UNIT- I

Blockchain Technology: Introduction, Scenarios, Challenges Articulated, Blockchain, Blockchain Characteristics, Opportunities Using Block chain, History of Block chain.
Evolution of Block chain: Evolution of Computer Applications, Centralized Applications, Decentralized Applications, Stages in Blockchain Evolution, Consortia, Forks, Public Block chain Environments, Type of Players in Blockchain Ecosystem, Players in Market.

Blockchain Technology -Introduction

1)Introduction: -

- "Blockchain" or "chain of blocks" is a term that has received a lot of attention in recent times due to raise in the value of **Cryptocurrencies** as well as the benefits of the technology.
- Harvard Business Review states that **blockchain is a foundational technology**, which has the potential to create new economies, social systems, and technical platforms.
- Blockchain also introduces concepts such as **democratization of trust, immutability of data or tamperproof data, consensus, and asynchronously replicated shared ledgers**. These create new possibilities and opportunities to perform business.
- **Blockchain has been getting more and more attention,** and this attention has created significant number of competing platforms at various levels of maturity.

2) Scenarios: -

Let Us consider few Business Scenarios to understand the problems that the world is facing:
a) Counterfeit detection
b) Ethical sourcing
c) Quality management
d) Needing to reveal more
e) Reducing faith in central banks

a) Counterfeit detection:

A pharmaceutical company has just moved into the emerging market with an invention.
The company has not been able to take any measures to control unauthorized players from moving counterfeit in market.
The company wants to have a way to trace how the product is moving from manufacturing facilities to distributors to retailers before ending up with customers.

b) Ethical sourcing:

A high-end restaurant chain boasts itself as an ethical organization committed to sustainability and social responsibility.
The chain works with multiple suppliers and farmers across the world to prepare best-in-class ingredients.
Recently, one of the outlets received negative publicity due to one of their suppliers sourcing vegetables from farms employing child labor and using inorganic fertilizers.
There needs to be efforts to gain back the trust of customers, proving to them that the food in their plates has come from a genuine source.

c) Quality management:

An automaker has outsourced quality check for smaller components from numerous suppliers.

Yearly audit by the manufacturer has revealed that interim reports at supplier sites get modified suspiciously.

The automaker cannot expose their systems to suppliers but still wants visibility about interim audit at sites.

d) Needing to reveal more:

A data analysis organization cares a lot about customer as well as employee privacy.

As a differentiator, the company wants to enroll the system where prospective employees would need to reveal minimum information while applying for jobs.

The company is also worried about misuse of the system and selects only qualified individuals.

They are looking for a system that can give control to prospective employees on what information is shared about them.

e) Reducing faith in central banks

Central banks are using monetary policies in a protectionist and short-sighted manner.

Some of the central banks run on IT systems that run on risk-prone centralized IT infrastructure, and there have been numerous cases of data theft.

A group of global citizens are searching for an alternative currency that is not politically influenced, and rewards all entities that show commitment to the cause of equitable terms.

3) Challenges Articulated: -

There are many common Challenges that are faced in Business Scenarios as listed below:

Disproportionate control and capability:

Protectionist approach makes organizations create their silo views of data and tactically share minimal requirements on case-to-case basis.

Organizations might not really have skills, capabilities, or technology to collaborate efficiently or in a way where not every participant has a level playing field.

Security: There are other cases where organizations are worried about security in interactions with other organizations.

Opaque systems

Stakeholders have a lot to gain through collaboration, but they might not be able to fully trust each other.

This trust deficit comes because while organizations do have common interests, there are some aspects where organizations prefer to be protectionists and do not want to be transparent.

Burden of intermediaries

Issues related to trust deficit, skill gap, technical knowhow, security, or operational efficiency used to be circumvented by intermediaries that used to fill the void.

The challenge really is to have intermediaries that can deliver value at the least cost that is possible.

4) What is Block Chain: -

Blockchain is literally **a chain of blocks, with each block containing certain data. The blocks are chained in such a way that it is not easy to break the chain**.

Blockchain was first introduced through a white paper authored by Satoshi Nakamoto.

Harvard Business Review defines blockchain as "**An open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way**."

Merriam Webster Dictionary defines blockchain as "A digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network or the technology used to create such a database."

Blockchain can also be defined as "**A system in which participants of a peer-to-peer network maintain distributed ledger that is secure, practically immutable and auditable**."

Let us understand few terms relevant to this Technology:

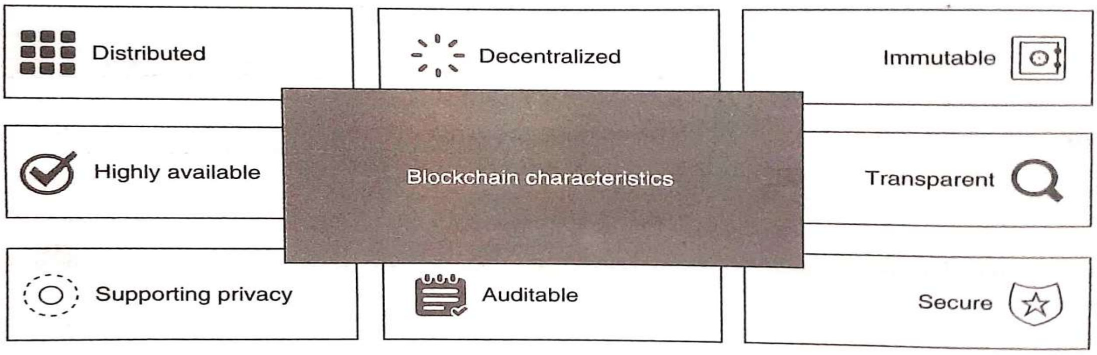
- **Parties/Participants:** Organizations or systems that participate in the network for reading or updating the data.
- **Open:** Protocols and details of working are not closed or proprietary. Blockchain protocols are published and documented for everyone's consumption.
- **Distributed ledger:** A log of transactions that is same from all the nodes connected and synced with the network. In simple terms, every participant has the same copy of the log they all are maintaining together.
- **Peer-to-peer network:** A network in which participants are connected to each other than a central server of a hub.
- **Permanent:** The ledger that is probabilistically impossible to change once it is agreed by the participants.

Blockchain Characteristics

Blockchain is literally **a chain of blocks, with each block containing certain data. The blocks are chained in such a way that it is not easy to break the chain**.

Harvard Business Review defines blockchain as "**An open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way**."

Let us try to understand the Characteristics of Blockchain Technology, as listed below:



Blockchain characteristics.

1)Distributed: Blockchain processes and stores data at multiple participants and so, by nature, blockchain is a distributed system.

2)Decentralized: The lack of central control is what makes blockchain a decentralized network. Decentralization helps blockchain maintain high availability.

3)Highly available: Distributed and decentralized nature of blockchain network helps ensure consumers that the network always has a node available to serve the requests; this is what makes blockchain highly available.

