**Documentation for Blockchain**

**Overview:**

A blockchain is “a distributed database that maintains a continuously growing list of ordered records, called blocks.” These blocks “are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network.”

**History:**

A blockchain was **created by a person (or group of people) using the name (or pseudonym) Satoshi Nakamoto in 2008 to serve as the public distributed ledger for bitcoin cryptocurrency transactions**, based on previous work by Stuart Haber, W. Scott Stornetta, and Dave Bayer.

**What was the first blockchain technology?**

Nakamoto uploaded blockchain source code to SourceForge in 2008 so software developers around the world could contribute to the project. The first modern blockchain was launched in **January 2009** along with the associated cryptocurrency, Bitcoin.

**Purpose of Blockchain Technology:**

1. A blockchain technology is an online ledger that user data structure, to simplify the way we transact.
2. It allows users to manipulate the ledger in a secure way without the help of a third party.
3. It allows a free cryptocurrency through a decentralized environment.
4. It provides great transparency because it is a type of distributed ledger. So our network participants share the same documentation as opposed to individual topics.
5. With blockchain, you do not need as many third parties or middleman to make guarantee and so, the cost can be reduced.
6. This technology offers new tools for authentication and authorization in the digital world that fulfill the needs of many centralized administrators. As a result, it enables the creation of new digital relationships.

**What are the benefits of a blockchain?**

Blockchain **increases trust, security, transparency, and the traceability of data shared across a business network** — and delivers cost savings with new efficiencies. Blockchain for business uses a shared and immutable ledger that can only be accessed by members with permission.

**How Does a Blockchain Work?**

The transaction process in a blockchain can be summarized as follows:

1. **Facilitating a transaction:**

A new transaction enters the blockchain network. All the information that needs to be transmitted is doubly encrypted using public and private keys.

1. **Verification of transaction:**

The transaction is then transmitted to the network of peer-to-peer computers distributed across the world. All the nodes on the network will check for the validity of the transaction like if a sufficient balance is available for carrying out the transaction.

1. **Formation of a new block:**

In a typical blockchain network there are many nodes and many transactions get verified at a time. Once the transaction is verified and declared a legitimate transaction, it will be added to the mem pool.  All the verified transactions at a particular node form a mem pool and such multiple mem pools form a block.

1. **Consensus Algorithm:**

The nodes that form a block will try to add the block to the blockchain network to make it permanent. But if every node is allowed to add blocks in this manner then it will disrupt the working of the blockchain network. To solve this problem, the nodes use a consensus mechanism to ensure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain, and only a valid block is securely attached to the blockchain. The node that is selected to add a block to the blockchain will get a reward and hence we call them “miners”. The consensus algorithm creates a hash code for that block which is required to add the block to the blockchain.

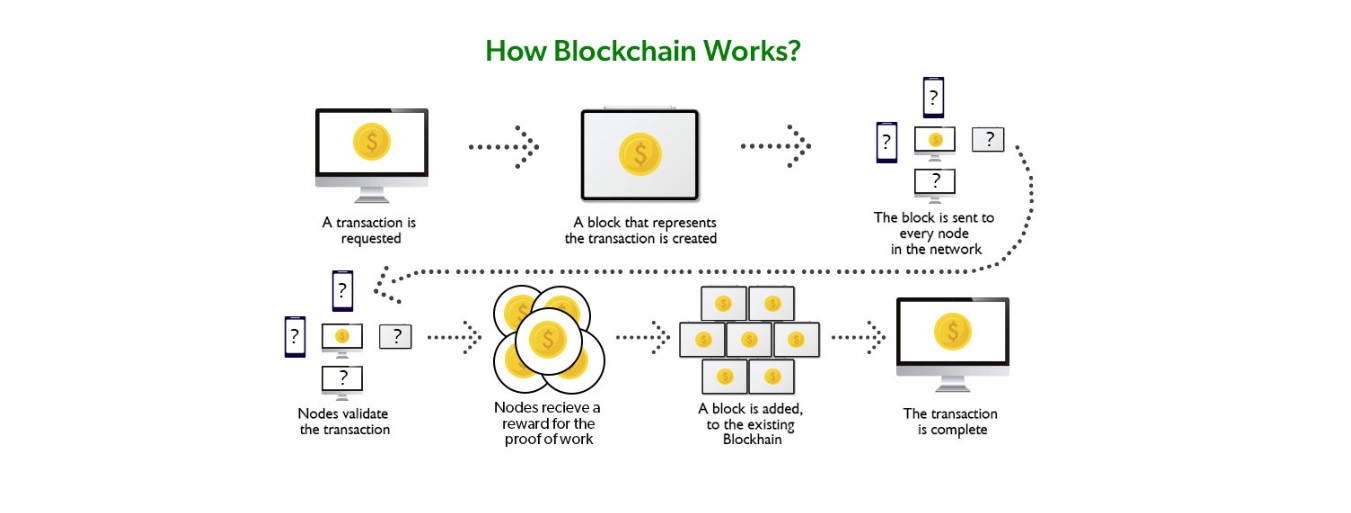
1. **Addition of the new block to the blockchain:**

