Name of Faculty : Munish Kumar	Discipline : Computer Engg.
Semester : 5th	Subject : Block Chain (MOOC)

❖ What is Blockchain?

Block chain is a distributed digital ledger technology (DLT) that stores data in a chain of blocks.

- Each block contains a set of transactions or information.
- Once data is added to a block, it is extremely difficult to alter, making it secure and tamper-proof.
- Blocks are linked using cryptography, forming a continuous chain — hence the name blockchain.
- It operates on a decentralized network (no central authority), where multiple participants (nodes) maintain and verify the same copy of the ledger.
- This ensures transparency, security, and trust among users.

Key Features:

- ◆ Decentralization – No single central authority controls it.
- ◆ Immutability – Data once recorded cannot be easily changed.
- ◆ Transparency – All participants can view transactions.
- ◆ Security – Cryptographic methods protect the data.
- ◆ Consensus Mechanisms – Transactions are validated by network agreement (e.g., Proof of Work, Proof of Stake)

History of Blockchain:

The history of blockchain is tied closely to the development of cryptocurrencies, but it has grown far beyond that.

■ **1991 – Early Concept**

Stuart Haber and W. Scott Stornetta introduced the idea of using cryptographically secured chains of blocks to store digital timestamps to prevent tampering.

■ **2008 – Birth of Blockchain**

A person or group under the pseudonym Satoshi Nakamoto introduced Bitcoin, the first practical use of blockchain.

The whitepaper “Bitcoin: A Peer-to-Peer Electronic Cash System” described blockchain as the underlying technology.

■ **2009 – Bitcoin Launch**

The first Bitcoin blockchain went live.

It was used to record peer-to-peer cryptocurrency transactions.

■ **2015 – Ethereum Era**

Vitalik Buterin launched Ethereum, expanding blockchain's use beyond money.

Introduced smart contracts, enabling decentralized applications (DApps).

■ **2017 – ICO & Blockchain Boom**

Initial Coin Offerings (ICOs) became popular.

Blockchain adoption spread into industries like finance, supply chain, healthcare, and identity management.

■ **2020 onwards – Modern Blockchain**

Rise of Decentralized Finance (DeFi), NFTs (Non-Fungible Tokens), and enterprise blockchain platforms.

Governments and companies started exploring Central Bank Digital Currencies (CBDCs) and private blockchains**.**

✅**In simple words:**
Blockchain started as a way to secure digital records (1991), became famous with Bitcoin (2009), expanded into smart contracts and decentralized apps (2015), and today is a foundation for modern innovations like DeFi, NFTs, and digital identity.

❖ Blockchain is a distributed database. How it differ from traditional database?

Blockchain as a Distributed Database

- In a traditional database, data is stored in centralized servers and managed by a single authority (e.g., bank, company).
- In blockchain, data is stored across a network of computers (nodes), and each node keeps a copy of the ledger.
- Instead of one central admin, blockchain uses consensus mechanisms (like Proof of Work or Proof of Stake) to validate data.

Aspect	Blockchain (Distributed Ledger)	Traditional Database
Control	Decentralized (no single owner; multiple participants share control)	Centralized (controlled by a single authority/organization)
Structure	Data stored in blocks linked in a chain	Data stored in tables (rows & columns)
Data	Immutable – once data is written, it	Mutable – data can be updated,

Aspect	Blockchain (Distributed Ledger)	Traditional Database
Modification	cannot be changed or deleted	deleted, or modified easily
Security	Secured using cryptography & consensus; tamper-resistant	Relies on access control, passwords, firewalls; can be hacked if central server is breached
Transparency	Public blockchains allow anyone to view data (high transparency)	Only admins or authorized users can view data
Validation	Consensus mechanism (Proof of Work, Proof of Stake, etc.)	Controlled by a central database administrator
Performance	Slower (due to consensus & cryptographic verification)	Faster (optimized for quick queries and updates)
Fault Tolerance	Very high – since copies exist on many nodes, failure of one node doesn't stop the system	Lower – if the central server fails, database becomes unavailable
Use Cases	Cryptocurrencies (Bitcoin, Ethereum), Supply Chain, Healthcare, Voting, Identity Management	Banking systems, ERP systems, Websites, Enterprise applications

Types of Blockchain

Blockchain technology has evolved into a versatile tool with various applications across industries. Understanding the different types of blockchain is essential for selecting the right solution for specific needs. Broadly categorized into public, private, consortium, and hybrid blockchains, each type offers unique characteristics, benefits, and use cases. Public blockchains enable open access and decentralization, while private blockchains prioritize security and control. Consortium blockchains serve collaborative networks, and hybrid blockchains combine features of both public and private models. This article discusses types of blockchain in detail.

➢ Permissionless Blockchain

A permissionless blockchain is a type of blockchain network that allows anyone to participate in the network without requiring special permissions or approvals.

1. **Open Access**: Anyone can join the network, validate transactions, and contribute to the blockchain. This openness fosters a decentralized environment where no single entity controls the network.
2. **Decentralization**: Permissionless blockchains operate on a decentralized network of nodes, which helps to distribute power and reduce the risk of censorship or manipulation by any single party.
3. **Consensus Mechanisms**: These blockchains typically use consensus algorithms such as network participants' Proof of Stake (PoS) to validate transactions and secure the

network. Participants compete to solve complex mathematical problems (in the case of PoW) or stake their own tokens (in PoS) to earn the right to validate new blocks.
4. **Transparency**: All transactions on a permissionless blockchain are recorded on a public ledger, allowing anyone to view transaction history and verify data integrity.
5. **Anonymity**: While transactions are transparent, participants often remain pseudonymous. Users are identified by their public keys rather than personal information, providing a layer of privacy.

➢ Permissioned Blockchain

A permissioned blockchain is a type of blockchain network that restricts access and participation to a select group of authorized users. Unlike permissionless blockchains, where anyone can join and validate transactions, permissioned blockchains require participants to obtain permission before they can access the network or perform certain actions.

1. **Access Control**: Only authorized participants can join the network, ensuring that all nodes are known and vetted. This allows for greater control over who can validate transactions and access data.
2. **Centralized Governance**: Typically governed by a consortium of organizations or a central authority, which makes decisions about network rules and policies.
3. **Enhanced Privacy**: Transactions and data are often more private, as sensitive information can be kept off-chain or shared only among authorized parties.
4. **Customizable Protocols**: Organizations can customize consensus mechanisms and other protocols to meet their specific needs and requirements.

Types of Blockchain

Here are the 4 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.

1. As the name is public this blockchain is open to the public, which means it is not owned by anyone.
2. Anyone having internet and a computer with good hardware can participate in this public blockchain.
3. All the computers in the network hold the copy of other nodes or blocks present in the network
4. In this public blockchain, we can also perform verification of transactions or records

Advantages:

1. **Trustable:** There are algorithms to detect fraud. Participants need not worry about the other nodes in the network.
2. **Secure:** This blockchain is large as it is open to the public. In a large size, there is a greater distribution of records.

3. **Anonymous Nature:** It is a secure platform to make your transaction properly at the same time, you are not required to reveal your name and identity to participate.
4. **Decentralized:** There is no single platform that maintains the network, instead every user has a copy of the ledger.

Disadvantages:

1. **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.
2. **Energy Consumption:** Proof of work is highly energy-consuming. It requires good computer hardware to participate in the network.
3. **Acceptance:** No central authority is there so governments are facing the issue of implementing the technology faster.

Use Cases:

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

1. These are not as open as a public blockchain.
2. They are open to some authorized users only.
3. These blockchains are operated in a closed network.
4. In this few people are allowed to participate in a network within a company/organization.

Advantages:

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

Disadvantages:

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

Use Cases:

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

3. Hybrid Blockchain

It is the mixed content of the private and public blockchain, where some part is controlled by some organization and other makes are made visible as a public blockchain.

1. It is a combination of both public and private blockchain.
2. Permission-based and permissionless systems are used.
3. User access information via smart contracts
4. Even if a primary entity owns a hybrid blockchain it cannot alter the transaction

Advantages:

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

Disadvantages:

1. **Efficiency:** Not everyone is in a position to implement a hybrid Blockchain. The organization also faces some difficulty in terms of efficiency in maintenance.
2. **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.
3. **Ecosystem:** Due to its closed ecosystem this blockchain lacks the incentives for network participation.

Use Case:

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

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

Advantages:

1. **Speed:** A limited number of users make verification fast. The high speed makes this more usable for organizations.
2. **Authority:** Multiple organizations can take part and make it decentralized at every level. Decentralized authority, makes it more secure.

3. **Privacy:** The information of the checked blocks is unknown to the public view. But any member belonging to the blockchain can access it.
4. **Flexible:** There is much divergence in the flexibility of the blockchain. Since it is not a very large decision can be taken faster.

Disadvantages:

1. **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.
2. **Transparency:** It can be hacked if the organization becomes corrupt. Organizations may hide information from the users.
3. **Vulnerability:** If a few nodes are getting compromised there is a greater chance of vulnerability in this blockchain

Use Cases:

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

❖ What Is Ethereum (ETH)?

Ethereum is an open-source software platform based on Blockchain technology that enables developers to build and deploy decentralized applications (i.e., applications that are not controlled by a single entity). You may construct a decentralized application in which the participants are the ones who make the decisions.

❖ What is the difference between Bitcoin blockchain and Ethereum?

Although bitcoin and ether are both digital currencies, the Ethereum blockchain differs significantly from the Bitcoin Blockchain. Bitcoin was created solely for the purpose of being a digital currency. whereas Ethereum blockchain is a broader version of blockchain technology. And it is a distributed ledger technology that organizations are using to create new services, however, Ethereum is much more stable than bitcoin.

❖ What Is Hashing in Blockchain?

The process of making an input item of any length represents an output item of a fixed length is referred to as hashing in the blockchain. Take, for example, the use of blockchain in cryptocurrencies, where transactions of varying lengths are run through a given hashing algorithm and all produce a fixed-length performance.

❖ What are the benefits of Blockchain Technology?

Blockchain technology has the following benefits:

- Blockchain technology employs advanced security compared to other networks or record-keeping systems. Prior to being recorded, all transactions must be agreed upon. A transaction is encrypted and connected to the previous transaction after it has been authorized.

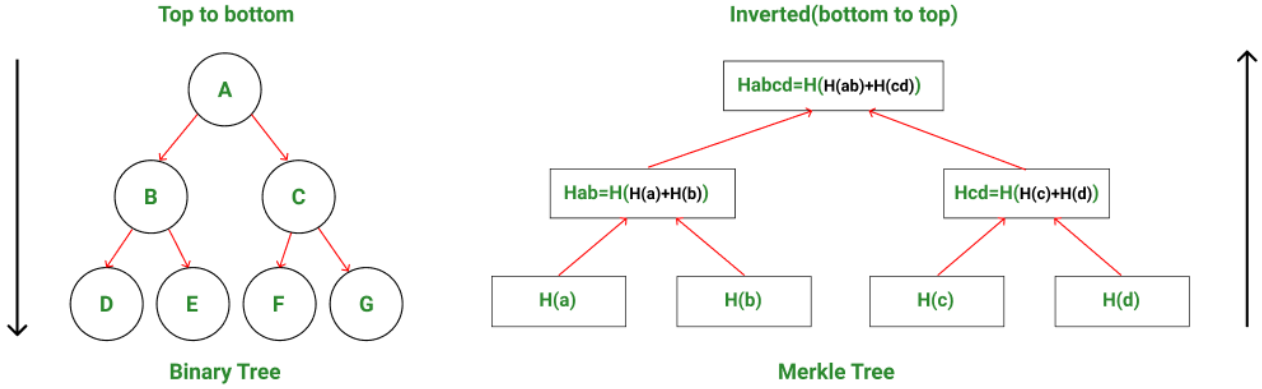
- Blockchain offers transparency. As one of the major problems in the new industry is transparency. An organization may use blockchain to create a completely decentralized network that eliminates the need for a centralized authority, increasing the system's transparency.
- Blockchain helps in reducing costs. Organizations will save a lot of money by using the blockchain instead of paying third-party vendors.
- Blockchain automates time-consuming processes in order to increase performance. With the aid of automation, it also eliminates human errors. As a result, blockchain increases efficiency and speed.
- The blockchain allows for immediate traceability. It generates an audit trail that records an asset's provenance at each stage of its journey which prevents fraud.

❖ What is meant by ledger in blockchain? What Is a Cryptocurrency Public Ledger?

In simple word the word ledger means records. A cryptocurrency public ledger is a record-keeping system. The ledger maintains participants' identities anonymously, their respective cryptocurrency balances, and a record of all the genuine transactions executed between network participants.

❖ How Do Merkle Trees Work?

- 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

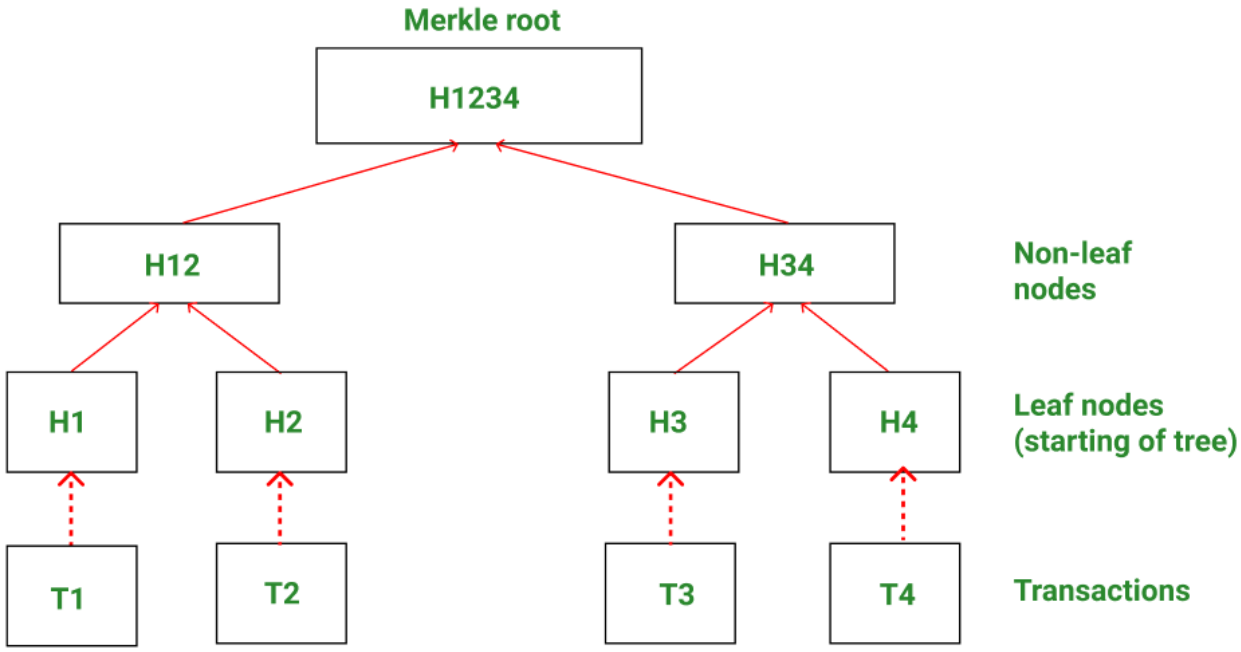
hash of H1 and H2 will be computed to form H12. Similarly, H34 is computed. Values H12 and H34 are parent nodes of H1, H2, and H3, H4 respectively. These are non-leaf nodes.

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.

❖ what is consensus mechanism in blockchain? Explain various types of consensus mechanism in details with examples

Consensus mechanisms are the protocols, algorithms, or other computer systems that allow cryptocurrencies to work. They are systems of agreement that determine the validity of transactions and governance of the blockchain. There are different types of consensus mechanisms with various benefits and drawbacks.

1. