

BLOCKCHAIN TECHNOLOGY
(BCS613A)

Module 1

Syllabus:

Distributed systems, CAP theorem, Byzantine Generals problem, Consensus. The history of blockchain, Introduction to blockchain, Various technical definitions of blockchains, Generic elements of a blockchain, Features of a blockchain, Applications of blockchain technology, Tiers of blockchain technology, Consensus in blockchain, CAP theorem and blockchain, Benefits and limitations of blockchain.

Textbook:

1. Imran Bashir. “Mastring BlockChain”, Third Edition, Packt – 2020

Reference Book:

1. Andreas M. , Mastering Bitcoin: Programming the Open Blockchain – O’rielly – 2017

Module 1

1.1 Distributed Systems:

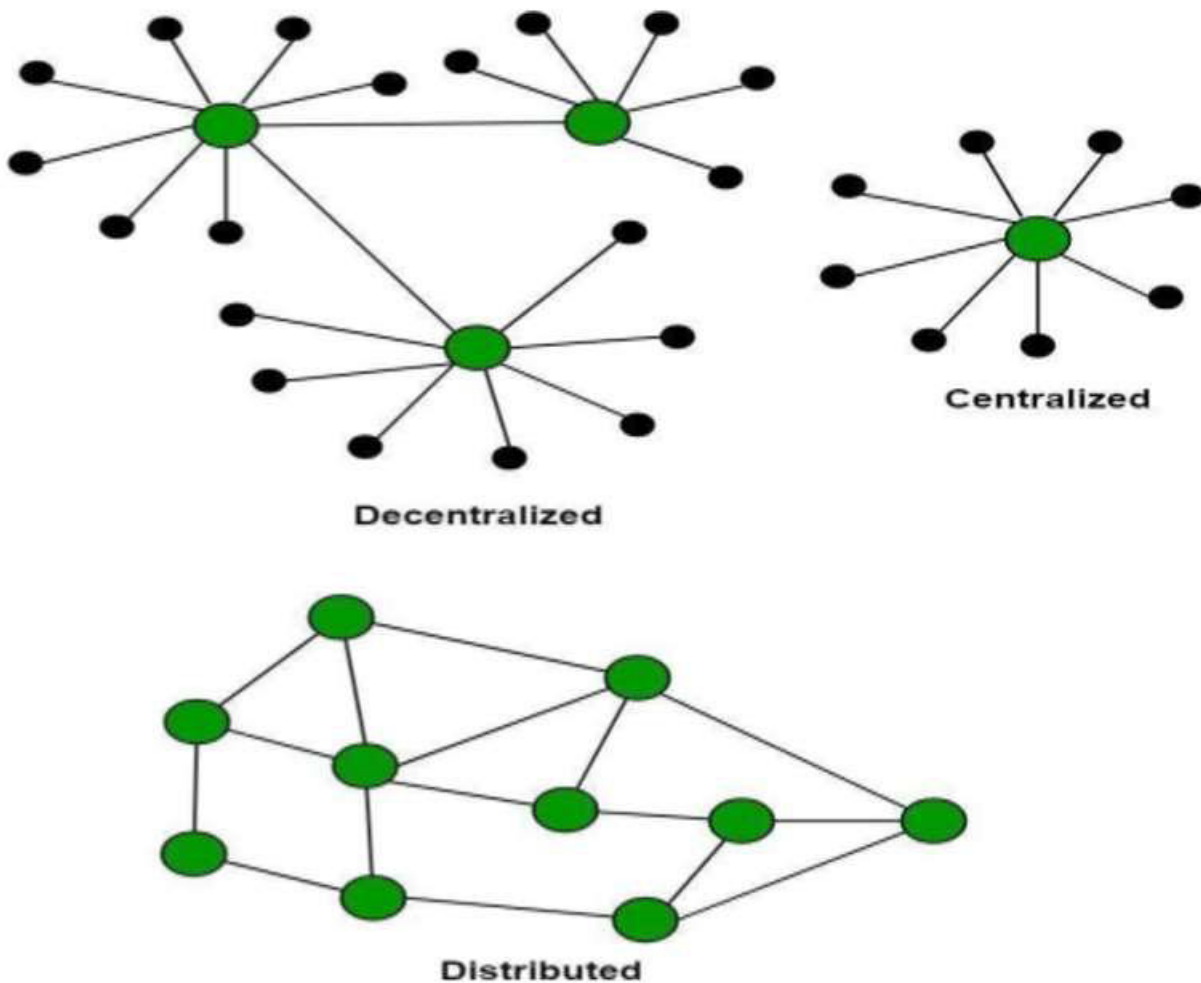
Understanding distributed systems is essential to our understanding blockchain, as blockchain was a distributed system at its core. It is a distributed ledger that can be centralized or decentralized. A blockchain is originally intended to be and is usually used as a decentralized platform. It can be thought of as a system that has properties of the both decentralized and distributed paradigms. It is a decentralized-distributed system.

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. For example, Google's search engine is based on a large distributed system; however, to a user, it looks like a single, coherent platform.

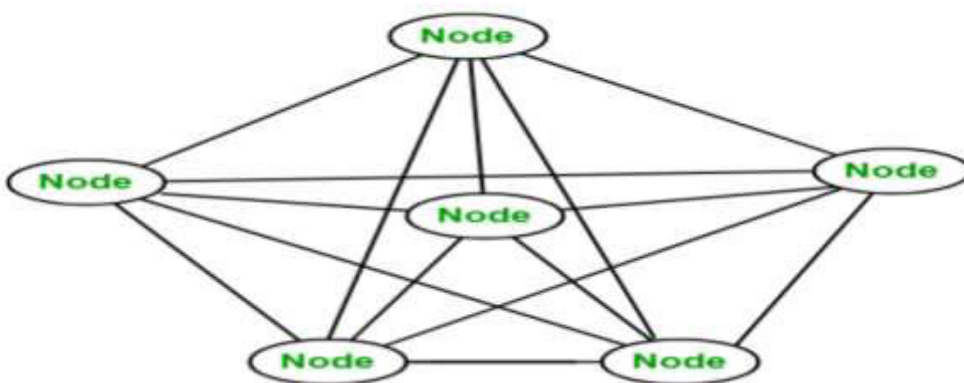
A **node** can be defined as an individual player in a distributed system. All nodes are capable of sending and receiving messages to and from each other. There is no Central Server or System which keeps the data of Blockchain. The data is distributed over Millions of Computers around the world which are connected with the Blockchain. This system allows Notarization of Data as it is present on every Node and is publicly verifiable. 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.

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. This arbitrary behavior can be intentionally malicious, which is detrimental to the operation of the network. Generally, any unexpected behavior of a node on the network can be categorized as Byzantine. This term arbitrarily encompasses any behavior that is unexpected or malicious.

The main challenge in distributed system design is coordination between nodes and fault tolerance. Even if some of the nodes become faulty or network links break, the distributed system should tolerate this and should continue to work flawlessly in order to achieve the desired result. This has been an area of active research for many years and several algorithms and mechanisms has been proposed to overcome these issues.



A network of nodes: A node is a computer connected to the Blockchain Network. Node gets connected with Blockchain using the client. Client helps in validating and propagates transaction on to the Blockchain. When a computer connects to the Blockchain, a copy of the Blockchain data gets downloaded into the system and the node comes in sync with the latest block of data on Blockchain. The Node connected to the Blockchain which helps in the execution of a Transaction in return for an incentive is called Miners.



Disadvantages of current transaction system:

- Cash can only be used in low amount transaction locally.
- Huge waiting time in the processing of transactions.
- Need to third party for verification and execution of Transaction make the process complex.
- If the Central Server like Banks is compromised, whole System is affected including the participants.
- Organization doing validation charge high process thus making the process expensive.

1.2 Building trust with Blockchain:

Blockchain enhances trust across a business network. It's not that you can't trust those who you conduct business with its that you don't need to when operating on a Blockchain network.

Blockchain builds trust through the following five attributes:

- **Distributed:** The distributed ledger is shared and updated with every incoming transaction among the nodes connected to the Blockchain. All this is done in real-time as there is no central server controlling the data.
- **Secure:** There is no unauthorized access to Blockchain made possible through Permissions and Cryptography .
- **Transparent:** Because every node or participant in Blockchain has a copy of the Blockchain data, they have access to all transaction data. They themselves can verify the identities without the need for mediators.
- **Consensus-based:** All relevant network participants must agree that a transaction is valid. This is achieved through the use of consensus algorithms.
- **Flexible:** Smart Contracts which are executed based on certain conditions can be written into the platform. Blockchain Network can evolve in pace with business processes.

