Contents

[**What is Blockchain?** 3](#_Toc80634234)

[What Blockchain is NOT! 3](#_Toc80634235)

[Blockchain Architecture 4](#_Toc80634236)

[What is a Block? 4](#_Toc80634237)

[Proof of Work 6](#_Toc80634238)

[Distributed P2P Network 7](#_Toc80634239)

[How Blockchain Transaction Works? 8](#_Toc80634240)

[Why do we need Blockchain? 8](#_Toc80634241)

[Blockchain versions 9](#_Toc80634242)

[Blockchain Variants 9](#_Toc80634243)

[Blockchain Use Cases 10](#_Toc80634244)

[Important Real-Life Use Cases of Blockchain 11](#_Toc80634245)

[What is Cryptocurrency? 12](#_Toc80634246)

[What is Bitcoin? 12](#_Toc80634247)

[BlockChain and Bitcoin: 12](#_Toc80634248)

[Blockchain vs. Shared Database 12](#_Toc80634249)

[Myths about Blockchain 13](#_Toc80634250)

[Limitations of Blockchain technology 13](#_Toc80634251)

**What is Blockchain?**

**Blockchain** can be defined as a chain of blocks that contains information. The technique is intended to timestamp digital documents so that it's not possible to backdate them or temper them. The purpose of blockchain is to solve the double records problem without the need of a central server.

The blockchain is used for the secure transfer of items like money, property, contracts, etc. without requiring a third-party intermediary like bank or government. Once a data is recorded inside a blockchain, it is very difficult to change it.

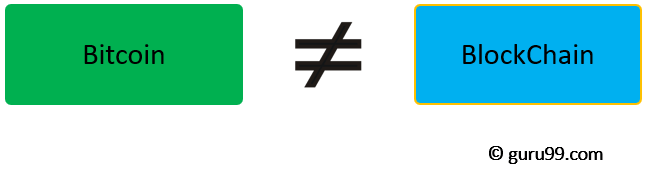
The blockchain is a software protocol (like SMTP is for email). However, Blockchains could not be run without the Internet. It is also called meta-technology as it affects other technologies. It is comprised of several pieces: a database, software application, some connected computers, etc.

Sometimes the term used for Bitcoin Blockchain or The Ethereum Blockchain and sometimes it's other virtual currencies or digital tokens. However, most of them are talking about the distributed ledgers.

In this Blockchain tutorial for beginners, you will learn Blockchain basics like:

* What is Blockchain?
* What Blockchain is NOT!
* Blockchain Architecture
* How Blockchain Transaction Works?
* Why do we need Blockchain?
* Blockchain versions
* Blockchain Variants
* Blockchain Use Cases
* Important Real-Life Use Cases of Blockchain
* Bitcoin cryptocurrency: Most Popular Application of Blockchain
* Blockchain vs. Shared Database
* Myths about Blockchain
* Limitations of Blockchain technology

## What Blockchain is NOT!

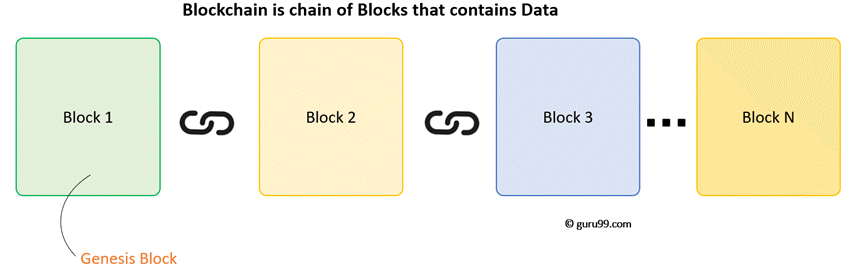


* Blockchain is not Bitcoin, but it is the technology behind Bitcoin
* Bitcoin is the digital token and blockchain is the ledger to keep track of who owns the digital tokens
* You can't have Bitcoin without blockchain, but you can have blockchain without Bitcoin.