4)Immutable: If the chain is designed in such a way that it cannot be broken, the data inside the blocks of chains cannot be modified. This non-modifiability is what makes transactions permanent on blockchain ledger and makes it immutable.

5)Transparent: Entries to the ledger are created by preset rules that are defined at network configuration. This sharing of data and logic encourages transparency in blockchain.

6)Auditable: Blockchain does not only share current state, but the entire journey or journal or log of how the state has been arrived. The log is available for each node to inquire. This makes activities happening on blockchain auditable.

7)Secure: Blockchain extensively utilizes encoding and encryption mechanisms for transaction creation, broadcast, and storage. More the participants, more secure and resilient the network becomes as even if one of the nodes is brought down by hackers, the rest of the participants continue working within the network.

8)Supporting privacy: Blockchain does not identify individuals with identifiers that store personal information. For example, a Transaction can be initiated by party A with out knowing any private information about party B.

9)Democratization of trust: Blockchain takes a radically different approach to build credibility by allowing participants to decide and execute rules or choose a decision-maker transparently for each transaction. This makes "trust" more democratic in the sense that a trustworthy peer is chosen each time from peers; the chosen node is not "appointed".

Blockchain Technology is evolving very fast and some of the implementations might not have one or more features of above list.

Opportunities using Blockchain

Introduction: -

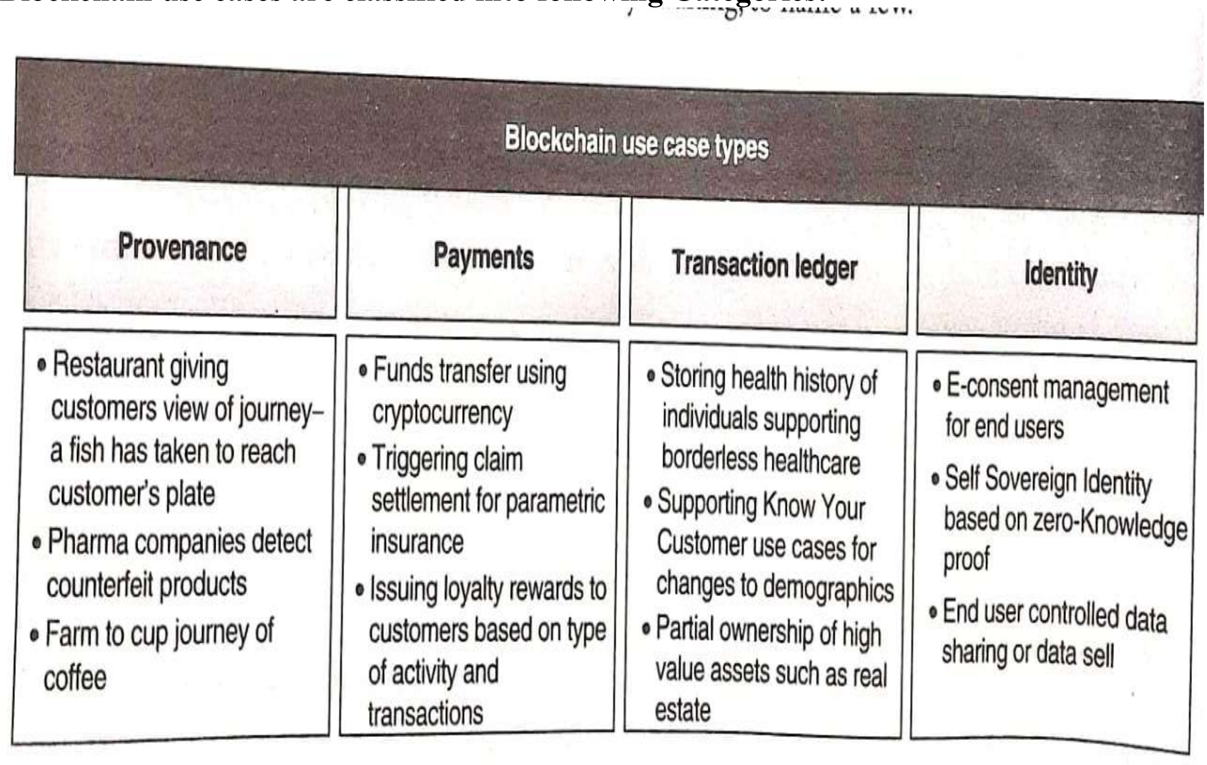
Blockchain is literally **a chain of blocks, with each block containing certain data. The blocks are chained in such a way that it is not easy to break the chain**.

Harvard Business Review defines blockchain as "**An open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way**."

Over the years Blockchain has grown beyond cryptocurrency. Traditionally, money has been used for transactions. With blockchain, money or cryptocurrency is being seen as Programmable money.

Moreover, shared ledger and other characteristics of blockchain are opening avenues for numerous other use cases. Participants who have a copy of the transaction can provide a view as to where exactly the material under observation has moved.

Blockchain use cases are classified into following Categories:



Blockchain use case types

Provenance	Payments	Transaction ledger	Identity
• Restaurant giving customers view of journey– a fish has taken to reach customer's plate • Pharma companies detect counterfeit products • Farm to cup journey of coffee	• Funds transfer using cryptocurrency • Triggering claim settlement for parametric insurance • Issuing loyalty rewards to customers based on type of activity and transactions	• Storing health history of individuals supporting borderless healthcare • Supporting Know Your Customer use cases for changes to demographics • Partial ownership of high value assets such as real estate	• E-consent management for end users • Self Sovereign Identity based on zero-Knowledge proof • End user controlled data sharing or data sell

Blockchain use cases.

Provenance:

Provenance use cases are also called as **track and trace** in cases where the aim is not essentially to know the origin but to know the touchpoints the product has with various participants.

There are other possible use cases belongs to same category like Counterfeit, detection, ethical sourcing, drug recall and Inventory Auditing etc.

Payments:

While **Payments use case is where the blockchain journey started**, evolution of blockchain to execute code based on certain conditions has created numerous possibilities in area of loyalty management, insurance claim settlement, etc.

Transaction Ledger:

Blockchain, when viewed as just **ledger of non-financial transactions with feature of immutability and transparency**, creates a whole new dimension of use cases.

For instance, Patient health history can be captured to identify events where detailed health reports can be stored off-chain and can be retried on need bases.

Similar use cases related to partial ownership of high -value assets, assisting regulators in implementation of Know Your Customer (KYC) requirements, supporting insurance subrogation, all fall under this category.

Identity:

Individuals has become significantly aware and concerned about sharing their private information.

They have also realized that they need to have control over data and they would want to get benefited for organizations that use their data.

These not only give control to end user for data belonging to them, it also creates new avenues for organizations to management consent and collect data through ethical and quality sources.
End users can also monetize their data at a rate and value that they feel is rightful.

History of Blockchain

Blockchain is literally **a chain of blocks, with each block containing certain data. The blocks are chained in such a way that it is not easy to break the chain**.

Harvard Business Review defines blockchain as "**An open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way**."

