BLOCKCHAIN TECHNOLOGY

- **Module-1 Introduction to blockchain technology**
- **Introduction:** Blockchain 101: Distributed systems, History of blockchain, Introduction to blockchain, Types of blockchain, CAP theorem and blockchain, Benefits and limitations of blockchain.
- **Decentralization:** Decentralization using Blockchain, Methods of decentralization, Routes to decentralization, Decentralized organizations **Textbook 1**:Ch 1, Ch 2

COURSE OUTCOMES

At the end of the course the student will be able to:	
22CSE562.1	Explain the fundamental building blocks of Blockchain technology.
22CSE562.2	Outline the basics of Bitcoin, bitcoin network and payments.
22CSE562.3	Appraise the concepts of smart contract and basics of Ethereum.
22CSE562.4	Develop block chain-based solutions and write smart contract using Solidity
22CSE562.5	Illustrate Hyperledger fabric and its framework, design principles and architecture
22CSE562.6	Analyse the principles of Hyperledger design.

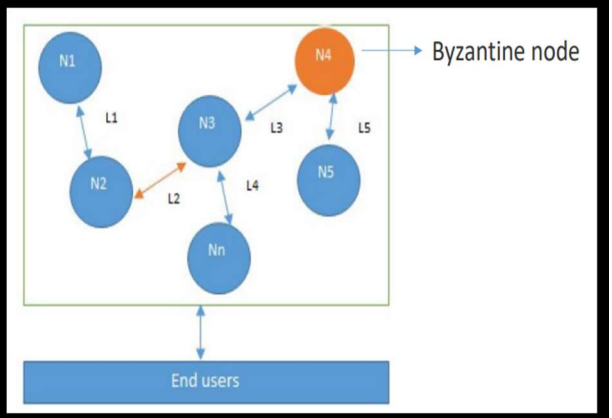
Introduction

- In 2008 a groundbreaking paper Bitcoin: "A Peer-to-Peer Electronic Cash System" was written on the topic of peer-to-peer electronic cash under the pseudonym Satoshi Nakamoto and introduced the term chain of blocks.
- This term over the years has now evolved into the word Blockchain.

Distributed systems

- It is the core of Blockchain Network.
- More precisely it is a decentralized distributed system.
- Distributed System: Computing paradigm whereby two or more nodes work with each other in a coordinated fashion in order to achieve a common outcome

- All nodes are capable of sending and receiving messages to and from each other.
- Nodes can be honest, faulty, or malicious and have their own memory and processor.
- A node that can exhibit arbitrary behavior is also known as a Byzantine node.



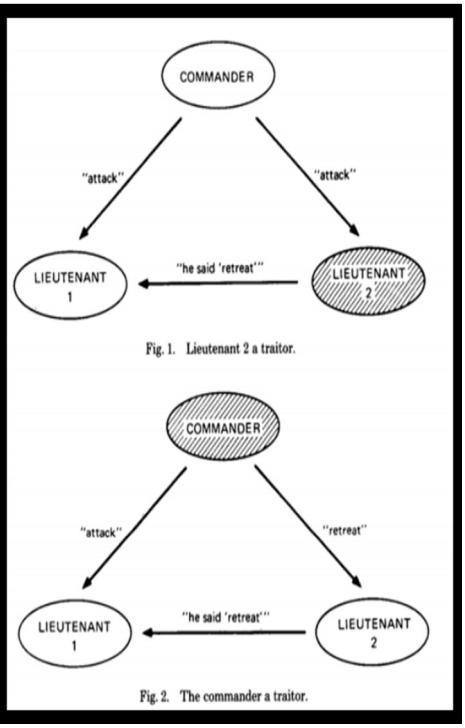
- Main Challenges in distributed system:
  - Coordination between nodes and
  - Fault tolerance
- Distributed systems are so challenging to design that a theorem known as the CAP theorem has been proved
- It states that a distributed system cannot have all much-desired properties simultaneously.

CAP theorem

- This is also known as Brewer's theorem, introduced originally by Eric Brewer as a conjecture in 1998; in 2002 it was proved as a theorem by Seth Gilbert and Nancy Lynch.
- The theorem states that any distributed system cannot have Consistency, Availability, and Partition tolerance simultaneously
  - Consistency is a property that ensures that all nodes in a distributed system have a single latest copy of data
  - Availability means that the system is up, accessible for use, and is accepting incoming requests and responding with data without any failures as and when required.
  - Partition tolerance ensures that if a group of nodes fails the distributed system still continues to operate correctly

Byzantine Generals problem

- In 1982 a thought experiment was proposed by Lamport et al.
- Problem Analysis:
  - Group of army generals who are leading different parts of the Byzantine army are planning to attack or retreat from a city.
  - The only way of communication between them is a messenger and they need to agree to attack at the same time in order to win.
  - The issue is that one or more generals can be traitors and can communicate a misleading message.
  - There is a need to find a viable mechanism that allows agreement between generals even in the presence of treacherous generals



The history of Blockchain

- THE CONCEPT OF ELECTRONIC CASH
- Since the 1980s, e-cash protocols have existed that are based on a model proposed by David Chaum.
- Fundamental issues that need to be addressed in e-cash systems are accountability and anonymity.
- David Chaum addressed both of these issues in his seminal paper in 1984 by introducing two cryptographic operations, namely blind signatures and secret sharing.
  - Blind signatures allow signing a document without actually seeing it and
  - Secret sharing is a concept that allows the detection of using the same e-cash token twice (double spending).