## Blockchain Architecture

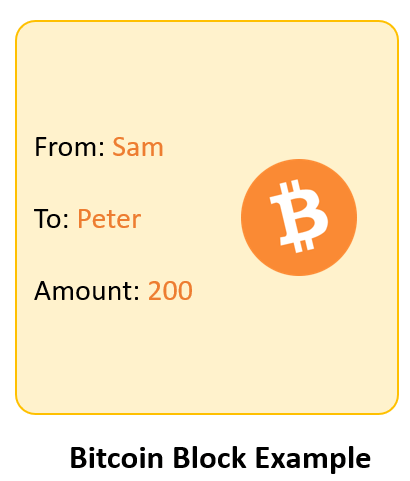
Now in this Blockchain Technology tutorial, let's study the Blockchain architecture by understanding its various components:

## What is a Block?



A Blockchain is a chain of blocks which contain information. The data which is stored inside a block depends on the type of blockchain.

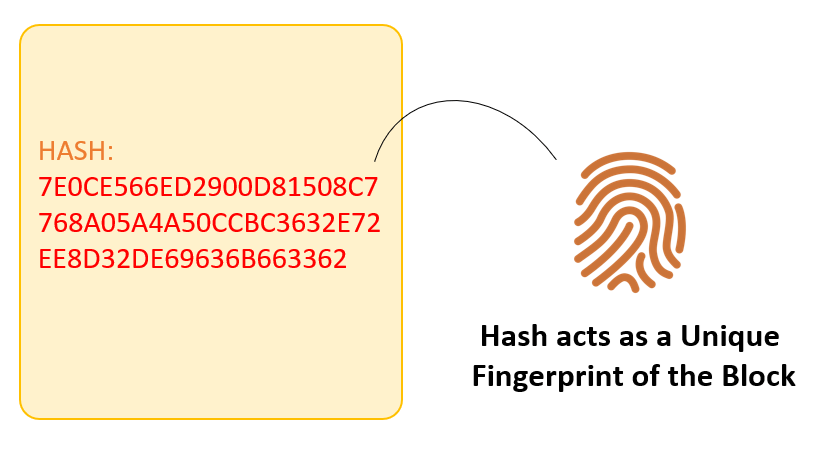
For Example, A Bitcoin Block contains information about the Sender, Receiver, number of bitcoins to be transferred.



The first block in the chain is called the **Genesis block**. Each new block in the chain is linked to the previous block.

**Understanding SHA256 - 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.



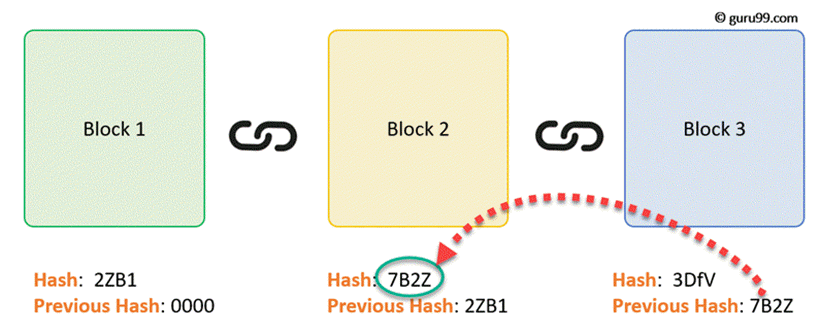
**What is SHA256 Hash**

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.

