Contents

UNIT
1

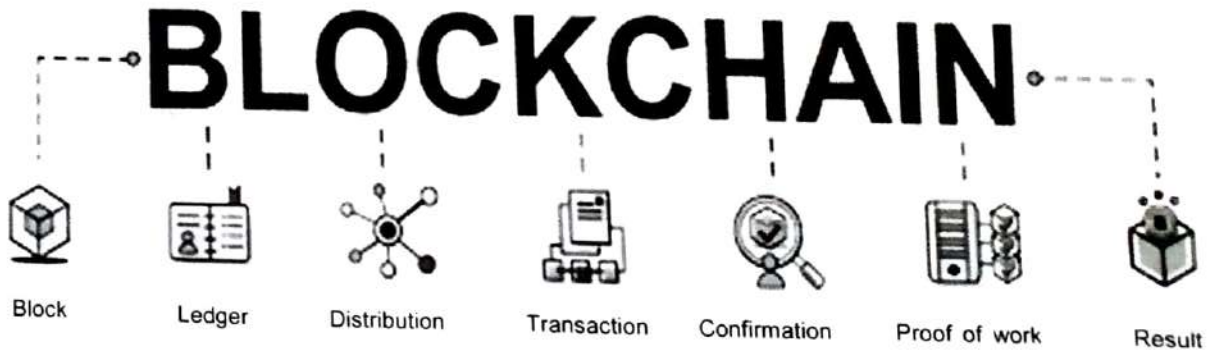
INTRODUCTION TO BLOCKCHAIN AND DISTRIBUTED LEDGERS

1.1 INTRODUCTION TO BLOCKCHAIN AND DISTRIBUTED LEDGER

Blockchain is a buzzword in today's technology and this technology is described as the most disruptive technology of the decade. Thus, Blockchain is used for the secure transference of items like money, contracts, property rights, stocks, and even networks without any requirement of Third Party Intermediaries like Governments, banks, etc. Once the data is stored in the Blockchain it becomes very difficult to manipulate the stored data. A Blockchain is a Network Protocol like SMTP. However, Blockchain cannot be run without the Internet. BlockChain is useful in many areas like Banking, Finance, Healthcare, Insurance, etc.

A blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way without the need for a central authority.

Blockchain can be defined as the Chain of Blocks that contain some specific Information. Thus, a Blockchain is a ledger i.e file that constantly grows and keeps the record of all transactions permanently. This process takes place in a secure, chronological (Chronological means every transaction happens after the previous one) and immutable way. Each time when a block is completed in storing information, a new block is generated.



❖ History of Blockchain :

In 1991, researcher scientists named Stuart Haber and W. Scott Stornetta introduce Blockchain Technology. These scientists wanted some Computational practical Solution for time-stamping the digital documents so that they couldn't be tempered or misdated. So both scientists together developed a system with the help of Cryptography. In this System, the time-stamped documents are stored in a Chain of Blocks.

After that in 1992, Merkle Trees formed a legal corporation by using a system developed by Stuart Haber and W. Scott Stornetta with some more features. Hence, Blockchain Technology became efficient to store several documents to be collected into one block. Merkle used a Secured Chain of Block which stores multiple data records in a sequence. However, this Technology became unused when Patent came into existence in 2004.

However, in the same year 2004, Cryptographic activist Hal Finney introduced a system for digital cash known as "Reusable Proof of Work". This step was the game-changer in the history of Blockchain and Cryptography. This System helps others to solve the Double Spending Problem by keeping the ownership of tokens registered on a trusted server.

After that in 2008, Satoshi Nakamoto conceptualized the concept of "Distributed Blockchain" under his whitepaper:"A Peer to Peer Electronic Cash System". He modified the model of Merkle Tree and created a system that is more secure and contains the secure history of data exchange. His System follows a peer- to-peer network of time stamping. His system became so useful that Blockchain become the backbone of Cryptography.

One of the famous uses of Blockchain is Bitcoin. The bitcoin is a crypto currency and s used to exchange digital assets online. Bitcoin uses cryptographic proof instead of third-party trust for two parties to execute transactions over the internet. Each transaction protects through digital signature.

❖ Distributed Systems :

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

Distributed systems are a computing model whereby two or more nodes work with each other in a coordinated fashion to achieve a common outcome. It is modeled in such a way that end users see it as a single logical platform. For example, Google's search engine is based on a large distributed system; however, to a user, it looks like a single, coherent platform.

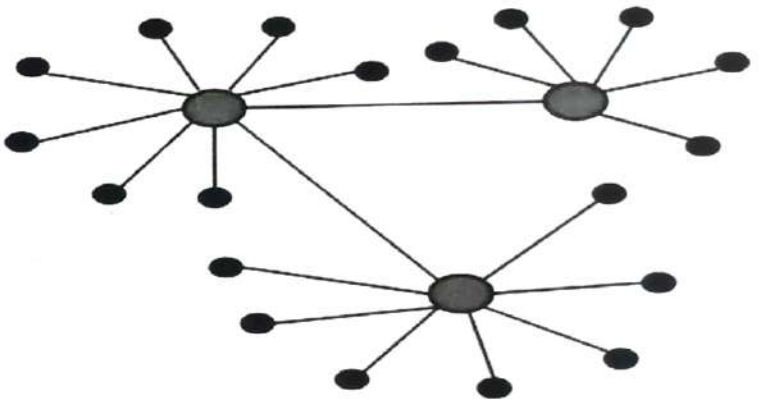
❖ Distributed ledger :

Distributed ledger is a database that is spread across multiple nodes or computing devices. It records, shares, and synchronizes data in a decentralized manner, allowing multiple parties to have a consistent view of information without the need for a central authority.

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

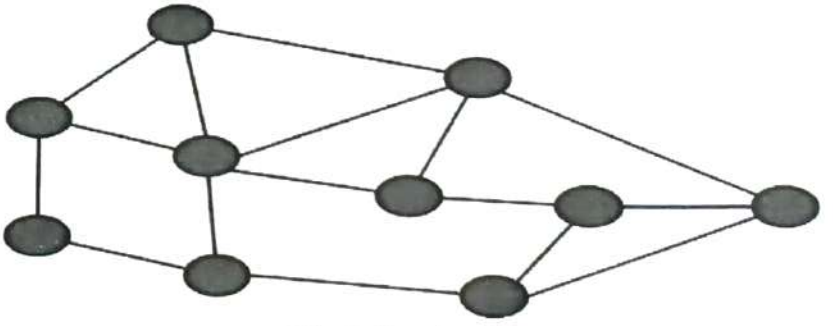
Nodes can be honest, faulty, or malicious and have their own memory and processor. A node that can exhibit arbitrary behavior is also known as a Byzantine node. This arbitrary behavior can be intentionally malicious, which is detrimental to the operation of the network. Generally, any unexpected behavior of a node on the network can be categorized as Byzantine. This term arbitrarily encompasses any behavior that is unexpected or malicious.

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



Decentralized

Centralized



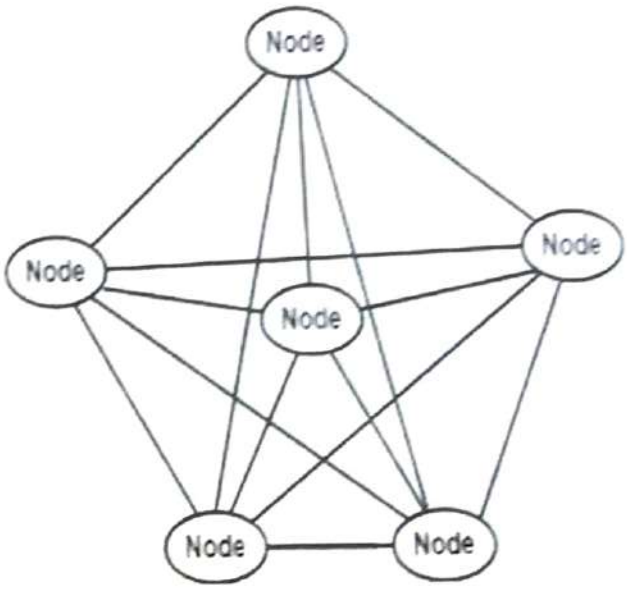
Distributed

❖ **Difference between Centralized,Decentralized and Distributed System :**

	Centralized	Distributed	Decentralized
Network/hardware resources	Maintained & controlled by single entity in a centralized location	Spread across multiple data centers & geographies; owned by network provider	Resources are owned & shared by network members; difficult to maintain since no one owns it
Solution components	Maintained & controlled by central entity	Maintained & controlled by solution provider	Each member has exact same copy of distributed ledger
Data	Maintained & controlled by central entity	Typically owned & managed by customer	Only added through group consensus
Control	Controlled by central entity	Typically, a shared responsibility between network provider, solution provider & customer	No one owns the data & everyone owns the data
Single Point of Failure	Yes	No	No
Fault tolerance	Low	High	Extremely high
Security	Maintained & controlled by central entity	Typically, a shared responsibility between network provider, solution provider & customer	Increases as # of network members increase
Performance	Maintained & controlled by central entity	Increases as network/ hardware resources scale up and out	Decreases as # of network members increase
Example	ERP system	Cloud computing	Blockchain

❖ **A network of nodes :**

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



[Blockchain Network]

❖ **Disadvantages of current transaction system:**

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

❖ **Advantages of Distributed Ledger :**

- **Decentralization:**

Distributed ledgers eliminate the need for a central authority, distributing control among network participants.

- **Real-Time Updating :**

Changes made to the ledger are reflected in real-time across all nodes. This ensures that all participants have access to the most up-to-date information.

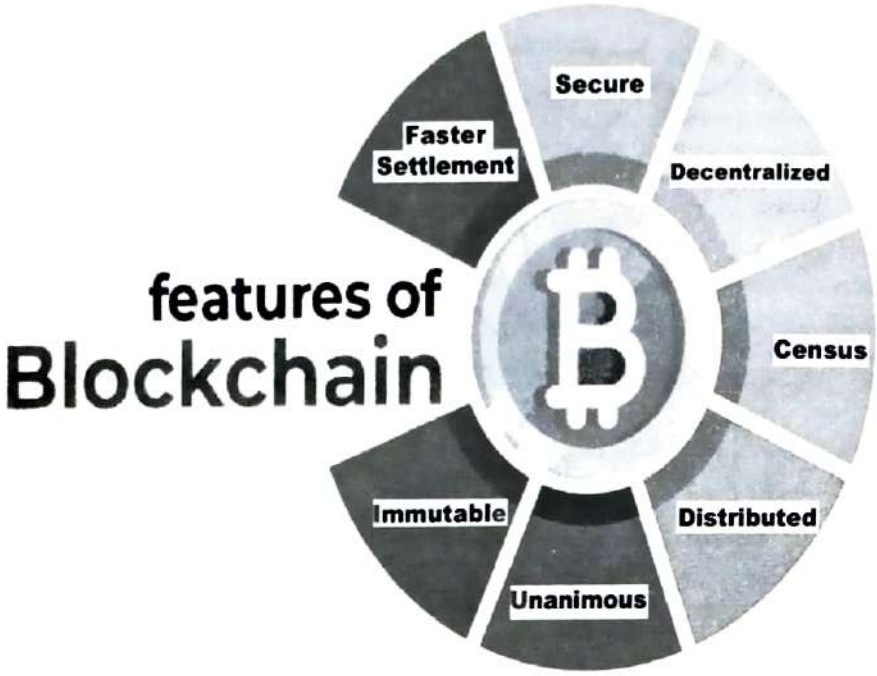
- **Security :**

The use of cryptographic techniques ensures the security of the data stored in the distributed ledger. Consensus mechanisms also contribute to maintaining the integrity of the information.

- **Efficiency :**

Distributed ledgers streamline processes by removing intermediaries, reducing the time and costs associated with traditional centralized systems.

❖ **Key Features of Blockchain :**



- **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.

- **Unanimous**

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

- **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.

- **Consensus Mechanisms**

Blockchain networks rely on consensus algorithms to validate and agree on the state of the ledger. Common mechanisms include Proof of Work (used in Bitcoin) and Proof of Stake.

- **Decentraiization**

Unlike traditional centralized systems, blockchain operates on a peer-to-peer network where no single entity has control. This decentralization enhances transparency and security.

- **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.

- **Faster Settlement**

Traditional banking systems are prone to many reasons for fallout like taking days to process a transaction after finalizing all settlements, which can be corrupted easily. On the other hand, blockchain offers a faster settlement compared to traditional banking systems. This blockchain feature helps make life easier.

Blockchain technology is increasing and improving day by day and has a really bright future in the upcoming years. The transparency, trust, and temper proof characteristics have led to many applications of it like bitcoin, Ethereum, etc. It is a pillar in making the business and governmental procedures more secure, efficient, and effective.

❖ **More Features of Blockchain**

- **Smart Contracts**

Blockchain platforms like Ethereum allow the implementation of smart contracts. These are self-executing contracts with coded terms, automating processes and reducing the need for intermediaries.

- **Transparency**

All participants in the blockchain network have access to the same information, promoting transparency and reducing the risk of fraud. Because every node or participant in Blockchain has a

copy of the Blockchain data, they have access to all transaction data. They themselves can verify the identities without the need for mediators.

1.2 APPLICATION, LIMITS, AND CHALLENGES OF BLOCKCHAIN

❖ Applications of Blockchain :

- **Crypto currencies :**

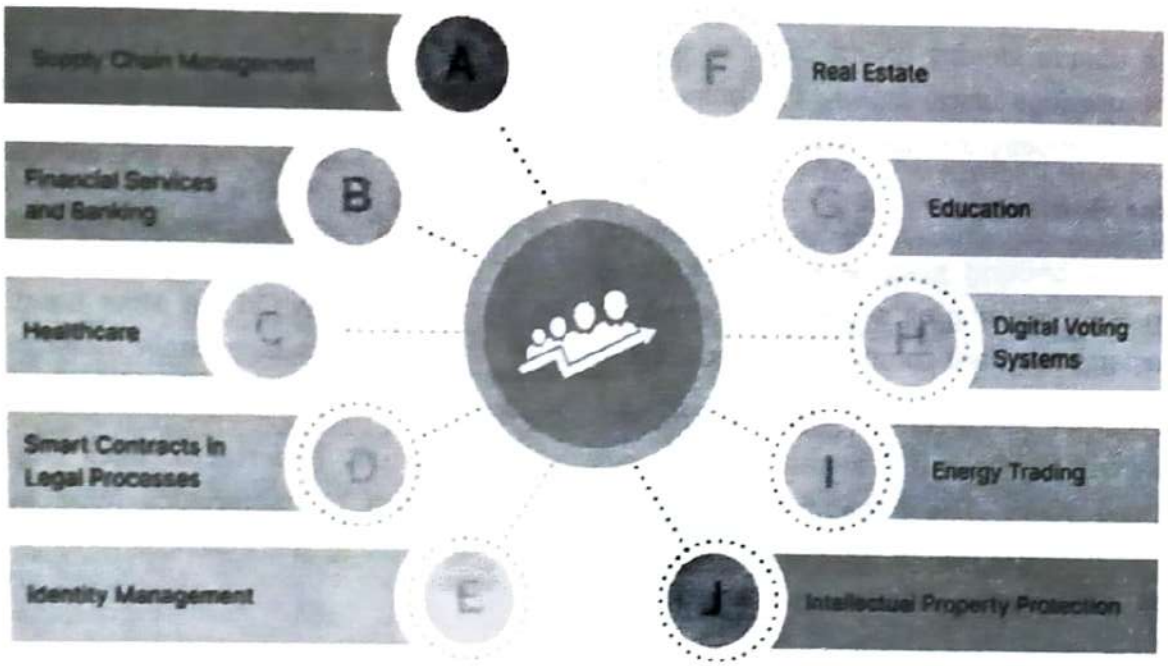
The most well-known application is the creation and management of crypto currencies like Bitcoin and Ethereum.

- **Smart Contracts :**

Blockchain enables the execution of self-executing contracts with programmable terms, automating processes in a trustless manner.

- **Supply Chain Management :**

Blockchain can enhance transparency, traceability, and efficiency in supply chains by recording and validating each transaction in the production and distribution process.



- **Financial Services :**

Facilitates faster and more cost-effective cross-border payments, reduces fraud, and provides financial inclusion for the unbanked.

- **Healthcare :**

Improves the security and interoperability of health records, streamlines data sharing, and enhances patient privacy.

- **Identity Management :**

Decentralized identity solutions on blockchain can provide secure and verifiable identity verification.

- **Voting Systems :**

Enhances the security and transparency of voting processes, reducing the risk of fraud and manipulation.

- **Real Estate :**

Streamlines property transactions by reducing paperwork, ensuring transparency in ownership records, and preventing fraudulent activities.

- **Education**

Blockchain can streamline and authenticate academic credentials. Academic certificates, degrees, and other qualifications can be securely stored on the blockchain, making it easy for employers and institutions to verify the authenticity of an individual's educational achievements.

- **Energy Trading**

Blockchain facilitates peer-to-peer energy trading by securely recording and validating transactions on a decentralized ledger. This use case enables individuals and businesses to buy and sell excess renewable energy directly, fostering a more efficient and sustainable energy ecosystem.

- **Intellectual Property Protection**

In the realm of intellectual property, blockchain can be used to establish and protect ownership rights. Digital assets such as patents, copyrights, and trademarks can be securely registered on the blockchain, providing a transparent and tamper-proof record of ownership.

Limits of Blockchain

- **Scalability :**

Blockchain networks face challenges in handling a large number of transactions simultaneously, leading to scalability issues.

- **Energy Consumption :**

Proof of Work (PoW) consensus mechanisms, such as those used by Bitcoin, require significant energy consumption, leading to environmental concerns.

- **Interoperability :**

Different blockchain platforms may lack interoperability, hindering seamless communication and collaboration between them.

- **Regulatory Challenges :**

Evolving and varying regulations worldwide can pose challenges for the widespread adoption of blockchain technologies.

- **User Education :**

The complexity of blockchain technology can be a barrier to widespread adoption, requiring user education for successful implementation.

❖ **Challenges of Blockchain :**

- **Security Concerns :**

While blockchain provides strong security through cryptographic techniques, vulnerabilities in smart contracts or consensus mechanisms can still pose risks.

- **Legal and Regulatory Issues :**

Lack of clear regulations and legal frameworks for blockchain applications can create uncertainty and hinder adoption.

- **Standardization :**

The absence of universal standards can impede interoperability between different blockchain platforms and limit collaboration.

- **Privacy Concerns :**

Balancing the transparency of blockchain with the need for data privacy remains a challenge, especially in applications like healthcare and identity management.

- **Adoption Barriers :**

The inertia of existing systems, resistance to change, and the need for education create challenges in adopting blockchain solutions.

- **Costs and Complexity :**

Initial setup costs, as well as the complexity of implementing and maintaining blockchain systems, can be obstacles for some organizations.

- **Immutable Data :**

While immutability is strength, it can become a challenge if errors or fraudulent transactions are recorded, as correcting them can be difficult.

1.3 BASICS OF CRYPTOGRAPHY : PUBLIC KEY, PRIVATE KEY, ASYMMETRIC ENCRYPTION MODEL, HASHING, SIGNATURE SCHEMES AND ELLIPTIC CURVE CRYPTOGRAPHY

Cryptography :

Cryptography is technique of securing information and communications through use of codes so that only those people for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix "graphy"

means "writing". In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, and verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

❖ Techniques used For Cryptography :

In today's age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

❖ Private Key :

In private key, the same key (or secret key) is used by both the parties, i.e., the sender and receiver, for Encryption/Decryption technique.

The sender uses the secret key and encryption algorithm for encryption, whereas for decryption, the receiver uses this key and decryption algorithm. In Secret Key Encryption/Decryption technique, the algorithm used for encryption is the inverse of the algorithm used for decryption. It means that if the combination of addition and multiplication is used in the encryption algorithm, then the decryption algorithm will use the combination of subtraction and division.

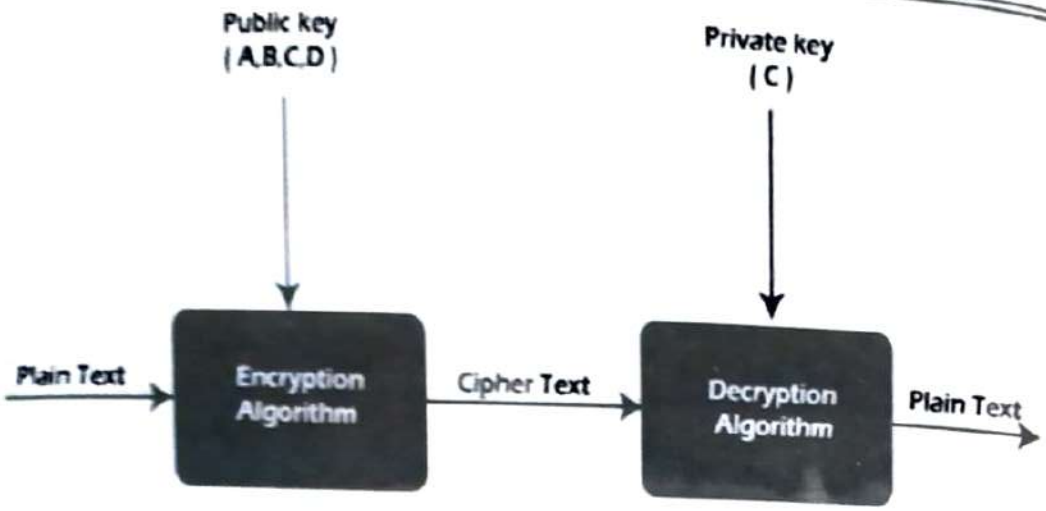
The secret key encryption algorithm is also known as symmetric encryption algorithm because the same secret key is used in bidirectional communication. The mechanism of private key is faster than the mechanism of public-key cryptography. The reason for this is that the size of the key is small.

❖ Public key :

It is an encryption technique that uses a pair of keys (public and private key) for secure data communication. In the pair of keys, the public key is for encrypting the plain text to convert it into cipher text, and the private key is used for decrypting the cipher text to read the message.

The private key is given to the receiver while the public key is provided to the public. Public Key Cryptography is also known as asymmetric cryptography.

The public key can be shared without compromising the security of the private one. All asymmetric key pairs are unique, so a message encrypted with a public key can only be read by the person who has the corresponding private key. The keys in the pair have much longer than those used in symmetric cryptography. So, it is hard to decipher the private key from its public counterpart. RSA algorithm is the most common algorithm for asymmetric encryption in use today.



❖ Features Of Cryptography are as follows :

- **Confidentiality :**

Information can only be accessed by the person for whom it is intended and no other person except him can access it.

- **Integrity :**

Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

- **Non-repudiation :**

The creator/sender of information cannot deny his intention to send information at later stage.

- **Authentication :**

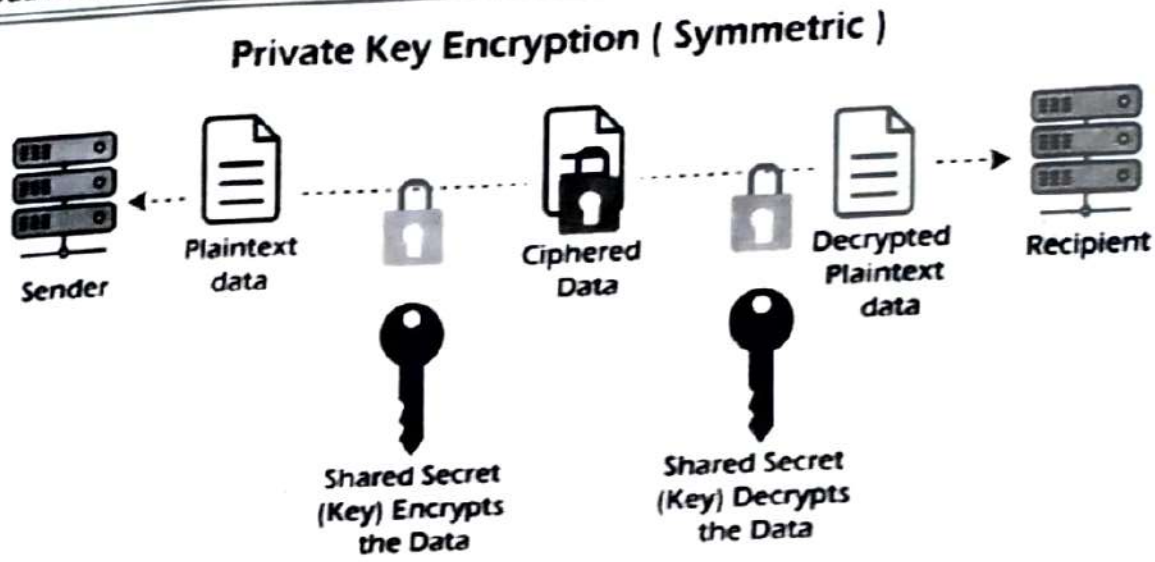
The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

❖ Types Of Cryptography :

In general there are three types of cryptography:

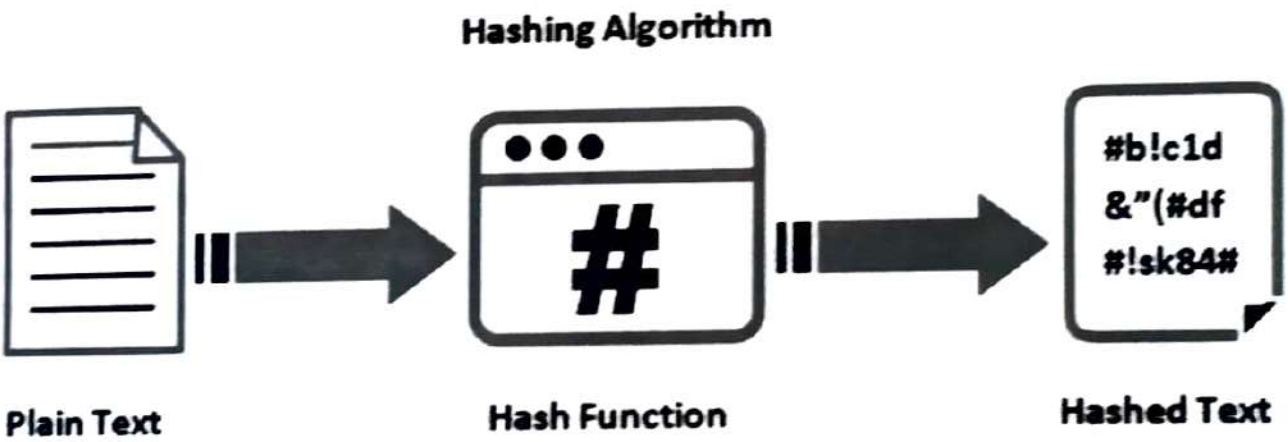
- **Symmetric Key Cryptography :**

It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system are Data Encryption System (DES) and Advanced Encryption System (AES).



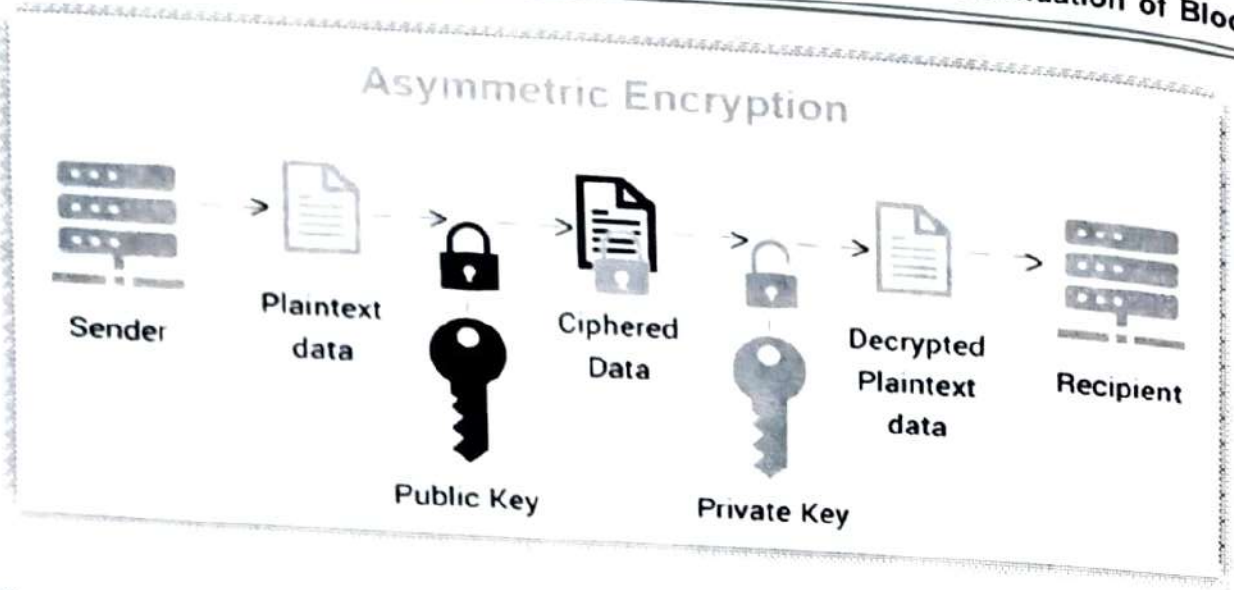
- **Hash Functions :**

There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.



- **Asymmetric Key Cryptography :**

Under this system a pair of keys is used to encrypt and decrypt information. A receiver's public key is used for encryption and a receiver's private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows his private key. The most popular asymmetric key cryptography algorithm is RSA algorithm.



❖ **Difference between Symmetric key and Asymmetric key Encryption**

Differentiator	Symmetric Key Encryption	Asymmetric Key Encryption
No of Keys	Only one key is used,and the same key is used for encryption and decryption	Two different keys called the public and the private keys are used for encryption and decryption
Complexity and speed of execution	It's a simple technique and because of this the encryption process can be carried out quickly	It's a much more complicated technique than symmetric key encryption, because of this the encryption process can be carried out slowly
Length of keys	The length of the key is 128 or 256 bits based on security requirement	The length of the key is much larger, e.g the recommended RSA key size is 2048 bits or higher
Usage	Used when large chunks of data need to be transferred	It is used in smaller transactions, primarily to authenticate and establish a secure communication channel prior to the actual data transfer
Security	The secret key is shared so the risk of compromise is higher	The primary key is not shared so overall more secure than symmetric key encryption
Example	AES,DES,RC4	RSA, Diffie-hellman ,ECC

❖ Applications of Cryptography:

- **Computer passwords**

Cryptography is widely utilized in computer security, particularly when creating and maintaining passwords. When a user logs in, their password is hashed and compared to the hash that was previously stored. Passwords are hashed and encrypted before being stored. In this technique, the passwords are encrypted so that even if a hacker gains access to the password database, they cannot read the passwords.

- **Digital Currencies**

To safeguard transactions and prevent fraud, digital currencies like Bitcoin also use cryptography. Complex algorithms and cryptographic keys are used to safeguard transactions, making it nearly hard to tamper with or forge the transactions.

- **Secure web browsing**

Online browsing security is provided by the use of cryptography, which shields users from eavesdropping and man-in-the-middle assaults. Public key cryptography is used by the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols to encrypt data sent between the web server and the client, establishing a secure channel for communication.

- **Electronic signatures**

Electronic signatures serve as the digital equivalent of a handwritten signature and are used to sign documents. Digital signatures are created using cryptography and can be validated using public key cryptography. In many nations, electronic signatures are enforceable by law, and their use is expanding quickly.

- **Authentication**

Cryptography is used for authentication in many different situations, such as when accessing a bank account, logging into a computer, or using a secure network. Cryptographic methods are employed by authentication protocols to confirm the user's identity and confirm that they have the required access rights to the resource.

- **Crypto currencies**

Cryptography is heavily used by cryptocurrencies like Bitcoin and Ethereum to safeguard transactions, thwart fraud, and maintain the network's integrity. Complex algorithms and cryptographic keys are used to safeguard transactions, making it nearly hard to tamper with or forge the transactions.

- **End-to-End Encryption**

End-to-end encryption is used to protect two-way communications like video conversations, instant messages, and email. Even if the message is encrypted, it assures that only the intended receivers can read the message. End-to-end encryption is widely used in communication apps like WhatsApp and Signal, and it provides a high level of security and privacy for users.

❖ **Advantages**

- **Access Control :**

Cryptography can be used for access control to ensure that only parties with the proper permissions have access to a resource. Only those with the correct decryption key can access the resource thanks to encryption.

- **Secure Communication :**

For secure online communication, cryptography is crucial. It offers secure mechanisms for transmitting private information like passwords, bank account numbers, and other sensitive data over the internet.

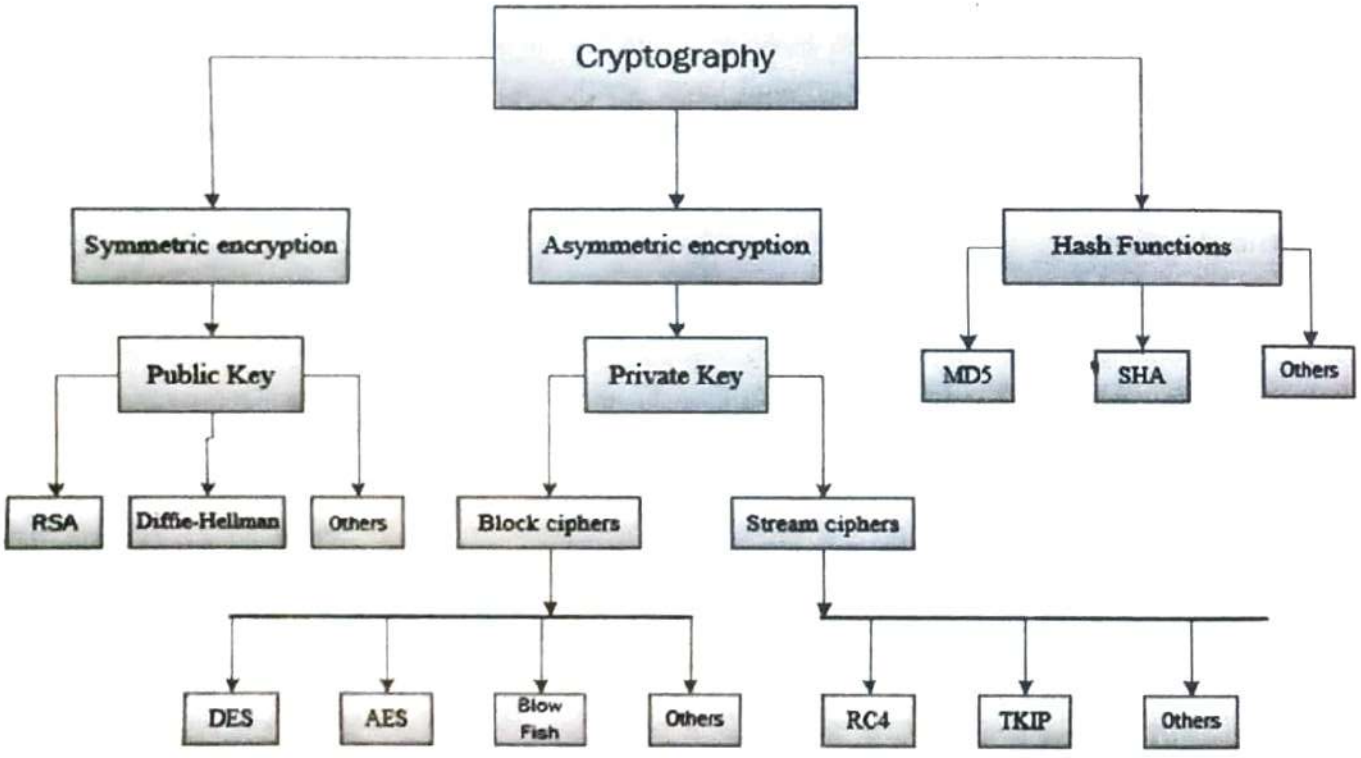
- **Protection against attacks :**

Cryptography aids in the defence against various types of assaults, including replay and man-in-the-middle attacks. It offers strategies for spotting and stopping these assaults.