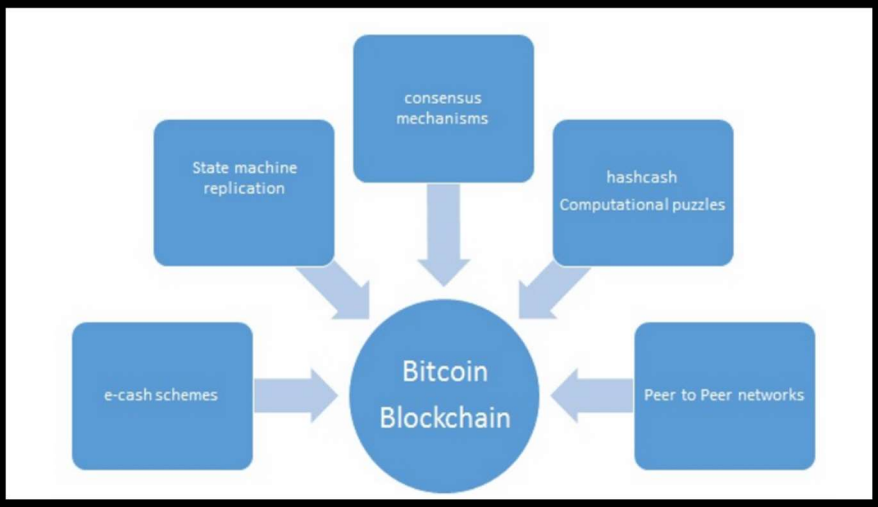
- After this other protocols emerged such as Chaum, Fiat, and Naor (CFN), e-cash schemes that introduced anonymity and double spending detection.
- Brand's ecash is another system that improved on CFN, made it more efficient, and introduced the concept of security reduction.
  - Security reduction is a technique used in cryptography to prove that a certain algorithm is secure by using another problem as a comparison

- The idea of using computational puzzles or pricing functions to prevent e-mail spam was introduced originally in 1992 by Cynthia Dwork and Moni Naor
- A different but relevant concept called hashcash was introduced by Adam Back in 1997 as a PoW system to control e-mail spam.
- In 1998 b-money was introduced by Wei Dai and proposed the idea of creating money via solving computational puzzles such as hashcash. It's based on a peer-to-peer network where each node maintains its own list of transactions.

- Another similar idea by Nick Szabo called BitGold was introduced in 2005 and also proposed solving computational puzzles to mint digital currency.
- In 2005 Hal Finney introduced the concept of cryptographic currency by combining ideas from b-money and hashcash puzzles but it still relied on a centralized trusted authority.

- In 2009 the first practical implementation of a cryptocurrency named bitcoin was introduced;
- For the very first time it solved the problem of distributed consensus in a trustless network.
- It uses public key cryptography with hashcash to provide a secure, controlled, and decentralized method of minting digital currency.
- The key innovation is the idea of an ordered list of blocks composed of transactions and cryptographically secured by the PoW mechanism.
- This ordered list of block are names as BLOCKCHAIN

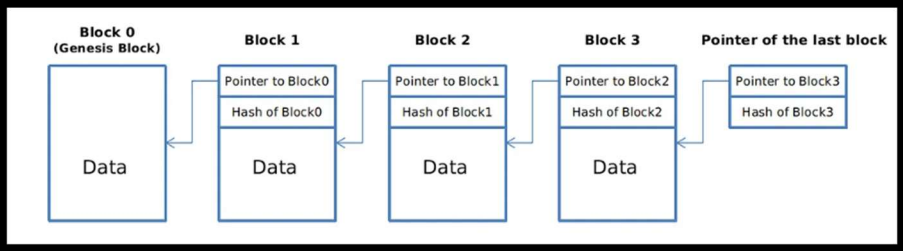
The various ideas that helped with the invention of bitcoin and blockchain



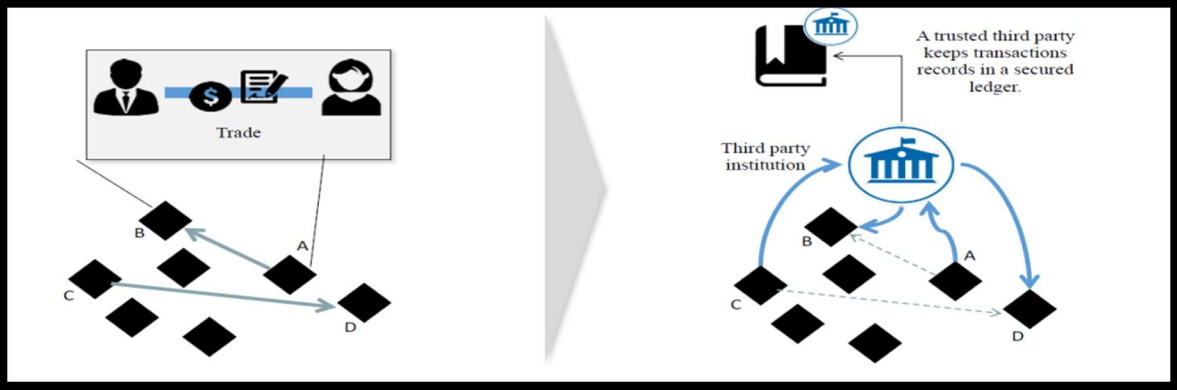
Introduction to blockchain

- Definitions:
- Blockchain at its core is a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers.
- Various technical definitions of blockchains:
- Blockchain is a decentralized consensus mechanism. In a blockchain, all peers eventually come to an agreement regarding the state of a transaction.
- Blockchain is a distributed shared ledger. Blockchain can be considered a shared ledger of transactions.
- Blockchain is a data structure; it is basically a linked list that uses hash pointers instead of normal pointers. Hash pointers are used to point to the previous block

- Blockchain is a data structure; it is basically a linked list that uses hash pointers instead of normal pointers. Hash pointers are used to point to the previous block

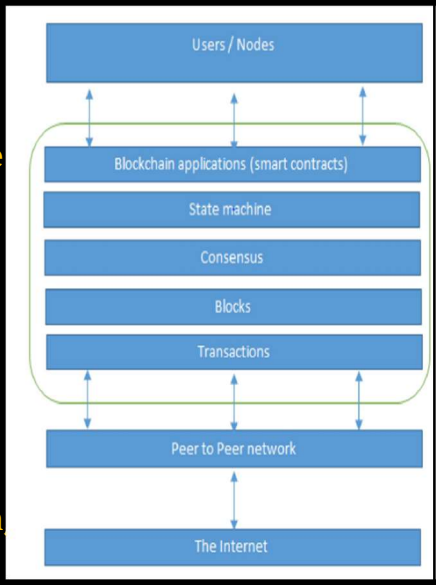


- From a business point of view a blockchain can be defined as a platform whereby peers can exchange values using transactions without the need for a central trusted arbitrator.



