

ZETECH UNIVERSITY

UNIT NAME: BLOCK CHAIN TECHNOLOGY

UNIT CODE: BCE 413

LESSON 1

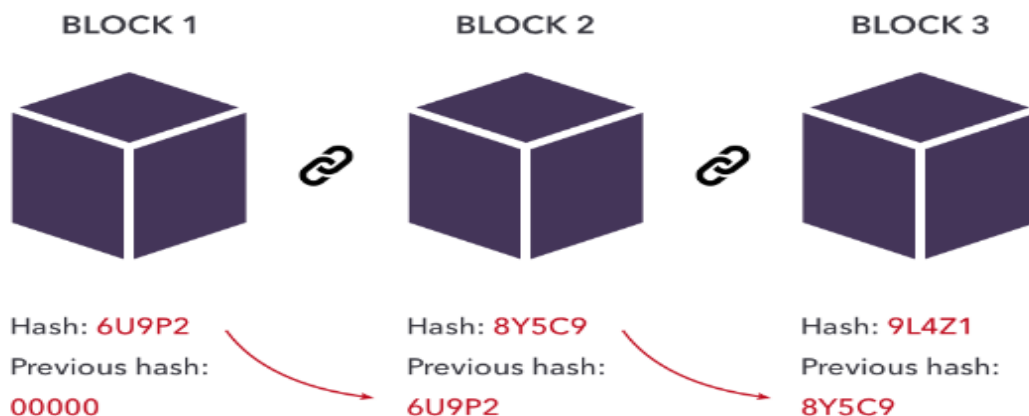
- Definition of Block Chain
- Major features of Block chain
- Benefits of Block Chain Technology
- Four types of Block chain

What Is Block Chain Technology?

Block Chain is a method/list of recording information that makes it impossible or difficult for the system to be changed, hacked, or manipulated.

Block - A block is a set of transactions that happen over the network.

Chain - chain is where blocks are linked to each other in a way that the next block contains hash of the previous one.



Characteristics of Block chain.

- (a) **secured using cryptography** -it ensures that the privacy of the user is maintained and data cannot be altered.
- (b) **Not controlled by a central authority**- unlike modern financial institutions, no body controls the data within a Block chain.
- (c) **Access to anyone on the network**-same of data to everyone

Block chain also known as a "distributed ledger". That powers Bitcoin.

Distributed ledgers are the databases shared across a network and spread over various geographical locations.

A ledger is a collection of financial accounts and, in such a case, distributed means spread out and controlled globally.

Thus, distributed ledgers are held and reorganized by multiple parties in different locations and institutions.

In simpler words, the digital ledger Google Sheets is a web-based application that enables users to create, update and modify spreadsheets and share the data online in real time.

What Are the Benefits of Block Chain Technology?

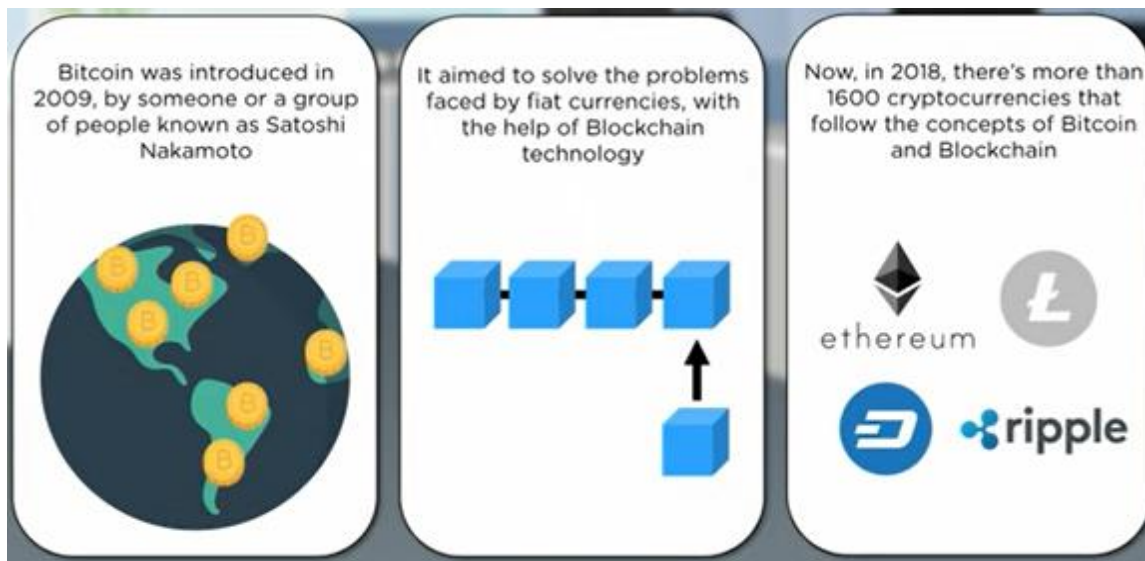
1. It is an **immutable public digital ledger**, which means when a transaction is recorded, it cannot be modified
2. **Due to the encryption feature**, Block chain is always secure
3. **The transactions are done instantly and transparently**, as the ledger is updated automatically
4. **As it is a decentralized system**, no intermediary fee is required
5. **The authenticity** of a transaction is verified and confirmed by participants