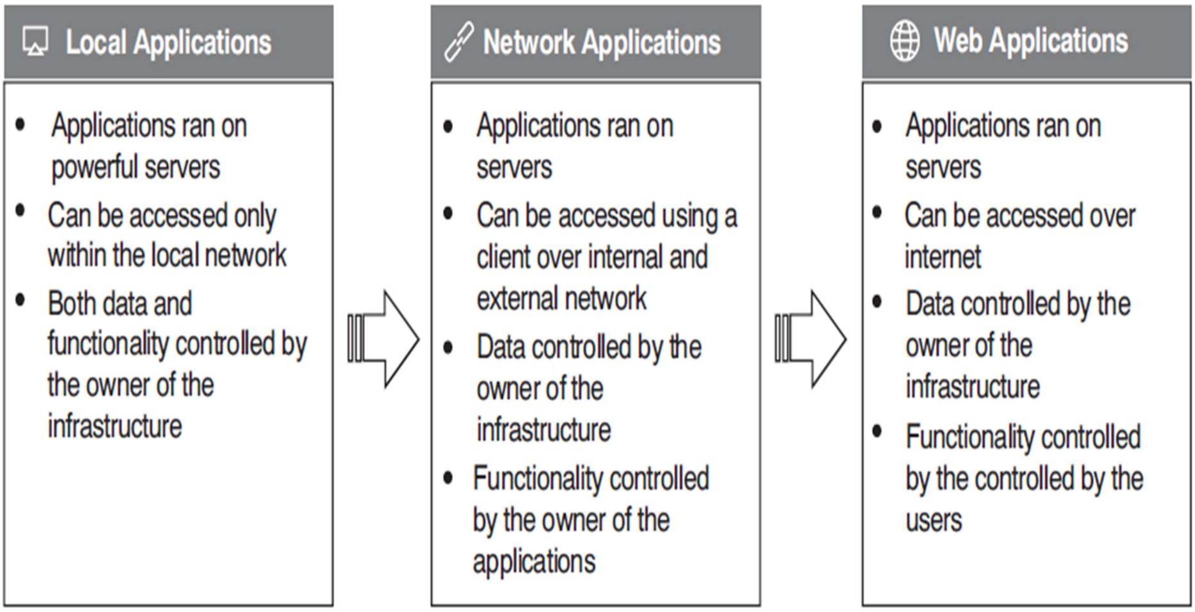
- **Fei stone**
  - While blockchain as we know is a new concept, the idea of having a distributed ledger was discovered long back in Fei Stone Application.
- In **1991**, Stuart Haber and W Scott Stornetta ideated using **a system where document timestamps could not be tempered with using cryptography.**
- In **1992**, Stornetta, Bayer, and Haber explained the use of Merkle trees for **improving efficiency working with this chain of blocks.**
- In **2008**, Satoshi Nakamoto **proposed a peer-to-peer transaction cash system using blockchain**, where a method was proposed so that blocks can be added to the chain with all participants being given a level playing field.
- From **2010 to 2012** was the period of initial transactions on **bitcoin**.
- From **2014 through 2015**, major players in this technical domain, such as **Hyperledger, Ethereum, and R3, were introduced**.
- From **2016** onwards, there have been significant advances in protocols, **building smart contracts, event processing, and creating and supporting decentralized apps**, among other things.

Evolution of Computer Applicaitos

Introduction: -

To discuss about how Blockchain Technology has evolved over the years, it is important to know about evolution of Computer Applications, since it will help us to understand why and how block chain came into existence.

The Evolution of Computer Applications can be perceived from different perspectives, but we have listed here a bird's eye view of the evolution of Computer Applications.



Local Applications

- Applications ran on powerful servers
- Can be accessed only within the local network
- Both data and functionality controlled by the owner of the infrastructure

Network Applications

- Applications ran on servers
- Can be accessed using a client over internal and external network
- Data controlled by the owner of the infrastructure
- Functionality controlled by the owner of the applications

Web Applications

- Applications ran on servers
- Can be accessed over internet
- Data controlled by the owner of the infrastructure
- Functionality controlled by the controlled by the users

Local Applications: -

There were Applications that used to run on powerful servers that were available locally within the network. The users of these applications had to be with in the local network.

For Example, an Airline application running on a server residing in a particular city could not be accessed from other applications of the same airline residing on different Servers.

The data and functionality of the application resided on powerful central servers that were controlled by the owner of the application which also owned the infrastructure. Functionality controlled by the owner refers to the fact that the booking of tickets could be done only by the airlines, that is, an employee of the airline.

Network applications: -

These were applications that ran on powerful servers that were accessible over a network. Applications could also talk to each other to achieve desired business functionality. The users of these applications still needed to be part of either local or external network of the owning organization.

For example, airline application running on a server in the city headquarters could now be accessed from other branches of that airline operating in different cities. Employees of that airline could access these applications from any city that is part of a network.

The data and functionality of the application resided on powerful central servers that were controlled by the owner of the application which also owned the infrastructure. Functionality controlled by the owner refers to the fact that the booking of tickets could be done only by the airlines, that is, an employee of the airline.

Web applications: -

These are applications that can be accessed over the Internet. These can run on powerful servers or multiple distributed commodity servers.

During all these stages, data completely resides on centralized servers that are owned and controlled by the owners of the application. Though the control of functionality is transferred to the end customers during the era of web applications, the code that fulfils functionality still executes on centralized servers allowing censorship to the owners of the application in changing the logic in whichever way they want.

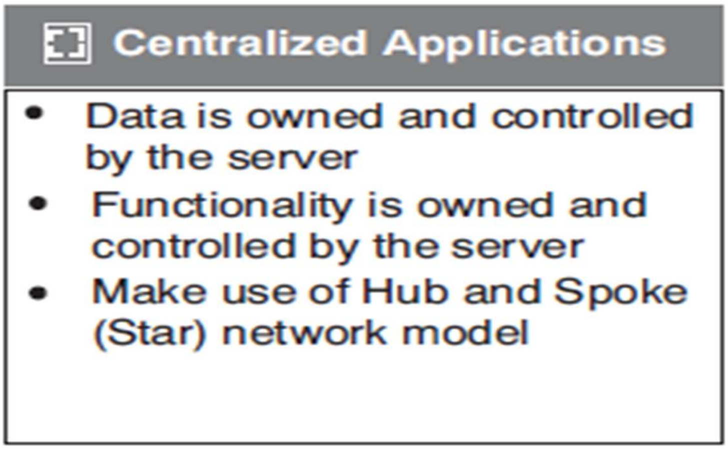
Hence, all the above-mentioned applications are classified as centralized applications. These entities who own the data can monetize data belonging to their users and sometimes even manipulate data to conceal their mistakes. There were also risks of data breach for data owned by these single entities.

Centralized Applications Vs. Decentralized Applications

The problems faced in centralized applications lead to the evolution of decentralized applications.