- **Compliance with legal requirements :**

Cryptography can assist firms in meeting a variety of legal requirements, including data protection and privacy legislation.

❖ **Types of Cryptography Algorithms :**



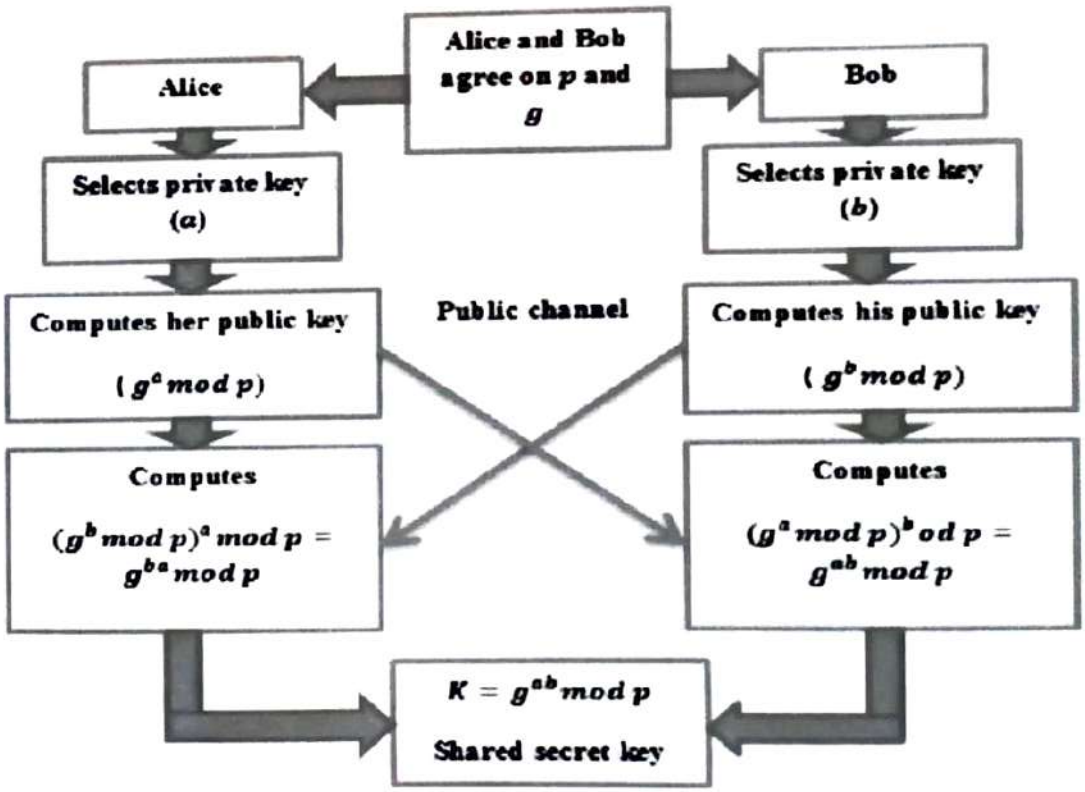
➢ **Diffie-Hellman Key exchange algorithm :**

Symmetric encryption has always been a reliable method of cryptography for the exchange of private information. A glaring flaw has always been the difficulty in sharing the requisite secret key with the

receiver of the message. It can intercept any key transmitted over an insecure channel by hackers, who can then use the same key to decrypt the encrypted cipher texts.

The Diffie Hellman algorithm solves this problem using one-way functions that enable only the sender and receiver to decrypt the message using a secret key. Now, you will learn more about how the one-way functions help in the transmission of keys.

Diffie-Hellman algorithm is one of the most important algorithms used for establishing a shared secret. At the time of exchanging data over a public network, we can use the shared secret for secret communication. We use an elliptic curve for generating points and getting a secret key using the parameters.



Diffie-Hellman Key Exchange

Bob and Alice know and have the following :
$p = 23$ (a prime number) $g = 11$ (a generator)

Alice chooses a secret random number $a = 6$

Alice computes : $A = g^a \bmod p$

$A = 11^6 \bmod 23 = 9$

Bob chooses a secret random number $b = 5$

Bob computes : $B = g^b \bmod p$

$B = 11^5 \bmod 23 = 5$

Alice receives B = 5 from Bob

Bob receives A = 9 from Alice

Secret Key = $K = B^a \bmod p$

$K = 5^6 \bmod 23 = \boxed{8}$

Secret Key = $K = A^b \bmod p$

$K = 9^5 \bmod 23 = \boxed{8}$

The common secret key is : 8

1. We will take four variables, i.e., P (prime), G (the primitive root of P), and a and b (private values).
2. The variables P and G both are publicly available. The sender selects a private value, either a or b, for generating a key to exchange publicly. The receiver receives the key, and that generates a secret key, after which the sender and receiver both have the same secret key to encrypt.

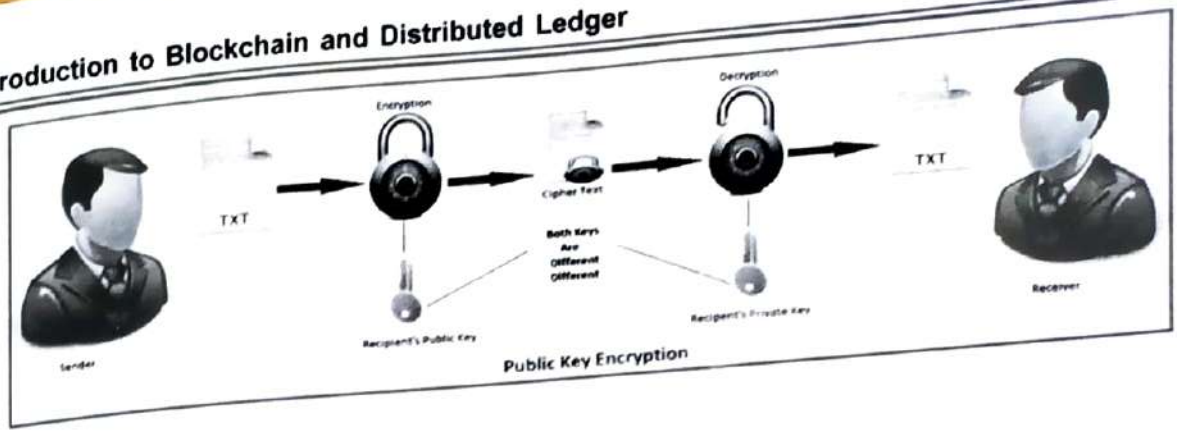
➢ RSA Algorithm

RSA Algorithm is used to encrypt and decrypt data in modern computer systems and other electronic devices. RSA algorithm is an asymmetric cryptographic algorithm as it creates 2 different keys for the purpose of encryption and decryption. It is public key cryptography as one of the keys involved is made public. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman who first publicly described it in 1978.

RSA makes use of prime numbers (arbitrary large numbers) to function. The public key is made available publicly (means to everyone) and only the person having the private key with them can decrypt the original message.

The RSA algorithm holds the following features –

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: private key and public key.



RSA Algorithm Steps

Step - 1 : Select two prime numbers p and q where $p \neq q$.

Step - 2 : Calculate $n = p * q$.

Step - 3 : Calculate $\Phi(n) = (p-1)^* (q-1)$.

Step - 4 : Select e such that, e is relatively prime to Φ(n, i.e. (e, $\Phi(n = 1$ and $1 < e < \Phi(n)$

Step - 5 : Calculate $d = e^{-1} \bmod \Phi(n)$ or $ed = 1 \bmod \Phi(n)$.

Step - 6 : Public key = {e, n}, private key = {d, n}.

Step - 7 : Find out cipher text using the formula,

$C = P^e \bmod n$ where, $P < n$ where C = Cipher text, P = Plain text, e = Encryption key and n=block size.

Step - 8 : $P = C^d \bmod n$. Plain text P can be obtain using the given formula. where, d = decryption key

RSA algorithm explanation with example step by step:

Step - 1 : Select two prime numbers p and q where $p \neq q$.

Example, Two prime numbers p = 13, q = 11.

Step - 2 : Calculate $n = p * q$.

Example, $n = p * q = 13 * 11 = 143$.

Step - 3 : Calculate $\Phi(n) = (p-1) * (q-1)$.

Example, $\Phi(n) = (13 - 1) * (11 - 1) = 12 * 10 = 120$.

Step - 4 : Select e such that, e is relatively prime to $\Phi(n)$, i.e. $(e, \Phi(n)) = 1$ and $1 < e < \Phi(n)$.

Example, Select e = 13, gcd (13, 120) = 1.

Step - 5 : Calculate $d = e\text{-}1 \bmod \Phi(n)$ or $e * d = 1 \bmod \Phi(n)$

Example, Finding d: $e * d \bmod \Phi(n) = 1$

$13 * d \bmod 120 = 1$

(How to find: $d * e = 1 \bmod \Phi(n)$

$d = ((\Phi(n) * i) + 1) / e$

$d = (120 + 1) / 13 = 9.30$ ($\because i = 1$)

$d = (240 + 1) / 13 = 18.53$ ($\because i = 2$)

$d = (360 + 1) / 13 = 27.76$ ($\because i = 3$)

$d = (480 + 1) / 13 = 37$ ($\because i = 4$))

Step - 6 : Public key = {e, n}, private key = {d, n}.

Example, Public key = {13, 143} and private key = {37, 143}.

Step - 7 : Find out cipher text using the formula, $C = Pe \bmod n$ where, $P < n$.

Example, Plain text P = 13. (Where, $P < n$)

$C = Pe \bmod n = 1313 \bmod 143 = 52$.

Step - 8 : $P = Cd \bmod n$. Plain text P can be obtain using the given formula.

Example, Cipher text C = 52

$P = Cd \bmod n = 5237 \bmod 143 = 13$.

Examples :

Question: P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 6, then what will be cipher text value according to RSA algorithm? Again calculate plain text value from cipher text.

Solution:

1. Two prime numbers P=7, Q=17
2. $n = P * Q = 17 * 7 = 119$ [redacted]
3. $\Phi(n) = (P-1) * (Q-1) = (17-1) * (7-1) = 16 * 6 = 96$ **$\Phi(n) = 96$**
4. Public key E = 5. [redacted]
5. Calculate d = 77. $d = ((\Phi(n) * i) + 1) / e$ **d= 77**

   $d = ((96*1)+1) / 5 = 19.4$

   $d = ((96*2)+1) / 5 = 38.6$

   $d = ((96*3)+1) / 5 = 57.8$

   $d = ((96*4)+1) / 5 = 77$ (Stop finding d because getting integer value)
6. Public key = {e, n} = {5, 119}, private key = {d, n} = {77, 119}.
7. Plain text PT = 6, $CT = PT^E \bmod n = 6^5 \bmod 119 = 41$. **Cipher Text = 41**
8. Cipher text CT = 41, $PT = CT^d \bmod n = 41^{77} \bmod 119 = 6$. [redacted]

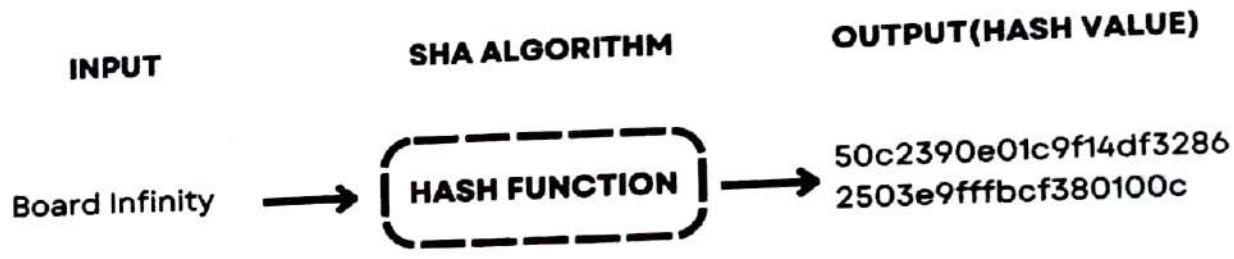
Question: In a public key cryptosystem using RSA algorithm, user uses two prime numbers 5 and 7. He chooses 11 as Encryption key, find out decryption key. What will be the cipher text, if the plaintext is 2? Decrypt the cipher text, what will be the value of plain text?

Solution:

1. Two prime numbers $p = 5, q = 7$
2. $n = p * q = 5 * 7 = 35$
3. $\Phi(n) = (p-1) * (q-1) = (5-1) * (7-1) = 4 * 6 = 24$ **$\Phi(n) = 24$**
4. Public key $e = 11$. **e = 11**
5. Calculate $d = 11$. $d = ((\Phi(n) * i) + 1) / e$ **d = 11**
6. Public key = $\{e, n\} = \{11, 35\}$, private key = $\{d, n\} = \{11, 35\}$.
7. Plain text $P = 2$, $C = P^e \bmod n = 2^{11} \bmod 35 = 18$. **Cipher Text = 18**
8. Cipher text $C = 18$, $P = C^d \bmod n = 18^{11} \bmod 35 = 2$. **Plain Text = 2**

❖ Secure Hash Algorithm 1 (SHA-1) :

SHA-1 is a cryptographic hash function that produces a 160-bit hash value (also known as a message digest) from an input message of any size, up to $2^{64} - 1$ bits. SHA-1 was designed by the National Security Agency (NSA) and published by the National Institute of Standards and Technology (NiST) in 1995 as a part of the Secure Hash Standard (SHS).SHA-1 is a one-way function, which means it is computationally infeasible to derive the original message from its hash value.



Properties of SHA-1 :

SHA-1 has several properties that make it suitable for various applications:

1. Collision Resistance :

The primary goal of a hash function is to produce a unique hash value for each input message. SHA-1 ensures that two different messages are highly unlikely to produce the same hash value, making it resistant to collision attacks.

2. One-way Function :

SHA-1 is a one-way function, which means it is impossible to derive the original message from its hash value. This property is essential in digital signatures, password storage, and other security applications.

3. Fixed Output Length :

SHA-1 produces a fixed-size output of 160 bits, regardless of the input message size. This makes it easy to compare hash values and store them in databases.

Applications of SHA-1 :

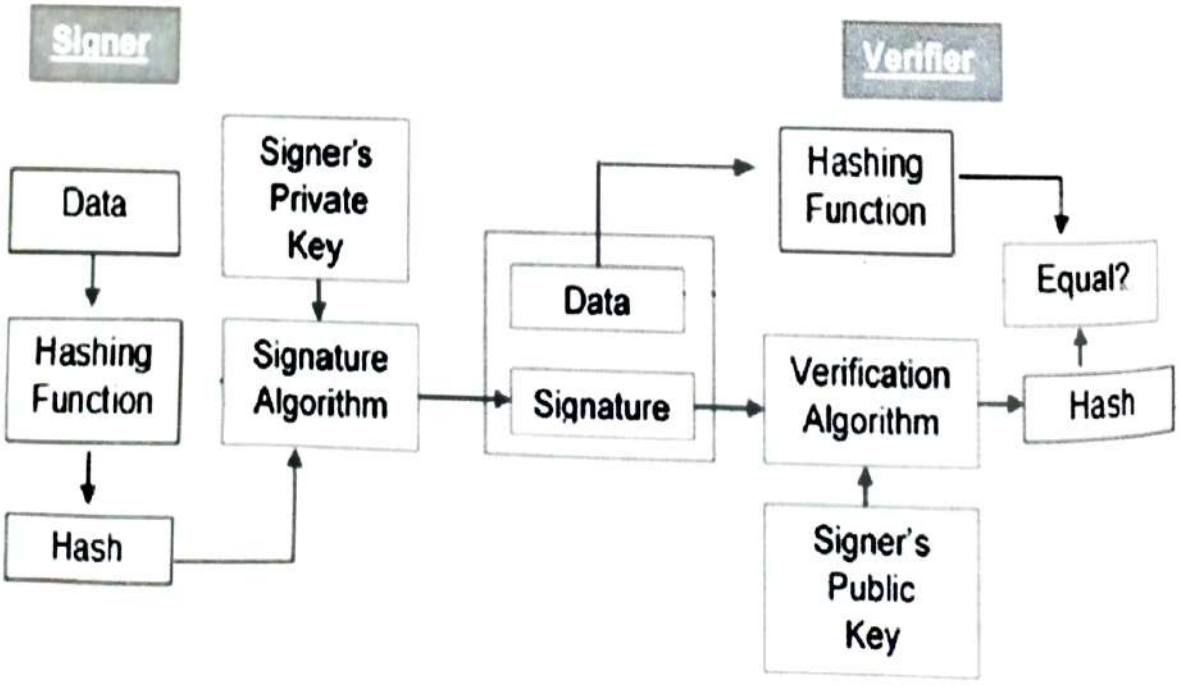
SHA-1 is used in various applications, including:

1. Digital Signatures: SHA-1 is used in digital signature algorithms such as Digital Signature Standard (DSS) to ensure data integrity and non-repudiation.
2. Password Storage: SHA-1 is used to store passwords in databases. Instead of storing the actual password, the system stores the hash value of the password, making it difficult for attackers to steal passwords.
3. Secure Communications: SHA-1 is used in secure communication protocols such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL) to ensure data integrity and confidentiality.

❖ **Signature Schemes :**

A signature scheme is a cryptographic technique that allows a party to produce a digital signature on a message.Digital signatures serve as a way to verify the authenticity and integrity of a message or document. Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

The process involves a signing algorithm that uses a private key to generate the signature and a verification algorithm that uses the corresponding public key to verify the signature's authenticity.Popular signature schemes include RSA (Rivest–Shamir–Adleman), DSA (Digital Signature Algorithm), and ECDSA (Elliptic Curve Digital Signature Algorithm).



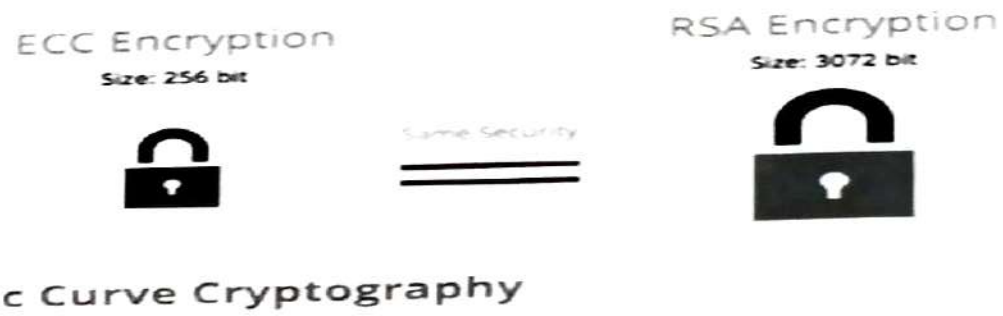
❖ Elliptic Curve Cryptography (ECC) :

ECC is a type of public-key cryptography based on the mathematics of elliptic curves over finite fields.

Public-key cryptography involves pairs of keys: a public key, which can be shared openly, and a private key, which must be kept secret.

ECC provides the same level of security as traditional public-key cryptography systems (like RSA) with much shorter key lengths, making it more efficient in terms of computational resources.

The security of ECC is based on the difficulty of the elliptic curve discrete logarithm problem, which is believed to be computationally infeasible to solve efficiently.

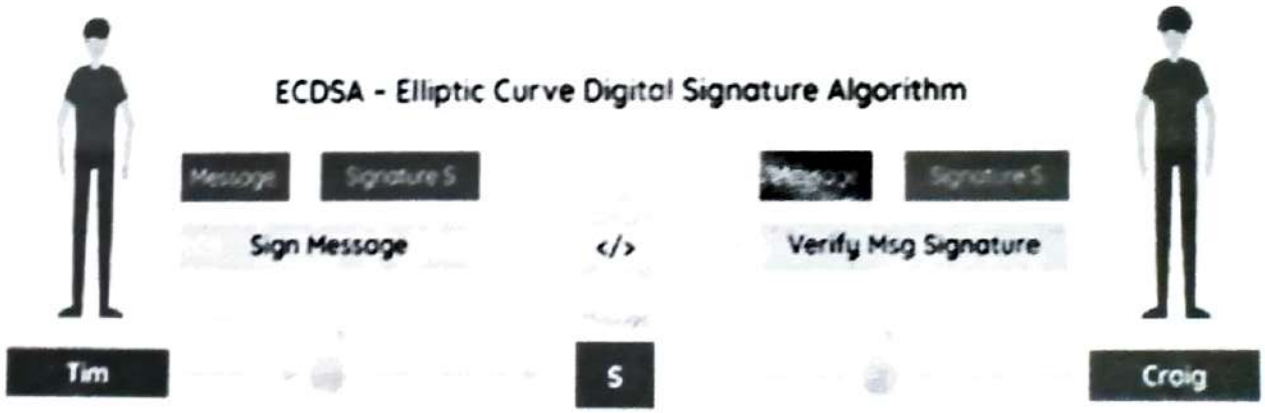


❖ Elliptic Curve Digital Signature Algorithm (ECDSA) :

ECDSA is a widely used digital signature algorithm based on elliptic curve cryptography.

It provides a means of creating and verifying digital signatures, similar to other signature schemes but with the advantages of shorter key lengths and faster computation.

ECDSA involves the use of elliptic curve mathematics to sign and verify digital signatures, making it particularly attractive for resource-constrained environments such as mobile devices and IoT devices. With ECDSA, we can have the same level of security as RSA but with smaller keys which means less data which translates into faster transactions.



1.4 CONSISTENCY, AVAILABILITY, AND PARTITION TOLERANCE IN BLOCKCHAIN

❖ CAP theorem :

The CAP theorem, also known as Brewer's theorem, was introduced by Eric Brewer in 1998 as a conjecture. In 2002, it was proven as a theorem by Seth Gilbert and Nancy Lynch. The theorem states that any distributed system cannot have consistency, availability, and partition tolerance simultaneously.

Consistency, Availability, and Partition Tolerance (CAP) are principles that are often discussed in the context of distributed systems, and they are particularly relevant when considering the design and operation of blockchain systems.

- **Consistency :**

In the context of distributed systems, consistency ensures that all nodes in the system see the same data at the same time. It means that when a write operation is completed, all subsequent read operations will return the updated data.

Achieving strong consistency in a distributed system often involves coordination among nodes, which can introduce latency and impact system performance.

- **Availability :**

Availability ensures that every request to the system receives a response, without guaranteeing that it contains the most recent version of the data.

A highly available system is one that remains operational despite node failures or other issues. High availability is crucial for systems that need to provide continuous service even in the face of failures.

- **Partition Tolerance :**

Partition tolerance deals with the system's ability to continue operating even when network partitions occur. A network partition happens when communication between nodes is disrupted, leading to a separation of the system into independent sub-systems.

In a distributed system, achieving partition tolerance means that the system can still function, providing both consistency and availability, even when network partitions occur.

The CAP theorem, proposed by computer scientist Eric Brewer, states that a distributed system can achieve at most two out of the three CAP properties at any given time. In the context of blockchain:

❖ Blockchain and CAP :

Many blockchain systems prioritize partition tolerance, ensuring that the network remains functional even if some nodes are unreachable or the network is temporarily split.

Bitcoin, for example, sacrifices some level of consistency in favor of availability and partition tolerance. Nodes may temporarily have different views of the blockchain due to network delays or forks, but eventually, the system converges to a consistent state.

Exercises

MCQs :

1. Blockchain is a peer-to-peer _____ distributed ledger technology that makes the records of any digital asset transparent and unchangeable.
   A. Decentralized
   B. Demanding
   C. Secure
   D. Popular
2. Blockchain networks are much _____ and deal with no real single point of failure.
   A. Simpler
   B. Easier to scale
   C. Convenient
   D. Faster
3. Bitcoin is a crypto currency, which is an application of Blockchain.
   A. True
   B. False
4. Blockchain can perform user transactions _____ .
   A. With the help of the third party
   B. Without involving any third party
   C. Without involving any owned
   D. Without involving any authenticated
5. Who introduced the digital online crypto currency known as Bitcoin?
   A. Satoshi Nakamoto
   B. Nick Szabo
   C. Wei Dai
   D. Hal Finney
6. Which of the following is not a type of encryption ?
   A. Symmetric encryption
   B. Asymmetric encryption
   C. Hashing
   D. Compression
7. Which type of encryption uses the same key for both encryption and decryption ?
   A. Symmetric encryption
   B. Asymmetric encryption
   C. Hashing
   D. None of the above
8. Which of the following is an example of a hash function?
   A. SHA-1
   B. RSA
   C. AES
   D. Diffie-Hellman

Questions :

1. What is the difference between private key and public key ?
2. Write the comparison between centralized and decentralized system.
3. What exactly are encryption and decryption ?
4. What is plaintext , cipher text, Caesar cipher ?

* * *

UNIT
2

STRUCTURE OF BLOCKCHAIN

2.1 Types of Blockchain : Public and private; Permissioned and permission less; tokenized and token less Blockchain.

2.2 Side chain.

2.3 Core Components of Blockchain.

2.4 Distributed identity : Public and private keys, Digital identification, and wallets.

2.5 Decentralized network, Distributed ledger.

2.6 Data structure of a Blockchain

2.1 TYPES OF BLOCKCHAIN : PUBLIC AND PRIVATE; PERMISSIONED AND PERMISSION LESS; TOKENIZED AND TOKEN LESS BLOCKCHAIN

Before starting with blockchain, let's first understand the concept of crypto currency.

❖ **Cryptocurrency** :

Cryptocurrencies are digital or virtual currencies that use cryptography for security and operate on decentralized networks, typically based on blockchain technology. Blockchain is a distributed ledger that records all transactions across a network of computers. There are thousands of cryptocurrencies, but I'll provide explanations for some of the most well-known ones as of my last knowledge update in January 2022 :

1. **Bitcoin (BTC)** :

Bitcoin is the first and most well-known cryptocurrency, created by an unknown person or group of people using the pseudonym Satoshi Nakamoto in 2009. It is often referred to as digital gold and is used as a store of value and a medium of exchange.

2. **Ethereum (ETH)** :

Ethereum is a decentralized platform that enables the creation and execution of smart contracts and decentralized applications (DApps). It introduced the concept of a blockchain with a built-in programming language, allowing developers to build more complex applications beyond simple transactions.

3. **Ripple (XRP)** :

Ripple aims to facilitate fast and low-cost international money transfers. It is both a platform and a currency. Ripple Labs, the company behind XRP, focuses on providing solutions for financial institutions to improve cross-border payments.

4. Litecoin (LTC) :

Created by Charlie Lee in 2011, Litecoin is often considered the silver to Bitcoin's gold. It is designed to offer faster transaction confirmation times and uses a different hashing algorithm (Scrypt) than Bitcoin.

5. Cardano (ADA) :

Cardano is a blockchain platform that aims to provide a more secure and scalable infrastructure for the development of decentralized applications and smart contracts. It emphasizes a research-driven approach and peer-reviewed development.

6. Polkadot (DOT) :

Developed by Dr. Gavin Wood, one of the co-founders of Ethereum, Polkadot is a multi-chain network that enables different blockchains to interoperate and share information. It seeks to address issues of scalability and interoperability in blockchain networks.

7. Chainlink (LINK) :

Chainlink is a decentralized oracle network that enables smart contracts to securely interact with external data sources, APIs, and payment systems. It plays a crucial role in connecting blockchain-based smart contracts with real-world data.

8. Stellar (XLM) :

Stellar is a blockchain platform designed for fast and low-cost cross-border transactions. It aims to facilitate the movement of money and assets between people and institutions, with a focus on financial inclusion.

9. Binance Coin (BNB) :

Binance Coin is the native cryptocurrency of the Binance exchange. Initially created as an ERC-20 token on the Ethereum blockchain, it later migrated to Binance Chain. BNB is used to pay for transaction fees on the Binance exchange and participate in token sales on the Binance Launchpad.

10. Dogecoin (DOGE) :

Originally started as a meme, Dogecoin has gained popularity and is often used for tipping and charitable donations. It features the Shiba Inu dog from the "Doge" meme as its logo.

These are just a few examples, and the cryptocurrency space is continually evolving with new projects and technologies emerging. It's important to note that the cryptocurrency market is highly volatile, and investors should conduct thorough research before participating.

❖ Advantages and disadvantages of cryptocurrency

Cryptocurrencies offer several advantages and disadvantages, and it's essential to consider both aspects before getting involved. Keep in mind that the cryptocurrency space is dynamic, and the landscape may change over time. As of my last knowledge update in January 2022, here are some key advantages and disadvantages :

❖ **Advantages** :

1. **Decentralization** :

   - Advantage : Cryptocurrencies operate on decentralized blockchain networks, reducing the control of central authorities. This can enhance security and prevent single points of failure.

2. **Security** :

   - Advantage : Cryptography ensures the security of transactions and the integrity of the blockchain. Public and private keys provide a secure way to control ownership and access.

3. **Reduced Transaction Costs** :

   - Advantage : Cryptocurrency transactions often have lower fees compared to traditional financial systems, especially for international transfers.

4. **Financial Inclusion** :

   - Advantage : Cryptocurrencies can provide financial services to people without access to traditional banking systems, promoting financial inclusion.

5. **24/7 Accessibility** :

   - Advantage : Cryptocurrencies operate on a global scale and are accessible 24/7, allowing users to make transactions at any time without being restricted by geographical or time-zone limitations.

6. **Ownership and Control** :

   - Advantage : Users have greater control and ownership of their funds as they hold their private keys. This reduces the risk of assets being frozen or seized by third parties.

7. **Innovation in Finance** :

   - Advantage : Cryptocurrencies and blockchain technology have spurred innovation in various sectors, including finance, supply chain, healthcare, and more.

❖ **Disadvantages** :

1. **Volatility** :

   - Disadvantage : Cryptocurrency prices are highly volatile, leading to significant fluctuations in value. This volatility can pose risks for investors and users.

2. **Regulatory Uncertainty** :

   - Disadvantage : Regulatory frameworks for cryptocurrencies are still evolving, leading to uncertainty and potential legal and regulatory risks for users and businesses.

3. **Irreversibility of Transactions** :

   - Disadvantage : Cryptocurrency transactions are typically irreversible. If a user makes a mistake or falls victim to fraud, it may be challenging to recover funds.

4. **Lack of Consumer Protections :**
   - Disadvantage : Unlike traditional banking systems, cryptocurrencies lack many consumer protection measures. Users are responsible for the security of their private keys and the custody of their assets.

5. **Limited Acceptance :**
   - Disadvantage : While acceptance is growing, cryptocurrencies are not universally accepted as a form of payment. Limited adoption can restrict their utility in daily transactions.

6. **Environmental Concerns :**
   - Disadvantage : Some cryptocurrencies, such as Bitcoin, use energy-intensive mining processes, leading to environmental concerns about their carbon footprint.

7. **Technological Challenges :**
   - Disadvantage : Cryptocurrencies and blockchain technology are still developing, and there are technical challenges such as scalability, interoperability, and usability that need to be addressed.

❖ **Difference between Conventional and Digital Currency**

Basis of comparison	Conventional Currency	Digital Currency
Type	Real	Virtual
Portability	Yes	Highly portable
Acceptance	National	Global
Secure	Moderate	High
Decentralized	No (Controlled by bank)	Yes (Controlled by complex math)
Smart(Programmable)	No	Yes

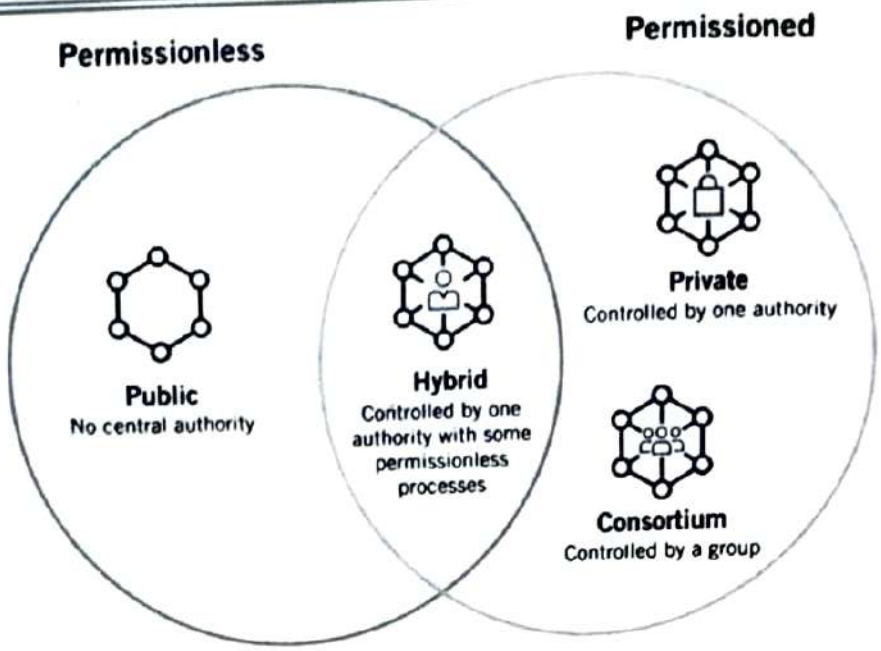
❖ **Types of Blockchain**

Blockchain technology comes in various types, each with its own characteristics, consensus mechanisms, and use cases. Here are some of the main types of blockchains :

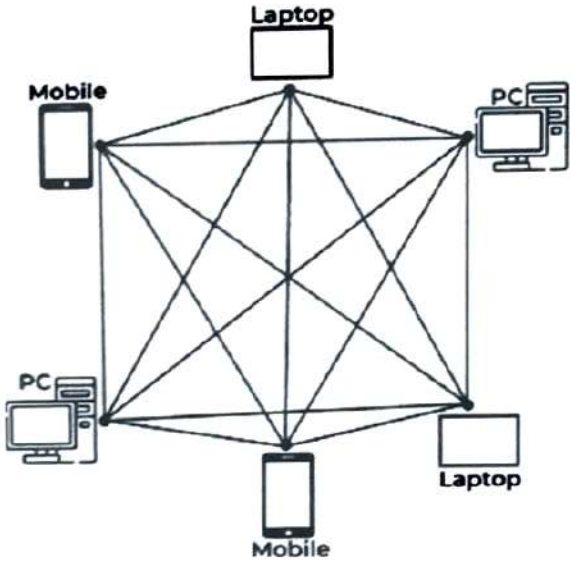
1. Public Blockchain

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

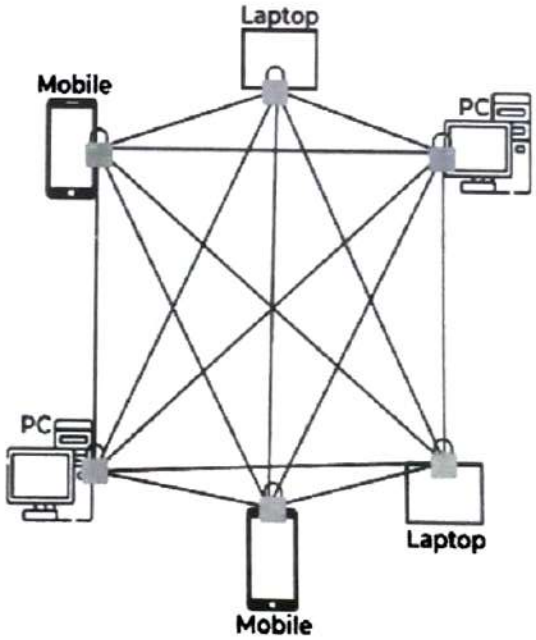
- **Acceptance :**

  No central authority is there so governments are facing the issue to implement the technology faster.