1.3 CAP theorem:

The CAP theorem, also known as Brewer's theorem, was introduced by Eric Brewer in 1998 as a conjecture. In 2002, it was proven 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, current, and identical copy of the data. 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. The blockchain is a means for achieving state machine replication.
- Availability means that the nodes in the system are up, accessible for use, and are accepting

VI SEM

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. The CAP theorem states that a distributed database system has to make a tradeoff between Consistency and Availability when a Partition occurs. A distributed database system is bound to have partitions in a real-world system due to network failure or some other reason. The CAP Theorem is comprised of three components (hence its name) as they relate to distributed data stores:

Consistency. All reads receive the most recent write or an error.

Availability. All reads contain data, but it might not be the most recent.

Partition tolerance. The system continues to operate despite network failures (ie; dropped partitions, slow network connections, or unavailable network connections between nodes.)

In normal operations, your data store provides all three functions. But the CAP theorem maintains that when a distributed database experiences a network failure, you can provide either consistency or availability. It's a tradeoff. All other times, all three can be provided. But, in the event of a network failure, a choice must be made. In the theorem, partition tolerance is a must. The assumption is that the system operates on a distributed data store so the system, by nature, operates with network partitions. Network failures will happen, so to offer any kind of reliable service, partition tolerance is necessary—the P of CAP. That leaves a decision between the other two, C and A. When a network failure happens, one can choose to guarantee consistency or availability:

- High consistency comes at the cost of lower availability.
- High availability comes at the cost of lower consistency.

1.4 Byzantine Generals problem

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. Nodes can be honest, faulty, or malicious, and they have memory and a processor. A node that exhibits irrational behavior is also known as a Byzantine node after the Byzantine Generals problem. This type of inconsistent behavior of Byzantine nodes can be intentionally malicious, which is detrimental to the operation of the network. Any unexpected behavior by a node on the network, whether malicious or not, can be categorized as Byzantine.

A small-scale example of a distributed system is shown in the following diagram. 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 a partition in the network. The primary challenge of a distributed system design is the coordination between nodes and fault tolerance. Even if some (a certain threshold dictated by the

VI SEM

consensus protocol) 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.

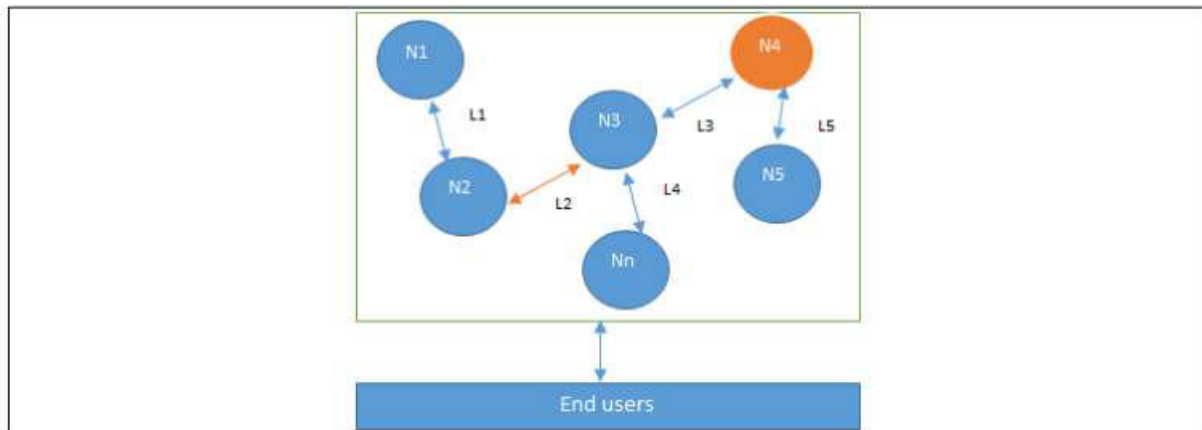


Figure 1.3: Design of a distributed system: N4 is a Byzantine node and L2 is broken or a slow network link

Fig 1.1: Byzantine node

This problem has been an active area of distributed system design research for many years, and several algorithms and mechanisms have been proposed to overcome these issues. Distributed systems are so challenging to design that a theory 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.

1.5 Consensus

Consensus is the backbone of a blockchain, as it provides the decentralization of control. The choice of the consensus algorithm to utilize is governed by the type of blockchain in use; ie 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 mechanisms that are more suitable for permissioned blockchains, such as Proof of Authority (PoA) or traditional Byzantine fault-tolerant consensus mechanisms. Therefore, it is essential to choose an appropriate consensus algorithm for a particular blockchain project. **Consensus** is a process of achieving 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 on a common state or value among multiple nodes even though the failure of some nodes is known as distributed consensus.

1.6 History of Blockchain

In 1991, researcher scientists named Stuart Haber and W. Scott Stornetta introduce Blockchain

VI SEM

Technology. These scientists wanted some Computational practical Solution for time-stamping the digital documents so that they couldn't be tempered or misdated. So both scientists together developed a system with the Cryptography. In this System, the time-stamped documents are stored in a Chain of Blocks. After that in 1992, Merkle Trees formed a legal corporation by using a system developed by Stuart Haber and W. Scott Stornetta with some more features. Hence, Blockchain Technology became efficient to store several documents to be collected into one block. Merkle used a Secured Chain of Block which stores multiple data records in a sequence. However, this Technology became unused when Patent came into existence in 2004. However, in the same year 2004, Cryptographic activist Hal Finney introduced a system for digital cash known as "Reusable Proof of Work". This step was the game-changer in the history of Blockchain and Cryptography. This System helps others to solve the Double Spending Problem by keeping the ownership of tokens registered on a trusted server.

After that in 2008, Satoshi Nakamoto conceptualized the concept of "Distributed Blockchain" under his white paper: "A Peer to Peer Electronic Cash System". He modified the model of Merkle Tree and created a system that is more secure and contains the secure history of data exchange. His System follows a peer- to- peer network of time stamping. His system became so useful that Blockchain become the backbone of the Cloud Cryptography. After that, the evolution of Blockchain is steady and promising and became a need in various fields. Blockchain technology is so secure that the following surprising news will give proof about that. A person named, James Howells was an IT worker in the United Kingdom, he starts mining bitcoins which are part of Blockchain in 2009 and stopped this in 2013. He spends \$17,000 on it and after he stopped he sells the parts of his laptop on eBay and keep the drive with him so that when he needs to work again on bitcoin he will utilize it but while cleaning his house in 2013, he thrashed his drive with garbage and now his bitcoins cost nearly \$127 million. This money now remains unclaimed in the Bitcoin system.

The blockchain is the public ledger of all Bitcoin transactions that have ever been executed. It is constantly growing as miners add new blocks to it (every 10 minutes) to record the most recent transactions. The blocks are added to the blockchain in a linear, chronological order. Each full node (i.e., every computer connected to the Bitcoin network using a client that performs the task of validating and relaying transactions) has a copy of the blockchain, which is downloaded automatically when the miner joins the Bitcoin network. The blockchain has complete information about addresses and balances from the genesis block (the very first transactions ever executed) to the most recently completed block. Blockchain is the backbone Technology of Digital Cryptocurrency BitCoin. The blockchain is a distributed database of records of all transactions or digital event that have been executed and shared among

VI SEM

participating parties. Each transaction verified by the majority of participants of the system. It contains every single record of each transaction.

BitCoin is the most popular cryptocurrency an example of the blockchain. Blockchain Technology Records. Transaction in a Digital Ledger which is distributed over the Network thus making it incorruptible.

Anything of value like Land Assets, Cars, etc. can be recorded on Blockchain as a Transaction. One of the famous use of Blockchain is Bitcoin. The bitcoin is a cryptocurrency and is used to exchange digital assets online. Bitcoin uses cryptographic proof instead of third-party trust for two parties to execute transactions over the internet. Each transaction protects through digital signature.

