Unit 1

Introduction:

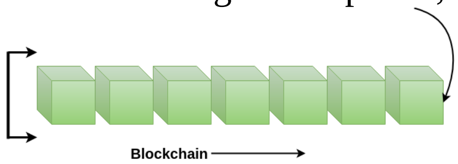
What is Blockchain?

A blockchain is a constantly growing ledger which keeps a permanent record of all the transactions that have taken place in a secure, chronological, and immutable way.

Let's breakdown the definition,

- **Ledger:** It is a file that is constantly growing.
- **Permanent:** It means once the transaction goes inside a blockchain, you can put up it permanently in the ledger.
- **Secure:** Blockchain placed information in a secure way. It uses very advanced cryptography to make sure that the information is locked inside the blockchain.
- **Chronological:** Chronological means every transaction happens after the previous one.
- **Immutable:** It means as you build all the transaction onto the blockchain, this ledger can never be changed.

A blockchain is a chain of blocks which contain information. Each block records all of the recent transactions, and once completed goes into the blockchain as a permanent database. Each time a block gets completed, a new block is generated.



How does Blockchain Technology Work?

- **Transaction Initiation:** A user initiates a transaction.
- **Validation:** Nodes verify the transaction's validity.
- **Block Creation:** Valid transactions are grouped into a block.
- **Consensus:** Nodes agree on the block's validity through consensus mechanisms.
- **Adding to the Chain:** Verified blocks are added to the existing chain.
- **Distribution:** Updated blockchain is synchronized across all nodes.
- **Cryptography:** Security measures like encryption and digital signatures secure the transactions.
- **Continued Transactions:** The process continues with new transactions added to the chain.

Disadvantages of the current transaction system:

- Cash can only be used in low-amount transactions locally.
- The huge waiting time in the processing of transactions.
- The need for a third party for verification and execution of Transactions makes the process complex.
- If the Central Server like Banks is compromised, the whole system is affected including the participants.
- Organizations doing validation charge high process thus making the process expensive.

Need of Blockchain:

- **Time-saving:** No central Authority verification is needed for settlements making the process faster and cheaper.
- **Cost-saving:** A Blockchain network reduces expenses in several ways. No need for third-party verification. Participants can share assets directly. Intermediaries are reduced. Transaction efforts are minimized as every participant has a copy of the shared ledger.
- **Tighter security:** No one can tamper with Blockchain Data as it is shared among millions of Participants. The system is safe against cybercrimes and Fraud.
- **Collaboration:** It permits every party to interact directly with one another while not requiring third-party negotiation.
- **Reliability:** Blockchain certifies and verifies the identities of every interested party. This removes double records, reducing rates and accelerating transactions.

Application of Blockchain:

1. **Cryptocurrency Wallet:** Create a simple cryptocurrency wallet application that allows users to send and receive digital assets.
2. **Smart Contract:** Implement a simple smart contract on the Ethereum blockchain that can be used to manage a digital token or asset.
3. **Voting System**: Create a blockchain-based voting system that allows for secure and transparent voting while maintaining voter anonymity.
4. **Supply Chain Management:** Develop a blockchain-based system for tracking the movement of goods and services through a supply chain, providing greater transparency and traceability.
5. **Identity Management:** Create a decentralized digital identity management system that allows users to control their personal information and share it securely with others.

Advantages of Blockchain Technology:

- **Decentralization:** The decentralized nature of blockchain technology eliminates the need for intermediaries, reducing costs and increasing transparency.
- **Security:** Transactions on a blockchain are secured through cryptography, making them virtually immune to hacking and fraud.
- **Transparency:** Blockchain technology allows all parties in a transaction to have access to the same information, increasing transparency and reducing the potential for disputes.
- **Efficiency:** Transactions on a blockchain can be processed quickly and efficiently, reducing the time and cost associated with traditional transactions.
- **Trust:** The transparent and secure nature of blockchain technology can help to build trust between parties in a transaction.

Disadvantages of Blockchain Technology:

- **Scalability:** The decentralized nature of blockchain technology can make it difficult to scale for large-scale applications.
- **Energy Consumption:** The process of mining blockchain transactions requires significant amounts of computing power, which can lead to high energy consumption and environmental concerns.
- **Adoption:** While the potential applications of blockchain technology are vast, adoption has been slow due to the technical complexity and lack of understanding of the technology.
- **Regulation:** The regulatory framework around blockchain technology is still in its early stages, which can create uncertainty for businesses and investors.
- **Lack of Standards:** The lack of standardized protocols and technologies can make it difficult for businesses to integrate blockchain technology into their existing systems.

Peer To Peer (P2P) Network:

A peer-to-peer (P2P) network is based on the concept of decentralisation, which allows the participants to conduct transactions without needing a central server. The peers or nodes (usually a computer) communicate with each other on the network freely without an intermediary.

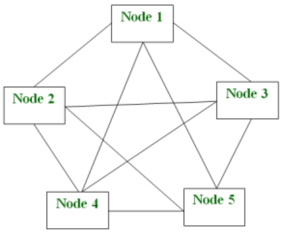
Types of P2P networks:

1. **Unstructured P2P networks:** In this type of P2P network, each device is able to make an equal contribution. This network is easy to build as devices can be connected randomly in the network. But being unstructured, it becomes difficult to find content. For example, Napster, Gnutella, etc.
2. **Structured P2P networks:** It is designed using software that creates a virtual layer in order to put the nodes in a specific structure. These are not easy to set up but can give easy access to users to the content. For example, P-Grid, Kademlia, etc.
3. **Hybrid P2P networks:** It combines the features of both P2P networks and client-server architecture. An example of such a network is to find a node using the central server.

P2P Network Architecture:

In the P2P network architecture, the computers connect with each other in a workgroup to share files, and access to internet and printers.

- Each computer in the network has the same set of responsibilities and capabilities.
- Each device in the network serves as both a client and server.
- The architecture is useful in residential areas, small offices, or small companies where each computer act as an independent workstation and stores the data on its hard drive.
- Each computer in the network has the ability to share data with other computers in the network.
- The architecture is usually composed of workgroups of 12 or more computers.



P2P Architecture

How Does P2P Network Work?

Let's understand the working of the Peer-to-Peer network through an example. Suppose, the user wants to download a file through the peer-to-peer network then the download will be handled in this way:

- If the peer-to-peer software is not already installed, then the user first has to install the peer-to-peer software on his computer.
- This creates a virtual network of peer-to-peer application users.
- The user then downloads the file, which is received in bits that come from multiple computers in the network that have already that file.
- The data is also sent from the user's computer to other computers in the network that ask for the data that exist on the user's computer.

Thus, it can be said that in the peer-to-peer network the file transfer load is distributed among the peer computers.

Applications of P2P Network:

- **File sharing:** P2P network is the most convenient, cost-efficient method for file sharing for businesses. Using this type of network there is no need for intermediate servers to transfer the file.
- **Blockchain:** The P2P architecture is based on the concept of decentralization. When a peer-to-peer network is enabled on the blockchain it helps in the maintenance of a complete replica of the records ensuring the accuracy of the data at the same time. At the same time, peer-to-peer networks ensure security also.
- **Direct messaging:** P2P network provides a secure, quick, and efficient way to communicate. This is possible due to the use of encryption at both the peers and access to easy messaging tools.
- **Collaboration:** The easy file sharing also helps to build collaboration among other peers in the network.
- **Content distribution:** In a P2P network, unline the client-server system so the clients can both provide and use resources. Thus, the content serving capacity of the P2P networks can actually increase as more users begin to access the content.
- **IP Telephony:** Skype is one good example of a P2P application in VoIP.

Advantages of P2P Network:

- **Easy to maintain:** The network is easy to maintain because each node is independent of the other.

- **Less costly:** Since each node acts as a server, therefore the cost of the central server is saved. Thus, there is no need to buy an expensive server.
- **No network manager:** In a P2P network since each node manages his or her own computer, thus there is no need for a network manager.
- **Adding nodes is easy:** Adding, deleting, and repairing nodes in this network is easy.
- **Less network traffic:** In a P2P network, there is less network traffic than in a client/ server network.

Disadvantages of P2P Network:

- **Data is vulnerable:** Because of no central server, data is always vulnerable to getting lost because of no backup.
- **Less secure:** It becomes difficult to secure the complete network because each node is independent.
- **Slow performance:** In a P2P network, each computer is accessed by other computers in the network which slows down the performance of the user.
- **Files hard to locate:** In a P2P network, the files are not centrally stored, rather they are stored on individual computers which makes it difficult to locate the files.

Public Ledger:

The public ledger refers to the decentralized and transparent record of all transactions that have occurred on the network. This ledger contains a chronological list of blocks, each containing multiple transactions, and is accessible to anyone in the network.

Key Aspects of the Public Ledger:

1. **Transparency:** The ledger is open and visible to all participants in the network. Anyone can view the transactions, though the identities of the involved parties may be pseudonymous or encrypted depending on the blockchain's design.

2. **Decentralization:** Multiple copies of the ledger exist across the network's nodes. Each node maintains its own copy, ensuring that there's no single point of failure or control.

3. **Immutable Record:** Once a block is added to the chain, it becomes extremely difficult to alter or delete the data it contains. This immutability is maintained through cryptographic techniques and consensus mechanisms.

4. **Verification and Consensus:** Transactions are validated and added to the ledger through a consensus mechanism agreed upon by the network participants. This ensures that only valid transactions are recorded.

5. **Transaction History:** The ledger maintains a complete history of all transactions, providing a transparent and auditable record of the entire transactional history from the genesis block (the first block) to the most recent one.

The public ledger is a fundamental component of blockchain technology, enabling trust-less and secure transactions while promoting transparency and accountability within the network.

Double Spend Problem:

What Is Double-Spending?

Double-spending occurs when a digital currency or token is spent more than once. In a digital cash system, it's akin to counterfeiting, where the same money is used for multiple transactions. This poses a critical challenge for any system aiming to facilitate trust-less and secure transactions without a central authority.

How Does Double Spending Happen?

1. Digital Replication: If someone can duplicate their digital currency, they could spend the same tokens in multiple transactions before the network detects the duplication.

2. Race Condition: When two conflicting transactions spending the same funds are broadcasted simultaneously or nearly so, the network may temporarily accept both. However, only one transaction can eventually be added to the blockchain, leading to a potential double-spend scenario.

Types Of Double Spending Attacks:

1. Race Attack: The attacker attempts to send two conflicting transactions at the same time to different parts of the network. This creates a situation where the network may accept one transaction while rejecting the other.

2. Finney Attack: Named after Hal Finney, this attack involves a miner pre-mining a block containing a transaction that spends the same coins they just received. They secretly mine a longer chain that invalidates the original transaction, benefiting from the block reward without the transaction being included in the main chain.

Key Components that Prevent Double Spending in a Blockchain based System:

1. Consensus Mechanism: By utilizing Proof of Work (PoW), Proof of Stake (PoS), or other consensus algorithms, blockchain networks achieve agreement on which transactions are valid, preventing multiple conflicting transactions from being added to the chain.

2. Confirmation: Waiting for a certain number of confirmations from subsequent blocks in the blockchain significantly reduces the risk of a transaction being reversed or double-spent.

How Bitcoin Handles Double Spending?

Bitcoin employs a decentralized network of nodes and miners to achieve consensus. Miners compete to solve complex mathematical puzzles to add new blocks to the chain. This process makes it computationally infeasible to rewrite transaction history, significantly reducing the risk of double spending.

Solutions To Prevent Double Spending:

1. **Confirmation Wait:** Merchants or recipients often wait for a certain number of confirmations (blocks added to the chain after the transaction) to consider a transaction final and secure.

2. **Detective Work:** Monitoring the network for conflicting transactions or any unusual activity helps prevent potential double spending.

3. **Consensus Mechanisms:** Implementing robust consensus mechanisms like PoW, PoS, or other algorithms ensures agreement on the validity of transactions.

4. **Zero-Confirmation Transactions:** Some systems accept transactions without confirmations but at a higher risk, suitable for low-value transactions or cases where instant validation is essential.

By utilizing these preventive measures, blockchain systems work to mitigate the risks associated with double spending, ensuring the integrity and security of transactions within the network.