After the newly created block has got its hash value and is authenticated, now it is ready to be added to the blockchain. In every block, there is a hash value of the previous block and that is how the blocks are cryptographically linked to each other to form a blockchain. A new block gets added to the open end of the blockchain.

1. **Transaction complete:**

As soon as the block is added to the blockchain, the transaction will take place and 20 BTCs will get transferred from Jack’s wallet to Phil’s wallet. The details of the transaction are permanently secured on the blockchain.

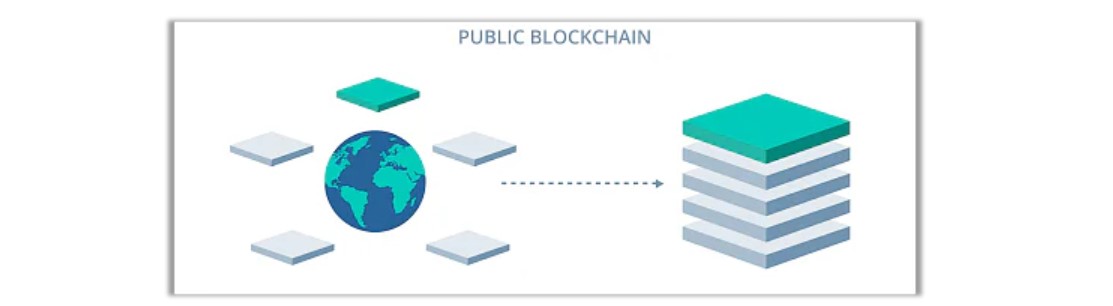
Anyone on the network can fetch the information and confirm the transaction. This will help to keep track of all the transactions and to verify whether any user is trying to double spend. For example, if Jack tries to carry out a transaction in the future, the rest of the nodes can check Jack’s past transaction records to check whether Jack has enough balance to carry out the current transaction. If there is enough balance then the transaction will be approved.



**Types of Blockchain:**

There are majorly four types of Blockchain –

1. **Public Blockchain:**

****

It is a permission less distributed ledger on which anybody can join and conduct transactions.

It is a non-restrictive form of the ledger in which each peer has a copy. This also means that anyone with an internet connection can access the public Blockchain.

This user has access to historical and contemporary records and the ability to perform mining operations.

These complex computations must be performed to verify transactions and add them to the ledger.

On the blockchain network, no valid record or transaction may be altered. Because the source code is usually open, anybody can check the transactions, uncover problems, and suggest fixes.

**Advantages of Public Blockchain -**

Trustable: Public Blockchain nodes do not need to know or trust each other because the proof-of-work procedure ensures no fraudulent transactions.

Secure: A public network can have as many participants or nodes as it wants, making it a secure network. The higher the network's size, the more records are distributed, and the more difficult it is for hackers to hack the entire network.

Open and Transparent: The data on a public blockchain is transparent to all member nodes. Every authorized node has a copy of the blockchain records or digital ledger.

**Disadvantages of Public Blockchain -**

Lower TPS: The number of transactions per second in a public blockchain is extremely low. This is because it is a large network with many nodes which take time to verify a transaction and do proof-of-work.

