4 Permissioned Blockchain : Hyperledger Fabric

Module - IV

Syllabus

Introduction to Framework, Tools and Architecture of Hyperledger Fabric Blockchain.

Components : Certificate Authority, Nodes, Chain codes, Channels, Consensus : Solo, Kafka, RAFT Designing Hyperledger Blockchain Other Challenges : Interoperability and Scalability of blockchain.

Self-learning Topics : Fundamentals of Hyperledger Composer.

4.1 Introduction to Hyperledger

- In order to improve cross-industry blockchain technology, the Linux Foundation produced the open source initiative known as Hyperledger.
- "Hyperledger is an open sourced community of communities to benefit an ecosystem of Hyperledger based solution providers and users focused on blockchain related use cases that will work across a variety of industrial sectors." – Brian Behlendorf, Executive Director of Hyperledger
- Hyperledger is neither a Blockchain nor a company, nor is it a cryptocurrency. It is a piece of software used to build one's own custom blockchain service.
- A cross-industry open source collaborative project called Hyperledger was developed to advance blockchain technologies.
- Global leaders in banking, supply chains, technology, IOT, and finance are participating in the collaboration with Linux Foundation, which is also being hosted by the Linux Foundation.
- According to the Hyperledger philosophy, multiple private chains will manage multiple markets around the world.
- Since each business is distinct in its own right, applications that cater to these businesses should be created using individualized rules. Unlike Ethereum, which frequently forces programmers to create their applications using generic protocols.
- In late 2015, a small group of developers launched the Hyperledger project.
- These developers were from a range of industries, including data science, manufacturing, banking, etc., and they shared the objective of making blockchain technology more usable to developers and enterprises.

Why is Hyperledger necessary ?

- Public blockchains do not support private and confidential transactions.
- Public blockchain is having issues with scalability.
- The developers discovered during extensive testing that blockchain networks, where each peer must simultaneously run consensus and validate each and every transaction, suffer greatly in terms of scalability.
- Additionally, since a transaction's integrity is protected by a number of safeguards, transactions that require some level of anonymity and privacy cannot be carried out on public blockchains.

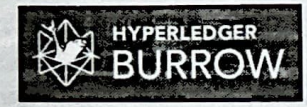
4.2 Introduction to Hyperledger Framework

There are five blockchain frameworks.

1. **Hyperledger Iroha :** Based on Hyperledger Fabric, Iroha was developed for mobile development projects and developed by Soramitsu, Hitachi, NTT Data, and Colu. Both a novel chain-based Byzantine fault tolerant consensus method called Sumeragi and cutting-edge, domain-driven C++ architecture are featured in it.

2. **Hyperledger Fabric (HLF) :** The modular architecture of Hyperledger Fabric, which was created by IBM, is meant to serve as a foundation for other systems or applications. It makes use of containers to hold smart contracts known as chaincode, which constitute the system's application logic, and plug-and-play elements like consensus and membership services.

3. **Hyperledger Burrow :** Originally developed as a client-built modular blockchain to the specifications of the Ethereum Virtual Machine, Hyperledger Burrow was first made available by Monax and Intel (EVM).



4. **Indy Hyperledger :** The Sovrin Foundation originally contributed to Indy, a Hyperledger project designed to offer independent identity on distributed ledgers. Hyperledger Indy provides the following tools, libraries, and reusable parts for building digital identities with blockchains or other distributed ledgers:

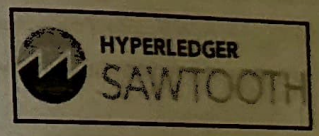
a) **Indy-Node :** In order to make digital identities based on blockchain or other distributed ledgers interoperable between administrative domains, apps, and any other silo, Hyperledger Indy offers tools, libraries, and reusable components. Indy can be used alone or in conjunction with other blockchains to power the decentralisation of identification. A self-sovereign identification ecosystem is offered by Indy Node on top of a distributed ledger.

b) **Indy-Agent :** Messages are used by agents to communicate with one another. Agents are a combination of functionality and storage. Asking about controlling identities and carrying them to other agents in order to establish relationships is the responsibility of the agents.

c) **Indy-Ledger**

- Provides a basic, immutable, ordered log of transactions that is backed by a merkle tree and is written in Python.

- Producing verifiable evidence of presence and data consistency in this manner is effective.
- Benefits of Hyperledger Indy
  - Multiple system integration
  - Self-sovereignty
  - **Privacy :** Being decentralized in nature, Indy assures complete privacy to the user. The digital identity created by Hyperledger Indy can be used across multiple applications and domains, thus making it super compatible.
  - **Peer-to-peer interaction :** The platform involves peer-to-peer interaction rather than depending on a centralized intermediary.
  - **Zero-knowledge proof :** Zero-knowledge proofs allow you to disclose only needed information without having to release any other information.
  - **Minimized Identity theft :** Due to DIDs, the issue of identity thefts will reduce significantly since they are unique and owned by a single user.
  - **System efficiency :** The RBFT consensus protocol makes Hyperledger Indy very efficient.



5. **Hyperledger Sawtooth :** Sawtooth was developed by Intel and incorporates a revolutionary consensus mechanism known as Proof of Elapsed Time that Intel developed (PoET). The distributed consensus goal of PoET is to be attained as quickly as feasible. With support for both permissioned and permissionless deployments and acknowledgement of varied requirements, Hyperledger Sawtooth offers a lot of potential in a lot of domains. Sawtooth is made to be adaptable.

4.3 Tools and Architecture of Hyperledger Fabric Blockchain

4.3.1 Hyperledger Tools

Currently, the Hyperledger project includes five tools, all of which are hosted by the Linux Foundation.

1. **Hyperledger Composer :** is a collection of collaborative tools for constructing blockchain business networks that accelerates the creation of smart contracts and blockchain applications as well as their deployment over a distributed ledger. Hyperledger composer was developed by IBM and Oxchains.
2. **Hyperledger Caliper :** Currently under incubation, caliper is a blockchain benchmarking tool that enables users to assess the effectiveness of a particular implementation using specified use cases. This one was developed by engineers from various organizations.

3. **Hyperledger Cello :** Hyperledger Cello was first provided by IBM and sponsored by Intel, Huawei, and Soft... For the blockchain ecosystem, it is a widely used blockchain module kit. The effort required to create, maintain, a... terminate blockchains is greatly reduced by Cello. Furthermore, because it provides a multi-tenant chain servi... this tool can work on top of a variety of infrastructures like virtual machines, bare metal, and container platform...
4. **Hyperledger Explorer :** Hyperledger Explorer was created to help programmers create interactive w... applications. It was first made available by Intel, IBM, and DTCC. Using the tool, users can view, deploy, invoke, an... query blocks, transaction data, chaincodes, and other data that is kept on a Blockchain ledger.
5. **Hyperledger Quilt :** A blockchain tool for businesses called Hyperledger Quilt was first made available by IB... Data and Ripple. Ledger system interoperability is made possible by Quilt. The Interledger Protocol (ILP) i... payment protocol for transferring value between distributed and non-distributed ledgers, enables it to accomplish this.

4.3.2 Hyperledger Fabric

- Hyper ledger fabric is a private and permissioned blockchain.
- It is a framework for building, deploying, and maintaining blockchains for businesses that, as a result, ensures trust among business partners and responsibility.
- It runs smart contracts called "chaincode" within Docker containers.
- Through a reputable MSP (Membership Service Provider) , users of the Hyperledger Fabric network sign up.
- The ability to create channels in the hyper ledger fabric enables a group of users to construct their own ledger of transmissions.
- Shared ledger : HF has a ledger subsystem comprising two components,

  The world state and transaction log.
- The ledger's current state is described by the world state component. It is a ledger database.
- The transaction log component keeps track of all transactions that have contributed to the world state's current value.

4.3.2(A) Advantages of Hyperledger Fabric

- PKI-based identity management (public key infrastructure)
- Efficient processing through segregation of consensus and chaincode execution
- Privacy and confidentiality via 'channels'

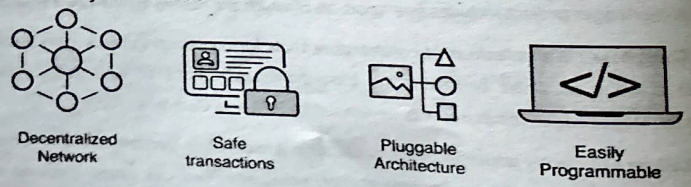


Fig. 4.3.1

4.3.2(B) Hyperledger Fabric Architecture

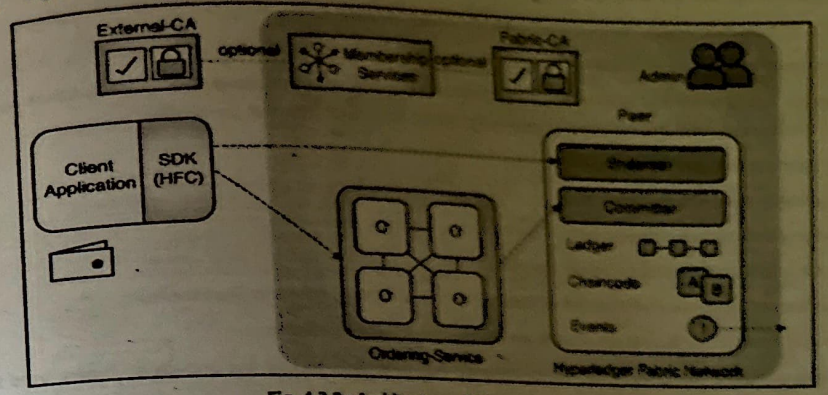


Fig. 4.3.2 : Architecture of Hyperledger Fabric

"Members" refers to the businesses that support the growth of the Hyperledger Fabric network.

4.3.2(c) Components of Hyperledger Fabric

- Nodes
  - Client
  - Peer
  - Ordering Service
- Fabric CA
- Channel
- Membership Service Provider (MSP)
- Chaincode

Client

- Represents the end user or client applications which trigger blockchain events.
- Clients are software programmes that propose transactions on a network on behalf of a person.
- Clients interact with both their fellow customers and the ordering service.
- The client interacts with the network using a Fabric SDK.
- When reading or writing data from a Fabric blockchain the client interacts with the SDK. To ensure that a legitimate client has started the network transaction, the CA authority issues a certificate to the client as well.

Peer

- The group of peer nodes or peers is a vital component of a Hyperledger Fabric blockchain network.
- Because they monitor ledgers and smart contracts, peers are essential.

- Peers are nodes that are active participants in the network.
- Peer is the location where the blockchain data and ledger are kept.
- There must be more than one peer in the production.
- Peers are a redundant and flexible component that can be added, stopped, changed, or deleted. Client applica can communicate with the services that peers offer thanks to a set of APIs that peers offer.
- One peer may be part of many channels.
- Every single channel is inside the peer.
- It endorse any update of the ledger
- You can create a backup of the ledger from the peer.
- All nodes and peers within the blockchain network are equal in public networks like Ethereum.
- All nodes/peers in the Blockchain network are not equal in Hyperledger Fabric.
- The role, behavior, and tasks carried out by the peers may differ even though the underlying binary used for ea peer may be the same (version differences are acceptable).
- The following list includes the typical categories of "roles" that peers are given :

  Endorsing peer, anchor peer, and Ordering peer

Endorsing Peers

- All peers have the capability to act as an endorsing peer, and will validate transactions.
- The additional duty of supporting a transaction falls on a special class of committing peers called endorsing peer
- They accept the client's request for a transaction and approve it.
- A ledger and a copy of the smart contract are deployed on each endorsing peer.
- The transaction simulation is the primary purpose of the endorser.
- It produces the Read/Write sets that are supplied to the client and is carried out in line with the smart contract o the client's private copy of the ledger.
- Although the transaction is not recorded in the ledger during simulation.

Anchor Peers

- We require some peers in order to have communication across an organization because the Fabric network ca span multiple ones.
- Not all peers have this ability, but there are some unique peers—the Anchor peer—who are the only ones with this permission.
- Anchor peers are well-known outside of the organization.
- The anchor peers for the participating organizations are encoded in the genesis block at the time the network i first created.
- As a result, let's say Organization-A peers will have access to Organization-B anchor peers' gossip.
- However, because regular peers are unknown to those outside the organization, the non-anchor peer Organization-B cannot connect with the peer in Organization-A.

- Through peer update transactions, anchor peers can be added to a Live network.

Ordering Peers

- It interacts with other peer nodes and approves the entry of transaction blocks into the ledger
- It doesn't store smart contracts.
- It doesn't keep a ledger.

