BLOCKCHAIN

Siva Kumar Ronanki

Distributed systems

- **Distributed systems** are a computing paradigm whereby two or more nodes work with each other in a coordinated fashion to achieve a common outcome.
- It is modeled in such a way that end users see it as a single logical platform.
- Ex: Google's search engine is based on a large distributed system, but to a user, it looks like a single, coherent platform.
- A **node** can be defined as an individual player in a distributed system
- All nodes are capable of sending and receiving messages to and from each other.
- A node that exhibits irrational behavior is also known as a **Byzantine node** after the Byzantine Generals Problem.
- *The Byzantine Generals problem: https://www.geeksforgeeks.org/byzantine-generals-problem-in-blockchain/*

Design of a distributed system

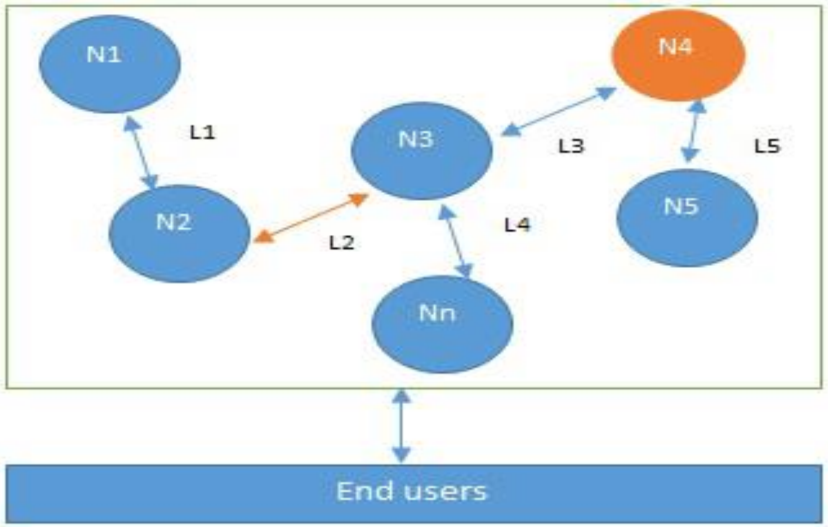


Fig: Design of a distributed system: N4 is a Byzantine node, L2 is broken or a slow network link

- This distributed system has six nodes out of which one **(N4)** is a Byzantine node leading to possible data inconsistency
- **L2** is a link that is broken or slow, and this can lead to partition in the network.

Challenges in Distributed Systems

- Coordination between nodes and fault tolerance
- Even if some of the nodes become faulty or network links break, the distributed system should be able to tolerate this and continue to work to achieve the desired result.
- Distributed systems are so challenging to design that a hypothesis known as the **CAP theorem** has been proven, which states that a distributed system cannot have all three of the much-desired properties simultaneously; that is, consistency, availability, and partition tolerance.

The history of blockchain and Bitcoin

- Blockchain was introduced with the invention of Bitcoin in 2008.
- Its practical implementation occurred in 2009.

Electronic cash:

- Since the 1980s, e-cash protocols have existed that are based on a model proposed by David Chaum.
- Two fundamental e-cash system issues need to be addressed: **accountability** and **anonymity.**
- **Accountability** is required to ensure that cash is spendable only once (double-spend problem) and that it can only be spent by its rightful owner.
- Double spend problem arises when same money can be spent twice
- **Anonymity** is required to protect users' privacy

Blind signatures and secret sharing

- David Chaum solved these problems (**accountability** and **anonymity)** in 1980s by using two cryptographic operations, namely **blind signatures** and **secret sharing**.
- ***Blind signatures*** allow for signing a document without actually seeing it.
- ***Secret sharing*** is a concept that enables the detection of double spending, that is using the same e-cash token twice (doublespending).
- In 2009, the first practical implementation of an electronic cash (e-cash) system was named Bitcoin
- It used **public key cryptography** with a **Proof of Work** (**PoW**) mechanism to provide a secure, controlled, and decentralized method of minting digital currency.

Blockchain

- Blockchain 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

Peer-to-peer:

- This means that there is no central controller in the network, and all participants talk to each other directly.
- This property allows for cash transactions to be exchanged directly among the peers without a third-party involvement, such as by a bank.

Distributed ledger:

- This means that a ledger is spread across the network among all peers in the network, and each peer holds a copy of the complete ledger.

Cryptographically-secure:

- This means that cryptography has been used to provide security services which make this ledger secure against tampering and misuse.
- These services include non-repudiation, data integrity, and data origin authentication.

Blockchain

Append-only:

- This means that data can only be added to the blockchain in *time-ordered sequential order*.
- This property implies that once data is added to the blockchain, it is almost impossible to change that data and can be considered practically immutable.
- There may be some legitimate reasons to change data in the blockchain once it has been added, such as the *right to be forgotten* or *right to erasure* (also defined in **General Data Protection (GDPR)** ruling)

Blockchain

Updateable via consensus:

- In this scenario, no central authority is in control of updating the ledger.
- Instead, any update made to the blockchain is validated against strict criteria defined by the blockchain protocol and added to the blockchain only after a consensus has been reached among all participating peers/nodes on the network.
- To achieve consensus, there are various consensus facilitation algorithms which ensure that all parties are in agreement about the final state of the data on the blockchain network and resolutely agree upon it to be true.