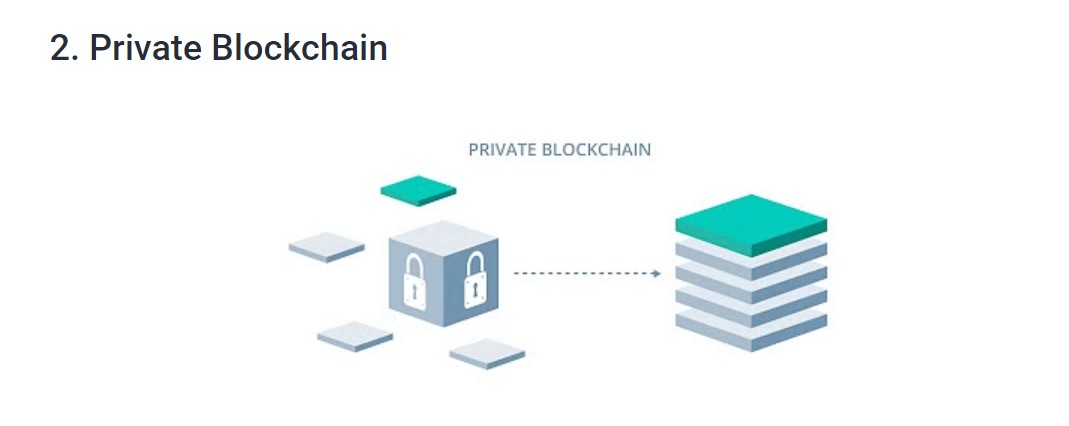
Scalability Issues: Its transactions are processed and completed slowly. This harms scalability. Because the more we try to expand the network's size, the slower it will become.

High Energy Consumption: The proof-of-work device is expensive and requires lots of energy. Technology will undoubtedly need to develop energy-efficient consensus methods.

**Uses of Public Blockchain** -

Voting: Governments can use a public blockchain to vote, ensuring openness and trust.

Fundraising: Businesses or initiatives can use the public Blockchain to improve transparency and trust.

*  A blockchain network operates in a private context, such as a restricted network, or is controlled by a single identity.
* While it has a similar peer-to-peer connection and decentralization to a public blockchain network, this Blockchain is far smaller.
* They are often run on a small network within a firm or organization rather than open to anybody who wants to contribute processing power.
* Permissioned blockchains and business blockchains are two more terms for them.

**Advantages of Private Blockchain -**

* **Speed**: Private Blockchain transactions are faster. This is because a private network has a smaller number of nodes, which shortens the time it takes to verify a transaction.
* **Scalability:** You can tailor the size of your private Blockchain to meet your specific requirements. This makes private blockchains particularly scalable since they allow companies to easily raise or decrease their network size.

**Disadvantages of Private Blockchain -**

* **Trust Building**: In a private network, there are fewer participants than in a private network.
* **Lower Security:** A private blockchain network has fewer nodes or members, so it is more vulnerable to a security compromise.
* **Centralization:** Private blockchains are limited in that they require a central Identity and Access Management (IAM) system to function. This system provides full administrative and monitoring capabilities.

### Uses of Private Blockchain -

* **Supply Chain Management:** A private blockchain can be used to manage a company's supply chain.
* **Asset Ownership:** A private blockchain can be used to track and verify assets.
* **Internal Voting:** Internal voting is also possible with a private blockchain.

### Hybrid Blockchain:

### 

* Organizations who expect the best of both worlds use a hybrid blockchain, which combines the features of both private and public blockchains.
* It enables enterprises to construct a private, permission-based system alongside a public, permission less system, allowing them to choose who has access to certain Blockchain data and what data is made public.
* In a hybrid blockchain, transactions and records are typically not made public, but they can be validated if necessary by granting access via a smart contract.

**Advantages of Hybrid Blockchain -**

* **Secure:** Hybrid Blockchain operates within a closed environment, preventing outside hackers from launching a 51 percent attack on the network.
* **Cost-Effective**: It also safeguards privacy while allowing third-party contact. Transactions are inexpensive and quick and scale better than a public blockchain network.