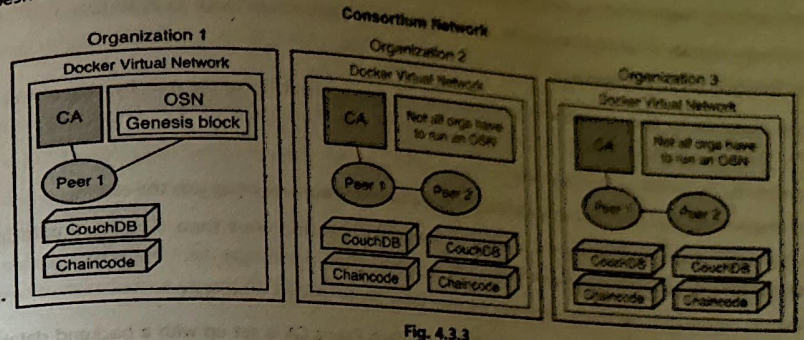


Fig. 4.3.3

- Nodes in the network run in Docker Containers on Virtual Machines in the Cloud or locally.
- Each organization will join 1 or more channels.
- Each organization will designate 1 or more peers as 'Anchor Peers'

Ordering Service Nodes

- Responsible for maintaining consensus among peers.
- Ordering service is actually the heart of consensus algorithm and the heart of Hyperledger fabric
- Main role is to provide the order of operations.
- Before committing anything to the ledger it must pass through the ordering service.
- It is responsible for verification, security, policy, verification etc.

Hyperledger Fabric CA

- A Certificate Authority (CA) for Hyperledger Fabric is the Hyperledger Fabric CA.
- It offers Enrolment Certificates for issuing.
- It performs certificate revocation and renewal.
- It consists of both server and client components.
- It offers identity registration services or establishes a user registry connection with LDAP.

Channels

- A private "subnet" of communication between two or more particular network participants is referred to as a channel.
- Members of the organization, anchor peers for each member, the shared ledger, the chaincode application, and the ordering service nodes all contribute to the definition of a channel.

- Every party must be authenticated and authorized to transact on that channel.
- There is independent ledger in each channel.
- A membership service provider assigns a unique identification to each peer when they join a channel (MSP).
- Channels are completely isolated. They are completely isolated instances of hyper ledger fabric. They have diff... ledgers, different height of blocks, policies, rules.
- We can make a policy about who can see the data in the channel and who can make an operation.

MSP (Membership Service Provider) :

- Making digital IDs for team peers and organization users is the responsibility of the membership service prov... (MSP).
- It provides the credentials to various entities in the network.
- An existing network must have its peers' identities defined before a new entity may join the channel.
- An MSP implementation called Fabric CA offers a method for enrolling users from a network participant a... granting them with digital IDs (X.509 certificates).
- Members in organization can create certificates for their participants and infrastructure.
- Typically, a Docker container is used to execute Fabric CA. Each Fabric CA is set up with a backend database t... holds the registered identities and their X.509 certificates. The default is SQLite, but there are additio... alternatives, including PostgreSQL or MySQL. Users' private keys are not stored by Fabric CA.
- Identity is going to be a digital certificate and users are going to be using this digital certificate to signed t... transactions and submit them to the blockchain and the advantage of signing is that they authenticate with t... blockchain that they are a legitimate user and it also ensure that they get the right access privileges on t... blockchain for the transactions they are performing.

Chaincodes

- Similar to a smart contract, a chaincode often manages business logic approved by network participants.
- All our business logic is inside the chaincode.
- It is written in **Go langauage**. Implementation of Java and javascript are on the way.
- Chaincode may be installed in every peer and channel.
- It enforces rules to read and altering state. Chaincode execution results in a state change in ledger.

Transaction Flows

- The steps of Fabric's transaction flow are proposal, packaging, and validation. In order to distribute newer bloc... on the network, the orderer is in charge of packaging and takes part in the validation process.
- Consensus is achieved using the following transaction flow :

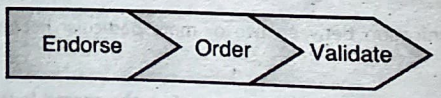


Fig. 4.3.4

Endorsement

- The client application will send the transaction to a small number of peers, who will then execute it and concur that the result is the same for all of them.
- Therefore, they will all locate the transaction's output and add their signatures to it.
- To confirm that this transaction is a genuine transaction and all outputs are the identical, the client application must obtain confirmation from numerous peers in the networks.
- We shall discuss the submission of the transactions for ordering once you have gathered enough signatures.

Order

- Various users and/or multiple applications may be submitting these transactions to order.
- As a result, the ordering service will now make sure that they are all completely arranged across all nodes.
- When using the ordering service, you must first identify the order of all the transactions before you can resolve the validation.
- The ordering service's main objective is to provide an entire order for published transactions and cut blocks with ordered transactions; it cannot do transaction validations.

Validate

- For instance you should not be performing two transactions simultaneously that modify the same state.
- So this is equivalent to the double spending problem that we would have seen in bitcoin. If you have just a 20 rupees balance in a bank account, you should not be transferring 20 rupees to two different people trying to double spend that money.
- So validation is if two transactions are going simultaneously only one of them can succeed and which one succeeds will depend on the ordering service.
- Every subsequent transaction attempting to edit the same transaction in the same block will be validated after the first transaction that successfully modifies the data element. This is the validation stage.
- There are many options for ordering services in Hyperledger Fabric. There are several ways to order services in Hyperledger Fabric.
  - SOLO
  - Simplified Byzantine Fault Tolerance

4.4 Solo (deprecated in V2.X)

- The ordering service's Solo implementation, which just has one ordering node, is exclusively meant for testing.
- It has been deprecated and might be completely deleted in a later version. For a comparable function, Current Solo users ought to transition to a single-node Raft network.
- Solo is a brand-new blockchain technology developed exclusively by Biglab to facilitate peer-to-peer transactions in micropayments like IoT, lending, loyalty, and other similar applications.
- A transaction in this case is only approved by one node, hence the term Solo.

- **Why do we need Solo ?**
  - The expenses and reaction times associated with blockchain transactions are considerable. Bitcoin c... between $10 to $20 every transaction, and the processing time might take up to 10 minutes. Accordin... Blockchain.com, the confirmation time for a bitcoin transaction is 78 minutes on average. However, ... average time on Sunday was as long as 1,188 minutes.
  - Ethereum charges between $1 and $2 USD for each transaction, and there is a 1- 2 minute delay.
  - Use of a new blockchain network is required to support micropayments, such as those involved with IoT, ma... and fintech applications. This network must incur the least amount of costs while offering the highest volu... of transactions per second.
- **How ?**
  - Solo is designed to enable a Region, which could be an application domain like IOT or a physically defin... area such as a city, state, or country.

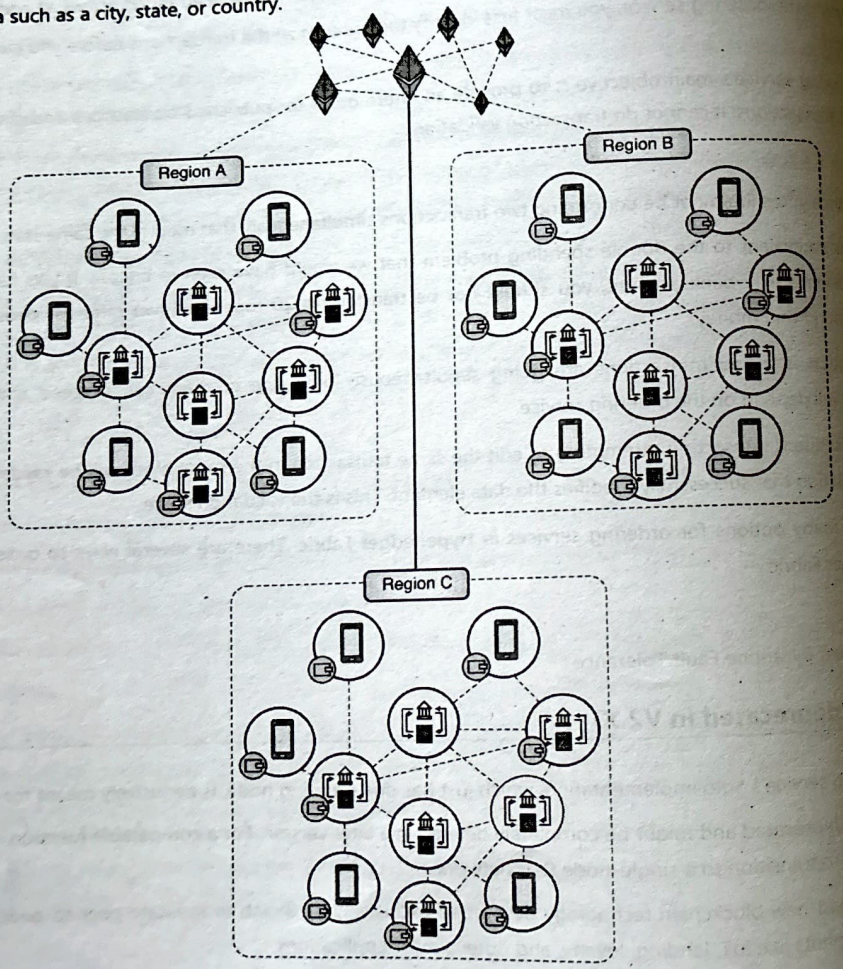


Fig. 4.4.1

- To broaden its geographic reach, a Solo network might connect to another one over the enormous Ethereum network. Solo should work successfully across all ETH nodes that support ERC-20 tokens as long as ETH can support ERC-20 token transactions. We will use an ETH tool and client software to issue ERC-20 tokens like Mozo at each connecting Bridge with Solo. This is done so that when the ETH client software is updated, we can just plug in our Bridge.

- A Solo region contains a number of Data Nodes that schedule the transactions and store the distributed ledger for that region.
- Since Data Nodes operate as dispersed nodes in the same distributed ledger for the entire region, they can support one another.
- Millions of mobile devices and PCs will execute transactions simultaneously thanks to Solo, which also maintains a predictable transaction delay characteristic in the form of network transit delay, data node scheduling, and negligible transaction processing delay. We can promise that all transactions will be swift and well-organized in a given area.
- Users of Solo must have a wallet that can be identified by a private key they privately generated. They should also give a public key to Solo so that it can use it to check the authenticity of their signatures. Every user has a distinct address.
- After the initial successful handshake, it will connect with n nodes for failover switching and service recovery. This failover switching is a portion of SOLO's main responsibility.

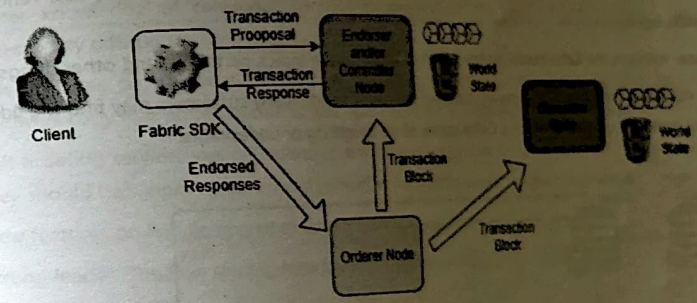


Fig. 4.4.2

- When a user initiates a transaction outside of its Solo region, the transaction will travel through the Bridge, the Ethereum network, and back to a destination Solo, unless it is an exchange from Mozo to ETH, in which case the destination will be a third-party exchange that supports the buying and selling of ERC-20 tokens. As a result of the need to use the ETH blockchain network, the transaction fee is higher than it would be within a Solo zone.
- Please take note that the ETH blockchain technique can be used to restrict double spending, and that perceived hackers can be detected by data analysis at the Audit DataNode and minimized through random transaction checking with other DataNodes.

- Because Solo is designed for small payments, the number of transactions is anticipated to be in the millions, so we can accept an alternative to decentralization to reduce broadcast storms and save enormous network capac... A possibility might be a distributed ledger with multiple shards.

4.5 Kafka (deprecated in v2.X)

- Created by LinkedIn and now a part of Apache, Apache Kafka is an open source platform for the instant storag... and analysis of massive data.
- It stores and analyzes massive data quickly via the message system, or queue.
- The ordering service nodes (OSNs) of Hyperledger Fabric utilise your Kafka cluster to provide an ordering servic... to your blockchain network.
- Apache Kafka is a crash fault tolerant (CFT) solution that makes use of a "leader and follower" node arrangemen... much as Raft-based ordering.
- A ZooKeeper ensemble is used by Kafka for management.
- **Zookeeper**
  - The Apache ZooKeeper project, which is free and open source, enables clusters to spread data like configuration, name, and group services across sizable clusters.
  - ZooKeeper employs a hierarchical key-value store. used in situations with high availability. Apache Java-based ZooKeeper is published under the Apache License 2.0. Some major corporations, like Rackspace, Yahoo, eBay and Reddit, use it.
  - Zookeeper monitors the Kafka cluster nodes' health as well as Kafka topics, partitions, and other things.
- Since Fabric v1.0, there has been a Kafka-based ordering service; however, many customers may find the additional administrative labour required to maintain a Kafka cluster to be unsettling or undesirable.