What Block chain is NOT!

-Block chain is not Bitcoin, but it is the technology behind Bitcoin

-Bitcoin is the digital token, and the block chain is the ledger to keep track of who owns the digital tokens

-You can't have Bitcoin without block chain, but you can have a block chain without Bitcoin.



Bitcoin mining refers - to ensuring that transactions are valid and added to the Bitcoin block chain correctly using a global network of computers running the Bitcoin code.

Blockchain has 4 major features

1. Public distributed ledger
2. Hash encryption
3. Proof of work
4. Mining

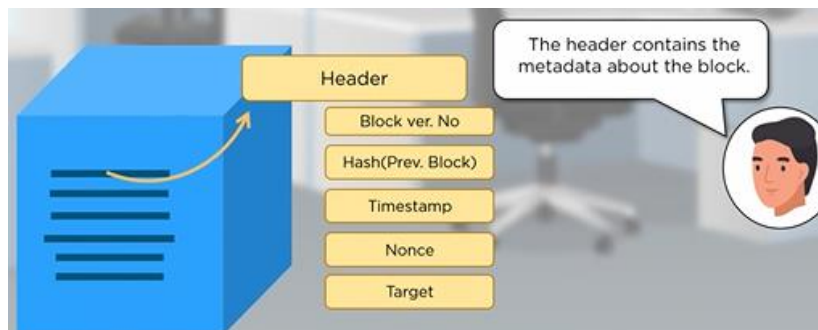
1. Public distributed ledger –

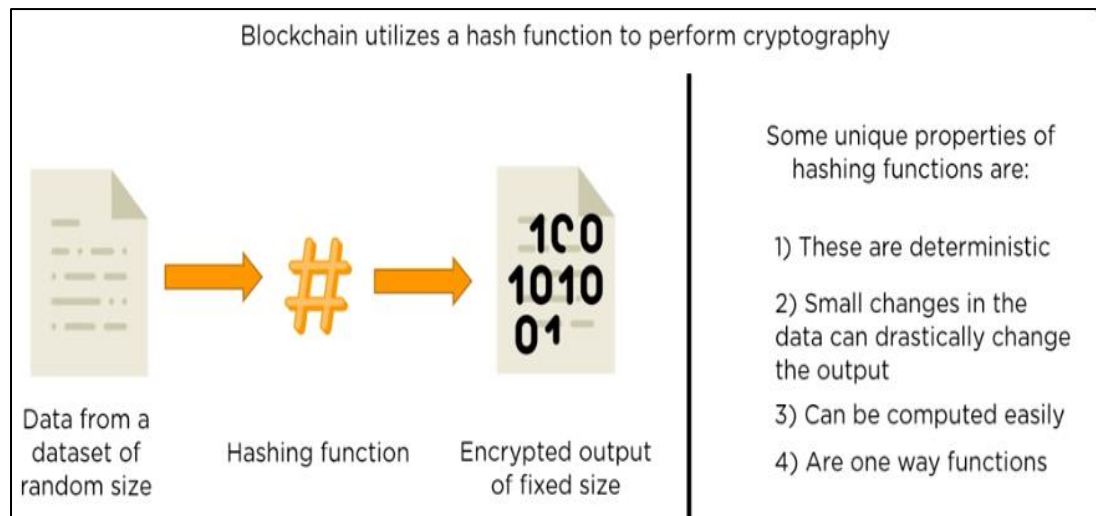
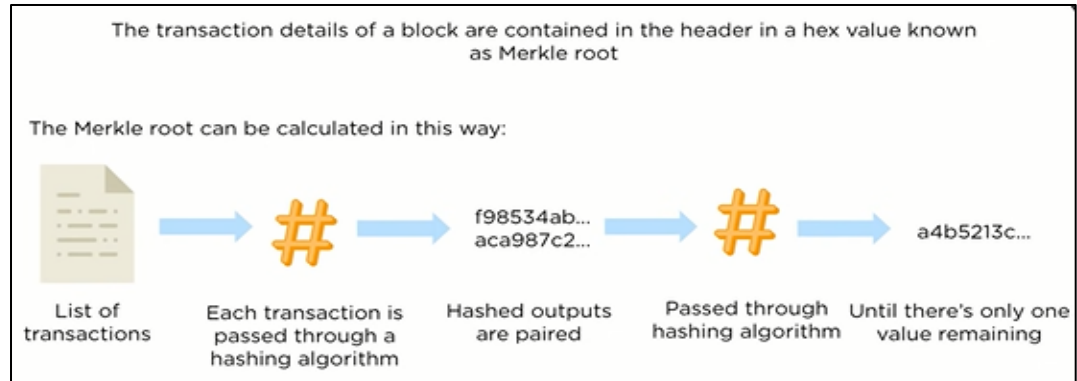
- A block chain is a decentralized public distributed ledger that is used to record transactions across many computers
- A distributed ledger is a database that is shared among the users of the block chain network
- The transactions are accessed and verified by users associated with the bitcoin network, thereby making it less prone to cyberattack