Examples : 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.

Examples : 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.

Examples : 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

Example : Tendermint and Multichain.

❖ **Difference between Public and Private Blockchain**

Sr. No.	Public Blockchain	Private Blockchain
1	Open, anyone can join the network	Restricted and Permissioned, a new member joins the network via invitation
2	Each node has equal transmission power	Only certain nodes can create new transactions
3	Low speed of transaction accomplishment	Fast speed of transaction accomplishment
4	Long transaction approval frequency	Short transaction approval frequency

Sr. No.	Public Blockchain	Private Blockchain
5	High cost of each transaction	Comparatively cheap cost of each transaction
6	Proof-of-work, proof-of-stack consensus protocols for the adding on a new block	Pre-approved participants initiate adding of a new block
7	Anonymus	Nonymous
8	Requires no trust among members	Members need to trust each other
9	Large energy consumption	Long energy consumption

❖ **Permissioned blockchain**

A permissioned blockchain is a blockchain network requiring explicit permission from a central authority to join the network and participate in the consensus process. Only approved nodes can enter the network, validate transactions, and create new blocks.

Permissioned blockchains are often used in enterprise applications where the network is closed and controlled by a single entity, such as a financial institution or a government agency. These networks offer a higher level of security and control, as the central authority can carefully vet and approve nodes before they are allowed to join the network.

Characteristics of Permissioned Blockchains

Permissioned blockchains have many characteristics that set them apart from permissionless blockchains.

1. **Controlled Access :** As mentioned earlier, permissioned blockchains require explicit permission from a central authority to join the network. This means that only approved nodes are allowed to participate in the consensus process and validate transactions.
2. **Centralized Governance :** Permissioned blockchains are often controlled by a single entity, such as a financial institution or a government agency. This central authority has the power to make decisions about the operation of the network and can implement changes to the protocol as needed.
3. **Enhanced Security :** Because only approved nodes can join the network, permissioned blockchains offer higher security than permissionless blockchains. This is because the central authority can carefully vet and approve nodes before they are allowed to join the network, reducing the risk of malicious actors.
4. **Limited Scalability :** Permissioned blockchains are often limited in terms of scalability due to the controlled access to the network. Because only a limited number of nodes are allowed to participate in the consensus process, the network may need help to handle a large volume of transactions.

❖ Permissionless blockchain

A permissionless blockchain is a blockchain network that allows anyone to join the network and participate in the consensus process without explicit permission. These networks are open and decentralized; any node can join and participate in validating transactions and creating new blocks.

Permissionless blockchains are often used in public applications where the network is open and transparent, such as the Bitcoin and Ethereum networks. These networks offer a high degree of decentralization and security, as they are not controlled by a single entity and are resistant to censorship and tampering.

Characteristics of Permissionless Blockchains

Permissionless blockchains have several characteristics that set them apart from permissioned blockchains.

1. **Open Access** : Permissionless blockchains allow anyone to join the network and participate in the consensus process without explicit permission. This means that any node can join the network and participate in validating transactions and creating new blocks.
2. **Decentralized Governance** : Permissionless blockchains are decentralized and are not controlled by a single entity. No central authority makes decisions about the network's operation, and changes to the protocol are implemented through a consensus process.
3. **Enhanced Decentralization** : Because permissionless blockchains are open and decentralized, they offer a higher degree of decentralization than permissioned blockchains. This means the network is resistant to censorship and tampering, as no central authority can change the protocol.
4. **Improved Scalability** : Permissionless blockchains are often more scalable than permissioned blockchains, as any node can join the network and participate in the consensus process. This means the network can handle a large volume of transactions as long as enough nodes support the load.

❖ Difference between Permissioned and Permissionless Blockchain

Category	Permissioned	Permissionless
Speed	Faster	Slower
Privacy	Private membership	Transparent and open – anyone can become a member
Legitimacy	Legal	Illegal
Ownership	Managed by a group of nodes pre-defined	Public ownership-no one owns the network
Decentralization	Partially decentralized	Truly decentralized
Cost	Cost-effective	Not so cost effective
Security	Less Secure	More secure

❖ Tokenized Blockchains

These are standard blockchains that generate cryptocurrencies through a consensus process using mining or initial distribution. In a tokenized blockchain, assets are represented by digital tokens. These tokens are essentially digital counterparts or representations of real-world assets, such as currency, real estate, stocks, or even other cryptocurrencies. These tokens can be transferred, traded, or exchanged on the blockchain just like physical assets in the real world. Smart contracts often play a crucial role in governing the behavior of these tokens, enabling automation and programmability.

Example : Ethereum and Binance Smart Chain are examples of blockchain platforms that support the creation and management of tokens through smart contracts

❖ Tokenless Blockchains

These blockchains are not real blockchains as they do not have the ability to transfer values, but they can be useful when it is not required to transfer value between nodes and there is only the need to transfer data among already trusted parties. A tokenless blockchain doesn't rely on native digital tokens to represent assets. Instead, the focus is on the blockchain itself as a ledger for recording and verifying transactions. Transactions on a tokenless blockchain are typically linked directly to the transfer of a cryptocurrency (e.g., Bitcoin) without the need for additional token representations. The blockchain primarily serves as a decentralized and distributed ledger.

Examples : Bitcoin is a prime example of a tokenless blockchain. In the Bitcoin network, the primary purpose is to transfer and store the cryptocurrency (BTC) directly without the need for additional tokens.

Tokenized vs Tokenless : Tokenized ledgers require cryptocurrency coins to operate. These ledgers are constructed around an incentive system that provides coins to those who operate the network. On the other hand, tokenless ledgers do not have such systems in place.

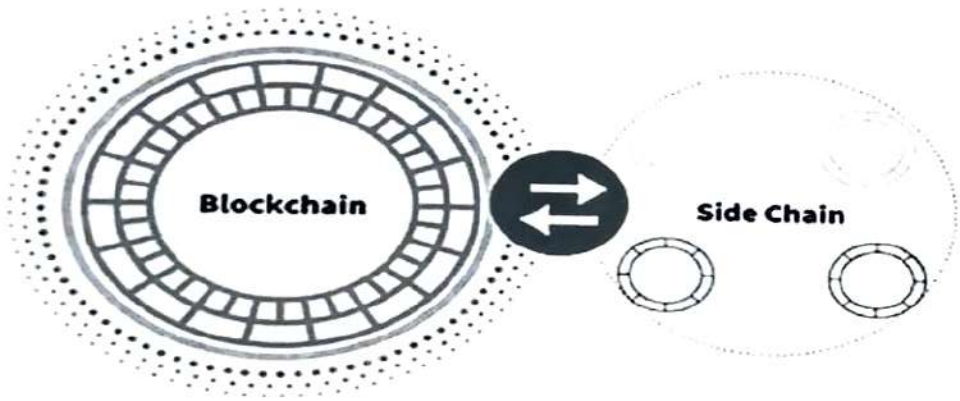
❖ Blockchain Architecture Vs Centralized Database

Sr. No.	Blockchain Architecture	Centralized Database
1	There is no dependence on third parties	Databases have central controls and administrations.
2	The data cannot be changed/deleted	Authorized users can change/delete data.
3	Adding/removing parties; no change in system architecture is required	Adding/removing parties; requires a change in system architecture.
4	Database management/maintenance costs are low.	Database management/maintenance costs are high.
5	High level verification is done with certificate verification	User authentication; provided with username and password.

6	The process flow is determined without the need for changes in the system architecture.	Changing process flow requires a changes in the system architecture.
7	All users have Open ledger where data is held.	The data is kept in a single centre.
8	It is compatible with the deed transfer process steps in the existing structure.	It is necessary to adapt the deed transfer process steps of the existing structure.
9	Users are provided to manage transactions in groups(Smart Contracts)	There is no structure like grouping transactions.
10	The blocks are stored with time stamps	The timestamps can be added only manually.
11	Suitable where trust between parties is not required.	Central reliable authority is needed.
12	The process flow is kept together with the data in the blocks.	Process flow can be added manually with the logging mechanism.

2.2 SIDECHAIN

A sidechain is a separate blockchain that is interoperable with a main blockchain but operates somewhat independently. The concept of sidechains was introduced to address certain scalability and functionality issues in blockchain networks.



Here are key points about sidechains :

1. ***Interoperability*** :

A sidechain is designed to work alongside a main blockchain, often referred to as the "parent" or "main" chain. The two chains are interoperable, allowing assets to be transferred between them.

2. **Scalability :**

One of the main purposes of sidechains is to address scalability concerns. By offloading some transactions or smart contract executions to a sidechain, the main blockchain can alleviate congestion and potentially improve overall performance.

3. **Customization and Specialization :**

Sidechains can be designed with specific features or functions tailored to certain use cases or industries. For example, a sidechain could be optimized for faster transaction confirmation times, lower fees, or enhanced privacy features.

4. **Two-Way Peg :**

The mechanism for transferring assets between the main chain and the sidechain is often facilitated by a concept called a "two-way peg." This ensures that assets are securely locked on the main chain when moved to the sidechain and vice versa.

5. **Security :**

Sidechains need to maintain a certain level of security to ensure the integrity of the transferred assets. Various mechanisms, including cryptographic proofs, are employed to secure transactions on sidechains.

Examples :

An element, developed by Blockstream, is a platform that enables the creation of sidechains for Bitcoin. RSK (Rootstock) is another example, providing a sidechain that is compatible with the Bitcoin blockchain and supports smart contracts.

Use Cases :

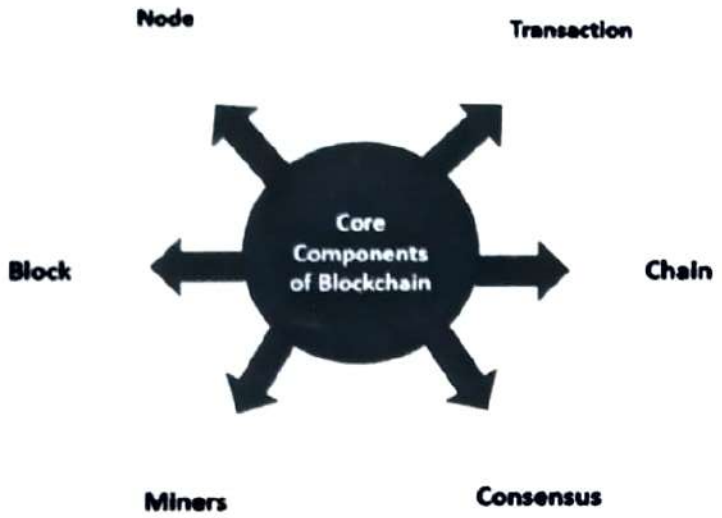
Sidechains are employed to experiment with new features, test scalability solutions, and enable specialized functionalities without directly impacting the main blockchain. They are particularly useful in situations where the main chain might be more conservative in implementing changes.

Challenges :

Despite the advantages, challenges exist, such as ensuring the security of assets on sidechains and managing the complexity of cross-chain interactions. Additionally, the concept of sidechains has evolved, and there are alternative solutions, like Layer 2 scaling solutions, that aim to address similar scalability issues.

Sidechains are part of the broader landscape of blockchain scaling solutions and interoperability protocols, offering a way to extend the capabilities of existing blockchains while maintaining a connection to the security and decentralization of the main chain.

2.3 CORE COMPONENTS OF BLOCKCHAIN



1. **Node** :

Nodes are network participants and their devices permit them to keep track of the distributed ledger and serve as communication hubs in various network tasks. A block broadcasts all the network nodes when a miner looks to add a new block in transactions to the blockchain.

2. **Transactions** :

A transaction refers to a contract or agreement and transfers of assets between parties. The asset is typically cash or property. The network of computers in blockchain stores the transactional data as copy with the storage typically referred to as a digital ledger.

3. **Block** :

A block in a blockchain network is similar to a link in a chain. In the field of crypto currency, blocks are like records that store transactions like a record book, and those are encrypted into a hash tree. There are a huge number of transactions occurring every day in the world. It is important for the users to keep track of those transactions, and they do it with the help of a block structure. The block structure of the blockchain is mentioned in the very first diagram in this article.

4. **Chain** :

Chain is the concept where all the blocks are connected with the help of a chain in the whole blockchain structure in the world. And those blocks are connected with the help of the previous block hash and it indicates a chaining structure.

5. **Miners :**

Blockchain mining is a process that validates every step in the transactions while operating all cryptocurrencies. People involved in this mining they called miners. Blockchain mining is a process to validate each step in the transactions while operating cryptocurrencies.

6. **Consensus :**

A consensus is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies. It is useful in record keeping and other things.

2.4 DISTRIBUTED IDENTITY : PUBLIC AND PRIVATE KEYS, DIGITAL IDENTIFICATION, AND WALLETS

Distributed identity involves the use of cryptographic principles and blockchain technology to establish, manage, and verify digital identities in a decentralized and secure manner. Several key components play a crucial role in the implementation of distributed identity systems :

1. **Public and Private Keys :**

- **Public Key :**

  This is a cryptographic key that is shared openly and serves as an address to which others can send encrypted messages or assets. In the context of distributed identity, a public key can be associated with an individual's identity.

- **Private Key :**

  This is a secret key known only to the individual to whom it belongs. It is used to decrypt messages sent to the associated public key and to sign transactions or messages, providing a secure way to prove ownership.

2. **Digital Identification :**

- **Digital Identity :**

  Digital identity refers to the representation of an individual's identity in the digital realm. It includes various attributes such as name, age, address, and other relevant information. In a distributed identity system, these attributes are often cryptographically linked to the individual's public key.

- **Decentralized Identifiers (DIDs) :**

  DIDs are a type of identifier that is created, owned, and controlled by the subject of the identifier. DIDs are typically associated with a public-private key pair and are registered on a blockchain or decentralized identity system.

3. **Wallets** :

- **Digital Wallets** :

  Digital wallets are software tools that store and manage public and private key pairs. In the context of distributed identity, a digital wallet can securely store the private keys associated with an individual's identity, allowing them to sign transactions or provide proof of identity.

- **Self-Sovereign Identity (SSI)** :

  SSI is a concept that emphasizes the individual's control over their own identity. With SSI, individuals use their digital wallets to manage and share their identity information without relying on a central authority. Blockchain technology often underlies SSI systems to provide security and decentralization.

4. **Blockchain Technology** :

- **Decentralized Ledger** :

  Blockchain serves as a decentralized and tamper-resistant ledger to record and verify identity-related transactions. It allows for the secure storage of identity attributes and transactions, and it enables the creation of decentralized identity systems.

- **Smart Contracts** :

  Smart contracts on blockchain platforms can be used to execute predefined rules related to identity verification and management. For example, a smart contract can govern the issuance or revocation of digital credentials.

5. **Digital Signatures** :

Digital signatures, generated using private keys, play a crucial role in proving the authenticity of messages, transactions, or identity-related claims. Verification of digital signatures ensures that the information has not been tampered with and comes from the legitimate owner of the private key.

Distributed identity systems leverage these components to create a more secure, privacy-focused, and user-controlled approach to identity management. Users have greater control over their personal information, reducing the reliance on centralized authorities and mitigating the risks associated with data breaches and identity theft.

❖ **Cryptocurrency Wallets**

Cryptocurrency wallets are digital tools that enable users to store, manage, and interact with their cryptocurrencies. These wallets don't actually store the coins but keep the private keys necessary to access and manage the assets on the respective blockchain. There are various types of cryptocurrency wallets, each with its own set of features, security measures, and use cases. Here are some common types of cryptocurrency wallets :

1. **Software Wallets** :

- Online Wallets : These are wallets hosted on the cloud, accessible via a web browser. They are convenient but potentially less secure due to the online nature. Examples include Coinbase, Binance, and Kraken wallets.

- Desktop Wallets : Installed on a computer, desktop wallets provide more control over security. Popular options include Exodus, Electrum, and Bitcoin Core.
- Mobile Wallets : Designed for smartphones, mobile wallets offer portability. They can be either custodial (controlled by a third party, e.g., Coinbase) or non-custodial (you control your private keys, e.g., Trust Wallet, MyEtherWallet).

2. **Hardware Wallets :**
   - Physical devices that securely store private keys offline. They are less susceptible to online hacking as they are not connected to the internet when not in use. Examples include Ledger Nano S, Ledger Nano X, and Trezor.

3. **Paper Wallets :**
   - A paper wallet is a physical document containing your public and private keys. It's typically printed or written down and should be kept in a safe place. However, creating and using paper wallets require caution and a good understanding of security practices.

4. **Brain Wallets :**
   - A brain wallet is a type of wallet where the user memorizes a passphrase instead of storing a physical or digital copy. However, relying solely on memory can be risky if the passphrase is forgotten or easily guessable.

5. **Multi-Signature Wallets :**
   - Multi-signature (multisig) wallets require multiple private keys to authorize a cryptocurrency transaction. They are often used for added security in business settings or joint accounts.

6. **Web Wallets :**
   - Web wallets are wallets provided by online platforms. Users access them through a web browser and are subject to the security measures implemented by the platform. It's crucial to use reputable platforms with strong security protocols.

7. **Deterministic Wallets :**
   - Deterministic wallets generate a sequence of public and private key pairs from a single seed. This seed can be used to restore the entire wallet in case of loss or theft.

When choosing a cryptocurrency wallet, factors such as security, ease of use, and the specific needs of the user should be considered. Hardware wallets are generally considered more secure for long-term storage (cold stor age), while software wallets are convenient for everyday transactions (hot wallets). It's important to follow best practices for securing private keys and to keep backups in case of device loss or failure.

2.5 DECENTRALIZED NETWORK, DISTRIBUTED LEDGER

❖ Centralization VS Decentralization

	Centralization	Decentralization
Network	Controlled by and dependent on a single entry in a particular location	Control and authority are shared by all the network members/nodes
Data Control	Maintained by central server/entity	Everyone owns the exact same copy of the data and is only added via the community consensus mechanism
Point of failure	A single point of failure	No single point of failure
Security level	Maintained by central server/entity	Ensured by several cryptographic algorithms and consensus mechanisms applied
Performance	Depends on central server efficiency	Depends on the members of the network and the consensus mechanism used
Type of Infrastructure	Permissioned	Permissioned, Permissionless and Consortium
Example	Banking system	Blockchain

Decentralized networks and distributed ledgers are fundamental concepts in blockchain technology, playing key roles in achieving the decentralization, security, and transparency that are characteristic of blockchain systems.

1. Decentralized Network :

Definition : A decentralized network refers to a network architecture in which no single entity or central authority has control over the entire network. Instead, the network is distributed among multiple nodes (computers) that participate in the validation, consensus, and maintenance of the network. Blockchain is a decentralized peer-to-peer network. It provides an efficient way to work with unknown parties without trusting each other. Blockchain is a transparent and immutable (data can't be modified later) network that enables append-only records. Therefore, it's easier and more secure to share information among different parties.

Characteristics :

- **Peer-to-Peer Communication :** Nodes in a decentralized network communicate directly with each other without relying on a central server or intermediary.

- **Redundancy :** Information is redundantly stored across multiple nodes, reducing the risk of a single point of failure and enhancing resilience.
- **Autonomy :** Each node in the network has equal status, and decisions are often made through consensus mechanisms agreed upon by the participating nodes.

❖ **What are the Benefits of Decentralization ?**

Following are the benefits of implementing the decentralization model in Blockchain.

- **Trustless yet cooperated ecosystem**

A decentralized network eliminates the need to trust another party. Each network member carries the exact same copy of data. Hence, even if a node gets corrupted or tampered with. It will either be corrected or rejected by other network members collectively.

- **Real-time data distribution and reconciliation**

Data in a decentralized network are distributed in real-time. That leaves absolutely no option for data loss or incorrect data. Therefore, even if there's some non-relevant or incorrect data in the network. It could be easily eliminated by sending the correct copy of the data.

- **Eliminate dependency on a single entity.**

Decentralization provides an equal amount of power, authority, and responsibility to each member of the network. Hence, the power and dependency are shifted from a central entity to all the members in the network. In brief, it's for the network and by the network.

- **Reduces the chances of massive failure**

In the case of a centralized network, if the central entity gets disrupted. The following connected nodes get down as well. Hence, led to network shutdown or failure. However, a decentralized network it greatly reduces the chances of the whole system getting down at once.

- **Faster transactions**

Transaction in a decentralized network is much faster than in a centralized network. As it skips over the intermediate processing and transactions. Hence, results in faster transactions.

- **Examples :**
  - Blockchain networks, such as Bitcoin and Ethereum, operate on decentralized networks where nodes validate transactions and reach consensus through mechanisms like Proof of Work (Bitcoin) or Proof of Stake (Ethereum).

2. **Distributed Ledger :**

Definition :

A distributed ledger is a digital record of transactions or other data that is duplicated and distributed across the entire network of computer systems in a blockchain. It is maintained collaboratively by the

network nodes through a consensus protocol. A blockchain is a digital ledger of transactions that are distributed across the entire network of computers (or nodes) on the blockchain. Distributed ledgers use independent nodes to record, share, and synchronize transactions in their respective electronic ledgers instead of keeping them in one centralized server. A blockchain uses several technologies like digital signatures, distributed networks, and encryption/ decryption methods including distributed ledger technology to enable blockchain applications.

Blockchain is one of the types of DLT in which transactions are recorded with an unchangeable cryptographic signature called a hash. That is why distributed ledgers are often called blockchains.

Characteristics :

- **Decentralized :**

It is a decentralized technology and every node will maintain the ledger, and if any data changes happen, the ledger will get updated. The process of updating takes place independently at each node. Even small updates or changes made to the ledger are reflected and the history of that change is sent to all participants in a matter of seconds.

- **Immutable :**

Distributed ledger uses cryptography to create a secure database in which data once stored cannot be altered or changed.

- **Append only :**

Distributed ledgers are append-only in comparison to the traditional database where data can be altered.

- **Distributed :**

In this technology, there is no central server or authority managing the database, which makes the technology transparent. To counter the weaknesses of having one ledger to rule all, So that there is no one authoritative copy and have specific rules around changing them. This would make the system much more transparent and will make it a more decentralized authority. In this process, every node or contributor of the ledger will try to verify the transactions with the various consensus algorithms or voting. The voting or participation of all the nodes depends on the rules of that ledger. In the case of bitcoin, the Proof of Work consensus mechanism is used for the participation of each node.

- **Shared :**

The distributed ledger is not associated with any single entity. It is shared among the nodes on the network where some nodes have a full copy of the ledger while some nodes have only the necessary information that is required to make them functional and efficient.

- **Smart Contracts :**

Distributed ledgers can be programmed to execute smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. This allows for transactions to be automated, secure, and transparent.

- **Fault Tolerance :** Distributed ledgers are highly fault-tolerant because of their decentralized nature. If one node or participant fails, the data remains available on other nodes.

Advantages :

- **Security :**

The decentralized nature of the ledger, combined with cryptographic techniques, enhances security and reduces the risk of fraudulent activities.

- **Trust :**

Participants can trust the information on the ledger without relying on a central authority, as the ledger is maintained collectively.

- **Efficiency :**

Transactions can be verified and added to the ledger more efficiently through decentralized consensus mechanisms.

- **Transparency :**

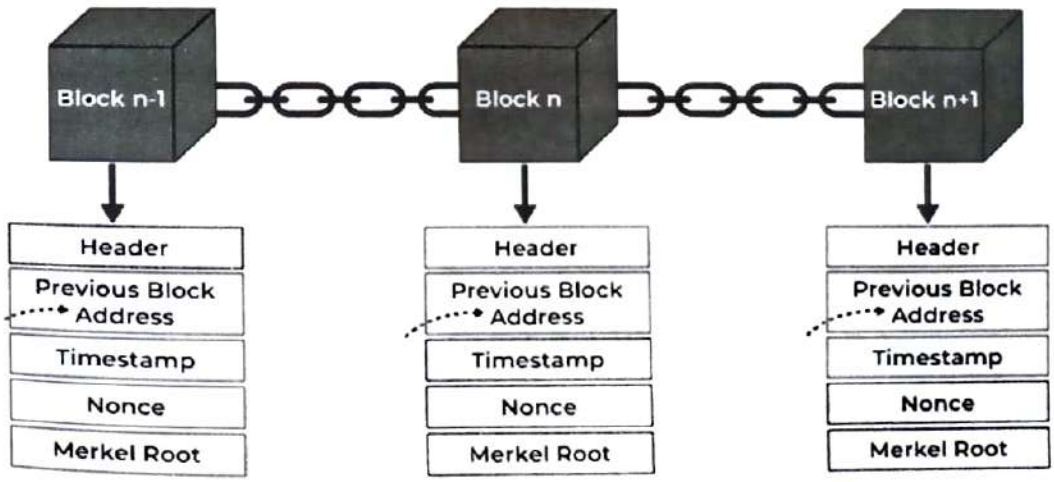
Distributed ledgers are transparent because every participant can see the transactions that occur on the ledger. This transparency helps in creating trust among the participants.

Examples :

In a blockchain, the ledger is distributed across all nodes, and each node has a copy of the entire transaction history. Every new block added to the blockchain contains a set of transactions, and once validated, it becomes part of the distributed ledger.

In summary, a decentralized network refers to the distribution of control and decision-making across multiple nodes, while a distributed ledger involves the duplication and distribution of a digital record of transactions across the network. Together, these concepts form the foundation for the decentralized, secure, and transparent nature of blockchain technology.

2.6 DATA STRUCTURE OF A BLOCKCHAIN



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 $i+1^{th}$ block to the i^{th} block using the hash. In short, it is a reference to the hash of the previous (parent) block in the chain.

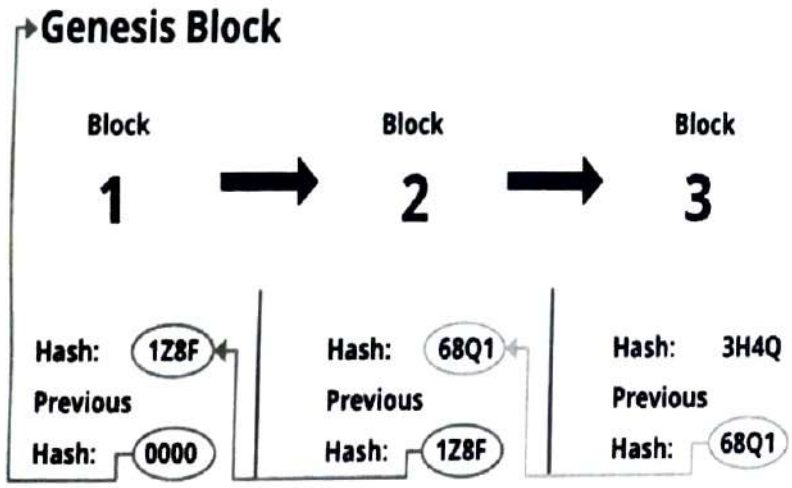
3. **Timestamp** : It is a system verify the data into the block and assigns a time or date of creation for digital documents. The timestamp is a string of characters that uniquely identifies the document or event and indicates when it was created.

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.

❖ **Genesis Block in Blockchain**

The Genesis Block is the first block in the blockchain and contains unique characteristics that distinguish it from the posterior blocks in the chain. It's the only block that doesn't source a former block, as there are no blocks before it. rather, the Genesis Block is hard coded into the blockchain's protocol as the starting point.



Key characteristics of the Genesis Block include :

1. **Unique Identifier :** The Genesis Block is distinguished by its unique identifier or block number (often set to 0) and is the initial entry in the blockchain.

2. **No Previous Block Reference** : Since it is the first block, there is no reference to a previous block's hash. In the block header, the "previous block hash" field typically contains a placeholder or is left empty.

3. **Coinbase Transaction** : The first transaction in the Genesis Block is known as the coinbase transaction. It is a special transaction that creates new cryptocurrency units and may contain a message or reference commemorating an event or intention of the blockchain's creation.

4. **Establishing the Blockchain** : The creation of the Genesis Block marks the beginning of the blockchain. Once it is established, subsequent blocks reference it, creating a chronological and immutable chain of blocks.

5. **Hardcoded Information** : The Genesis Block may include hardcoded information, such as a timestamp, a message from the creator, or any other data deemed significant by the developers.

For example, in the case of Bitcoin, the Genesis Block was mined by Satoshi Nakamoto on January 3, 2009. The coinbase transaction included a message referencing a newspaper headline from that day, emphasizing the timestamp and linking it to the financial crisis.

Overall, the Genesis Block is a foundational element of blockchain technology, and its unique features make it an important element in the development and functioning of blockchain networks.

Why Genesis Block is Needed ?

The Genesis Block is a critical element of a blockchain network because it serves as the foundation for the entire network. Then are some reasons why the Genesis Block is demanded

- **Initializing the Network** : The Genesis Block is the veritably first block in a blockchain, and it's used to initialize the network. It contains a set of hardcoded data that sets the foundation for posterior blocks, similar to the network's original parameters, the first deals, and the cryptographic hash that identifies the block.

- **Ensuring Consensus** : Because the Genesis Block is the first block in a blockchain, it's used to establish an agreement among network actors about the original state of the network. This is important because blockchain networks calculate on an agreement medium to ensure that all actors agree on the current state of the network.

- **Providing a Fixed Starting Point** : The Genesis Block provides a fixed starting point for the blockchain, which ensures that all posterior blocks can be vindicated and traced back to the veritably first block. This is important for icing the integrity of the blockchain and precluding fraudulent or vicious exertion.

- **Setting the Block Price** : In numerous blockchain networks, the Genesis Block is the only block that has a fixed block price. This is important because it incentivizes miners to start booby-trapping the network and contribute calculating power to secure the network.

- **Establishing Historic Significance** : The Genesis Block has significant literal and artistic significance in the blockchain world, as it represents the birth of a new period of decentralized peer-to-peer networks. It's a symbol of the eventuality for decentralized technologies to transfigure society and produce a more fair and indifferent fiscal system.

Significance of Genesis Block

- **Starting point of the Network** : It serves as the foundation and starting point of every blockchain network.
- **Contains critical information** : It contains critical information that establishes the original state of the network, similar to difficulty position, network rules, and a maximum number of coins.
- **Serves as a reference point** : It serves as a reference point for all posterior blocks in the chain, linking them together in a tamper-apparent way.
- **Makes blockchain immutable** : Any changes made to the Genesis Block would abate the entire chain, making it impossible to add new blocks or conduct deals on the network.
- **Nonfictional significance** : The Genesis Block has a nonfictional and cultural significance as it marks the birth of the first blockchain network, Bitcoin, and the morning of a new period of decentralized technology. It paved the way for the development of other blockchain-grounded operations and cryptocurrencies.

Exercises

❑ **MCQs :**

1. What is the genesis block ?

   A. Any block created by the founder

   B. The last block created in the Blockchain

   C. The first block of a Blockchain

   D. The first transaction in each block

2. Bitcoin is based on _____ blockchain.

   A. Private B. Public

   C. Public Permissioned D. Permissioned

3. What time did Bitcoin Network Start ?

   A. August 2004 B. November 2008

   C. January 2009 D. December 2011

4. The transaction Merkle Tree root value in a Bitcoin block is calculated using.
   A. Hash of transactions
   B. Previous block's hash
   C. Number of transactions
   D. None of the above

5. In blockchain, a block is consist of _____
   A. Transaction data
   B. A Hash point
   C. A Timestamp
   D. All of the above

6. The process of creating new bitcoins is known as _____
   A. Sourcing
   B. Financing
   C. Mining
   D. None of the above

7. _____ characteristic makes blockchain tamper-proof.
   A. VPN
   B. Crypt ocurrency
   C. Immutability
   D. All of the above

Questions :

1. Explain the structure of Blockchain
2. What is the difference between blockchain and database?
3. Briefly discuss what are the different types of Block chains?
4. Describe the key characteristics of public blockchain. In which situation permissionless blockchain can be used?.
5. Describe the key features of private Blockchain.
6. Describe the key features of consortium Blockchain.
7. Differentiate between permissioned blockchain v/s permissioned less blockchain.

***

UNIT

3 ESSENTIALS OF BLOCKCHAIN

3.1 CONSENSUS MECHANISMS IN BLOCKCHAIN

Data consistency and security are the principles that guide blockchain technology. There are different mechanisms and algorithms blockchains use to regulate their working throughout the chain to achieve this. In this unit, we will learn about the various blockchain consensus mechanisms and their types.

❖ What is a Consensus Mechanism ?

Blockchains are decentralized, so no single entity is allowed to set the truth. All the participating entities (computers) usually do not know each other; thus, determining who is telling the truth or has the correct set of data becomes difficult. This is where a consensus mechanism is required, which helps these computers agree on the truth.