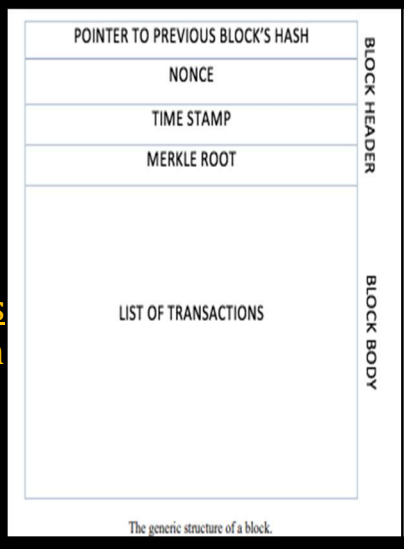
The network view of a blockchain

- At the bottom layer, there is the internet, which provides a basic communication layer for any network.
- In this case, a peer-to-peer network runs on top of the internet, which hosts another layer of blockchain.
- That layer contains transactions, blocks, consensus mechanisms, state machines, and blockchain smart contracts. All of these components are shown as a single logical entity in a box, representing blockchain above the peer-to-peer network.
- Finally, at the top, there are users or nodes that connect to the blockchain and perform various operations such as consensus, transaction verification, and processing.



A "Block" in a Blockchain

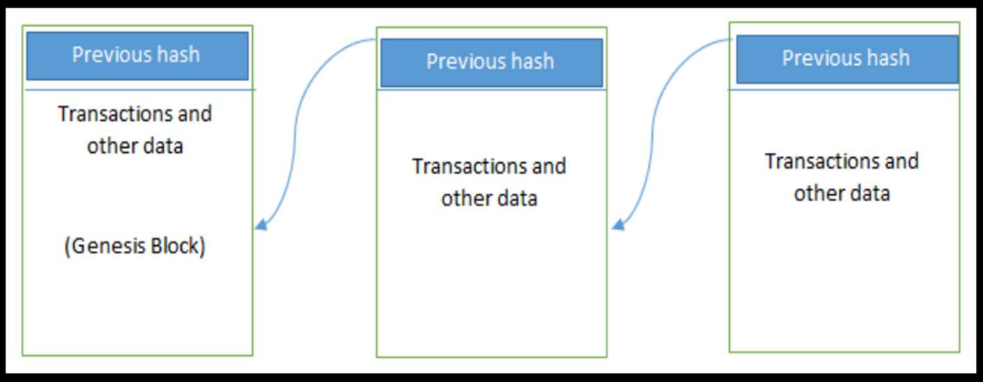
•A block is merely a selection of transactions bundled together and organized logically.
•A transaction is a record of an event, ex:transferring cash from a sender's account to a beneficiary's account.
•A block is made up of transactions, and its size varies depending on the type and design of the blockchain in use.
•A reference to a previous block is included in the block unless it is a genesis block.



The generic structure of a block.

- A genesis block is the first block in the blockchain that is hardcoded when the blockchain was first started.
- The structure of a block is dependent on the type and design of a blockchain but generally has essential attributes.
- The block header is composed of: pointer to previous block, timestamp, nonce, and Merkle root.
- The block body contains the transactions of that block.
- A nonce is a number that is generated and used only once, mainly for PoW consensus algorithms and replay protection.
- Merkle root is a hash of all the nodes of a Merkle tree and allows efficient verification of transactions in a block.

Structure of a generic blockchain



Generic elements of a blockchain

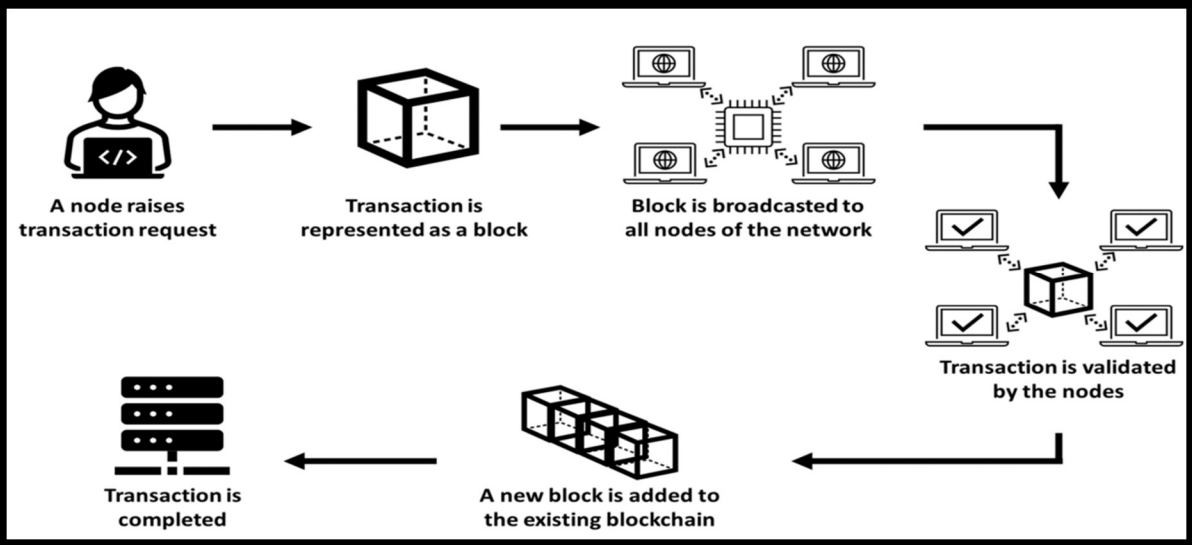
- ADDRESSES
  - Addresses are unique identifiers
  - An address is usually a public key or derived from a public key.
- TRANSACTION
  - Fundamental unit of a blockchain.
  - A transaction represents a transfer of value from one address to another.
- BLOCK
  - A block is composed of multiple transactions and other elements, such as the previous block hash (hash pointer), timestamp, and nonce.
- PEER-TO-PEER NETWORK
  - Network topology whereby all peers can communicate with each other and send and receive messages
- SCRIPTING OR PROGRAMMING LANGUAGE
  - Scripts are predefined sets of commands for nodes to transfer tokens from one address to another and perform various other functions
  - Scripts or programs perform various operations on a transaction in order to facilitate various functions. For example, in Bitcoin, transaction scripts are predefined in a language called Script,