Blockchain

- Blockchain can be thought of as a layer of a distributed peer-to-peer network running on top of the internet.

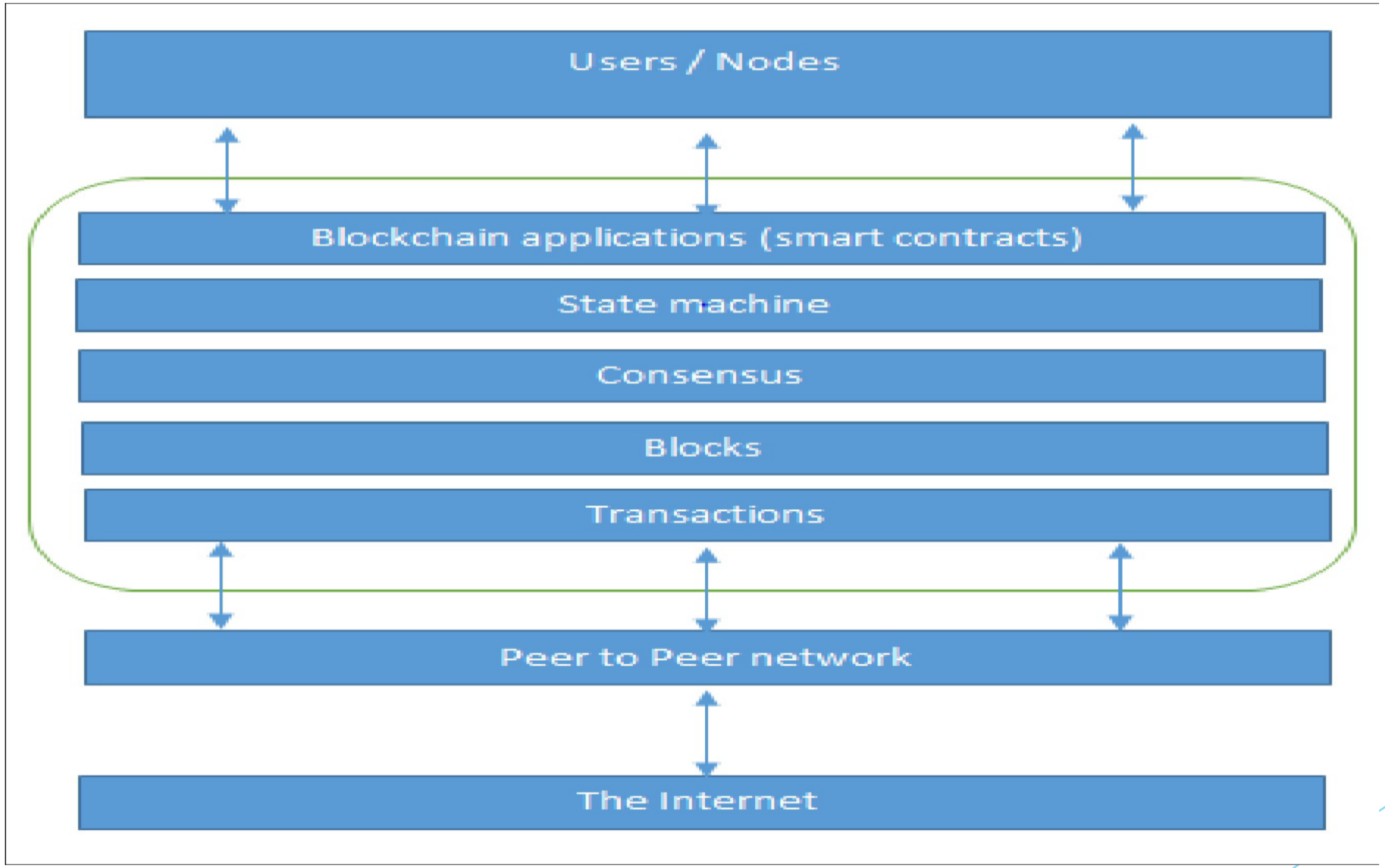


Fig: The network view of a blockchain

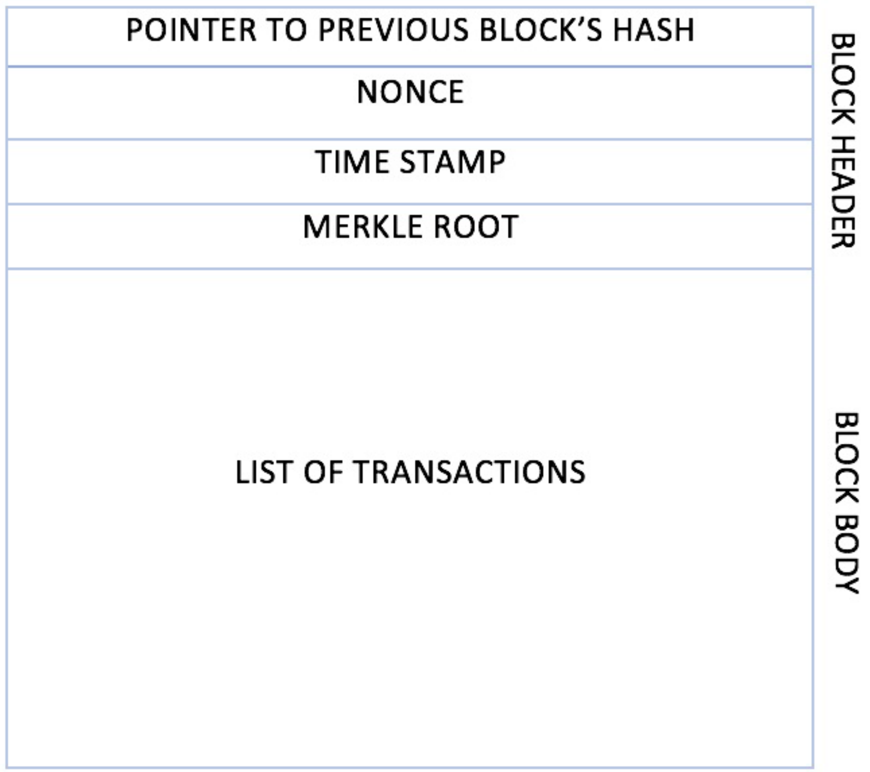
Blockchain

- At the bottom layer in the preceding diagram, there is the internet, which provides a basic communication layer for any network.
- A peer-to-peer network runs on top of the internet, which hosts another layer of blockchain that contains transactions, blocks, consensus mechanisms, state machines, and blockchain smart contracts.
- 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** is merely a selection of transactions bundled together and organized logically.
- A **genesis block** is the first block in the blockchain that is hardcoded at the time the blockchain was first started. The structure of a block is also dependent on the type and design of a blockchain
- A **transaction** is a record of an event, for example, the event of 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.

Blockchain

- A **nonce** is a number that is generated and used only once. A nonce is used extensively in many cryptographic operations to provide replay protection, authentication, and encryption.
- **Merkle root** is a hash of all of the nodes of a Merkle tree.