Features of Blockchain:

features of
Blockchain
Faster Settlement
Secure
Decentralized
Census
Distributed
Unanimous
Immutable

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.

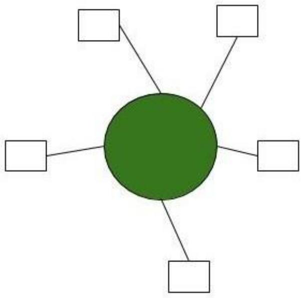
Distributed ledger is one of the important features of blockchains due to many reasons like:

- 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.

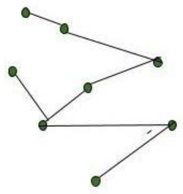
3. Decentralized: Blockchain technology is a decentralized system, which means that there is no central authority controlling the network. Instead, the network is made up of a large number of nodes that work together to verify and validate transactions. Each and every node in the blockchain network will 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 concreate.
- Users now have control over their properties and they don’t have to rely on third-party to maintain and manage their assets.



Centralised Network



Decentralised network

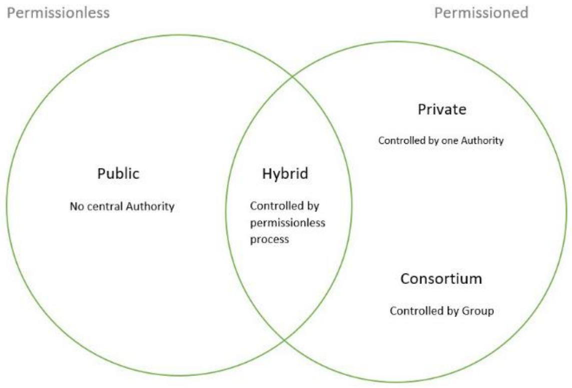
4. Secure: All the records in the blockchain are individually encrypted. Using encryption adds another layer of security to the entire process on the blockchain network. Since there is no central authority, it does not mean that one can simply add, update or delete data on the network.

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.

Types of Blockchain:

There are 4 types of blockchain:

- Public Blockchain.
- Private Blockchain.
- Hybrid Blockchain.
- Consortium Blockchain.



1. 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 computer in the network hold the copy of other nodes or block present in the network.
- In this public blockchain, we can also perform verification of transactions or records.

Advantages:

- **Trustable:** There are algorithms to detect no fraud. Participants need not worry about the other nodes in the network
- **Secure:** This blockchain is large in size as it is open to the public. In a large size, there is 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 in order 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 high energy-consuming. It requires good computer hardware to participate in the network
- **Acceptance:** No central authority is there so governments are facing the issue to implement the technology faster.

Use Cases: Public Blockchain is secured with proof of work or proof of stake they can be used to displace traditional financial systems. The more advanced side of this blockchain is the smart contract that enabled this blockchain to support decentralization. Examples of public blockchain are Bitcoin, Ethereum.

2. 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.

- 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.

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 user has the 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.

3. Hybrid Blockchain: 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.
- User access information via smart contracts.
- Even a primary entity owns a hybrid blockchain it cannot alter the transaction.

Advantages:

- **Ecosystem:** 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 the 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 health care industry, government, real estate, and financial companies. It provides a remedy where data is to be accessed publicly but needs to be shielded privately. Examples of Hybrid Blockchain are Ripple network and XRP token.

4. Consortium Blockchain: It is a creative approach that solves the needs of the organization. This blockchain validates the transaction and also initiates or receives transactions.

- Also known as Federated Blockchain.
- This is an innovative method to solve the organization's needs.
- Some part is public and some part is private.
- In this type, more than one organization manages the blockchain.

Advantages:

- **Speed:** A limited number of users make verification fast. The high speed makes this more usable for organizations.
- **Authority:** Multiple organizations can take part and make it decentralized at every level. Decentralized authority, makes it more secure.
- **Privacy:** The information of the checked blocks is unknown to the public view. but any member belonging to the blockchain can access it.
- **Flexible:** There is much divergence in the flexibility of the blockchain. Since it is not a very large decision can be taken faster.

Disadvantages:

- **Approval:** All the members approve the protocol making it less flexible. Since one or more organizations are involved there can be differences in the vision of interest.
- **Transparency:** It can be hacked if the organization becomes corrupt. Organizations may hide information from the users.
- **Vulnerability:** If few nodes are getting compromised there is a greater chance of vulnerability in this blockchain.

Use Cases: It has high potential in businesses, banks, and other payment processors. Food tracking of the organizations frequently collaborates with their sectors making it a federated solution ideal for their use. Examples of consortium Blockchain are Tendermint and Multichain.

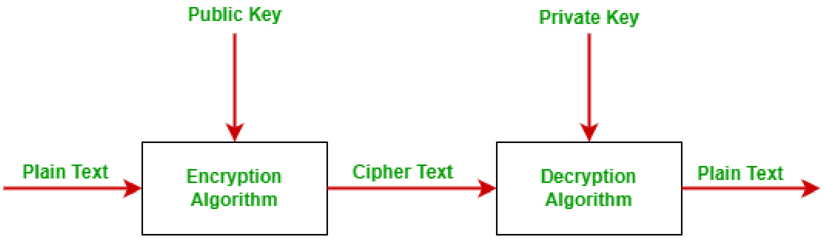
Difference between Public and Private blockchain :

Basis of Comparison	Public Blockchain	Private Blockchain
Access	In this type of blockchain anyone can read, write and participate in a blockchain. Hence, it is permissionless blockchain. It is public to everyone.	In this type of blockchain read and write is done upon invitation, hence it is a permissioned blockchain.
Network Actors	Don’t know each other	Know each other
Decentralized Vs Centralized	A public blockchain is decentralized.	A private blockchain is more centralized.
Speed	Slow	Fast
Transactions per second	Transactions per second are lesser in a public blockchain.	Transaction per second is more as compared to public blockchain.
Security	A public network is more secure due to decentralization and active participation. Due to the higher number of nodes in the network, it is nearly impossible for ‘bad actors’ to attack the system and gain control over the consensus network.	A private blockchain is more prone to hacks, risks, and data breaches / manipulation. It is easy for bad actors to endanger the entire network. Hence, it is less secure.
Energy Consumption	A public blockchain consumes more energy than a private blockchain as it requires a significant amount of electrical resources to function and achieve network consensus.	Private blockchains consume a lot less energy and power.
Examples	Bitcoin, Ethereum, Monero, Zcash, Dash, Litecoin, Stellar, Steemit etc.	R3 (Banks), EWF (Energy), B3i (Insurance), Corda.

Unit 2

Public Key Cryptography:

Most of the time blockchain uses public-key cryptography, also known as asymmetric-key cryptography. Public key cryptography uses both public key and private key in order to encrypt and decrypt data. The public key can be distributed commonly but the private key cannot be shared with anyone. It is commonly used for two users or two servers in a secure way.



Public Key: Public keys are designed to be public. They can be freely given to everyone or posted on the internet. By using the public key, one can encrypt the plain text message into the cipher text. It is also used to verify the sender authentication. In simple words, one can say that a public key is used for closing the lock.

Private Key: The private key is totally opposite of the public key. The private key is always kept secret and never shared. Using this key we decrypt cipher text messages into plain text. In simple words, one can say that the private key is used for opening the lock.

Why Do We Need Public-Key Cryptography?

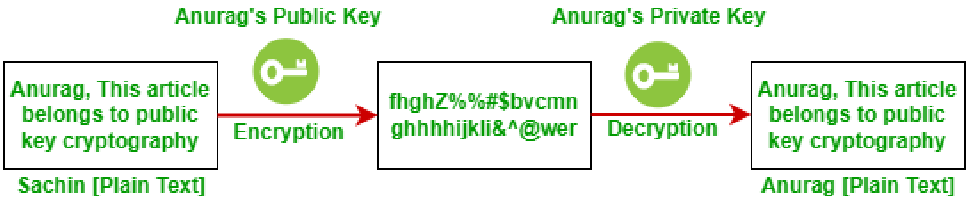
- In symmetric-key cryptography, a single key is used to encrypt and decrypt the message. Here, the possibility of data loss or unauthorized access to data is high. To overcome the unauthorized access of data and data sent securely without any loss, we use public-key cryptography.
- Public-key cryptography is more secure than symmetric-key cryptography because the public key uses two keys to encrypt and decrypt the data
- Public-key cryptography allows users to hide the data that they want to send. The sender encrypts the data and the receiver decrypts the data. The encrypted message is not understood by unauthorized users.

Working On Public-Key Cryptography

Suppose, the sender wants to send some important message to the receiver.

- The sender first creates a message in the form of plain text which is in a readable format.
- The sender knows the public key of the receiver but doesn't know the private key of the receiver because the receiver keeps secret his private key. With the help of the public key of the receiver and the private key of the sender, the sender generates the encrypted message i.e. called cipher text. Cipher text is in an unreadable format. In this step, plain text converts into cipher text.
- Now, cipher text reaches the receiver end. The receiver knows its own private key, and with the help of the private key receiver converts the cipher text into readable format i.e. plain text.

The below example shows the working of public-key cryptography.


Anurag's Public Key
Anurag's Private Key
Anurag, This article belongs to public key cryptography
Encryption
fhghZ%%#$bvcmn ghhhhijkli&^@wer
Decryption
Anurag, This article belongs to public key cryptography
Sachin [Plain Text]
Anurag [Plain Text]

Let us try to under the working of public-key cryptography with an example. Suppose Sachin is the sender who wants to send a message to Anurag. Here Anurag is the receiver.

- Sachin uses Anurag's public key to encrypt the message and Anurag uses his own private key to decrypt the message.
- First Sachin creates plain text. Sachin has access to Anurag's private key and cipher text. Using Anurag's public key and his own public key,
- Sachin will generate an encrypted message i.e. cipher text which is in an unreadable format. After applying the encryption process plain text converts into cipher text.
- Now, Anurag receives a cipher text. First Anurag will decrypt the cipher text message into a readable format. For decrypting Anurag will use the private key. Now cipher text converts into plain text and is readable by the receiver. Because Sachin keeps his private key, Anurag knows that this message couldn't have come from anyone else. This is also called a digital signature.

Benefits of Public-key Cryptography:

- **Authentication:** It ensures to the receiver that the data received has been sent by the only verified sender.
- **Data integrity:** It ensures that the information and program are changed only in a specific and authorized manner.
- **Data confidentiality:** It ensures that private message is not made available to an unauthorized user. It is referred to as privacy or secrecy.
- **Non-repudiation:** It is an assurance that the original creator of the data cannot deny the transmission of the said data to a third party.
- **Key management:** Public-key cryptography allows for secure key management, as the private keys are never transmitted or shared. This eliminates the need for a secure channel to transmit the private key, as is required in symmetric key cryptography.
- **Digital signatures:** Public-key cryptography allows for the creation of digital signatures, which provide non-repudiation and can be used to verify the authenticity and integrity of data.
- **Key exchange:** Public-key cryptography enables secure key exchange between two parties, without the need for a pre-shared secret key. This allows for secure communication even if the parties have never communicated before.
- **Secure communication:** Public-key cryptography enables secure communication over an insecure channel, such as the internet, by encrypting the data with the public key of the recipient, which can only be decrypted by the recipient's private key.

Limitation of Public-Key Cryptography:

- One can encrypt and decrypt the fixed size of messages or data. If there is an attempt to encrypt or decrypt a large size of the message then the algorithm demands high computational power.
- The main disadvantage of this algorithm is that if the receiver losses its private key then data/message will be lost forever.
- If someone has access private key then all data will be in the wrong hand.
- There are many secret-key which is faster than public-key cryptography.
- **Key distribution:** The process of securely distributing public keys to all authorized parties can be difficult and time-consuming, especially in large networks.
- **Performance:** Public-key cryptography is generally slower than symmetric-key cryptography due to its more complex algorithms, making it less suitable for applications that require fast processing speeds.

Hash Functions:

What is Hash Functions?

Hash functions are mathematical algorithms that convert input data of any size into a fixed-size string of characters, known as a hash value or digest. These functions play a crucial role in cryptography by producing unique outputs for specific inputs.