- VIRTUAL MACHINE
  - A virtual machine allows Turing complete code to be run on a blockchain (as smart contracts) Ex: Ethereum Virtual Machine (EVM) and Chain Virtual Machine (CVM)
- STATE MACHINE
  - A blockchain can be viewed as a state transition mechanism
  - Changes state as a result of Transaction execution and validation process by nodes
- NODES
  - A node in a blockchain network performs various functions depending on the role it takes.
  - A node can propose and validate transactions and perform mining to facilitate consensus and secure the blockchain.
- SMART CONTRACTS
  - These programs run on top of the blockchain and encapsulate the business logic to be executed when certain conditions are met.

Features of a blockchain

- DISTRIBUTED CONSENSUS
  - This enables a blockchain to present a single version of truth that is agreed upon by all parties without the requirement of a central authority.
- TRANSACTION VERIFICATION
  - Any transactions posted from nodes on the blockchain are verified based on a predetermined set of rules.
  - Only valid transactions are selected for inclusion in a block.
- PLATFORMS FOR SMART CONTRACTS
  - A blockchain is a platform where programs can run that execute business logic on behalf of the users.
- TRANSFERRING VALUE BETWEEN PEERS
- GENERATING CRYPTOCURRENCY
- PROVIDER OF SECURITY
  - Blockchain is based on proven cryptographic technology that ensures the integrity and availability of data.
- IMMUTABILITY
  - Records once added onto the blockchain are immutable. • Achieved through hash pointer.
- UNIQUENESS

How blockchain accumulates blocks?



Steps

- 1. A node starts a transaction by first creating and then digitally signing it with its private key. Transaction is a data structure that represents transfer of value between users on the blockchain network.
- 2. A transaction is propagated (flooded) by using a flooding protocol, called Gossip protocol, to peers that validate the transaction based on preset criteria. Usually, more than one node are required to verify the transaction.
- 3. Once the transaction is validated, it is included in a block, which is then propagated onto the network. At this point, the transaction is considered confirmed.
- 4. The newly-created block now becomes part of the ledger, and the next block links itself cryptographically back to this block. This link is a hash pointer. At this stage, the transaction gets its second confirmation and the block gets its first confirmation.
- 5. Transactions are then reconfirmed every time a new block is created. Usually, six confirmations in the Bitcoin network are required to consider the transaction final.

Tiers of blockchain technology

- Blockchain 1.0:
  - This was introduced with the invention of bitcoin.
  - Basically, used for cryptocurrencies.
  - Generation 1 of blockchain technology
  - All alternative coins and bitcoin fall into this category.
  - This includes core applications such as payments and applications.
- Blockchain 2.0:
  - Generation 2.0 blockchains are used by financial services and contracts are introduced in this generation.
  - This includes various financial assets, for example derivatives, options, swaps, and bonds.
  - Applications that are beyond currency, finance, and markets are included at this tier

- Blockchain 3.0:
  - Generation 3 blockchains are used to implement applications beyond the financial services industry.
  - Used in more general-purpose industries such as government, health, media, the arts, and justice.
- Blockchain X.0:
  - This is a vision of blockchain singularity where one day we will have a public blockchain service available that anyone can use just like the Google search engine.
  - It will provide services in all realms of society.

Benefits and limitations of blockchain

- Decentralization: This is a core concept and benefit of the blockchain. There is no need for a trusted third party or intermediary to validate transactions; instead, a consensus mechanism is used to agree on the validity of transactions.
- Transparency and trust: Because blockchains are shared and everyone can see what is on the blockchain, this allows the system to be transparent. As a result, trust is established. This is more relevant in scenarios such as the disbursement of funds or benefits where personal discretion in relation to selecting beneficiaries needs to be restricted.
- Immutability: Once the data has been written to the blockchain, it is extremely difficult to change it back. It is not genuinely immutable, but because changing data is so challenging and nearly impossible, this is seen as a benefit to maintaining an immutable ledger of transactions.
- High availability: As the system is based on thousands of nodes in a peer-to-peer network, and the data is replicated and updated on every node, the system becomes highly available. Even if some nodes leave the network or become inaccessible, the network as a whole continues to work, thus making it highly available. This redundancy results in high availability.

- Highly secure: All transactions on a blockchain are cryptographically secured and thus provide network integrity.
- Simplification of current paradigms: The current blockchain model in many industries, such as finance or health, is somewhat disorganized. In this model, multiple entities maintain their own databases and data sharing can become very difficult due to the disparate nature of the systems. However, as a blockchain can serve as a single shared ledger among many interested parties, this can result in simplifying the model by reducing the complexity of managing the separate systems maintained by each entity.
- Faster dealings: In the financial industry, especially in post-trade settlement functions, blockchain can play a vital role by enabling the quick settlement of trades. Blockchain does not require a lengthy process of verification, reconciliation, and clearance because a single version of agreed-upon data is already available on a shared ledger between financial organizations.
- Cost saving: As no trusted third party or clearing house is required in the blockchain model, this can massively eliminate overhead costs in the form of the fees which are paid to such parties.