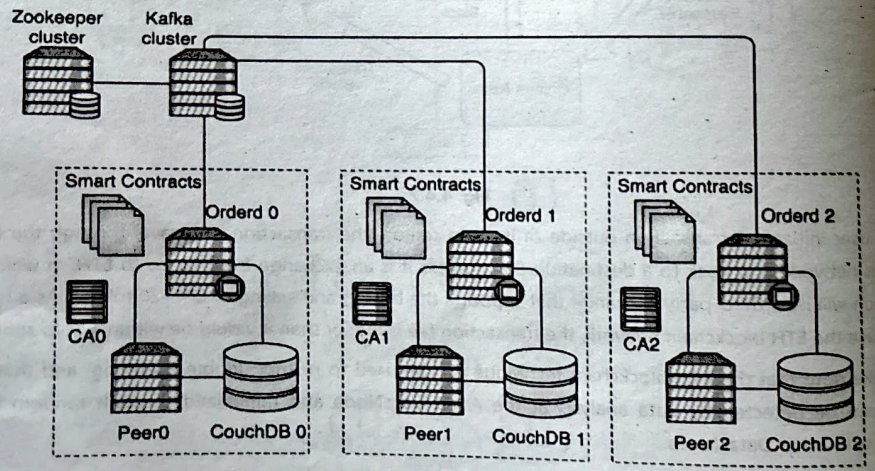


Fig. 4.5.1 : Kafka

- Large networks cannot be used to run Kafka and Zookeeper. Kafka should be run in a small group of hosts even though it is CFT. Practically speaking, this means that only one company should manage the Kafka cluster. Given this, using Kafka (which Fabric enables) with ordering nodes controlled by different organizations does not decentralize the nodes because eventually, all of the nodes connect to a Kafka cluster that is managed by a single company.
- Since Kafka is supported natively, users must obtain the necessary images and figure out how to utilise Kafka and ZooKeeper on their own. Similarly, Apache, the open-source creator of Kafka, handles support for Kafka-related issues rather than Hyperledger Fabric.
- The administrator of the orderer organization chooses how many nodes they want to utilize on a specific channel and Kafka uses a pool of servers (referred to as "Kafka brokers").

4.6 RAFT Designing Hyperledger Blockchain

- Raft is a crash fault tolerant (CFT) ordering service that is based on the etcd implementation of the Raft protocol as of version 1.4. (a distributed, reliable key-value store for the most critical data of a distributed system).
- It finds a solution to the issue of getting numerous servers to concur on a shared state even in the presence of failures.
- It is designed to be an alternative to Paxos..
- Diego Ongaro and John Ousterhout of Stanford University created the Raft algorithm. Raft was created to have a better knowledge of consensus because its predecessor, the Leslie Lamport-developed Paxos Algorithm, is exceedingly difficult to comprehend and use.
- Raft operates on a "leader and follower" architecture, where a leader node is chosen (per channel) and the followers copy that node's decisions. Raft operates by having the cluster choose a leader.
- Raft ordering services' design enables several businesses to contribute nodes to a distributed ordering service, and they should be simpler to set up and administer than Kafka-based ordering systems.
- New features on Raft compared to other consensus algorithms
- Strong leader (The flow starting from leader to the followers)
- Leader election (based on random timers)
- Membership changes (mechanisms for changing the set of servers when configuration overlaps)
- The RAFT algorithm is similar to pBFT but in RAFT only the leader node can establish communication with other nodes and take decisions about the state of the transaction.
- Raft needs to run on 5 servers to tolerate the failure of two of them.
- Time is divided into short, arbitrary-length terms by the Raft algorithm. The term number, which is a monotonically growing number, is used to identify each term. Each node is present in one of the three states: leader, follower and candidate. Raft divides consensus into three phases :
  - **Leader Election :** If an existing leader fails then a new leader needs to be elected.
  - **Log replication :** To ensure that every copy is current, the leader duplicates log to other nodes.

- **Safety :** If one of the nodes has previously committed a log entry to an index, node cannot apply a different log entry at that index.

- There are three possible states for each server: leader, follower, or candidate.
- At first, there is only one leader and every other node is a follower. Followers are obedient and only respond when leaders and candidates ask them to. All client requests are handled by the leader. When a client contacts a follower, the follower directs the customer's communication to the leader. A new leader is chosen using the candidate state method.

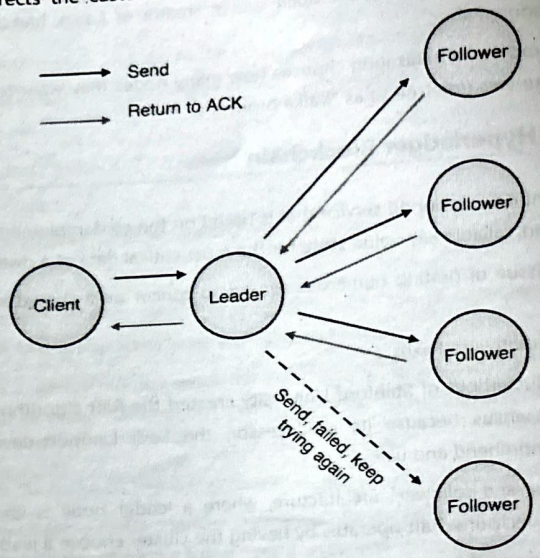


Fig. 4.6.1

- Randomized timer is used to elect the leader in each term. If a leader is not elected in a term, candidates will time out and initiate the election for the next term. Leader candidates log should be most up-to-date compared to log at followers. If a candidate's log is less up-to-date compared to potential follower, then follower rejects the candidate.
- Node begins as a follower and if it does not receive a heartbeat message from the leader within election time then it assumes that the leader is dead. It then takes the candidate state to send out a "RequestVote". If a candidate node gets majority approvals from follower nodes, then it becomes leader.
- Only leaders can append log entries as per client requests. After receiving a request from the client, the leader appends entry to its log. This new entry then sends to all the follower nodes. When the majority of followers confirms this message, the leader commits the message and sends a heartbeat message to clients and followers. This consensus mechanism is used in Quorum for consortium setting.

4.6.1 How does RAFT Work ?

- There is only ever one elected leader for an RAFT cluster
  - which communicates with client directly

- It is in charge of overseeing log replication on the cluster's other servers.
- It governs until it falters or becomes disconnected, at which point a new leader is chosen.

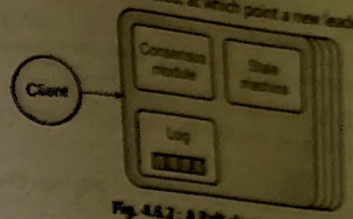


Fig. 4.6.2 : A Raft cluster

- One leader and several followers and all client requests go through the leader.
- A client submits a request.

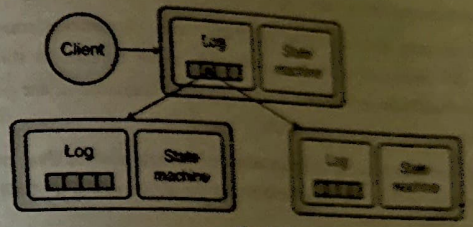


Fig. 4.6.3

- Leader stores requests on its log and forwards it to its followers.
- The followers log the request and record their acceptance of it.

- **Leader Election**

1. The leader updates their state machines by sending "heartbeats" to other nodes so all down terms they are online.

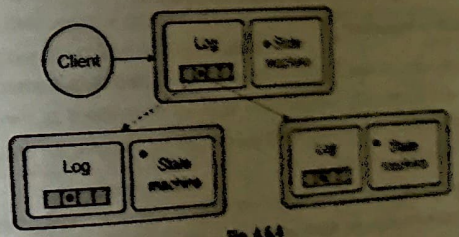


Fig. 4.6.4

2. Other nodes begin an election cycle if they no longer receive a "heartbeat."
3. The followers choose a new leader.
4. The new leader is chosen when the first contender times out.

- **Log Replication**

1. Requests from clients are accepted by Leader which adds them to its log.
2. Leader duplicates its log to other servers to make sure all other nodes have carried out that request.

4.7 Other Challenges : Interoperability and Scalability of Blockchain

4.7.1 Blockchain Scalability

- Scalability - How much scalability is possible without compromising effectiveness? Scalability in this context simply refers to how many transactions the system can process in a unit of time.
- The majority of blockchain platforms still lack adequate scalability. This technique heavily depends on network congestion for transactions.
- As a result, the network will slow down more as more users join it. Although there are solutions on the way, the blockchain is still ill-suited to meet needs in the real world.
- It should be noted that scaling does not necessarily mean a reduction in transaction latency. Indeed, sometimes scalability enhancements come at the expense of higher latency.
- At the moment, Permissionless blockchains based on proof of work can process roughly 10 transactions per second. Blockchains with permissions usually have substantially higher transaction throughputs. The rationale behind this is that individuals in charge, those who approve blockchain transactions, are generally a predetermined group of corporate instances and are known beforehand.
- It is most likely the topic of conversation on Ethereum because it is more obvious than other blockchain network issues. Transaction volumes on Ethereum skyrocketed during the ICO boom and DeFi summer, as would be expected with widespread use.
- Currently, Ethereum can only handle 15 to 30 transactions per second. Slow TPS numbers may cause network congestion due to the rising transaction volume, which will delay transaction completion and result in exorbitant transaction fees.
- The processing capacity of Ethereum is a big problem for applications built on the network because dApps like games or decentralized exchanges demand rapid transaction finality. This is likely why many use cases, like automation or machine learning, haven't achieved adoption on Ethereum.

Why is blockchain scalability important?

- The past few years have seen a huge increase in the popularity of blockchain transactions. As a result, large numbers of people have started using blockchains that might not be equipped to handle the flow. To remain relevant in a market where blockchains and blockchain technologies are emerging left and right, these blockchains must develop intelligent scaling challenges.
- Cryptocurrencies must improve if they are to compete with Visa and Mastercard, two of the world's most popular payment systems. Cryptocurrencies are significantly behind Visa and Mastercard, which purportedly handle thousands of transactions each second. For instance, Ethereum has a cap of 20 transactions per second, but Bitcoin has a cap of 7, Litecoin has a cap of 56, and Bitcoin Cash, according to some, has a cap of three digits. The creators of significant blockchains have proposed a range of strategies to deal with this issue.
- For the purpose of increasing transactions per second, scaling is necessary.

Constraints and factors affecting blockchain scalability

- Transactions volume size
- Block's size

- How many transactions are in a block.
- How frequently blocks are added to the chain.
- How nodes work together in a chain.
- How nodes assemble the chain of transactions.

Standard methods for scaling blockchain

- Off chain computations.
- Side chains.
- State channels.
- Sharding protocols.
- Improved consensus protocols.
- Lightning network.
- Reducing Blocktime or Increasing BlockSize.

State channel approach

- The state channel approach, which applies the same concept to any type of state-altering action often carried out on a blockchain, is the generic form of payment channels.

Sidechain approach

- Using a two-way peg, a sidechain is a separate blockchain that is connected to its parent blockchain. In other words, we are able to transfer assets to the sidechain before returning to the main chain.

Ethereum sharding approach

- Sharding has been used in a range of systems, from commercial database optimization to Google's global spanner database, and is really far older than blockchain technology. Sharding is essentially a specific approach to horizontally splitting data within a database. More generally, the database is divided into tiny chunks known as "shards," which when combined from the original database.

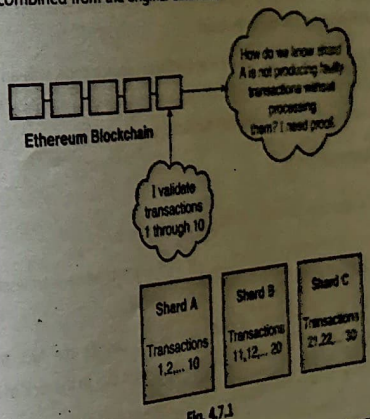


Fig. 4.7.1

Improved consensus protocols

- Enhancing consensus protocols is one of the most frequently suggested solutions for the blockchain scalability issue. Popular blockchain networks like Bitcoin now use the Proof of Work consensus protocol. The Proof of Work consensus process provides trustworthy security, but it is incredibly slow. As a result, the Proof-of-Stake consensus method is seen by many blockchain networks as a viable way to address scalability difficulties. Miners are required to use a lot of computer power to solve cryptographic algorithms in order to use the PoS consensus mechanism. On the contrary, it guarantees consensus by choosing validators based on network stakes. The use of PoS consensus could dramatically increase Ethereum networks' capacity while enhancing security and decentralization.
- **Lightning Network** Another well-known example of an off-chain strategy for blockchain scalability is the Lightning Network. It utilizes private, off-chain channels across the primary blockchain network to take advantage of smart contract capability. Off-chain routes may offer cheaper, faster transactions. Most importantly, Lightning Network lightens the load on the mainchain by rerouting transactions away from it. As a result, users no longer need to pay mining fees or endure lengthy block confirmation delays.