1.7 Introduction to Blockchain

- In 2008, a groundbreaking paper, entitled “Bitcoin: A Peer-to-Peer Electronic Cash System”, was written under the pseudonym of Satoshi Nakamoto.
- No one knows the actual identity of Satoshi Nakamoto. After introducing Bitcoin in 2009, he remained active in the Bitcoin developer community until 2011.
- He then handed over Bitcoin development to its core developers and simply disappeared.

Blockchain defined

1. **Layman's definition:** Blockchain is an ever-growing, secure, shared recordkeeping system in which each user of the data holds a copy of the records, which can only be updated if all parties involved in a transaction agree to update.
2. **Technical definition:** Blockchain is a *peer-to-peer, distributed ledger* that is *cryptographically secure, append-only*, immutable (extremely hard to change), and *updateable via consensus* or agreement among peers.
3. **Peer-to-peer :** There is no central controller in the network, and all participants (nodes) talk to each other directly. This property allows for transactions to be conducted directly among the peers without third-party involvement, such as by a bank.
4. **Distributed ledger :** Blockchain is a "distributed ledger," which 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.
5. **Cryptographically secure :** Cryptography has been used to provide security services that make this ledger secure against tampering and misuse. These services include non-repudiation, data integrity, and data origin authentication.
6. **Append-only :** Data can only be added to the blockchain in time-sequential order. This property implies that once data is added to the blockchain, it is almost impossible to change that data and it can be considered practically immutable.

7. **Updatable via consensus** : Blockchain is updateable only via consensus. This leads to decentralization. No central authority is in control of updating the ledger. To achieve consensus, there are various consensus facilitation algorithms that ensure all parties agree on the final state of the data on the blockchain network and resolutely agree upon it to be true.

1.8 Blockchain architecture:

Blockchain by layers

Blockchain can be thought of as a layer of a distributed peer-to-peer network running on top of the internet. It is analogous to SMTP, HTTP, or FTP running on top of TCP/IP:

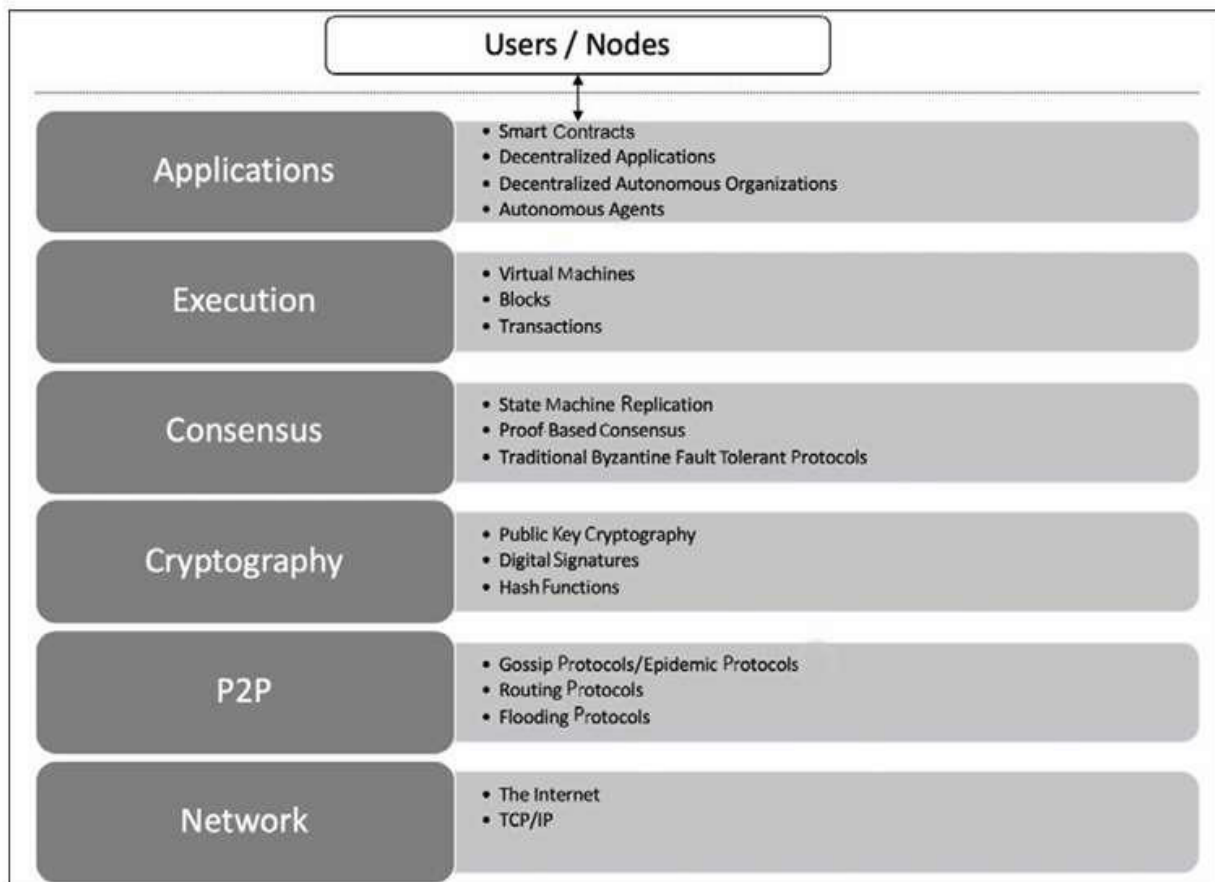


Fig 1.2 : The architectural view of a generic blockchain

Blockchain in business

- A blockchain can be defined as a platform where peers can exchange value/e-cash using transactions without the need for a centrally trusted arbitrator.
- This disintermediation allows blockchain to be a decentralized consensus mechanism.

If no banks or central clearing houses are required, then it leads to cost savings, faster transaction speeds, and more trust.

1.9 Generic elements of a blockchain

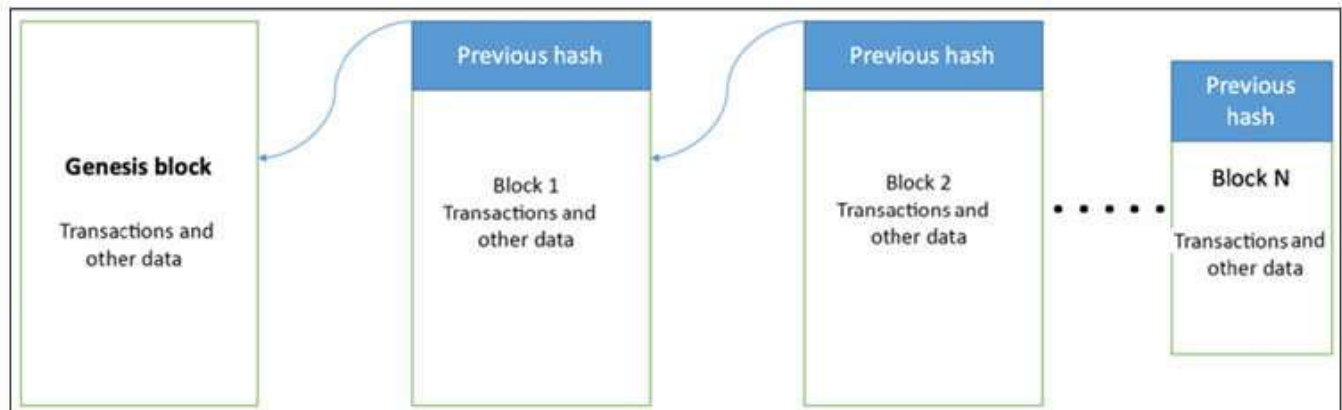


Fig 1.3 Generic structure of a blockchain

Elements in blockchain:

1. **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.
2. **Transaction:** A transaction is the fundamental unit of a blockchain. A transaction represents a transfer of value from one address to another.
3. **Block:** A block is composed of multiple transactions and other elements. A block is composed of a block header and a selection of transactions bundled together and organized logically.

A block contains the following elements:

- **A reference to a previous block** is also included in the block unless it is a genesis block. This reference is the hash of the header of the previous block.
- A block also includes the **nonce** value for transaction replay protection.
- A **timestamp** is the creation time of the block.
- **Merkle root** in a blockchain block is the combined hash of the transactions in the block. Merkle trees are widely used to validate large data structures securely and efficiently.
- The block contains **transactions** that make up the block body. A transaction is a record of an event.