- As with any technology, some challenges need to be addressed in order to make a system more robust, useful, and accessible. Blockchain technology is no exception.
- In fact, much effort is being made in both academia and industry to overcome the challenges posed by blockchain technology.
- The most sensitive blockchain problems are as follows:
- Scalability
- Adaptability
- Regulation
- Relatively immature technology
- Privacy

Types of blockchain

- **1. Public Blockchain**
  - Open to everyone.
  - Anyone can join, read, write, or validate transactions.
  - Fully decentralized.
  - Example: **Bitcoin, Ethereum**
- **2. Private Blockchain**
  - Controlled by a single organization.
  - Only authorized members can join and validate.
  - More secure but less decentralized.
  - Example: **Hyperledger, Corda**
- **3. Consortium (Federated) Blockchain**
  - Controlled by a group of organizations instead of one.
  - Only selected participants can validate transactions.
  - Good for business collaboration.
  - Example: **Energy Web Foundation, IBM Food Trust**
- **4. Hybrid Blockchain**
  - Combination of public + private blockchain.
  - Some data is public, some private.
  - Gives flexibility: transparency + controlled access.
  - Example: **Dragonchain**

- **Public** = open for all
- **Private** = controlled by one
- **Consortium** = controlled by many
- **Hybrid** = mix of open + controlled

Public Blockchain

- It is a permissionless distributed ledger on which anybody can join and conduct transactions.
- It is a non-restrictive form of the ledger in which each peer has a copy. This also means that anyone with an internet connection can access the public Blockchain.
- This user has access to historical and contemporary records and the ability to perform mining operations.
- Complex computations must be performed to verify transactions and add them to the ledger.
- On the blockchain network, no valid record or transaction may be altered. Because the source code is usually open, anybody can check the transactions, uncover problems, and suggest fixes.

- Advantages of Public Blockchain –
  - Trustable: Public Blockchain nodes do not need to know or trust each other because the proof-of-work procedure ensures no fraudulent transactions.
  - Secure: A public network can have as many participants or nodes as it wants, making it a secure network. The higher the network's size, the more records are distributed, and the more difficult it is for hackers to hack the entire network.
  - Open and Transparent: The data on a public blockchain is transparent to all member nodes. Every authorized node has a copy of the blockchain records or digital ledger.
- Disadvantages of Public Blockchain –
  - Lower TPS: The number of transactions per second in a public blockchain is extremely low. This is because it is a large network with many nodes which take time to verify a transaction and do proof-of-work.
  - Scalability Issues: Its transactions are processed and completed slowly. This harms scalability. Because the more we try to expand the network's size, the slower it will become.
  - High Energy Consumption: The proof-of-work device is expensive and requires lots of energy. Technology will undoubtedly need to develop energy-efficient consensus methods.

- Uses of Public Blockchain –
  - Voting: Governments can use a public blockchain to vote, ensuring openness and trust.
  - Fundraising: Businesses or initiatives can use the public Blockchain to improve transparency and trust.

Private Blockchain

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

- Advantages of Private Blockchain –
  - Speed: Private Blockchain transactions are faster. This is because a private network has a smaller number of nodes, which shortens the time it takes to verify a transaction.
  - Scalability: You can tailor the size of your private Blockchain to meet your specific requirements. This makes private blockchains particularly scalable since they allow companies to easily raise or decrease their network size.
- Disadvantages of Private Blockchain –
  - Trust Building: In a private network, there are fewer participants will validate the transaction than in a private network.
  - Lower Security: A private blockchain network has fewer nodes or members, so it is more vulnerable to a security compromise.
  - Centralization: Private blockchains are limited in that they require a central Identity and Access Management (IAM) system to function. This system provides full administrative and monitoring capabilities.

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

Hybrid Blockchain

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

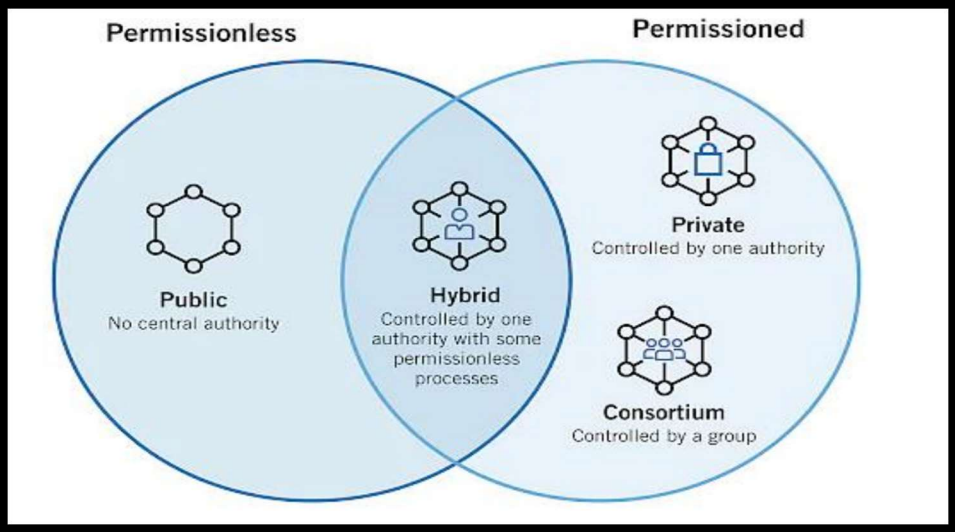
- Advantages of Hybrid Blockchain –
  - Secure: Hybrid Blockchain operates within a closed environment, preventing outside hackers from launching a 51 percent attack on the network.
  - Cost-Effective: It also safeguards privacy while allowing third-party contact. Transactions are inexpensive and quick and scale better than a public blockchain network.
- Disadvantages of Hybrid Blockchain –
  - Lack of Transparency: Because information can be hidden, this type of blockchain isn't completely transparent.
  - Less Incentive: Upgrading can be difficult, and users have no incentive to participate in or contribute to the network.

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

Consortium Blockchain

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

- Advantages of Consortium Blockchain –
  - Secure: A consortium blockchain is more secure, scalable, and efficient than a public blockchain network. It is like private and mixed blockchains, has access controls.
- Disadvantages of Consortium Blockchain –
  - Lack of Transparency: The consortium blockchain has a lower degree of transparency. If a member node is infiltrated, it can still be hacked, and the Blockchain's rules can render the network inoperable.
- Uses of Consortium Blockchain –
  - Banking and Payments: A consortium can be formed by a group of banks working together. They have control over which nodes will validate transactions.
  - Research: A consortium blockchain can be employed to share research data and outcomes.
  - Food Tracking: It is also used for food tracking.