Reducing blocktime or increasing blocksize

- SegWit, a component of Bitcoin's solutions, essentially raises the block size. The block size cap for Bitcoin was introduced a year after it was created. The new 1 MB block size limit wasn't a problem at the time. The network was less active, and neither the size nor the volume of the transactions were sufficient to completely fill the 1 MB blocks.
- However, as the number of Bitcoin users expanded, it became obvious that a 1 MB block size restriction was insufficient to support them. It was suggested to increase block size from 1 MB to 8 MB. The community was unable to come to a consensus, hence the blockchain was forked.
- One segment of the community continued to use the 1 MB blocksize limit of the initial Bitcoin Core blockchain. The block size limit was first raised to 8 MB and then later to 32 MB for those who chose the Bitcoin Cash fork. Bitcoin Cash can handle more transactions at once because blocks are now 32 times bigger. By decreasing block duration, the network throughput can also be increased.
- The Litecoin blockchain, which started out as a clone of the Bitcoin source code, was an example of this. The main distinction is that its block time, which is under 2.5 minutes, is far quicker than Bitcoin's. With a peak throughput of 56 transactions per second as a result, it can process transactions more quickly.

4.7.2 Blockchain Interoperability

Interoperability - Will a blockchain get along with other cryptocurrencies?

- The ability of blockchains to interchange data and use one another's data while seamlessly moving digital assets is known as blockchain interoperability.
- Interoperability is a key flaw in blockchain platform technology. Despite the fact that there are numerous blockchain systems currently in use, they have all been individually built due to the lack of a universal standard.
- Cross-chain communication can streamline many businesses, however the blockchain network is still very far from being fully functional and interoperable.

- Interoperability between blockchain networks refers to the capacity to share, use, and access data without the aid of a middleman or centralized authority. Interoperability issues may make mass adoption nearly impossible.
- Consider having a Yahoo email account and needing to open a new Gmail account in order to communicate information to a Gmail account. If there is no compatibility, then this occurs. A blockchain and interoperability would enable tokenization of an NFT by a dApp allowing an artist to get payment in any cryptocurrency.
- The excellent thing is that over the past year, there have been numerous interoperability projects created to bridge the gap among various blockchains. Several of them attempt to connect other private networks or public blockchains to private networks.

Why is interoperability for blockchains so important?

- The simplicity of data integration and sharing enhances transactions.
- Greater industry-wide cooperation - Blockchain technology is used in almost every business. It can be challenging for businesses operating in different blockchains that are in different industries to communicate with one another and share data. When chains are interconnected within a single network, industries can share information, benefit from one another's strengths, and create a common ecosystem culture. Working in such a connected digital environment could eventually help businesses in developing new goods and services.
- It increases the chances that value chain-based projects, including those in finance and trade, will succeed.
- Transacting with many tokens and across chains is simple.
- Data is more effectively organised as a result of the ease with which it may now flow from one network to another.
- It increases the security and safety of the blockchain network.

How Does Interoperability With Blockchains Work?

- Since each blockchain is unique, new methods of interoperability are required. The lack of third-party integration is what all of the techniques have in common, keeping Web 3.0's status as a decentralized technology. In order to achieve interoperability, the widely used technology cross-chain enables data exchange between DLT designs or external systems. The cross-chain protocol simplifies interoperability across several blockchain networks and allows data sharing across many of them. The cross-chain protocol enables direct user-to-user communication. As a result, blockchains with similar networks can exchange information and value.

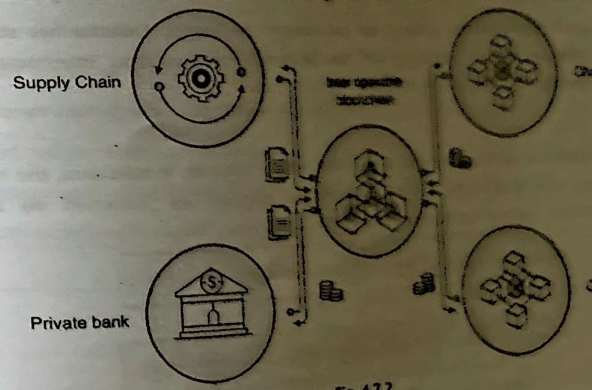


Fig. 4.7.2

- A further method that is frequently used to complete transactions between blockchains is known as an "atomic swap," which is based on peer-to-peer (P2P) cryptocurrency exchanges. Atomic swaps enable cross-blockchain token exchange between two parties. Another common method is a relay, which links two blockchains and enables each blockchain's smart contracts to monitor for activity on the other. Relays allow blockchain networks to stay updated on what's going on on other chains. They work chain-to-chain, allowing a single contract to act as the central client for numerous other nodes over numerous chains without the need for distributed nodes. This enables it to immediately validate particular central headers and the full transaction history. However, the relay approach's security requires a lot of money to operate and maintain.

Constraints and factors affecting blockchain interoperability

- Combining several trust mechanisms
- Transactional bottlenecks

Common approach / solutions/ projects for blockchain interoperability

- Sidechains
- Oracles
- Bridges and swaps
- Blockchain routers
- Open protocols
- Multichain frameworks
- Cosmos
- Polkadot
- Harmony
- Chainlink
- Networks like Polkadot, Cosmos, and Harmony have become well-known examples of how to integrate blockchain technology. Cosmos has been adopted as the ideal option by a number of networks, including Ethereum.
- The Inter Blockchain Communication protocol was just released by Cosmos. Polkadot has started a similar protocol.These protocols facilitate messaging and inter-blockchain communication. Interoperability between several cryptocurrencies is bridged through Harmony.

Sidechains

- Two active blockchains can communicate with one another using a sidechain. In sidechains, the mainchain and sidechain are two distinct blockchains. The mainchain and sidechain are connected via a cross-chain communication protocol, and each maintains a list of assets.

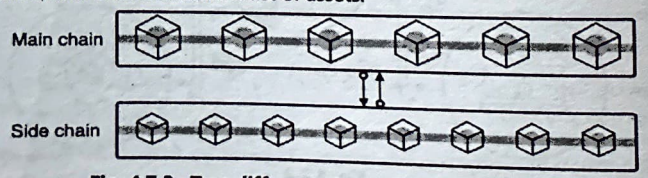


Fig. 4.7.3 : Two different blockchains in sidechains

- Sidechains serve as a two-way connector by having a mechanism for transferring assets between the main chain and sidechain. Examples of blockchain interoperability initiatives include Minieverible, BTC Relay, Pox Network, and RSK.

Oracles

- Oracles bridge the informational gap with the on-chain and off-chain contents in the domain of blockchain technology. By ensuring that various ecosystems relate to a single source of truth, decentralized oracle services like Chainlink assist in guaranteeing that off-chain data is given to blockchain-enabled smart contracts.

Blockchain routers

- Multiple blockchain networks can communicate with one another thanks to blockchain routers. According to the design of the blockchain router, the many blockchain networks, such as Bitcoin, Ethereum, and others, are seen as terminal components known as sub-chains in the routing network.
- Sub-chains cannot directly communicate with one another; only a blockchain router may be used for this. A cross-chain communication protocol, for instance, is used by the blockchain router to allow communication across sub-chains. A blockchain stores all of the data registered on sub chains. The blockchain router enables communication between sub chains and builds a trust bridge across chains.

Review Questions

Q.1 What is Hyperledger? Why it is required?

Q.2 Explain different Hyperledger frameworks.

Q.3 Short note on Hyperledger fabric.

Q.4 Explain the architecture of Hyperledger fabric.

Q.5 Explain the components of Hyperledger fabric.

Q.6 Write a short note on Solo.

Q.7 Write a short note on Kafka.

Q.8 Explain RAFT consensus algorithm.

Q.9 Explain different challenges faced by Blockchain technology.

Q.10 Write a short note on scalability in Blockchain.

Q.11 Explain different approaches of scalability in blockchain.

Q.12 Explain different approaches of interoperability in blockchain.

5

Module - V

Cryptoassets and Cryptocurrencies

Syllabus

ERC20 and ERC721 Tokens, comparison between ERC20 & ERC721, NFT, ICO, STO, Different Crypto currencies

Self-learning Topics: Defi, Metaverse, Types of cryptocurrencies

5.1 Introduction : Cryptoassets and Cryptocurrencies

- Now that we have looked at blockchain and Bitcoin in previous modules, and you have an understanding of how the basic technology works, let's look at the overall cryptocurrency market.
- The phrases "cryptocurrencies" and "crypto-assets" are frequently used interchangeably, which confuses new users and authorities and prevents debate on the assets' future.
- Therefore, we will explore what a crypto-asset is in this section and how it differs from a cryptocurrency.
- One kind of crypto-asset is a cryptocurrency. A crypto-asset is an umbrella term; the key sauce behind most blockchain-based applications.

5.1.1 Cryptoassets

- A crypto-asset is a digital asset that uses peer-to-peer networking, encryption, and a public ledger to control the creation of new units, validate transactions, and safeguard the transactions without any involvement of middlemen
- Using peer-to-peer networking and cryptography, crypto-assets help decentralized businesses, cutting out the middlemen and lowering prices. You often need a crypto-asset to make anything happen, whether you're using the internet of things (IOT), making payments, or sharing files.
- Whatever serves as a value store qualifies as an asset. The ability to store value and convert into cash when necessary is the sole basis for the name "cryptoassets," which are digital assets.
- **A digital representation of wealth that is cryptographically protected is called a crypto asset.**
- There are around 1591 crypto assets. Four categories exist:
  1. Platform tokens/crypto commodities
  2. Utility tokens
  3. Transactional tokens

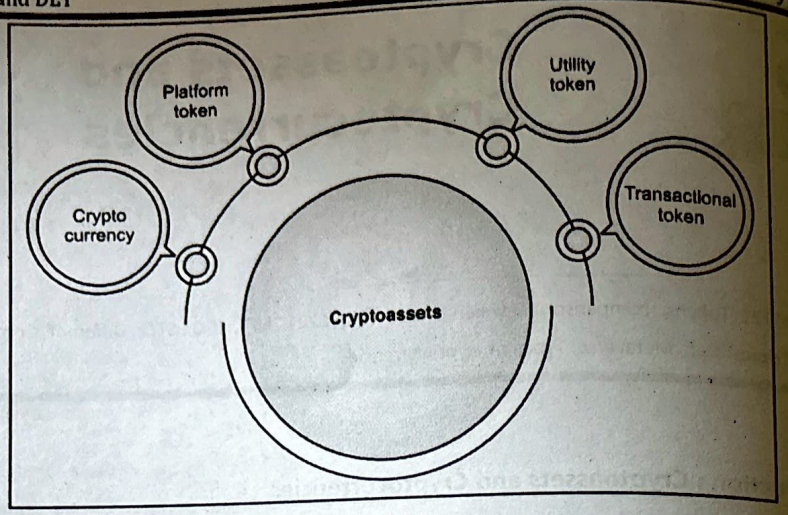


Fig. 5.1.1

5.1.2 Cryptocurrency

The most well-known kind of crypto-asset is a cryptocurrency. Litecoin, Dash, and Bitcoin are among examples. These crypto assets' sole function is to serve as money or digital currency, providing consumers with a more secure and decentralized experience.

What is cryptocurrency ?

- These were developed as a decentralized substitute for fiat money that could be used for international transactions.
- Users may transmit exactly what they want without a third party's participation thanks to cryptocurrency and blockchain technologies.
- Cryptocurrency is a decentralized encrypted digital currency that can be mined, moved between peers, and verified in a public ledger.
- They change in value according to supply and demand, much like conventional fiat currencies.
- It is a money that opposes both systems and financial institutions.
- Its worth is not determined by any established economic metric.
- It is intended to be unaffected by government interference and control.
- It doesn't have a real, concrete existence.
- It is not released by a centralized body.
- It is not subject to any regulations from the market authority.
- A transaction is secret and anonymous; no one can tell who you are, what you bought, or for how much.

Brief History

- The first cryptocurrency, Bitcoin, was introduced in 2008.

- Altcoins first started to surface in 2011.
- 2014 saw a massive altcoin launch.
- The top 5 cryptocurrencies by market capitalization are Ethereum, Bitcoin Cash, Ripple, Litecoin, and Dash.

Benefits of Cryptocurrency

1. Simple to carry
2. simple, quick, and safe
3. Decentralized structure
4. Customer privacy
5. Transparency

Disadvantages of Cryptocurrency

1. Lack of knowledge and understanding
2. Volatility risk

Top 7 Crypto Currencies

- Bitcoin
- Ethereum
- Litecoin
- Peercoin
- Dashcoin
- Namecoin
- Novacoin
- Ripplecoin

5.1.3 Some Important Terms

How are tokens defined ?

- For those who are very unfamiliar with Ethereum, we should define tokens in detail before talking about ERC-20 and ERC-721 tokens.
- Digital assets called tokens are created on a cryptocurrency's blockchain. A token is built on an existing blockchain, as opposed to a coin, which is built on its own original blockchain. Ex. On the Ethereum network, ERC-20 tokens are created.
- A particular asset or utility is represented by a token, which typically sits on top of another blockchain.
- In Ethereum, a custom token of any kind is merely a component of a token "contract." Each token contains a small database that tracks who owns what. This "token" is only an item in the token "contract," and this contract just lists who owns this token.
- **Technically, a token never actually resides in your wallet. Your token is actually just a record in the database of tokens contracts that will read something like, "0xffoaYOURWALLET = 1000 tokens."**

- It resembles a pin code that you enter at an ATM to check the balance of your bank account in a strange way.