Centralized applications: -

- Centralized applications can be classified as applications where both data and functionality (business logic) reside on a server that is owned and controlled by a single entity.
- This entity can be an organization or an individual. Current day web applications such as banking applications come under this category.
- For **example**, the customer logs into their banking account using username and password; they maintain their account which includes checking their balance and transfer of money to other accounts.
- The username, password, and other account details of the customer reside on the server.
- Similarly, the business logic involved in checking balance and transfer of money resides and is executed on the server.



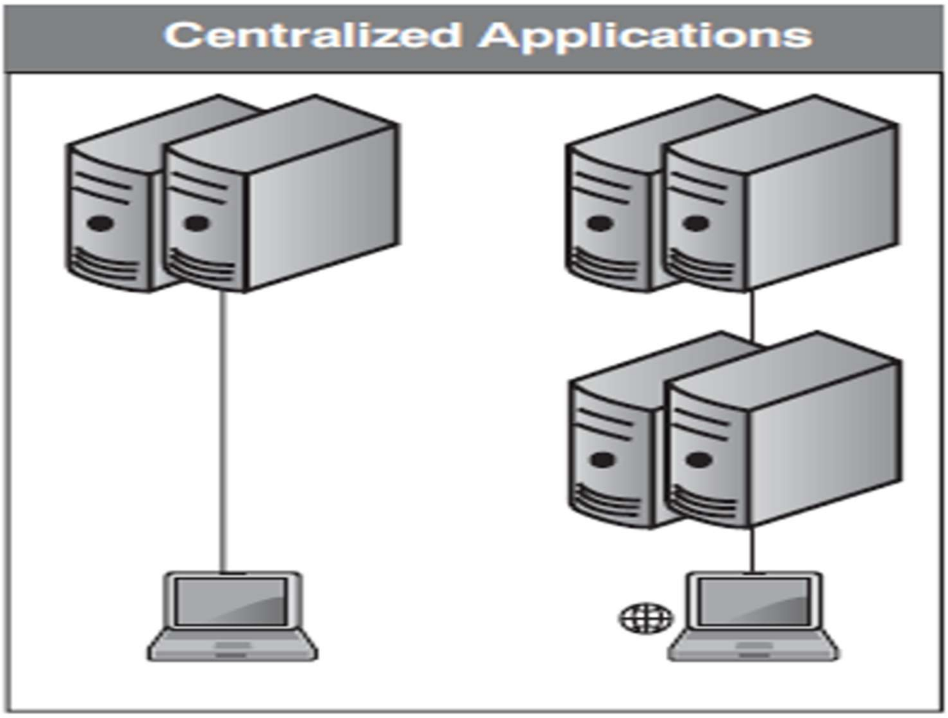
Centralized Applications

- Data is owned and controlled by the server
- Functionality is owned and controlled by the server
- Make use of Hub and Spoke (Star) network model

It should be noted that networked as well as web applications are also centralized applications. The reason for this is that while computing might be distributed in both cases, data is centralized.

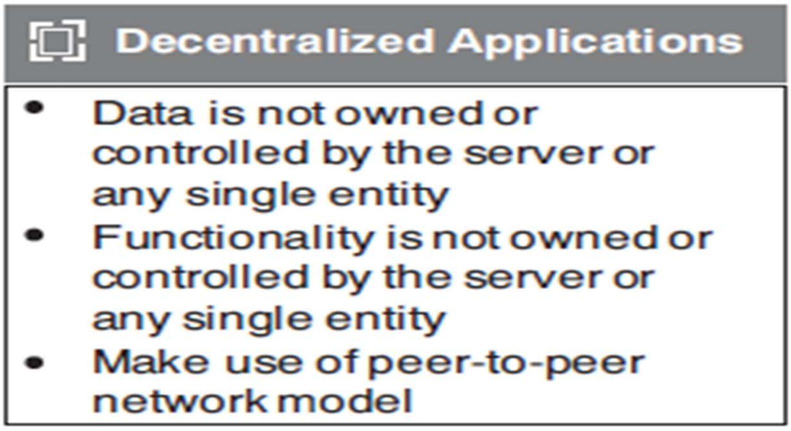
Even organization systems such as hotel booking from independent portals or credit card transaction authorization processes are also centralized systems.

Even when multiple organizations collaborate to provide end-user functionality. every participant tries to share as less data as possible to each other. So, while functionality and data are broken into pieces to be stored at different participant's locations, each participant acts as independently



Decentralized applications:

- Decentralized applications are applications where both data and functionality (business logic) reside on multiple servers that are not owned or controlled by a single entity.
- It means that in case of decentralized applications, **servers are not in the master/slave mode, all servers act like peers and these servers are not centrally controlled by any single entity.**
- Cryptocurrencies such as bitcoin is an example of this application.
- For example, the customer maintains his/her bitcoin account using the cryptographic keys. A cryptographic key is a combination of data that is used to unlock a cryptographic function.
- But her the cryptographic key nor the account data are maintained in a single server or controlled by a single entity.



Decentralized Applications

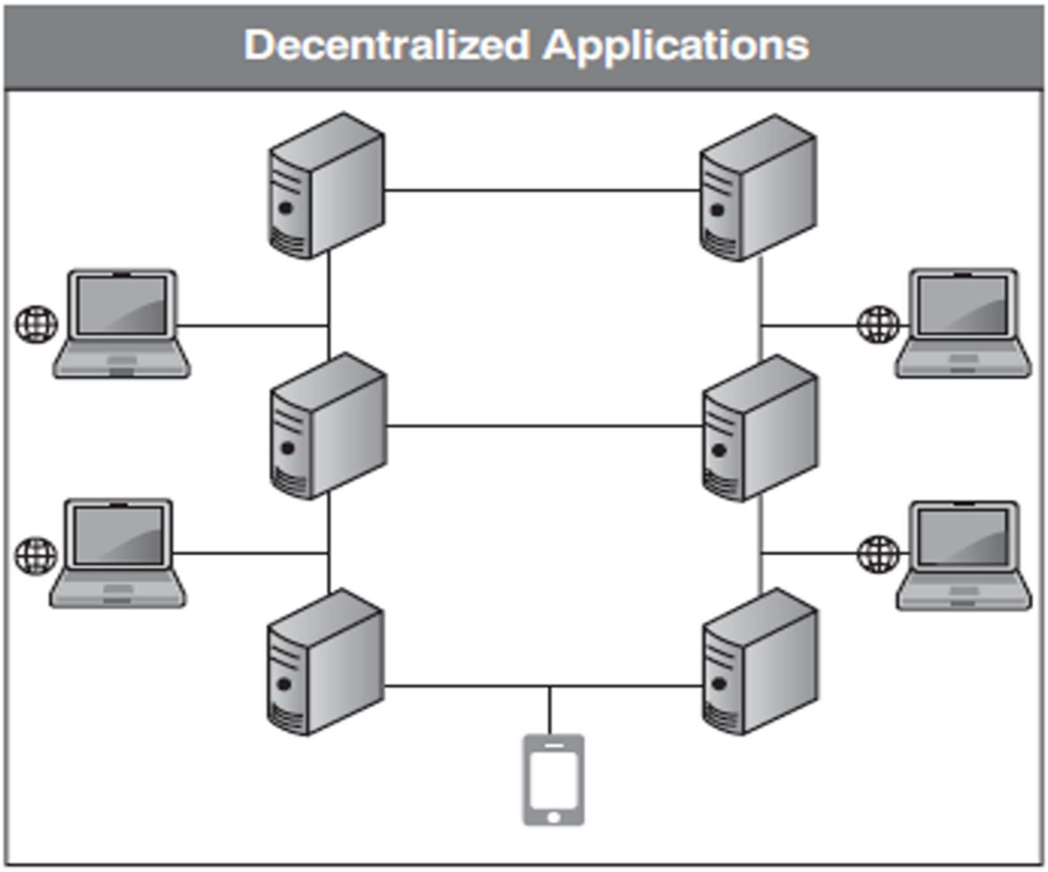
- Data is not owned or controlled by the server or any single entity
- Functionality is not owned or controlled by the server or any single entity
- Make use of peer-to-peer network model