2. Hash encryption – a hash algorithm is a mathematical function that transforms any input into a fixed size output.

- ✓ usable in block chain technology – the hash function needs to be collision resistant, which means that it is difficult to find two inputs that produce the same output.
- ✓ A hash algorithm is considered secure until it is possible to find a collision for it. Once this has occurred, it is officially deprecated, like MD5 and SHA-1.
- ✓ The current used secure hash method is SHA-256 where SHA stands for Secure Hash Algorithm. Published in 2001. SHA-256 is a patented cryptographic hash function that outputs a value that is 256 bits long.
 - a. one must know the content of a block.
 - b. A block is a container that holds transaction details

A block has two parts:





- 1) Same input will produce same output.
- 2) Any change to the input produces an output that's drastically different from previously obtained outputs.
- 3) The output values can be obtained without a whole lot of calculation.
- 4) **One-way** method. You can't determine input from reverse engineering.i.e Chronological order.

To ensure security, Blockchains also include digital signatures

Users are provided their own private and public keys



Private key

Used by user to control his/her account. This is kept as a secret by the user



Public key

Used to identify the user in the network. This is shared by the user

3. Proof of Work

Proof of work (PoW) is a method to validate transactions in a block chain network by solving a complex mathematical puzzle called mining.

Note: Users trying to solve the puzzle are called miners.

Proof of work involves people around the world (called miners) competing to be the first one to add a block to the Blockchain