Different type of Tokens

1. Equity tokens serve as a representation of a company's shares and equity.
2. Utility tokens: a means of gaining access to goods and services
3. Payment tokens : Tokens for making payments for goods and services
4. Security tokens save personal data to electronically authenticate a person's identity. Ex. DAO.

Table 5.1.1

Coins (Cryptocurrency)	Tokens
Native to its own blockchain technology, or built onto a blockchain	Built on top of an existing blockchain
Mining is the main method of distribution	Primarily distributed through ICOs
It takes a great amount of time and effort to create.	It is comparatively simple to make
It is used to store or transfer money	It is valid with one merchant

1. Fungible Vs Non-Fungible Assets

- An asset that can be exchanged for another one, much like money can, is fungible.
- This can be better understood by thinking about money. The value of one Indian rupee is the same as the next. It makes no difference which you have because they are all equal in terms of worth, value, and purpose. Where those rupees came from or may ultimately go is irrelevant to the individual using them or the person receiving them.
- Similar to this is how shares of corporations work. For example, if you were to purchase 500 shares of TCS, you wouldn't care which 500 shares you received as long as you got 500 shares of TCS. These don't have any nitpicky characteristics or specifications to pick from.
- However, a non-fungible asset is not the same as its equivalents. Due to their uniqueness, non-fungible tokens (sometimes referred to as NFTs) are digital assets that are difficult to trade for other assets. Any form of collectible is the most observable example of a non-fungible asset. Consider a piece of art that has special meaning for the owner and would be challenging to swap for another piece of art because of the discrepancy in their perceived valuations.
- In contrast, a non-fungible asset is one that cannot be exchanged for another asset because no two assets are alike and do not have the same values.
- Similar to exchanging a fruit for a puppy because they are not the same and do not have the same value, trying to exchange non-fungible assets in the same way as fungible assets is absurd.
- Your home or car are two examples of non-fungible assets you could encounter on a daily basis. After a long day at work, you wouldn't want your neighbour to say, "Hello, I've switched your house for mine, and your automobile for mine too. Have a good day, and here are the keys! "
- Even if they are the same make and model, two houses and two cars do not have the same values since they have different histories and owners. Such assets are similar to non-fungible assets.

2. Platform tokens / Crypto commodities

- For the purpose of serving as a platform for the growth of other decentralized projects, platform tokens were developed.
- Ethereum is the biggest platform token. NEO and EOS are two more instances.
- A hardware and software foundation for the creation of decentralized applications is provided by Ethereum's decentralized platform (dApps).
- With the advent of smart contracts, new projects can now be created on the Ethereum platform and create their own self-executing smart contracts on the blockchain. The Ethereum platform allows new projects to create their own ERC20 tokens.

3. Utility / Protocol Tokens

- ERC20 tokens created on the Ethereum network are typically utility tokens (or occasionally protocol tokens).
- OmiseGO, Filecoin, Bancor, and BAX are a few examples.
- These tokens are typically made specifically for the project issuing them, with a specific goal in mind.
- They can be traded in for particular products and services like distributed storage, in-app money, or more practical uses.
- The projected usage of these tokens in the project for which they were developed typically determines their value.

4. Transactional Tokens

These crypto-assets are less prevalent. Ripple, IOTA, and Stellar are a few examples. Fast cross-border payments are made possible by transactional tokens, which also provide process transparency. These are typically blockchain-based tokens like Ripple, but they can also include internet of things tokens like IOTA.

5.2 ERC20 and ERC721 Tokens

- Before the introduction of the token standard, blockchain developers frequently designed tokens based on personal preferences, which made it difficult for token ecosystems to communicate with one another and restricted interoperability.
- ERCs (Ethereum Request for Comments) and EIPs (Ethereum Improvement Proposals) were developed by Ethereum developers to address this issue. These help in outlining the guidelines and necessary operations for tokens produced on the Ethereum blockchain, greatly facilitating integrations and interactions.
- Programmers of smart contracts use the Ethereum blockchain platform to create standardized documents known as ERCs. These documents lay out the guidelines that coins based on Ethereum must follow.
- ERC-20 is now the most popular standard for Ethereum tokens, however there are also ERC-223, ERC-721, and ERC-777 standards.

5.2.1 ERC20 (Fungible Tokens)

- The Ethereum blockchain's first token standard, ERC-20, makes it possible to create fungible tokens.
- Febian Vogelstellar developed the ERC-20 standard back in 2015.

- All tokens built on the Ethereum platform should adhere to ERCs, which are programming standards or rules.
- Within the crypto community, it is the most popular and well-known standard.
- Each ERC20 token can be used with any other. For instance, fungible tokens stand for assets like fiat money, an ounce, and ICOs that can have their value substituted with something else of equal or greater worth.
- The main advantage is that a token may be interacted with in a standard way by any application or other smart contract without the need to know specifics about the token.
- Start-ups in particular are benefiting from the ERC-20 token. Millions of dollars are successfully raised by several firms through token sales.
- ERC 20 contracts have millions of tokens and these get distributed to owners. You can own multiple tokens and all the tokens have the same value.
- It is a standard protocol just like HTTP. It regulates the tokenization and ensures that the technical specifications of the tokens are met. If a token does not meet regularity, it won't be called ERC20 token.
- The following digital assets might theoretically be represented by an ERC-20 token:
  - financial resources in the real world, such as stock in a corporation, dividends on shares, etc.
  - Tickets for a web-based game or scheme.
  - points earned through online gaming.
- A smart contract's ability to create fungible tokens is defined by the ERC-20 protocol. Its primary techniques include :

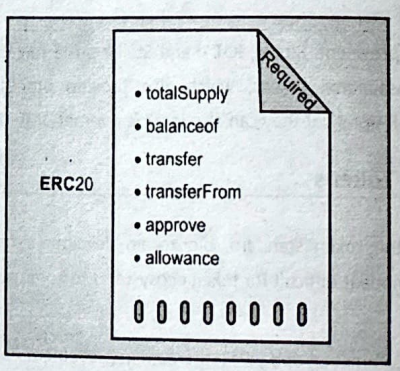


Fig. 5.2.1

  - name( ) (optional) : The name of the token.
  - Symbol( ) (optional) : The symbol of the token. With the symbol component , users could find the ticker symbol for the token.
  - decimals( )(optional): The decimal places of the token. This allows for fungibility.
  - totalSupply(): The total number of existing tokens.
  - balanceOf(): The total number of tokens owned by a particular account.
  - transfer(): Moves a number of tokens from the caller's account to a specified address.
  - transferFrom(): Same as transfer(), but it also specifies the address to move tokens from.

  - allowance(): The number of tokens a spender is allowed to spend on behalf of the owner via transferFrom().
  - approve(): Sets the number of tokens a spender is allowed to spend.
  - With the exception of the first three labeled (optional), which enhance usability, all of these techniques are strictly necessary in an ERC-20 smart contract.
  - Additionally, an ERC-20 contains two events: Transfer (which is triggered whenever tokens are transferred) and Approved (which is triggered if the approve() method is successfully called).

5.2.2 ERC 721

- Non-Fungible Tokens, or NFTs, are the common names for ERC-721 tokens.
- NFTs, also known as non-fungible tokens, are becoming more and more popular. From digital content tokenization to a physical asset
- Nastassia Sachs, Dieter Shirley, and William Entriken developed the ERC-721 standard.
- ERC 721 contracts are similar to ERC 20 contracts, you can still generate as many tokens as you want and distribute these and you can own multiple tokens.
- Difference is that ERC 721 tokens have extra functions and contain metadata. These are called smart contracts because of this each token can have unique properties making each token unique and you can't exchange one token for another because none are exactly the same.
- NFTs give programmers the ability to tokenize ownership of any type of data in any format.
- As a result, it became clear what could be a token on a blockchain.
- ERC-721 has its own set of standards, just like the ERC-20 Standard.
- ERC-721 signifies:
  - a special piece of digital content.
  - stuff from social media, such as Reels, Tweets, and images.
  - Collect ibles and gaming equipment.
  - video game characters.
- Typical ERC-721 smart contract mechanisms include:
  - balanceOf(): The number of tokens in the owner's account.
  - ownerOf(): The tokenId of the owner.
  - safeTransferFrom(): Safely transfers tokens from the owner's address to the recipient's. The tokenId must be specified as a parameter.
  - transferFrom(): Same function as safeTransferFrom(), but generally not recommended.
  - approve(): Allows an address to transfer a token identified by its tokenId, into another account. It triggers the Approval event.
  - setApprovalForAll(): Allows an operator to call safeTransferFrom or transferFrom for any token owned by the caller.
  - getApproved(): Gets the approved account for a specific tokenId.

- isApprovedForAll(): Checks if an operator is allowed to manage all the assets of the owner.

Additionally, it includes events such as Transfer (which occurs whenever ownership of any NFT changes) and Approval (which activates when the approved address for an NFT is changed).

5.3 Comparison between ERC20 and ERC721

Table 5.3.1

Criteria	ERC20	ERC721
Fungibility	Fungible in nature	Non-Fungible in nature
Token Identity	The various tokens do not differ much from one another.	Each token has a distinct identity and is distinguishable from the others.
Collecting Tokens	Tokens issued by ERC-20 are not collectible.	ERC-721 tokens are a collectible similar to fiat money.
Can Transfer	Value exchange between users	Rights transfer
Adoption	Commonly adopted	Acceptance levels are limited.
Value fluctuation	ERC-20 tokens continue to have the same value.	Depending on their rarity and uniqueness, ERC-721 tokens' value changes.
Divisibility	can be divided and divided in various ways; even 0.1% of the token can be shared.	ERC-721 tokens cannot be divided.
Ownership functions	There are no designated specific ownership functions.	Special ownership features may be made available via ERC 721 tokens.
Recovery	No mechanism for recovery	A recovery mechanism is put in place. If the address is fake, go back to your wallet.
Examples	Binance Coin, Dogecoin, Dai, OmiseGo, Maker	Decentraland, Crypto Kitties, Ethermon

5.4 NFT

We will discuss NFT in this section, including what they are, how they connect to cryptocurrencies, and other financial-related topics.

5.4.1 What does an NFT Mean?

- A Non-Fungible Token (NFT) is a type of digital acid that simulates actual things from the real world, including artwork, music, in-game objects, and films.
- They are traded online, frequently with the aid of cryptocurrencies, and are typically encrypted using the same programmes as many other cryptocurrencies.

- Relationship between NFTs and cryptos
  - Except for one commonality, NFTs and cryptocurrency tokens are distinct. They are comparable because they were all created using the same type of programming, which is cryptography.
  - Regarding fungibility, NFTs and cryptos differ from one another. The fungibility is the only difference, then.
  - While cryptocurrencies as traditional currency are fungible, NFTs are not.
  - Fungibility is the capacity to trade one thing for another.
- Most of the time, NFT can be considered one of the most distinctive characteristics that sets them apart from all other tokens. Since each token is unique, no two users can exchange or trade them at the same rate or break them up into smaller parts like money because of this.
- NFTs are a category of digital tokens where each token is distinct and possesses special qualities.
- The most popular token standard currently used by NFT is the Ethereum token standard. Typically, a variety of NFTs are made using the ERC-721 and ERC-1155 token standards.
- EOS, FLOW, Tezos, and other cryptocurrencies offer a particular token standard for creating NFTs in addition to Ethereum.
- NFTs can help digital artists or any type of artist in preventing plagiarism by tokenizing their work and making it impossible to copy.
- There is no way to delete or change the ownership of any NFTs because they are all recorded on the blockchain network, which has an immutable ledger.
- When compared to other cryptocurrencies like Ethereum or Bitcoin, NFTs are more versatile and Physical items or collectibles can be lost, broken, or destroyed by users, while NFTs cannot be taken or destroyed. Once a user acquires ownership, they have permanent ownership.
- NFTs are impossible to duplicate and thus third parties cannot misuse an artist's intellectual property.
- CryptoPunks, Axie Infinity, Decentraland, and Open Sea are well-known NFT initiatives.
- Users can buy and trade NFTs on a variety of NFT platforms, including OpenSea, Mintable, and Nifty Gateway.

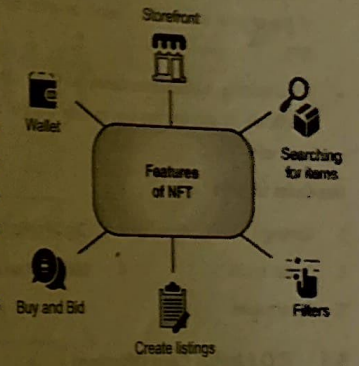


Fig. 5.4.1

5.4.2 Attributes of NFTs

- **Uniqueness :** NFTs are distinct since no two NFTs are alike and they cannot be used interchangeably. Each NFT's metadata is an unchangeable record that serves as its certificate of authenticity.
- **Ownership :** NFTs are stored in an associated account on a DLT. The original developers of the NFT have the private key to the account where the NFT is stored, and they are free to transfer the NFT to any other account.
- **Transparency :** Since public distributed ledgers are decentralized and irreversible, where records of token issuance, transfer, and activity can be publicly confirmed, buyers may trust and confirm the legitimacy of a specific NFT.