- Merkle trees are widely used to validate the large data structures securely and efficiently.
- In the blockchain world, Merkle trees are commonly used to allow efficient verification of transactions.
- Merkle root in a blockchain is present in the block header section of a block, which is the hash of all transactions in a block.
- Verifying only the Merkle root is required to verify all transactions present in the Merkle tree instead of verifying all transactions one by one.

The generic structure of a block.



Generic elements of a blockchain

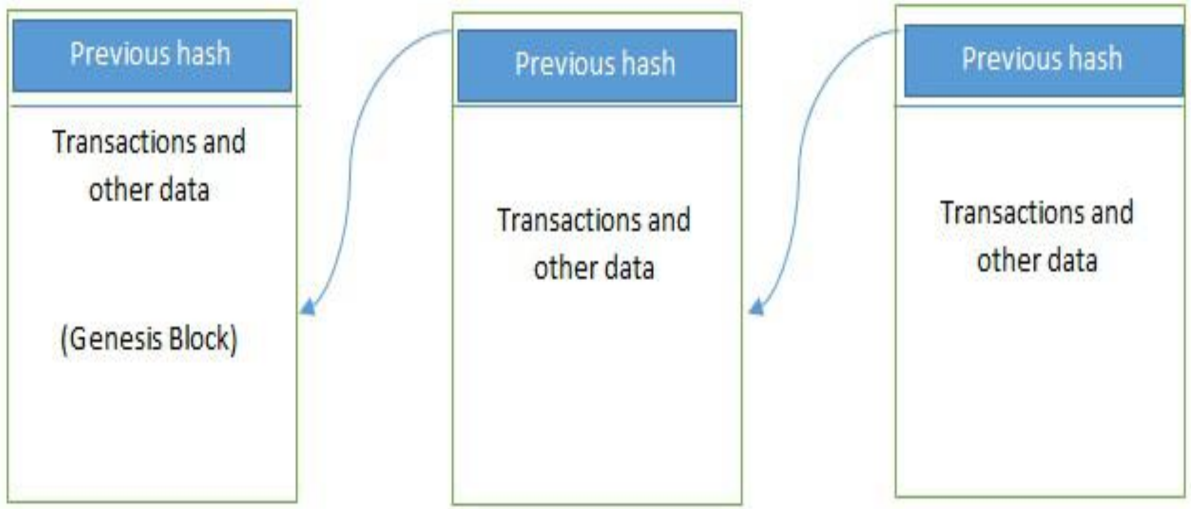


Fig: Generic structure of a blockchain

- Elements of a generic blockchain are described as follows:

- **Address:** Addresses are unique identifiers used in a blockchain transaction to denote senders and recipients. An address is usually a public key or derived from a public key. While addresses can be reused by the same user, addresses themselves are unique.
- A single user may not use the same address again and generate a new one for each transaction. This newly-created address will be unique.
- A good practice is for users to generate a new address for each transaction in order to avoid linking transactions to the common owner, thus preventing identification.