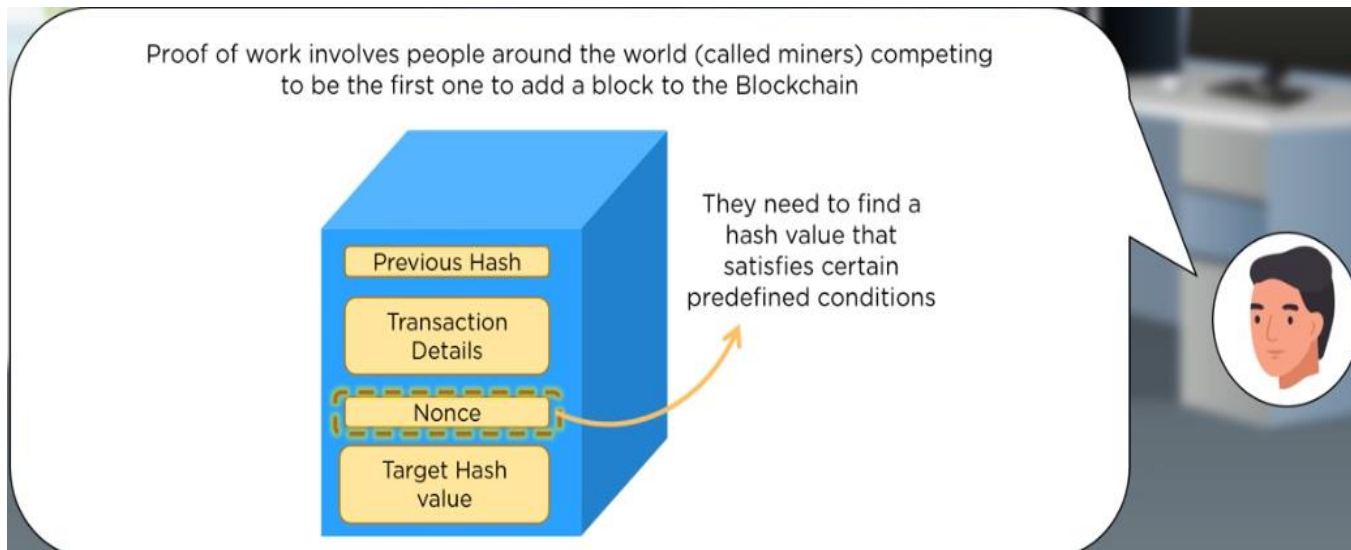
Competing miners around the world



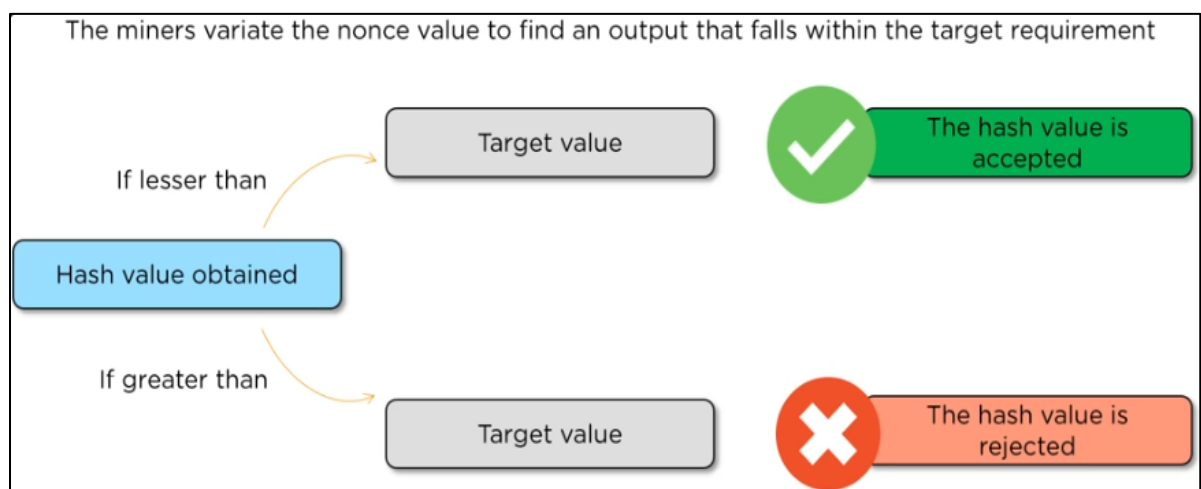
Try to solve a mathematical puzzle



To be the first one to be rewarded and to add a block to the Blockchain



this target hash value is decided months in advance

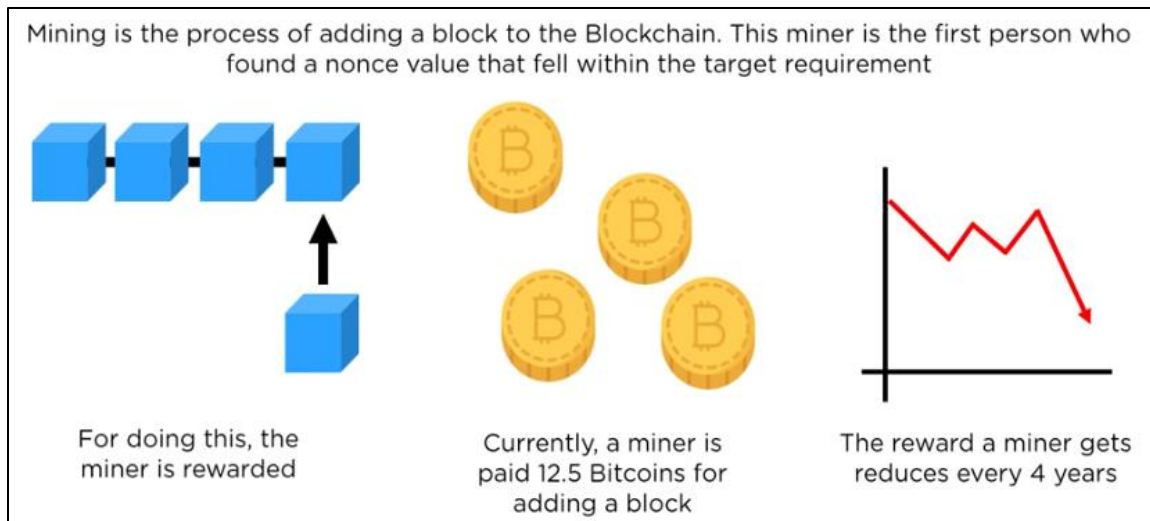


- ✓ And thanks to the hashing algorithms used, this claim can be easily verified by others
- ✓ that's a whole lot of work! what's a miner's payoff here?
- ✓ for all his/her hard work, they get paid in Bitcoins! sometimes they get other forms of remuneration as well!

4. Mining

In Block chain, when miners use their resources (time, money, electricity, etc.) to validate a new transaction and record them on the public ledger, they are given a reward.

Note: As a reward, the miner gets 12.5 BTC (bitcoins)



- ✓ the 12.5 Bitcoin reward is justified, as mining is a very expensive process. it has a heavy toll on electricity, computing power and other resources

Why is Block Chain Popular?

The block chain is used for the secure transfer of items like money, property, contracts, etc, without requiring a third-party intermediary like a bank or government.

Once data is recorded inside a block chain, it is very difficult to change it.

By using blockchain we can track orders and payments from end to end.

Advantage using block chain:

- It provides greater trust among users.
- It provides greater security among data.
- Reduce the cost of production.
- Improve Speed.
- Invocation and tokenization.
- It provides immutable records.
- Smart contracts

Disadvantages using block chain:

- Data modification is not possible.
- It requires large storage for a large database.
- The owner cannot access the private key again if they forget or lose it.