- **Indivisibility :** As far as their utility is concerned, NFTs have always been indivisible. For instance, since only one person can use the seat, an airline ticket cannot be purchased in part; someone must pay the whole price.
- **Scarcity :** NFTs can be difficult to obtain by, which contributes to their value. Although developers are free to produce as many assets as they want, they also have the option of setting a cap on the number of NFT to create a sense of scarcity.
- **Easily Transferable :** NFTs are only used when they are unique, and they are only bought and traded in specific markets.
- **Indestructible :** The fact that the non-fungible tokens are controlled and operated via blockchain raises the security level for them. This establishes that these NFTs cannot under any circumstances be removed or destroyed.

5.4.3 How Does it Work ?

- It's vital to remember that neither the blockchain nor the NFT include any storage for the actual artwork.
- Just its characteristics, such as the file's fingerprint or hash, a token's name and symbol, and if available, a link to an IPFS-hosted file. Large data may be stored and shared effectively using IPFS, a file sharing technology. It uses cryptographic hashes, which are conveniently stored on a blockchain.
- The creator of the NFT still holds the copyright and reproduction rights, but the token owner is the rightful owner of the original artwork. As a result, an artist can continue to sell prints together with his original works of art as NFTs.
- By submitting a blockchain transaction, you can now sell it. This data can never be altered with thanks to the blockchain. It also enables you to keep track of a token's correct owner and the price at which it has previously been sold.

Use Cases of NFTs

1. Gaming
2. Digital collectible
3. Digital assets
4. Identification and certification
5. Social tokens

5.5 ICO (Initial Coin Offering)

- Initial Coin Offering (ICO) is crypto- equivalent of the IPO (Initial Public Offering)
- The purpose is to raise capital, where digital proprietary tokens are sold.
- A company conducts an initial coin offering (ICO) when it sells tokenized cryptographic assets to raise money for its operations.
- If the initiative is successful, those who purchase the tokens early will save money because they are essential to the project. Until the amount of money they need to raise is met, the firm often opens the sale of tokens for a brief period of time.
- It is a source of funding for new businesses. ICOs are startup companies' efforts to generate money through crowdfunding. The startup's own coin provides the incentive for participating in these crowdsourcing efforts.
- To investors or speculators, a certain amount of cryptocurrency is offered in the form of tokens.

- Through cryptocurrency exchanges, tokens are listed.
- MasterCoin, which was released in 2012, was the first ICO.
- In 2014, Ethereum held a token sale to raise money. In the first 12 hours, it raised 3,700 BTC, or about $2.3 million at the time.
- Since ICOs are largely unregulated, investors must be extremely cautious and diligent while learning about and making investments in them.

Major Parties In ICOs

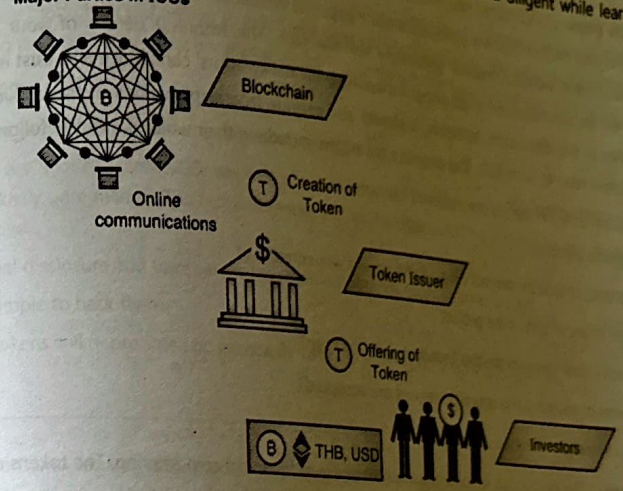


Fig. 5.5.1

Phases of ICO

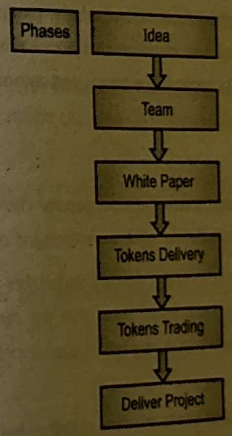


Fig. 5.5.2

1. **Idea :** It should be obvious that the team and company's first crucial step is to comprehend how blockchain technology will work in the business world and what specifically they intend to provide customers and investors using the technology. The business chooses the recipients of its fundraising effort and develops the necessary information about the business or project for possible investors.

2. **Team :** Building a talented staff throughout ICO development is a self-explanatory necessity. The founders can only go as far as the team will allow them to: someone needs to create the product, and other team members will handle marketing, community support, etc. In addition to the core staff, companies require advisers. One of the advisors should ideally be a lawyer with some background in ICO support. If not, hire a contract securities lawyer to make sure you are adhering to KYC and AML regulations.

3. **Create White paper :** In consideration of securities laws, investors will write white papers. Along with organizing the ICO, the crypto project typically produces a white paper, or pitchbook, which it makes accessible to interested investors via a new website created specifically for the coin. The technical details of your cryptocurrency technology will be presented in a white paper. Increasing potential investors' confidence and trust is, of course, the main objective of this document. However, it should also provide legal explanations of the applicable securities laws and related rules to your ICO. The project's promoters include in their white paper the following significant information regarding the ICO:

   - The project's objective
   - The prerequisite that the project would fulfill once it was completed
   - Estimated financial cost of the project
   - How much virtual currency are the founders going to keep?
   - What forms of payment and which currencies are accepted?
   - The ICO campaign's duration

4. **Tokens delivery :** The production of tokens is the next phase of the initial coin offering. The tokens are essentially digital representations of assets or services on the blockchain. These blockchain platforms are used to create the tokens. Because a business does not have to write the code from the start as is necessary to create new coins, the process of creating tokens is rather straightforward. Instead, the production of the tokens is possible with only small code alterations on existing blockchain platforms that power existing cryptocurrencies like Ethereum. You must create a smart contract in order to generate the tokens and automate the token distribution procedure. The ERC-20 token is the industry standard.

5. **Tokens trading**

   - The Ethereum blockchain technology is now the most popular choice for ICO launches since it offers smart contracts, the key mechanism for automating token generation and distribution.
   - In order to bring in new investors, a company typically undertakes a promotion campaign concurrently. To reach the broadest investor base, it should be noted that the campaigns are frequently run online. The advertising of ICOs is now prohibited on a number of sizable online platforms, including Facebook and Google.

6. **Execute project :** The tokens are made available to investors after they have been created. Multiple rounds may be used to structure the offering. The company can then utilize the funds raised from the ICO to provide a new good or service, and investors can either anticipate using their token purchases to gain access to these goods and services now, or they can wait for the value of their tokens to increase.

Advantages of ICO

1. It is relatively inexpensive and simple for businesses to start practically globally.

2. Typically, obtaining regulatory permissions is simple.
3. Token owners may remain anonymous.
4. Tokens can be traded on both controlled and decentralized exchanges.
5. High liquidity: An asset is said to have high liquidity if it can be bought or sold quickly on the market without materially altering its value.
6. Less paperwork is required : Traditional assets like initial public offerings (IPOs), stocks, bonds, and other exchange forms are dependent on numerous regulatory filings, which can take time and effort. The fact that ICOs use blockchain technology to maintain a ledger of their numerous transactions is what makes them more alluring than IPOs and other traditional assets. This enables the instantaneous updating of data.

Disadvantages of ICO

1. In most jurisdictions, there is no investor protection
2. There are a lot of scams : ICOs are frauds, and uninformed investors are the victims of this fraud because they are mostly unregulated. The fact that money lost to the scam won't be reimbursed and is possibly its biggest drawback.
3. Normal disclosure and transparency requirements do not apply to token issuers.
4. It is simple to hack them.
5. The tokens will depreciate and eventually lose all of their value if the ICO project fails.

5.6 STO

- Utility tokens and security tokens are the two categories under which tokens fall.
- Tokens that guarantee future use of a good or service are known as utility tokens. They serve a purpose and are not intended to be investments. A Starbucks gift card is an example. You are not really expecting to make money when you sell the gift card if you purchase it at a discount. In essence, you have paid in advance and anticipate drinking coffee at a later time.
- Security tokens are tokens that stand in for tradable financial assets, such as a company's stock or bond. Security tokens are designed as an investment option; they provide dividend payments, profit sharing, or interest payments that imply potential future earnings.

Security tokens and utility tokens both make profit-related promises.

5.6.1 Why Security Tokens ?

- Back then, there were a lot of scams and manipulations because the ICO industry was essentially unregulated. When everyone else had purchased a certain token, investors artificially inflated its price before selling off all of their shares. Other instances involved businesses that, when the ICO finished and the money was raised, simply disappeared, taking the money with them.
- According to a recent analysis, ICOs held in 2017 were 80% frauds. Nobody seeks authorization to conduct an ICO. All that is required is the setup of a website, some tokens, and the beginning of general public sales. Public outcry grew as things became out of control. Regulators then sought to look into whether these alleged tokens should actually be classified as securities.
- Security Token Offering can help in this situation.

- Security Financial securities that adhere to SEC requirements include tokens or digital assets. They offer a wide range of financial rights to investors, including equity, dividends, profit-sharing, buy-back rights, and much more.
- The underlying coins are traded on the blockchain, and the smart contract contains all the rights.

5.6.2 Security Token Offerings (STO)

- A sector that wants to raise money will issue a security token offering (STO).
- Similar to an ICO, a security token offering (STO) issued digital tokens that were connected to actual assets like corporate shares or real estate investment trusts (REIT). As a result, they are considered investment contracts and are subject to current securities laws.
- The key benefit is that security tokens are supported by trustworthy resources and are subject to control and regulation under current security legislation.
- STOs are more secure than ICOs since the SEC only approves projects that are legitimate and sincere in their goals.
- It benefits the blockchain project to comply with governmental regulations and may even put an end to the fight between the blockchain and regulators.

How to offer a Security Token ?

- You must register a security with the SEC if you wish to issue it. It is a difficult and costly procedure designed for established businesses.

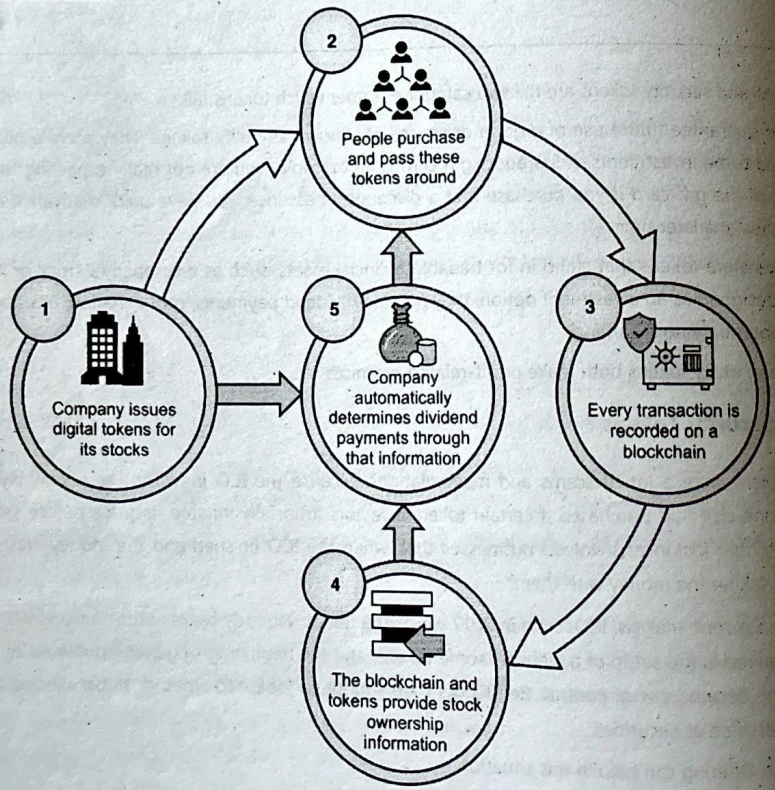


Fig. 5.6.1

Advantages of STO

1. Offerings of security tokens are governed internationally.
2. Regulations cut down on fraud.
3. Trades in STOs take place on trusted exchanges.
4. Tokens are supported by movable property, money rights, equity, or debt.
5. Investors have access to larger markets thanks to STOs because practically any asset class can be tokenized.
6. From the perspective of the fundraiser, a larger investor base can be attracted because digital assets are simple to advertise and transfer across borders.
7. Cheaper option for firms than an IPO
8. Without a broker, investors can exchange security tokens among themselves.

Disadvantages of STO

1. STO only makes the investment available to accredited investors.
2. Many investors and businesses choose not to participate in STOs because of the lock up time and the cost of compliance.
3. Better suited for investors that are digital natives.