The cryptographic keys are known only to the user; in the case of bitcoin, the keys are known to only the user.

If the user loses the key, then the account is lost forever and no one can recover the account, not even the provider of the account or address. This means that there is no authority that has indiscriminate rights.

Organizations will not be able to clean the slate for their benefit because they have access to the systems.

This technical immutability of information has potential to create transparent environment which is not skewed by any of the participants.



Stages in Blockchain Evolution

Introduction: -

Decentralized applications are applications where both data and functionality (business logic) reside on multiple servers that are not owned or controlled by a single entity.

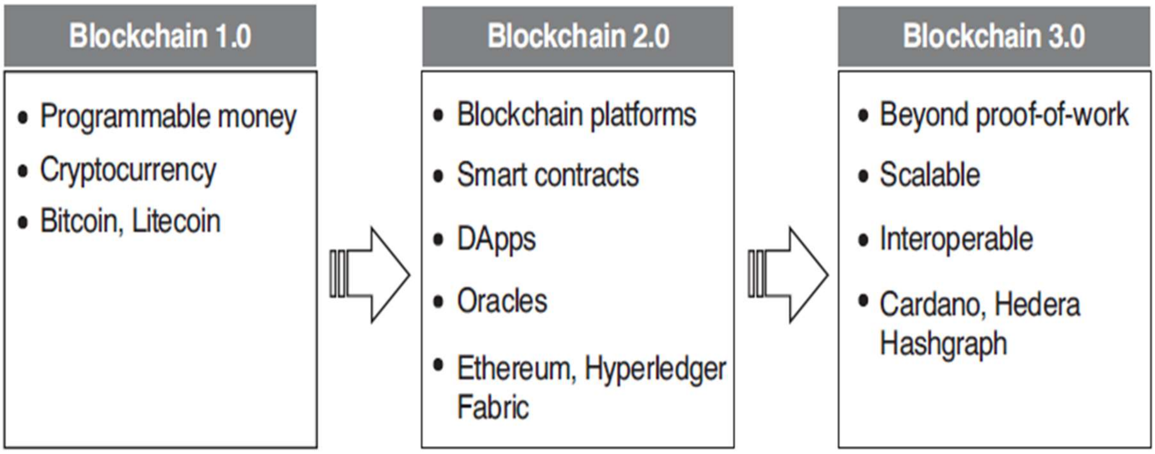
There can be various ways for implementing Decentralized Applications, but the concept of block chain has been the first one to make it a reality.

The first step in the evolution of this reality can be considered as blockchain being invented to solve a particular problem that would make decentralized cryptocurrency a reality.

This was followed by creation of blockchain platform that would allow users to build custom applications.

The recent development in blockchain focuses on building a new blockchain platform that addresses all the challenges in the initial blockchain platforms besides addressing domain-related changes such as compliance.

The above-mentioned trend can be categorized a blockchain 1.0, Blockchain 2.0, and Blockchain 3.0 as shown below:



Blockchain 1.0:

Blockchain 1.0 had cryptocurrency as a central theme. It created new money known as cryptocurrency. This Internet of money supporting programmable money that was not managed by any central bank aimed to challenge the status quo and indiscriminate behavior of central banks of different countries.

Initially, the aim was to support transactions and reward miners, but as time progressed, it tried to improve transaction throughput by changing parameters that can improve the speed at which blocks get chained.

Examples of blockchain networks on Blockchain 1.0 are listed and explained below:

Bitcoin: The first network that introduced cryptocurrency to the world was bitcoin. It introduced the phenomenon of storing, securing, and performing transactions without the need for a bank or for that matter any centralized authority. Bitcoin has evolved and has been accepted in the market to an extent that it stands at market capitalization of 150 billion dollars, as of September 2019.

Altcoins: Lite Coin, launched after bitcoin, is also a cryptocurrency that focused on reducing the transaction time and enabling instant, near zero cost payments to anyone in the world with market capitalization of 3.4 billion. Ripple is a payment protocol that connects banks, payment providers, digital asset exchanges, and Corporates. Bytecoin, Namecoin, and Dogecoin are a few other examples of cryptocurrencies that made their mark during the initial evolution period.

Blockchain 2.0:

While cryptocurrencies were gaining in popularity, people reckoned that the concept of blockchain could be applied in many areas of life outside of digital currencies and this is where we witnessed the emergence of Blockchain 2.0

The key focus of Blockchain 2.0 was to take the engine used in cryptocurrencies, that is, blockchain, **to build platforms that would allow users to build business applications that provide transparency, immutability, and other desirable features**. Blockchain networks also started becoming more of software platforms than a network infrastructure in this version.

A software platform is a combination of software technologies that has prebuilt reusable or configurable components along with guidelines for development. This way, the developers can concentrate on building business functionalities, since low level and reusable requirements are already implemented by the platform.

Similarly, a blockchain platform comes bundled with a group of predefined functionalities such as storing and reading from ledger, consensus, validation, wallet, smart contracts, etc.

The key traits that dominated this segment of blockchain networks are **smart contracts, decentralized applications, and oracles.**

Smart Contracts:

In simple words, smart contract is piece of custom written code implementing business logic. This smart Contract will be deployed on all the nodes of the blockchain network. A typical smart contract contains all the business rules for negotiating the terms of a contract, verifying the contract followed by executing the agreed terms. This is one of the key features that made blockchain useful in many industries beyond crypto currency.

Decentralized Applications:

Smart contracts enable people to build business logic that is not controlled or executed by a single business entity since they were stored and executed on all the nodes of the blockchain network. This has open doors for a new breed of applications known as decentralized applications.

The decentralized application has its backend running on decentralized peer-to-peer (P2P) network allowing users or frontend access the functionality available on the decentralized network.

One of the most popular blockchain networks in Blockchain 2.0 has been **Ethereum.** This global, open-source platform helped people to create decentralized applications through the use of smart contracts.