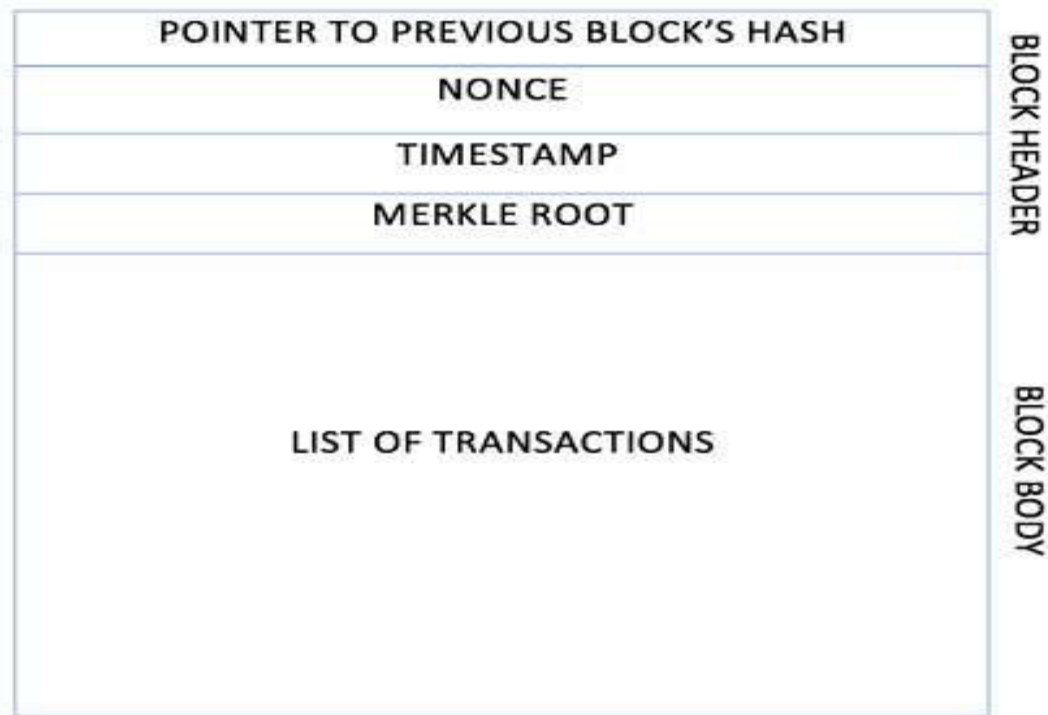


Fig 1.4 The generic structure of a block

Peer-to-peer network: is a network topology wherein all peers can communicate with each other and send and receive messages.

The scripting or programming language:

- In Bitcoin, transaction scripts are predefined in a language called **Script**, which consists of sets of commands that allow nodes to transfer bitcoins from one address to another.
- Script is a limited language, that only allows essential operations that are necessary for executing transactions.
- To facilitate arbitrary program development on a blockchain, a **Turing complete** programming language is needed

Virtual machine:

- A virtual machine allows Turing complete code to be run on a blockchain (as smart contracts). However, virtual machines are not available on all blockchains.
- Various blockchains use **Ethereum Virtual Machine (EVM)** and **Chain Virtual Machine (CVM)**.
- EVM is used in the **Ethereum blockchain**, while CVM is 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 as a result of transaction execution.

Smart contracts:

- These programs run on top of the blockchain and encapsulate the **business logic** to be executed when certain conditions are met.

Node:

- A node can **validate transactions** and **perform mining** to facilitate consensus.
- This goal is achieved by following a **consensus protocol** (most commonly PoW).
- Nodes can also perform other functions such as **simple payment verification**.
- Nodes also perform a **transaction signing function**.
- 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.
- There are also standards related to tokens; on Ethereum, there are **ERC20, ERC721**.
- These programs are enforceable and **automatically executable**.
- The smart contract feature is not available on all blockchain platforms.
- Smart contracts have many use cases, not limited to **identity management, capital markets, trade finance, record management, insurance, and e-governance**.

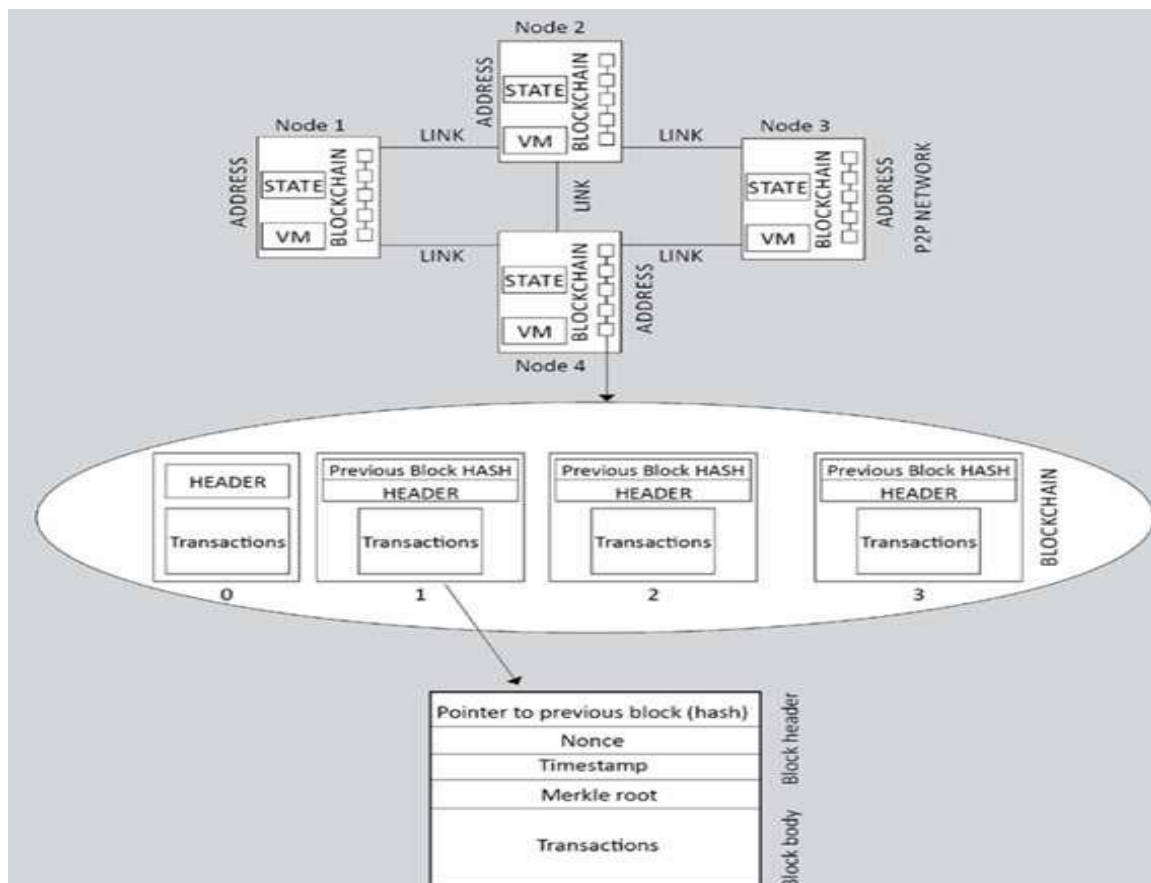


Fig 1.5 Generic structure of a blockchain network

How blockchain works

- Nodes are either miners who create new blocks and mint cryptocurrency (coins) or block signers who validate and digitally sign the transactions.
- A critical decision that every blockchain network has to make is to figure out which node will append the next block to the blockchain.
- This decision is made using a consensus mechanism.
- General scheme for **creating blocks**. It gives a **General idea of how blocks are** generated and what the relationship is between **transactions and blocks**.

Transaction is initiated:

- A node **starts a transaction** by first creating it and then **digitally signing** it with its private key.
- A **transaction** can represent various actions in a blockchain.
- Most commonly, this is a **data structure** that represents the **transfer of value** between **users on the blockchain network**.
- The transaction data structure usually consists of some **logic of transfer of value**, related rules, source and destination addresses, and other validation information.
- Transactions are usually either a cryptocurrency transfer (transfer of value) or smart contract call that can perform any desired operation.
- A transaction occurs between two or more parties.