Other types of blockchains

- Sidechains
- Permissioned ledger
- Distributed ledger
- Shared ledger
- Fully private and proprietary blockchains
- Tokenized blockchains
- Tokenless blockchains

Consensus in blockchain

- Distributed computing concept that has been used in blockchain
- It provide a means of agreeing to a single version of truth by all peers on the blockchain network.
- different types of blockchain consensus mechanisms
  - PROOF OF WORK
  - PROOF OF STAKE
  - DELEGATED PROOF OF STAKE
  - PROOF OF ELAPSED TIME
  - DEPOSIT-BASED CONSENSUS
  - PROOF OF IMPORTANCE
  - FEDERATED CONSENSUS OR FEDERATED BYZANTINE CONSENSUS
  - REPUTATION-BASED MECHANISMS
  - PRACTICAL BYZANTINE FAULT TOLERANCE

PROOF OF WORK

- Relies on proof that enough computational resources have been spent before proposing a value for acceptance by the network
- This is used in bitcoin and other cryptocurrencies.

PROOF OF STAKE

- This algorithm works on the idea that a node or user has enough stake in the system.
- This idea was first introduced by Peercoin and is going to be used in the Ethereum blockchain.
- Another important concept in Proof of Stake (PoS) is coin age, which is a derived from the amount of time and the number of coins that have not been spent.
- In this model, the chances of proposing and signing the next block increase with the coin age.

DELEGATED PROOF OF STAKE

- Delegated Proof of Stake (DPOS) is an innovation over standard PoS whereby each node that has stake in the system can delegate the validation of a transaction to other nodes by voting.
- This is used in the bitshares blockchain

PROOF OF ELAPSED TIME

- Introduced by Intel, it uses Trusted Execution Environment (TEE)
- It provide randomness and safety in the leader election process via a guaranteed wait time.
- It requires the Intel SGX (Software Guard Extensions) processor in order to provide the security guarantee and for it to be secure.

DEPOSIT-BASED CONSENSUS

- Nodes that wish to participate on the network have to put in a security deposit before they can propose a block.

PROOF OF IMPORTANCE

- This idea is important and different from Proof of Stake.
- Proof of importance not only relies on how much stake a user has in the system but it also monitors the usage and movement of tokens by the user to establish a level of trust and importance.
- This is used in NEMcoin

FEDERATED CONSENSUS OR FEDERATED BYZANTINE CONSENSUS

- Used in the Stellar consensus protocol, nodes in this protocol keep a group of publicly trusted peers.
- Propagates only those transactions that have been validated by the majority of trusted nodes.

REPUTATION-BASED MECHANISMS

- As the name suggests, a leader is elected on the basis of the reputation it has built over time on the network.
- This can be based on the voting from other members.

PRACTICAL BYZANTINE FAULT TOLERANCE

- Practical Byzantine Fault Tolerance (PBFT) achieves state machine replication, which provides tolerance against Byzantine nodes.

- 1. Proof of Work (PoW)
- Miners solve complex mathematical puzzles.
- First to solve adds the block and earns a reward.
- Very secure but energy-intensive.
- Example: Bitcoin, Ethereum (before 2022).

- 2. Proof of Stake (PoS)
- Validators are chosen based on how many coins they "stake" (lock up).
- No heavy energy use like PoW.
- More stake = higher chance to validate.
  Example: Ethereum (after Merge), Cardano.

- 3. Delegated Proof of Stake (DPoS)
- Coin holders vote for a small group of trusted delegates (validators).
- Delegates validate transactions on behalf of everyone.
- Faster and more democratic but can become centralized.
  Example: EOS, TRON.

- 4. Proof of Elapsed Time (PoET)
- Used in permissioned (private) blockchains.
- Instead of solving puzzles, nodes wait for a random time.
- The one with the shortest wait wins the right to create a block.
  Example: Hyperledger Sawtooth.

- 5. Deposit-Based Consensus
- Similar to PoS. Participants deposit tokens.
- If they act dishonestly, their deposit is slashed (taken away).
- Encourages honest behavior.

- 6. Proof of Importance (PoI)
- Not only based on coins (like PoS) but also on activity and reputation.
- Factors: transaction frequency, relationships with others, and stake.
  Example: NEM blockchain.

7. Federated Consensus / Federated Byzantine Consensus
- A set of pre-selected trusted nodes validate transactions.
- Faster and less energy use.
- Good for consortium blockchains (banks, enterprises).
  Example: Ripple (XRP), Stellar.

- 8. Reputation-Based Mechanisms
- Validators are chosen based on their past behavior and trustworthiness.
- Misbehavior lowers reputation, making them less likely to be chosen.
  Example: EigenTrust algorithm (used in some research blockchains).

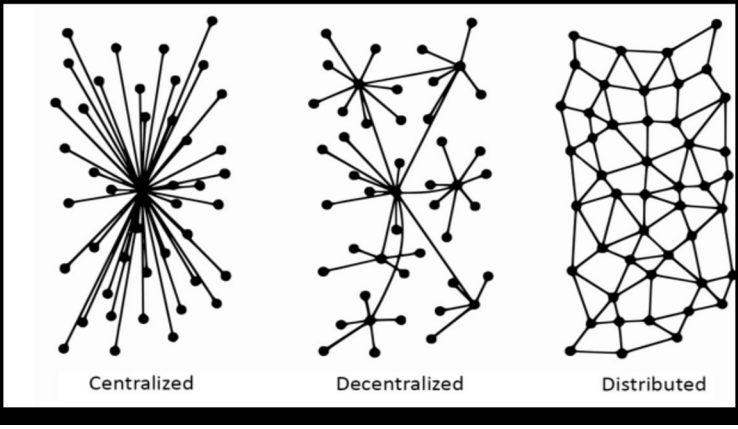
- 9. Practical Byzantine Fault Tolerance (PBFT)
- Designed to work even if some nodes are malicious (Byzantine fault).
- Nodes exchange messages and agree on a block using voting rounds.
- Very efficient for small networks (low latency, high speed).
  Example: Hyperledger Fabric uses PBFT variants.