Ethereum, despite being a platform, has its own native cryptocurrency called ether. Similar to bitcoin, ether is scarce and not controlled any entity such as a government. Ethereum is primarily a public blockchain platform that helps in creation of public blockchain-based applications.

Oracles:

Though business logic is implemented in start contracts, business decisions often rely on inputs needed from external sources. Smart contracts do not communicate directly with the outside world.

Here, we need to remember that smart contracts run on multiple nodes of the network, which means that all the versions of smart contracts running on multiple nodes need to communicate with the same outside source and the result of execution of the smart contracts on all these nodes should provide the same value.

This would result in unnecessary complexities, besides the data provided by the external source may not be reliable.

This is where oracles come in and provide reliable inputs that are needed by smart contracts. Oracles provide a mechanism to interact with the outside world and get reliable external data.

Smart contracts do not communicate with the oracles. The oracles would call the methods of the smart contract with the necessary inputs. The oracles may also streamline the inputs before sending them to the smart contracts. The oracles do not decide the final outcome, they merely provide the inputs and it is upto the smart contracts to use these inputs or reject them while making the final decision.

Blockchain 3.0:

Though Blockchain 2.0 provided enormous potential using blockchain platforms, it had some key issues that acted as showstoppers for mainstream adoption.

Blockchain 3.0 platforms primarily focus on fixing these issues and making blockchain relevant and meaningful for various use cases

Consensus:

Consensus is a revolutionary mechanism introduced in bitcoin, which provided a solution for finalizing a transaction. The consensus mechanisms used in Blockchains 1.0 and 2.0 were mainly utilizing proof- of-work algorithms.

Proof-of-work refers to the class of algorithms that utilize expensive computation for solving a cryptographic puzzle. The time needed to solve the puzzle in bitcoin was approximately 10 minutes whereas the time needed in Ethereum has been approximately 14 seconds. Overall, a transaction cannot be achieved in milliseconds, which is the requirement in most business applications in today's world.

The **Cardano platform** is working on a proof-of-stake consensus known as Ouroboros, which they claim is the first secure peer reviewed consensus. Proof-of-stake refers to the class of algorithms that utilize the stake placed by participants by investing in cryptocurrency.

Scalability:

Scalability refers to the **Capability of a system to handle increasing amount of work**. Due to the delay in the Consensus mechanisms involved, blockchain networks are not able to handle more than few transactions per second as compared to VISA network, which can handle thousands of transactions per second.

This is clearly evident from the many instances that we have seen in bitcoin and Ethereum, where a transaction gets bogged during peak usage. Though addressing consensus would play a major role in the resolution of the scalability problem, there are other issues to be considered for scalability.

For example, each node in the network has to validate all the previous transactions before finalizing the new transactions. Blockchain 3.0 is focusing on algorithms that would address this problem.

Interoperability

Blockchain 3.0 supports interoperability between the platforms. In a pragmatic scenario, it is possible that many enterprises can end up using different platforms. Hence, interoperability is crucial when enterprises try to integrate their functionalities for full-scale automation.

For **example**, an insurance company selling policies on blockchain may like to integrate with payment providers for accepting cryptocurrencies or with a bank for accepting fiat currencies Blockchain 3.0 is trying to address interoperability by coming up with newer protocols that would allow different blockchain networks and platforms to interact with each other.

As a first step, standardization is gradually introduced in the blockchain platforms. Blockchain platforms have started collaborating with each other and recommend adherence to each other's specifications and standards.

Consortia

Introduction: -

The **consortium** will have representatives from each of the organizations or parties involved and they will define the mission, drive the implementation, and govern the blockchain network and standards to extract value out of blockchain technologies.

Based on the drivers for organizations to come together, the Consortium can be classified as -business focused Consortium
-Technology focused Consortium
-Hybrid Consortium

Business Focused Consortium: -

Consortium formed by organizations looking forward to making use of blockchain for business-specific use cases is a business-focused Consortium. This type of consortium analyses business cases for using block chain while adhering to compliance and regulatory requirements.

The **consortium usually forms focus groups or special interest groups to conduct detailed analysis, do proof-of-concepts, and come with specifications as well as guidelines on how blockchain can benefit the business domain.** Usually, the detailed analysis includes studying the impact of blockchain on regulations and can suggest amendment to the regulations, defining standards as well as best practices during implementation of blockchain.

An **example** of such a consortium is **B3i**. It is a blockchain insurance industry initiative and focuses on improving efficiency across insurance and reinsurance domain through blockchain.

Hashed Health blockchain consortium is another example of a business consortium that focuses on creating an ecosystem that leverages blockchain for healthcare solutions.

Digital Trade Chain is another business-focused consortium created by a group of banks to harness the power of distributed ledger technology for commerce applications.

PhUSE consortium promotes research and standardization in the area of blockchain for the pharma domain.

Technology focused Consortium: -

A **consortium focusing on creating generic reusable blockchain platforms is a technology-focused consortium**. This consortium includes representatives & participants from various technology-based organizations.

This consortium also forms focus groups that study various technical challenges as well as business challenges **in adopting blockchain**. Based on its analysis, it can create reusable blockchain platforms and tools.

It also does various proof-of-concepts to understand the challenges involved in the various businesses as well as the technology challenges: Business-related challenges include compliance and privacy whereas technology- related challenges cover performance, scalability, and inventions to emerging problems in the landscape.

For **Example**, **Hyperledger is technology-focused consortium**, which aims to create advances across industry blockchain technologies. The consortium has released various blockchain platforms, the most notable one being Hyperledger Fabric platform that employs a modular architecture allowing plug and play of various components such as consensus and membership services.

Enterprise Ethereum Alliance is other example of technology-focused consortium, which has been created to increase the adoption of Ethereum in enterprises.

Hybrid Consortium: -

A consortium that aims to focus on both technology and business challenges in the area of blockchain considered as hybrid consortium. This consortium does not identify or align themselves to a particular domain.

R3 consortium is an example of a hybrid consortium. It has more than 300 firms as its members working together to build blockchain-based application in industries such as finance, insurance, healthcare, etc.

R3 consortium have also built their own blockchain platform known as Corda to build business application using blockchain.

Forks

Introduction: -

Blockchain is a decentralized application not controlled by any single entity. This means that any update to the blockchain software needs agreement from all the parties running the network.

As because blockchain is a decentralized processing system, changes to software must go along with data as well.

Software fork occurs when two or more versions of software are developed separately out of a single base version, creating two or more separate and independently managed source codes. This branching usually known as forked-off version of the software.

In the context of blockchain, **fork** might refer to a software update to the blockchain software that is agreed upon by a set of participants from a network under consideration.

The type of software update and its implication due to the update is categorized as

-hard fork and
-soft fork.

Hard Fork: -

Hand fork happens when software update to blockchain is not compatible with the previous version. The update will result in the network splitting into two, with one group upgrading to a new version while the other group with participants that opt out of the update.

Hard forks generally occur when a majority of the nodes decide to go with the update while a minority of the nodes are against it.