Table 5.6.1

ICO	STO
The issuer will manage the token sale.	The security token issuer handles the fundraising.
Startups, public enterprises, and SMEs are issuers.	Issuers include huge corporations, SMEs, startups, and public companies.
There are issues with trust because some token issuers provide false information.	high levels of trust due to the tokens' inherent value
Project teams handle all of the marketing and advertising	The project's crew handles the marketing and advertising.
Investors bear all of the risk.	Fully compliant and regulated
There is no need for a legal or regulatory structure.	Regulations that are complicated and regulated by KYC/AML checks
extremely unsafe because transactions take place on ICO project websites that might not have the necessary security safeguards.	Being controlled by US SEC rules makes the coin extremely secure.
High risk and little investor protection.	Each token is a security that safeguards investors' rights.
Coins are listed on standard cryptocurrency exchanges.	Specialized security token exchanges and platforms list tokens.
Investors are completely anonymous.	Investor-friendly transparency
Launch costs are low.	the average cost of launch

ICO	STO
Low liquidity	Average liquidity exists.
Useful token	backed-by-real-world assets tokens
To purchase and store tokens, you must have a crypto wallet.	Users don't have to give up ownership and control of the business.
Whitepaper is published	Offering memorandum

5.7 Different Crypto Currencies

- A form of digital or virtual money used for transactions is called a cryptocurrency.
- With the exception of the fact that it uses encryption rather than having a physical form, it resembles actual money quite a deal.
- There are already more than a thousand distinct cryptocurrencies available worldwide.
- 18000 different cryptocurrencies with a $2 trillion market cap as of March 2022.
- Among cryptocurrencies, Bitcoin and Altcoins are the two most popular types.
- The original currency is bitcoin. Several more cryptocurrencies were developed after Bitcoin. All of these cryptocurrencies are referred to as altcoins (alternet coins).

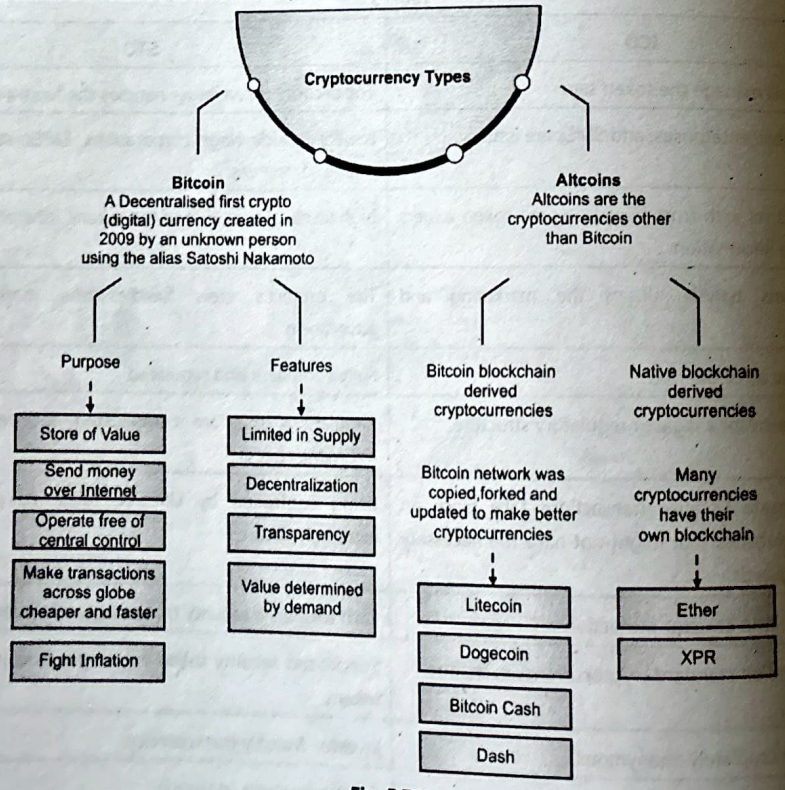


Fig. 5.7.1

Table 5.7.1 : Main Cryptocurrencies

Crypto-Currency	Symbol	Logo	Date of Release	Programming Language
Bitcoin	BTC XBT, ₿		2008	C++
Ethereum	ETH		2015	C++, Go
Ripple	XRP		2013	C++
Litecoin	LTC		2011	C++
Monero	XMR		2014	C++
Dash	NEO		2014	C++
Zcash	ZEC		2016	C++
Petro	XPD		2018	C++
Namecoin	NMC		2011	C++
Swiftcoin	STC		2011	
Bytecoin	BCN		2012	
Peercoin	PPC		2012	C++
Stellar	XLM		2014	C, C++

Fig. 5.7.2

Example

1. Bitcoin

- It functions as an electronic payment system and a cryptocurrency.
- Satoshi Nakamoto founded the company in 2008.
- It is first decentralized payment network
- It is a peer-to-peer system.
- The market value of bitcoin is $331 billion.
- 1 BTC = $17,238

2. Ethereum

- By market capitalization, Ethereum, which launched in 2015, is the second-largest cryptocurrency behind Bitcoin.
- It enables programmers to create and execute a wide range of applications.
- Ethereum was split into Ethereum (ETH) and Ethereum Classic (ETC)
- The market value of Ethereum is $157 billion.

- 1 ETH = $1287

3. Solana

- A public blockchain network called Solana features smart contract functionality.
- A blockchain platform called Solana is intended to run scalable, decentralized apps. Solana offers a higher transaction throughput and lower transaction costs when compared to other blockchains like Ethereum.
- Its native cryptocurrency is SOL.
- The market capitalization of Solana is $11.98 billion.
- 1 ETH = $13

4. Litecoin

- Litecoin (LTC), which launched in October 2011 and was inspired by Bitcoin, was one of the first altcoins.
- Peer-to-peer cryptocurrency Litecoin (LTC) was founded in 2011 by Charlie Lee, a former Google employee.
- Based on Bitcoin's original source code and has many similarities to bitcoin.
- Litecoin was created to be more practical for daily use and to be utilised for less expensive transactions.
- The market capitalization of Litecoin is US$3.4 billion.
- 1 LTC= $78.11 USD

5. Ripple

- Major banks and financial service companies use the worldwide payments network Ripple.
- In order to facilitate quick currency conversion between various currencies, Ripple developed the cryptocurrency known as XRP. XRP is used in Ripple products.
- The market capitalization of Ripple is US$17 billion.
- 1 XRP= $0.39 USD

Review Questions

Q.1 Define and explain cryptoassets.

Q.2 Explain the term cryptocurrency in detail.

Q.3 Explain cryptocurrency, token and differentiate between cryptocurrency and tokens.

Q.4 What is fungible and non-fungible tokens.

Q.5 Short note on ERC20 tokens.

Q.6 Short note on ERC 721 tokens.

Q.7 Differentiate between ERC20 and ERC721.

Q.8 Explain NFT in detail.

Q.9 Write a short note on Initial Coin Offerings (ICO)

Q.10 Write a short note on Security tokens (STO)

Q.11 Compare and differentiate ICO and STO.

Q.12 Explain different cryptocurrencies available in market.

□□□

6 Blockchain Applications and Case Studies

UNIT - VI

Syllabus

Blockchain in IoT, AI, Cyber Security

Self-learning Topics : Applications of Blockchain in various domains Education, Energy, Healthcare, real estate, logistics, supply chain

6.1 Blockchain in IoT

IOT is an Internet of things, these are devices which are very portable. It is also very small and thus interconnected device one such as Wi-Fi security is a bit concern.

Issues in traditional usage of IOT

- Single point of IOT intelligence and access is compromised.
- Data may be incomplete, misleading and inaccurate.
- Data privacy may be compromised.

For a variety of IOT transactions, the blockchain serves as a distributed transaction ledger.

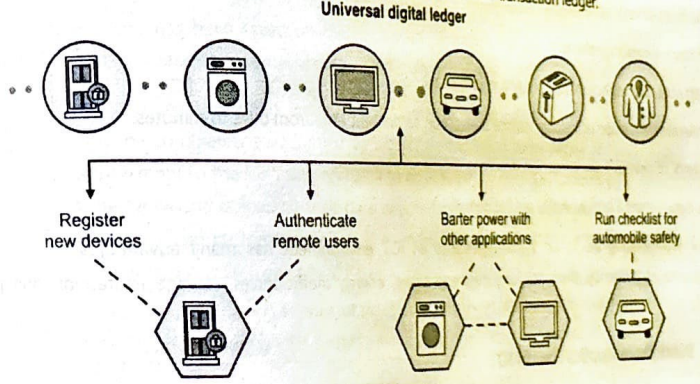


Fig. 6.1.1

- The centralized components of IoT systems can be replaced by a blockchain. A smart contract can be utilized whenever data needs to be moved from one location to another. For instance, a smartphone app allows the user to communicate directly with the blockchain while installing an IoT device. The IoT network and the blockchain are directly interconnected.
- According to the type of IoT device and its background functionalities, cloud storage may be required because the quantity of data that can be saved on the blockchain is constrained. Data can be stored via hybrid ways while still benefiting from the blockchain's security features.

- In a conventional, centralized IoT system, a server would house the application logic. This server becomes a single point of failure when IoT devices communicate with it. All of the IoT devices would be impacted if this point were to malfunction or become compromised.
- The application functionality would reside in the smart contracts managed by the network peers in a decentralized Internet of Things (IOT) architecture. If one peer goes down, it won't affect the IoT devices, eliminating the single point of failure problem.
- If a decentralized P2P ecosystem is required for an IoT application, blockchain can address privacy and security concerns.
- Attack routes aiming at the application servers will be eliminated by the security of an IoT network with a blockchain. Additionally, it would guarantee the integrity and secrecy of data transfer procedures including device management and file transfers. All transactions would be encrypted with public keys, allowing only the legitimate recipient node to decipher the data. Beyond a single point of failure system, the blockchain service's availability has also been improved.
- If an IoT application needs to maintain the payment process for its offered services outside the control of third parties, blockchain may be a promising secure option.
- The blockchain can be one of the best choices if IoT applications need to keep logs and traceability of sequential transactions.

6.1.1 Blockchain's Advantages in IoT

1. Secured transactions, reduced tampering and frauds
2. Build trust among stakeholders
3. Introduce traceability of data
4. Smart contracts replace middleman and intermediary
5. Accelerate transaction processing: reduce transaction settlement time from days to minutes.
6. Network of devices make consensus decisions.
7. Raw data is shared and anomalies are flagged.
8. While incorporating blockchain technologies into an IOT environment has many advantages, there are also disadvantages. Presently, there are long overhead times, energy inefficiencies, storage limitations, and privacy issues.

6.1.2 Blockchain Applications in IOT

- In blockchain-supported smart-IoT systems, protocols for behavior collection and verification were proposed. To protect IoT devices from fraudulent attack, blockchain was implemented in the IoT behavior controller system to store, track, and identify IoT devices.
- To address recent issues with the present centralized security network architecture and defend against potential future attacks on smart homes, a blockchain-based smart house utilizing Gateway network architecture and IOT was proposed.

Table 6.1.1

Industry	Use cases of IOT + Blockchain	IOT data
Logistics	Track, observe, and report on the status and placement of containers will be easy with blockchain. Improve the way cargo are packed and moved across shipping routes.	Location Temperature Handling Carrier GPS
Finance	Make it possible for connected devices to contribute sensor readings to pay for usage using pay-per-use models.	Items consumed Location visited Usage of device
Automotive	Vehicle warranty and service records, documentation of completed repairs, and records of parts put into cars.	Parts inventory Service performed
Smart Homes	Remote control of the home security system from a smartphone is made possible by IoT blockchain. Blockchain technology and biometric security have been integrated by the system to ensure that no one can tamper with the data collected from smart devices. For increased security, sensitive user data is kept on the blockchain, including: • Biometrics • Recognition of voice • facial identification Data that has been saved on the blockchain cannot be changed after that point, and only the appropriate individual is allowed access.	Biometric, voice, face
Agriculture	The food manufacturing industry, from farms to supermarkets to homes, might be completely transformed by blockchain and IoT. A larger degree of improvement to the food supply chain can be achieved by placing IoT sensors in the farms and uploading their data directly to the blockchain Distributors, merchants, and customers can use it to make educated judgements about purchasing a certain crop or food item. In order to avoid having to wait for payment after harvest, producers can also presell products through the system's marketplace using smart contracts.	Soil quality Crop quality
Pharmacy Industry	Every day that goes by, the problem of fake medications in the pharmaceutical industry gets worse. The pharmacy sector is accountable for: • Developing drugs • The production of medications • Drug distribution • Consequently, it is challenging to trace the full route of medications. The transparency and traceability of blockchain technology makes it possible to track drug shipments from their point of origin to their final destination.	Drug unique ID or QR code Drug's combination Location Price

6.1.3 Blockchain-enabled IOT: Case Studies

Several industries are testing blockchain. And occasionally, we observe that there is an industry-specific connection between blockchain and IoT in particular sectors.