How do Hash Functions Work?

1. One-Way Function: Hash functions are designed to be one-way, making it practically impossible to reverse-engineer the original input from the hash.

2. Deterministic Output: For the same input, a hash function always generates the same output.

3. Fixed Output Size: Regardless of input size, the output hash length remains constant.

4. Avalanche Effect: A small change in the input significantly alters the hash output.

5. Collision Resistance: It's exceedingly rare for two different inputs to produce the same hash output.

Types of Cryptographic Hash Functions:

1. SHA (Secure Hash Algorithm): Includes SHA-256, SHA-384, SHA-512, etc., offering varying hash lengths.

2. MD5 (Message Digest Algorithm 5): Once widely used but now considered weak due to vulnerabilities.

3. Blake, Keccak, and Others: Various other hash functions designed with specific features and security levels.

Uses of Hash Functions in Blockchain:

1. Data Integrity: Each block in a blockchain contains a unique hash value of the previous block, ensuring the integrity of the entire chain. Even a slight alteration in the block's content would change its hash, revealing tampering attempts.

2. Merkle Trees: Hash functions help construct Merkle trees, efficient data structures used in blockchain to summarize and verify large sets of data.

3. Mining and Proof of Work: In mining processes (like in Bitcoin), miners compete to find a nonce value that, when hashed with the block's data, meets certain criteria, providing proof of work.

4. Address Generation: Cryptocurrency addresses are often derived from public keys using hash functions, providing anonymity and security.

5. Smart Contracts: Hash functions are used to verify and execute smart contracts by ensuring that the contract's code hasn’t been altered.

Hash functions serve as the backbone of blockchain technology, ensuring the immutability of data, enhancing security, facilitating consensus mechanisms, and enabling various cryptographic functionalities essential for a decentralized and secure system.

Secure Hash Algorithms (SHA-256):

What is Hashing?

Hashing involves the conversion of input data, irrespective of its size or type, into a fixed-size string of characters using a mathematical algorithm known as a hash function. This process generates a unique output, called a hash, that serves as a digital fingerprint representing the input data.

What is the SHA-256 Algorithm?

SHA-256, part of the SHA-2 (Secure Hash Algorithm 2) family, is a widely adopted cryptographic hash function. It operates by producing a 256-bit (32-byte) hash value from input data. This algorithm stands out for its robustness and usage across numerous security applications due to its reliability and resistance to cryptographic attacks.

Characteristics of the SHA-256 Algorithm:

1. **Fixed Output Size:** Always generates a 256-bit output, regardless of the input's size, ensuring consistency and predictability in hash length.

2. **Deterministic Nature:** For a given input, it consistently generates the same hash output, facilitating data validation and verification.

3. **One-Way Functionality:** It's computationally infeasible to reverse-engineer the original input from the hash value, ensuring data security.

4. **Collision Resistance:** The probability of two distinct inputs producing the same hash output is astronomically low, ensuring uniqueness.

5. **Security Measures:** Designed with robust defenses against cryptographic attacks, ensuring data integrity and confidentiality.

Steps in SHA-256 Algorithm:

1. Message Padding: Input data is padded to achieve a multiple of 512 bits, preparing it for processing.

2. Initialization Constants: Specific constants, acting as initial hash values, are set before computation.

3. Message Processing: Input data undergoes processing in blocks of 512 bits, subjected to multiple transformation rounds.

4. Compression Function: Each block goes through multiple iterations of complex cryptographic transformations, updating the hash value.

5. Final Hash Output: After processing the entire input data, the SHA-256 algorithm produces a 256-bit hash value.

Applications of SHA Algorithm:

1. Blockchain Technology: SHA-256 ensures the integrity of blockchain data by generating unique hash values for transactions, securing the immutability of blocks.

2. Digital Signatures: Utilized to verify the authenticity of messages or data by producing and verifying digital signatures.

3. Password Hashing: Safeguarding passwords by hashing them before storage to prevent exposure and ensuring security.

4. Integrity Checks: Guaranteeing data integrity during transmission or storage by generating hash values for verification and validation.

5. Cryptography: Integral in various cryptographic protocols and security mechanisms to ensure authenticity and security across multiple domains.

SHA-256 serves as a cornerstone in guaranteeing data integrity, security, and authenticity across an array of technological applications, particularly in blockchain where it secures the transactional immutability within blocks.

Digital Signatures:

What is a Digital Signature?

A digital signature is a cryptographic technique that authenticates the origin, identity, and integrity of digital messages, documents, or transactions. It operates using asymmetric encryption, where a pair of cryptographic keys—a private key and a public key—are used to sign and verify data.

How Digital Signatures Work in Blockchain:

1. Private and Public Key Pair:

- Each participant in a blockchain has a unique pair of keys.
- **Private Key:** Kept securely by the owner and used to create digital signatures.
- **Public Key:** Shared with others and used to verify signatures.

2. Signing the Transaction:

- When a participant initiates a transaction in the blockchain, they use their private key to generate a digital signature unique to that transaction.
- The signature is created by applying a mathematical algorithm to the transaction data and the private key.

3. Verification Process:

- The signed transaction, along with the sender's public key, is broadcasted to the network.
- Other participants use the public key to verify the signature's authenticity and integrity.
- Verification confirms that the signature was indeed created by the corresponding private key.

4. Authentication and Validation:

- If the signature is successfully verified, it validates that the transaction came from the owner of the private key, ensuring authenticity and integrity.
- This process prevents unauthorized alterations to the transaction data during transmission and confirms the identity of the sender.

Advantages of Digital Signatures in Blockchain:

1. **Authentication:** Provides strong proof that a transaction originates from a specific participant, validating their identity.

2. **Integrity:** Ensures that the transaction data has not been tampered with or altered in transit.

3. **Non-Repudiation:** Prevents the sender from denying involvement in the transaction, establishing accountability and trust.

4. **Security:** Enhances the overall security of blockchain networks by safeguarding transactions from unauthorized alterations and ensuring only authorized participants can interact.

Importance in Blockchain:

- **Transaction Security:** Digital signatures play a crucial role in securing transactions on the blockchain, ensuring only authorized participants can initiate valid transactions.

- **Immutable Records:** Once a transaction is signed and included in a block, its integrity is preserved, making it nearly impossible to modify without detection.

- **Consensus and Validation:** Digital signatures are fundamental in the consensus process, where nodes validate transactions, maintaining the trust and integrity of the decentralized network.

Digital signatures are integral to the robustness and security of blockchain technology, providing a foundation for trust, accountability, and tamper-resistant transactions within decentralized networks.

Merkle Tree:

Merkle tree is a fundamental part of blockchain technology. It is a mathematical **data structure** composed of hashes of different blocks of data, and which serves as a summary of all the transactions in a block. It also allows for efficient and secure verification of content in a large body of data. It also helps to verify the consistency and content of the data. Both Bitcoin and Ethereum use Merkle Trees structure. Merkle Tree is also known as **Hash Tree**.

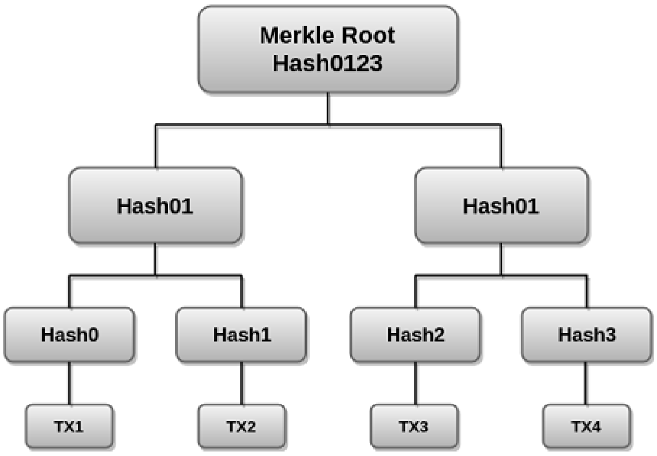
The concept of Merkle Tree is named after **Ralph Merkle**, who patented the idea in **1979**. Fundamentally, it is a data structure tree in which every **leaf node** labelled with the hash of a data block, and the **non-leaf node** labelled with the cryptographic hash of the labels of its child nodes. The leaf nodes are the lowest node in the tree.

How do Merkle Trees Work?

A Merkle tree stores all the transactions in a block by producing a digital fingerprint of the entire set of transactions. It allows the user to verify whether a transaction can be included in a block or not.

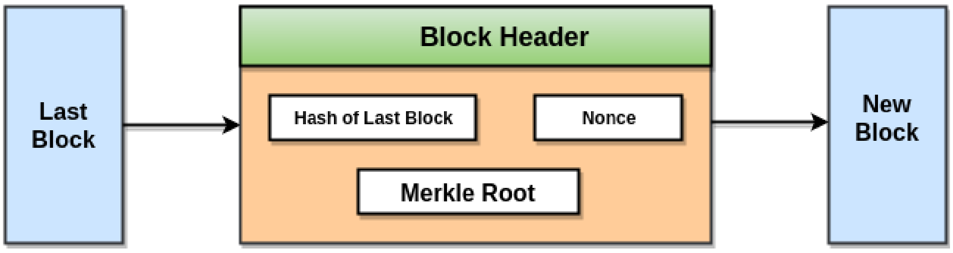
Merkle trees are created by repeatedly calculating hashing pairs of nodes until there is only one hash left. This hash is called the Merkle Root, or the Root Hash. The Merkle Trees are constructed in a bottom-up approach.

Every leaf node is a hash of transactional data, and the non-leaf node is a hash of its previous hashes. Merkle trees are in a binary tree, so it requires an even number of leaf nodes. If there is an odd number of transactions, the last hash will be duplicated once to create an even number of leaf nodes.



The above example is the most common and simple form of a Merkle tree, i.e., **Binary Merkle Tree**. There are four transactions in a block: **TX1**, **TX2**, **TX3**, and **TX4**. Here you can see, there is a top hash which is the hash of the entire tree, known as the **Root Hash**, or the **Merkle Root**. Each of these is repeatedly hashed, and stored in each leaf node, resulting in Hash 0, 1, 2, and 3. Consecutive pairs of leaf nodes are then summarized in a parent node by hashing **Hash0** and **Hash1**, resulting in **Hash01**, and separately hashing **Hash2** and **Hash3**, resulting in **Hash23**. The two hashes (**Hash01** and **Hash23**) are then hashed again to produce the Root Hash or the Merkle Root.

Merkle Root is stored in the **block header**. The block header is the part of the bitcoin block which gets hash in the process of mining. It contains the hash of the last block, a Nonce, and the Root Hash of all the transactions in the current block in a Merkle Tree. So having the Merkle root in block header makes the transaction **tamper-proof**. As this Root Hash includes the hashes of all the transactions within the block, these transactions may result in saving the disk space.



The Merkle Tree maintains the **integrity** of the data. If any single detail of transactions or order of the transaction's changes, then these changes reflected in the hash of that transaction. This change would cascade up the Merkle Tree to the Merkle Root, changing the value of the Merkle root and thus invalidating the block. So everyone can see that Merkle tree allows for a quick and simple test of whether a specific transaction is included in the set or not.

Merkle trees have three benefits:

- It provides a means to maintain the integrity and validity of data.
- It helps in saving the memory or disk space as the proofs, computationally easy and fast.
- Their proofs and management require tiny amounts of information to be transmitted across networks.

Unit 3

Introduction:

Bitcoin is a pioneering cryptocurrency that revolutionized the financial landscape by introducing a decentralized digital currency and a groundbreaking technology called blockchain. Here's an introduction to Bitcoin within the realm of blockchain:

What is Bitcoin?

Bitcoin, introduced in a 2008 whitepaper by an anonymous entity known as Satoshi Nakamoto, is a decentralized digital currency. It operates without a central authority or intermediary, utilizing a peer-to-peer network to facilitate secure, transparent, and trustless transactions.