CAP theorem and Blockchain

- In blockchains consistency is sacrificed in favor of availability and partition tolerance.
- In this scenario, Consistency (C) on the blockchain is not achieved simultaneously with Partition tolerance (P) and Availability (A), but it is achieved over time.
- This is called eventual consistency, where consistency is achieved as a result of validation from multiple nodes over time.

Chapter.2: Decentralization

- The basic idea of decentralization is to distribute control and authority to peripheries instead of one central authority being in full control of the organization.



Comparison: Centralized vs. Decentralized vs. Distributed

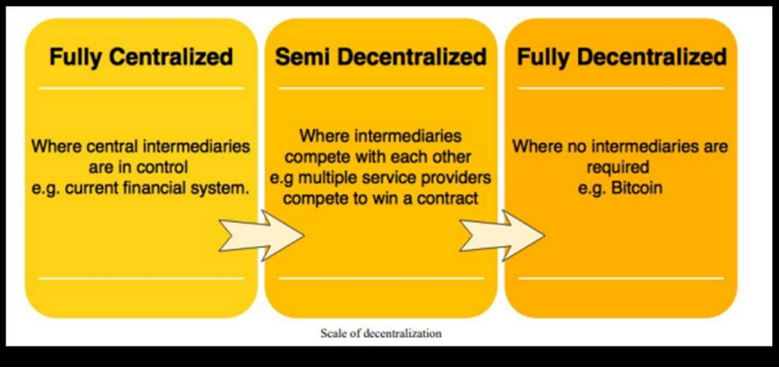
Characteristics	Centralized	Decentralized	Distributed
Maintenance	Low	Moderate	High
Scalability	Low	Moderate	High
Data Access	Accessing the same data by multiple users takes more time	Accessing data from the network is easy	Data can be accessed rapidly from a database
Single Point of Failure	Yes	No	No
Fault Tolerance	Low	Extremely High	High
Examples	ERP system	Blockchain	Cloud Computing

Methods of decentralization

- Disintermediation
  - Intermediary is no longer required and decentralization is achieved by disintermediation
    - Ex: Imagine that you want to send money to a friend in another country. You go to a bank who, for a fee, will transfer your money to the bank in that country. In this case, the bank maintains a central database that is updated, confirming that you have sent the money. With blockchain technology, it is possible to send this money directly to your friend without the need for a bank. All you need is the address of your friend on the blockchain.
- Through competition (Contest-driven decentralization)
  - A group of service providers compete with each other in order to be selected for the provision of services by the system. This paradigm does not achieve complete decentralization
  - Ensures that an intermediary or service provider is not monopolizing the service.
  - In Blockchain, Smart contracts can choose an external data provider from a large number of providers based on their reputation, previous score, reviews, and quality of service.

Contest-driven decentralization

- On the left-hand side, the conventional approach is shown where a central system is in control; on the right-hand side, complete disintermediation is achieved as intermediaries are entirely removed. Competing intermediaries or service providers are shown in the center. At that level, intermediaries or service providers are selected based on reputation or voting, thus achieving partial decentralization.



Routes to decentralization

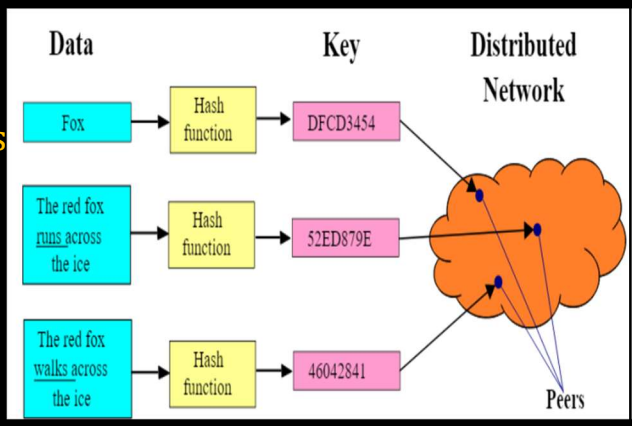
- How to decentralize
- A framework has been proposed by Arvind Narayanan and others that can be used to evaluate the decentralization requirements of a variety of things in the context of blockchain technology.
- The framework proposes four questions that, once answered, provide a clear idea as to how a system can be decentralized.
  1.What is being decentralized?
  2. What level of decentralization is required?
  3. What blockchain is used?
  4. What security mechanism is used?
  EXAMPLE
  A money transfer system
  Answer 1: Money transfer system.
  Answer 2: Disintermediation.
  Answer 3: Bitcoin.
  Answer 4: Atomicity.

Blockchain and full ecosystem decentralization

- Blockchain itself is a distributed ledger that runs on top of conventional systems.
- These elements include:
  - Storage
  - Communication
  - Computation.

Storage

- Data can be stored directly in a blockchain
- Major disadvantage of this approach is that blockchain is not suitable for storing large amounts of data by design.
- Not suitable for storing images or large blobs of data.
- A better alternative is to use distributed hash tables (DHTs).



- Two main requirements here are high availability and link stability
- Inter Planetary File System (IPFS) by *Juan Benet* possesses both of these properties and the vision is to provide a decentralized World Wide Web.
- IPFS uses Kademlia DHT and merkle DAG (Directed Acyclic Graph) to provide the storage and searching functionality, respectively.
- The incentive mechanism is based on a protocol known as Filecoin that pays incentives to nodes that store data using the BitSwap mechanism.
- BigChainDB is another storage layer decentralization project aimed at providing a scalable, fast, and linearly scalable decentralized database