Generic elements of a blockchain

- **Transaction**: A transaction is the 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**: As the name implies, a peer-to-peer network is a network topology wherein all peers can communicate with each other and send and receive messages.
- **Scripting or programming language**: 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**, which consist of sets of commands that allow nodes to transfer tokens from one address to another.
- Script is a limited language, however, in the sense that it only allows essential operations that are necessary for executing transactions, but it does not allow for arbitrary program development.
- Bitcoin script language cannot be called *Turing complete*. In simple words, Turing complete language means that it can perform any computation.
- Turing complete languages need loops and branching capability to perform complex computations.
- Therefore, Bitcoin's scripting language is not Turing complete, whereas Ethereum's Solidity language is.

Generic elements of a blockchain

- **Virtual machine**: A *virtual machine* allows Turing complete code to be run on a blockchain (as smart contracts); whereas a transaction script is limited in its operation.
- Various blockchains use virtual machines to run programs such as **Ethereum Virtual Machine** (**EVM**) and **Chain Virtual Machine** (**CVM**).
- EVM is used in Ethereum blockchain, while CVM is a virtual machine developed for and used in an enterprise-grade blockchain called **Chain Core**.

- **State machine**: A blockchain can be viewed as a state transition mechanism whereby a state is modified

from its initial form to the next one and eventually to a final form by nodes on the blockchain network as a

result of a transaction execution, validation, and finalization process.

Generic elements of a blockchain

- **Node**: A node in a blockchain network performs various functions depending on the role that it takes on.
- A node can propose and validate transactions and perform mining to facilitate consensus and secure the blockchain.
- This is achieved by following a **consensus protocol** (most commonly PoW).
- Nodes can also perform other functions such as simple payment verification (lightweight nodes), validation, and many other functions depending on the type of the blockchain used and the role assigned to the node.
- Nodes also perform a transaction signing function.
- Transactions are first created by nodes and then also digitally signed by nodes using private keys as proof that they are the legitimate owner of the asset.
- This asset is usually a token or virtual currency, such as Bitcoin, but it can also be any real-world asset represented on the blockchain by using tokens(NFTs).

Generic elements of a blockchain

- **Smart contract:** These programs run on top of the blockchain and encapsulate the business logic to be executed when certain conditions are met.
- The smart contract feature is not available on all blockchain platforms, but it is now becoming a very desirable feature due to the flexibility and power that it provides to the blockchain applications.
- Smart contracts have many use cases, identity management, capital markets, trade,finance, record management, insurance, and e-governance.

Features of a blockchain

- **Distributed consensus**: Distributed consensus is the primary underpinning of a blockchain. This mechanism allows a blockchain to present a single version of the truth, which is agreed upon by all parties without the requirement of a central authority.
- **Transaction verification**: Any transactions posted from the nodes on the blockchain are verified based on a predetermined set of rules. Only valid transactions are selected for inclusion in a block.
- **Platform for smart contracts**: A blockchain is a platform on which programs can run to execute business logic on behalf of the users.
- Not all blockchains have a mechanism to execute *smart contracts*; however, this is a very desirable feature, and it is available on newer blockchain platforms such as Ethereum and Multichain.
- **Generation of cryptocurrency:** A blockchain can create cryptocurrency as an incentive to its miners who validate the transactions and spend resources to secure the blockchain.
- **Uniqueness**: This blockchain feature ensures that every transaction is unique and has not already been spent (double-spend problem).
- This feature is especially relevant with cryptocurrencies, where detection and avoidance of double spending are a vital requirement.

Features of a blockchain

- **Smart property:** It is now possible to link a digital or physical asset to the blockchain in such a secure and precise manner that it cannot be claimed by anyone else.
- You are in full control of your asset, and it cannot be double-spent or double-owned.
- While it is true that many **Digital Rights Management** (**DRM**) schemes are being used currently along with copyright laws, but none of them is enforceable in such a way as blockchain based DRM can be.
- Blockchain can provide DRM functionality in such a way that it can be enforced fully.
- Another example is **PS3 hack**, also copyrighted digital music, films and e-books are routinely shared on the internet without any limitations.
- We have copyright protection in place for many years, but digital piracy refutes all attempts to fully enforce the law on a blockchain, however, if you own an asset, no one else can claim it unless you decide to transfer it.

Features of a blockchain

- **Provider of security:** The blockchain is based on proven cryptographic technology that ensures the integrity and availability of data.
- Generally, confidentiality is not provided due to the requirements of transparency.
- This limitation is the leading barrier to its adoption by financial institutions and other industries that require privacy and confidentiality of transactions.
- A more recent example is Zcash, which provides a platform for conducting anonymous transactions.
- Other security services, such as non-repudiation and authentication, are also provided by blockchain, as all actions are secured using private keys and digital signatures.
- **Immutability**: This is another critical feature of blockchain: once records are added to the blockchain, they are immutable.
- There is the remote possibility of rolling back changes, but this is to be avoided at all costs as doing so would consume an exorbitant amount of computing resources.
- For example, with Bitcoin if a malicious user wants to alter previous blocks, then it would require computing the PoW once again for all those blocks that have already been added to the blockchain.
- This difficulty makes the records on a blockchain essentially immutable.