Key Elements of Bitcoin:

1. **Decentralization:** Unlike traditional currencies controlled by governments or financial institutions, Bitcoin operates on a decentralized network of computers (nodes), eliminating the need for a central authority.
2. **Blockchain Technology:** The underlying technology powering Bitcoin is the blockchain—a distributed ledger that records all transactions across the network in a secure, transparent, and immutable manner.
3. **Cryptographic Security:** Transactions on the Bitcoin network are secured using cryptographic techniques. Each participant has a pair of cryptographic keys—a private key for transaction authorization and a public key for verification.
4. **Limited Supply:** Bitcoin has a capped supply of 21 million coins, creating scarcity and potentially affecting its value over time.

How Bitcoin Works:

1. **Transactions:** Users can send and receive bitcoins through digital wallets. Each transaction is broadcast to the network and recorded on the blockchain.
2. **Mining:** The process of verifying and adding transactions to the blockchain is called mining. Miners use computational power to solve complex mathematical puzzles and validate transactions. Successful miners are rewarded with newly minted bitcoins and transaction fees.
3. **Consensus Mechanism:** Bitcoin uses Proof of Work (PoW) as its consensus mechanism, ensuring agreement on the validity of transactions and maintaining the integrity of the blockchain.

4. **Security and Immutability:** Once a transaction is confirmed and added to a block, it becomes practically irreversible due to the cryptographic hashing and decentralized nature of the blockchain.

Significance of Bitcoin in Blockchain:

- **Pioneering Cryptocurrency:** Bitcoin introduced the concept of digital currency and blockchain technology, laying the foundation for a new financial ecosystem.
- **Decentralization and Trust:** It demonstrates the potential for decentralized systems to facilitate secure and transparent transactions without the need for intermediaries.
- **Influence on Innovation:** Bitcoin's success has inspired the development of numerous cryptocurrencies, blockchain-based applications, and innovative financial solutions.

Bitcoin's emergence as the first decentralized cryptocurrency marked a paradigm shift in the way we perceive and utilize currency, paving the way for the exploration and adoption of blockchain technology across various industries and applications.

Transaction:

A Bitcoin transaction is the transfer of Bitcoin between parties. It's a core unit in the Bitcoin network, recording the movement of Bitcoin from one address to another.

Components of a Bitcoin Transaction:

1. **Inputs:** References to previous transaction outputs (UTXOs - Unspent Transaction Outputs) that act as the source of funds for the new transaction. Each input contains a cryptographic signature proving ownership.
2. **Outputs:** Destination addresses where the Bitcoin is sent. Each output specifies the amount of Bitcoin being transferred and the recipient's address.
3. **Transaction ID (TXID):** A unique identifier generated for each transaction, serving as its digital fingerprint on the blockchain.
4. **Fee:** A small amount of Bitcoin paid by the sender as an incentive for miners to include the transaction in a block.

Key Points about Transactions in Bitcoin:

1. **Immutable Records:** Once a transaction is confirmed and added to a block, it becomes a permanent and immutable part of the blockchain's history.
2. **Verification and Consensus:** Transactions are validated by network nodes, ensuring they adhere to Bitcoin's rules before being included in a block. Consensus mechanisms ensure agreement on the validity of transactions.
3. **Confirmation:** Transactions require confirmations by being included in blocks added to the blockchain. Multiple confirmations increase the transaction's security and reliability.
4. **Transaction Lifecycle:** Transactions are initiated, broadcasted to the network, validated by miners, included in blocks, and finally confirmed by being added to the blockchain.
5. **Transaction Types:** Apart from regular transfers, Bitcoin transactions can involve various functionalities like multi-signature transactions, where multiple signatures are required for a transaction to be valid, or the use of scripts allowing more complex operations.

Transactions in the Bitcoin blockchain facilitate the transfer of value between participants, ensuring the secure and decentralized movement of Bitcoin while maintaining transparency and integrity through the blockchain's distributed ledger.

Transaction life-cycle in Blockchain:

This lifecycle follows the journey of a single transaction as it makes its way through each stage in the process of joining the blockchain. Transaction in simple words is the process of sending money by the sender and the receiver receiving it. The Blockchain transaction is also quite similar, but it is made digitally.

Let us understand the various stages in a blockchain transaction life cycle with the help of an example.
Sourav and Suraj are two **Bitcoin** users. Sourav wants to send 1 bitcoin to Suraj.

1. First, Sourav gets Suraj's wallet address (a wallet in the blockchain is a digital wallet that allows users to manage their transactions). Using this information, he creates a new transaction for 1 bitcoins from his wallet and includes a transaction fee of 0.003 bitcoin.

2. Next, he verifies the information and sends the transaction. Each transaction that is initiated is signed by a digital signature of the sender that is basically the private key of the sender. This is done in order to make the transaction more secure and to prevent any fraud.

3. Sourav's wallet then starts the transaction signing algorithm which signs his transaction using his private key.

4. The transaction is now broadcasted to the memory pool within the network.

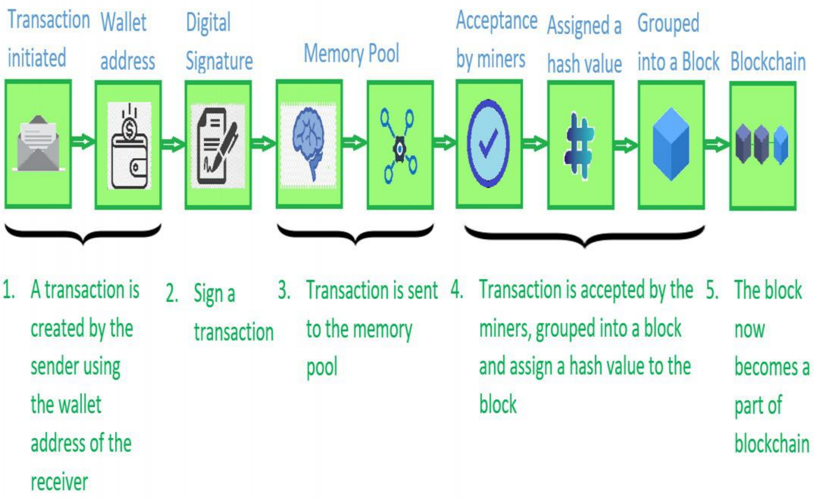
5. This transaction is eventually accepted by the miners. These miners, group this transaction into a block, find the **Proof of Work**, and assign this block a **hash value** to be mapped into the blockchain.

6. This block is now placed on the Blockchain.

7. As this block gains confirmation, it is accepted as a valid transaction in the network.

8. Once this transaction is accepted, Suraj finally gets his bitcoin.

The below diagram is a pictorial representation of the various stages in a transaction life cycle as discussed above.


Transaction initiated
Wallet address
Digital Signature
Memory Pool
Acceptance by miners
Assigned a hash value
Grouped into a Block
Blockchain
1. A transaction is created by the sender using the wallet address of the receiver
2. Sign a transaction
3. Transaction is sent to the memory pool
4. Transaction is accepted by the miners, grouped into a block and assign a hash value to the block
5. The block now becomes a part of blockchain

Transaction life-cycle in Blockchain

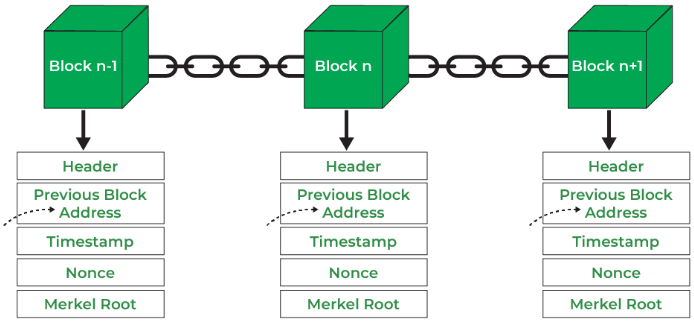
Structure:

What is Blockchain Architecture?

Blockchain is a technology where multiple parties involved in communication can perform different transactions without third-party intervention. Verification and validation of these transactions are carried out by special kinds of nodes.

Benefits of Blockchain:

- It is safer than any other technology.
- To avoid possible legal issues, a trusted third party has to supervise the transactions and validate the transactions.
- There’s no one central point of attack.
- Data cannot be changed or manipulated, it’s immutable.



1. **Header:** It is used to identify the particular block in the entire blockchain. It handles all blocks in the blockchain. A block header is hashed periodically by miners by changing the nonce value as part of normal mining activity, also Three sets of block metadata are contained in the block header.
2. **Previous Block Address/ Hash:** It is used to connect the i+1th block to the ith block using the hash. In short, it is a reference to the hash of the previous (parent) block in the chain.
3. **Timestamp:** It is a system verify the data into the block and assigns a time or date of creation for digital documents. The timestamp is a string of characters that uniquely identifies the document or event and indicates when it was created.
4. **Nonce:** A nonce number which uses only once. It is a central part of the proof of work in the block. It is compared to the live target if it is smaller or equal to the current target. People who mine, test, and eliminate many Nonce per second until they find that Valuable Nonce is valid.

5. **Merkel Root:** It is a type of data structure frame of different blocks of data. A Merkle Tree stores all the transactions in a block by producing a digital fingerprint of the entire transaction. It allows the users to verify whether a transaction can be included in a block or not.

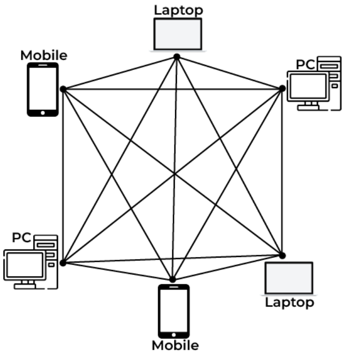
Key Characteristics of Blockchain Architecture:

- **Decentralization:** Eliminates the need for a central authority, ensuring data stability via consensus algorithms.
- **Persistency:** Transactions, once included, can't be deleted or altered, preventing invalid transactions from continuing.
- **Anonymity:** Users interact with generated addresses, maintaining privacy, though perfect privacy isn't guaranteed due to permanent records.
- **Auditability:** Tracks transactions through the Unspent Transaction Output (UTXO) model, enabling easy tracking and protection between transactions.
- **Transparency:** While transactions are transparent and trackable through addresses, they hide personal identity, ensuring fairness for all involved.
- **Cryptography:** Ensures security by implementing cryptographic techniques to safeguard blockchain data using ciphertext and ciphers.

Types of Blockchain Architecture:

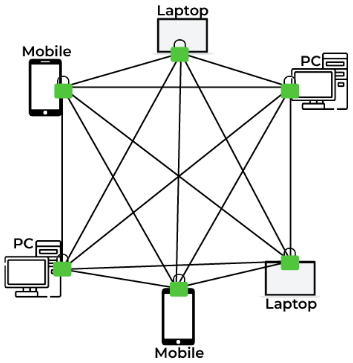
1. Public Blockchain:

- Open for anyone to join and participate, promoting decentralization and self-governance.
- Enables read, write, and audit activities openly, ensuring data immutability once validated.
- **Advantages:** Encourages network growth, immutability, rapid transactions.
- **Disadvantages:** Can be costly, potential identity issues, occasional slow processing, integration challenges.



2. Private Blockchain:

- Permission-based access limits network participation to authorized entities in transactions.
- Managed by an entity, controlling access rights and permissions within the network.
- **Advantages:** Controlled access, partial immutability.
- **Disadvantages:** Trust issues due to restricted access, vulnerability with increased participants.



3. Consortium Blockchain:

- Governed by a group of organizations and possibly by the government, fostering increased privacy and security.
- Intermediate decentralization, designed and accessed by collaborating organizations.
- **Advantages:** Aims for faster outputs, scalability, low transaction costs.
- **Disadvantages:** Relationship instability, lacks a clear economic model, flexibility issues.

Core Components of Blockchain Architecture:

1. **Node:** Network participants maintaining the distributed ledger, facilitating communication and new block additions.
2. **Transactions:** Contractual agreements transferring assets between parties, stored as a digital ledger copy.
3. **Block:** Record structures storing encrypted transactions, forming a chain-like structure in the blockchain.
4. **Chain:** Connects blocks through previous block hashes, establishing a sequential structure.
5. **Miners:** Validate cryptocurrency transactions in the mining process, ensuring their accuracy.
6. **Consensus:** Fault-tolerant mechanism achieving network agreement among distributed systems, crucial for record-keeping and stability.