Bitcoin Cash is an example of a hard fork that happened on 1st August 2017. Bitcoin Cash allows larger blocks in blockchain, which they claim to process more transactions per second.

Soft Fork: -

Soft fork happens when the software update is compatible with the previous version of the software.

In such cases, the network will not split into two, but the same network shall have two versions of software, with one group of nodes running the new version and the other group of nodes running the older version.

Bitcoin's **SegWit** update is a soft fork that changes the way the data is stored. SegWit is the short form for Segregate witness, which proposes to segregate the digital signature from the transaction data allowing more transactions to be included in the blocks.

Public Blockchain Environments

Introduction: -

Blockchain is a software-based system and it is going to evolve over time and will need changes.

Which fork or branch would survive will depend upon the competency of the fork that includes adaption by network participants and capabilities of the group that have pushed through the update.

Software updates need to be tested before they move to production. There are various network environments that are useful to perform such updates, some of them are listed below:

-Mainnet
-Testnet
-Local

Mainnet: -

Mainnet refers to the live production network of a blockchain. The cryptocurrency used in Mainnet possesses real value since all transactions are real transactions stored on the live ledger.

Each and every Transaction involves costs that are paid using the native currency of the blockchain network. Every member who solves the consensus is incentivized by payment in native coins.

For private blockchain networks, Mainnet will be the production system on which real transactions would happen. Change management on Mainnet needs to be controlled in the same way as source code management that happens on enterprise production systems.

Moreover, in case of blockchain, changes to the Mainnet need to analyze version compatibility and impact to decentralized applications that are connecting to the network.

In the event of soft fork, version compatibility of decentralized applications would be even more complicated if the user interface does not take care of version compatibility and availability of the data on the node that it is connected

Testnet :-

Testnet refers to non-production network of blockchain involving actual players performing activities similar to what they perform in production environment. In short, it is a network involving actual players for the purpose of testing.

The cryptocurrency used in the test network does not possess any value since all transactions are fake transactions. There is no cost involved in the transactions. No incentives are paid for the consensus. The size of the network might also not be as large as production and data on Testnet can be regularly wiped off or cleaned based on the decision by all the participants.

Consensus mechanism in Testnet need not be the same as production environment as the aim is to get more testing done with least cost to the network providers.

In private blockchain, it is an integration testing environment where participants would validate their test cases before pushing changes to production.

Decentralized applications also need to be connected to Testnet to validate functionality and ensure there are no issues due soft forking scenarios.

Bitcoin Testnet uses proof-of-work for consensus similar to the Mainnet.

Ethereum network has multiple test networks. Some examples of Ethereum Testnet are Ropsten, Rinkeby, and Kovan. Among these Ropsten uses proof-of-work for consensus whereas Rinkeby and Kovan uses proof-of-authority as consensus mechanism.

Local :-

This refers to the development network. This can also be a single node network created using simulators.

This is required because in the process of development, changes are very frequent and might not always working.

It does not make sense to even have a network to perform transactions. A simulation is enough to validate if desired changes is working fine or not.

One more thing to keep in mind is to understand how the local network is set up. As local network is simulation, not everything that works on local ne work might work in the same manner as Testnet or production.

For example, a decentralized application might get a very quick response as well as confirmation about finalization of a transaction from a simulated local network.

The same might not happen over local network and the experience an end user gets because of these will be very challenging and different.

An example is ganache and ganache-cli f development on Ethereum blockchain

Type of Players in Blockchain Ecosystem

Introduction: -

Blockchain is not just a technology solution, but it creates alternate avenues to perform business and it is supported by different participants to create an ecosystem.

let us understand players in ecosystem.

-End User
-Blockchain Exchanges and Support Organizations
-Blockchain Consortium
-Blockchain Node Owners
-Blockchain Mining Software and Hardware Providers
-Blockchain Mining Pools
-Blockchain Infrastructure Providers
-Blockchain Solution Developers
-Blockchain Solution Sponsor and Network Participants

Not all the players might be part of specific solutions, but this list shall give a good view to readers on where they would fit in.

End User: -

Business users using distributed applications utilizing blockchain are business users. They might not really always be aware or expected to be aware of the fact that the system they are using is powered by a blockchain.

Rather, the solution shall be such that they must not be required to know how blockchain functions.

End users might be investment firms that aim to get benefits of already set up blockchain networks.

Blockchain Exchanges and Support Organizations: -

Blockchain exchanges help provide facilities and services to end users to perform blockchain transactions.

These exchanges also help in conversion and trading of fiat currencies with cryptocurrencies.

Exchanges also provide additional services such as wallet applications that facilitate end users to perform blockchain Transactions.

Binance, Coinbase, Bitfinex are some examples of bitcoin exchanges.

There are also organizations or groups that support end users through monitoring blockchain networks and provide enquiry facilities on networks; these all are considered as support organizations.

Blockchain Consortium: -

Multiple organizations come together to identify use cases and solve business problems in specific domain or technology using blockchain platforms.

A consortium takes various initiatives such as sessions, conferences, and open-source projects.

Benefits of these include but are not limited to influence creation of industry-specific standards, incubate business ideas, and help in the evolution of blockchain technology in specific domains.

Blockchain Node Owners: -

These are organizations or individuals that create, manage, and monitor blockchain network nodes.

These nodes that are managed can be mining nodes, super nodes, full nodes or lightweight nodes.

For public blockchain networks, it has become increasingly difficult to set up a miner node that mines as infrastructure, and the energy required is considerably high.

Blockchain Mining Software and Hardware Providers: -

Blockchain mining assisted by dedicated and customized software and hardware. More so because public blockchain networks have been designed to reward those who have put efforts in the game.

This has created an industry that provides chipsets, software, and other implementation services that can create a financially rewarding node. Some **examples** of these are **Bitmain, Halong mining, and MicroBT**.

Blockchain Mining Pools: -

With competition among miners to win a reward becoming increasingly high, collaboration among miners to solve the puzzle and profit sharing later became more rewarding than individuals attempting to complete it.

Blockchain mining pools help miners pool their resources to get the puzzle solved. While this really defies the initial concept of miners competing with each other, mining pools are major puzzle winners in the current scenario.

Btc.com, blockchain.com and bitclub are some examples of mining pools.

Blockchain Infrastructure Providers: -

These are organizations that are providing individual or packaged products including infrastructure such as servers, network, mining software, etc., to other organizations that want to utilize blockchain for their benefit.

Moreover, these players focus on enterprises aiming to implement blockchain use cases that do not focus on public blockchain cryptocurrency networks.
Some players in this segment include **Microsoft, Intel, Amazon, and IBM**.

Blockchain Solution Developers: -

Blockchain developers help implementation of solutions based on blockchain technologies.

They also help build necessary bridges between traditional enterprise systems, creating meaningful business solutions.

System integrators and consultants are organizations that provide a pool of blockchain-skilled people.

Consultant and developers might be freelance individuals also contributing to the overall ecosystem.

These individuals, either freelancers or from organizations, also help identify and define use cases, prepare meaningful business case, demonstrate proof of concept as well as help organizations realize a defined use case.