There are different types of consensus mechanisms that have been developed; each has its unique properties and tradeoffs in terms of how secure the agreement is and who gets to vote on what. The general purpose of a consensus mechanism is to manage which participant in the network gets to set the state of truth which everyone else follows and agrees on. 'Consensus' simply means an agreement between a group of people, and in the world of blockchain it is an important concept

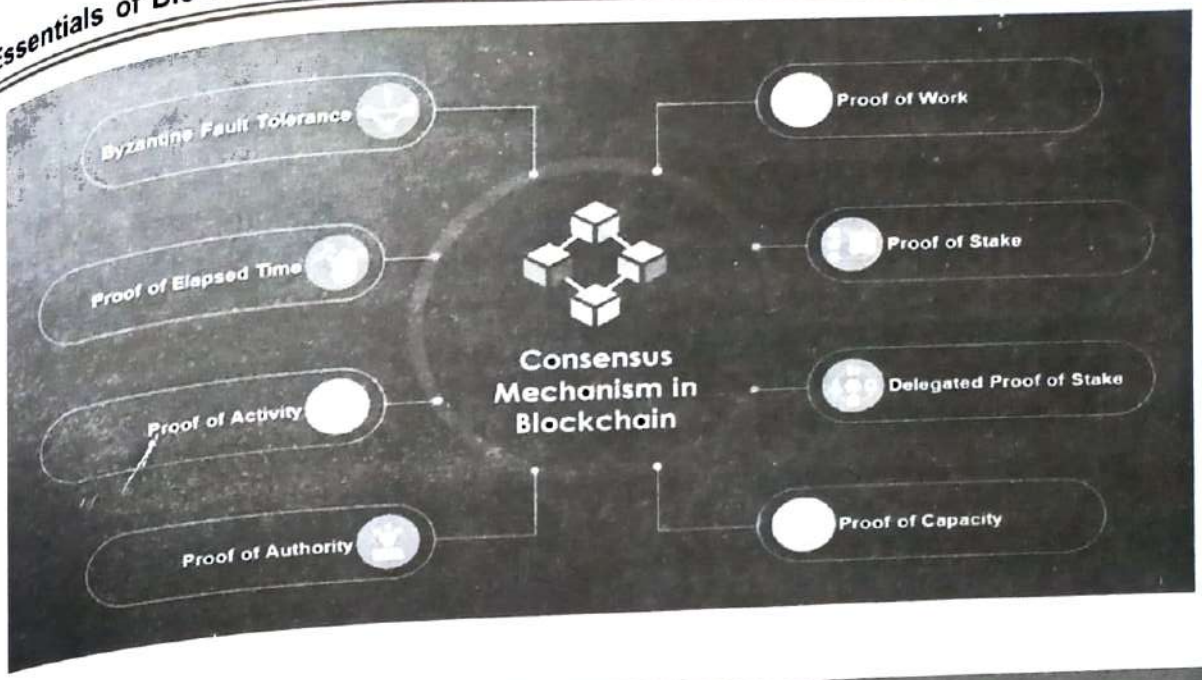
❖ Types of Consensus Mechanisms

Let us discuss the different types of consensus mechanisms:

1. PoW :

Proof of Work is the first and most recognizable consensus mechanism developed by Bitcoin's founder Satoshi Nakamoto.

'Proof' refers to the solution of a highly-complex problem, and 'work' refers to the process of solving the same. Crypto coin miners compete to solve the problem and gain the right to process the transaction. The fastest solver receives a mining fee from the traders of these coins.



DIFFERENT TYPES OF CONSENSUS MECHANISMS

PROOF OF WORK (PoW)

- PoW lets miners add a new block to the network based on the computation done to find the correct block hash.

PROOF OF STAKE (PoS)

- PoS uses a staking mechanism where participants lock up some of their coins to get selected for block addition.

DELEGATED PROOF OF STAKE (DPoS)

- In DPoS mechanism, the block delegates' selection is based on voting. It's an additional layer to PoS.

PROOF OF IMPORTANCE (PoI)

- PoI rewards users with importance scores which eventually helps them to become block harvesters.

PROOF OF CAPACITY (PoC)

- PoC uses the storage capacity for mining a block in a decentralized network.

PROOF OF ELAPSED TIME (PoET)

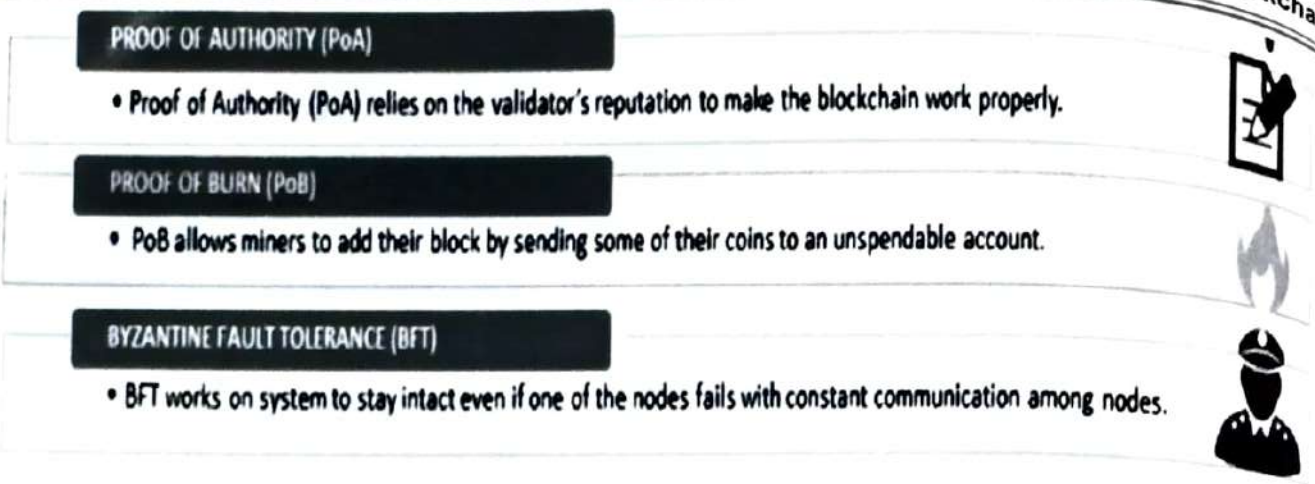
- PoET uses a time-lottery-based consensus mechanism, distributing wait time to each participating node.

PROOF OF ACTIVITY (PoA)

- Proof of Activity (PoA) combines the capabilities of proof of work (PoW) and Proof of Stake (PoS) algorithms.

PROOF OF ACTIVITY (PoA)

- Proof of Activity (PoA) combines the capabilities of proof of work (PoW) and Proof of Stake (PoS) algorithms.



This mechanism tracks and verifies the creation and transactions across blockchain networks. It enables miners by allowing them to validate new transactions and is extremely secure. However, it has several cons, such as high electricity requirements and difficulty for individual miners.

Proof of work depends on an army of miners, or validators, to verify transactions through solving arbitrary mathematical problems in the race for a block prize. In PoW, miners compete with each other to find the transaction hash, and the miner who finds the hash first is allowed to add the transaction to a block and then mine the block. The process of finding the block hash is very computation-intensive; having a high hash rate is aimed by the miners and thus generates more rewards.

Examples : Bitcoin, Dogecoin, Litecoin

2. PoS :

PoW requires enormous electricity due to intense computational requirements to catch the hash. In Proof of Stake, miners/validators stake their tokens and are allowed to mine/validate transactions. A miner doesn't have to compete with each other; a miner is chosen randomly to mine the transaction hash. Usually, the higher the number of tokens staked, the higher the chances for a miner to get selected. Ethereum will be moving to a PoS consensus model from its current PoW consensus model, with Ethereum 2.0 now known as Ethereum upgrades.

This mechanism requires comparatively less energy, transaction time and a lower fee. There is a security risk as if an owner owns 51% or more coins of a particular coin, then that person will get sole ownership of its network.

Examples : Coins like Etherium 2.0, Polkadot, Cosmos, Cardano, ThorChain, Nxt and Algorand

3. DPoS :

Delegate Proof of Stake is a variation of PoS; in this mechanism, all the token holders can collectively choose to elect a list of nodes to mine blocks. Token holders can also vote on network changes, etc. This gives all token holders ownership of the network.

In this approach to determining consensus, network participants cast votes via staking pools for their favored delegate, those who are presumed to be best equipped to protect the network, based on reputation. As a result, validating privileges are reserved and awarded at random only to a team of top tier candidates. At any point in time, a validator can be surpassed by someone deemed more trustworthy.

This system is efficient and democratic. It improves from the original proof-of-stake method by being more financially inclusive to users and provides incentive for validators to remain accountable in keeping the network alive.

While there is an obvious tradeoff of decentralization, a delegated proof-of-stake protocol may be considered too high maintenance for some users as it requires a healthy level of engagement. Appointing network control to a few over many also increases its vulnerability to malicious actors, such as in a 51 percent attack.

Examples : EOS, Lisk, Ark, Tron, BitShares, Steem

4. **PoH :**

Proof of History came into existence because of Solana; it cryptographically verifies the passage of time between two events using a sequence of computations. It uses a cryptographically secure function input must be executed entirely to generate output, and the output cannot be determined from the input.

Proof of history integrates the element of time into a blockchain's protocol. During the verification process, timestamps are embedded into the hash of each generated block, chronicling a network's transaction history in a singular, unbroken chain. It's important to note that this verification method is only viable as a supplement to another protocol. The hybrid consensus algorithm is most often seen working in tandem with a proof-of-work or proof-of-stake system.

It's fast and secure without negating a platform's existing state of decentralization. Proof of history is also associated with low transaction costs, or "gas fees." The most well known platform that uses proof of history, Solana.

A major disadvantage to high transaction speeds is the amount of data that accumulates. The hardware fit to run such advanced software disqualifies the average user from being able to serve the network as a validator.

Examples : Solana

5. **POA : Proof of Authority**

Favored by private or permissioned blockchains, a proof-of-authority consensus mechanism selects validators based on reputation rather than a user's digital assets. In this system, a group of validators are pre-approved in a selection process that often includes a background check.

This method is highly scalable and requires virtually no computing power.

Any structure designed to concentrate power compromises decentralization. Additionally, validator's pseudo-anonymity is forfeited, as public identifiability is part of the deal.

Examples : Xodex, JP Morgan (JPMCoin), VeChain (VET) and Ethereum Kovan testnet

6. **POA : Proof of Activity :**

This mechanism is a combination of both Proof of Work and Proof of Stake. It has been designed to combine the best features of PoW and PoS. In the beginning, the Proof-of-Activity mechanism functions like PoW. Once a new block is completed, it starts to function like a Proof-Of-Stake mechanism.

Examples : Coins such as DCR (Decred)

7. **Proof of Capacity :**

In the Proof of Capacity consensus, validators are supposed to invest their hard drive space instead of investing in expensive hardware or burning coins. The more hard drive space validators have, the better their chances of getting selected for mining the next block and earning the block reward.

The PoC mechanism heavily relies on free space available in the hard drive. This is because there are many solutions to a coin's hash problem that a trader needs to store. It is highly efficient as compared to PoW and PoC mechanisms.

Examples : Coins such as Burst, Storj, SpaceMint and Chia

8. **Proof of Burn (PoB) :**

With PoB, instead of investing in expensive hardware equipment, validators 'burn' coins by sending them to an address from where they are irretrievable. By committing the coins to an unreachable address, validators earn the privilege to mine on the system based on a random selection process. Thus, burning coins here means that validators have a long-term commitment in exchange for their short-term loss. Depending on how the PoB is implemented, miners may burn the native currency of the Blockchain application or the currency of an alternative chain, such as bitcoin. The more coins they burn, the better their chances of being selected to mine the next block. While PoB is an interesting alternative to PoW, the protocol still wastes resources needlessly. And it is also questioned that mining power simply goes to those who are willing to burn more money.

PoB aims to improve the quality of blockchain so that it can be used easily and extensively as a tool for faster and more secured transactions. After PoW and PoS, PoB is designed to prevent fraud activities on a blockchain network.

Examples : Bitcoin

9. Proof of Elapsed Time :

PoET is one of the fairest consensus algorithms which chooses the next block using fair means only. It is widely used in permissioned Blockchain networks. In this algorithm, every validator on the network gets a fair chance to create their own block. All the nodes do so by waiting for a random amount of time, adding proof of their wait in the block. The created blocks are broadcasted to the network for others' consideration. The winner is the validator which has the least timer value in the proof part. The block from the winning validator node gets appended to the Blockchain. There are additional checks in the algorithm to stop nodes from always winning the election, and stop nodes from generating the lowest timer value.

Intel Corporation created this mechanism to permit blockchain to decide the person who will create the next block. It uses a lottery system to decide the next block creator. Thus, it gives a fair chance to all traders to create the next block. It is an efficient process involving utilizing lesser resources and low energy consumption.

10. PBFT : Practical Byzantine Fault Tolerance

Practical Byzantine Fault Tolerance is a consensus algorithm introduced in the late 90s by Barbara Liskov and Miguel Castro. pBFT was designed to work efficiently in asynchronous(no upper bound on when the response to the request will be received) systems. It is optimized for low overhead time. Its goal was to solve many problems associated with already available Byzantine Fault Tolerance solutions.

Byzantine Fault Tolerance(BFT) is the feature of a distributed network to reach consensus(agreement on the same value) even when some of the nodes in the network fail to respond or respond with incorrect information. The objective of a BFT mechanism is to safeguard against the system failures by employing collective decision making(both – correct and faulty nodes) which aims to reduce to influence of the faulty nodes. BFT is derived from Byzantine Generals' Problem.

Nodes in a pBFT enabled distributed system are sequentially ordered with one node being the primary(or the leader node) and others referred to as secondary(or the backup nodes). Any eligible node in the system can become the primary by transitioning from secondary to primary(typically, in the case of a primary node failure). The goal is that all honest nodes help in reaching a consensus regarding the state of the system using the majority rule.

11. PoI : Proof of Importance

Proof of Importance (PoI) in blockchain sets new standards for network participants or coin hoarders to become eligible for harvesting a new block of transactions in the network. It rewards users with importance scores, which eventually help them become block harvesters. One of the biggest disadvantages of PoS is to promote the rich getting richer syndrome.

The PoI consensus algorithm was introduced by the NEM (New Economy Movement) blockchain in 2015 to overcome the drawbacks of PoS. Their cryptocurrency coin is called XEM. Proof of Importance in blockchain resolves the limitations of PoS by assigning consensus addresses and importance scores. Think of importance scores as a trust or reputation score in the network. A higher score means the network trusts you more to verify or forge the new block of transactions. Hence, higher chances of getting selected as block harvesters (miners in the PoI mechanism).

With PoI, your chances of verifying the transaction isn't solely dependent on your stakes. However, it depends on how many transactions and the quality of the transactions you have processed in the past.

Choosing a consensus mechanism depends on various factors, including the goals of the blockchain network, the desired level of decentralization, scalability requirements, and the trade-offs between security and efficiency. Each mechanism has its strengths and weaknesses, and the choice often reflects the priorities of the blockchain's developers and community.

❖ **What are the advantages of the consensus mechanism?**

Consensus mechanisms offer several advantages, such as :

- **No barriers to participation**

  Any crypto trader or miner across the globe can participate in a consensus mechanism. There are few barriers to participation in a consensus for any crypto coin.

- **Builds trust among users**

  Traders and miners of a particular coin across the globe must agree to approve a decision. This, in turn, builds trust among the users.

- **Establishes security**

  Consensus mechanisms maintain the transparency of trading for all coins. Thus, traders can ensure that no fraud occurs during a transaction.

❖ **What are the disadvantages of the consensus mechanism?**

The minor disadvantages of a consensus mechanism include :

- **Severe chances of hacking**

  There lies a chance of hacking known as 51% hack, which stands out as a potential attack on a consensus mechanism.

- **Excessive use of electricity**

  There is a heavy requirement for electricity for the PoW mechanism to function.

With very few associated disadvantages, the consensus mechanism is a great security tool for a decentralised form of trade. This allows traders and miners across the globe to establish a connection and trust among themselves and benefit from the mechanism.

❖ **Comparison of Consensus Algorithms**

Consensus Mechanism	Advantages	Disadvantages	Protocols using it
Proof of Work	Decentralized structure High level of security Acceptable level of scalability	High block time Energy Inefficiency Hardware dependency	Bitcoin Dogecoin Litecoin
Proof of Stake	Fast block creation time High throughput Energy efficiency Scalability (but less than POW) Independence to special hardware	Suffer from centralization Lower cost of misbehaving	Tezos Cardano Ethereum
Delegated Proof of Stack	Scalability Energy efficiency Low cost transaction	Semi-centralization Highly susceptible to 51% attack	EOS Ark Tron
Practical Byzantine Fault Tolerance	High throughput Energy efficiency	Not scalable Susceptible to sybil attacks	Hyper ledger Fabric Zilliqa
Proof of Capacity	No special hardware More decentralized	Susceptible to grinding attackSpace privilege applies	Burstcoin Permacoin
Proof of Authority	Transactional speed Tighter security	Not decentralized Break anonymity	VeChain Plam Network Xodex

3.2 CONFIRMATION AND FINALITY : THE LIMITS OF PROOF OF-WORK, ALTERNATIVE OF PROOF OF WORK

❖ **Confirmation**

Confirmation refers to the act of including a transaction in a block and adding that block to the blockchain. Each confirmation increases the level of certainty that the transaction is final and cannot be reversed. The more confirmations a transaction has, the higher the level of finality.

❖ Transaction finality

Transaction finality refers to the guarantee that once a transaction is recorded on the blockchain like Ethereum or Bitcoin, it cannot be reversed or altered. It provides certainty and trust in the integrity of transactions within a decentralized network.

Transaction finality stands as a vital feature that secures the immutability and irreversibility of cryptocurrency transactions. It's an assurance that once a transaction is completed, it becomes part of an immutable ledger – unalterable, irreversible, and beyond cancelation.

Transaction finality plays a crucial role in achieving trust and security in blockchain transactions. It ensures that once a transaction is completed, it cannot be altered, reversed, or revoked.

This guarantee of immutability is essential for building trust among participants in the crypto ecosystem. With traditional financial systems, there is always a risk of transactions being tampered with or canceled, leading to potential fraud and disputes.

In blockchain technology, transaction finality guarantees that once a transaction is confirmed on the blockchain through consensus mechanisms and cryptographic algorithms, it becomes part of an immutable ledger that can be relied upon by all nodes on the network.

This level of reliability and assurance enhances security and eliminates the need for intermediaries to validate and confirm transactions.

❖ Importance in Achieving Trust and Security in Blockchain Transactions

The importance of achieving transaction finality goes beyond just trust; it also contributes to the overall security of cryptocurrency transactions. In traditional banking systems, fraudulent activities such as double-spending are possible due to the centralized nature of control over transactions.

With blockchain technology and its focus on decentralization, transaction finality prevents such fraudulent activities from occurring. Once a transaction has been confirmed on the blockchain through multiple block confirmations (a process where subsequent blocks reference previous blocks' hashes), it becomes practically impossible to alter or manipulate without detection.

Ensuring transaction finality in blockchain technology not only provides trust and security but also establishes a solid foundation for decentralized finance built on distributed ledger technology.

❖ Ensuring Immutability and Tamper-Proof Nature of Transactions

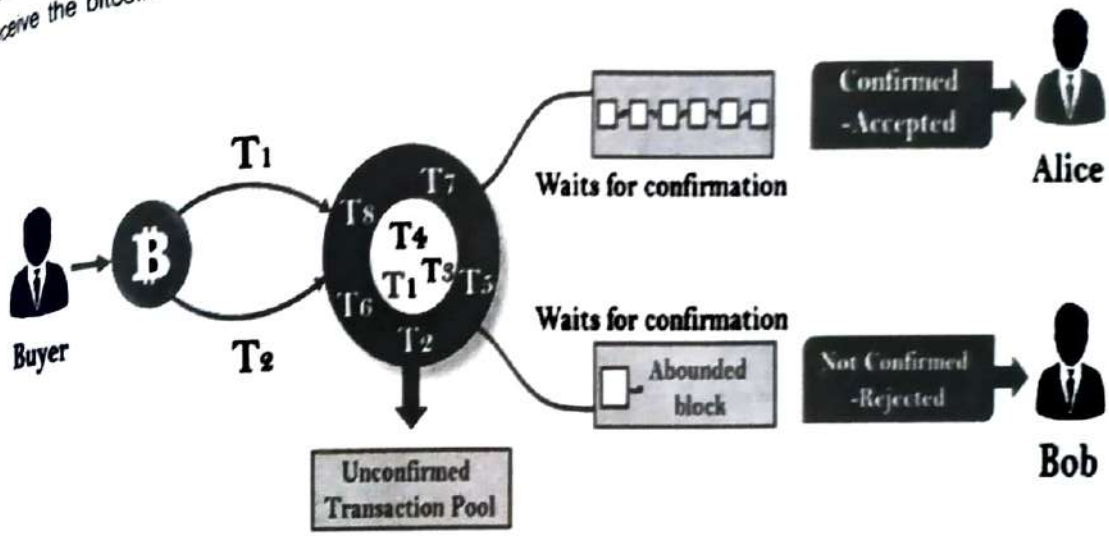
Transaction finality ensures the immutability and tamper-proof nature of transactions on the blockchain. Once a transaction is finalized, it becomes immutable and cannot be altered or reversed.

This ensures that the integrity of the transaction remains intact, providing a high level of trust and security for all parties involved. The use of cryptographic algorithms in blockchain technology further enhances this tamper-proof nature by adding an additional layer of protection to prevent unauthorized changes to transactions.

With transaction finality, participants can have confidence that once a transaction is confirmed, it cannot be revoked or manipulated retroactively. This feature not only safeguards against fraud but also establishes a reliable and transparent system for financial interactions within the cryptocurrency ecosystem.

Double Spending Problem

Let us suppose you have 1 BTC and try to spend it twice. You made the 1 BTC transaction to Alice. Again, you sign and send the same 1 BTC transaction to Bob. Both transactions go into the pool of unconfirmed transactions where many unconfirmed transactions are stored already. The unconfirmed transactions are transactions which do not pick by anyone. Now, whichever transaction first got confirmations and was verified by miners, will be valid. Another transaction which could not get enough confirmations will be pulled out from the network. In this example, transaction T1 is valid, and Alice will receive the bitcoin.



Suppose two different miners will pick both transactions at the same time and start creating a block. Now, when the block is confirmed, both Alice and Bob will wait for confirmation on their transaction. Whichever transaction first got confirmations will be validated first, and another transaction will be pulled out from the network.

Now suppose if both Alice and Bob received the first confirmation at the same time, then there is a race will be started between Alice and Bob. So, whichever transaction gets the maximum number of confirmations from the network will be included in the blockchain, and the other one will be discarded.

Avoiding Double-Spending and Fraud

Transaction finality avoids double-spending and fraud in blockchain technology. With traditional payment systems, there is always a risk that the same amount of money can be spent multiple times, leading to fraudulent transactions.

Transaction finality ensures that once a transaction is recorded on the blockchain ledger, it becomes immutable and cannot be altered or revoked.

This makes it virtually impossible for anyone to create duplicate transactions or manipulate the system for fraudulent purposes. The importance of transaction finality in preventing double-spending and fraud highlights the integrity and security provided by blockchain technology, making it a trusted platform for conducting secure transactions in the digital realm.

The table below shows different blockchains and their average time to finality.

Blockchain	Consensus Algorithm	Average time to mine a block	Average Time to Finality
Bitcoin	PoW	10mins	60mins (6 confirmations)
Ethereum	PoW	15 secs	6 mins (25 confirmations)
Nxt	DPoS	1 min	720 mins (720 blocks)

- **Different Approaches to Achieving Transaction Finality**

Blockchain technology uses different approaches to ensure transaction finality.

1. Probabilistic Finality

Probabilistic finality is one of the oldest types of finality in blockchain. It is achieved when the probability of a transaction being reversed becomes negligible after a certain number of verifications/ confirmations. In a proof-of-work (PoW) blockchain network like Bitcoin, probabilistic finality is achieved when a transaction is included in a block mined and added to the longest chain. As more blocks are added to the chain, the transaction's reversal probability decreases exponentially. However, there is still a very small chance that a chain reorganization could occur, potentially reversing the transaction.

Probabilistic finality in blockchain is also used in proof-of-stake (PoS) and delegated proof-of-stake (DPoS) blockchain networks, where validators stake their tokens as collateral to secure the network and confirm transactions. The higher the number of staked tokens, the higher the level of security and finality achieved.

2. Absolute Finality

Absolute finality is next on our list, which in theory, provides complete and irreversible confirmation of a transaction. In an absolute finality system, once a transaction is recorded on the blockchain, it is considered permanent and cannot be reversed or tampered with.

Some blockchain networks, such as Ripple and Stellar, use consensus algorithms that achieve absolute finality through a process known as federated consensus. A group of trusted validators is responsible for confirming transactions and maintaining the network in a federated consensus system. Once a validator has confirmed a transaction, it is considered final and cannot be reversed. There are

more decentralized networks like Cosmos and Algorand that use consensus algorithms like PBFT and DPoS which is said to help them achieve absolute finality.

Absolute finality in blockchain provides a high level of certainty for transactions while maintaining high security but typically requires high trust in the validators who confirm the transactions.

3. Immediate Finality

Immediate finality or instant finality is a more recently developed phrase, particularly by Shardeum. It is often confused with absolute finality. Immediate finality, in reality, is something that is extremely hard to achieve and would require transformational iterations in the way typical blockchains perform consensus and processes the transactions.

Achieving absolute finality in a public blockchain, at times, require sufficient confirmation by a certain number of subsequent blocks to ensure the transaction's irreversibility. In other cases, a randomly selected validator on a blockchain network proposes a new block and broadcasts it before other participants validate the block in each round of consensus followed by a final round of consensus. While BFT and other recent consensus algorithms can offer faster finality compared to say PoW consensus, they still have a relatively high latency period due to the need for multiple rounds of communication and validation when compared to Shardeum.

4. Economic Finality

Economic finality is the third one on our list where finality is achieved through the network's economic incentives. In a blockchain network that uses economic finality, transactions are confirmed based on the cost of reversing them.

For example, in a PoW blockchain network, an attacker must spend significant resources to reverse a transaction, making it economically infeasible. As a result, economic finality in blockchain provides high security and certainty. However, it is not completely foolproof, as there is still a small chance that an attacker with enough resources could potentially reverse a transaction.

5. Finality in Proof of Work

Most PoW blockchain systems have a property called Longest chain of work, which helps determine consensus.

When miners mine a block, they are always looking to add a block to the longest chain. However, it's entirely possible at any moment in time that there exists more than one chain.

A chain can split into two different forks when two different miners mine a block at the same time. At this moment the active main chain has split into two different forks and it's quite difficult to determine which fork is the valid chain.

In this scenario, both forks will continue to validate blocks and add new blocks. Once one of the chains validates a block before the other chain completes it becomes the longest chain. The longest chain is the one with the longest most valid blocks attached.

The longest chain becomes officially the accepted chain and the transactions mined on the shorter chain are rejected. However, it's possible the transactions rejected on the shorter chain have been included in other blocks on the longest chain.

Example of Attacks that can affect PoW Finality

1. Selfish mining
2. 51% Attack

- **Finality in Proof of Stake(Alternative of proof of work)**

Different PoS based blockchains have different designs for attaining finality. There are multiple implementations of PoS such delegated proof of stake, proof of authority etc. Attaining finality in PoS systems is a major discussion in today PoS blockchain based systems.

For example, Nxt protocol only allows reorganising the last 720 blocks which means that the transactions in (current_block_height - 720) blocks before can be said to be "Final" although transactions with 10 confirmations can be said to be reliable. But still there are still some issues with this design.

Another example is Casper FFG, one of Ethereum implementation of PoS will achieve "Finality" by introducing the notion of "validators", in addition to miners. The validators are responsible for confirming the blockchain at key checkpoints — approximately every 100 blocks. At these checkpoints, once 2/3 of the validators confirm a particular block then it becomes finalized. Once finalized, it will no longer be possible to change any of the blocks before the checkpoint. These checkpoints guarantee that history can never be changed on the blocks proceeding the checkpoint.

Example of Attacks that can affect PoS Finality

1. Nothing at Stake
2. Sybil Attack

- **What Types of Attacks Could Impact Finality in Blockchain Networks ?**

Although consensus algorithms and network protocols used in blockchain networks are largely effective, they are marginally vulnerable to a few attacks that could impact finality. Some of the most common types of attacks are :

1. 51% attack
2. Selfish mining
3. DOS attacks
4. Shard attacks/Cross-shard attacks
5. Timejacking attacks
6. Nothing-at-stake attacks

1. **51% Attack**

A 51% attack (a majority attack) happens when a single entity or group regulates more than 50% of the network's hash rate. This allows the attacker to control the network and prevent other miners from validating transactions. In such a scenario, the attacker could reorganize the blockchain and reverse previously confirmed transactions, undermining finality in blockchain.

2. **Selfish Mining**

Selfish mining is an attack where a miner or group of miners selectively reveal blocks to the network to gain an advantage over other miners. The attacker withholds valid blocks and only reveals them when they have mined additional blocks, which gives them an unfair advantage over other miners. This can lead to different miners having different versions of the blockchain, leading to a fork in the chain and undermining finality.

3. **DOS Attacks**

Here, an attacker overwhelms a particular shard on a sharded chain with a high volume of malicious transactions or requests, leading to a denial of service for legitimate users of that shard. Proof of Stake consensus, rate limiting, maximizing decentralization, horizontal scalability, randomizing, and auto-rotating validators are some of the ways DOS attacks can be prevented.

4. **Shard Attacks/Cross-shard Attacks**

In this case, an attacker gains control over a significant number of shards or exploits the vulnerabilities in the communication between different shards allowing them to manipulate transactions or disrupt the consensus process within those shards. Leaderless consensus, appropriate reputation/consensus mechanisms, gossip protocols, auto-rotating validators after every epoch cycle, and maximizing decentralization are some of the ways that can help prevent shard attacks.

5. **Timejacking Attacks**

Timejacking attacks manipulate the timestamps of blocks to either slow down or speed up the blockchain's progress. By doing so, attackers can disrupt the finality and consensus mechanisms of the network. Networks with low fairness are particularly vulnerable to these attacks.

6. **Nothing-at-stake Attacks**

In a nothing-at-stake attack, validators or miners intentionally create multiple forks or conflicting blocks without incurring any cost. This undermines the finality of transactions as consensus cannot be reached on a single version of the blockchain.

3.3 BLOCK REWARDS AND MINERS AND DIFFICULTY UNDER COMPETITION

- **What Is Bitcoin Mining ?**

Bitcoin mining is the process of validating the information in a blockchain block by generating a cryptographic solution that matches specific criteria. When a correct solution is reached, a reward in the form of bitcoin and fees for the work done is given to the miner(s) who reached the solution first.

Over time, the reward for mining Bitcoin is reduced. This reward process continues until there are 21 million bitcoin circulating. To limit inflation, bitcoin creator Satoshi Nakamoto designed bitcoin to ultimately have only 21 million bitcoins. This is why the size of bitcoin block rewards is halved after the creation of every 210,000 blocks, which takes around four years. Once that number is reached, the bitcoin reward is expected to cease, and Bitcoin miners will be rewarded through fees paid for the work done.

- **Bitcoin Halving and Its Impact on Mining Rewards**

Bitcoin halving is a phenomenon that occurs every four years, which cuts the block reward miners receive in half. This means that the amount of bitcoins produced through mining decreases by 50%.

The most recent Bitcoin halving occurred in May 2020, which reduced the reward from 12.5 to 6.25 BTC per block.

The reduction in mining rewards affects the profitability of mining for smaller operators and can lead to increased consolidation among mining pools. It also leads to an increase in competition, requiring miners to improve their hardware and software optimization strategies if they want to maintain profitability.

Bitcoin halving plays a critical role both economically and technologically within cryptocurrency networks.

- **How Does Bitcoin Mining Work ?**

Here's a simplified example to explain the process. Say you ask friends to guess a number between 1 and 100. Your friends don't have to guess the exact number; they just have to be the first to guess a number less than or equal to your number. If you think of the number 19 and a friend comes up with 21, another 55, and yet another 83, they lose because they all guessed more than 19. But if you have three friends left, and the next one guesses 16, they win, and the others don't get a chance to guess. The one who guessed 16 was the first to guess a number less than or equal to 19.

In this case, the number you chose, 19, represents the target hash the Bitcoin network creates for a block, and the random guesses from your friends are the guesses from the miners.

- **What Is a Block Reward ?**

The bitcoin block reward is made up of two components : newly generated coins and transaction fees. They are given to miners for successfully securing the network by validating blocks.

Bitcoin block rewards are new bitcoins awarded to cryptocurrency miners for being the first to solve a complex math problem and creating a new block of verified bitcoin transactions. The miners use networks of computers to do this, and every time a new block is created it is verified by all the other competing miners. Then a new math problem is introduced and the miners start over. New blocks are added to the blockchain network roughly every 10 minutes.

- **The Role of Miners in the Bitcoin Network**

Miner is an actor who participates in cryptocurrency transactions, and in turn, plays a crucial role both in creating new cryptocurrencies and in verifying transactions on the blockchain. It adds new blocks to the existing chain, and ensures that these additions are accurate.

Miners play a crucial role in the Bitcoin network by verifying transactions and adding them to the blockchain ledger. Essentially, they compete with other miners to solve complex mathematical puzzles that are associated with each transaction.

This process ensures that transactions on the Bitcoin network are secure and verified. Miners act as guardians of the decentralized ledger system, ensuring its integrity through their computational power.

They contribute to maintaining a secure network that is resistant to fraud and hacking attempts while also regulating the circulation of bitcoins in the market through their mining efforts and fees charged for transactions processed.

- **How Bitcoin Mining Works**

Bitcoin mining is the process through which **new bitcoins are produced** and transactions are validated on the Bitcoin network. Here's how it works :

1. Miners compete to solve a mathematical puzzle generated by a transaction.
2. They do this by running specialized software that processes complex calculations to crack the code.
3. The first miner to solve the puzzle gets to add a new block of verified transactions to the blockchain.
4. As a reward, they receive newly generated bitcoins and any transaction fees associated with those transactions.
5. This creates an incentive for miners to continue verifying transactions and adding blocks to the chain, which in turn helps keep the network secure.

Bitcoin mining is essentially a competition among miners to validate transactions and add them to the blockchain in exchange for newly generated coins and fees.

- **What is Mining difficulty ?**

Every blockchain has a mining process by which miners can generate fresh coins. An algorithm regulates how difficult it is for the miners to mine a certain block. This difficulty is known as mining difficulty.

For mining a block, a miner must solve complex mathematical problems by finding a valid hash. As the process progresses, the network adjusts the rate so miners can find valid hashes. Each blockchain has its algorithm to regulate this adjustment. The algorithm increases or decreases the mining difficulty based on the rate at which miners can mine a block.

In recent times, the number of miners has increased manifold. Thus automatically, the mining difficulty of blockchains has also increased. Let's take an example for you to understand better. Bitcoin is a cryptocurrency that has become very popular. As a result, the number of miners on that blockchain has also increased.

The more the number of miners, the more computing power is used in the peer-to-peer network. And as a result, greater is the competition for the limited block rewards. Thus to adjust the rate at which miners can find blocks, the network raises its hash power.