There are different kinds of consensus mechanism algorithms, each of which works on different principles:

1. **Proof of Work (PoW):** Requires nodes to prove work done for the right to add transactions by solving cryptographic puzzles.
2. **Proof of Stake (PoS):** An energy-efficient alternative to PoW, based on staking cryptocurrency for transaction validation.
3. **Proof of Capacity (PoC):** Allows nodes to share memory space in the blockchain network.
4. **Proof of Elapsed Time (PoET):** Cryptographically encrypts time passage for resource-efficient agreement.

Genesis Block:

What is Genesis Block?

The Genesis Block represents the very first block in a blockchain. It's the foundational block that initializes the entire blockchain network. This block has no predecessor and serves as the starting point from which subsequent blocks extend.

Features of Genesis Block:

- **Unique Identifier:** It has a unique block number (often "0" or "1") as it precedes all other blocks.
- **No Previous Block Reference:** Since it's the first block, it lacks a reference to a previous block's hash.
- **Coinbase Transaction:** Typically includes a special transaction, known as the "coinbase transaction," which mints the initial cryptocurrency units in the blockchain.
- **Distinct Parameters:** Can contain unique settings, such as network configurations or initial protocols specific to the genesis of the blockchain.

Why Genesis Block is Needed?

- **Foundation Establishment:** It creates the initial building block for the blockchain, acting as its seed.
- **Historical Record:** Preserves critical data, including the first transactions or messages embedded by the creator.
- **Blockchain Inception:** Enables the launch and functionality of the entire blockchain network.

How to Verify Genesis Block:

- **Absence of Previous Hash:** Ensures that the block has no reference to a previous block's hash.
- **Unique Content Confirmation:** Verifies specific parameters or transactions unique to the genesis block's creation.

Significance of Genesis Block:

- **Symbolic Beginning:** Marks the inception of the blockchain, often accompanied by unique messages or data.
- **Immutable Commencement:** Data within the genesis block remains unalterable, forming an immutable record of the blockchain's origin.
- **Network Launchpad:** Acts as the starting point for the network, laying the groundwork for subsequent blocks and network operations.

Examples of Genesis Block:

- **Bitcoin:** Bitcoin's Genesis Block, mined by Satoshi Nakamoto in 2009, included a special message referencing a headline from The Times newspaper about bank bailouts during the 2008 financial crisis. It contained the text "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."
- **Ethereum:** Ethereum's Genesis Block, launched in 2015, carried unique settings and configurations that initiated the Ethereum blockchain and the Ether cryptocurrency.

The Genesis Block holds historical and symbolic significance, marking the commencement of blockchain networks and preserving immutable records of their origins. It's an essential element in understanding the genesis and evolution of decentralized systems like Bitcoin and Ethereum.

Bitcoin Mining:

What Is Bitcoin Mining?

Bitcoin mining is the process of validating and adding new transactions to the Bitcoin blockchain. Miners compete to solve complex mathematical puzzles to create new blocks, securing the network and earning rewards in the form of bitcoins.

Why Bitcoin Needs Miners:

Bitcoin relies on a decentralized network of miners to validate transactions and ensure consensus without a central authority. Miners' efforts secure the network, preventing double-spending and maintaining the integrity of the blockchain.

Why Mine Bitcoin?

Miners are incentivized by rewards - earning bitcoins for their efforts. Additionally, mining supports the network's security and transaction verification, contributing to the decentralized nature of Bitcoin.

How Much Is the Reward?

Initially, miners received 50 bitcoins per block. This reward halves approximately every four years through a process called "halving." As of now, it stands at 6.25 bitcoins per block.

What You Need to Mine Bitcoins

Mining requires specialized hardware (ASICs), access to low-cost electricity, a wallet to receive rewards, and mining software for computation.

The Mining Process:

Miners compete to solve complex mathematical puzzles, attempting to find a nonce that results in a hash below a target value. The first miner to solve it adds a new block to the blockchain and receives the reward.

What Are Mining Pools?

Mining pools are collaborations of miners who combine computational power to increase the chances of finding blocks collectively. Rewards are distributed among pool members based on their contributions.

Downsides of Mining:

- **Energy Consumption:** Mining consumes significant electricity, leading to environmental concerns.
- **High Entry Barriers:** Cost of specialized equipment and electricity can make mining less accessible to individuals.
- **Mining Centralization:** Large mining pools or entities can concentrate power, potentially impacting decentralization.

Bitcoin mining is a crucial process that supports the functionality and security of the Bitcoin network. While it offers rewards, it also poses challenges such as resource consumption and increasing centralization.

Difference between Hard Forks and Soft Forks in the Bitcoin Blockchain:

Aspect	Hard Fork	Soft Fork
Definition	Fundamental change requiring all nodes to upgrade.	Non-breaking upgrade allowing old nodes to accept new rules.
Compatibility	Creates a permanent divergence in the blockchain.	Maintains backward compatibility with the existing chain.
Node Consensus	Requires a majority of nodes to upgrade to the new rules.	Only needs a majority of miners to enforce new rules.
Rules Modification	Permits addition of new rules or changes to consensus rules.	Imposes stricter rules, restricting certain transactions.
Reversibility	Irreversible change, cannot revert to the old chain.	Potentially reversible by the network if necessary.
Community Consensus	Often contentious, causing community debates and splits.	Generally easier to achieve consensus among the community.
Example	Bitcoin Cash resulted from a hard fork of the Bitcoin blockchain.	SegWit was a soft fork implemented in the Bitcoin network.

Hard forks create a permanent split in the blockchain, necessitating all nodes to adopt the new rules, while soft forks maintain backward compatibility and can be adopted by nodes without creating a split.

Consensus Algorithms in Blockchain:

Blockchain operates without a central authority, ensuring security, immutability, and transparency. Consensus protocols are fundamental to Blockchain, enabling nodes to reach agreement on ledger states. They establish trust among unknown peers in a decentralized environment, ensuring that added blocks represent the network's agreed truth.

Proof of Work (PoW):

- Utilized in Bitcoin.
- Solves complex puzzles via computational power to mine blocks.

Practical Byzantine Fault Tolerance (PBFT):

- Allows nodes to reach consensus despite malicious actors.

Proof of Stake (PoS):

- Used in Ethereum.
- Validators invest in coins rather than computational power, validating blocks based on their stakes.

Delegated Proof Of Stake (DPoS):

- Relies on vote delegation; block rewards distributed accordingly.

Proof of Burn (PoB):

- Validators 'burn' coins irretrievably to mine blocks.

Proof of Capacity:

- Validators use hard drive space for mining.

Proof of Elapsed Time:

- Fairly selects the next block based on validators' wait time.

Various other consensus algorithms exist, like Proof of Activity, Proof of Weight, and Leased Proof of Stake, each tailored to specific network needs. The choice of consensus mechanism is critical, as it ensures the proper functioning and verification of transactions within Blockchain networks.

Proof of Work (PoW):

Proof of Work (PoW) is a consensus algorithm widely used in cryptocurrencies, aiming to validate transactions and create new blocks in the blockchain. Initially conceptualized in 1993, PoW was later employed by Satoshi Nakamoto in Bitcoin's paper in 2008. The term "proof of work" was coined in a publication by Markus Jakobsson and Ari Juels in 1999.

Principle and Purpose:

- PoW requires complex computations to mine blocks, offering a solution that's hard to find but easy to verify.
- Its aim is to establish agreement among nodes in a trustless environment, validating transactions and adding new blocks to the blockchain.

How PoW Works:

- Miners, nodes engaged in mining, solve computational puzzles to create blocks in the blockchain.
- The process involves validating transactions and appending them in chronological order to form a block.
- Miners compete to solve these complex mathematical problems for economic rewards, which decrease over time.

Mining and Energy Consumption:

- Mining verifies transactions, but the energy-intensive aspect involves linking new blocks to the existing blockchain.
- Miners receive rewards (currently 6.25 bitcoins) for successfully mining a block, with rewards halving periodically.
- Bitcoin adjusts mining difficulty to maintain a steady block creation rate (approximately one block every 10 minutes).

Bitcoin's PoW System:

- The Hashcash Proof of Work system underpins Bitcoin's mining process.
- Miners must find a nonce (unique value) that, when appended to data, results in a hash lower than the target hash.

Cryptographic Protocols:

- Commonly used cryptographic protocols include SHA-256 (used in Bitcoin) and others like Scrypt, SHA-3, scrypt-jane, and scrypt-n.

Challenges with PoW:

- **Risk of majority control:** A controlling entity owning 51% or more nodes can manipulate the blockchain.
- **Time and resource consumption:** Mining involves a time-consuming process that requires substantial computing power, leading to resource wastage.
- **Delayed transactions:** Transaction confirmation might take 10-60 minutes due to the mining process, causing delays.

Despite being widely used, PoW faces challenges regarding energy consumption, time inefficiency, and the risk of centralized control.

Proof of Stake (PoS):

Proof of Stake (PoS) is a consensus algorithm used in Blockchain to attain distributed agreement, initially proposed by Quantum Mechanic, and later detailed by Sunny King, leading to the introduction of Proof-of-Stake-based Peercoin.

Purpose: Addresses the energy-intensive nature of Proof-of-Work (PoW) used in Bitcoin.

Mechanics:

- Nodes stake a cryptocurrency amount, vying to validate a new block and earn fees.
- Selection combines stake quantity, coin-age, and randomization for fairness.

Workflow:

1. Nodes transact; PoS pools these transactions.
2. Nodes stake to become the validator for the next block, selected via the algorithm.
3. Validator verifies and publishes the block; stake remains locked until 'OK'-ed by other nodes.
4. If verified, validator gets stake and reward; else, stake is lost, marked 'bad,' and process restarts.

Features:

- Limited circulating coins; no creation of new coins (initiated by PoW).
- Transaction fees accumulate as rewards.
- Prevents a 51% attack due to the expensive nature of owning 51% of the cryptocurrency.

Advantages:

- Energy-efficient, as nodes don't compete like in PoW.
- Encourages decentralization by offering linear rewards, not exponential like PoW.
- Security against attacks due to the high cost of owning a majority stake.

Weaknesses:

- Potential centralization if a group owns a substantial stake.
- PoS is a relatively newer technology, still under research.
- 'Nothing at Stake' problem, where nodes face no disadvantage in supporting multiple blockchains during forks.

Blockchains using PoS:

- Ethereum (Casper update)
- Peercoin
- Nxt

Variants of PoS:

- Regular PoS
- Delegated PoS
- Leased PoS
- Masternode PoS

Practical Byzantine Fault Tolerance (pBFT):

Practical Byzantine Fault Tolerance (pBFT) is a consensus algorithm created in the late 90s by Barbara Liskov and Miguel Castro. It efficiently operates in asynchronous systems, optimizing for low overhead time. pBFT addresses issues present in existing Byzantine Fault Tolerance solutions, finding applications in distributed computing and blockchain.

What is Byzantine Fault Tolerance?

Byzantine Fault Tolerance ensures network consensus, even if some nodes fail to respond or provide incorrect information. It's derived from the Byzantine Generals' Problem, where a collective decision-making mechanism is employed to reduce the influence of faulty nodes.

How pBFT Works:

- Nodes are ordered, with a primary and secondary node configuration.
- All honest nodes aim to reach a consensus through the majority rule.
- A practical BFT system can function when the number of malicious nodes is less than one-third of all nodes, enhancing security as nodes increase.

Phases of pBFT Consensus Rounds:

1. Client sends a request to the primary node.
2. Primary node broadcasts the request to all secondary nodes.
3. Nodes perform the service and send replies to the client.
4. Successful service occurs when the client receives 'm+1' matching replies from different nodes.

Advantages of pBFT:

- Energy efficiency without complex computations (unlike PoW).
- Transaction finality without multiple confirmations.
- Low reward variance, incentivizing all nodes participating in decision-making.

Limitations of pBFT:

- Inefficiency with large networks due to high communication overhead.
- Vulnerability to Sybil attacks as the network size increases.

Proof of Burn (PoB):

What is Proof of Burn?

