, distributed ledgers have no central data store or administration functionality.

**What are Blockchain protocols?**

A **blockchain protocol** is a common term for consensus methods. These methods are different systems that are implemented to reach consensus and validate transactions within a **blockchain** network. Some of them require investors to purchase physical mining.

**How many Blockchain protocols are there?**

The world got introduced to the **blockchain** with the Bitcoin network. Following different objectives and use cases that were envisioned, different **protocols** were designed. We will look at the key features of three major **blockchain protocols**

**How do you create a Blockchain protocol?**

**Step-by-step Guide**

1. Find Your Niche. ...
2. Design a Workflow for **Blockchain** Integration. ...
3. Choose Between New and Existing **Blockchain**. ...
4. Choose Between Private and Public **Blockchain**.
5. Choose a Relevant Consensus Mechanism.
6. Choose a Relevant Platform. ...
7. Decide Whether You Need Smart Contracts. ...
8. **Making** a Final Decision.

**Consensus in blockchain**

What Is a **Consensus** Mechanism? A **consensus** mechanism is a fault-tolerant mechanism that is used in computer and **blockchain** systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies.

All the decisions are taken by the leader or a board of decision makers. This isn’t possible in a [blockchain](https://blockgeeks.com/guides/what-is-blockchain-technology/) because a blockchain has no “leader”. For the blockchain to make decisions, they need to come to a consensus using “consensus mechanisms”.

So, how do these consensus mechanisms work and why did we need them? What are some of the consensus mechanisms used in cryptocurrencies?

**What are consensus mechanisms?**

“Consensus decision-making is a group decision-making process in which group members develop, and agree to support a decision in the best interest of the whole. Consensus may be defined professionally as an acceptable resolution, one that can be supported, even if not the “favourite” of each individual. Consensus is defined by Merriam-Webster as, first, general agreement, and second, group solidarity of belief or sentiment.”

In simpler terms, consensus is a dynamic way of reaching agreement in a group. While voting just settles for a majority rule without any thought for the feelings and well-being of the minority, a consensus on the other hand makes sure that an agreement is reached which could benefit the entire group as a whole.

From a more idealistic point-of-view, Consensus can be used by a group of people scattered around the world to create a more equal and fair society.

A method by which consensus decision-making is achieved is called “consensus mechanism”.

So now what we have defined what a consensus is, let’s look at what the objectives of a consensus mechanism are

* **Agreement Seeking:** A consensus mechanism should bring about as much agreement from the group as possible.
* **Collaborative:** All the participants should aim to work together to achieve a result that puts the best interest of the group first.
* **Cooperative:** All the participants shouldn’t put their own interests first and work as a team more than individuals.
* **Egalitarian:** A group trying to achieve consensus should be as egalitarian as possible. What this basically means that each and every vote has equal weightage. One person’s vote can’t be more important than another’s.
* **Inclusive:** As many people as possible should be involved in the consensus process. It shouldn’t be like normal voting where people don’t really feel like voting because they believe that their vote won’t have any weightage in the long run.
* **Participatory:** The consensus mechanism should be such that everyone should actively participate in the the overall process.

**Which consensus mechanisms should be used for an entity like blockchain.**

Before bitcoin, there were loads of iterations of peer-to-peer decentralized currency systems which failed because they were unable to answer the biggest problem when it came to reaching a consensus. This problem is called “[Byzantine Generals Problem](https://en.wikipedia.org/wiki/Byzantine_fault_tolerance)”.

**Permission in Blockchain**

A **blockchain** can be built and accessed in multiple ways. There are certain other **blockchains** that need special **permissions** to read, access, and write information on them. ... It may also include maintaining the identity of each **blockchain** participant on the network. Such **blockchains** are called permissioned **blockchains**.

**Is ethereum permission Blockchain?**

With respect to permissioning, **Ethereum** is a public, permissionless **blockchain**. Some groups, mostly industry consortia, have adapted **Ethereum's** open-source protocol to run their own **permissioned**, private instance of **Ethereum**. .

### ****Permissioned and Permissionless Blockchains:****

The basic distinction of these is clear from the terms itself. A permissioned blockchain needs prior approval before using whereas a permissionless blockchain lets anyone participate in the system. Though the two systems might sound similar, they cannot be used for the same things. People might not be keen on using a permissioned cryptocurrency as one of the major drawbacks of crypto is that no one has control over how it works. For example, a company like Maersk, that uses [**blockchain technology**](https://www.blockchain-council.org/blockchain-certification/) to track its shipping logistics, will not want to store its confidential information onto a permissionless blockchain.

### ****Advantages of Permissioned Blockchains****

Some of the notable advantages are:

* **These offer more efficient performance when compared to public blockchain networks.**
* **These have clearly defined governance structures.**
* **High customizability.**
* **Access controls.**
* **Better Scalability.**

### ****Disadvantages of Permissionless Blockchains****

Some of the prominent disadvantages are:

* **Security is entirely reliant on the integrity of its members.**
* **These are more prone to censorship and regulation.**
* **Less Transparent.**
* **Vulnerable to hacks and manipulation.**
* **Less anonymous.**

### ****Advantages and Disadvantages of Permissionless Blockchains****

These are the most reliable in terms of security as the chances for collusion by bad actors with malicious intentions is minimum. These potential events are softened by the high number of nodes present in the network. Anyone will be able to access the ledger and check the correctness of transactions or see if the data entered is consistent. As these are widely-open, anyone can use it without creating any additional infrastructure. These are some of the notable advantages of permissionless blockchains.

The major drawback is that they are quite slow. They can validate only a limited number of transactions per second. These entail a high amount of energy consumption. One of the biggest threats of these blockchains is the 51% attack risk. A small number of nodes have the ability to make the network more vulnerable to hacking risks and collusions.

### ****Conclusion****

Both permissioned and permissionless blockchains are branches of the same technology that have been developed for different needs. Both have their own advantages and can help benefit different technologies depending on the use cases.

**Privacy in Blockchain**

A key aspect of **privacy in blockchains** is the use of private and public keys. **Blockchain** systems use asymmetric cryptography to secure transactions between users. In these systems, each user has a public and private key. ... Public keys can be shared with other users in the network because they give away no personal data.

**Can Blockchain be private?**

A **private blockchain** is an invitation-only network governed by a single entity. Entrants to the network require permission to read, write or audit the **blockchain**. There **can** be different levels of access and information **can** be encrypted to protect commercial confidentiality.

**What is the point of a private Blockchain?**

In a **blockchain** that is **private**, each user does not have equal rights within it. Users are granted permissions to access certain types of data and complete specific functions. Everything else remains closed. The mechanism of access depends on the rules set forth by the network creator.

**Blockchain architecture and design**

We will describe the blockchain structure, its components, and their interaction, namely:

* Nodes within P2P network
* Properties of block & genesis block
* Transactions within the ledger
* The validation process - mining
* The “consensus” within a blockchain architecture
* Proof-of-work

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.

In general, blockchain technology has the core characteristics of decentralization, accountability, and security. This technique can improve operational efficiency and save costs significantly. The demand and usage of applications built on blockchain architecture will only evolve. Thus, it makes now the right time to get educated on this topic.