Applications of blockchain technology

- **Financial services:** Blockchain can be used to track and record financial transactions, such as payments, loans, and investments. This can help to reduce fraud and errors, and to improve transparency and efficiency.
- **Supply chain management:** Blockchain can be used to track the movement of goods and products throughout the supply chain. This can help to improve visibility and traceability, and to reduce counterfeiting and fraud.
- **Identity management:** Blockchain can be used to create secure and immutable digital identities. This can help to improve security and privacy, and to make it easier to verify identities.
- **Healthcare:** Blockchain can be used to store and share medical records, securely and confidentially. This can help to improve patient care, and to reduce costs.
- **Voting:** Blockchain can be used to create secure and transparent voting systems. This can help to increase voter turnout, and to reduce fraud.
- **Intellectual property:** Blockchain can be used to register and track intellectual property, such as patents, copyrights, and trademarks. This can help to protect intellectual property rights, and to reduce counterfeiting.
- **Real estate:** Blockchain can be used to track the ownership of real estate, and to facilitate real estate transactions. This can help to reduce fraud and errors, and to improve transparency and efficiency.

Applications of blockchain technology

- Here are some of the future applications of blockchain:
- **Stock trading:** Blockchain can be used to create a more efficient and transparent stock trading system. This could reduce costs and increase liquidity.
- **Healthcare data access:** Blockchain can be used to securely store and share healthcare data. This could improve patient care and research.
- **Crowdfunding:** Blockchain can be used to create a more secure and transparent crowdfunding platform. This could make it easier for people to raise money for their projects.
- **Wills and inheritances:** Blockchain can be used to create a more secure and transparent way to store wills and other legal documents. This could help to prevent fraud and disputes.
- **Voting:** Blockchain can be used to create a more secure and transparent voting system. This could increase voter turnout and reduce the risk of fraud.
- **Cloud storage**: Blockchain can be used to create a more secure and decentralized cloud storage system. This could reduce costs and improve privacy.
- **Decentralized credit scoring**: Blockchain can be used to create a more decentralized and transparent credit scoring system. This could improve access to credit for people who are traditionally underserved by the financial system.
- **Charity accountability:** Blockchain can be used to create a more transparent and accountable way to track donations to charities. This could help to ensure that donations are used effectively.

Tiers of blockchain technology

- **Blockchain 1.0**: This tier was introduced with the invention of Bitcoin, and it is primarily used for cryptocurrencies.
- Also, as Bitcoin was the first implementation of cryptocurrencies, it makes sense to categorize this first generation of blockchain technology to include only cryptographic currencies.
- All alternative cryptocurrencies as well as Bitcoin fall into this category. It includes core applications such as payments and applications.
- This generation started in 2009 when Bitcoin was released and ended in early 2010.

- **Blockchain 2.0**: This second blockchain generation is used by financial services and smart contracts.
- This tier includes various financial assets, such as derivatives, options, swaps, and bonds.
- Applications that go beyond currency, finance, and markets are incorporated at this tier.
- Ethereum, Hyperledger, and other newer blockchain platforms are considered part of Blockchain 2.0.
- This generation started when ideas related to using blockchain for other purposes started to emerge in 2010.

Tiers of blockchain technology

- **Blockchain 3.0**: This third blockchain generation is used to implement applications beyond the financial services industry and is used in government, health, media, the arts, and justice.
- Again, as in Blockchain 2.0, Ethereum, Hyperledger, and newer blockchains with the ability to code smart contracts are considered part of this blockchain technology tier.
- This generation of blockchain emerged around 2012 when multiple applications of blockchain technology in different industries were researched.

- **Blockchain X.0**: This generation represents a vision of blockchain singularity where one day there will be a public blockchain service available that anyone can use just like the Google search engine.
- It will be a public and open distributed ledger with general-purpose rational agents (*Machina economicus*) running on a blockchain, making decisions, and interacting with other intelligent autonomous agents on behalf of people, and regulated by code instead of law or paper contracts.
- This does not mean that law and contracts will disappear, instead law and contracts will be implementable in code.

Types of blockchain

- Based on the way that blockchain has evolved over the last few years, it can be divided into multiple categories with distinct though sometimes partially-overlapping attributes.
- These blockchain types can occur on any blockchain tier, as there is no direct relationship between

  those tiers and the various types of blockchain.
- Distributed ledgers
- Distributed Ledger Technology (DLT)
- Blockchains
- Ledgers

Distributed ledgers (Types of blockchain)

- *distributed ledger* is a broad term describing shared databases
- All blockchains technically fall under the umbrella of shared databases or distributed ledgers.
- Although all blockchains are fundamentally distributed ledgers, all distributed ledgers are not

  necessarily a blockchain.
- A critical difference between a distributed ledger and blockchain is that a distributed ledger does not necessarily consist of blocks of transactions to keep the ledger growing.
- Blockchain is a special type of shared database that is comprised of blocks of transactions.
- An example of a distributed ledger that does not use blocks of transactions is R3's Corda. Corda is a distributed ledger which is developed to record and manage agreements and is especially focused on financial services industry.