This maintains the time a miner or a mining pool can successfully mine a block. The more the hash power, the more difficult it will be to find valid hashes for a block. Currently, it takes about 10 minutes to mine a Bitcoin block.

After every 2,016 blocks are mined, Bitcoin adjusts its mining difficulty. The difficulty will increase based on the number of miners and their combined hash power.

Benefits of Mining difficulty

Mining difficulty may seem to you as a hindrance on your path to getting block rewards. However, it has its benefits too. They are :

- **Security of the network**

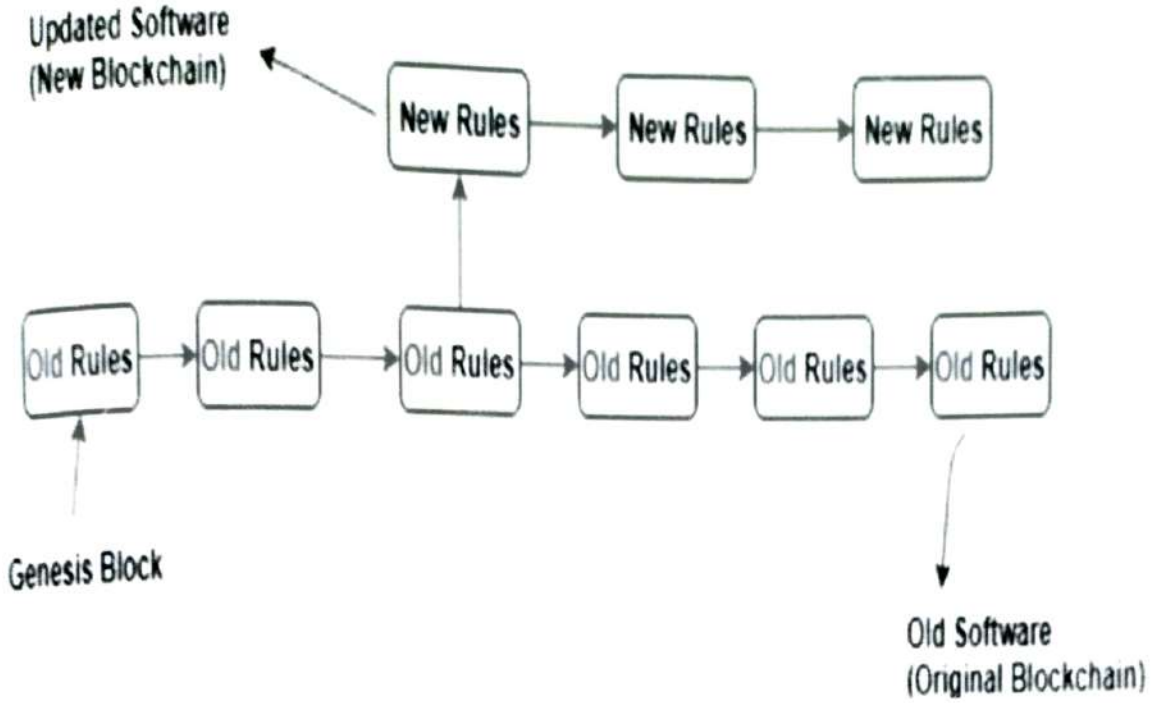
As the mining difficulty increases, it becomes more difficult for a hacker to conduct a malicious attack on the network. Due to the increasing difficulty, miners use special ASIC mining computers that make trillions of guesses each second to find the correct hash for a block. A mining pool has scores of such systems on its floor to conduct the process. Thus, it is very difficult for hackers to get enough computing power for majority control and launch an attack.

- **A steady mining rate**

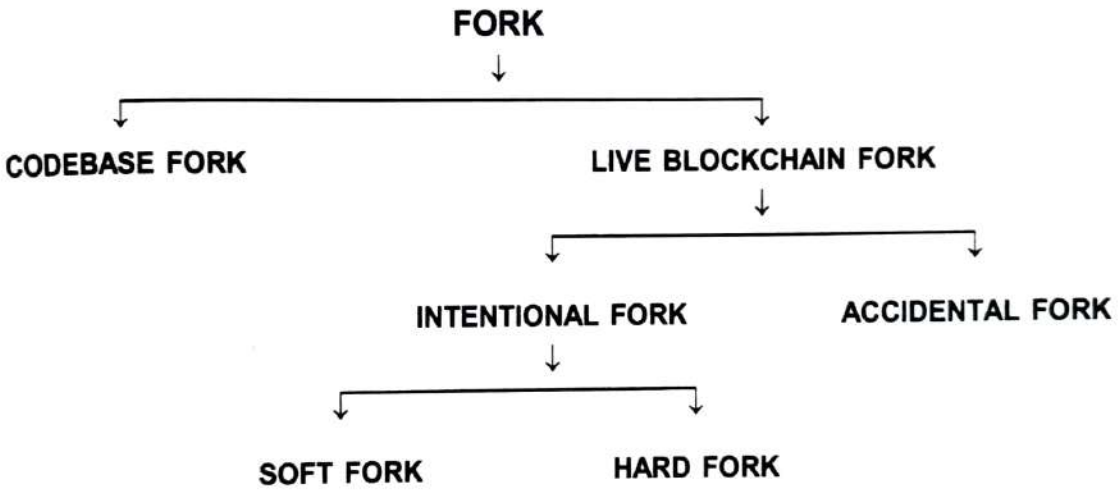
A miner's computing power differs from person to person and pool to pool. Thus to maintain parity in the mining process, the blockchain network raises or lowers its mining difficulty. This ensures that the network is generating blocks at a steady rate.

3.4 FORKS AND CONSENSUS CHAIN

Forks in blockchain means copying the code and modifying it to create a new software or product. In open-source projects Forks are very common and used widely. So, cryptocurrencies like Ethereum and Bitcoin are decentralized and open software so that anyone can contribute. As they are open-sources they rely on their communities to make the software more secure and reliable. Also open source with the help of fork can make user interface more interactive and look good, helping in gaining more users worldwide. In open source the code is visible to everyone, anyone can modify, edit, access there is no copyright claims for such actions.



- **Types of Forks :**



Basically forks are divided into two categories i.e. Codebase Fork and Live Blockchain Fork. And then Live Blockchain Fork is divided into further two parts i.e. Intentional Fork and Accidental Fork, as you can see in the above mentioned figure the Intentional fork is then further divided into two parts i.e. Soft Fork and Hard Fork.

- **Codebase Fork :**

In codebase blockchain fork you can copy the entire code of a particular software. Let us take BITCOIN as an example, so suppose you copied the whole blockchain code and modified it according to your need, say that you decreased the block creation time, made some crucial changes and created a faster software than BITCOIN and publish / launch it has a new whole software named against you, by completing the whole white paper work process. So in these way a new BLOCKCHAIN will be created from an empty blank ledger.

- **Live Blockchain Fork :**

Live Blockchain fork means a running blockchain is been divided further into two parts or two ways. So in live blockchain at a specific page the software is same and from that specific point the chain is divided into two parts. So in context to this fork the Live Blockchain Fork can occur because of two reasons :

- **Accidental Fork / Temporary Fork :**

When multiple miners mine A new block at nearly the same time, the entire network may not agree on the choice of the new block. Some can accept the block mined by one party, leading to a different chain of blocks from that point onward while others can agree on the other alternatives (of blocks) available. Such a situation arises because it takes some finite time for the information to propagate in the entire blockchain network and hence conflicted opinions can exist regarding the chronological order of events.

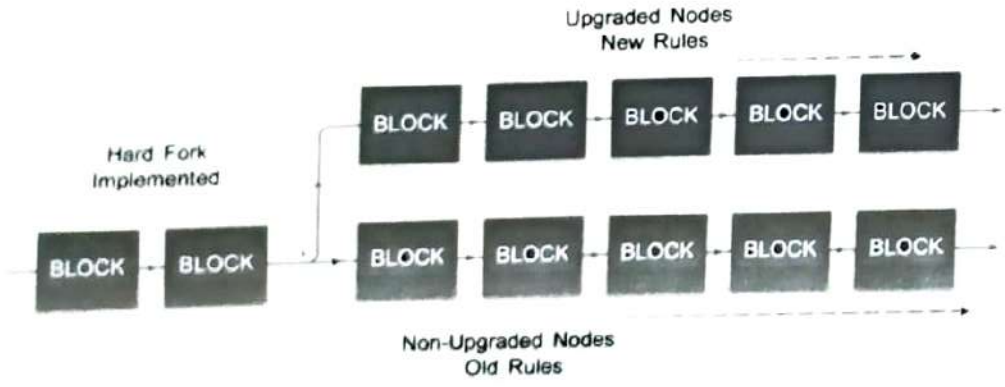
- **Intentional Fork :**

In intentional fork the rules of the blockchain are been changed, knowing the code of the software and by modifying it intentionally. This gives rise to two types of forks which can occur based on the backwards-compatibility of the blockchain protocol and the time instant at which a new block is mined. So Intentional fork can be of two types :

- **Hard Forks :**

A hard fork is a radical change in a cryptocurrency protocol that is incompatible with the previous versions. This means that nodes with the older protocol (pre-fork) aren't able to process transactions or push new blocks to the post-fork (newer) blockchain; similarly, any transaction on the forked (newer) chain is not valid on the older chain. All nodes and miners have to upgrade to the latest version of the protocol if they want to be on the new forked chain.

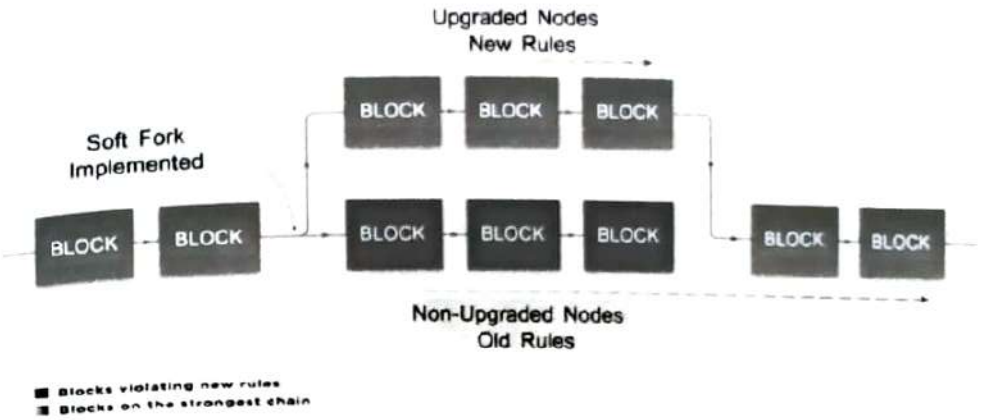
HARD FORK



Soft Forks :

A soft fork is a change in a cryptocurrency protocol that keeps it backward compatible. In essence, non-updated nodes are still able to process transactions and push new blocks to the blockchain, so long as they follow the new protocol rules. This kind of fork requires only a majority of the miners upgrading to adjust to the new rules, as opposed to a hard fork, which requires (almost) all nodes to upgrade and agree on the new version.

SOFT FORK



❖ **Hard Fork VS Soft Fork**

Hard Fork	Soft Fork
A hard fork occurs when a blockchain network splits into two distinct versions, typically because one set of users wants to expand the program's functionality. In contrast, the other wants to maintain the present version.	A soft fork occurs when an update is made to an existing blockchain network for older features to continue functioning properly with the upgraded version.
They are a permanent divergence from the existing blockchain. Thereby forming a different blockchain.	They are minor modifications made to the existing blockchain.
A user on the old blockchain cannot interact with the new blockchain.	Non-upgraded users can enjoy the benefit of the new features as upgraded users.
A dividing community arises from a hard fork because there are always two parties involved.	Security issues arise from soft forks because malicious parties may use them to validate transactions that don't adhere to network requirements.
When a hard fork occurs, new crypto currencies are often the outcome.	No new currency is created as a result of a soft fork.
A hard fork protocol update is backward-incompatible.	A soft fork protocol update is backward-compatible.

❖ **Why do Blockchain Forks Occur?**

As mentioned before, there are several reasons why blockchain forks are needed, namely :

1. Adding New Functionality

A new blockchain fork is created whenever there is an addition needed to the current functionalities of the existing chain.

2. Fixing Security Issues

Blockchains sometimes require certain changes to the code and protocols in place for maximized security, which would require the generation of a blockchain fork.

3. Reverse Transactions

Since a blockchain is mainly a set of codes that can be amended in case of malicious transactions or security breaches, the whole community can reverse all the transactions of a particular period. It leads to the generation of a secondary chain but is an effective security method.

3.5 SYBIL ATTACKS AND THE 51% ATTACK

Sybil Attack

A Sybil Attack is a form of online security violation where an entity has numerous fake identities on a blockchain for malicious reasons. Sybil Attack is a type of attack seen in peer-to-peer networks in which a node in the network operates multiple identities actively at the same time and undermines the authority/power in reputation systems. The main aim of this attack is to gain the majority of influence in the network to carry out illegal(with respect to rules and laws set in the network) actions in the system. A single entity(a computer) has the capability to create and operate multiple identities(user accounts, IP address based accounts). To outside observers, these multiple fake identities appear to be real unique identities.

Formal Model

The model used in the Sybil Attack paper is a simple one. It consists of :

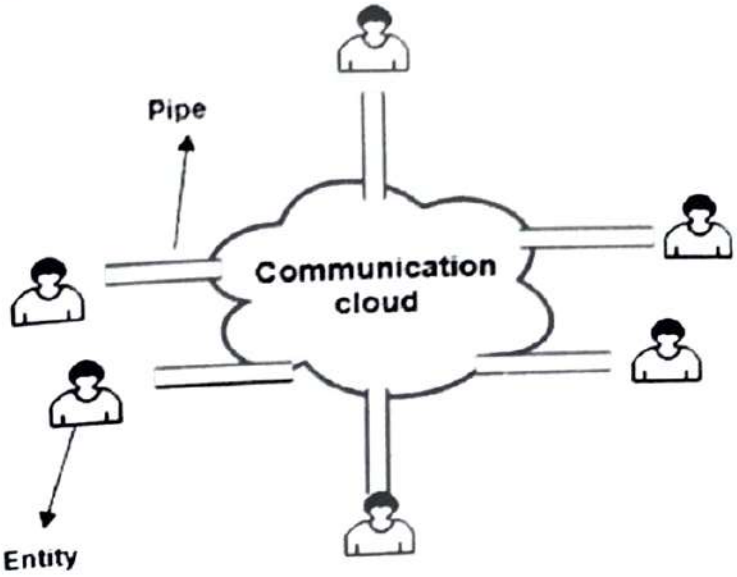
❖ **E entities = c(correct) entities + f(faulty) entities**

correct – entities that follow the protocols and rules setup in the network honestly(whose honesty is verified).

faulty – entities whose behavior are arbitrary and can't be predicted. They don't honestly follow the protocols and rules in the network.

❖ **A communication cloud** : A very general cloud through which messages between different entities travel.

❖ **pipe** : to connect an entity with the communication cloud



Types of sybil attack

- In a direct attack, the honest nodes are influenced directly by the sybil node(s).
- In an indirect attack, the honest node(s) are attacked by a node which communicates directly with the sybil node(s). This middle node is compromised as it's under malicious influence of sybil node(s).

How the Bitcoin network prevents sybil attack ?

Bitcoin network uses the Proof of Work(PoW) consensus algorithm to prove the authenticity of any block that is added to the blockchain. A considerable amount of computing power is required to do the work which provides incentive to the miners to do honest work(a bitcoin reward; currently 12.5 bitcoins for every block mined) and no incentive for the faulty work. The transactions are verified by every node and rejected as invalid if faulty transactions are included in the block. A type of sybil attack, called the 51% attack is also practically impossible in the bitcoin network because of so many miners, it is very difficult for a single organization to control 51% of the miners.

Ways to prevent sybil attack

- **Giving different power to different members**

This is on the basis of reputation systems. Members with different power levels are given different reputation levels.

- **Cost to create an identity**

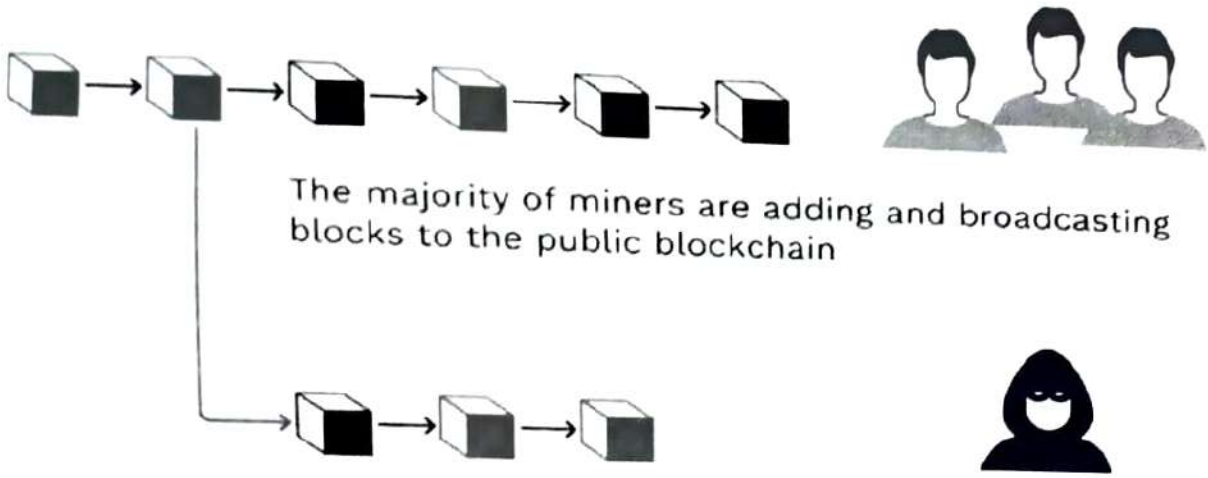
To prevent multiple fake identities in the network, we can put a cost for every identity that aims to join the network. A point to note is that it makes more sense to make it infeasible to operate multiple fake identities at the same time rather than creating new identities. Multiple identities can enforce security, anonymity, censorship prevention.

- **Validation of identities before joining the network**
  - **Direct validation** : An already established member verifies the new joiner of the network
  - **Indirect validation** : An established member verifies some other members who can, in turn, verify other new network joiners. As the members verifying the new joiners are verified and validated by an established entity, the new joiners are trusted to be honest.

❖ **51% Attack**

A 51% attack is an attack on a cryptocurrency blockchain by a group of miners who control more than 50% of the network's mining hash rate(Hash rate is the measure of the computational power of a proof-of-work (PoW) cryptocurrency network, group, or individual. The hash rate is used to determine the mining difficulty of a blockchain network and can be used as a gauge of securityHash rates are measured by the number of guesses each mining computer makes per second to solve for the hash on a blockchain network). Owning 51% of the nodes on the network theoretically gives the controlling parties the power to alter the blockchain.

The attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users. They would also be able to reverse transactions that were completed while they were in control. Reversing transactions could allow them to double-spend coins, one of the issues consensus mechanisms like proof-of-work were created to prevent.



The majority of miners are adding and broadcasting blocks to the public blockchain

An attacker is adding blocks to a private blockchain and not broadcasting them to the public blockchain

❖ **How Does A 51% Attack Work ?**

General sequence of events that typically characterizes such an attack :

1. Accumulate Power :

The first step involves the attacker accumulating more than half (51%) of the network's computational or hashing power. This could be accomplished by acquiring substantial hardware resources or convincing a large number of miners to join a pool under the attacker's control.

2. **Partitioning :**

The attacker, now commanding a majority of the network's hashing power, effectively segregates their group from the main network while still maintaining internal communication. Despite this separation, the hacking group proceeds with mining operations but refrains from sharing their progress with the primary network or receiving updates from it. Consequently, two parallel versions of the blockchain start evolving independently.

3. **Fast-Paced Mining :**

Due to their superior hashing power, the attacker's group is able to add blocks to their version of the blockchain faster than the rest of the network. Over time, the difference in length between the two versions of the chain becomes statistically proportional to the difference in hashing power between the two groups.

4. **Reintegration and Dominance :**

Once the hacking group rejoins the network, the two competing versions of the blockchain propagate through the entire network. According to the consensus protocol's rules, the nodes keep the longest blockchain, and the shorter one is discarded. This means all the blocks added by the main network during the separation period get orphaned, and their transactions are released back into the Mempool.

5. **Potential Threats :**

Upon successful execution, a 51% attack can open Pandora's box of threats that can significantly impact a blockchain network and its participants. These threats range from financial fraud in the form of double-spending to outright denial of service attacks that paralyze network functionality.

❖ Risks And Consequences Of A 51% Attack

A successful attack can have significant implications for a blockchain network and its users. Here's what happens :

- **Double-Spending** : This is the most feared consequence. The attacker could spend their money twice — first, they perform a regular transaction and then change the blockchain to show they never used the money at all.
- **Denial-of-Service (DoS) Attack** : The hacker takes over and blocks the addresses of other miners for a while. This stops the good guys – the honest miners – from getting back control of the network. As a result, the attacker's false chain of transactions can become permanent.
- **Transaction Reversal** : The attacker can block payments between some or all users. This disrupts the normal operation of the network and can lead to significant delays in transaction confirmations, undermining confidence in the network's reliability.
- **Damage to Reputation** : Also, the attack can severely damage a blockchain's reputation. This can lead to a loss of trust among current and potential users, resulting in a significant drop in the value of the associated cryptocurrency and deterring new users or investors from joining the network.

❖ Prevention Of 51% Attacks

Mitigating these risks can be challenging, but various methods have been proposed :

- **Change Of Consensus Algorithm**

Switching to a different consensus algorithm serves as a viable approach in reducing the likelihood of 51% attacks. Proof of Work (PoW), the initial consensus mechanism employed by many blockchains, renders itself susceptible to such attacks due to its mining concentration risk.

Alternatively, the Proof of Stake (PoS) consensus mechanism is less prone to such attacks as it requires a hacker to possess the majority of the blockchain's total stake, often a prohibitively expensive venture.

- **Delaying Blockchain Confirmations**

Another effective deterrent involves delaying blockchain confirmations. This method buys time for the network to detect and potentially ward off a 51% attack. By extending the transaction confirmation time, attackers would need to sustain control over 51% of the network for a more extended period, dramatically increasing the cost and difficulty of such an attack.

- **Penalty System**

Instituting a penalty system serves as another viable defensive strategy. For instance, the application of slashing conditions in PoS blockchains penalizes malicious actors by confiscating a portion or all of their staked tokens if they are found to be acting against the network's rules. This punitive measure significantly raises the stakes for any would-be attackers and can serve as a potent deterrent.

- **Blockchain Protocol Audit**

Lastly, regular blockchain protocol audits are a crucial aspect of any comprehensive security strategy. These audits meticulously scrutinize the protocol to detect vulnerabilities, including potential avenues for a 51% attack. By identifying and addressing these weaknesses proactively, blockchain developers can considerably reinforce their network's defenses.

Exercises

❑ MCQs :

1. The alternatives to POW are _____ .

   A. Delegated Proof Of Stake B. Proof of stake

   C. Both A and B D. None of the above

2. The term used for a blockchain splits is _____ .

   A. A division B. A merger C. A fork D. None of the above

3. Proof of Stake is _____ .

   A. A transaction and block verification protocol

   B. A certificate needed to use the blockchain

   C. All of the above

   D. None of the above

4. The process of creating new bitcoins is known as _____
   A. Sourcing B. Financing C. Mining D. None of the above
5. The maximum number of bitcoins that can be created is _____
   A. 21 million B. 25 million C. 11 million D. 100 million
6. The maximum number of bitcoins that can be created is _____
   A. 21 million B. 25 million C. 11 million D. 100 million
7. _____ is used for storing bitcoins.
   A. Wallet B. Block C. All of above D. None of above
8. The process of creating new bitcoins is known as _____
   A. Sourcing B. Financing C. Mining D. None of the above
9. What is a genesis block?
   A. The first block of a Blockchain
   B. A famous block that hard coded a hash of the Book of Genesis onto the blockchain
   C. The first block after each block halving
   D. The 2nd transaction of a Blockchain
10. What was the first use of blockchain?
    A. Bitcoin B. Ethereum C. Ripple D. Tether

Questions :

1. What is Transaction Finality ?
2. Differentiate : Consensus Vs Finality
3. What is Confirmation in Terms of Transaction Finality ?
4. How is Finality Achieved in Blockchain Protocols ?
5. What is the Importance of Finality in the World of Blockchain ?
6. What is Wallet ?
7. Why is Forking Needed in Blockchain ?
8. Differentiate soft and hard fork.
9. What is a 51% attack ?
10. Differentiate Proof-of-work v/s Proof-of-stake protocol.
11. What is Consensus algorithm ? What are the types of consensus algorithms ?

***

UNIT
4

CONCEPTUALIZATION OF BLOCKCHAIN AS CRYPTOCURRENCY

4.1 Bitcoin : Merkle tree and bitcoin.

4.2 Bitcoin and the Eventual Consistency, Byzantine fault tolerance.

4.3 Bitcoin and secure hashing, bitcoin block-size, bitcoin mining.

4.4 Proof of Work, Bitcoin Scripting.

4.5 Blockchain collaborative implementations: Hyper ledger, corda- ERC 20 and token.

4.1 BITCOIN : MERKLE TREE AND BITCOIN

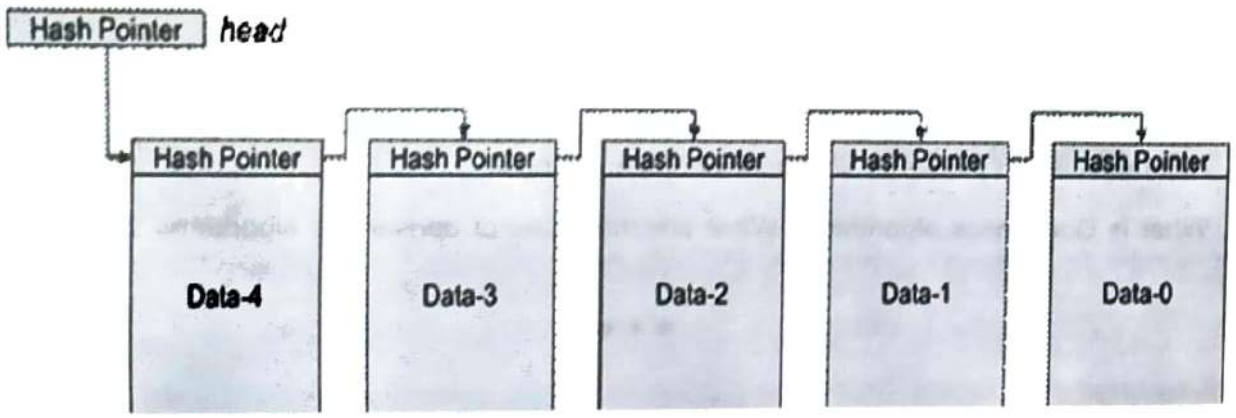
Before we jump into Bitcoin, we will introduce two storage structures that Bitcoin uses: blockchain and Merkle trees. Both are built using hash pointers.

❖ Hash Pointers

A cryptographic hash serves as a checksum for a message. If a message has been modified, it will yield a different hash. By associating a hash with a message, we have a basis for managing the integrity of that message: being able to detect if the message gets changed.

One way of associating a hash with a message is with the use of hash pointers. Pointers are used in data structures to allow one data element to refer to another. In processes, a pointer is a memory location. In distributed systems, a pointer may be a name or IP address of a computer and object identifier. A hash pointer is a tuple that contains a traditional pointer along with the hash of the data element that is being pointed to. It allows us to validate that the information being pointed to has not been modified.

❖ Tamper-resistant linked-lists : Blockchain



The same structures that use pointers can be adapted to use hash pointers to create tamper-evident structures. For example, a linked list can be constructed with each element containing a hash pointer to the next element instead of a pointer.

Adding a new block is easy. You allocate the block, copy the head hash pointer into it (the next pointer), and update the head hash pointer to point to the new block and contain a hash of that block.

If an adversary modifies, say, data block 1, we can detect that. The hash pointer in Data-2 will point to Data-1 but the hash of Data-1 will no longer match the hash in the pointer. For a successful attack, the adversary will also need to modify the hash value in the hash pointer in block 2. That will make the hash pointer in block 3 invalid, so that will need to be changed. The adversary will need to change all the hash pointers leading up to the head of the list. If we're holding on to the head of the list (e.g., in a variable or some trusted storage) so that the adversary cannot modify it, then we will always be able to detect tampering. A linked list using hash pointers is called a blockchain.

◆ What Is a 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 referred to as "binary hash trees."

A Merkle tree is a data structure that is used in computer science applications. In bitcoin and other cryptocurrencies , Merkle trees serve to encode blockchain data more efficiently and securely.

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 ?

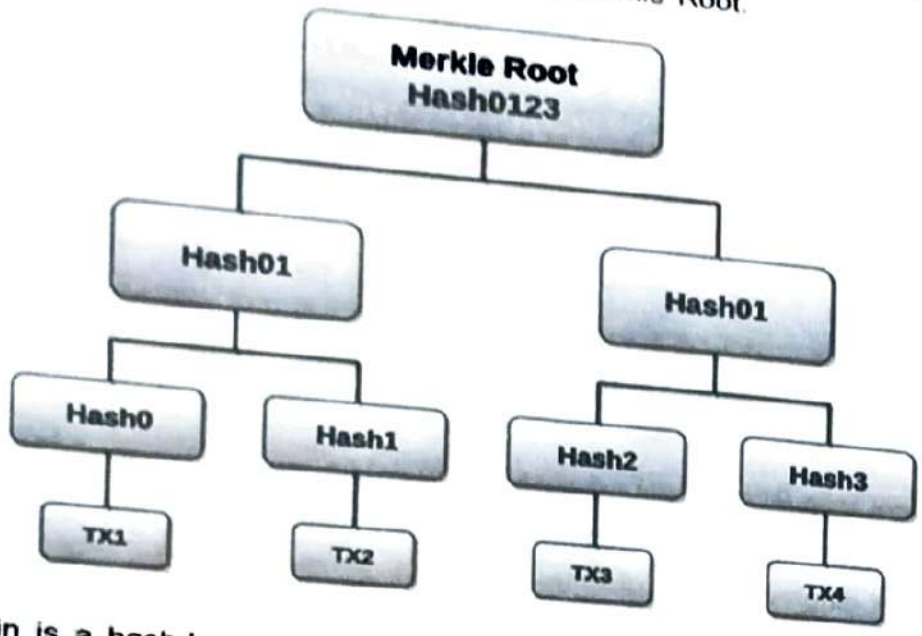
A Merkle tree stores all the transactions in a block by producing a digital fingerprint of the entire set of transactions. It allows the user to verify whether a transaction can be included in a block or not.

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,

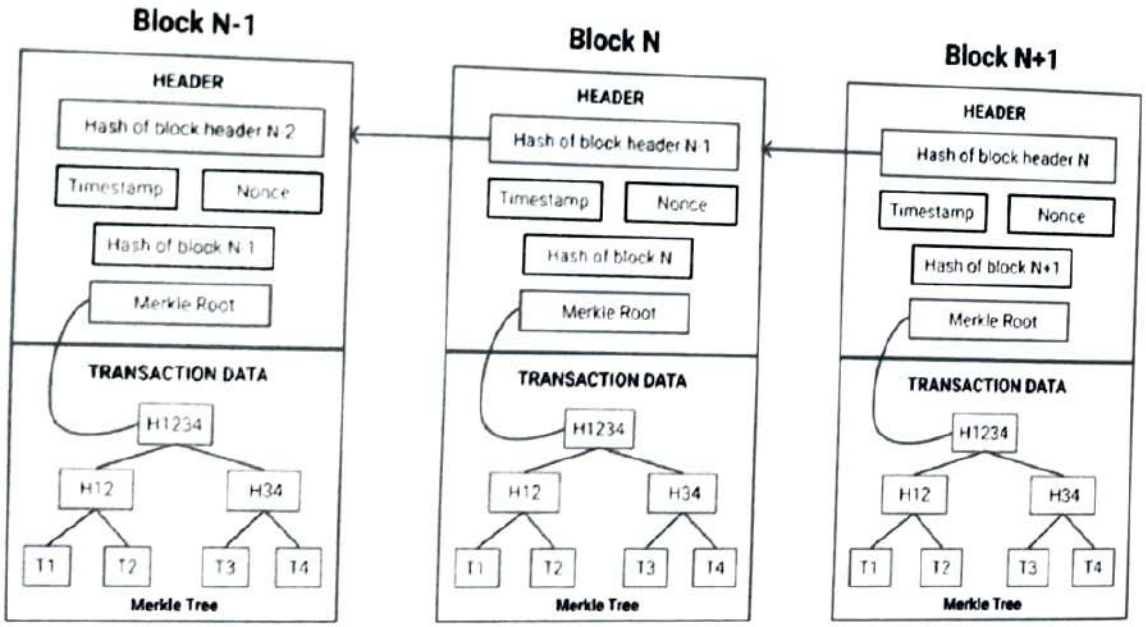
and separately hashing Hash2 and Hash3, resulting in Hash23. The two hashes (Hash01 and Hash23) are then hashed again to produce the Root Hash or the Merkle Root.



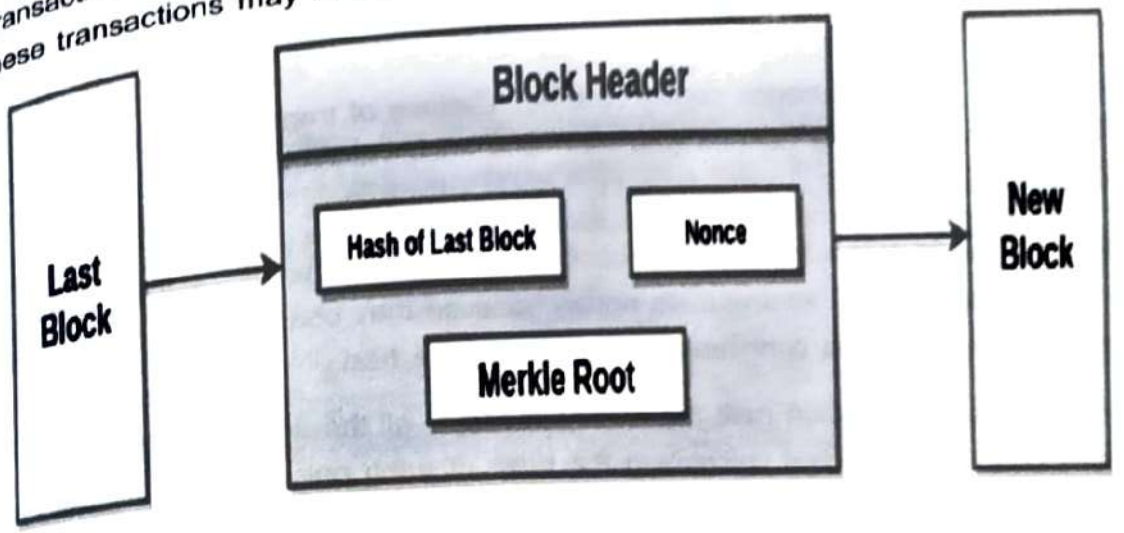
The blockchain is a hash-based linked list of blocks, where each block consists of a header and transactions. The transactions are arranged in a tree-like fashion, known as the Merkle tree.