**Disadvantages of Hybrid Blockchain -**

* **Lack of Transparency:** Because information can be hidden, this type of blockchain isn't completely transparent.
* **Less Incentive:** Upgrading can be difficult, and users have no incentive to participate in or contribute to the network.

### Uses of Hybrid Blockchain -

* **Real Estate:** Real-estate companies can use hybrid networks to run their systems and offer information to the public.
* **Retail:** The hybrid network can also help retailers streamline their processes.
* **Highly Regulated Markets:** Hybrid blockchains are also well-suited to highly regulated areas like the banking sector.

### 4. Consortium Blockchain:

### 

* In the same way that a hybrid blockchain has both private and public blockchain features, a Consortium blockchain, also known as a federated blockchain, does.
* However, it differs because it involves various organizational members working together on a decentralized network.
* Predetermined nodes control the consensus methods in a consortium blockchain.
* It has a validator node responsible for initiating, receiving, and validating transactions. Transactions can be initiated or received by member nodes.

**Advantages of Consortium Blockchain -**

* **Secure:** A consortium blockchain is more secure, scalable, and efficient than a public blockchain network. It, like private and mixed blockchains, has access controls.

**Disadvantages of Consortium Blockchain -**

* **Lack of Transparency:** The consortium blockchain has a lower degree of transparency. If a member node is infiltrated, it can still be hacked, and the Blockchain's rules can render the network inoperable.

**Uses of Consortium Blockchain -**

* **Banking and Payments**: A consortium can be formed by a group of banks working together. They have control over which nodes will validate transactions.
* **Research:** A consortium blockchain can be employed to share research data and outcomes.
* **Food Tracking:** It is also apt for food tracking.

### ****Is Blockchain Secure?****

In the most basic way, one can think of a blockchain as a linked list. Each of the next items in the list is dependent on the previous item, except for the first block, also known as the genesis block, which is hardcoded into the blockchain. In the blockchain, each block contains the hash of the previous block’s header and a hash of the transactions in the Merkle tree of the current block. In this way, each block is cryptographically chained to the previous block. Let’s understand with an example what happens when someone attempts to change a transaction or block data in a blockchain network.

* Suppose, there is a chain of 10 blocks, where the 10th block depends on the 9th block, the 9th block depends on the 8th block, and so on.
* In this way, the 10th block depends on all the previous blocks and the genesis block as well.
* If someone tries to change data on the 2nd block, then the attacker will have to change data on all the later blocks as well, otherwise, the blockchain will become invalid since the later blocks depend on the hash value present in the 2ndblock and the 2nd block has changed, but not the later blocks.
* Thus, as the blocks are added, immutability increases as changing the block is an expensive operation.
* Also, to add/change a block in a blockchain, a consensus algorithm is used by nodes in the blockchain network. In order to compensate for the change in one block, one must have to recalculate the hash of every block to update the hash value of the block header in the next block. This will involve a lot of time and computational resources.
* In order to succeed with such kind of attack, the hacker has to simultaneously control and change 51% or more copies of the blockchain so that their new copy becomes the majority copy and thus the agreed-upon chain.
* Thus, requiring an immense amount of time, money, and computational resources.

### What are 5 key components of a blockchain system?

* Distributed Ledger.
* Peer-to-peer network – P2P.
* Consensus Mechanism.
* Cryptography.
* Virtual Machine.

**What the Future Looks Like:**

If the past tells us anything, it is that once blockchains become a necessary part of everyday life, we will stop talking about them. That’s what happens to the essential technical underpinnings of killer apps.

When Microsoft Office was introduced, everyone talked about Windows for a while. Your PC had to be Windows-compatible. You had to buy a copy of Windows. You had to make sure that your version of Windows was updated to run the latest version of Office.

And then, once Windows reached critical mass, people didn’t need to talk about it so much. Office users could take Windows for granted. Windows continued to be essential, but user focus shifted to the apps that ran on Windows, not on the technical foundation.

That’s what blockchain’s future looks like. For a while, blockchain will be at the forefront. We look for developers who can create blockchain apps. We look for services that can integrate blockchain apps with non-blockchain data or services that run on incompatible blockchains. We focus on scalability and security.

When the revolution comes, it will be because blockchain technology is a mature, stable foundation for the apps and services we want. We’ll focus on those, and we’ll stop talking so much about blockchain.