Some **examples** of these are **Infosys, Accenture, Deloitte, TCS, and Wipro**.

Blockchain Solution Sponsor and Network Participants: -

These organizations wish to solve real business problems by utilizing blockchain technologies.

They work with all the players to identify and implement meaningful use cases and reap benefits of blockchain technology.

At times, an organization or individual might not be a sponsor but might be a participant working with a node integrated through their enterprise system or through a decentralized application interface.

Players in Market

Introduction:

There are many Real Time Applications and Supporting Technologies running for Blockchain, some of them are listed below:

- Bitcoin:
- MultiChain:
- Ethereum
- Hyperledger
- R3 Corda
- Ethereum Quorum
- Other Blockchain Networks or Platforms
  - Ripple:
  - Hyperledger SawTooth
  - NEO
  - Cardano
  - Hedera Hashgraph

Bitcoin: -

Bitcoin is a cryptocurrency and a payment network that uses cryptographic techniques and transactions.

The inventor of bitcoin who goes by the name Satoshi Nakamoto is still not known to the world. He submitted the whitepaper explaining the protocol and also shared the first implementation of the protocol.

Bitcoin uses distributed public ledger for maintaining a record of the transactions on all the nodes that comprise the bitcoin network.

As mentioned earlier, bitcoin is a public non-permissioned blockchain network as anyone in the world can become a member of the network as long as they provide necessary processing power.

Bitcoin Core is the software that runs the blockchain network. Any person who uses to run a bitcoin node needs to download, install, and run the Bitcoin Core software.

The software also contains a secure digital wallet that can be used to store, receive, and send bitcoins.

MultiChain: -

MultiChain is a platform that helps create private or consortium blockchain networks in simple ways.

MultiChain is based on blockchain protocol and software used in bitcoin. While the software is derived from blockchain, MultiChain has some significant differences in terms of mining and privacy.

Since MultiChain is targeted only for private or consortium blockchain networks, it allows permissions to be defined at the network level on who creates assets, sends assets, and receives assets.

Similarly, it allows mining to be performed without proof-of-work, using the concept of validations in a round robin fashion saving compute power. MultiChain provides a simple API and command line interface.

One of the key features of MuluChain is asset. Any business entity can be represented as an asset in MultiChain. The asset can be easily created using the simple API.

Users can also send and receive assets. Though this makes implementation of business functionality easy, custom business rules cannot be implemented on MultiChain. Any Business rules surrounding the creation and transfer of assets has to be coded outside the MaltChain blockchain that is known as an off-chain code.

Ethereum: -

Ethereum is a global, open-source platform for decentralized applications. It was proposed by a cryptocurrency programmer and researcher, Vitalik Buterin, in late 2013. However, it went live on 30 July 2015.

Ethereum represents generation 2.0 in blockchain evolution journey. It provides a decentralized virtual machine, the Ethereum Virtual Machine, which can execute scripts on an Ethereum node. These scripts are known as Smart Contracts.

The virtual machine's instruction set, in contrast to others like Bitcoin Script, is thought to be Turing-complete which means that it is like any other high-level language that can supports writing any logic in it.

It should be noted though that it is very costly to execute programs on Ethereum network: doing even simple additions can cost a fortune.

Ethereum is not just a blockchain network, it is a distributing computing platform and operating system. Ethereum allows users to create their own operations of any complexity they wish.

In this way, it serves as a platform for many different types of decentralized blockchain applications, including but not limited to cryptocurrencies.

Hyperledger: -

Hyperledger is a multi-project open-source collaborative effort hosted by The Linux Foundation, created to advance cross-industry blockchain technologies.

Hyperledger Fabric is the most popular and the most widely used framework among the Hyperledger projects.

Hyperledger Fabric is an open-source distributed ledger technology platform that is permissioned in nature and designed for use in enterprise contexts.

It offers some key differentiating capabilities as compared to other popular distributed ledger or blockchain platforms. Hyperledger introduces concepts of channels where ledger sharing can happen in only selected participants.

A single network can support multiple channels allowing same infrastructure use for multiple use cases. Hyperledger also implements "orderer" nodes that create blocks on network. This makes Hyperledger more of a shared ledger than a blockchain.

The architecture of Hyperledger Fabric is highly modular and configurable. It enables innovation, versatility. and optimization for a wide spectrum of industry use cases such as healthcare, insurance, banking, supply chain, supply chain, and even digital music delivery. Fabric also allows pluggable consensus protocols.

R3 Corda: -

Corda is an open-source distributed ledger platform, which empowers private interactions between businesses. Though the origin of Corda was driven by the requirements of financial industry, it has wider applicability across different industries and use cases which require shared ledger.

Corda's design is different from a traditional blockchain system as it does not use a chain of blocks linked by hash to store data.

However, it uses unspent transaction output (UTXO) model to structure and validate the actions.

The fundamental building block in Corda is known as "state object", which represents a specific instance of a specific real-world contract or a section of it.

Transaction validation services are provided by special nodes on Conda network known as notaries,

Ledger visibility in Corda is controlled and confined to a group of concerned parties. In this way, it ensures strict privacy.

Ethereum Quorum: -

Ethereum Quorum n a permissioned implementation of Ethereum, focusing on data privacy. It is a software fork of Ethereum and maintained in line with Ethereum releases.

On Ethereum Quorum, private transaction and private contracts are implemented with encrypted message exchange.

As it is focused only on enterprise uses cases, it offers alternatives consensus mechanisms such as Raft Consens, and Istanbul BFT.

In Ethereum, node permissions are supported using smart contracts, allowing only known parties to join the network. With better choice of consensus protocols, it offers higher performance compared to Ethereum public blockchain

Other Blockchain Networks or Platforms: -

Ripple:

Ripple is a payment protocol for real-time gross settlement system (RTGS), currency exchange, and remittance network.

This is not a blockchain platform and is purely focused on cryptocurrency

Hyperledger Saw Tooth:

Hyperledger Saw Tooth provides a platform to build distributed ledger applications using modular architecture and also supports deploying and running them. It enables creation of both permissioned and non-permissioned networks.

NEO

NEO is a blockchain platform and cryptocurrency. It is also referred to as "Ethereum of China". NEO focuses on Digital Assets, Digital Identity and smart contracts to create a smart economy.

Cardano

Cardano is also a blockchain platform and cryptocurrency. Cardano is developing a smart contract platform that seeks to deliver more advanced features than any other protocol previously developed.

The algorithm, Ouroboros, is claimed to be the first provably secure proof-of-stake algorithm that is peer reviewed by academics.

Cardano can be classified as Blockchain 3.0 technology since its primary aim is to address the shortcomings of Blockchain 2.0 technologies.

Hedera Hashgraph

Hedera Hashgraph is a distributed ledger technology using graph, such as structure, for the network.

It uses asynchronous Byzantine Fault Tolerance for consensus and gossip protocol for communication.

Hedera Hashgraph can also be classified as Blockchain 3.0 technology.

---------************----------