- **Smart Parking :** Urbanization and population growth one of the biggest problems facing government agencies around the world is parking. People wasted time and gas driving great distances in search of a parking space. With the help of blockchain and IOT, a system can provide parking solutions that cover all aspects of the problem.
- **Smart Logistics Services :** Trade, Logistics and Shipping. Currently, a wide range of stakeholders are involved in freight logistics, including manufacturers, forwarders, shippers, custom agents, and insurers. The majority of these parties track shipments using various technologies. With varying objectives, there are numerous interested and dependent parties, including shipper, insurance, and manufacturer. Use a shared ledger that is blockchain-enabled IOT to track the movement of shipping containers.
- **Blockchain and IoT in Insurance :** Smart contracts and the improvement of a number of procedures, including claims management, are the primary uses of blockchain in the insurance industry.
- **Supply chain :** IoT is applicable to supply chains. The global supply chain involves numerous participants in numerous locations. Pharmaceuticals and food suppliers are two examples. Blockchain and IoT can be combined to improve all supply chains.

6.2 Blockchain in AI

- Two of the trendiest technological topics nowadays are blockchain and artificial intelligence. Researchers have been talking about and investigating the pairing of the two technologies despite the fact that their respective uses and developing parties are very different.
- A blockchain is a distributed, decentralized, unchangeable ledger that is used to store encrypted data, per definition. On the other hand, AI is the tool or the brain that will make it possible to analyze the data gathered and make decisions based on it.
- Without a doubt, each technology has a unique level of complexity, but both blockchain and AI are in situations where they may complement and support one another.
- Combining these two technologies makes sense since they can each influence and act upon data in distinct ways, and doing so can increase data exploitation to new heights.
- The basic architecture of blockchain may be improved, and the potential of AI can be increased, by incorporating machine learning and AI into it.

6.2.1 How is AI helped by Blockchain?

- While data science or big data includes making predictions from vast volumes of data, blockchain is focused on confirming data.
- stopping harmful activity
- Making predictions
- Blockchain makes analyses of data in real time very efficiently.

- Blockchain also could help AI become more clear and understandable and allow us to track and understand the motivations behind machine learning judgements.
- Blockchain and its ledger can capture all the information and factors that go into a machine learning conclusion.

6.2.2 Blockchain Applications in AI

1. Data protection
2. Data Monetization
3. Supply chain transparency
4. Creating diverse data sets
5. Smart computing power
6. Cryptocurrency analysis

6.2.3 Blockchain-enabled AI : Case Studies

1. We can examine cryptocurrency trends using AI technologies for individualized investment goals. To assist users in making investing decisions, the system examines the data of more than 6,000 coins and collects market insights and updates. Large organizations like Coinbase, Amazon, and Facebook have all made use of this service.
2. Increasing efficiency of supply chains and transparency in the coffee, lumber, fisheries, and mineral sectors is another application that makes use of AI and blockchain. As blockchain provides the documentation of a product's supply chain from seed to final product, the system's artificial intelligence analyzes crops and forecasts growing patterns. In order to establish a more transparent and moral journey from bean to cup, this technique has integrated mobile apps, bots, and blockchain into the coffee supply chain. The blockchain immutably records the farm from where the beans originated as well as the precise specs of a coffee shipment, while the system's AI evaluates coffee bean quality and forecasts weather and growing patterns. To guarantee prompt and equitable payment to all parties, it even serves as a payment ledger.
3. A system can develop software to simplify care and administrative activities in the healthcare sector using blockchain and AI technologies. For professionals, the system offers a variety of solutions that may be used to manage credentials, automate multi-party contracts, streamline product design, and more. The use of blockchain makes products accessible across distributed ledgers and facilitates team project activities.
4. AI collaboration - a framework that enables open access to the forecast and input data of the model, Smart contract to improve the model and use smart contracts to host an updated model.
5. Commanders at military operational centers frequently have to make prompt choices using data from many intelligence sources. A system that combines artificial intelligence, machine learning, and private blockchain to enable decision-making for operational centers. This system combines data from several sources using a variety of AI agents in order to forecast and assess the present choice. The blockchain in this framework serves two functions. To ensure that all AI agents are using the same dataset for analysis, separate AI agents might first check to see if they are running in the same blockchain state as other agents. It can compare and analyze decision results more effectively. Second, the blockchain record rewards the AI agents to encourage them to help decision-making.

6. AI-powered blockchain application for smart cities- Urban countries experience increasing levels of traffic congestion, which can be solved by traffic authorities limiting the overall number of vehicles on the road. The permit will encourage drivers to use alternate modes of transportation, such as cycling and public transportation, and it will help reduce the number of vehicles on the road. The Tradable Mobility Pass (TMP), a trading platform for traffic permits, allows for the trading of these permits in the open market. However, the implementation of these permits is challenging, even though Blockchain smart contracts may play a significant role in improving the viability of the solution. With the use of the Ethereum Blockchain, it will be possible to create smart contracts that would enable a dynamic road toll system with increased toll rates during rush hours to ease traffic congestion. By imposing higher prices on primary roadways that encourage other road users to seek alternate routes and improve traffic flow on primary roads, the smart contract and en-route tradable permit can also help to give precedence to emergency vehicles. Shared mobility of big vehicles is another application of blockchain technology that maintains traffic flow while reducing the likelihood of accidents that cause air drag and 20% of fuel usage.

- Now let's talk about how blockchain could help the government manage smart cities. In order to promote transparency and lower corruption, the government can employ blockchain technology to record revenue, expenses, and government contracts. By utilizing smart contracts, the Blockchain can potentially be utilized in the voting process. The Blockchain can be used to prove that a voter can only cast one ballot. This will increase openness and lessen voting process manipulation. Additionally, Blockchain can offer a platform to consolidate people' identities in one location. For example, by connecting a person's national identification, passport, and birth and death certificates to the Blockchain, identity fraud will be decreased.
- To improve road safety, particularly by expanding public transportation, and to meet the needs of those who are most at risk, such as women, children, people with disabilities, and the elderly, while also ensuring that everyone has access to safe, affordable, accessible, and sustainable transportation systems. These goals, which mainly involve reducing pollution by encouraging the use of public transportation, can be accomplished through the application of AI technology. The implementation of blockchain-AI technology in the transportation sector is thought to be facilitating the achievement of the Sustainable Development Goal.
- Moreover, AI transforms processes in several industry sectors and services, such as food, health, water, and energy services, acting as an enabler for a low-carbon economy and assisting in the development of sustainable cities. Smart appliances and other linked technologies, like electric driverless vehicles, can assist consumers in lowering their carbon footprints. Through the use of (TMP) Tradable Mobility Permit and IoT sensors on highways, Blockchain-AI is being utilized to monitor and lessen traffic congestion.
- The decentralized peer-to-peer energy trading and itemizing the cost of equipment that the AI analytics create allow the users to minimize energy costs and dramatically reduce CO2 emissions. These new improvements in the energy sector made possible by the Blockchain-AI also benefit consumers.

6.3 Blockchain in Cyber Security

- Maintaining the security of online data is crucial as more and more individuals use the Internet for daily activities and routines. Due to its centralized network, the current internet infrastructure is vulnerable to cyber attacks, which causes fraud and data theft. Blockchain, a popular phrase recently, has been credited with helping to safeguard online data. The greatest hazard to the general public is cyberattacks.

- However, blockchain is the best option for enhancing cybersecurity across businesses and safeguarding our data from manipulation. The security of several areas, including networks, apps, agreements, and proof of ownership, has been enhanced by blockchain applications.
- Cybersecurity is the field of procedures and strategies used to guard against unwanted access to and attack on networks, computers, data, and other sensitive information. Information technology security or computer security that safeguards data or information are other names for cyber security. Cybersecurity, in a nutshell, is the defence against data theft on computers and the Internet.
- The following are some of the primary categories of cyber security.
  - Application security
  - Cloud security
  - Network security
  - Critical infrastructure security
  - IoT security
- The following are the most frequent types of cyberattacks:
  - Cross-site scripting attack
  - Phishing attack
  - Denial of service (DoS) and distributed denial of service attacks (DDoS) and many more.
  - Ransomware attack
  - Malware
  - Man-in-the Middle attack
- Challenges in cyber security
  1. Preventing data theft
  2. False data entry prevention
  3. Protecting centralized data

6.3.1 Cybersecurity using Blockchain

- Every business and industrial area is boosted by the emerging technology known as blockchain.
- Cybercriminals are becoming more sophisticated and persistent as they try to steal important data, including financial information, health records, intellectual property, personally identifiable information, and other types.
- Therefore, using its features like data encryption, auditability, operational resilience, and immutability, and transparency, blockchain could potentially boost cyber-defence that stops fraudulent operations through consensus processes and detects data theft.
- Despite providing IT resources with remarkable levels of protection, the current security solutions are nonetheless prone to malfunction.
- This is due to the fact that the majority of security products are set up to function independently while protecting an IT resource.

- Hackers may choose to target a particular security solution, disable it, and then proceed to attack the now-exposed IT resource, as has been the case with attacks like DDoS (Distributed Denial of Service).
- Due to distributed security tools' improved ability to provide protection better than a single tool, blockchain can help boost the level of security currently in place.
- The three fundamental characteristics of blockchains that help avoid cyber attacks are that they are a **trustless system**, are **immutable**, and have **network consensus**. The blockchain helps to thwart significant attacks.

Fig. 6.3.1

- The idea of human trust is absent from blockchain systems. This only means that any code or functions that can be created to run as long as the network is online. Blockchain networks are designed with the assumption that any one node could attack it at any time. Consensus mechanisms like proof of work make sure that even if this occurs, the network will still carry out its intended duties without human interference or trickery.
- Any attempt to tamper with a blockchain database would be detected and stopped by network consensus. Therefore, if one node were to become compromised and malicious actions were to be carried out, the other nodes would immediately detect the issue and simply refrain from carrying out the inappropriate behavior.
- A blockchain offers a way to decentralize security and distribute digital information.
- Blockchain technology can be used to stop cybercrimes like identity theft, fraud, and data theft.

6.3.2 Blockchain Applications in Cyber Security

Here are just a few examples of the numerous situations in which blockchain technology is being used more broadly in the area of data security. This will grow with time, and as a result, there will be a growing need for Blockchain experts who can assist with it.

1. **Encrypted private messaging**
   - Social media sites capture a lot of metadata, and the majority of users use unreliable and weak passwords to safeguard their services and data. To enable end-to-end encryption and secure user data, many messaging firms are converting to Blockchain.
   - A common security protocol is built using blockchain. In order to provide cross-messenger communication features, it creates a uniform API structure. Social networking sites like Twitter and Facebook have been the target of countless hacks that resulted in data breaches and gave user information to the wrong people. Such cyberattacks are prevented by blockchain technology.
2. **A secure authentication system**
   - Passwords and other authentication systems are vulnerable to hacking and exploitation. People frequently use passwords that are simple to decipher. The adoption of password managers worsens the situation because an increasing number of people use them as storage vaults for all of their security information.

   - If the flaw had gone undiscovered, hackers would have had access to machines via the browser extension, enabling them to collect credentials.
   - With SSL certificates in place of passwords, distributed public key infrastructure is used by blockchain-based security systems to authenticate users and devices. Blockchain enables password-free authentication by combining robust authentication with the elimination of single points of vulnerability. Since certificate data is handled on the blockchain, false certificates cannot be created or used by hackers.
3. **A decentralized storage system**

   It is crucial to create a safer environment for all the personal information that we publish on a medium as society moves online more quickly. The majority of firms continue to store their data centrally, which makes it simpler for hackers to steal data. Because blockchain-based decentralized storage systems can thwart hacks and theft of company data.
4. **DNS security**

   Since most DNS is centralized, hackers have the ability to disrupt the links between a domain name and IP address and to take down a website. Recently, hackers have tried to combine DNS attacks with DDOS attempts to temporarily disable websites. By storing your data or information immutably on a decentralized, distributed ledger and using immutable smart contracts to power connections, blockchain technology can make it more difficult for hackers to access your data or information.
5. **Edge device security using identity authentication**

   Access points into core networks are particularly vulnerable when using edge devices. One illustration is a worker who uses their own insecure phone to get into the company's servers. The first step in plugging some of the most obvious network entry points that hackers could exploit is to make sure that these devices, as well as the core network itself, are protected using multi-step authentication processes and blockchain level, decentralized threat mitigation protocols.
6. **Blockchain for recovery and backup**

   Utilizing blockchain technology in secure storage and recovery systems is one of the most cutting-edge blockchain applications.
7. Blockchain doesn't need passwords since it uses numerous authentication processes, biometric data, or private keys to verify that users are who they claim to be. These systems protect our information more effectively than usernames, passwords, etc.

6.3.3 Benefits of Blockchain in Cyber Security

1. Blockchain provides decentralizing data storage that removes honey pot.
2. It provides high security with the help of cryptography which is by default a part of blockchain.
3. Distribution of multi-signature logins and public keys.
4. Verifies data ownership and integrity
5. Reduces vulnerability
6. Quick transactions
7. Mitigating DoS attacks