- PoB is a consensus algorithm used in Blockchain networks, addressing drawbacks of Proof of Work (PoW).
- Validators 'burn' coins irretrievably, sacrificing them to earn the right to mine, replacing the computational power utilized in PoW.
- By sending coins to an inaccessible address, validators earn the privilege to mine via a random selection process.

Purpose of Proof of Burn:

- PoB addresses PoW's energy-intensive nature and high capital requirements.
- Validators demonstrate commitment to the currency by sacrificing coins for long-term potential gains.

How Proof of Burn Works:

- Validators send coins to inaccessible addresses, reducing the coin supply permanently.
- Reduced availability potentially increases coin value.
- Continuous burning maintains mining capacity, ensuring fairness for latecomers.

Comparison with Proof of Stake (PoS):

- PoB ensures permanent scarcity compared to PoS, where coins return to circulation after validators unlock them.
- Advantages of PoB include reduced energy consumption, fairer coin distribution, and long-term commitment incentives.
- Disadvantages involve risk, potential resource wastage, and the "rich getting richer" scenario due to accumulated coins.

Proof of Burn presents an innovative approach to consensus algorithms, balancing sustainability, fairness, and commitment within Blockchain networks.

Proof of Elapsed Time (PoET):

Proof of Elapsed Time (PoET) is a consensus algorithm developed by Intel in 2016 for blockchain networks, aiming to reduce energy consumption and resource intensity associated with other methods like Proof of Work (PoW).

What is Proof of Elapsed Time (PoET)?

PoET determines the next block creator in a permissioned blockchain. It works on a randomized timer system that allocates a wait time to each network node. The node with the shortest wait time wakes up, generates a new block, and broadcasts this to the network.

How Does PoET Work?

1. Random Wait Time: Every node generates a random wait time and sleeps for that duration.

2. Block Creation: The node with the shortest wait time becomes the block leader, creates a new block, and adds it to the chain.

3. Network Broadcasting: Information about the new block spreads across the network, and the process repeats for the next block.

PoET Benefits:

- **Low Power Consumption:** Nodes can conserve energy by 'sleeping' for specified periods.
- **Resource Efficiency:** Reduces resource intensity and scales well for faster transaction processing.
- **High Transaction Rate:** Can achieve up to a million transactions per second.
- **Equal Opportunity:** Fair opportunity for all network participants with the time object activation.
- **Permissioned Security:** Ensures network security against cyber threats.

PoET Limitations:

- **Specialized Hardware:** Requires specific hardware, limiting widespread adoption.
- **Compatibility Challenges:** Relies on Intel's technology, which might pose compatibility issues with other tools.

Comparison between PoW, PoS, and PoET:

Parameters	**PoW**	**PoS**	**PoET**
Blockchain type	Permissionless	Both	Both
Transaction finality	Probabilistic	Probabilistic	Probabilistic
Transaction rate	Low	High	Medium
Token needed	Yes	Yes	No
Cost of participation	Yes	Yes	No
Scalability of peer network	High	High	High
Trust model	Untrusted	Untrusted	Untrusted

Unit 4

Smart Contracts:

A Smart Contract, also known as a crypto-contract, automates the execution and enforcement of digital asset transfers based on predefined conditions. Operating like a traditional contract but enforced by code, it can be executed directly as programmed.

Smart Contract Evolution:

- **Bitcoin's Smart Contracts:** Initially, Bitcoin facilitated simple smart contracts for value transfer, checking basic conditions like available sender funds.
- **Ethereum's Advancements:** Ethereum expanded smart contract capabilities by using a Turing-complete language, allowing complex custom contracts. In contrast, Bitcoin contracts were limited by a Turing-incomplete language.
- **Common Platforms:** Ethereum, Solana, Polkadot, and Hyperledger fabric are among the commonly used smart contract platforms.

Features:

- **Distributed:** Contracts are replicated and distributed across all network nodes, ensuring unchangeable conditions.
- **Deterministic:** Contracts execute predefined functions only under specific conditions, delivering consistent outcomes.
- **Immutable:** Once deployed, contracts cannot be altered but can be removed if previously implemented.
- **Autonomous:** No intermediaries; contracts are made and executed by involved parties with no central control.
- **Customizable:** Contracts can be modified before deployment to serve specific purposes.
- **Transparent & Trustless:** Code visibility on a public ledger eliminates the need for third-party verification.

Capabilities:

- **Accuracy:** Executes precisely as programmed, ensuring accuracy based on the programmed logic.
- **Automation:** Automates manual tasks/processes.
- **Speed:** Reduces transaction processing time through coded automation.
- **Backup & Security:** Each blockchain node maintains a shared ledger, providing a robust backup and secure encryption against tampering.
- **Cost Savings:** Eliminates intermediaries, reducing paperwork and associated costs.
- **Information Management:** Manages user agreements and application-related data.

Working:

- **Contract Creation:** Details and permissions written in code form the contract.
- **Triggering Conditions:** Specific events or conditions initiate contract execution.
- **Code Execution:** The contract's logic executes autonomously upon meeting conditions.
- **Blockchain Updates:** Executed contracts are recorded across all network nodes, becoming unmodifiable ledger entries.

Applications:

- **Real Estate & Vehicle Ownership:** Facilitates transparent transactions and tracks ownership.
- **Music Industry:** Manages music ownership and royalties transparently.
- **Government Elections:** Enhances transparency and security in voting processes.
- **Healthcare & Management:** Automates payment processes and streamlines decisions.

Advantages:

- **Recordkeeping:** Maintains a secure, chronological record of transactions.
- **Autonomy & Reduced Fraud:** Direct dealings, less reliance on intermediaries, and reduced fraudulent activities.
- **Enhanced Trust & Cost Efficiency:** Immutable, direct agreements, reduced costs, and paperwork.

Challenges:

- **Regulatory Limitations:** Lack of international regulations complicates oversight.
- **Complex Implementation:** Still a relatively new and complex concept.
- **Immutability & Alignment:** Immutability challenges revisions, requiring new contracts for changes. Ensuring alignment with all parties' intentions can be difficult.

Smart contracts revolutionize business agreements but face challenges related to regulations, complexity, and immutability. Despite challenges, they offer enhanced trust, cost efficiency, and automation across various industries.

Ethereum:

What is Ethereum?

Ethereum is a Blockchain network that introduced a built-in Turing-complete programming language that can be used for creating various decentralized applications(also called Dapps). The Ethereum network is fuelled by its own cryptocurrency called ‘ether’.

- The Ethereum network is currently famous for allowing the implementation of smart contracts. Smart contracts can be thought of as ‘cryptographic bank lockers’ which contain certain values.
- These cryptographic lockers can only be unlocked when certain conditions are met.
- Unlike bitcoin, Ethereum is a network that can be applied to various other sectors.
- Ethereum is often called Blockchain 2.0 since it proved the potential of blockchain technology beyond the financial sector.
- The consensus mechanism used in Ethereum is Proof of Stakes(PoS), which is more energy efficient when compared to that used in the Bitcoin network, that is, Proof of Work(PoW). PoS depends on the amount of stake a node holds.

History of Ethereum:

- **2013:** Ethereum was first described in Vitalik Buterin’s white paper in 2013 with the goal of developing decentralized applications.
- **2014:** In 2014, EVM was specified in a paper by Gavin Wood, and the formal development of the software also began.
- **2015:** In 2015, Ethereum created its genesis block marking the official launch of the platform.
- **2018:** In 2018, Ethereum took second place in Bitcoin in terms of market capitalization.
- **2021:** In 2021, a major network upgrade named London included Ethereum improvement proposal 1559 and introduced a mechanism for reducing transaction fee volatility.
- **2022:** In 2022, Ethereum has shifted from PoW(Proof-of-Work) to PoS(Proof-of-State) consensus mechanism, which is also known as Ethereum Merge. It has reduced Ethereum’s energy consumption by ~ 99.95%.

Features of Ethereum

1. **Smart contracts:** Ethereum allows the creation and deployment of smart contracts. Smart contracts are created mainly using a programming language called solidity. Solidity is an Object Oriented Programming language that is comparatively easy to learn.
2. **Ethereum Virtual Machine (EVM):** It is designed to operate as a runtime environment for compiling and deploying Ethereum-based smart contracts.
3. **Ether:** Ether is the cryptocurrency of the Ethereum network. It is the only acceptable form of payment for transaction fees on the Ethereum network.
4. **Decentralized applications (Dapp's):** Dapp has its backend code running on a decentralized peer-to-peer network. It can have a frontend and user interface written in any language to make calls and query data from its backend. They operate on Ethereum and perform the same function irrespective of the environment in which they get executed.
5. **Decentralized autonomous organizations (DAO's):** It is a decentralized organization that works in a democratic and decentralized fashion. DAO relies on smart contracts for decision-making or decentralized voting systems within the organization.

Type of Ethereum Accounts:

Ethereum has two types of accounts: An externally owned account (EOA), and a Contract account. These are explained as following below:

- **Externally owned account (EOA):** Externally owned accounts are controlled by private keys. Each EOA has a public-private key pair. The users can send messages by creating and signing transactions.
- **Contract Account:** Contract accounts are controlled by contract codes. These codes are stored with the account. Each contract account has an ether balance associated with it. The contract code of these accounts gets activated every time a transaction from an EOA or a message from another contract is received by it. When the contract code activates, it allows to read/write the message to the local storage, send messages and create contracts.

How Does Ethereum Work?

Ethereum implements an execution environment called Ethereum Virtual Machine (EVM).

- When a transaction triggers a smart contract all the nodes of the network will execute every instruction.
- All the nodes will run The EVM as part of the block verification, where the nodes will go through the transactions listed in the block and runs the code as triggered by the transaction in the EVM.
- All the nodes on the network must perform the same calculations for keeping their ledgers in sync.
- Every transaction must include:
  - Gas limit.
  - Transaction Fee that the sender is willing to pay for the transaction.
- If the total amount of gas needed to process the transaction is less than or equal to the gas limit then the transaction will be processed and if the total amount of the gas needed is more than the gas limit then the transaction will not be processed the fees are still lost.
- Thus it is safe to send transactions with the gas limit above the estimate to increase the chances of getting it processed.

Real-World Applications of Ethereum:

- **Voting:** Voting systems are adopting Ethereum. The results of polls are available publicly, ensuring a transparent fair system thus eliminating voting malpractices.
- **Agreements:** With Ethereum smart contracts, agreements and contracts can be maintained and executed without any alteration. Ethereum can be used for creating smart contracts and for digitally recording transactions based on them.
- **Banking systems:** Due to the decentralized nature of the Ethereum blockchain it becomes challenging for hackers to gain unauthorized access to the network. It also makes payments on the Ethereum network secure, so banks are using Ethereum as a channel for making payments.
- **Shipping:** Ethereum provides a tracking framework that helps with the tracking of cargo and prevents goods from being misplaced.
- **Crowdfunding:** Applying Ethereum smart contracts to blockchain-based crowdfunding platforms helps to increase trust and information symmetry. It creates many possibilities for startups by raising funds to create their own digital cryptocurrency.

Benefits of Ethereum:

- **Availability:** As the Ethereum network is decentralized so there is no downtime. Even if one node goes down other computing nodes are available.
- **Privacy:** Users don’t need to enter their personal credentials while using the network for exchanges, thus allowing them to remain anonymous.
- **Security:** Ethereum is designed to be unhackable, as the hackers have to get control of the majority of the network nodes to exploit the network.
- **Less ambiguity:** The smart contracts that are used as a basis for trade and agreement on Ethereum ensure stronger contracts that differ from the normal traditional contracts which require follow-through and interpretation.
- **Rapid deployment:** On Ethereum decentralized networks, enterprises can easily deploy and manage private blockchain networks instead of coding blockchain implementation from scratch.
- **Network size:** Ethereum network can work with hundreds of nodes and millions of users.
- **Data coordination:** Ethereum decentralized architecture better allocates information so that the network participants don’t have to rely on a central entity to manage the system and mediate transactions.

Drawbacks of Ethereum:

- **Complicated programming language:** Learning solidity from programming smart contracts on Ethereum can be challenging and one of the main concerns is the scarcity of beginner-friendly classes.
- **Volatile cryptocurrency:** Ethereum investing can be risky as the price of Ether is very volatile, resulting in significant gains as well as a significant loss.
- **Low transaction rate:** Bitcoin has an average transaction rate of 7TPS and Ethereum has an average speed of 15 TPS which is almost double that of bitcoin but it is still not enough.