Transaction is validated and broadcast:

- A transaction is propagated (broadcast) usually by using data-dissemination protocols, such as Gossip protocol, to other peers that validate the transaction based on specific validity criteria.
- Before a transaction is propagated, it is also verified to ensure that it is valid.

Find new block:

- When the **transaction is received** and validated by special participants called miners on the blockchain network, it is included in a block, and the **process of mining starts**.
- This process is also sometimes referred to as "**finding a new block**."
- Here, nodes called miners race to finalize the block they've created by a process known as mining.

New block found:

- Once a miner solves a mathematical puzzle (or fulfills the requirements of the consensus mechanism implemented in a blockchain), the block is considered "found" and finalized.
- At this point, the transaction is considered confirmed.
- Usually, in cryptocurrency blockchains such as Bitcoin, the miner who solves the mathematical puzzle is also rewarded with a certain number of coins as an incentive for their effort and the

resources they spent in the mining process.

Add new block to the blockchain:

- The newly created block is validated, transactions or smart contracts within it are executed, and it is propagated to other peers.
- Peers also validate and execute the block.
- It now becomes part of the blockchain (ledger), and the next block links itself cryptographically back to this block.
- This link is called a hash pointer.
- **Transaction complete:** As soon as the block is added to the blockchain the transaction is completed and the details of this transaction are permanently stored in the block. Anyone can fetch the details of the transaction and confirm the transaction.

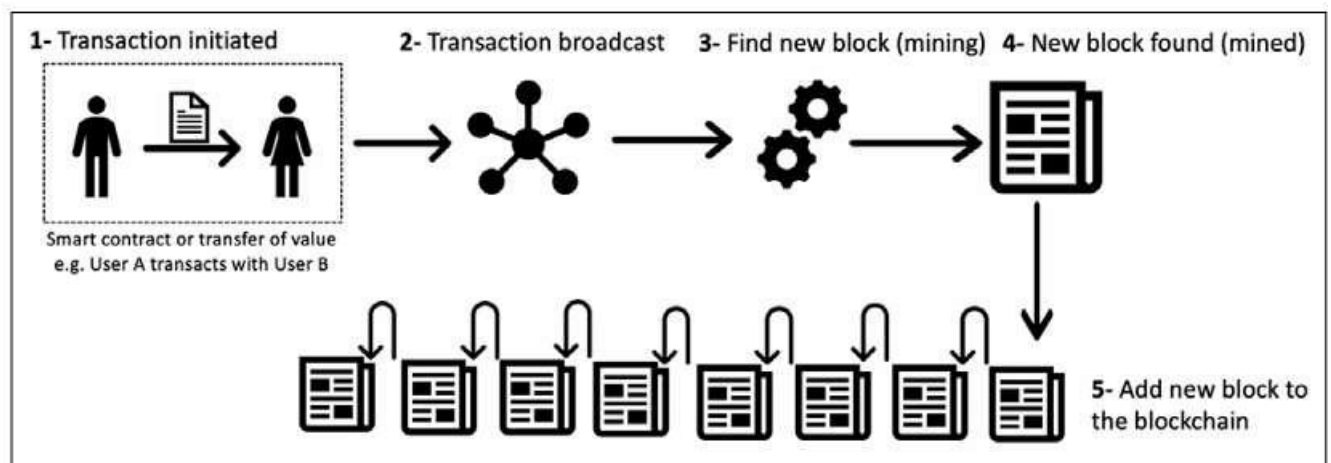


Fig 1.6 How a block is generated

1.10 Benefits, features, and limitations of blockchain

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

1. Decentralization:

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.

2. Transparency and trust:

As 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.

3. 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.

4. 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.

5. Highly secure:

- All transactions on a blockchain are cryptographically secured and thus provide network integrity.
- Any transactions posted from the nodes on the blockchain are verified based on a predetermined set of rules.
- Only valid transactions are selected for addition in a block.
- 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 the privacy and confidentiality of transactions.
- As such, the privacy and confidentiality of transactions on the blockchain are being researched very actively, and advancements are already being made.
- 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.

6. 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 different 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.

7. 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, understanding, and clearance because a single version of agreed-upon data is already available on a shared ledger between financial organizations.

8. 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.

9. Platform for smart contracts:

- A blockchain is a platform on which programs can run that execute business judgement on behalf of the users.
- This is a very useful feature but not all blockchains have a mechanism to execute smart contracts.
- It is available on platforms such as Ethereum and MultiChain, but not on Bitcoin.

10. Smart property:

- It is possible to link a digital or physical asset to the blockchain in such a secure and detailed 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.
- Compare this with a digital music file, for example, which can be copied many times without any controls.
- While it is true that many Digital Rights Management (DRM)schemes are being used currently along with copyright laws, none of them are enforceable in the way a blockchain-based DRM can be.
- Blockchain can provide digital rights management functionality in such a way that it can be enforced fully.
- There are famously broken DRM schemes that looked great in theory but were hacked due to one limitation or another.
- Copyrighted digital music, films, and e-books are routinely shared on the internet without any limitations.
- We have had 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.
- This feature has far-reaching implications, especially in DRM and e-cash systems where double-spend detection is a crucial requirement.
- The double-spend problem was first solved without the requirement of a trusted third party in Bitcoin.
- 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 stood by blockchain technology

1.11 Blockchain problems are as follows:

1. Scalability: Currently, blockchain networks are not as scalable as, for example, current financial networks.

2. Adoption: Often, blockchain is seen as a emerging technology. Even though this perspective is rapidly changing, there is still a long way to go before the mass agreement of this technology. The challenge here is to allow blockchain networks to be easier to use so that adoption can increase. several other challenges such as scalability (introduced previously) exist, which must be solved in order to increase adoption.

3. Regulation: Due to its decentralized nature, **regulation is almost impossible** on blockchain. This is sometimes seen as a barrier toward adoption because, traditionally, due to the existence of regulatory authorities, consumers have a certain level of confidence that if something goes wrong they can hold someone accountable. However, in blockchain networks, no such regulatory authority and control exists, which is an avoiding factor for many consumers.

4. Relatively immature technology: As compared to traditional IT systems that have benefited from decades of research, blockchain is still a new technology and requires a lot of research to achieve development.

5. Privacy and confidentiality: Privacy is a concern on public blockchains such as Bitcoin where everyone can see every single transaction. This transparency is not desirable in many industries such as the financial, law, or medical sectors. This is also a known concern and a lot of valuable research with some perfect solutions has already been developed. further research is still required to drive the mass adoption of blockchain.

1.12 Types of blockchain

Blockchain has evolved over the last few years, categorization of blockchain, based upon its evolution and usage . Different types of blockchains from a technical and business use perspective. The various types of blockchain are:

- Distributed ledgers
- Distributed Ledger Technology (DLT)
- Blockchains
- Ledgers
- **Types of blockchain** Blockchain technology has evolved into a versatile tool with various applications across industries. Understanding the different types of blockchain is essential for selecting the right solution

VI SEM

- **for specific needs.**
- Broadly categorized into **public, private, consortium, and hybrid blockchains**, each type offers unique characteristics, benefits, and use cases.
- **Public blockchains** enable open access and decentralization, while **private blockchains** prioritize security and control.
- **Consortium blockchains** serve collaborative networks, and **hybrid blockchains** combine features of both public and private models.

Distributed ledgers

- Distributed ledger is a broad term describing shared databases;
- hence, 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 blockchains.
- A critical difference between a distributed ledger and a blockchain is that a distributed ledger does not necessarily consist of blocks of transactions to keep the ledger growing.
- Rather, a blockchain is a special type of shared database that is comprised of blocks of transactions.
- **Corda** is a distributed ledger that is developed to record and manage agreements and is especially focused on the financial services industry.
- 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

- over the last few years, the terms distributed ledger or DLT have grown to be commonly used to describe **blockchain in the finance industry**.
- Sometimes, blockchain and DLT are used interchangeably.
- In fact, DLT is now a very active and booming area of research in the financial sector.
- From a financial sector point of view, DLTs are permissioned blockchains that are used by groups.