Each Block has

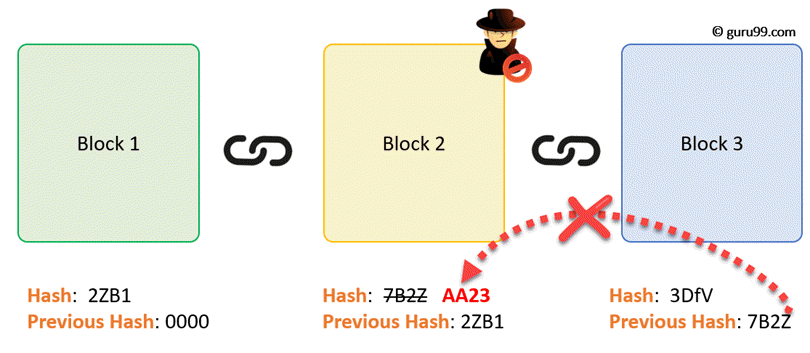
* Data
* Hash
* Hash of the previous block

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.



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.



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

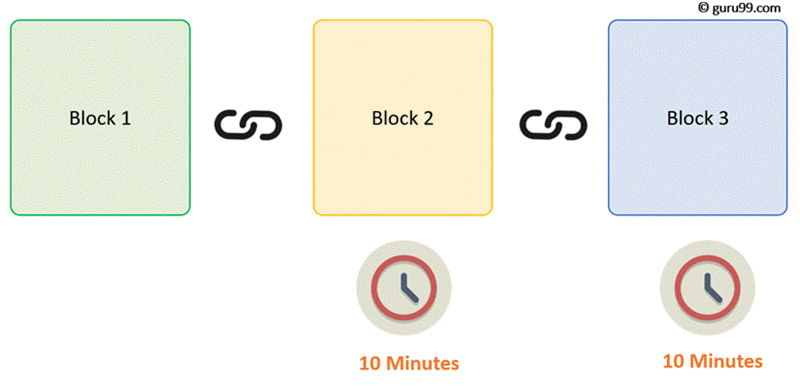
## Proof of Work

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.

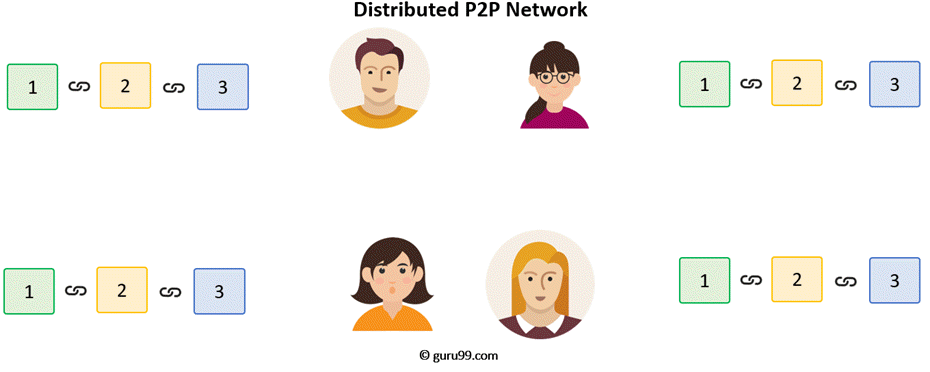
In case of Bitcoin, it takes almost 10 minutes to calculate the required proof-of-work to add a new block to the chain. Considering our example, if a hacker would to change data in Block 2, he would need to perform proof of work (which would take 10 minutes) and only then make changes in Block 3 and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



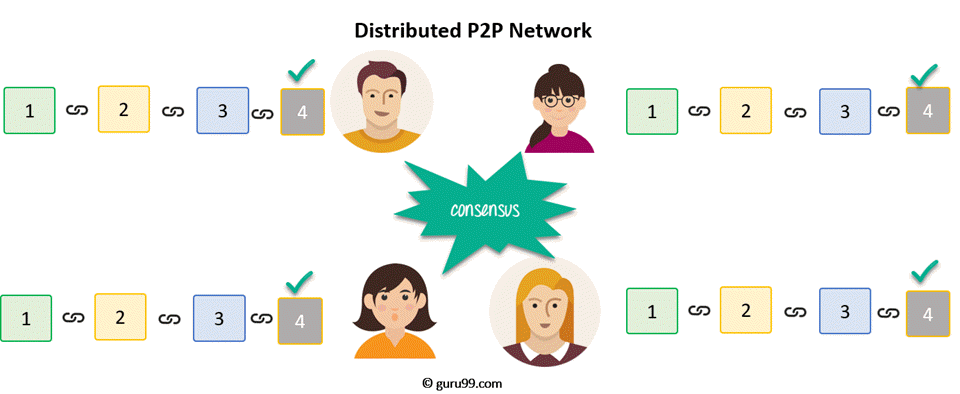
This kind of mechanism makes it quite tough to tamper with the blocks so even if you tamper with even a single block, you will need to recalculate the proof-of-work for all the following blocks. Thus, hashing and proof-of-work mechanism make a blockchain secure.