❖ **What Is a Merkle Root?**

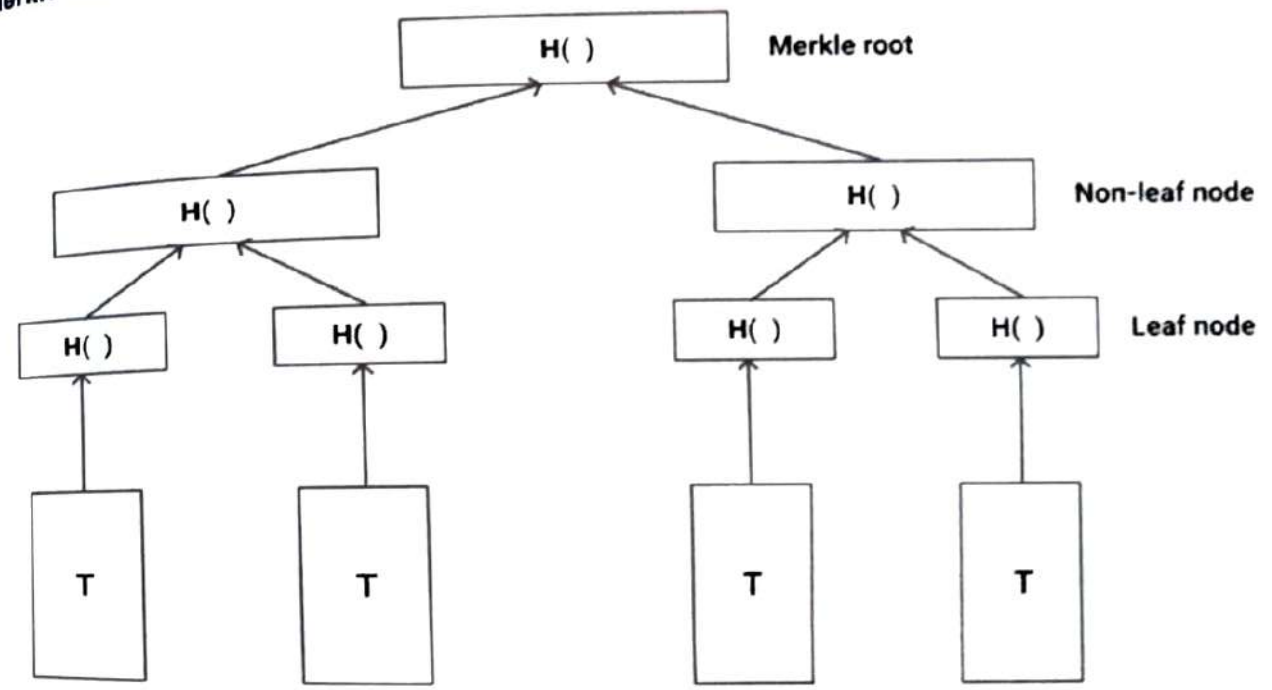
- A Merkle root is a simple mathematical method for confirming the facts on a Merkle tree.
- They're used in crypto currency to ensure that data blocks sent through a peer-to-peer network are whole, undamaged, and unaltered.
- They play a very crucial role in the computation required to keep crypto currencies like bitcoin and ether running.



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.



- **Merkle Tree Structure**



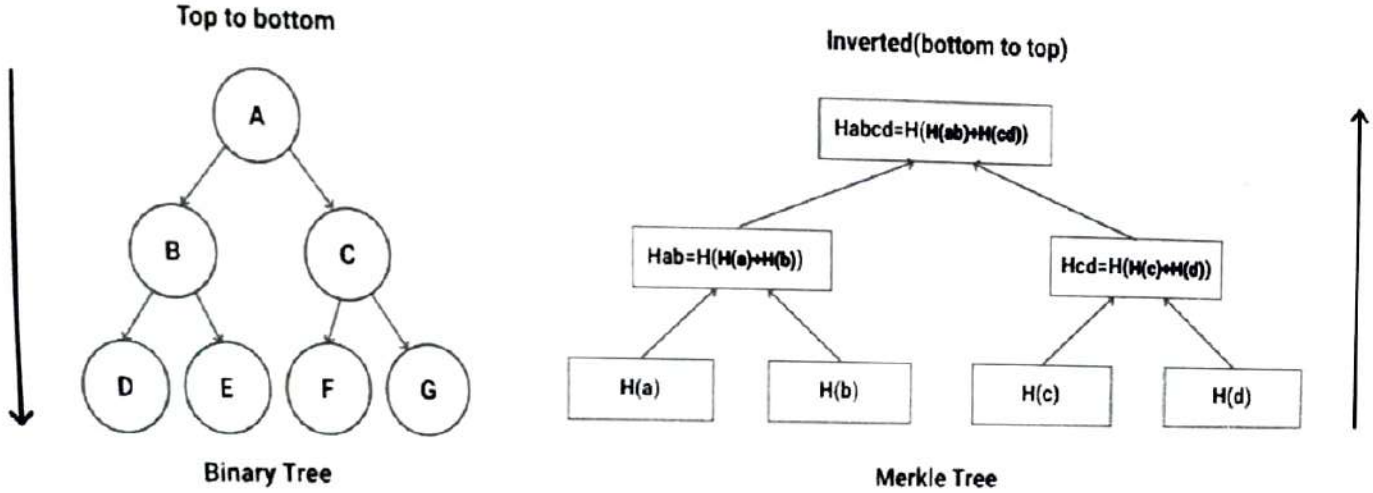
H( ) : Hash value
T : transaction

1. A blockchain can potentially have thousands of blocks with thousands of transactions in each block. Therefore, memory space and computing power are two main challenges.
2. It would be optimal to use as little data as possible for verifying transactions, which can reduce CPU processing and provide better security, and this is exactly what Merkle trees offer.

3. In a Merkle tree, transactions are grouped into pairs. The hash is computed for each pair and this is stored in the parent node. Now the parent nodes are grouped into pairs and their hash is stored one level up in the tree. This continues till the root of the tree. The different types of nodes in a Merkle tree are:

   - **Root node** : The root of the Merkle tree is known as the Merkle root and this Merkle root is stored in the header of the block.
   - **Leaf node** : The leaf nodes contain the hash values of transaction data. Each transaction in the block has its data hashed and then this hash value (also known as transaction ID) is stored in leaf nodes.
   - **Non-leaf node** : The non-leaf nodes contain the hash value of their respective children. These are also called intermediate nodes because they contain the intermediate hash values and the hash process continues till the root of the tree.

- A Merkle tree is constructed from the leaf nodes level all the way up to the Merkle root level by grouping nodes in pairs and calculating the hash of each pair of nodes in that particular level. This hash value is propagated to the next level. This is a **bottom-to-up** type of construction where the hash values are flowing from down to up direction.
- Hence, by comparing the Merkle tree structure to a regular binary tree data structure, one can observe that Merkle trees are actually **inverted down**.



Binary tree direction vs Merkle tree direction

Example : Consider a block having 4 transactions- T1, T2, T3, T4. These four transactions have to be stored in the Merkle tree and this is done by the following steps-

Step 1 : The hash of each transaction is computed.

H1 = Hash(T1).

Step 2 : The hashes computed are stored in leaf nodes of the Merkle tree.

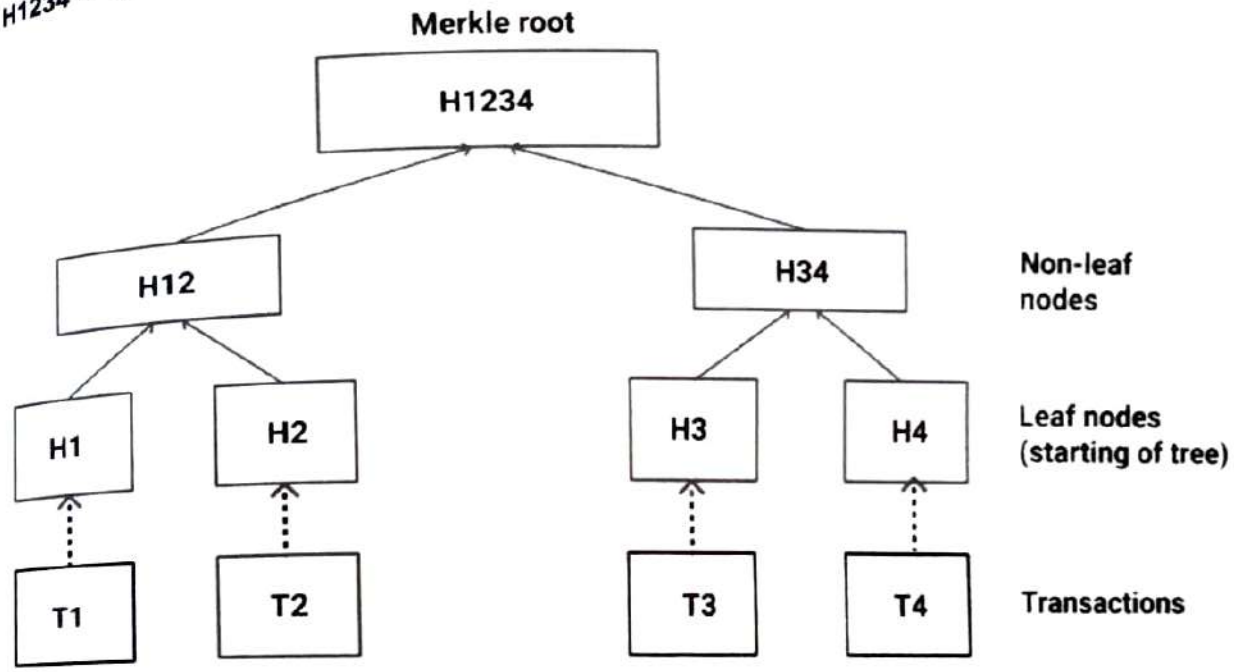
Step 3 : Now non-leaf nodes will be formed. In order to form these nodes, leaf nodes will be paired together from left to right, and the hash of these pairs will be calculated. Firstly hash of H1 and H2 will be computed to form H12. Similarly, H34 is computed. Values H12 and H34 are parent nodes of H1, H2, and H3, H4 respectively. These are non-leaf nodes.

H12 = Hash(H1 + H2)

H34 = Hash(H3 + H4)

Step 4 : Finally H1234 is computed by pairing H12 and H34. H1234 is the only hash remaining. This means we have reached the root node and therefore H1234 is the Merkle root.

H1234 = Hash(H12 + H34)



Merkle tree works by hashing child nodes again and again till only one hash remains.

Key Points :

- In order to check whether the transaction has tampered with the tree, there is only a need to remember the root of the tree.
- One can access the transactions by traversing through the hash pointers and if any content has been changed in the transaction, this will reflect on the hash stored in the parent node, which in turn would affect the hash in the upper-level node and so on until the root is reached.
- Hence the root of the Merkle tree has also changed. So Merkle root which is stored in the block header makes transactions tamper-proof and validates the integrity of data.
- With the help of the Merkle root, the Merkle tree helps in eliminating duplicate or false transactions in a block.

- It generates a digital fingerprint of all transactions in a block and the Merkle root in the header is further protected by the hash of the block header stored in the next block.

❖ **Why Merkle Trees are Important For Blockchain?**

- In a centralized network, data can be accessed from one single copy. This means that nodes do not have to take the responsibility of storing their own copies of data and data can be retrieved quickly.
- However, the situation is not so simple in a distributed system.
- Let us consider a scenario where blockchain does not have Merkle trees. In this case, every node in the network will have to keep a record of every single transaction that has occurred because there is no central copy of the information.
- This means that a huge amount of information will have to be stored on every node and every node will have its own copy of the ledger. If a node wants to validate a past transaction, requests will have to be sent to all nodes, requesting their copy of the ledger. Then the user will have to compare its own copy with the copies obtained from several nodes.
- Any mismatch could compromise the security of the blockchain. Further on, such verification requests will require huge amounts of data to be sent over the network, and the computer performing this verification will need a lot of processing power for comparing different versions of ledgers.
- Without the Merkle tree, the data itself has to be transferred all over the network for verification.
- Merkle trees allow comparison and verification of transactions with viable computational power and bandwidth. Only a small amount of information needs to be sent, hence compensating for the huge volumes of ledger data that had to be exchanged previously.

❖ **Benefits of Merkle Tree in Blockchain**

Merkle trees provide four significant advantages -

- Validate the data's integrity: It can be used to validate the data's integrity effectively.
- Takes little disk space: Compared to other data structures, the Merkle tree takes up very little disk space.
- Tiny information across networks: Merkle trees can be broken down into small pieces of data for verification.
- Efficient Verification: The data format is efficient, and verifying the data's integrity takes only a few moments.

4.2 BITCOIN AND THE EVENTUAL CONSISTENCY, BYZANTINE FAULT TOLERANCE

Bitcoin and the Eventual Consistency

Bitcoin operates on a decentralized and distributed ledger technology called blockchain. The concept of eventual consistency, however, is more commonly associated with distributed databases. Let's explore both concepts and see how they relate.

1. **Bitcoin :**
   - Decentralization: Bitcoin is a decentralized crypto currency, meaning there is no central authority or entity controlling it. Instead, a network of nodes (computers) maintains a shared ledger through a consensus mechanism called proof-of-work.
   - Consistency in Bitcoin: Bitcoin's blockchain achieves a form of consistency through its consensus algorithm. Nodes in the network agree on the state of the ledger, and transactions are added to the blockchain in a sequential and consistent manner through the mining process.

2. **Eventual Consistency**:
   - Distributed Databases: Eventual consistency is a concept often associated with distributed databases. In a distributed system, data is spread across multiple nodes, and each node can accept and process updates independently.
   - Consistency Models:
   - Strong Consistency: In a strongly consistent system, all nodes see the same data at the same time. However, achieving strong consistency in a distributed system can come at the cost of increased latency and reduced availability, as all nodes must agree before returning a result.
   - Eventual Consistency: Instead of enforcing immediate consistency, eventual consistency allows nodes to have different views of the data at any given time. However, given enough time and no further updates, all nodes will eventually converge to the same state.

3. **Relation :**
   - While Bitcoin doesn't explicitly adhere to the concept of eventual consistency as defined in distributed databases, there are some parallels.
   - Bitcoin achieves consensus through a probabilistic process (proof-of-work), and over time, all nodes in the network converge to the same blockchain state.
   - The eventual consistency in Bitcoin is a result of the decentralized consensus mechanism rather than a deliberate design choice for distributed database systems.

In summary, while Bitcoin and eventual consistency are not directly aligned concepts, the decentralized nature and consensus mechanism of Bitcoin contribute to a form of eventual consistency over time as all nodes in the network converge to a consistent state of the blockchain.

Bitcoin, as a decentralized and distributed cryptocurrency, operates on the principles of consensus and eventual consistency. Here's how eventual consistency evident in the context of Bitcoin:

1. **Decentralized Consensus :**
   - Bitcoin relies on a decentralized network of nodes that maintain a shared ledger called the blockchain.
   - Nodes in the network reach consensus on the state of the ledger through a process known as proof-of-work. Miners compete to solve complex mathematical problems, and the first one to solve it gets the right to add a new block of transactions to the blockchain.
2. **Probabilistic Consensus :**
   - Bitcoin's consensus is probabilistic. It means that, at any given moment, different nodes in the network may have slightly different views of the blockchain.
   - However, as more blocks are added to the chain and more proof-of-work is expended, the probability of consensus among nodes increases.
3. **Block Finality :**
   - While transactions are considered "confirmed" once included in a block, the concept of finality in Bitcoin is probabilistic. It's possible that a block could be orphaned if another miner discovers a competing block around the same time.
   - As more blocks get added to the blockchain after a particular block, the probability of that block being part of the accepted, irreversible history increases.
4. **Longest Chain Rule:**
   - Bitcoin follows the principle of the longest chain rule. In case of conflicting blocks, nodes generally adopt the longest valid blockchain as the correct one.
   - This rule ensures that, over time, the entire network converges to a single valid blockchain, providing a form of eventual consistency.
5. **Network Latency :**
   - Due to network latency and the time it takes for information to propagate across the decentralized network, different nodes might temporarily have different views of the blockchain.
   - However, as nodes receive updated information and reach consensus, eventual consistency is achieved.

While the term "eventual consistency" is more commonly associated with distributed databases, the principles of decentralized consensus in Bitcoin result in a similar outcome over time. The probabilistic nature of block confirmation and the adherence to the longest chain rule contribute to the eventual convergence of the entire network to a consistent state of the blockchain.

❖ **Byzantine fault tolerance**

Byzantine Fault Tolerance is a property of a distributed system that allows it to function correctly even if some of the nodes in the network are faulty or malicious. A Byzantine failure is a failure in which a node in a distributed system provides incorrect or misleading information to other nodes.

In a Byzantine failure, it is not possible to distinguish between faulty nodes and nodes that are providing correct information. BFT algorithms are designed to tolerate Byzantine failures by ensuring that the system can reach consensus even if some nodes are providing incorrect information.

BFT algorithms work by dividing nodes in the network into groups and requiring them to exchange messages with each other. By exchanging messages, nodes can validate the information being provided by other nodes and ensure that all nodes agree on the current state of the system. There are several BFT algorithms that are commonly used in blockchain technology, including Practical Byzantine Fault Tolerance (PBFT), Federated Byzantine Agreement (FBA), and others.

❖ **Classic Byzantine Generals Problem**

The classic Byzantine Generals Problem is a well-known problem in distributed systems that illustrate the challenges of achieving consensus in a network with faulty or malicious nodes. The problem is as follows: a group of Byzantine generals are surrounding a city and must coordinate their attack. The generals can only communicate with each other through messengers, and some of the messengers may be traitors who will send false information to the other generals.

In this scenario, the generals must agree on a plan of attack, but they cannot trust the information being provided by their messengers. If too many messengers are traitors, the generals may not be able to coordinate their attack effectively, and the attack may fail.

This problem is similar to the challenges faced by blockchain networks, where nodes must agree on the current state of the network, but some nodes may be faulty or malicious.

❖ **Practical Byzantine Fault Tolerance (PBFT)**

Practical Byzantine Fault Tolerance (PBFT) is one of the most well-known BFT algorithms used in blockchain technology. PBFT is designed to be fast and efficient while still providing strong Byzantine Fault Tolerance. In PBFT, nodes are divided into three groups: a leader node, a set of replica nodes, and a set of client nodes.

The leader node is responsible for proposing new transactions or blocks to the network. The replica nodes are responsible for validating the proposal by exchanging messages with each other. If two-thirds of the replica nodes agree on the proposal, it is considered to be validated, and the leader node adds it to the blockchain.

PBFT ensures that all nodes in the network have a copy of the blockchain and can validate new transactions and blocks before they are added to the blockchain.

One of the main advantages of PBFT is that it provides strong Byzantine Fault Tolerance, meaning that it can tolerate a large number of faulty or malicious nodes. Additionally, PBFT is relatively fast

compared to other consensus algorithms, as it requires only a few rounds of communication between nodes before consensus can be reached.

Drawbacks of PBFT

Despite its many advantages, PBFT has several limitations. One of the main drawbacks of PBFT is that it requires a high level of network connectivity between nodes. If nodes are not able to communicate with each other quickly and reliably, consensus may not be reached, and the network may become fragmented.

Additionally, PBFT is not well-suited for networks with a large number of nodes, as the number of messages required to reach consensus increases exponentially as the number of nodes in the network grows.

- **Federated Byzantine Agreement (FBA)**

Federated Byzantine Agreement (FBA) is a BFT algorithm that is designed to be more flexible and scalable than PBFT. FBA is based on the idea of federating groups of nodes into smaller sub-networks, each with its own consensus mechanism. Nodes in a sub-network communicate with each other to reach consensus on the state of the network, and then the sub-networks communicate with each other to agree on a global state.

FBA is designed to be more flexible than PBFT because it allows nodes to choose which sub-networks they want to join.

Nodes can choose to join multiple sub-networks or only one, depending on their needs and resources.

Additionally, FBA is designed to be more scalable than PBFT because it does not require all nodes to communicate with each other directly. Instead, nodes communicate with a subset of other nodes, reducing the amount of communication required to reach consensus.

Limitations of FBA

While FBA has many advantages over PBFT, it also has some limitations. One of the main limitations of FBA is that it is more complex than PBFT, as it requires nodes to manage multiple sub-networks and consensus mechanisms. This can make it more difficult to implement and maintain, particularly for smaller networks with limited resources.

Additionally, FBA is still a relatively new technology, and there is limited real-world experience with using it in large-scale blockchain networks. As a result, it is not yet clear how well FBA will perform in practice, particularly in networks with a large number of nodes or in networks with high levels of network congestion.

Comparison of PBFT and FBA

Feature	PBFT	FBA
Number of Nodes	Fewer nodes(<1000)	Larger number of nodes
Network Connectivity	High network connectivity	Moderate network connectivity
Scalability	Limited scalability	More scalable
Complexity	Less complex	More complex
Fault Tolerance	Strong Byzantine Fault Tolerance	Moderate Byzantine Fault Tolerance

Applications :

- Byzantine Fault Tolerance is particularly important in blockchain and crypto currency systems, where achieving consensus among distributed nodes is essential for the security and reliability of the network.

Challenges:

- Achieving Byzantine Fault Tolerance involves addressing challenges such as network latency, the potential for collusion among faulty nodes, and the efficiency of the consensus algorithm.

Byzantine Fault Tolerance is a crucial concept in distributed systems, providing mechanisms to ensure that nodes can reach a consensus even in the presence of faulty or malicious participants. This is particularly relevant in the context of blockchain and crypto currency networks where trustless and decentralized operation is a fundamental goal.

4.3 BITCOIN AND SECURE HASHING, BITCOIN BLOCK-SIZE, BITCOIN MINING

What Is a Hash ?

A hash is a mathematical function that converts an input of arbitrary length into an encrypted output of a fixed length. Thus, regardless of the original amount of data or file size involved, its unique hash will always be the same size. Moreover, hashes cannot be used to "reverse-engineer" the input from the hashed output since hash functions are "one-way" (like a meat grinder; you can't put the ground beef back into a steak). Still, if you use such a function on the same data, its hash will be identical, so you can validate that the data is the same (i.e., unaltered) if you already know its hash.

Hashing is also essential to blockchain management in cryptocurrency.

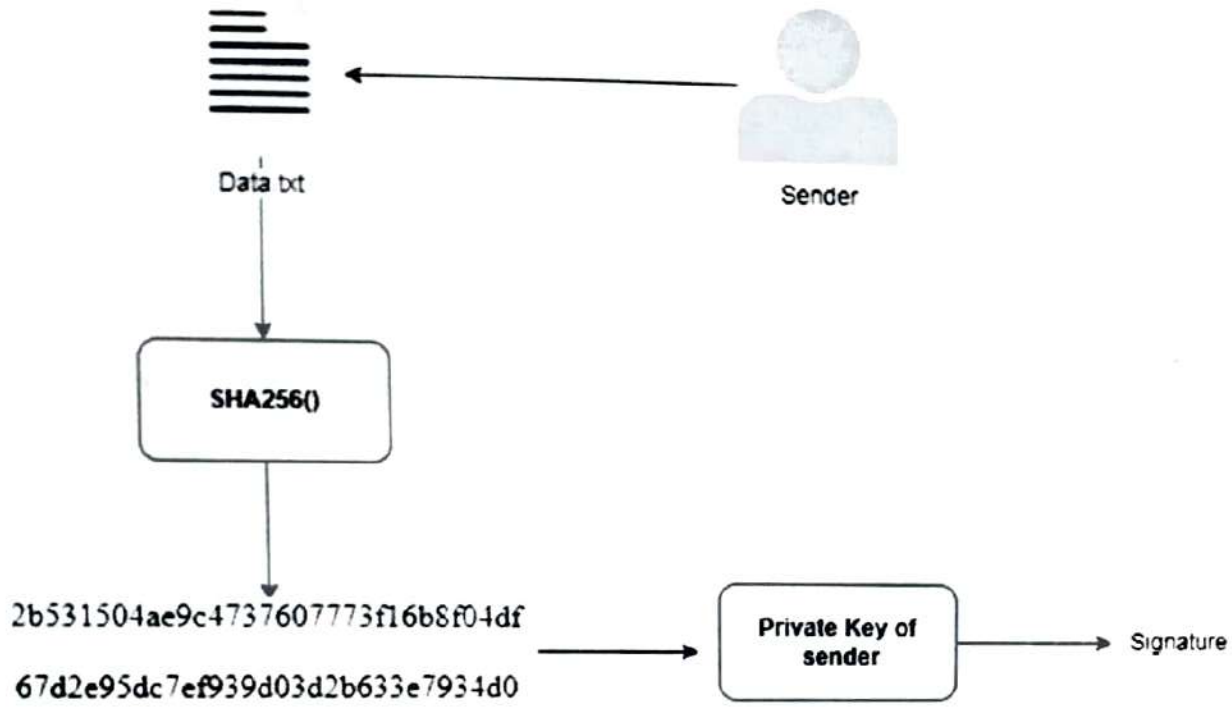
What is SHA-256 ?

A secure hashing algorithm or commonly referred to as SHA-256, is an unkeyed cryptographic hashing function that takes an input of variable length and produces a 256-bit long hash output.

❖ Uses of SHA-256 in blockchain

SHA-256 is one of the first and most prominently used hashing algorithms in blockchains like Bitcoin, Bitcoin Cash, and Bitcoin SV. SHA-256 is used in various stages in a blockchain, most prominently:

- Consensus mechanism : Miners calculate the hash of new blocks to be created using SHA-256 by varying the value of nonce in a bitcoin block until they reach the hash below the threshold. Then that block can be accepted into the ledger.
- Chains of blocks : Each block in the ledger contains a hash generated by SHA-256 referring to the preceding block in the chain.
- Digital signatures : Transactions use digital signatures to maintain integrity, the information used in the transaction is hashed using SHA-256, and then it is encrypted with the sender's private key to generate a signature. The miner then verifies this signature to validate the transaction.



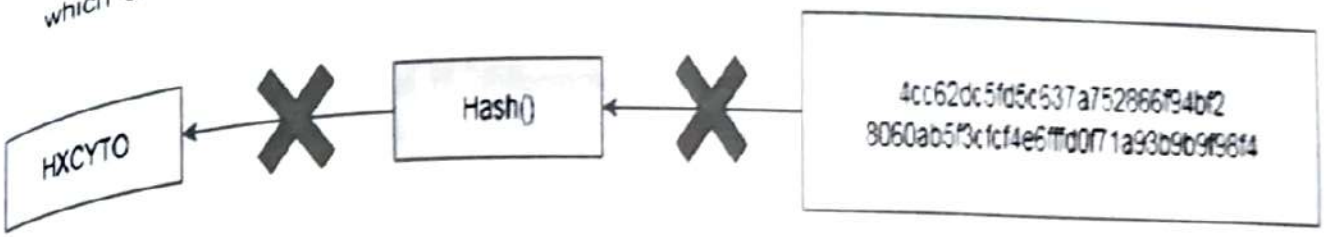
Process of signature generation

❖ What makes SHA-256 an ideal candidate for blockchain ?

SHA-256 offers security and reliability. Here are some of the main features of SHA-256, which make it perfect to be used as the main hashing function in a blockchain:

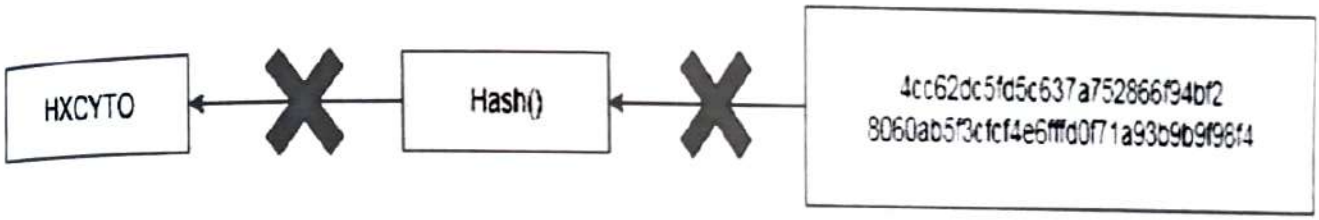
- Collision resistant : No two input values can produce the same hash output. This ensures that every block in the blockchain ledger is assigned a unique hash value.
- They can be hidden : It is difficult to guess the input value for a hash function from its output.

- Preimage resistance : The input cannot be recreated given a hash value. This ensures that during the proof of work in bitcoin, the miners cannot guess the value of nonce by converting the acceptable hash back into the input; instead, they have to use the brute force method, which ensures that the work is done.



The input value can not be calculated based on the hash

- Deterministic : The hash function's output should always remain the same, given that the input remains the same. This is a basic property of digital signatures, as the computed hash against a given input should remain consistent when calculated by the receiver and sender.
- Large output : The 256-bit output adds up to 22562256 possibilities making it impossible to apply the brute force solution to crack the hash.
- Avalanche effect : If there is a small change in the input, the output changes dramatically. This makes sure that the hash value can not be guessed based on the input values. This makes the hash more secure.



The input value can not be calculated based on the hash

These features of the SHA-256 make it an ideal candidate for blockchains as it provides security and reliability like no other.

Bitcoin block- size

- The block size in Bitcoin refers to the maximum size of a block of transactions that can be added to the blockchain. As per January 2022, the default maximum block size is 1 megabyte (MB).
- The block size is a crucial parameter because it determines the capacity of the Bitcoin network to process transactions. A larger block size can accommodate more transactions, potentially reducing congestion and transaction fees. However, it also poses challenges such as increased resource requirements for nodes.

❖ Bitcoin Mining

Bitcoin mining is the process by which transactions are verified on the blockchain. It is also the way new bitcoin are entered into circulation. "Mining" is performed using hardware and software to generate a cryptographic number that matches criteria. The first miner to find the solution to the problem receives the bitcoin reward and the process begins again.

Bitcoin mining is the process of validating the information in a blockchain block by generating a cryptographic solution that matches specific criteria. When a correct solution is reached, a reward in the form of bitcoin and fees for the work done is given to the miner(s) who reached the solution first.

Over time, the reward for mining Bitcoin is reduced. This reward process continues until there are 21 million bitcoin circulating. Once that number is reached, the bitcoin reward is expected to cease, and Bitcoin miners will be rewarded through fees paid for the work done.

The bitcoin reward that miners receive is an incentive that motivates people to assist in the primary purpose of mining: to legitimize and monitor Bitcoin transactions, ensuring their validity.

How Does Bitcoin Mining Work ?

Here's a simplified example to explain the process. Say you ask friends to guess a number between 1 and 100. Your friends don't have to guess the exact number; they just have to be the first to guess a number less than or equal to your number. If you think of the number 19 and a friend comes up with 21, another 55, and yet another 83, they lose because they all guessed more than 19. But if you have three friends left, and the next one guesses 16, they win, and the others don't get a chance to guess. The one who guessed 16 was the first to guess a number less than or equal to 19.

In this case, the number you chose, 19, represents the target hash the Bitcoin network creates for a block, and the random guesses from your friends are the guesses from the miners.

The Hash

At the heart of Bitcoin mining is the hash. The hash is a 64-digit hexadecimal number that is the result of sending the information contained in a block through the SHA256 hashing algorithm. This part of the process takes little time to complete—in fact, you can generate a hash in less than one second, pasting some content into an online SHA256 hash generator. This is the encryption method used by Bitcoin to create a block hash.

Target Hash

The target hash, used to determine mining difficulty, is the number miners are trying to solve for when they mine. This number is a hash generated by the network converted from hexadecimal to decimal form.

Mining

Bitcoin mining requires the mining program to generate a random hash and append another number to it called the nonce, or "number used once." When a miner begins, it always starts this number at

zero. The nonce changes by one every attempt—first, it's 0, then 1, 2, 3, and so on. If the hash and nonce generated by the miner are more than the target hash set by the network, the attempt fails, and the miner tries again.

Every miner on the network does this until a hash and nonce combination is created that is less than or equal to the target hash. The first to reach that target receives the reward and fees, and a new block is opened. Once that block fills up with information (about one megabyte), it is closed, encrypted, and mined.

The Bitcoin network is made up of thousands of devices that mine 24 hours per day. Because the mining reward goes to the first to solve the problem, they are all competing. This competition led miners to create pools to gain an advantage over other miners because they needed more computational power to increase their chances of winning.

Proof-of-Work

The mining process is what you hear called proof-of-work (PoW)—it takes a lot of energy and computational power to reach the goal of less than or equal to a target hash. The work done is viewed as the validation proof needed, so it's called proof-of-work.

Rewards

The reward for successfully validating a block is bitcoin. In 2009, you'd receive 50 bitcoin for mining a block. But the block reward is halved every 210,000 blocks (or roughly every four years), so in 2013, the reward amount declined to 25, then 12.5, then 6.25. In Bitcoin's next halving event, the reward will change to 3.125.

Another incentive for Bitcoin miners to participate in the process is transaction fees. In addition to rewards, miners also receive fees from any transactions contained in that block of transactions. When Bitcoin reaches its planned limit of 21 million (expected around 2140), miners will be rewarded with fees for processing transactions that network users will pay. These fees ensure that miners still have the incentive to mine and keep the network going. The idea is that competition for these fees will cause them to remain low after halving events are finished.

Halving

Approximately every four years, the reward that miners receive is halved in an event known as the "halving." This is programmed into the Bitcoin protocol to control the rate at which new bitcoins are created and ensure a capped supply of 21 million bitcoins.

Bitcoin mining requires specialized hardware, known as ASICs (Application-Specific Integrated Circuits), due to the intense computational power required. It's worth noting that as more miners participate in the network, the difficulty of the PoW puzzle adjusts to maintain a roughly 10-minute block time.

Mining can be done individually or in mining pools, where participants combine their computational power to increase the chances of successfully mining a block and sharing the rewards proportionally.

It's important to consider the environmental impact of Bitcoin mining, as the process consumes a significant amount of electricity, primarily in regions where energy is cheap. There are ongoing discussions within the cryptocurrency community about finding more energy-efficient consensus mechanisms.

4.4 PROOF OF WORK, BITCOIN SCRIPTING

❖ What is proof of work in bitcoin mining ?

In bitcoin mining, proof of work is a consensus mechanism that refers to the process where bitcoin miners verify bitcoin transactions. Proof of work requires miners to solve a hash function, or a complex mathematical puzzle.The first miner to solve the puzzle is rewarded with a newly minted bitcoin.