- **VI SEM**

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

Public Blockchain

- These blockchains are completely open to following the idea of decentralization.
- They don't have any restrictions, anyone having a computer and internet can participate in the network.
- As the name is public this blockchain is open to the public, which means it is not owned by anyone.
- Anyone having internet and a computer with good hardware can participate in this public blockchain.
- All the computers in the network hold the copy of other nodes or blocks present in the network
- In this public blockchain, we can also perform verification of transactions or records.

Advantages:

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

- **Disadvantages:**

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

- **Examples**

- Bitcoin and Ethereum are both considered public blockchains.

Private Blockchain

- These blockchains are not as decentralized as the public blockchain only selected nodes can participate in the process, making it more secure than the others.

VI SEM

- These are not as open as a public blockchain.
- They are open to some authorized users only.
- These blockchains are operated in a closed network.
- In this few people are allowed to participate in a network within a company/organization.
- **Use Cases:**
- With proper security and maintenance, this blockchain is a great asset to secure information without exposing it to the public eye.
- Therefore companies use them for internal auditing, voting, and asset management.
- An example of private blockchains is Hyperledger, Corda.

Advantages:

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

Disadvantages:

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

Use Cases:

- With proper security and maintenance, this blockchain is a great asset to secure information without exposing it to the public eye.
- Therefore companies use them for internal auditing, voting, and asset management.
- An example of private blockchains is Hyperledger, Corda.

Hybrid Blockchain(semi-private)

- It is the mixed content of the private and public blockchain, where some part is controlled by some organization and other makes are made visible as a public blockchain.
- It is a combination of both public and private blockchain.
- Permission-based and permissionless systems are used.

VI SEM

- User access information via smart contracts
- Even if a primary entity owns a hybrid blockchain it cannot alter the transaction

Advantages:

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

Disadvantages:

- **Efficiency:** Not everyone is in a position to implement a hybrid Blockchain.
- The organization also faces some difficulty in terms of efficiency in maintenance.
- **Transparency:** There is a possibility that someone can hide information from the user.
- If someone wants to get access through a hybrid blockchain it depends on the organization whether they will give or not.
- **Ecosystem:** Due to its closed ecosystem this blockchain lacks the incentives for network participation.

Use Case:

- It provides a greater solution to the healthcare industry, government, real estate, and financial companies.
- It provides a remedy where data is to be accessed publicly but needs to be protected privately.
- Examples of Hybrid Blockchain are the Ripple network and XRP token.

Sidechains

- coins can be moved from one blockchain to another and then back again.
- 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 that is un-spendable, and this process makes the "burnt" coins irrecoverable.
- This mechanism is used to bootstrap a new currency or introduce scarcity, which results in the increased value of the coin.

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;

VI SEM

- Instead, an agreement protocol is used 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 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 planned 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

- 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

- A need to share data and provide some level of guarantee of the authenticity of the data.
- A fully private and proprietary blockchain is a type of blockchain network that restricts access only to authorized users.
- An example of this type of blockchain might be to allow for collaboration and the sharing of data between various government departments.
- In that case, no complex consensus mechanism is required, apart from simple SMR and an agreement protocol with known central validators.

Tokenized blockchains

- 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

- These blockchains are designed in such a way that they do not have the basic unit for the transfer of value.
- 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 fully private blockchains, the only difference being that the use of tokens is not required.
- This can also be thought of as a shared distributed ledger used for storing and sharing data between the participants.

- Most of the permissioned blockchains can be seen as an example of tokenless blockchains, for example, Hyperledger Fabric or Quorum.
- Tokens can be built on these chains as an application, but basically these blockchains do not have a token associated with them.

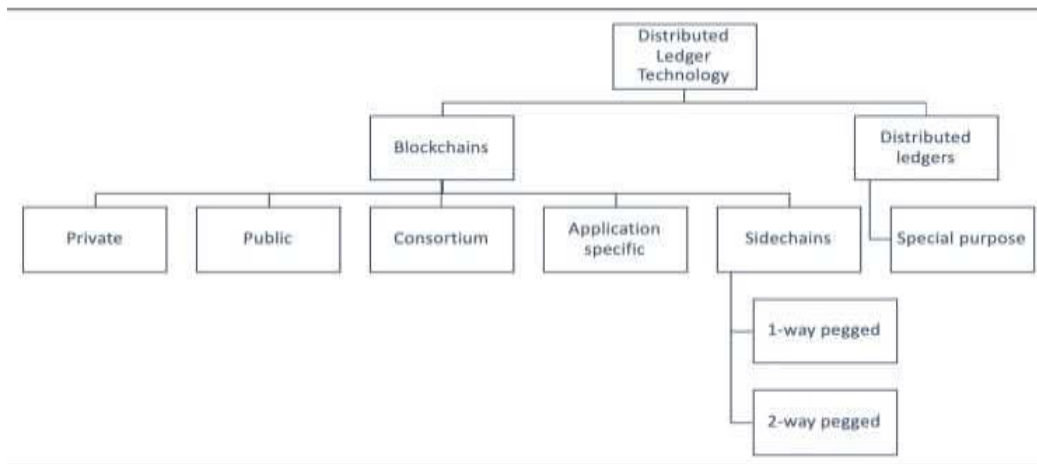


Figure 1.10: DLT hierarchy

Fig 1.7:DLT Hierarchy

- **Consensus** is a process of achieving 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 on a common state or value among multiple nodes even though the failure of some nodes is known as distributed consensus.
- Blockchain is a distributed decentralized network that **provides immutability, privacy, security, and transparency**.
- There is no central authority present to validate and verify the transactions,.
- This is possible only because of the presence of the **consensus protocol** which is a core part of any Blockchain network.
- A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a **common agreement** about the present state of the distributed ledger.
- consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment.
- Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain.

VI SEM

- The Blockchain consensus protocol consists of some specific objectives such as **coming to an agreement, collaboration, cooperation, equal rights to every node, and mandatory participation** of each node in the consensus process.
- Thus, a consensus algorithm aims at finding a common agreement that is a win for the entire network.

1.13 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.
- For more than three decades, this concept has been researched by computer scientists in industry and academia.
- With the beginning of blockchain and Bitcoin, consensus mechanisms have come into the fame again and gained considerable popularity.
- There are **various requirements for a consensus mechanism**.
- **Agreement:** All honest nodes decide on the same value.
- **Integrity:** This is a requirement that no node can make the decision more than once in a single consensus cycle.
- **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 correctly in the presence of faulty or malicious nodes (Byzantine nodes).
- **Termination:** All honest nodes terminate the execution of the consensus process and eventually reach a decision.
- **Types of consensus mechanisms**
- All consensus mechanisms are developed to deal with faults in a distributed system and to allow distributed systems to reach a final state of agreement.
- There are two general categories of consensus mechanisms.
- These categories deal with all types of faults (fail-stop types).
- **Traditional fault tolerance-based:**
- With no compute-intensive operations, such as partial hash reversal(as in Bitcoin PoW), this type of consensus mechanism relies on a simple scheme of nodes that publish and verify signed messages in a number of phases.
- Eventually, when a certain number of messages are received over a period of rounds (phases), then an agreement is reached.
- To achieve fault tolerance, replication is used.
- This is a standard and widely used method to achieve fault tolerance.

VI SEM

- There are two types of faults that a node can experience.

These common types of consensus mechanisms are as follows:

- **Proof-based consensus mechanisms:** This arrangement requires nodes to contest in a leader-election lottery, and the node that wins proposes the final value.
- The **algorithm works** on the principle of providing **proof of some work** and the control of some authority or tokens to win the right of proposing the next block.
- **For example**, the PoW mechanism used in Bitcoin falls into this category, where a miner who solves the computational puzzle as **proof of computational effort** expended wins the right to add the next block to the blockchain.
- **Fail-stop faults:**
 - This type of fault occurs when a node simply has crashed.
 - Fail-stop faults are the easier ones to deal with of the **two fault types**.
 - Paxos or the RAFT protocol, normally used to deal with this type of fault. These faults are simpler 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 opponents, a software bug, or data corruption.
- SMR protocols such as Practical Byzantine Fault Tolerance (PBFT) was developed to address this second type of faults
- Many other implementations of consensus protocols have been proposed in traditional distributed systems.
- Paxos is the most famous of these protocols.
- It was introduced by Leslie Lamport in 1989.
- With Paxos, nodes are assigned various roles such as Proposer, Acceptor, and Learner.
- Nodes or processes are named replicas, and consensus is achieved in the presence of faulty nodes by an agreement among a majority of nodes.
- An alternative to Paxos is RAFT, which works by assigning any of three states; that is, Follower, Candidate, or Leader to the nodes.
- A Leader is elected after a Candidate node receives enough votes, and all changes then have to go through the Leader.
- The Leader commits the proposed changes once replication on the majority of the follower nodes is completed.