Gas and Fees:

Ethereum Gas is a section that calculates the quantity of calculation action that it takes to perform specific functions. Every function that carries position in Ethereum like transactions and smart contracts etc. performance needs some part of gas. It is essential to the blockchain P2P network because it is the power that authorizes it to accomplish exactly what an automobile needs fuel to drive. Gas refers to the cost required to complete a deal on the Ethereum network.

Facts about Ethereum Gas:

- Gas prices are delivered in the form of Ethereum's born money, the currency of Ethereum is ETH.
- Gas costs are indicated in "gwei" which is a movement of Ethereum, every single "gwei" is equivalent to 0.000000001 ETH.
- For sample, rather than stating that the gas costs 0.000000001 ether, say, the gas costs 1 "gwei".
- The term "gwei" means "Giga-wei", which is equivalent to 1,000,000,000 "wei".
- "Wei" is called after "Wei Dai" that is the creator of b-money (least unit of ETH).

GWEI:

Gwei is a combination of "giga" and "wei". It is a sect of the blockchain technology ETH, this coin is operated on the Ethereum P2P network. ETH is a blockchain medium, like Bitcoin and Binance, where users can make transactions with respect to buying and selling interests and benefits without the involvement of an intermediator.

Example:

For example, Rahul needs to give 1 ETH to Shubham. During the transaction, the gas boundary is 21000 units, and the gas price is 200 gwei.

Total fee costs = Gas units (limit) Gas price per unit

= 21000 200

= 4,200,000 gwei (0.0042 ETH)

- When Rahul dispatched the funds, 1.0042 ETH would be subtracted from Rahul's account.
- Shubham would be credited 1.0000 ETH only as 0.0042 is the fess of Miner.

Now **after upgradation**, increased advantages presented by the difference contain more profitable trade fee computation, typically more rapid trade inclusion, and canceling the ETH distribution by burning a portion of trade fees.

- Beginning with the peer-to-peer network upgrade, each block unit has a ground fee, the lowest price per unit of gas for inclusion in this block unit, estimated by the network founded on request.
- Because the ground fee of the trade fee is burnt, users are also hoped to put a tip in their dealings.
- The information pays miners for managing and breeding user trades in blocks and is hoped to be set automatically by most wallets.

Total fee after upgradation = Gas units (limit) (Base fee + Tip)

For example, Shubham has to pay 1 ETH to Rahul. This process has a gas limit of 21000 units and a base fee of 100 gwei. Shubham includes a tip of 10 gwei.

Total fee after upgradation = Gas units (limit) (Base fee + Tip)

= 21000 (100 + 10)

= 2,310,000 gwei (0.00231 ETH).

- When Shubham sends the funds, 1.00231 ETH will be subtracted from Shubham's account.
- Rahul will be credited 1.0000 ETH and 0.00021 ETH will be received by the miner as the tip.
- A ground fee of 0.0021 ETH is ignited.

Gas Fees:

The gas fees include Base, Priority, Max, and calculating fees. Let's discuss these terms in detail.

1. Base fees:

- Each alliance has a ground fee which serves as a fund price.
- The ground fee is figured alone of the existing alliance and is rather specified by the alliances before it pushes trade prices better for users.
- When the block is excavated the base fee is "burned", dragging it from regulation.
- The ground fee is evaluated by instructions that compare the length of the earlier block with the marked size.
- The base fee intention rise by a max of 12.5% per block if the marked block size is surpassed.

2. Priority fee:

- Apart from the base fee obtained, the advancement presented a priority fee i.e. tip to miners to contain a trade in the alliance.
- Without tips, miners can see it financially possible to drill cleared blocks because they can obtain the exact alliance prize.
- Under normal circumstances, a little tip provides miners with the slightest encouragement to maintain a transaction.
- For dealings that require getting preferentially conducted ahead of different trades in the same block, a more elevated tip will be essential to endeavor to outbid contending trades.

3. Max fee:

- To conduct trade on the P2P network, users can select the greatest limit they are inclined to spend for their dealing to be completed.
- This additional circumference is called the max fee/Gas.
- For a trade to be completed, the max fee must surpass the aggregate of the base and priority fees.
- The trade sender is repaid the contrast between the max fee and the total of the ground(base) fee and tip.

4. Calculating fees:

- The main benefit of the upgrade is enhancing the user's knowledge when charging trade fees.
- In the wallets that sustain the upgrade rather than explicitly commenting to pay the transaction from a wallet, providers will automatically set a suggested transaction fee (base fee + suggested priority fee) to decrease the quantity of complexness loaded on their users.

Importance of Gas Fees:

Below are some of the reasons why gas fess is important:

- Gas fees help support the Ethereum peer-to-peer network security.
- By demanding a price for every analysis performed on the web grid, it prevents evil performers from spamming the web grid.
- To evade unexpected or malicious endless circles or different computational wastage in principle, every trade is needed to set a boundary to how multiple computational efforts of code implementation can operate.
- The basic division of accounting is "gas".
- A trade organizes a boundary and any unit of gas not utilized in trade is replaced (i.e. max fee – (base fee + tip)).

Why gas fees can go high?

- Increased gas prices exist because of the fame of Ethereum.
- Conducting any function on Ethereum needs depleting gas, and the gas area is determined per alliance.
- Prices contain measures, holding or exploiting data, and swallowing various parts of "gas" units.
- As app functionality produces additional complexity, the digit of functions a wise contract achieves also develops, representing each trade brings up more additional area of a fixed measure block.
- If the demand is quite high, users must present a more elevated tip payment to try and outbid other users' dealings.
- A more increased tip can construct it additional possible that your trade will convey into the subsequent block.

Initiative to reduce gas costs:

- The ETH efficiency advancements should eventually manage some of the gas cost points, allowing the medium to process thousands of trades globally per moment.
- Second layer scaling is a direct ambition to significantly enhance gas prices, user knowledge, and scalability.
- The recent proof-of-stake(POS) sample based on the Beacon Chain, should decrease heightened control consumption and dependence on technological hardware.
- This chain resolve permits decentralized ETH P2P networks to compromise and support network security while restricting gas consumption by rather demanding an economic responsibility.

Strategies to reduce gas costs:

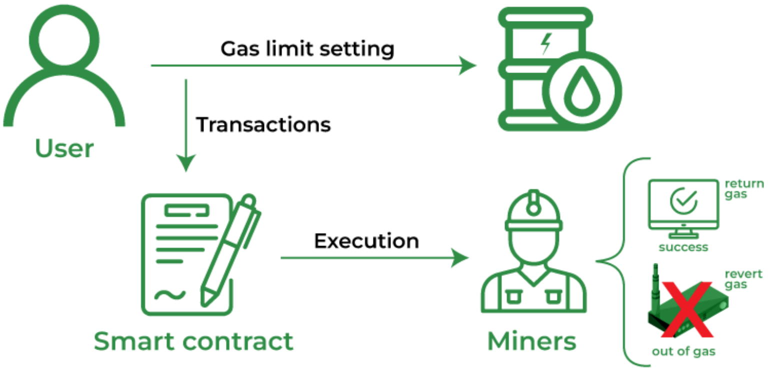
- Strategies to decrease gas costs for ETH, Users can select a direction to display the important status of the user's transaction.
- Miners intention perform trades that suggest a more increased tip per gas, as they hold the tips that users spend and resolve be slightly tilted to conduct transactions with more down tips specified.
- If users like to observe gas costs, then they can send ETH for smaller, user can utilize multiple other tools given below:
- Etherscan, Blocknative ETH Gas Estimator, ETH Gas Station, and Cryptoneur Gas Fees Calculator aid in assessing Ethereum gas prices for both Class 0 and Class 2 EIP-1559 transactions.

Why do gas fees exist?

- Gas prices assist maintain the Ethereum grid safe. By demanding a price for every analysis performed on the grid, it controls harmful attackers from spamming the grid.
- To bypass unexpected code, every trade needs to set a limitation to the multiple computational efforts of regulation performance.
- The absolute unit of analysis is “gas”.
- Moreover, a trade contains a limitation, any gas not operated in a transaction is produced to the user (i.e. max fee – (base fee + tip) is produced).

How does block size affect the base fees?

The base fee is computed by a procedure that resembles the dimensions of the last block (the part of gas utilized for all the trades) with the target size. The base fee will rise by a most of 12.5% per alliance if the target block size is overextended.



The World State:

The "world state" in a blockchain context refers to the current state of the entire system at any given point in time. It's a crucial concept in understanding how blockchain networks function, particularly in systems like Ethereum.

What is the World State?

1. **Data Structure:** The world state is essentially a database or data structure that represents the current status of all accounts and their balances, as well as other essential information in a blockchain network.
2. **Immutable State:** In a blockchain, once a block is added and validated, it contributes to the world state. This state reflects the result of all transactions executed and accepted in the network. Once a block is appended to the chain, the world state gets updated accordingly.
3. **Account Information:** The world state contains detailed information about all accounts (externally owned accounts and smart contracts), including their current balances, code, storage, and nonce (a value representing the number of transactions sent from an account).
4. **Historical Records:** Every change in the world state is recorded, but the world state itself represents the current state of the system. The historical data is retained in the blockchain as a sequence of blocks.

Role of World State in Blockchain:

1. **Efficiency:** It streamlines the process of verifying transactions by allowing nodes to quickly access the current state of all accounts without needing to recompute from the beginning of the blockchain.
2. **Transaction Verification:** When a new transaction occurs, nodes verify its validity by checking against the world state. For instance, they check if the sender has enough balance to complete the transaction.
3. **Consistency and Integrity:** As the blockchain is immutable and append-only, the world state maintains the integrity and consistency of the system by reflecting the cumulative effects of all transactions.
4. **Smart Contract Execution:** For Ethereum and similar platforms, the world state is vital for executing smart contracts. When a contract is executed, it modifies the world state by updating account balances or other data as per the contract's logic.

How it's Represented:

- **Merkle Trees:** To efficiently represent the world state, blockchain networks often use Merkle trees—a data structure that enables quick and secure verification of large data sets by hashing them into a tree-like structure.
- **State Roots:** In Ethereum, the world state is represented by a state root, which is essentially the root hash of a Merkle Patricia tree. This root is included in each block header, providing a quick way to check the integrity of the world state.

The world state concept provides an efficient means for blockchain networks to maintain a comprehensive and verifiable representation of the system's state at any given moment, crucial for ensuring the network's reliability and consistency.

Ethereum Virtual Machine (EVM):

Introduction:

EVM serves as the runtime environment for executing smart contracts within the Ethereum network. Isolated from the system, it ensures that operations within it do not impact external data or programs. It interprets and executes smart contract code written in languages like Solidity.

Purpose of EVM:

- Acts as Ethereum's "world computer," executing smart contracts securely.
- Supports complex scripts, enabling the creation of crypto-contracts.
- Facilitates automated execution of conditions within smart contracts, ensuring predetermined outcomes.

How Does EVM Work?

- EVM executes scripts defining operations on Ethereum's blockchain.
- Smart contracts define exchanges of assets and information based on preset conditions.
- Utilizes a Turing-complete environment, enabling execution of virtually any computer-based task.
- Forms the foundation for decentralized applications (DApp’s) within the Ethereum ecosystem.
- Consists of the EVM component (running Solidity) and facilitates metadata storage (uncles).

How Gas Relates to EVM's Performance:

- Gas measures computational power, determining the execution time for transactions and contracts.
- Each transaction has a gas limit; complexity increases gas consumption.

Benefits of EVM:

- Executes untrusted code securely without risking data.
- Allows complex smart contracts to interact across platforms.
- Provides deterministic processing and facilitates distributed consensus.

Downsides of EVM:

- Incurs high costs for storing data and executing transactions.
- During network congestion, gas prices rise, impacting transaction processing.

- Requires technical expertise for smart contract development and use.