The hash function used in bitcoin mining is Secure Hash Algorithm 256-bit, or SHA-256. It takes an input and produces a unique output known as a hash. A miner's computational power is measured by their hash rate, which represents the number of hashes they calculate per second.

❖ Bitcoin scripting

Bitcoin scripting is a system used to define the conditions under which a Bitcoin transaction can be spent. Bitcoin transactions typically involve the transfer of bitcoins from one address (an output from a previous transaction) to another address. To ensure security and control over funds, transactions are often associated with certain conditions that must be met for the bitcoins to be spent. These conditions are defined using a simple scripting language.

Here are the key components of Bitcoin scripting :

1. **ScriptPubKey (Output Script) :** This script is part of the output of a Bitcoin transaction and specifies the conditions that must be satisfied for the bitcoins to be spent. It's essentially a locking script that defines who can spend the bitcoins and under what conditions. The conditions are specified in a scripting language known as Script.

2. **ScriptSig (Input Script) :** This script is part of the input to a Bitcoin transaction and provides the data necessary to satisfy the conditions specified in the ScriptPubKey. It's essentially an unlocking script that fulfills the requirements set by the ScriptPubKey.

3. **Script Language :** Bitcoin uses a Forth-like scripting language. It's a stack-based language where operations are performed on a stack of items. The language includes various opcodes, each representing a specific operation. Common operations include checking cryptographic signatures, comparing values, and performing logical operations.

4. **Standard Transaction Types :** While Bitcoin scripting is quite flexible, there are standard transaction types that most wallets and nodes understand. For example, Pay-to-Public-Key-Hash (P2PKH) and Pay-to-Script-Hash (P2SH) are common standard transaction types used in Bitcoin.

   - **P2PKH :** In a P2PKH transaction, the conditions to spend bitcoins involve providing a valid signature for a specific public key hash.

- **P2SH** : P2SH allows for more complex scripting conditions by having the conditions themselves hashed and provided in the ScriptPubKey. The spending transaction then includes the original script, known as the redeem script.

Bitcoin scripting provides a high level of flexibility, allowing users to create various types of transactions with different spending conditions. However, the scripting language intentionally lacks certain features to ensure the security and simplicity of the Bitcoin system.

It's important to note that while Bitcoin scripting is powerful, its capabilities are intentionally limited to maintain the security and integrity of the Bitcoin network. More complex scripting languages and smart contract functionality are often associated with other blockchain platforms like Ethereum.

4.5 BLOCKCHAIN COLLABORATIVE IMPLEMENTATIONS : HYPER LEDGER, CORDA- ERC 20 AND TOKEN

Hyperledger, Corda, ERC-20, and tokens are all related to blockchain technology, but they represent different frameworks, platforms, and standards used for collaborative implementations of distributed ledger systems. Let's briefly explore each of them:

Hyperledger :

Hyperledger is an open-source project under the Linux Foundation where people can come and work on the platform to develop blockchain-related use cases.

Hyperledger provides the platform to create personalized blockchain services according to the need of business work. Unlike other platforms for developing blockchain-based software, Hyperledger has the advantage of creating a secured and personalized blockchain network.

- It is created to support the development of blockchain-based distributed ledgers.
- It includes a variety of enterprise-ready permissioned blockchain platforms.
- It is a global collaboration for developing high-performance and reliable blockchain and distributed ledger-based technology frameworks.

❖ **Need of Hyperledger**

Below are some of the reasons stating the need for a hyperledger project:

- To enhance the efficiency, performance, and transactions of various business processes.
- It provides the necessary infrastructure and standards for developing various blockchain-based systems and applications for industrial use.
- It gets rid of the complex nature of contractual agreements, as the legal issues are taken care of.
- Hyperledger offers the physical separation of sensitive data.

- It decreases the need for verification and enhances trust, thus optimizing network performance and scalability.

Hyperledger Technology Layers

Hyperledger uses the following key business components:

1. **Consensus layer** : It takes care of creating an agreement on the order and confirming the correctness of the set of transactions that constitute a block.
2. **Smart layer** : This layer is responsible for processing transaction requests and authorizing valid transactions.
3. **Communication layer** : It takes care of peer-to-peer message transport.
4. **Identity management services** : these are important for establishing trust on the blockchain.
5. **API** : It enables external applications and clients to interface with the blockchain.

❖ **Hyperledger Advantages**

- Flexibility : Hyperledger provides a high degree of flexibility and modularity, allowing developers to customize and configure the platform to meet their specific needs.
- Security : Hyperledger has a strong focus on security, with features such as access control, identity management, and encryption. This makes it well-suited for enterprise applications that require a high level of security.
- Scalability : Hyperledger is designed to handle large-scale enterprise applications, with the ability to support thousands of transactions per second.
- Privacy : Hyperledger allows for the creation of private, permissioned blockchain networks, which means that only authorized participants have access to the data on the network.
- Interoperability : Hyperledger provides a common platform for building blockchain applications, which makes it easier to integrate with other systems and applications.

❖ **Hyperledger Disadvantages**

- Complexity : Hyperledger can be complex to set up and maintain, particularly for organizations that are new to blockchain technology. This can require significant technical expertise and resources.
- Limited decentralization : Hyperledger is a permissioned blockchain platform, which means that only authorized parties can participate in the network. While this can provide increased security and privacy, it also means that the network is less decentralized than public blockchain platforms.
- Limited community : While Hyperledger has a growing community of developers and contributors, it is still smaller than some other blockchain platforms. This could make it more difficult to find support and resources.

- Limited smart contract functionality : Hyperledger offers limited smart contract functionality compared to some other blockchain platforms. While this may be sufficient for some use cases, it could be a disadvantage for organizations that require more advanced smart contract capabilities.

Hyperledger Tools

There are numerous projects under hyperledger project itself. These projects include:

1. **Hyperledger Fabric :**

Hyperledger Fabric is intended as a foundation for developing applications and solutions with modular architecture. It provides many benefits like permissioned networks, confidential transactions, etc.

2. **Hyperledger Sawtooth :**

It is an open-source project and used as an enterprise-level blockchain system used for creating and operating distributed ledger applications. Hyperledger sawtooth supports a variety of consensus algorithms like PBFT, and PoET.

3. **Hyperledger Indy :**

It is a project that is made for decentralized identity. It offers lots of libraries, tools, and reusable components for creating decentralized identities.

4. **Hyperledger Iroha :**

It is a blockchain platform designed for infrastructure projects that need distributed ledger technology. It is used to build identity management platforms like national IDs. It can integrate with Linux, macOS, and Windows platforms.

5. **Hyperledger Burrow :**

It is a framework for executing smart contracts in permissioned blockchains. The goal of Hyperledger burrow is to facilitate cross-industry applications for smart contracts. It is built around the BFT consensus algorithm.

6. **Hyperledger Caliper :**

It is a blockchain benchmark tool that allows users to measure the performance of a blockchain implementation with a set of predefined use cases. It will produce reports containing a number of performance indicators to serve as a reference when using the blockchain solutions like Hyperledger Burrow, Hyperledger Fabric, Hyperledger Iroha, and so on.

7. **Hyperledger Cello :**

It serves as an operational dashboard for Blockchain that reduces the effort required for creating, managing, and using blockchains. It provides an operational console for managing blockchain efficiently.

8. **Hyperledger Explorer** :

It is a user-friendly web application tool that is used to view, invoke, deploy, or query blocks, associated data, and network information stored in the ledger. It is regarded as an easy way that allows users to view the necessary network information of the blockchain.

9. **Hyperledger Besu** :

It is an Ethereum client designed to be enterprise-friendly for both public and private blockchain network use cases. It offers many useful features like EVM, several proof-of-authority protocols, a privacy transaction manager to ensure the privacy of transactions, etc.

❖ **Corda**

Corda is a blockchain platform that was specifically designed for use in enterprise settings. It was developed by R3, a blockchain software firm, and is open-source and built on top of the Java Virtual Machine (JVM).

Corda is a permissioned blockchain, meaning that access to the network is controlled and restricted to certain users or organizations. This makes it well-suited for businesses and other entities that need to maintain a high level of security and privacy.

Some of the key features of Corda include :

- Smart contracts : Corda allows for the creation and execution of smart contracts, which are self-executing contracts that can automate the processing of certain transactions and enforce the terms of an agreement.
- Privacy : Corda uses a unique approach to privacy that allows for transactions to be shared only with the relevant parties involved in the transaction, rather than being visible to the entire network.
- Interoperability : Corda was designed with interoperability in mind, and can integrate with other enterprise systems and blockchain networks.
- Scalability : Corda's architecture is designed to handle large volumes of transactions and data, making it suitable for use in enterprise settings.

Some potential use cases for Corda include:

- **Trade finance** : Corda can be used to create more efficient and secure trade finance processes, by automating the processing of trade documents and reducing the need for intermediaries.
- **Healthcare** : Corda can help to improve the efficiency and security of healthcare data sharing, by enabling secure and private sharing of patient data between different providers.
- **Supply chain management** : Corda can be used to track and verify the authenticity and provenance of goods as they move through the supply chain, reducing the risk of fraud and improving efficiency.

Overall, Corda is a powerful and flexible blockchain platform that has the potential to revolutionize enterprise operations.

Advantages :

- It provides enhanced security.
- It is stable and scalable

Disadvantages :

- It is not very flexible as only parties involved in the transaction can take part in the decision.

ERC-20

ERC-20 is the technical standard for fungible tokens created using the Ethereum blockchain. A fungible token is one that is exchangeable with another token, whereas the well-known ERC-721 non-fungible tokens (NFTs) are not.

ERC-20 allows developers to create smart-contract-enabled tokens that can be used with other products and services. These tokens are a representation of an asset, right, ownership, access, cryptocurrency, or anything else that is not unique in and of itself but can be transferred.

- Ethereum Request for Comment 20 (ERC-20) is the implemented standard for fungible tokens created using the Ethereum blockchain.
- ERC-20 guides the creation of new tokens on the Ethereum blockchain so that they are interchangeable with other smart contract tokens.
- Since its implementation, most Ethereum-based tokens have been created using the ERC-20 standard.

ERC-20 Contents

ERC-20 is a list of functions and events that must be implemented into a token for it to be considered ERC-20 compliant. These functions (called methods in the ERC) describe what must be included in the smart-contract-enabled token, while events describe an action. The functions a token must have are:1

- **TotalSupply :**

  The total number of tokens that will ever be issued

- **BalanceOf :**

  The account balance of a token owner's account

- **Transfer :**

  Automatically executes transfers of a specified number of tokens to a specified address for transactions using the token

- **TransferFrom** :

  Automatically executes transfers of a specified number of tokens from a specified address using the token

- **Approve**:

  Allows a spender to withdraw a set number of tokens from a specified account, up to a specific amount

- **Allowance**:

  Returns a set number of tokens from a spender to the owner

  The events that must be included in the token are:

- **Transfer**:

  An event triggered when a transfer is successful

- **Approval**:

  A log of an approved event (an event)

The following functions are optional and are not required to be included, but they enhance the token's usability:

- Token's name (optional)
- Its symbol (optional)
- Decimal points to use (optional)

Advantages of ERC20

- **Interoperability** :

One of the key benefits of ERC-20 tokens is their interoperability. Because they all follow the same standard, they can be easily exchanged with one another. This makes them highly versatile and useful for a wide range of applications. For example, if you have an ERC-20 token for one project, you can easily exchange it for another ERC-20 token for a completely different project.

- **Security** :

Another advantage of ERC-20 tokens is their security. Because they are built on the Ethereum Blockchain, they inherit the security features of the Blockchain itself. This includes features such as immutability, transparency, and decentralization, which make it extremely difficult for anyone to tamper with or manipulate the tokens.

- **Customizable** :

ERC-20 tokens are also highly customizable. Developers can create their own ERC-20 tokens and tailor them to their specific needs. This includes defining the total supply of tokens, the decimal places used for each token, and any additional functionality that is needed.

- **Transparency :**

In addition, ERC-20 tokens offer a high degree of transparency. Because all transactions involving ERC-20 tokens are recorded on the Ethereum Blockchain, it is possible to track the movement of tokens from one address to another. This makes it easy to verify the authenticity of a transaction and provides a high degree of transparency for token holders and investors.

- **Highly liquid :**

ERC-20 tokens are also highly liquid, meaning they can be easily bought and sold on cryptocurrency exchanges. This liquidity makes them a popular choice for investors and traders who are looking to profit from the volatility of the cryptocurrency market.

- **Ease of use :**

Another benefit of ERC-20 tokens is their ease of use. They can be easily created and managed using a variety of tools and platforms, such as MyEtherWallet, MetaMask, and Remix. This accessibility makes them accessible to developers and users alike, and encourages innovation and experimentation within the Blockchain ecosystem.

Disadvantages of ERC-20

- The lack of flexibility of ERC20 tokens is a major concern. While ERC20 tokens have standardized rules and regulations that provide stability, they also limit their functionality. For example, ERC20 tokens cannot be used for more complex and advanced purposes, such as creating smart contracts with more intricate conditions or automating certain processes. This can be a significant disadvantage for businesses or organizations that require more flexibility and customization in their token design.

- The security of ERC20 tokens is a critical issue that cannot be overlooked. As ERC20 tokens are built on the Ethereum Blockchain, they inherit the same security vulnerabilities that exist on the Ethereum network. This includes the risk of hacking, exploitation of smart contract bugs, and network congestion. While there are measures that can be taken to mitigate these risks, such as audits and the implementation of security protocols, they do not completely eliminate the potential for security breaches.

- The gas fees associated with ERC20 tokens can be a significant expense for investors. Gas fees are required for every transaction on the Ethereum network, and the cost of gas can fluctuate depending on the level of network congestion. This can make it difficult for investors to accurately predict the cost of their transactions, and can result in unexpected expenses. In addition, smaller investors may not have the financial resources to pay high gas fees, which can limit their ability to participate in the token economy.

- ERC20 tokens may not be universally accepted by all crypto currency exchanges. While ERC20 is a widely accepted standard, there are still exchanges that do not support ERC20 tokens. This can limit the liquidity of the token and make it harder for investors to trade on different platforms. It is important for investors to research the exchanges that support ERC20 tokens before investing, in order to ensure that they will be able to trade the token as desired.

- ERC20 tokens can suffer from poor governance and a lack of transparency. This can resu issues such as token dumping, insider trading, and conflicts of interest. In addition, the lack transparency can make it difficult for investors to make informed decisions about the token and erode trust in the token and its creators.

❖ **Token** :

When we talk about "token" in the context of blockchain, we are typically referring to a unit of val or representation of an asset that exists on a blockchain. Tokens are created and managed throug smart contracts and they can represent a variety of assets, from cryptocurrencies to real-world asset Here are some key aspects related to tokens in the context of collaborative implementations on blockchai

❖ **Token Standards** :

ERC-20 :

This is one of the most widely adopted standards for fungible tokens on the Ethereum blockchain. ERC-20 tokens follow a set of rules that make them compatible with various applications and services on the Ethereum platform. They include functions such as transferring tokens, checking balances, and approving spending limits.

ERC-721 (Non-Fungible Tokens - NFTs) :

Unlike ERC-20 tokens, ERC-721 tokens are non-fungible and represent unique assets. This standard is often used for creating digital collectibles, unique in-game items, and digital art on the Ethereum blockchain.

Other Standards :

Apart from ERC-20 and ERC-721, there are other token standards and proposals emerging in the blockchain space, such as ERC-1155, which supports both fungible and non-fungible tokens within a single contract.

❖ **Use Cases for Tokens** :

Cryptocurrencies :

Many tokens function as digital currencies, and they can be used for transactions within a specific blockchain ecosystem. Examples include Bitcoin (BTC) on the Bitcoin blockchain and Ether (ETH) on the Ethereum blockchain.

Utility Tokens :

Tokens can be created to provide access to specific services, platforms, or ecosystems. Holders of these tokens may enjoy certain privileges, such as discounted fees or access to premium features.

Security Tokens :

Tokens can represent ownership or shares in real-world assets, such as real estate or company equity. Security tokens are subject to regulatory compliance and may offer holders rights to dividends or voting privileges.

Governance Tokens :

Some tokens are designed to facilitate governance within a decentralized system. Holders of these tokens may have voting rights to influence decisions related to the protocol or platform.

❖ **Token Creation and Management :**

Smart Contracts :

Tokens are typically created and managed through smart contracts, self-executing contracts with the terms of the agreement directly written into code. Smart contracts define the rules for token creation, distribution, and behavior.

Token Wallets :

Users store and manage their tokens in digital wallets. These wallets may be software wallets (applications) or hardware wallets (physical devices).

❖ **Challenges and Considerations :**

Regulatory Compliance : The regulatory status of tokens can vary, and compliance with local regulations is crucial, especially for security tokens.

Interoperability : The interoperability of tokens across different blockchains is a challenge. Efforts are being made to create standards that enable token movement between different blockchain networks.

Tokens play a crucial role in the blockchain ecosystem, offering a versatile and programmable way to represent value and ownership on decentralized networks.

❖ **Differentiate between blockchain and bitcoin**

	Bitcoin	Blockchain
Definition	The initial cryptocurrency variant	A distributed ledger for storing records of transactions
Objective	Simplification and improvement in speed of transactions without any government restrictions	Providing an environment for peer-to-peer transactions with a low cost, secure and safe environment
Scope	Limited to the role of a currency	Better adaptability to change and more support of top companies
Trading	Only provides currency trading	Can support transfer of currencies as well as stocks, contracts and property rights
Strategy	Reducing the cost of intermediaries and time of transactions	Effective responsiveness to change for catering requirements of different industries

Blockchain and Bitcoin are related concepts, but they serve different purposes and have distinct characteristics. Let's differentiate between the two:

1. **Definition** :

   - Blockchain : A blockchain is a distributed and decentralized ledger technology that records transactions across a network of computers in a secure and transparent manner. It consists of a chain of blocks, each containing a list of transactions, linked together using cryptographic hashes.
   - Bitcoin : Bitcoin is a digital or cryptocurrency that operates on a blockchain. It is a decentralized form of currency that allows peer-to-peer transactions without the need for intermediaries like banks. Bitcoin transactions are recorded on a blockchain.

2. **Purpose** :

   - Blockchain : The primary purpose of blockchain technology is to provide a secure and transparent way of recording and verifying transactions. It has applications beyond cryptocurrencies, such as supply chain management, smart contracts, and decentralized applications (DApps).
   - Bitcoin : Bitcoin is a specific application of blockchain technology, designed to serve as a decentralized digital currency. It enables individuals to make transactions without the need for a central authority, like a bank.

3. **Technology vs. Currency:**

   - Blockchain : It is a technology that can be used for various purposes beyond cryptocurrencies. It is a decentralized and distributed ledger system that ensures transparency, security, and immutability of data.
   - Bitcoin : It is a digital currency that utilizes blockchain technology to enable peer-to-peer transactions. Bitcoin is just one of many applications that can be built on a blockchain.

4. **Decentralization** :

   - Blockchain : It operates on a decentralized network of nodes, with no single entity having control over the entire system. This decentralization enhances security and reduces the risk of fraud or manipulation.
   - Bitcoin : It is decentralized, meaning no central authority (like a government or a bank) controls it. The Bitcoin network relies on a consensus mechanism called proof-of-work to validate transactions and secure the network.

5. **Mining** :

   - Blockchain : Mining is a process associated with some blockchain networks (like Bitcoin) where participants (miners) use computational power to solve complex mathematical problems, adding new blocks to the chain and securing the network.

- Bitcoin : Bitcoin mining is the process by which new bitcoins are created and transactions are added to the blockchain. Miners compete to solve cryptographic puzzles, and the first one to solve it gets to add a new block to the Bitcoin blockchain and is rewarded with newly minted bitcoins.

UTXO

UTXO stands for Unspent Transaction Output.

- It is the amount of digital currency someone has left remaining after executing a transaction.
- When a transaction is completed, the unspent output is deposited back into the database as input which can be used later for another transaction.
- In a blockchain, particularly in systems using the UTXO model (like Bitcoin), a UTXO represents the output of a transaction that has not been spent. When a user initiates a cryptocurrency transaction, the inputs to that transaction are essentially UTXOs from previous transactions.
- UTXOs are created through the consumption of existing UTXOs. Every Bitcoin transaction is composed of inputs and outputs. Inputs consume an existing UTXO, while outputs create a new UTXO.
- For example,Suppose you have three UTXOs, each representing 1 BTC, 2 BTC, and 3 BTC, respectively.
- If you want to send someone 4 BTC, the transaction might use the 1 BTC and 3 BTC UTXOs as inputs, creating a new UTXO with 4 BTC assigned to the recipient.The remaining 2 BTC UTXO is "change" and may be sent back to yourself.

UTXO Model

- The UTXO model does not incorporate wallets at the protocol level. It is based on individual transactions that are grouped in blocks. The UTXO model is a design common to many cryptocurrencies, most notably Bitcoin.
- Cryptocurrencies that use the UTXO model do not use accounts or balances. Instead, UTXOs are transferred between users much like physical cash.
- Each transaction in the UTXO model can transition the system to a new state, but transitioning to a new state with each transaction is infeasible.
- The network participants must stay in sync with the current state.

❖ **Difference between Bitcoin and Ethereum**

Sr. No.	Bitcoin	Ethereum
1	Created by Satoshi Nakamoto	Created by Vitalik Buterin
2	Genesis block was mined on January 3.2009	Genesis block was mined on July 30.2015
3	Proof of work consensus	Proof of stack consensus(started as Pow)
4	Supply limit of 21 million BTC	Unlimited supply
5	Block time is 10minute	Block time is 15 seconds
6	7 transactions per second	30 transactions per second

Exercises

❑ **MCQs :**

1. Which trees are responsible for storing all transactions in a black through digital signatures of the complete set of transactions?

   A. Binary B. Merkle C. Red Black D. AVL

2. What is the term applied for splits in a blockchain network ?

   A. Mergers B. Divisions C. Forks D. None of the above

3. What is a dApp ?

   A. A blockchain network B. Type of cryptocurrency

   C. Decentralized application D. Hardware component

4. What is the incentive for miners to validate transactions ?

   A. Appreciation of the community B. Nonce

   C. Additional memory D. Block rewards

5. What is the security incident when attackers gain control over the blockchain network resources?

   A. Reentrancy attack B. 51% attack

   C. Brute force attack D. Invasion attack

6. What is the purpose of a nonce ?

   A. Follows nouns B. A hash function

   C. Prevents double spending D. Sends information to the blockchain network

7. What incentivizes the miners to give correct validation of transactions ?

A. A nonce B. More memory

C. A block reward D. Thumbs up from the community

8. Bitcoin is based on _____ blockchain.

A. Public B. Private C. Permissioned D. Public Permissioned

9. What powers the Ethereum Virtual Machine ?

A. Ether B. Gas C. Bitcoin D. Block Rewards

10. What is the process of creating new bitcoins popularly known as ?

A. Finding B. Mining C. Panning D. Sourcing

Questions :

1. What is Bitcoin Mining ?
2. What is Bitcoin? Explain the block structure of a Bitcoin blockchain.
3. Discuss briefly about Hash pointer and how it is used in Merkle tree.
4. Explain why Merkle Trees are Important for Blockchain.
5. Differentiate between Blockchain and Bitcoin.
6. Explain Bitcoin Script.
7. Explain the various hyper ledger fabric tools in detail
8. What do you mean by blocks in block chain technology ?
9. What is Hyper ledger? Write types of Ledgers.
10. What is Corda in Consortium Blockchain ? Explain

***

UNIT
5

DECENTRALIZATION USING BLOCKCHAIN

5.1 Blockchain and full decentralization, smart contract.

5.2 Decentralized autonomous organization (DAO).

5.3 Decentralized applications

5.1 Blockchain and full decentralization, smart contract

❖ Blockchain and full decentralization

What is decentralization ?

Decentralization in blockchain refers to the transfer of authority and decision-making from a centralized entity (person, organization, or group thereof) to a distributed network.

Decentralized networks are designed to reduce the amount of trust that members must have in one another and to prevent members from abusing power or authority in ways that undermine the network's functionality.

The following diagram shows an overview of a decentralized ecosystem. In the bottom layer, the Internet or mesh networks provide a decentralized communication layer. In the next layer up, a storage layer uses technologies to enable decentralization. Finally, in the next level up, the blockchain serves as a decentralized processing (computation) layer. Blockchain can, in a limited way, provide a storage layer too, but that severely hampers the speed and capacity of the system. The Identity and Wealth layers are shown at the top level which provide authentication and identification services with varying degrees of decentralization and security assumptions :

Decentralized ecosystem

❖ Is it necessary for a blockchain to be decentralized ?

A controlled or decentralized blockchain is both possible. The phrases decentralized and dispersed, on the other hand, should not be used interchangeably.

A blockchain is naturally distributed (i.e., numerous parties hold copies of the data) but not decentralized. Permission less or public blockchains and permission-based or private blockchains are the two sorts of blockchains.

Because each node in the network has a complete record of every data published on the blockchain, public blockchains are now decentralized. Bitcoin is a popular example of a decentralized blockchain.

Private blockchains, on the other hand, are centralized. Because the network size is managed and the amount of access to nodes is controlled by a single organization.

Decentralization should be done only when it is necessary. It is not necessary for a blockchain application to be totally decentralized. Any blockchain solution must meet the needs of the user, which may or may not involve certain decentralization levels.

❖ Why is decentralization important ?

Decentralization is not a new concept. When building a technology solution, three main network architectures are commonly considered: centralized, dispersed, and decentralized.

While decentralized networks are widely employed in blockchain technology, a blockchain application cannot simply be categorized as such. Rather, decentralization should be gradually expanded to all aspects of a blockchain program.

Decentralizing resource management and access in an application can result in better and more equitable service. Although decentralization has certain disadvantages, such as lower transaction throughput, the advantages of improved stability and service levels exceed the disadvantages.

❖ Types of decentralization in blockchain

Before we can comprehend the many sorts of decentralization in blockchain, we must first comprehend the various levels of decentralization in general. Decentralization levels are covered further down.

Fully Centralized :

A system in which the whole system is controlled and managed by a single central authority. Take, for instance, the banking system.

Semi-decentralized :

A system in which the entire system is controlled and managed by numerous intermediaries.

Fully Decentralized :

A system in which no middlemen are used to govern or administer it. Take Bitcoin, for example.

Architectural Decentralization :

This sort of decentralization is concerned with the number of physical computers in the system. And how many PCs can it withstand malfunctioning at the same time?

As a result, architectural decentralized blockchains are ones in which the same blockchain is run by various systems. The blockchain will now be unaffected even if one machine crashes. Bitcoin is a well-known example of decentralized blockchain architecture.

Political Decentralization :

This sort of decentralization refers to the number of people or groups in charge of or managing the computers in a system.

Bitcoin, for example, is politically decentralized since it is not owned by any organization or individual. The Bitcoin protocol is used by all nodes in the Bitcoin network.

Logical Decentralization :

This sort of decentralization is concerned with the representation of the system's interface and data structures. Bitcoin, for example, is not theoretically decentralized since it has a single agreed-upon state and operates as a single system.

❖ **Decentralization's Advantages**

Following are the advantages of decentralization

Provides a trustless environment :

No one has to know or trust anybody other in a decentralized blockchain network. In the form of a distributed ledger, each member of the network owns a copy of the exact same data. If a member's ledger is tampered with or corrupted in any manner, the majority of the network's members will reject it.

Increases the accuracy of data reconciliation :

Companies frequently share information with their partners. This data is then changed and kept in each party's data silos, only to be resurfaced when it's time to transfer it downstream. Each time data is converted, the possibility of data loss or inaccurate data entering the workstream increases.

Points of vulnerability are reduced :

Decentralization can help to mitigate sources of vulnerability in systems when single actors are overly reliant. Systemic failures might result from these flaws, such as the inability to provide promised services or inefficient service owing to resource exhaustion, recurrent outages, bottlenecks, a lack of appropriate incentives for effective service, or corruption.

Distributes resources more efficiently :

Decentralization may also aid in resource distribution optimization, ensuring that promised services are delivered with improved performance and consistency, as well as a lower risk of catastrophic failure.

Transparent :

Because decentralized blockchains are available to the public, they are transparent. The blockchain is open to everyone with an internet connection. Each participating node keeps a single copy of the data.

Full Control :

With decentralization, the blockchain's members or users have complete authority over the activities. Because there is no central authority, all of the blockchain's data, control, and power are in the hands of its users.

Immutable :

The data contained in a blockchain in a decentralized blockchain is nearly hard to alter. Because each alteration must be confirmed by each node in the blockchain network, this is the case.

Secure :

Decentralized blockchains are far more secure than centralized blockchains because they employ encryption to protect data. Furthermore, the data in the current block requires data from the preceding block to be cryptographically confirmed.

- **Disadvantages of decentralization in Blockchain**

Following are the disadvantages of decentralization –

Cost :

In an organization, decentralization might be costlier than centralization. Because it necessitates the development of communication-automation systems and technologies.

Conflict :

decentralization should only be employed when the consumers' needs are met. Because disputes might arise if users do not properly preserve decentralization.

Volatility :

Cryptocurrencies built on a decentralized blockchain are extremely volatile. This is due to the fact that cryptocurrencies, or possibly the entire technology, are relatively new to the market. As a result, a large number of individuals are investing in them.

Crime :

This is due to the fact that everything is done on the network anonymously, which might lead exploitation or misuse.

❖ Smart Contract

A Smart Contract (or cryptocontract) is a computer program that directly and automatically controls the transfer of digital assets between the parties under certain conditions. A smart contract works in the same way as a traditional contract while also automatically enforcing the contract. Smart contracts are programs that execute exactly as they are set up(coded, programmed) by their creators. Just like a traditional contract is enforceable by law, smart contracts are enforceable by code.

- The bitcoin network was the first to use some sort of smart contract by using them to transfer value from one person to another.
- The smart contract involved employs basic conditions like checking if the amount of value to transfer is actually available in the sender account.
- Later, the Ethereum platform emerged which was considered more powerful, precisely because the developers/programmers could make custom contracts in a Turing-complete language.
- It is to be noted that the contracts written in the case of the bitcoin network were written in a Turing-incomplete language, restricting the potential of smart contracts implementation in the bitcoin network.
- There are some common smart contract platforms like Ethereum, Solana, Polkadot, Hyperledger fabric, etc.

❖ History :

In 1994, Nick Szabo, a legal scholar, and a cryptographer recognized the application of a decentralized ledger for smart contracts. He theorized that these contracts could be written in code which can be stored and replicated on the system and supervised by the network of computers that constitute the blockchain. These smart contracts could also help in transferring digital assets between the parties under certain conditions.

❖ Features of Smart Contracts

The following are some essential characteristics of a smart contract:

1. Distributed :

Everyone on the network is guaranteed to have a copy of all the conditions of the smart contract and they cannot be changed by one of the parties. A smart contract is replicated and distributed by all the nodes connected to the network.

2. Deterministic :

Smart contracts can only perform functions for which they are designed only when the required conditions are met. The final outcome will not vary, no matter who executes the smart contract.

3. **Immutable :**

Once deployed smart contract cannot be changed, it can only be removed as long as the functionality is implemented previously.

4. **Autonomy :**

There is no third party involved. The contract is made by you and shared between the parties. No intermediaries are involved which minimizes bullying and grants full authority to the dealing parties. Also, the smart contract is maintained and executed by all the nodes on the network, thus removing all the controlling power from any one party's hand.

5. **Customizable :**

Smart contracts have the ability for modification or we can say customization before being launched to do what the user wants it to do.

6. **Transparent :**

Smart contracts are always stored on a public distributed ledger called blockchain due to which the code is visible to everyone, whether or not they are participants in the smart contract.

7. **Trustless :**

These are not required by third parties to verify the integrity of the process or to check whether the required conditions are met.

8. **Self-verifying :**

These are self-verifying due to automated possibilities.

9. **Self-enforcing :**

These are self-enforcing when the conditions and rules are met at all stages.

❖ **Capabilities of Smart Contracts**

1. **Accuracy :**

Smart contracts are accurate to the limit a programmer has accurately coded them for execution.

2. **Automation :**

Smart contracts can automate the tasks/ processes that are done manually.

3. **Speed :**

Smart contracts use software code to automate tasks, thereby reducing the time it takes to maneuver through all the human interaction-related processes. Because everything is coded, the time taken to do all the work is the time taken for the code in the smart contract to execute.

4. Backup :

Every node in the blockchain maintains the shared ledger, providing probably the best backup facility.

5. Security :

Cryptography can make sure that the assets are safe and sound. Even if someone breaks the encryption, the hacker will have to modify all the blocks that come after the block which has been modified. Please note that this is a highly difficult and computation-intensive task and is practically impossible for a small or medium-sized organization to do.

6. Savings :

Smart contracts save money as they eliminate the presence of intermediaries in the process. Also, the money spent on the paperwork is minimal to zero.

7. Manages information :

Smart contract manages users' agreement, and stores information about an application like domain registration, membership records, etc.

8. Multi-signature accounts :

Smart contracts support multi-signature accounts to distribute funds as soon as all the parties involved confirm the agreement.

❖ **Types of Smart Contracts**

When it comes to the types of smart contracts, they are classified into three categories — legal contracts, decentralized autonomous organizations or DAOs, and logic contracts. Here, we'll discuss each of the three in more detail.

1. Smart legal contract

Smart contracts are guaranteed by law. They adhere to the structure of legal contracts: "If this happens, and then this will happen." As smart contracts reside on blockchain and are unchangeable, judicial or legal smart contracts offer greater transparency than traditional documents among contracting entities.

The parties involved execute contracts with digital signatures. Smart legal contracts may be executed autonomously if certain prerequisites are fulfilled, for example, making a payment when a specific deadline is reached. In the event of failure to comply, stakeholders could face severe legal repercussions.

2. Decentralized autonomous organizations

DAOs are democratic groups governed by a smart contract that confers them with voting rights. A DAO serves as a blockchain-governed organization with a shared objective that is collectively controlled. No executive or president exists. Instead, blockchain-based tenets embedded within the

contract's code regulate how the organization functions and funds are allocated. VitaDAO is an example of this type of smart contract, where the technology powers a community for scientific research.

3. **Application logic contracts**

ALCs, or application logic contracts, consist of application-based code that typically remains synced with various other blockchain contracts. It enables interactions between various devices, like the Internet of Things (IoT) or blockchain integration. Unlike the other types of smart contracts, these are not signed between humans or organizations but between machines and other contracts.

❖ **How Do Smart Contracts Work?**

A smart contract is just a digital contract with the security coding of the blockchain.

- It has details and permissions written in code that require an exact sequence of events to take place to trigger the agreement of the terms mentioned in the smart contract.
- It can also include the time constraints that can introduce deadlines in the contract.
- Every smart contract has its address in the blockchain. The contract can be interacted with by using its address presuming the contract has been broadcasted on the network.