## Distributed P2P Network

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.



Let's see what happens 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.



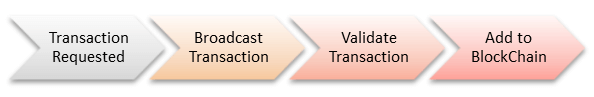
All these nodes in this network create a **consensus**. They agree about what blocks are valid and which are not. Nodes in the network will reject blocks that are tampered with.

So, to successfully tamper with a blockchain

* You will need to tamper with all blocks on the chain
* Redo the proof-of-work for each block
* 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?

## How Blockchain Transaction Works?



**Step 1)** Some person requests a transaction. The transaction could be involved cryptocurrency, contracts, records or other information.

**Step 2)** The requested transaction is broadcasted to a P2P network with the help of nodes.

**Step 3)** The network of nodes validates the transaction and the user's status with the help of known algorithms.

**Step 4)** Once the transaction is complete the new block is then added to the existing blockchain. In such a way that is permanent and unalterable.

## Why do we need Blockchain?

Here, are some reasons why Blockchain technology has become so popular.

**Resilience:** Blockchains is often replicated architecture. The chain is still operated by most nodes in the event of a massive attack against the system.

**Time reduction:** In the financial industry, blockchain can play a vital role by allowing the quicker settlement of trades as it does not need a lengthy process of verification, settlement, and clearance because a single version of agreed-upon data of the share ledger is available between all stack holders.

**Reliability:** Blockchain certifies and verifies the identities of the interested parties. This removes double records, reducing rates and accelerates transactions.

**Unchangeable transactions:** By registering transactions in chronological order, Blockchain certifies the inalterability, of all operations which means when any new block has been added to the chain of ledgers, it cannot be removed or modified.

**Fraud prevention:** The concepts of shared information and consensus prevent possible losses due to fraud or embezzlement. In logistics-based industries, blockchain as a monitoring mechanism act to reduce costs.

**Security:** Attacking a traditional database is the bringing down of a specific target. With the help of Distributed Ledger Technology, each party holds a copy of the original chain, so the system remains operative, even the large number of other nodes fall.

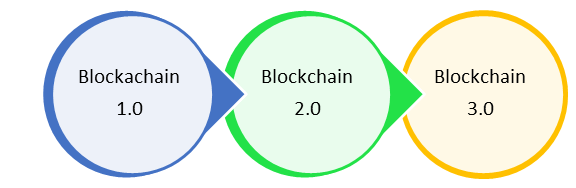
**Transparency:** Changes to public blockchains are publicly viewable to everyone. This offers greater transparency, and all transactions are immutable.

**Collaboration** – Allows parties to transact directly with each other without the need for mediating third parties.

**Decentralized:** There are standards rules on how every node exchanges the blockchain information. This method ensures that all transactions are validated, and all valid transactions are added one by one.

## Blockchain versions

Now in this Blockchain development tutorial, let's learn about Blockchain versions.



**Blockchain 1.0: Currency**

The implementation of DLT (distributed ledger technology) led to its first and obvious application: cryptocurrencies. This allows financial transactions based on blockchain technology. It is used in currency and payments. Bitcoin is the most prominent example in this segment.