Real life application of block chain:

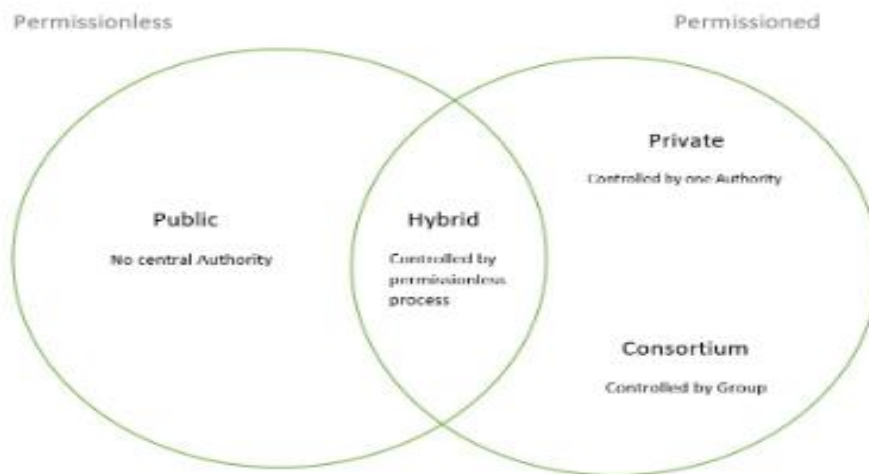
Here is a list of real world problem where we can use block chain:

- In a secure and full-proof voting management system.
- To supply chain management.

- In healthcare management.
- Real estate project.
- NFT marketplace.
- Avoid copyright and original content creation.
- In the personal identity system
- To make an immutable data backup.
- Internet of Things

There are 4 types of block chain:

1. Public Block chain.
2. Private Block chain.
3. Hybrid Block chain.
4. Consortium Block chain.



1. Public Block chain

These block chains are completely open to following the idea of decentralization. They don't have any restrictions, anyone having a computer and internet can participate in the network.

- As the name is public this block chain is open to the public, which means it is not owned by anyone.
- Anyone having internet and a computer with good hardware can participate in this public block chain.
- All the computer in the network hold the copy of other nodes or block present in the network
- In this public block chain, we can also perform verification of transactions or records

Advantages

- **Trustable** - There are algorithms to detect no fraud. Participants need not worry about the other nodes in the network
- **Secure** - This block chain is large in size as it is open to the public. In a large size, there is greater distribution of records
- **Anonymous Nature** - It is a secure platform to make your transaction properly at the same time, you are not required to reveal your name and identity in order to participate.
- **Decentralized** - There is no single platform that maintains the network, instead every user has a copy of the ledger.