The idea behind smart contracts is pretty simple. They are executed on a basis of simple logic, IF-THEN for example:

- IF you send object A, THEN the sum (of money, in cryptocurrency) will be transferred to you.
- IF you transfer a certain amount of digital assets (cryptocurrency, for example, ether, bitcoin), THEN the A object will be transferred to you.
- IF I finish the work, THEN the digital assets mentioned in the contract will be transferred to me.

Note : The WHEN constraint can be added to include the time factor in the smart contracts. It can be seen that these smart contracts help set conditions that have to be fulfilled for the terms of the contract agreement to be executed. There is no limit on how much IF or THEN you can include in your intelligent contract.

❖ **Smart Contract Working**

- **Identify Agreement :**

  Multiple parties identify the cooperative opportunity and desired outcomes and agreements could include business processes, asset swaps, etc.

- **Set conditions :**

  Smart contracts could be initiated by parties themselves or when certain conditions are met like financial market indices, events like GPS locations, etc.

- **Code business logic :**

  A computer program is written that will be executed automatically when the conditional parameters are met.

- **Encryption and blockchain technology :**

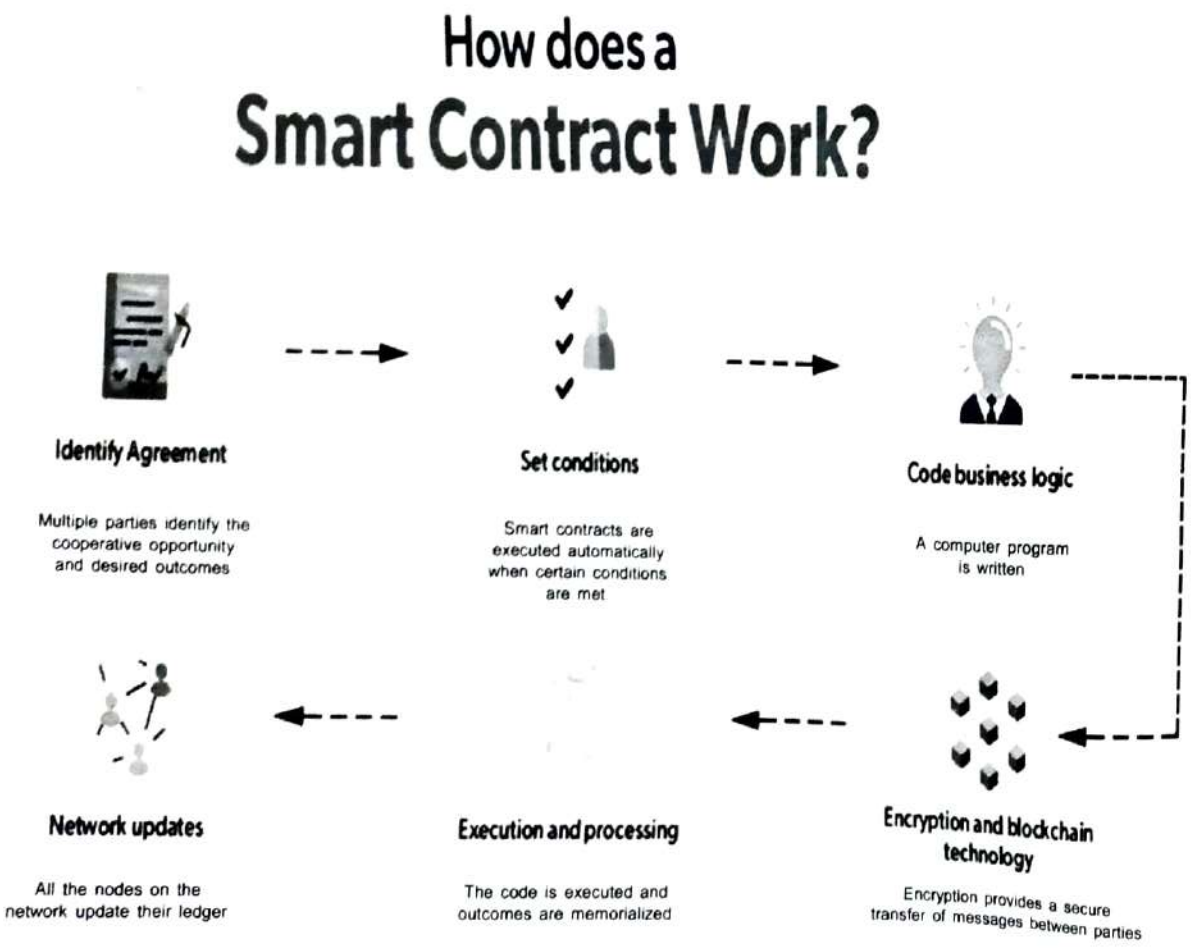
  Encryption provides secure authentication and transfer of messages between parties relating to smart contracts.

- **Execution and processing :**

  In blockchain iteration, whenever consensus is reached between the parties regarding authentication and verification then the code is executed and the outcomes are memorialized for compliance and verification.

- **Network updates :**

  After smart contracts are executed, all the nodes on the network update their ledger to reflect the new state. Once the record is posted and verified on the blockchain network, it cannot be modified, it is in append mode only.



Applications of Smart Contracts

Real Estate :

Reduce money paid to the middleman and distribute between the parties actually involved. For example, a smart contract to transfer ownership of an apartment once a certain amount of resources have been transferred to the seller's account(or wallet).

Vehicle ownership :

A smart contract can be deployed in a blockchain that keeps track of vehicle maintenance and ownership. The smart contract can, for example, enforce vehicle maintenance service every six months; failure of which will lead to suspension of driving license.

Music Industry :

The music industry could record the ownership of music in a blockchain. A smart contract can be embedded in the blockchain and royalties can be credited to the owner's account when the song is used for commercial purposes. It can also work in resolving ownership disputes.

Government elections :

Once the votes are logged in the blockchain, it would be very hard to decrypt the voter address and modify the vote leading to more confidence against the ill practices.

Management :

The blockchain application in management can streamline and automate many decisions that are taken late or deferred. Every decision is transparent and available to any party who has the authority(an application on the private blockchain). For example, a smart contract can be deployed to trigger the supply of raw materials when 10 tonnes of plastic bags are produced.

Healthcare :

Automating healthcare payment processes using smart contracts can prevent fraud. Every treatment is registered on the ledger and in the end, the smart contract can calculate the sum of all the transactions. The patient can't be discharged from the hospital until the bill has been paid and can be coded in the smart contract.

❖ Advantages of Smart Contracts

1. **Recordkeeping :**

   All contract transactions are stored in chronological order in the blockchain and can be accessed along with the complete audit trail. However, the parties involved can be secured cryptographically for full privacy.

2. **Autonomy :**

   There are direct dealings between parties. Smart contracts remove the need for intermediaries and allow for transparent, direct relationships with customers.

- **Code business logic :**

  A computer program is written that will be executed automatically when the conditional parameters are met.

- **Encryption and blockchain technology :**

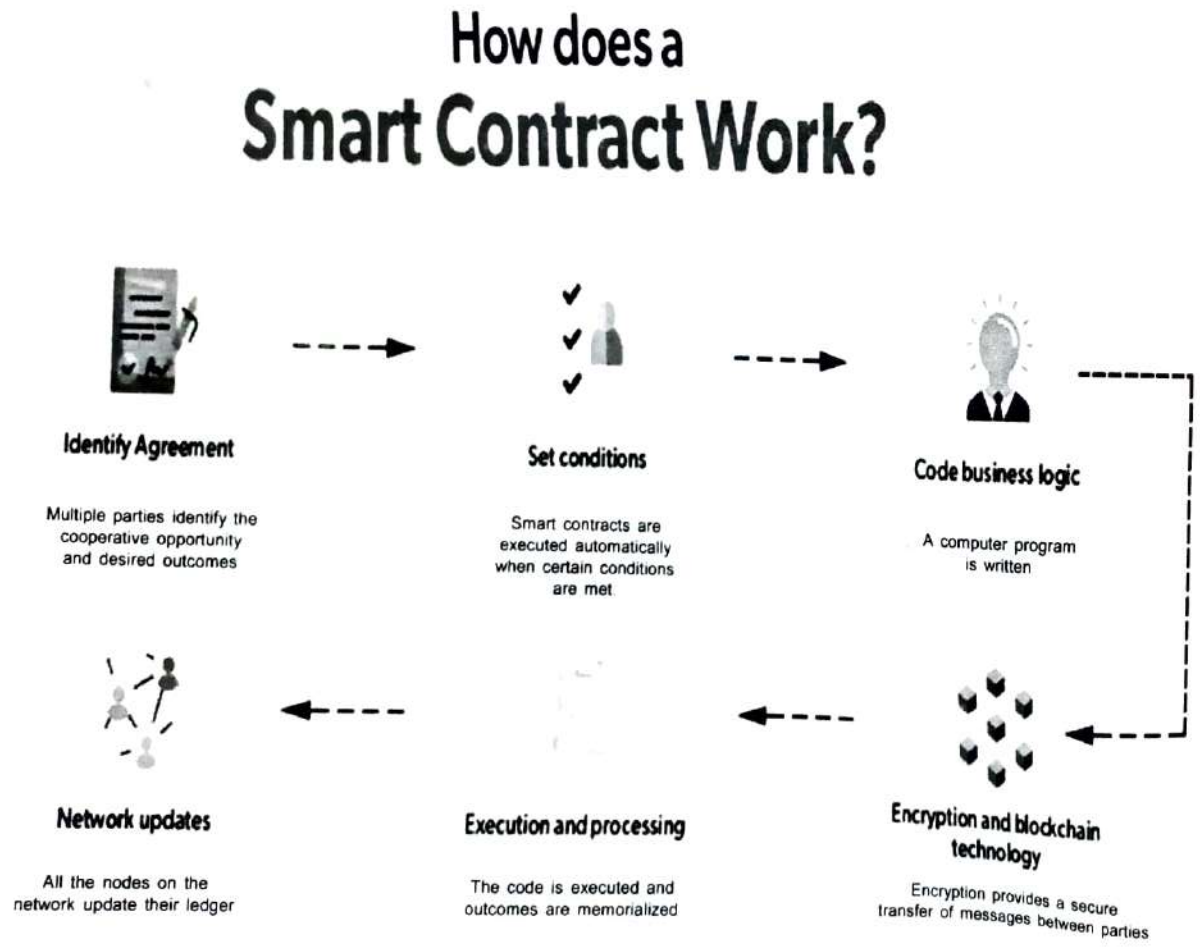
  Encryption provides secure authentication and transfer of messages between parties relating to smart contracts.

- **Execution and processing :**

  In blockchain iteration, whenever consensus is reached between the parties regarding authentication and verification then the code is executed and the outcomes are memorialized for compliance and verification.

- **Network updates :**

  After smart contracts are executed, all the nodes on the network update their ledger to reflect the new state. Once the record is posted and verified on the blockchain network, it cannot be modified, it is in append mode only.



Applications of Smart Contracts

Real Estate :

Reduce money paid to the middleman and distribute between the parties actually involved. For example, a smart contract to transfer ownership of an apartment once a certain amount of resources have been transferred to the seller's account(or wallet).

Vehicle ownership :

A smart contract can be deployed in a blockchain that keeps track of vehicle maintenance and ownership. The smart contract can, for example, enforce vehicle maintenance service every six months; failure of which will lead to suspension of driving license.

Music Industry :

The music industry could record the ownership of music in a blockchain. A smart contract can be embedded in the blockchain and royalties can be credited to the owner's account when the song is used for commercial purposes. It can also work in resolving ownership disputes.

Government elections :

Once the votes are logged in the blockchain, it would be very hard to decrypt the voter address and modify the vote leading to more confidence against the ill practices.

Management :

The blockchain application in management can streamline and automate many decisions that are taken late or deferred. Every decision is transparent and available to any party who has the authority(an application on the private blockchain). For example, a smart contract can be deployed to trigger the supply of raw materials when 10 tonnes of plastic bags are produced.

Healthcare :

Automating healthcare payment processes using smart contracts can prevent fraud. Every treatment is registered on the ledger and in the end, the smart contract can calculate the sum of all the transactions. The patient can't be discharged from the hospital until the bill has been paid and can be coded in the smart contract.

❖ Advantages of Smart Contracts

1. **Recordkeeping :**

   All contract transactions are stored in chronological order in the blockchain and can be accessed along with the complete audit trail. However, the parties involved can be secured cryptographically for full privacy.

2. **Autonomy :**

   There are direct dealings between parties. Smart contracts remove the need for intermediaries and allow for transparent, direct relationships with customers.

3. **Reduce fraud :**

Fraudulent activity detection and reduction. Smart contracts are stored in the blockchain. Forcefully modifying the blockchain is very difficult as it's computation-intensive. Also, a violation of the smart contract can be detected by the nodes in the network and such a violation attempt is marked invalid and not stored in the blockchain.

4. **Fault-tolerance :**

Since no single person or entity is in control of the digital assets, one-party domination and situation of one part backing out do not happen as the platform is decentralized and so even if one node detaches itself from the network, the contract remains intact.

5. **Enhanced trust :**

Business agreements are automatically executed and enforced. Plus, these agreements are immutable and therefore unbreakable and undeniable.

6. **Cost-efficiency :**

The application of smart contracts eliminates the need for intermediaries(brokers, lawyers, notaries, witnesses, etc.) leading to reduced costs. Also eliminates paperwork leading to paper saving and money-saving.

❖ **Challenges of Smart Contracts**

1. **No regulations :**

A lack of international regulations focusing on blockchain technology(and related technology like smart contracts, mining, and use cases like cryptocurrency) makes these technologies difficult to oversee.

2. **Difficult to implement :**

Smart contracts are also complicated to implement because it's still a relatively new concept and research is still going on to understand the smart contract and its implications fully.

3. **Immutable :**

They are practically immutable. Whenever there is a change that has to be incorporated into the contract, a new contract has to be made and implemented in the blockchain.

4. **Alignment :**

Smart contracts can speed the execution of the process that span multiple parties irrespective of the fact whether the smart contracts are in alignment with all the parties' intention and understanding.

5.2 DECENTRALIZED AUTONOMOUS ORGANIZATION (DAO)

DAO stands for Decentralized Autonomous Organization. The concept of a DAO was first proposed by Bit Shares, Steemit, and EOS (Block. one) founder Dan Larimer in the year 2015, and was further refined in the year 2016 by Ethereum's Vitalik Buterin. A decentralized autonomous organization is decentralized, autonomous, and an organization- as the name already suggests. It is a whole organization that is automated. It stores rules and processes in code. DAOs are often stateless and distributed over millions of computers. No single government could decide to take it down.

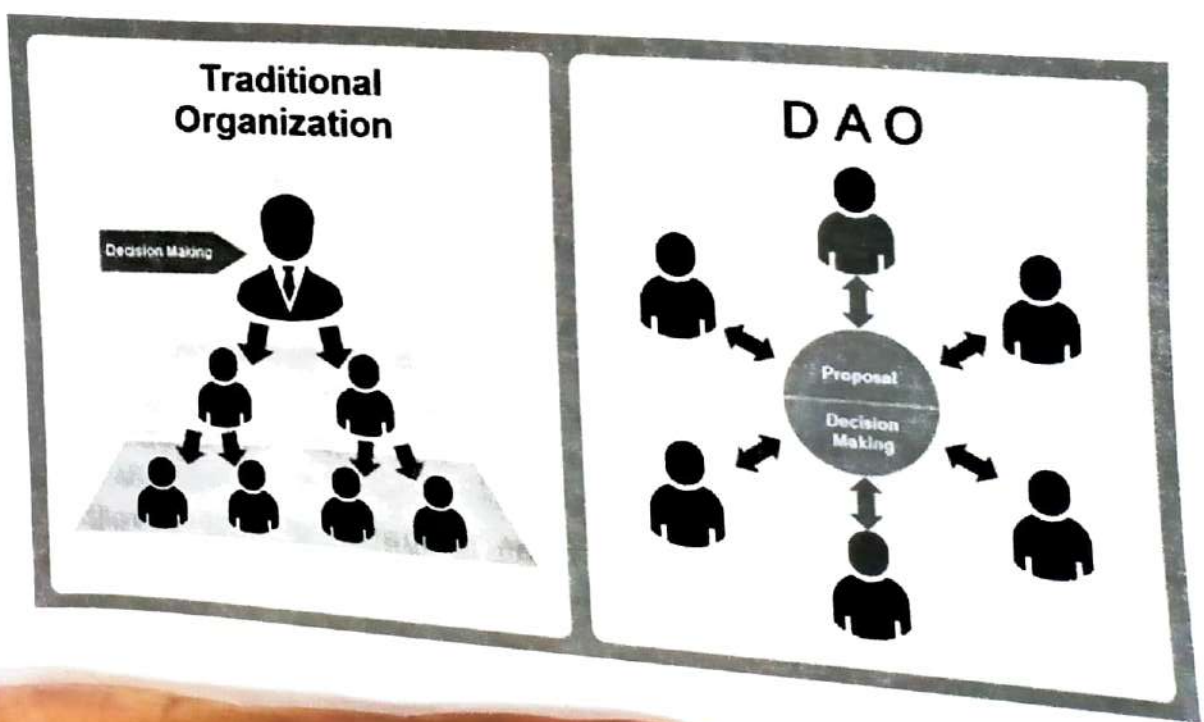
❖ **Components of DAO :**

1. **No central legal entity :** In DAO, there is no central legal entity, this means that no single entity is responsible for regulating the project.
2. **Self-enforcing code :** Smart contracts are created and extensively tested to make sure important details are not overlooked.
3. **Token acts as an incentive for validators :** Tokens are used in DAO for validators to motivate them and to ensure active, fair, and quick participation.

❖ **Need of DAO**

Beginning an association with somebody that includes financing and cash requires a great deal of confidence in the individuals you're working with. Yet, it's difficult to believe somebody you've just at any point associated with on the web. With DAOs you do not need to trust the other individual within the gathering, simply the DAO's code, which is 100% straightforward and evident by anybody. This opens up countless new freedoms for worldwide joint effort and coordination.

❖ **Traditional Organization Vs DAO**



DAO	Traditional Organizations
Casting a ballot is needed by individuals for any progressions to be implemented.	Depending on the structure, changes can be requested from the sole party, or casting a ballot might be advertised.
Votes were counted, and results were carried out consequently without a believed intermediary.	If casting a ballot is permitted, votes are counted inside, and the result of casting a ballot should be taken care of physically.
Completely democratized.	Usually progressive.
Administrations offered are taken care of consequently in a decentralized way.	Requires human taking care of, or halfway controlled mechanization, inclined to control.

❖ **Steps for Launching a DAO**

There are three major steps for launching a DAO :

1. Smart Contract Creation :

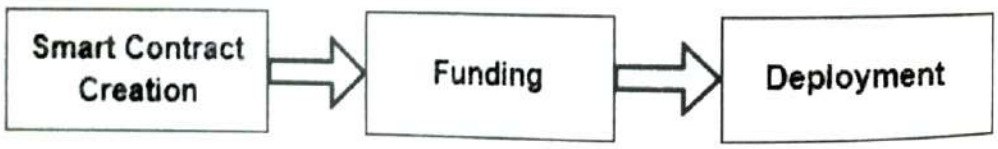
In this step, a developer or a group of developers create a smart contract behind the DAO. It is very important for the developer to extensively test the smart contracts before launching to make sure that they do not overlook important details. After launch, only the rules set can be changed through the governance system.

2. Funding :

After smart contracts are created and launched, the DAO needs to determine a way to receive funding. Sometimes, the tokens are sold to raise funds. These tokens give holders voting rights.

3. Deployment :

Once everything is set up and on track, the DAO needs to be deployed on the blockchain. From this point onwards, stakeholders decide the future of the organization. The developers who created the smart contracts, no longer influence the project.



❖ **DAO Examples**

Here are some examples illustrating how DAO can be utilized :

1. DASH :

The well-known computerized money Dash is an illustration of a decentralized independent association in light of the manner in which it is represented and the manner in which its planning framework is organized.

2. **A cause :**

One can acknowledge enrollment and gifts from anybody on the planet and the gathering can choose how they to spend gifts.

3. **A consultant organization :**

One can make an organization of workers for hire who pool their assets for office spaces and programming memberships.

4. **Adventures and awards :**

It is possible to make an endeavor store that pools speculation capital and decisions on dares to back. Reimbursed cash could later be rearranged among DAO individuals.

❖ **How Do DAOs Work?**

So far we are using people to "store" information instead. In order to know how much hiring a new person would cost? – There is a person answerable in the human resources department. Similarly, to get movement costs repaid?- There is a separate person responsible for this in the accounting.

- In a DAO, there is a code for that. Computers will take over much of the decision-making and operations we see nowadays. The final control, however, is still with humans, the shareholders. Shareholders have voting rights just like in regular corporations. They dictate the general direction and accept or decline initiatives.
- The general idea is to bring the benefits of blockchain technology to management.
- The blockchain is immutable, precise, and consistent. It is also transparent and open so that anyone could review companies. Strong consistency makes DAOs reliable business partners.
- Such an organization is also harder to put under pressure. It will be difficult to ban it from operating somewhere. As it is controlled by the organization members and not influenced by a central government authority to put under pressure.

❖ **DAO Membership**

There are various models for DAO membership. Membership can decide how casting ballot functions and other key pieces of the DAO.

1. **Token-based membership :**

Normally completely permissionless, contingent upon the token utilized. For the most part, these administration tokens can be exchanged for permissionless on a decentralized trade. Others should be procured by giving liquidity or another 'evidence of work'. In any case, just holding the symbolic awards admittance to casting a ballot. Ordinarily used to administer expansive decentralized conventions as well as tokens themselves.

Example : MakerDAO's token MKR is generally accessible on decentralized trades. So anybody can become tied up with having cast a ballot power on the Maker convention's future.

2. Share-based membership :

Offer-based DAOs are more allowed, yet at the same time very open. Any imminent individuals can present a proposition to join the DAO, typically offering recognition of some worth as tokens or work. Offers to address direct democratic force and possession. Individuals can exit whenever with their proportionate portion of the depository. Regularly utilized for all the nearer sew, human-driven associations like foundations, laborer assemblages, and venture clubs. Can administer conventions and tokens too.

Example : MolochDAO is centered around financing Ethereum projects. They require a proposition for enrollment so the gathering can evaluate whether you have the important mastery and funding to make educated decisions about possible grantees. You can't simply purchase admittance to the DAO on the open market.

❖ **Ethereum and DAOs**

Ethereum is the ideal establishment for DAOs for various reasons :

- Ethereum's own agreement is conveyed and set up enough for associations to trust the organization.
- The agreement code can't be changed once live, even by its proprietors. This permits the DAO to run by the principles it was modified with.
- Agreements can send/get reserves. Without this, there is a need for a believed delegate to oversee a bunch of reserves.
- The Ethereum people group has demonstrated to be more synergistic than cutthroat, taking into consideration best practices and emotionally supportive networks to arise rapidly.

❖ **Advantages of DAO**

1. Decentralization :

DAO emphasizes being driven by a collective rather than an individual. With DAO, participants have a much stronger say in the organization's direction.

2. Community Driven :

DAOs make it easy for communities worldwide to connect and build a prospering vision together. DAO is accessible to Individuals who may have had the opportunity in the past to connect and work together.

3. Principle-agent dilemma :

One of the main advantages of DAO is that it provides a solution for the principle-agent dilemma. This dilemma is a conflict in priorities between a person (principle) and the entities making decisions on their behalf (agent). One of the common examples of this is problems between Stakeholders and CEOs. DAO solves this problem through community governance. Here, principles don't have to trust agents who work on their behalf instead they work as a part of a group whose incentives are aligned.

❖ Disadvantages of DAO

This section lists some of the disadvantages of DAO :

1. **Security :**

DAO can be launched with just a few lines of code and given the immense tech stack a well-run DAO requires to operate effectively thus security remains a vulnerability as it requires significant technical expertise and it is expensive to keep best security practices implemented.

2. **Slow Decision Making :**

With DAO scaling there comes an issue of getting everyone to vote on proposals in a timely manner and with different time zones and investor priorities, keeping DAO participants up to date can be challenging.

3. **The Bikeshedding Effect :**

Parkinson's Law of Triviality states that the amount of time spent discussing an issue in an organization is inversely related to its importance in the scheme of things. This is also known as bike-shedding. It can have a negative impact on personal productivity as it causes inefficient management of time.

4. **No legitimate structure for circulating DAOs :**

DAOs can be circulated across different locales, and there's no legitimate structure for them. Any lawful issues that might emerge will probably require those required to manage various territorial laws in a convoluted fight in court. In July 2017, for instance, the United States Securities and Exchange Commission gave a report not really settled that the DAO sold protections as tokens on the Ethereum blockchain without approval, disregarding bits of protection law in the country.

❖ Future of DAO

The DAO as initially imagined had not returned as of mid-2020. Regardless, interest in decentralized independent associations as a more extensive gathering keeps on developing. While there are many waiting concerns and potential issues with respect to lawfulness, security, and construction, a few investigators and financial backers accept that this kind of association will ultimately come to conspicuousness, maybe in any event, supplanting customarily organized organizations.

❖ Criticism of DAO

There are likewise a couple of drawbacks to DAO :

1. One significant issue of being open-source is that securing business insider facts will end up being more troublesome.
2. Additionally, potential hackers can more easily detect weak spots in the system as they can openly access the source code. In rare cases, they could even slip their pieces of code into the software without being detected by the community. That way they could create their own loopholes.

5.3 DECENTRALIZED APPLICATIONS

Decentralized apps are digital applications or programs that are based on Blockchain and fundamentally different from normal applications. Unlike normal applications that run on centralized servers that belong to the company which owns them, dApps run on a decentralized peer-to-peer (P2P) network that is based on Blockchain.

❖ What are Decentralized Apps (dApps) ?

Decentralized applications or dApps are distributed, decentralized open-source software applications that run on a decentralized peer-to-peer network. Imagine the Twitter application that you have on your phone. You can post anything you want on Twitter but ultimately it's controlled by a single company that can delete your tweets if they violate community guidelines or some other reason. But if there was a Twitter-type dApp, then it would be decentralized and not owned by any one person. If you posted something there, nobody would be able to delete it including its creators.

Multiple people can create content and consume content on these applications that is free of any control and interference from one person. Below are some of the requirements of dApps :

1. Open Source :

dApps should be open source and its codebase should be freely available for all. Any changes in the structure or working of the app should only be taken with the agreement of the majority.

2. Decentralized :

dApps should be decentralized with all the information and operations stored on a public and decentralized Blockchain which would ensure security and transparency.

3. Incentive :

dApps should offer some sort of incentive to their users in the form of cryptographic tokens. These are a sort of liquid assets and they provide incentives for users to support the Blockchain dApp ecosystem.

4. Protocol :

dApps should have a particular protocol to demonstrate proof of value. This means showing the value of a particular process in a way that can be easily verified by others.

❖ How Do dApps Work ?

A dApp has a backend code running on a decentralized peer-to-peer network. It can also have a frontend code and a user interface that can be written in any language just as it is done for normal applications. The front end can be hosted on any decentralized server like IPFS. dApps work in a manner similar to normal applications except for the few differences that are discussed below :

The dApp working has the following features :

- **Decentralized :**

  A dApp operates on Ethereum which is an open public decentralized platform.

- **Deterministic :**

  dApps perform the same function irrespective of the environment in which they are executed.

- **Turing complete :**

  dApps can perform any action given the required resources.

- **Isolated :**

  dApps are executed in an Ethereum Virtual Machine which is a virtual environment that ensures that even if there is a bug in the smart contract, it won't hamper the normal functioning of the blockchain network.

❖ **Most Common Platforms for creating dApps**

There are many Blockchain platforms created by various companies. While the most popular and commonly heard one is Bitcoin, there are many others that are used to create dApps. These Blockchain platforms are further used as a base to create dApps. So let's see some of these now :

1. **Ethereum :**

Ethereum is the most popular decentralized, open-source blockchain in the world currently. It is used as the base for many Blockchain projects, including more than 2500 dApps. In fact, Ethereum is only second to Bitcoin in terms of its market value. Ethereum also has a native cryptocurrency known as BTH which is their version of Bitcoin. All in all, this is an excellent option for creating a dApp although it's a bit expensive.

2. **NEO :**

NEO is also a decentralized, open-source blockchain that aims to create a smart economy. It is also called the Chinese Ethereum and provides better options for scalability in dApps as compared to other Blockchain platforms. NEO is currently less popular than Ethereum with only about 100 dApps built using this technology. It's also quite expensive and can even charge higher fees than Ethereum in some cases.

3. **TRON :**

TRON is a comparatively new Blockchain platform as compared to Ethereum or NEO. However, it's quite popular and may even become a competitor to Ethereum in the future. TRON is particularly famous for gaming applications and gambling sites. There are around 1500 dApps created using this platform which makes it an excellent choice.

❖ **Popular dApps**

Below are some of the popular dApps :

1. **CryptoKitties** :

CryptoKitties is a fun app that is used for entertainment. You can buy kitties on the app using cryptocurrency and then breed and sell them at a profit. Apparently, cute cats are popular everywhere even on Blockchain because CryptoKitties was once responsible for 10% of Ethereum transactions daily.

2. **OpenSea** :

Open Sea is a dApp that encourages interaction between various games based on Blockchain. Gamers can exchange their collectibles from any cryptocurrency-based game on OpenSea. Currently, this dApp supports collectibles from Ethereum only, but they plan to expand in the future.

3. **WINk** :

WINk is the most popular dApp for gambling-based games in the market. It included everything from poker to dice games to sports betting. WINk is based on the TRON platform and the winners in betting get WIN tokens which can then be exchanged for BTT which is a sort of cryptocurrency like Bitcoin.

4. **IPSE** :

IPSE or InterPlanetary Search Engine is actually a search engine with Blockchain as its base. IPSE is based on the EOS blockchain and it uses the InterPlanetary File System (IPFS) which is an improvement over HTTP on the internet. A big advantage of IPSE over other conventional search engines is that it guarantees security and privacy on the internet.

5. **Blockchain Cuties** :

For anyone interested in CryptoKitties, Blockchain Cuties is a great option. It allows you to focus on multiple cue animals like puppies, bear cubs, lizards, etc. apart from kitties. Blockchain Cuties is a dApp that is accessible using multiple Blockchain platforms like Ethereum, NEO, TRON, etc., unlike CryptoKitties which favors Ethereum only.

❖ **Uses of dApps** :

Some examples of practical uses for dApps include :

- **Financial services** :

dApps can be used to facilitate peer-to-peer financial transactions, such as the exchange of currencies or the transfer of assets.

- **Supply chain management** :

dApps can be used to track the movement of goods through a supply chain, ensuring transparency and accountability.

- **Identity verification :**

dApps can be used to securely store and verify identity information, such as for voter rolls or passport applications.

- **Real estate :**

dApps can be used to facilitate the buying and selling of real estate directly between buyer and seller, as well as the tracking of property ownership and related documentation such as deeds.

- **Healthcare :**

dApps can be used to store and track healthcare records, as well as to facilitate the communication and collaboration of healthcare professionals.

- **Education :**

dApps can be used to create decentralized learning platforms, allowing students and teachers to interact and collaborate directly without the need for intermediaries.

- **Social media :**

dApps can be used to create decentralized social media platforms, allowing users to interact and share content without the need for a central authority.

- **Predictive markets :**

dApps can be used to create decentralized platforms for predictive markets, allowing users to make predictions on a variety of topics and potentially earn rewards for accurate predictions.

❖ Advantages of dApps

The following are some of the advantages of dApps :

1. **Fault tolerance :**

As dApps work on a decentralized platform, if a single node is working the network will be still; available but the performance will be severely downgraded.

2. **Privacy :**

Users don't need to submit real-world identity or any personal information to use any app-specific functionality.

3. **Data integrity :**

Data stored on the blockchain is immutable and tamper-proof due to the use of consensus algorithms. Hackers cannot forge transactions and the data stored on the blockchain is resistant to change.

4. **Flexible platform :**

The Ethereum platform provides a flexible environment for easy development of dApps.

5. **Verifiable behavior :**

Smart contracts can be analyzed and are guaranteed to execute in predictable ways without a need from monitoring or involvement from a central authority.

❖ **Disadvantages of dApps**

The following are some of the drawbacks of dApps :

1. **Performance Overhead :**

There is a lot of performance overhead to achieve the level of security, transparency, and integrity that Ethereum desires. Even the proof-of-work takes a lot of time and computational resources.

2. **Maintenance :**

dApps are hard to maintain, debug and update, as the code or data published to the blockchain are hard to modify and all bug fixes require consensus from all the peers on the network which is in most cases hard to achieve in a timely manner.

3. **Scalability :**

Decentralized networks are hard to scale than centralized networks.

4. **User experience :**

It is quite hard for the developers to design a user-friendly dApp as it requires users to use the public and private keys for login instead of the username and password that is being used in centralized applications.

5. **Centralization :**

Developing user-friendly, developer-friendly applications on top of Ethereum may end up developing a centralized service. Centralization may eliminate all the good features of the blockchain over the traditional model.

6. **Network Congestion :**

There is an issue of network congestion while using a dApp as one dApp uses too many computational resources, and the entire network gets backed up. If the number of transactions coming in is more than the 10-15 transactions that are being processed in a second then unconfirmed transactions will pile up.

Exercises

❑ **MCQs :**

1. What is a dApp in blockchain ?
   A. A decentralized application built on top of a blockchain
   B. An encryption algorithm used to secure data on the network
   C. A consensus mechanism used to validate transactions
   D. None of the above

2. What is a DAO in blockchain ?
   A. A Decentralized Autonomous Organization, run by smart contracts and governed bytoken holders
   B. A Distributed Application Organization, building decentralized applications ontop of blockchains
   C. A Decentralized Asset Offering, where new cryptocurrencies are sold toinvestors
   D. None of the above
3. What is a dApp ?
   A. A blockchain network
   B. Type of cryptocurrency
   C. Decentralized application
   D. Hardware component
4. Smart Contract characteristics do not include :
   A. Alterable
   B. Fast and cost-effective
   C. A high degree of accuracy
   D. Transparency
5. A contract in size is restricted to,
   A. 24576 Bytes
   B. 1 Kilo Bytes
   C. 23575 Bytes
   D. No limit
6. What is gas in Ethereum ?
   A. The fuel that powers smart contracts and transactions
   B. The consensus mechanism used by Ethereum
   C. The encryption algorithm used by Ethereum
   D. None of the above

❑ **Questions :**

1. What is a DAO ?
2. What is the Purpose of a DAO ?
3. What are dApps used for ?
4. How are dApps different from normal apps ?
5. Explain advantages and disadvantages of dApps.
6. Write difference between DAO and traditional organization.
7. Explain Smart contract.
8. Discuss types of decentralization in blockchain
9. Write various applications of smart contract.
10. What is the difference between a centralized and decentralized App ?

* * *