Conclusion:

The Ethereum Virtual Machine serves as the backbone of Ethereum's smart contract functionality, allowing for the secure execution of code and the creation of decentralized applications. While powerful, it comes with complexities and cost implications, necessitating technical proficiency for its effective use.

Ethereum Accounts:

Ethereum is a blockchain-based open-source cryptocurrency platform that encompasses smart contract functionality. Ether (ETH) serves as Ethereum's cryptocurrency, utilized for transactions and executing smart contracts. Ethereum extends beyond mere transactional capabilities, enabling app development and contract implementation.

What Are Ethereum Accounts?

Ethereum accounts function akin to bank accounts for holding, transferring Ether, and executing smart contracts. These accounts comprise an Ethereum address and a private key—20 bytes of the SHA3 hashed public key determine the Ethereum address.

Types of Ethereum Accounts:

1. Externally Owned Account (EOA): Similar to Bitcoin accounts, EOAs are controlled by a private key. They're created with wallets, enabling balance checks, transactions, and smart contract interactions. EOAs can trigger code execution in contract accounts.

Advantages:

- Enable diverse actions like token transfers or contract creation.
- Incapable of listing incoming transactions.

2. Contract-Based Account: Formed upon deploying contract code, these accounts are governed by contracts and accessed through unique addresses. They list incoming transactions and support Multisig Account functionality.

Advantages:

- Can initiate incoming transactions.

Disadvantages:

- Incurs gas costs for creation.
- Cannot independently trigger transactions.

Types of Contract Accounts:

Three types:

- **Simple Account:** Single owner account.
- **Multisig Account:** Contains multiple owner accounts.
- **Simplest Account:** Functions similarly to Multisig Account.

Externally Owned Accounts vs Contract-Based Accounts:

S. No.	Externally Owned Accounts	Contract Accounts
1.	This account is controlled by humans.	This account is controlled Contract Code.
2.	The private key is needed to access EOAs.	No key is needed to access Contract Accounts.
3.	EASs are created automatically on creating a wallet.	CA require EOAs to be activated.
4.	EOAs do not have their own associated code.	CAs have their own associated code.
5.	No execution fee is associated with EOAs.	The execution fee is associated with CAs.
6.	Code hash is an empty string.	Code hash represents the code associated with the account.

Fields in Ethereum Accounts:

1. Nonce: Tracks the number of transactions from an account, ensuring transaction uniqueness.

2. Ether Balance: Denotes the account's Ether holdings.

3. Contract Code: Present in contract accounts, immutable once executed.

4. Storage: Remains empty unless specified.

5. Code Hash: Hash representing the code in contract accounts; empty string for EOAs.

Externally Owned Accounts and Key Pairs:

- **Ownership:** EOA if controlled by a private key; smart-contract account if only an address exists.
- **Private Key:** Grants control and access to assets and contracts; kept secure by the user.
- **Public Key:** Account identity derived from the private key; used for transactions between accounts.

Decentralized Apps (dApp's) in Blockchain:

Decentralized apps (dApp's) are distinct digital applications or programs operating on a blockchain, differing fundamentally from regular applications. Unlike centralized applications running on servers owned by a single entity, dApp's function on a decentralized peer-to-peer (P2P) network based on blockchain technology.

What are Decentralized Apps (dApp's)?

Decentralized applications, or dApp's, are open-source software applications distributed across a decentralized P2P network. Imagine a Twitter-like app where posts are immutable—no single entity has the authority to delete content.

dApps have specific requirements:

1. **Open Source:** Codebase is openly available, requiring majority agreement for changes.
2. **Decentralization:** Operates on a public, decentralized blockchain, ensuring security and transparency.
3. **Incentive:** Provides cryptographic tokens as incentives to users supporting the dApp ecosystem.
4. **Protocol:** Demonstrates the value of a process in a verifiable manner.

How Do dApp's Work?

A dApp's backend code runs on a decentralized P2P network, similar to traditional applications but with distinct features:

- **Decentralization:** Operates on Ethereum, an open public decentralized platform.
- **Deterministic:** Performs consistently regardless of execution environment.
- **Turing Complete:** Can execute any action with requisite resources.
- **Isolated:** Executes within an Ethereum Virtual Machine, preventing smart contract bugs from disrupting the blockchain.

Most Common Platforms For Creating dApps:

Several Blockchain platforms are utilized for creating dApps, including:

- **Ethereum:** A leading decentralized open-source blockchain hosting over 2500 dApps, featuring its native cryptocurrency, Ether (ETH).
- **NEO:** Known as the Chinese Ethereum, focusing on scalability and hosting around 100 dApps.

- **TRON:** Emerging as a competitor to Ethereum, renowned for gaming and gambling apps and hosting approximately 1500 dApps.

Popular dApps:
Some noteworthy dApps include:

- **CryptoKitties:** Entertaining app for buying, breeding, and selling digital cats on the blockchain.
- **OpenSea:** Facilitates interaction among various blockchain-based game collectibles.
- **WINk:** A popular gambling dApp on TRON rewarding users with tokens.
- **IPSE:** A blockchain-based search engine ensuring privacy and security.
- **Blockchain Cuties:** Offers various collectible creatures accessible across multiple blockchain platforms.

Advantages of dApps:

- **Fault Tolerance:** Ensures availability despite individual node failures.
- **Privacy:** Users operate without revealing personal information.
- **Data Integrity:** Immutable and tamper-proof data on the blockchain.
- **Flexible Development:** Ethereum offers a flexible environment for dApp creation.
- **Verifiable Behavior:** Smart contracts execute predictably without central authority monitoring.

Disadvantages of dApps:

- **Performance Overhead:** Achieving high security involves significant computational resources.
- **Maintenance Complexity:** Hard to update and maintain code modifications requiring consensus.
- **Scalability Challenges:** Scaling decentralized networks poses challenges.
- **User Experience Complexity:** Involves using public and private keys, making user-friendly interfaces challenging.
- **Potential Centralization:** Designing user-friendly dApps may lead to centralized services, negating blockchain's benefits.
- **Network Congestion:** High usage of computational resources may lead to network congestion.

Conclusion: dApp’s, as the vanguard of blockchain innovation, offer heightened security and transparency, set to gain traction with the maturation of blockchain tech, inviting exploration and adoption for a diverse digital landscape.

Bitcoin vs Ethereum:

Basis	Bitcoin	Ethereum
Definition	Bitcoin (abbreviation: BTC; sign: □) is a decentralized digital currency that can be transferred on the peer-to-peer bitcoin network.	Ethereum is a decentralized global software platform powered by blockchain technology. It is most commonly known for its native cryptocurrency, ether (ETH).
Purpose	The purpose of bitcoin was to replace national currencies during the financial crisis of 2008.	The purpose of Ethereum was to utilize blockchain technology for maintaining a decentralized payment network and storing computer code.
Smart Contracts	Although bitcoin do have smart contracts, they are not as flexible or complete as Ethereum smart contracts. Smart contracts in Bitcoin does not have all the functionality that a programming language would give them.	Ethereum allows us to create smart contracts. Smart contracts are computer codes that is stored on a blockchain and executed when the predetermined terms and conditions are met.
Smart Contract Programming Language	Smart contracts on Bitcoin are written in programming languages like Script, Clarity.	Smart contracts on Ethereum are written in programming languages like Solidity, Vyper, etc.
Transactions	Generally, bitcoin transactions are only for keeping notes.	Ethereum transactions may contain some executable code.
Hash Algorithm	Bitcoin runs on the **SHA-256** hash algorithm.	Ethereum runs on the **Keccak-256** hash algorithm.
Consensus Mechanism	The Proof-of-Work (PoW) is the consensus mechanism used by the Bitcoin network.	The Proof-of-Stake is the consensus mechanism used by Ethereum.
Block Time	The block time of bitcoin is 10 minutes.	The block time of Ethereum is 14 to 15 seconds.
Block Limit	The bitcoin blockchain has a block limit of 1 MB.	The Ethereum blockchain does not have a block limit.
Popularity	Bitcoin is the most popular digital currency in the market to date.	Ether, native currency of Ethereum is the second-largest cryptocurrency after bitcoin to date.

Energy Consumption	Energy consumption is very high.	Energy consumption is very low as compared to bitcoin
Energy Consumption rate	Energy consumption rate of bitcoin mining system 3.2 Million household.	Energy consumption rate of bitcoin mining system 1.2 Million household.
Structure	Structure of bitcoin is simple and robust.	Structure of Ethereum is complex and feature rich
Rewards	Miner got nearly 6.25 BTC on successfully adding new block in network.	Miner got nearly 5 BTC along with same additional rewards on successfully adding new block in network.
Assets	Assets of Bitcoin is BTC.	Assets of Ethereum is Ether.

Unit 5

Blockchain Use Cases:

1. **Land Registry Records:**
   Blockchain technology's tamper-proof nature makes it ideal for maintaining land registry records. By digitizing these records on a blockchain, governments or authorities can ensure immutable documentation of property titles, ownership history, and transactions. This transparency significantly reduces the likelihood of fraudulent land deals and property disputes. Individuals and entities can access accurate, updated information on land ownership, contributing to a more secure and transparent real estate ecosystem.

2. **Cross-border payments over blockchain:**
   Traditional cross-border payments are often complex, involving multiple intermediaries and lengthy settlement times. Blockchain streamlines this process by offering a decentralized network for direct peer-to-peer transactions. Utilizing cryptocurrencies or stablecoins on blockchain networks for cross-border payments significantly reduces transaction fees, eliminates intermediaries, and accelerates settlement times, providing faster and more cost-effective global money transfers.

3. **Project Ubin:**
   Project Ubin, initiated by the Monetary Authority of Singapore (MAS) and collaborating financial institutions, explores blockchain's potential in enhancing the efficiency of interbank payments and securities settlements. The project aims to develop prototypes and test blockchain-based systems for interbank payments, cross-border transactions, and securities settlements. By leveraging blockchain technology, Project Ubin seeks to modernize Singapore's financial infrastructure and foster innovation in the banking sector.

4. **Food Security:**
   Blockchain's transparency and traceability features are instrumental in ensuring food security. Through blockchain-powered supply chain solutions, consumers can access comprehensive information about the journey of food products—from farm to table. Details about sourcing, production, transportation, and storage are recorded on an immutable ledger, enhancing food safety measures. This transparency minimizes food fraud and ensures adherence to quality and safety standards.

5. **Supply Chain Financing:**
   Blockchain-enabled supply chain financing optimizes financing processes by offering real-time visibility into transactions and inventory movements. Smart contracts on blockchain automatically trigger financing upon fulfilment of predefined conditions, reducing delays and improving cash flow for suppliers. Financial institutions benefit from reduced risks, as they gain real-time insights into the status of goods in transit.

6. **Voting System and Identity on Blockchain:**
   Blockchain-based voting systems ensure secure, transparent, and tamper-proof elections. The decentralized nature of blockchain prevents unauthorized access and manipulation of voting records. Additionally, blockchain technology enhances identity management by providing a secure platform for managing digital identities. Users have control over their identity data, reducing the risk of identity theft and ensuring data privacy in various applications.

7. **Supply Chain Management:**
   Blockchain revolutionizes supply chain management by creating an immutable and transparent record of transactions across the supply chain. Each transaction, from raw material procurement to product delivery, is securely recorded, allowing stakeholders to trace the entire journey of goods. This transparency enhances accountability, minimizes counterfeit products, and optimizes supply chain efficiency.

8. **Healthcare and Electronic Medical Records:**
   Blockchain secures electronic medical records by encrypting patient data and recording transactions securely on a decentralized ledger. Patients have ownership and control over their health data, allowing secure sharing among healthcare providers. Interoperability of health records across various institutions enhances care coordination, reduces medical errors, and ensures data integrity, ultimately improving healthcare outcomes.

9. **Blockchain and Metaverse:**
   Blockchain's integration in the metaverse ensures secure ownership and trade of digital assets within virtual environments. Blockchain provides a decentralized platform for creating and managing digital assets, virtual properties, and currencies used in virtual reality spaces. This technology enables the development of decentralized applications (dApp's) within the metaverse, fostering a decentralized virtual economy.

   Blockchain technology addresses industry-specific challenges, enhancing security, transparency, efficiency, and trust across various sectors.