Consensus in blockchain

- Consensus is a distributed computing concept that has been used in blockchain in order to

Consensus means of agreeing to a single version of the truth by all peers on the blockchain network.

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.
- **Byzantine fault tolerance (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.
- 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) 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 as follows:
- 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) consensus mechanisms scale very well but perform very slowly.
- The consensus algorithms available today, or that are being researched in the context of blockchain.
- The consensus algorithms available today are:
- **Proof of Work (PoW):** This type of consensus mechanism depends on proof that suitable computational resources have been spent before proposing a value for acceptance by the network.
- This consensus algorithm is used to select a miner for the next block generation.
- Bitcoin uses this PoW consensus algorithm.
- The central idea behind this algorithm is to solve a complex mathematical puzzle and easily give out a solution.
- This mathematical puzzle requires a lot of computational power and thus, the node who solves the puzzle as soon as possible gets to mine the next block.
- **Proof of Stake (PoS):** This is the most common alternative to PoW. Ethereum has shifted from PoW to PoS consensus.
- In this type of consensus algorithm, instead of investing in expensive hardware to solve a

VI SEM

- complex puzzle, validators invest in the coins of the system by locking up some of their coins as stakes.
- After that, all the validators will start validating the blocks.
- Validators will validate blocks by placing a bet on them if they discover a block that they think can be added to the chain.
- Based on the actual blocks added in the Blockchain, all the validators get a reward proportionate to their bets, and their stake increase accordingly.
- In the end, a validator is chosen to generate a new block based on its economic stake in the network.
- Thus, PoS encourages validators through an incentive mechanism to reach to an agreement.
- **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.
- **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 SGX (Software Guard Extensions) 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.
- **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.
- **Practical Byzantine Fault Tolerance (PBFT):** This mechanism achieves SMR, 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 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 a 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 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 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
- **Proof of Storage:** 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.
- **Proof of Authority (PoA):** This scheme utilizes the identity of the participants called validators as a stake on the network. Validators are known and have the authority to propose new blocks. Validators propose the new blocks and validate them as per blockchain rules. Commonly used PoA algorithms are Clique and Aura

1.15 CAP theorem and blockchain The CAP theorem, also known as Brewer's theorem, was introduced by Eric Brewer in 1998 as a conjecture. In 2002, it was proven 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, 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.

A Venn diagram is commonly used to visualize the CAP theorem:

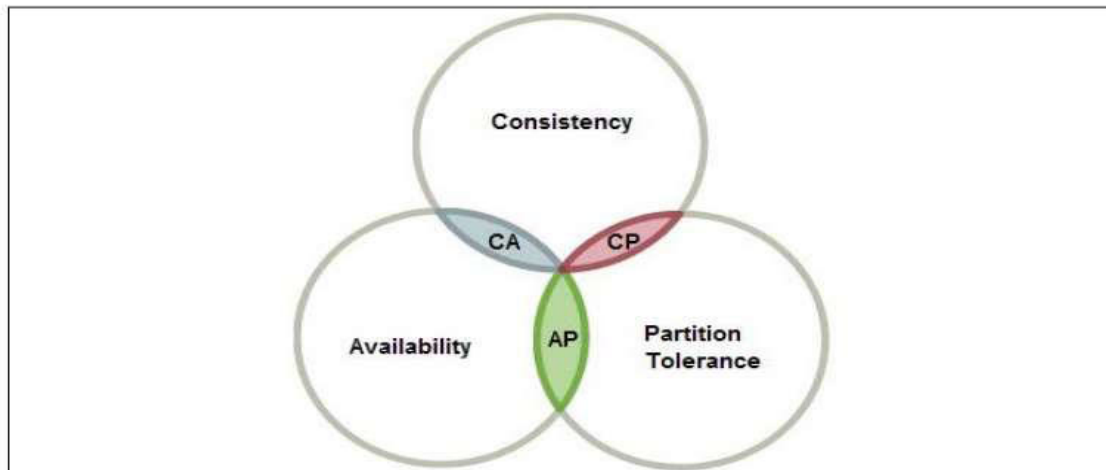


Figure 1.11: CAP theorem

Fig 1.8: CAP Theorem

The preceding diagram shows that only two properties at a time can be achieved. Either AP, CA, or CP. In summary: 1. If we opt for CP (consistency and partition tolerance), we sacrifice availability. 2. If we opt for AP (availability and partition tolerance), we sacrifice consistency. 3. If we opt for AC (availability and consistency), we sacrifice partition tolerance. Usually, a network partition cannot be ignored; therefore, the choice mostly becomes either consistency or availability in the case of a network partition. As shown previously, a distributed system cannot have consistency, availability, and partition tolerance simultaneously. This can be explained with the following example. Let's imagine that there is a distributed system with two nodes. Now, let's apply the three theorem properties on this smallest of possible distributed systems only with two nodes:

- **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, despite communication failure or delay between nodes, the network (distributed system) continues to operate. Now think of a scenario where a partition occurs, and nodes can no longer communicate with each other. If new updated data comes in now, it can only be updated on one node only.

In that case, if the node accepts the update, then only that one node in the network is updated and therefore consistency is lost. Now, if the update is rejected by the node, that would result in loss of availability. In that case, due to partition tolerance, both availability and

VI SEM

consistency are unachievable.

This is strange because somehow blockchain manages to achieve all of these properties—or does it?

It seems that the CAP theorem is violated by blockchain, especially in its most successful implementation, Bitcoin. However, this is not the case. 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. It means that there can be a temporary disagreement between nodes on the final state, but it is eventually agreed upon.

Now think of a scenario where a partition occurs, and nodes can no longer communicate with each other. If new updated data comes in now, it can only be updated on one node only. In that case, if the node accepts the update, then only that one node in the network is updated and therefore consistency is lost. Now, if the update is rejected by the node, that would result in loss of availability. In that case, due to partition tolerance, both availability and consistency are unachievable. This is strange because somehow blockchain manages to achieve all of these properties—or does it? It seems that the CAP theorem is violated by blockchain, especially in its most successful implementation, Bitcoin. However, this is not the case. 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. It means that there can be a temporary disagreement between nodes on the final state, but it is eventually agreed upon.

1.16 Features of Blockchain

A blockchain is a chain of blocks that contains information. Most people think that Blockchain is Bitcoin and vice-versa. But it's not the case. In fact, [Bitcoin](#) is a digital currency or cryptocurrency that works on [Blockchain Technology](#). Blockchain was invented by Satoshi Nakamoto. As the name suggests, Each block consists of a number of transactions, and each transaction is recorded in the form of a Hash. Hash is a unique address assigned to each block during its creation and any further modification in the block will lead to a change in its hash.

Let's have a look at the primary features of the blockchain technology:



1. Immutable

Immutability means that the blockchain is a permanent and unalterable network. Blockchain technology functions through a collection of nodes. Once a transaction is recorded on the blockchain, it cannot be modified or deleted. This makes the blockchain an immutable and tamper-proof ledger that provides a high degree of security and trust. Every node in the network has a copy of the digital ledger. To add a transaction every node checks the validity of the transaction and if the majority of the nodes think that it is a valid transaction then it is added to the network. This means that without the approval of a majority of nodes no one can add any transaction blocks to the ledger. Any validated records are irreversible and cannot be changed.

This means that any user on the network won't be able to edit, change or delete it.

2. Distributed

All network participants have a copy of the ledger for complete transparency. A public ledger will provide complete information about all the participants on the network and transactions. The distributed computational power across the computers ensures a better outcome.

Distributed ledger is one of the important features of blockchains due to many reasons like:

- In distributed ledger tracking what's happening in the ledger is easy as changes propagate really fast in a distributed ledger.
- Every node on the blockchain network must maintain the ledger and participate in the validation.
- Any change in the ledger will be updated in seconds or minutes and due to no involvement of intermediaries in the blockchain, the validation for the change will be done quickly.
- If a user wants to add a new block then other participating nodes have to verify the transaction. For a new block to be added to the blockchain network it must be approved by a majority of the nodes on the network.