Distributed ledgers (Types of blockchain)

- On the other hand, more widely-known blockchains like Bitcoin and Ethereum make use of blocks to update the shared database.
- a distributed ledger is distributed among its participants and spread across multiple sites or organizations.
- This type of ledger can be either private or public
- The fundamental idea here is that, unlike many other blockchains, the records are stored contiguously instead of being sorted into blocks.
- This concept is used in Ripple which is a blockchain and cryptocurrency based global payment network.

Distributed Ledger Technology:

- From a financial sector point of view, DLTs are permissioned blockchains that are shared and used

  between known participants.
- DLTs usually serve as a shared database, with all participants known and verified.
- They do not have a cryptocurrency or do not require mining to secure the ledger.

Public blockchains (Types of blockchain)

- As the name suggests, public blockchains are not owned by anyone.
- They are open to the public, and anyone can participate as a node in the decision-making process. Users may or may not be rewarded for their participation.
- All users of these *permissionless* or *unpermissioned* ledgers maintain a copy of the ledger on their local nodes and use a distributed consensus mechanism to decide the eventual state of the ledger.
- Bitcoin and Ethereum are both considered public blockchains.

- **Private blockchains**
- As the name implies, private blockchains are just that—private. That is, they are open only to a consortium or group of individuals or organizations who have decided to share the ledger among themselves.
- There are various blockchains now available in this category, such as HydraChain and Quorum.
- Optionally, both of these blockchains can also run in public mode if required, but their primary purpose is to provide a private blockchain.

Private blockchains(Types of private blockchain)

Semiprivate blockchains

- With *semiprivate blockchains*, part of the blockchain is private and part of it is public.
- Note that this is still just a concept today, and no real world POCs have yet been developed.
- With a semi-private blockchain, the private part is controlled by a group of individuals, while the public part is open for participation by anyone.
- This hybrid model can be used in scenarios where the private part of the blockchain remains internal and shared among known participants, while the public part of the blockchain can still be used by anyone, optionally allowing mining to secure the blockchain.
- This way, the blockchain as a whole can be secured using PoW, thus providing consistency and validity for both the private and public parts.
- This type of blockchain can also be called a *semi-decentralized* model, where it is controlled by a single entity but still allows for multiple users to join the network by following appropriate procedures.

Private blockchains(Types of private blockchain)

Sidechains

- More precisely known as *pegged sidechains*, this is a concept whereby coins can be moved from one blockchain to another and moved back again.
- Typical uses include the creation of new *altcoins* (alternative cryptocurrencies) whereby coins are burnt as a proof of an adequate stake.
- *Burnt* or *burning the coins* in this context means that the coins are sent to an address which is unspendable and this process makes the *burnt* coins irrecoverable. This mechanism is used to bootstrap a new currency or introduce scarcity which results in increased value of the coin.
- This mechanism is also called **Proof of Burn** (**PoB**) and is used as an alternative method for distributed consensus to **PoW** and **Proof of Stake** (**PoS**). The aforementioned example for burning coins applies to a **oneway**
- **pegged sidechain**: The second type is called a **two-way pegged sidechain**, which allows the movement of coins from the main chain to the sidechain and back to the main chain when required.
- This process enables the building of smart contracts for the Bitcoin network. Rootstock is one of the leading examples of a sidechain, which enables smart contract development for Bitcoin using this paradigm.
- It works by allowing a two-way peg for the Bitcoin blockchain, and this results in much faster throughput.

Private blockchains(Types of Private blockhains)

Permissioned ledger

- A *permissioned ledger* is a blockchain where participants of the network are already known and trusted.
- Permissioned ledgers do not need to use a distributed consensus mechanism; instead, an agreement protocol issued to maintain a shared version of the truth about the state of the records on the blockchain.
- In this case, for verification of transactions on the chain, all verifiers are already preselected by a central authority and typically there is no need for a mining mechanism.
- By definition, there is also no requirement for a permissioned blockchain to be private, as it can be a public

  blockchain but with regulated access control.
- For example, Bitcoin can become a permissioned ledger if an access control layer is introduced on top of it that verifies the identity of a user and then allows access to the blockchain.

Shared ledger(Types of blockchain)

- This is a generic term that is used to describe any application or database that is shared by the public or a consortium.
- Generally, all blockchains, fall into the category of a shared ledger.