**Blockchain 2.0: Smart Contracts**

The new key concepts are Smart Contracts, small computer programs that "live" in the blockchain. They are free computer programs that execute automatically, and check conditions defined earlier like facilitation, verification or enforcement. It is used as a replacement for traditional contracts.

**Blockchain 3.0: DApps:**

DApps is an abbreviation of decentralized application. It has their backend code running on a decentralized peer-to-peer network. A DApp can have frontend Blockchain example code and user interfaces written in any language that can make a call to its backend, like a traditional Apps.

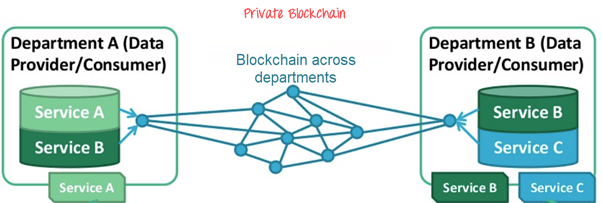
## Blockchain Variants

**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.

## Blockchain Use Cases

Blockchain Technology is used widely in the different sectors as given in the following table.

|  |  |
| --- | --- |
| Sector | Usage |
| Markets | * Billing, monitoring and Data Transfer * Quota management in the Supply Chain Network |
| Government Sector | * Transnational personalized governance services * Voting, propositions P2P bond, * Digitization of documents/ contracts and proof of ownership for transfers * Registry & Identify * Tele-attorney service * IP registration and exchange * Tax receipts Notary service and document registry |
| IOT | * Agricultural & drone sensor networks * Smart home networks * Integrated smartcity. * Smart home sensors * Self-driving car * Personalized robots, robotic component * Personalized drones * Digital Assistants |
| Health | * Data management * Universal EMR Health databanks * QS Data Commons * Big health data stream analytes * Digital health wallet Smart property * Health Token * Personal development contracts |
| Science & Art | * Supercomputing * Crowd analysis * P2P resources * Digital mind fit services |
| Finance & Accounting | * Digital Currency Payment * Payments & Remittance * Decartelized Capital markets using a network of the computer on the Blockchain * Inter-divisional accounting * Clearing & Trading & Derivatives * Bookkeeping |

## Important Real-Life Use Cases of Blockchain

**1.Dubai: The Smart City**

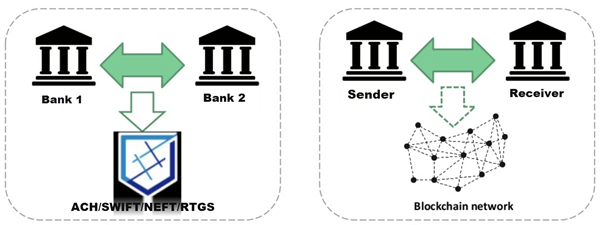
In the year 2016, smart Dubai office introduced Blockchain strategy. Using this technology entrepreneurs and developers will be able to connect with investor and leading companies. The objective is to implement blockchain base system which favors the development of various kind of industries to make Dubai 'the happiest city in the world.'

**2. Incent Customer retention**

Incent is CRaaS (Consumer retention as a service) based on the Blockchain technology. It is a loyalty program which is based on generating token for business affiliated with its related network. In this system, blockchain is exchanged instantaneously, and it can be stored in digital portfolios of user's phone or accessing through the browser.

**3. Blockchain for Humanitarian Aid**

In January 2017 the united nations world food program started a project called humanitarian aid. The project was developed in rural areas of the Sindh region of Pakistan. By using the Blockchain technology, beneficiaries received money, food and all type of transactions are registered on a blockchain to ensure security and transparency of this process.



## What is Cryptocurrency?

A cryptocurrency is one medium of exchange like traditional currencies such as USD, but it is designed to exchange the digital information through a process made possible by certain principles of cryptography. A cryptocurrency is a digital currency and is classified as a subset of alternative currencies and virtual currencies.