Disadvantages

- **Processing** - The rate of the transaction process is very slow, due to its large size. Verification of each node is a very time-consuming process.
- **Energy Consumption** - Proof of work is high energy-consuming. It requires good computer hardware to participate in the network
- **Acceptance** - No central authority is there so governments are facing the issue to implement the technology faster.

Use Cases: Public Block chain is secured with proof of work or proof of stake they can be used to displace traditional financial systems. The more advanced side of this block chain is the smart contract that enabled this block chain to support decentralization. Examples of public block chain are Bitcoin, Ethereum.

2. Private Block chain

These block chains are not as decentralized as the public block chain only selected nodes can participate in the process, making it more secure than the others.

- These are not as open as a public block chain.
- They are open to some authorized users only.
- These block chains are operated in a closed network.
- In this few people are allowed to participate in a network within a company/organization.

Advantages

- **Speed** - The rate of the transaction is high, due to its small size. Verification of each node is less time-consuming.
- **Scalability** - We can modify the scalability. The size of the network can be decided manually.
- **Privacy** - It has increased the level of privacy for confidentiality reasons as the businesses required.
- **Balanced** - It is more balanced as only some user has the access to the transaction which improves the performance of the network.

Disadvantages

- **Security** - *The number of nodes in this type is limited so chances of manipulation are there. These block chains are more vulnerable.*
- **Centralized** - *Trust building is one of the main disadvantages due to its central nature. Organizations can use this for malpractices.*
- **Count** - *Since there are few nodes if nodes go offline the entire system of block chain can be endangered.*

Use Cases: With proper security and maintenance, this block chain is a great asset to secure information without exposing it to the public eye. Therefore, companies use them for internal auditing, voting, and asset management. *An example of private block chains is Hyper ledger, Corda.*

3. Hybrid Block chain

It is the mixed content of the private and public block chain, where some part is controlled by some organization and other makes are made visible as a public block chain.

- It is a combination of both public and private block chain.
- Permission-based and permission less systems are used.
- User access information via smart contracts
- Even a primary entity owns a hybrid block chain it cannot alter the transaction

Advantages

- **Ecosystem** - *Most advantageous thing about this block chain is its hybrid nature. It cannot be hacked as 51% of users don't have access to the network*
- **Cost** - *Transactions are cheap as only a few nodes verify the transaction. All the nodes don't carry the verification hence less computational cost.*
- **Architecture** - *It is highly customizable and still maintains integrity, security, and transparency.*
- **Operations** - *It can choose the participants in the block chain and decide which transaction can be made public.*

Disadvantages

- **Efficiency** - *Not everyone is in the position to implement a hybrid Block chain. The organization also faces some difficulty in terms of efficiency in maintenance.*
- **Transparency** - *There is a possibility that someone can hide information from the user. If someone wants to get access through a hybrid block chain it depends on the organization whether they will give or not.*

- **Ecosystem** - Due to its closed ecosystem this block chain lacks the incentives for network participation.

***Use Case:** It provides a greater solution to the health care industry, government, real estate, and financial companies. It provides a remedy where data is to be accessed publicly but needs to be shielded privately. Examples of Hybrid Block chain are Ripple network and XRP token.*

4. Consortium Block chain

It is a creative approach that solves the needs of the organization. This block chain validates the transaction and also initiates or receives transactions.

- Also known as Federated Block chain.
- This is an innovative method to solve the organization's needs.
- Some part is public and some part is private.
- In this type, more than one organization manages the block chain.

Advantages:

- **Speed** - A limited number of users make verification fast. The high speed makes this more usable for organizations.
- **Authority** - Multiple organizations can take part and make it decentralized at every level. Decentralized authority, makes it more secure.
- **Privacy** - The information of the checked blocks is unknown to the public view. but any member belonging to the block chain can access it.
- **Flexible** - There is much divergence in the flexibility of the block chain. Since it is not a very large decision can be taken faster.

Disadvantages:

- **Approval** - All the members approve the protocol making it less flexible. Since one or more organizations are involved there can be differences in the vision of interest.
- **Transparency** - It can be hacked if the organization becomes corrupt. Organizations may hide information from the users.
- **Vulnerability** - If few nodes are getting compromised there is a greater chance of vulnerability in this block chain.

***Use Cases:** It has high potential in businesses, banks, and other payment processors. Food tracking of the organizations frequently collaborates with their sectors making it a federated solution ideal for their use. Examples of consortium Block chain are Tender mint and Multichain.*