We will know that blockchain technology has achieved its success when we stop talking about it.

**Pros and Cons of Blockchain Technology:**

**Major Pros of Blockchain Technology:**

### 1. Decentralized Trust:

### 

### One of its biggest strengths is that you no longer need to trust a third party to make any transaction. People using blockchain worldwide are confident sthat no single party is manipulating transactions, viewing personal information or performing any other activity breaching their privacy and security.

That doesn’t mean blockchain-based applications are always secure—that depends on how good developers are at creating secure code—but it does mean there are opportunities for better security than conventional applications. With blockchain, you can feel more confident about your data and identity.

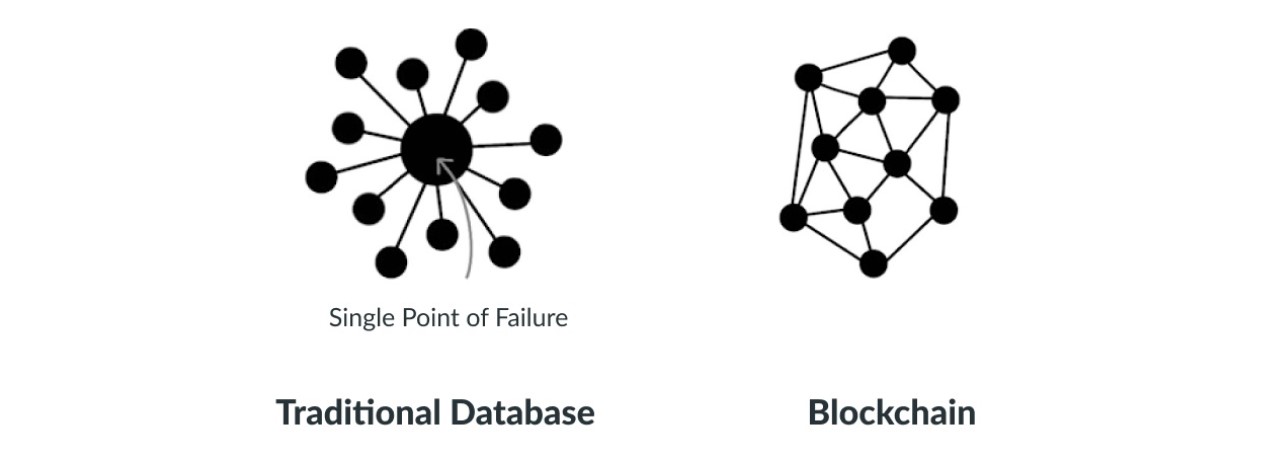
You only share what you want; companies cannot see your data without your permission. You can also feel more confident about getting paid for providing services. With blockchain, payment is instant; there’s no need to wait days for money orders or checks to clear.