Cryptocurrency is a bearer instrument based on digital cryptography. In this kind of cryptocurrency, the holder has of the currency has ownership. No other record kept as to the identity of the owner. In the year 1998, Wei Dai published "B-Money," an anonymous, distributed electronica cash system.

## What is Bitcoin?

Bitcoin was launched in 2009 by an unknown person called Satoshi Nakamoto. Bitcoin is a Peer-to-Peer technology which is not governed by any central authority or banks. Currently, issuing Bitcoins and managing transactions are carried out collectively in the network. It is presently the dominant cryptocurrency of the world. It is open source and designed for the general public means nobody owns the control of the Bitcoin. In fact, there are only 21 million Bitcoins issued. Currently, Bitcoin has a market cap of $12 billion.

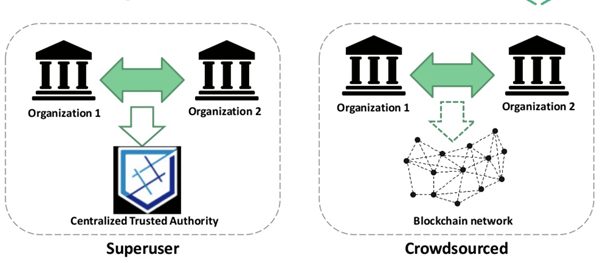
Anyone can use bitcoin without paying any process fees. If you are handling Bitcoin, the sender and receiver transact directly without using a third party.

## BlockChain and Bitcoin:

The blockchain is the technology behind Bitcoin. Bitcoin is the digital token, and blockchain is the ledger that keeps track of who owns the digital tokens. You can't have Bitcoin without blockchain, but you can have blockchain without Bitcoin. Other prominent cryptocurrencies

* Ethereum
* Bitcoin Cash
* Ripple
* Litecoin

## Blockchain vs. Shared Database



|  |  |  |
| --- | --- | --- |
| **Parameters** | **Blockchain** | **Shared Database** |
| Operations | Insert | Create/ Read/ Update and Delete |
| Replication | Full replication on every peer | Master-slave |
| Multi-master |
| Consensus | Most of the peers agree on the outcome of transactions. | Distributed transactions which held in two phases commit and Paxos. |
| Validation | Global rules enforced on the whole blockchain system. | Offers only local integrity constraints |
| Disintermediation | It is allowed with blockchain. | Not allowed. |
| Confidentiality | Fully confidential | Not totally confidential |
| Robustness | Fully robust technology. | Not entirely robust. |

## Myths about Blockchain

|  |  |
| --- | --- |
| **Myth** | **Reality** |
| It solves every problem | No, it is just a database |
| Trustless Technology | It can shift trust and also spread trust |
| Secure | It focuses integrity and not confidentiality |
| Smart contracts are always legal | It only executes parts of some legal contracts |
| Immutable | It only offers probabilistic immutability |
| Need to waste electricity | Emerging blockchains are efficient |
| It is inherently unsalable | Emerging blockchains are scalable |

## Limitations of Blockchain technology

Now in this beginners Blockchain tutorial, we will learn about limitations of Blockchain technology:

**Higher costs:** Nodes seek higher rewards for completing Transactions in a business which work on the principle of Supply and Demand

**Slower transactions:** Nodes prioritize transactions with higher rewards, backlogs of transactions build up

**Smaller ledger:** It not possible to a full copy of the Blockchain, potentially which can affect immutability, consensus, etc.

**Transaction costs, network speed:** The transactions cost of Bitcoin is quite high after being touted as 'nearly free' for the first few years.

**Risk of error:** There is always a risk of error, as long as the human factor is involved. In case a blockchain serves as a database, all the incoming data has to be of high quality. However, human involvement can quickly resolve the error.

**Wasteful:** Every node that runs the blockchain has to maintain consensus across the blockchain. This offers very low downtime and makes data stored on the blockchain forever unchangeable. However, all this is wasteful, because each node repeats a task to reach consensus.