Fully private and proprietary blockchains(Types of blockchain)

- There is no mainstream application of these types of blockchains, as they deviate from the core concept of decentralization in blockchain technology. It has specific private settings within an organization, there could be a need to share data and provide some level of guarantee of the authenticity of the data.
- An example of this type of blockchain might be to allow for collaboration and the sharing data between various government departments. In that case, no complex consensus mechanism is required, apart from simple state machine replication and an agreement protocol with known central validators. Even in private blockchains,
- tokens are not really required, but they can be used as means of transferring value or representing some real world asset.

Tokenized blockchains(Types of blockchain)

- These blockchains are standard blockchains that generate cryptocurrency as a result of a consensus process via mining or initial distribution.
- Bitcoin and Ethereum are prime examples of this type of blockchain.

Tokenless blockchains(Types of blockchain)

- These blockchains are designed in such a way that they do not have the basic unit for the transfer of value.
- However, they are still valuable in situations where there is no need to transfer value between nodes and only the sharing of data among various trusted parties is required.
- This is similar to full private blockchains, the only difference being that use of tokens is not required. This can also be thought of as a shared distributed ledger used for storing data.
- It does have its benefits when it comes to immutability, security, and consensus driven updates but are not used for common blockchain application of value transfer or cryptocurrency.

Consensus

- Consensus is the backbone of a blockchain and, as a result, it provides decentralization of control through an optional process known as **mining**.
- The choice of the **consensus algorithm** is also governed by the type of blockchain in use; that is, not all consensus mechanisms are suitable for all types of blockchains.
- For example, in public permissionless blockchains, it would make sense to use PoW instead of a simple agreement mechanism that is perhaps based on proof of authority.
- **Consensus** is a process of agreement between distrusting nodes on the final state of data. To achieve consensus, different algorithms are used.
- It is easy to reach an agreement between two nodes (in client-server systems, for example), but when multiple nodes are participating in a distributed system and they need to agree on a single value, it becomes quite a challenge to achieve consensus.
- This process of attaining agreement common state or value among multiple nodes despite the failure of some nodes is known as **distributed consensus**.

Consensus mechanism

- A **consensus mechanism** is a set of steps that are taken by most or all nodes in a blockchain to agree on a proposed state or value.
- There are various requirements that must be met to provide the desired results in a consensus mechanism. The following describes these requirements:
- **Agreement**: All honest nodes decide on the same value
- **Termination**: All honest nodes terminate execution of the consensus process and eventually reach a decision
- **Validity**: The value agreed upon by all honest nodes must be the same as the initial value proposed by at least one honest node
- **Fault tolerant**: The consensus algorithm should be able to run in the presence of faulty or malicious nodes (Byzantine nodes)
- **Integrity**: This is a requirement that no node can make the decision more than once in a single consensus cycle

Consensus in blockchain

- Consensus is a distributed computing concept that has been used in blockchain in order to provide a means of agreeing to a single version of the truth by all peers on the blockchain network.

The following describes the two main categories of consensus mechanisms:

- **Proof-based, leader-election lottery based, or the Nakamoto consensus** whereby a leader is elected at random (using an algorithm) and proposes a final value. This category is also referred to as the fully decentralized or permissionless type of consensus mechanism. This type is well used in the Bitcoin and Ethereum blockchain in the form of a PoW mechanism.

- **BFT-based** is a more traditional approach based on rounds of votes. This class of consensus is also known as the consortium or permissioned type of consensus mechanism

Consensus in blockchain

- BFT-based consensus mechanisms perform well when there are a limited number of nodes, but they do not scale well.
- On the other hand, leader-election lottery based (PoW) type consensus mechanisms scale very well but perform very slowly.
- The consensus algorithms available today, or that are being researched in the context of blockchain, are presented here. The following is not an exhaustive list, but it includes all notable algorithms.
- **Proof of Work (PoW)**: This type of consensus mechanism relies on proof that adequate computational resources have been spent before proposing a value for acceptance by the network.
- This scheme is used in Bitcoin, Litecoin, and other cryptocurrency blockchains.
- Currently, it is the only algorithm that has proven to be astonishingly(extremely surprising or impressive) successful against any collusion attacks on a blockchain network, such as the Sybil attack.

Consensus in blockchain

- **Proof of Stake (PoS)**: This algorithm works on the idea that a node or user has an adequate stake in the system; that is, the user has invested enough in the system so that any malicious attempt by that user would outweigh the benefits of performing such an attack on the network.
- This idea was first introduced by Peercoin, and it is going to be used in the Ethereum blockchain version called *Serenity*.
- Another important concept in PoS is **coin age**, which is a criterion derived from the amount of time and 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 (DPoS)**: This is an innovation over standard PoS, whereby each node that has a stake in the system can delegate the validation of a transaction to other nodes by voting.
- It is used in the BitShares blockchain.

Consensus in blockchain

- **Proof of Elapsed Time (PoET)**: Introduced by Intel in 2016, PoET uses a **Trusted Execution Environment** (**TEE**) to provide randomness and safety in the leader election process via a guaranteed wait time.
- It requires the Intel **Software Guard Extensions** (**SGX**) processor to provide the security guarantee for it to be secure.
- **Proof of Deposit (PoD)**: In this case, nodes that wish to participate in the network have to make a security deposit before they can mine and propose blocks.
- This mechanism is used in the Tendermint blockchain.
- **Proof of Importance (PoI)**: This idea is significant and different from PoS. PoI not only relies on how large a stake a user has in the system, but it also monitors the usage and movement of tokens by the user in order to establish a level of trust and importance.
- It is used in the NEM coin blockchain.