1. **Low Operational Cost:**

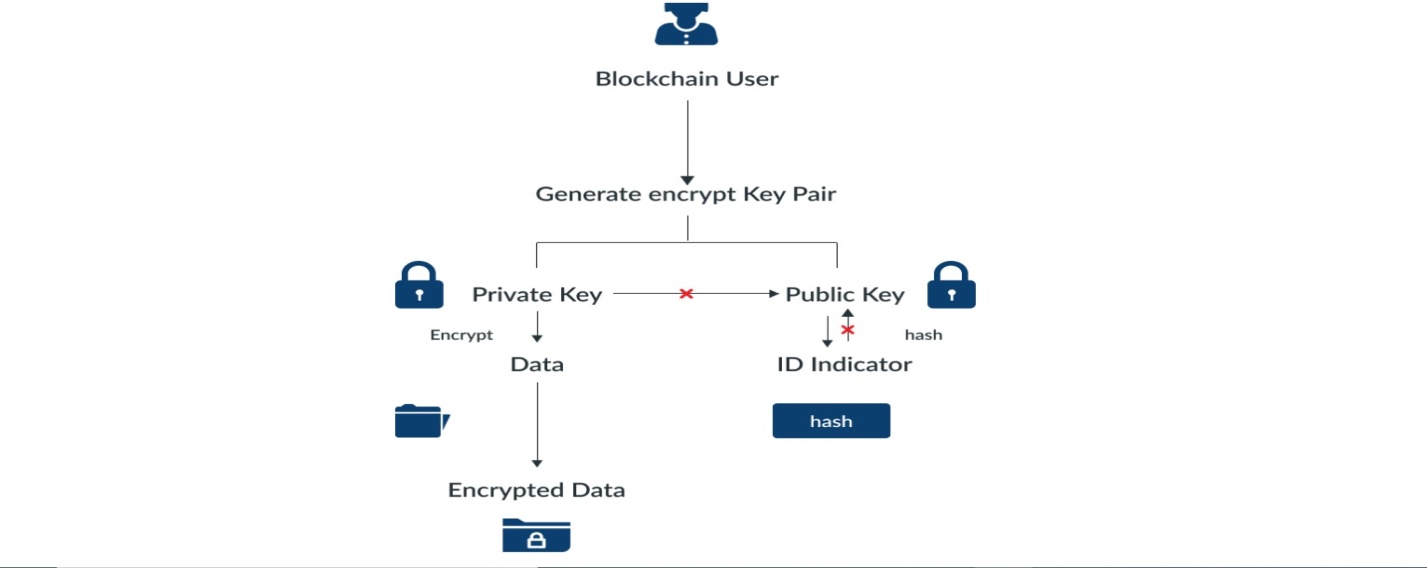
Blockchain reduces overhead costs as it has no centralized authority or servers to maintain operations. There is no payment processing or banking fees as it opts for peer-to-peer transactions without third-party approval. It embeds documents, agreements, or transactions within the system.

Blockchain encryptions are more secure against identity theft than conventional payment systems.

1. **No Single Point of Failure:**

****

1. **Enhanced Security And Confidentiality:**

****

Being distributed across a global network of computers and protected by cryptography, blockchain technology is inherently more secure than centralized systems.

As the Economist reports, it is tough to tamper with records once they are in there. Any attempt to alter one’s record will reflect immediately because copies and digital signatures are checked against each other automatically**.**

It has an added layer of confidentiality that secures your data from hackers. Transactions are impossible to trace or link back to an individual user. The user can select their names and e-mail addresses during transactions. You get the option to complete your transactions while remaining anonymous.

So, you can use blockchain-based services without worrying about advertisers tracking your activity or identity thieves accessing sensitive information such as credit card numbers.

### Quick Transactions:

Blockchain is capable of processing much faster transactions than any traditional bank. As a result, businesses that use blockchain instead of banks can save a considerable amount on fees.

[**Deloitte**](https://www2.deloitte.com/us/en.html) has predicted that blockchain technology could save companies up to billions in the form of banking fees. Blockchain’s decentralized structure doesn’t require massive data centers and expensive third-party verification. It also limits the number of people involved in monitoring the transactions.

### Reduces Fraud:

### 

Blockchain technology has some fantastic attributes that make it ideal for financial institutions to reduce forgery. It records every activity, making it impossible for anyone to make duplicate transactions.

Each block stores the financial information, and if any modification is made to a previous block, other nodes on the network rejected it.

Once your bank confirms your transaction, they can’t deny receiving the funds. On top of that, you could see that fraudulent activity happened when another node changed transactions.

Before going to my next point, I want to give crucial advice to companies who wish to deploy Blockchain within their organization. What is that? Since the technology is not so old and needs expertise, always hire a trusted [**Blockchain development company in India**](https://www.pixelcrayons.com/blockchain-development?utm_source=PCBlog-pros-cons-blockchain&utm_medium=blockchain-development&utm_campaign=DC).

### Transparent & Universal Recording System:

The transactions in the blockchain are recorded in a public ledger that anyone can view. All can see the amount stored in the wallet but cannot identify its owner.

A wallet could be tied to an individual or group. Still, if users want to remain anonymous, they must transfer their Bitcoins to another address (**e.g., a different Bitcoin wallet**) that isn’t linked with their real identity.

But even without anonymity features enabled, blockchain tech provides more transparency than traditional payment methods like credit cards and checks; you don’t need a bank intermediary (**or permission from one**) to see what or whom you paid or received money from.

### Better Accessibility:

A blockchain allows anyone with a computer and an internet connection to be part of its network. It is decentralized, meaning any single entity can’t control it—and everyone has equal access to it.

Anyone can make changes (**add information**) or add new blocks (**to store data**) to a blockchain, provided they know how to do so. Even non-tech individuals have the same access to blockchains! This openness makes blockchains much more accessible than traditional institutions like banks and financial services.

That doesn’t mean you shouldn’t be wary when dealing with blockchain providers: you should always research your choices before making any significant financial decisions.

### Prevents Double Spending:

Bitcoin transactions are verified by network nodes through cryptography and recorded in a publicly distributed ledger called a blockchain. This ensures safety by eliminating direct access to your money.

That’s why some say bitcoin is fungible—its value is equal even if its physical form changes. In other words, bitcoins derive their worth from mathematics alone, unlike fiat currencies like U.S. dollars or euros, which get their value from an organization’s financial standing.

It may sound silly to think that an individual bitcoin is identical to any other bitcoin, but it’s true; every single bitcoin carries all its transactional histories within that particular blockchain framework.

Once you own a bitcoin, it’s yours forever; there’s no threat of anyone ever taking that away from you. And once again: since there’s so much debate surrounding how many bitcoins will be released over time, there is only one way to find out by buying them!

1. **Seamless Integration Into Existing Systems:**

Blockchain offers seamless integration of their current financial systems into the outside networks.  It can be done in two ways: Blockchain as a Service (BaaS) and blockchain application platforms.

BaaS offers organizations a secure connection to blockchain networks using cloud services, while blockchain application platforms allow anyone – even those without cloud services – to use blockchain technology. The integration process is much more seamless than other means of blockchain access.

Blockchain as a Service allows businesses to connect directly with blockchain networks, giving them immediate access to these decentralized ledgers. It doesn’t force you to use one blockchain or another and gives you a higher level of control than some other methods.

Additionally, BaaS is typically quicker and easier to set up than other services, making it ideal for organizations that may need blockchains immediately, such as supply chain management applications.

## Major Cons of Blockchain Technology:

### Scalability:

### Blockchain is capable of handling fewer transactions per second. It causes delays in finalizing the massive volume of transactions resulting in poor scalability. However, several methods have been proposed to overcome this shortcoming, but none has been implemented till now.

### Security:

Blockchain is publicly accessible as a distributed ledger. It may attract any unknown visitor monitoring your wallet. Though there are several provisions to add privacy and encryption layers to enable your preferred privacy, all are not commonplace yet.

Moreover, much of your data is linked directly to your digital identity, so it could potentially expose parts of your private life that you wouldn’t necessarily want online. Security concerns often lead people to trust third-party solutions (**like exchanges**) over direct blockchain transactions, relinquishing control over personal assets.

* 1. **Cost:**

One of the biggest problems with blockchain technology is that it requires enormous energy. Because miners have to solve complicated math problems to get a payout, they need powerful rigs that consume tons of electricity.

As a result, sme blockchains are incredibly costly to run, especially for smaller businesses or individuals. You cannot make changes later; if you want your blockchain online, you must pay for it up front!

### Competitiveness:

### There is a lot of hype surrounding these industries trying to use blockchain. It leads to unnecessary competition between businesses as they opt for this technology and waste their time, money, and efforts even when it is useless for their business. Companies will have no alternative but to invest heavily to keep up with their competitors.

### Speed:

The other significant con to blockchain technology is its speed. Unlike a centralized database, blockchains require miners—or people with high-end computers and dedicated software that solve computational puzzles in exchange for new crypto tokens.

In simple terms, blockchain transactions take longer than traditional payment methods like cash or credit cards. This can be discouraging if you’re interested in using blockchain technology as a daily payment method.

## ****Conclusion:****

## Without a doubt, Blockchain technology’s benefits will soon attract businesses and organizations around the world to invest more in it. It is still in its starting phase but this, one of the newest technologies will take a little more time to gain traction and will require patience. However, the pros of Blockchain are hard to ignore, but the technology will indeed help various industries as the verification for every piece of data that goes in and through these Blockchain systems will be a preventer of many adversities.