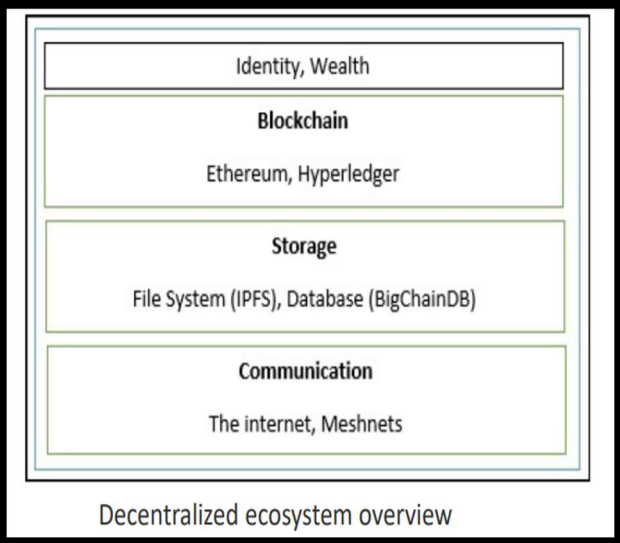
Communication

- It is generally considered that the Internet (the communication layer in blockchain) is decentralized.
- Services such as e-mail and online storage are all now based on a paradigm where the service provider is in control and users trust them to give them access to the service when required.
- This model is based on the trust of the central authority (the service provider) and users are not in control of their data; even passwords are stored on trusted third-party systems.
- There is a need to provide control to individual users in such a way that access to their data is guaranteed and is not dependent on a single third party

- Access to the Internet (the communication layer) is based on Internet service providers (ISPs) that act as a central hub for Internet users.
- If the ISP is shut down for political or any other reasons, then no communication is possible in this model.
- An alternative is to use mesh networks.
- They provide a decentralized alternative where nodes can talk directly to each other without a central hub such as an ISP.
- Ex: Firechat

Computation

- Decentralization of computing or processing is achieved by a blockchain technology such as Ethereum, where smart contracts with embedded business logic can run on the network.



Decentralized ecosystem overview

Decentralized organizations(DO)

- Decentralized organization (DOs) are software programs that run on a blockchain
- These are based on the idea of real human organizations with people and protocols.
- Once a DO is added to the blockchain in the form of a smart contract or a set of smart contracts, it becomes decentralized.
- Parties interact with each other based on the code defined within the DO software.

Decentralized autonomous organizations (DAO)

- Computer program than runs on top of a blockchain and embedded within it are governance and business logic rules.
- DAO and DO are basically the same thing, but the main difference is that DAOs are autonomous.
- They are fully automated and contain artificially intelligent logic.
- DOs lack this feature and rely on human input in order to execute business logic.
- Ethereum blockchain led the way with the introduction of DAOs for the first time.
- An Autonomous Agent (AA) is a piece of code that runs without human intervention.

Decentralized autonomous corporations(DAC)

- Decentralized autonomous corporations (DACs) are a similar concept but are considered a smaller subset of DAOs.
- General difference is
  - DAOs are usually considered to be nonprofit, whereas DACs can make money via shares offered to the participants and by paying dividends.
- These corporations can run a business automatically without human intervention based on the logic programmed within them

Decentralized autonomous societies(DAS)

- Decentralized autonomous societies (DASs) are a concept whereby entire societies can function on a blockchain.
- They include multiple complex smart contracts and a combination of DAOs and Decentralized applications (DAPPs) running autonomously.
- Many services that a government offers can be delivered via blockchain, such as Government Identity Card systems, passport issuance, and records of deeds, marriages, and births

Decentralized applications(DAPP)

- All ideas mentioned earlier come under the larger umbrella of decentralized applications.
- All DAOs, DACs, and DOs are basically decentralized applications that run on top of a blockchain in a peer-to-peer network.
- This is the latest advancement in technology with regard to decentralization.
- Decentralized applications or DAPPs are software programs that:
  - Run on their own blockchain,
  - Use another already existing established blockchain,
  - Use only protocols of an existing blockchain solution.

Requirements of a decentralized application

1. The DAPP should be fully open source and autonomous and no single entity should be in control of a majority of its tokens. All changes to the application must be consensus-driven based on the feedback given by the community.

2. Data and records of operations of the application must be cryptographically secured and stored on a public, decentralized blockchain in order to avoid any central points of failure.

3. A cryptographic token must be used by the application in order to provide access and rewards to those who contribute value to the applications, for example, miners in bitcoin.

4. The tokens must be generated by the decentralized application according to a standard cryptographic algorithm. This generation of tokens acts as a proof of the value to contributors (for example, miners).

Blockchain-based decentralized applications (DApps)-EXAMPLES

- KYC-Chain
  - This application provides a facility to manage Know Your Customer (KYC) data in a secure and convenient way based on smart contracts.
- OpenBazaar
  - This is a decentralized peer-to-peer network that allows commercial activities directly between sellers and buyers.
  - Distributed hash tables (DHTs) are used in a peer-to-peer network in order to enable direct communication and data sharing between peers.
  - It makes use of bitcoin as a payment network
- Lazooz
  - This is a decentralized equivalent of Uber.
  - It allows peer to- peer ride sharing and users can be incentivized by proof of movement and can earn Zooz coins

Platforms for decentralization

Ethereum

- Ethereum tops the list as being the first blockchain that introduced a Turing-complete language and the concept of a virtual machine.
- With the availability of this Turing complete language called Solidity, endless possibilities have opened for the development of decentralized applications.
- This was proposed in 2013,by *Vitalik Buterin* and provides a public blockchain to develop smart contracts and decentralized applications.
- Currency tokens on Ethereum are called Ethers

Maidsafe(Massive Array of Internet Disks – Secure Access for Everyone)

- Maidsafe provides a SAFE (Secure Access for Everyone) network that is made up of unused computing resources, such as storage, processing power, and the data connections.
- The files on the network are divided into small chunks of data that are encrypted and distributed throughout the network randomly.
- This data can only be retrieved by its respective owner.
- One key innovation is that duplicate files are automatically rejected on the network
- It uses Safecoin as a token to incentivize its contributors.

Lisk

- Lisk is a blockchain application development and cryptocurrency platform.
- It allows developers to use JavaScript to build decentralized applications and host them in their own respective sidechains.
- Lisk uses the Delegated Proof of Stake (DPOS) mechanism for consensus to secure the network and propose blocks.
- It uses the Node.js and JavaScript backend whereas the frontend allows the use of standard technologies, such as CSS3, HTML5, and JavaScript.
- Lisk uses LSK coin as a currency on the blockchain.