Consensus in blockchain

- **Federated consensus or federated Byzantine consensus**: This mechanism is used in the stellar consensus protocol. Nodes in this protocol retain a group of publicly-trusted peers and propagate only those transactions that have been validated by the majority of trusted nodes.
- **Reputation-based mechanisms**: As the name suggests, a leader is elected by the reputation it has built over time on the network. It is based on the votes of other members.
- **PBFT**: This mechanism achieves state machine replication, which provides tolerance against Byzantine nodes. Various other protocols including PBFT, PAXOS, RAFT, and **Federated Byzantine Agreement** (**FBA**) are also being used or have been proposed for use in many different implementations of distributed systems and blockchains.
- **Proof of Capacity (PoC)**: This scheme uses hard disk space as a resource to mine the blocks. This is different from PoW, where CPU resources are used. In in PoC, hard disk space is utilized for mining and as such is also known as *hard drive mining*. This concept was first introduced in the Burstcoin cryptocurrency.

Consensus in blockchain

- **Proof of Activity (PoA)**: This scheme is a combination of PoS and PoW, which ensures that a stakeholder

is selected in a pseudorandom but uniform fashion.

- This is a comparatively more energy-efficient mechanism as compared to PoW. It utilizes a new concept called *Follow the Satoshi*.
- In this scheme, PoW and PoS are combined together to achieve consensus and good level of security. This scheme is more energy efficient as PoW is used only in the first stage of the mechanism, after the first stage it switches to PoS which consumes negligible energy.
- **Proof of Storage (PoS)**: This scheme allows for the outsourcing of storage capacity.
- This scheme is based on the concept that a particular piece of data is probably stored by a node *which* serves as a means to participate in the consensus mechanism.
- Several variations of this scheme have been proposed, such as Proof of Replication, Proof of Data Possession, Proof of Space, and Proof of Space-Time.

CAP theorem and blockchain

- **CAP theorem**, also known as Brewer's theorem, was introduced by Eric Brewer in 1998 as conjecture. In 2002, it was proven as a theorem by Seth Gilbert and Nancy Lynch.
- The theory states that any distributed system cannot have consistency, availability, and partition tolerance simultaneously:
- **Consistency** is a property which ensures that all nodes in a distributed system have a single, current, and identical copy of the data.
- **Availability** means that the nodes in the system are up, accessible for use, and are accepting incoming requests and responding with data without any failures as and when required. In other words, data is available at each node and the nodes are responding to requests.
- **Partition tolerance** ensures that if a group of nodes is unable to communicate with other nodes due to network failures, the distributed system continues to operate correctly. This can occur due to network and node failures.

CAP theorem and blockchain

- **Consistency** is achieved if both nodes have the same shared state; that is, they have the same up-to-date

  copy of the data.

- **Availability** is achieved if both nodes are up and running and responding with the latest copy of data.
- **Partition tolerance** is achieved if communication does not break down between two nodes (either due to

  network issues, Byzantine faults, and so forth), and they are able to communicate with each other.

- To achieve fault tolerance, replication is used. This is a standard and widely-used method to achieve fault tolerance.
- Consistency is achieved using consensus algorithms in order to ensure that all nodes have the same copy of the data. This is also called **state machine replication**.

CAP theorem and blockchain

- The blockchain is a means for achieving state machine replication. In general, there are two types of faults that a node can experience.
- Both of these types fall under the broader category of faults that can occur in a distributed system:
- **Fail-stop fault**: This type of fault occurs when a node merely has crashed. Fail-stop faults are the easier ones to deal with of the two fault types. Paxos protocol, introduced earlier in this chapter, is normally used to deal with this type of fault. These faults are simple to deal with
- **Byzantine faults**: The second type of fault is one where the faulty node exhibits malicious or inconsistent behavior arbitrarily. This type is difficult to handle since it can create confusion due to misleading information.
- This can be a result of an attack by adversaries, a software bug, or data corruption.
- State machine replication protocols such as PBFT was developed to address this second type of faults.

CAP theorem and blockchain

- Strangely, it seems that the CAP theorem is violated in the blockchain, especially in its most successful

  implementation, Bitcoin.

- 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.
- The concept of mining was introduced in Bitcoin for this purpose.
- **Mining** is a process that facilitates the achievement of consensus by using the PoW consensus algorithm.
- At a higher level, mining can be defined as a process that is used to add more blocks to the blockchain.

Benefits and limitations of blockchain

- The notable benefits of blockchain technology are as follows:
- **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.

Benefits and limitations of blockchain

- **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**: 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.

Benefits and limitations of blockchain

- **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. The most sensitive blockchain problems

  are as follows:

- Scalability
- Adaptability
- Regulation
- Relatively immature technology
- Privacy