- In a blockchain network, no node will get any sort of special treatment or favors from the network. Everyone will have to follow the standard procedure to add a new block to the network.

3. Decentralized

Blockchain technology is a decentralized system, which means that there is no central authority controlling the network. Instead, the network is made up of a large number of nodes that work together to verify and validate transactions. Each and every node in the blockchain network will have the same copy of the ledger.

Decentralization property offers many advantages in the blockchain network:

- As a blockchain network does not depend on human calculations it is fully organized and fault-tolerant.
- The blockchain network is less prone to failure due to the decentralized nature of the network. Attacking the system is more expensive for the hackers hence it is less likely to fail.
- There is no third-party involved hence no added risk in the system.
- The decentralized nature of blockchain facilitates creating a transparent profile for every participant on the network. Thus, every change is traceable, and more concrete.
- Users now have control over their properties and they don't have to rely on third-party to maintain and manage their assets.

4. Secure

All the records in the blockchain are individually encrypted. Using encryption adds another layer of security to the entire process on the blockchain network. Since there is no central authority, it does not mean that one can simply add, update or delete data on the network. Every information on the blockchain is hashed cryptographically which means that every piece of data has a unique identity on the network. All the blocks contain a unique hash of their own and the hash of the previous block. Due to this property, the blocks are cryptographically linked with each other. Any attempt to modify the data means to change all the hash IDs which is quite impossible.

5. Consensus

Every blockchain has a consensus to help the network to make quick and unbiased decisions. Consensus is a decision-making algorithm for the group of nodes active on the network to reach an agreement quickly and faster and for the smooth functioning of the system. Nodes might not trust each other but they can trust the algorithm that runs at the core of the network to make decisions. There are many consensus algorithms available each with its pros and cons. Every blockchain must

VI SEM

have a consensus algorithm otherwise it will lose its value.

6. Unanimous

All the network participants agree to the validity of the records before they can be added to the network. When a node wants to add a block to the network then it must get majority voting otherwise the block cannot be added to the network. A node cannot simply add, update, or delete information from the network. Every record is updated simultaneously and the updations propagate quickly in the network. So it is not possible to make any change without consent from the majority of nodes in the network.

7. Faster Settlement

- Traditional banking systems are prone to many reasons for fallout like taking days to process a transaction after finalizing all settlements, which can be corrupted easily. On the other hand, blockchain offers a faster settlement compared to traditional banking systems. This blockchain feature helps make life easier.
- Blockchain technology is increasing and improving day by day and has a really bright future in the upcoming years. The transparency, trust, and temper proof characteristics have led to many applications of it like bitcoin, Ethereum, etc. It is a pillar in making the business and governmental procedures more secure, efficient, and effective.
- **More Features of Blockchain**
- **Smart Contracts** – Blockchain technology enables the creation and execution of smart contracts, which are self-executing contracts that automatically execute when certain conditions are met. Smart contracts have the potential to revolutionize various industries by providing a secure and transparent way to execute contracts.
- **Transparency** – The blockchain ledger is public and transparent, which means that anyone can access and view the transactions on the network. This makes it a highly transparent system that is resistant to fraud and corruption.
- **Applications of Blockchain** – Blockchain technology has a wide range of applications across various industries. Some of the most well-known applications include cryptocurrency, supply chain management, identity verification, and voting systems. However, blockchain technology has the potential to revolutionize many other industries as well, such as healthcare, real estate, and finance.
- **Conclusion:** In conclusion, blockchain technology is a revolutionary technology that has the potential to transform various industries. Its decentralized, secure, transparent, and immutable nature make it a highly desirable platform for various applications. As the technology continues to evolve and mature, we can expect to see more innovative use cases for blockchain technology in the future.

- **Best Applications of Blockchain in the Real World**

- Blockchain is distributed which means everyone obtains a copy in the case of a public blockchain. So it is very difficult to modify the data in the blockchain because to do so every copy in every location would need to be changed (which is near to impossible) This makes blockchain both distributed and immutable along with maintaining transparency as the data in the block is not hidden in any way. All of these properties of blockchain ensure the highest levels of security which is why it is so popular in many applications that prioritize security and transparency. Nowadays, Blockchain applications are used by companies on a large scale.

So let's see some applications of Blockchain in the real world.

1. Asset Management

Asset Management is one of the biggest applications of Blockchain. Blockchain plays a big part in the financial world and it is no different in asset management. In general terms, asset management involves the handling and exchange of different assets that an individual may own such as fixed income, real estate, equity, mutual funds, commodities, and other alternative investments. Normal trading processes in asset management can be very expensive, especially if the trading involves multiple countries and cross-border payments. In such situations, Blockchain can be a big help as it removes the need for intermediaries such as brokers, custodians, brokers, settlement managers, etc. Instead, the blockchain ledger provides a simple and transparent process that removes the chances of error.

2. Cross-Border Payments

Have you ever tried any applications of Blockchain which make cross-border payments in different currencies from one country to another? This can be a long complicated process and it can take many days for the money to arrive at its destination. Blockchain has helped in simplifying these cross-border payments by providing end-to-end remittance services without any intermediaries. There are many remittance companies that offer Blockchain services which can be used to make international remittances within 24 hours.

3. Healthcare

Blockchain can have a big impact on healthcare using smart contracts and healthcare is one of the biggest applications of blockchain. These smart contracts mean that a contract is made between 2 parties without needing any intermediary. All the parties involved in the contract know the contract details and the contract is implemented automatically when the contract conditions are met. This can be very useful in healthcare wearing personal health records can be encoded via Blockchain so they are only accessible to primary healthcare providers with a key. They also help in upholding the HIPAA Privacy Rule which ensures that patient information is confidential and not accessible to everyone.

4. Cryptocurrency

Perhaps one of the most popular applications of Blockchain is in [Cryptocurrency](#). Who hasn't heard about Bitcoin and its insane popularity? One of the many advantages of cryptocurrency using blockchain as it has no geographical limitations. So crypto coins can be used for transactions all over the world. The only important thing to keep in mind is exchange rates and that people may lose some money in this process. However, this option is much better than regional payment apps such as Paytm in India which are only relevant in a particular country or geographical region and cannot be used to pay money to people in other countries.

5. Birth and Death Certificates

There are many people in the world who don't have a legitimate birth certificate, especially in the poorer countries of the world. According to UNICEF, one-third of all children under the age of five don't have a birth certificate. And the problem is similar to death certificates as well. However, Blockchain can help in solving this problem by creating a secure repository of birth and death certificates that are verified and can only be accessed by authorized people. Isn't it an amazing Blockchain application?

6. Online Identity Verification

It is not possible to complete any financial transactions online without online verification and identification. And this is true for all the possible service providers any user might have in the financial and banking industry. However, blockchain can centralize the online identity verification process so that users only need to verify their identity once using blockchain and then they can share this identity with whichever service provider they want. Users also have the option to choose their identity verification methods such as user authentication, facial recognition, etc. Among the several applications of Blockchain, this application is widely used blockchain application is the entire industry.

7. Internet of Things

The Internet of Things is a network of interconnected devices that can interact with others and collect data that can be used for gaining useful insights. Any system of "things" becomes IoT once it is connected. The most common example of [IoT](#) is perhaps the Smart Home where all the home appliances such as lights, thermostats, air conditioners, smoke alarms, etc. can be connected together on a single platform. But where do the applications of Blockchain come into this? Well, Blockchain is needed for providing security for this massively distributed system. In IoT, the security of the system is only as good as the least secured device which is the weak link. Here Blockchain can ensure that the data obtained by the IoT devices are secure and only visible to trusted parties.

8. Copyright and Royalties

Applications of blockchain have also touched the Creative industry as well. Copyright and royalties are a big issue in creative sectors like music, films, etc. These are artistic mediums and it doesn't sound like they have any link with Blockchain. But this technology is quite important in ensuring security and transparency in the creative industries. There are many instances where music, films, art, etc. is plagiarized and due credit is not given to the original artists. This can be rectified using Blockchain which has a detailed ledger of artist rights. Blockchain is also transparent and can provide a secure record of artist royalties and deals with big production companies. The payment of royalties can also be managed using digital currencies like Bitcoin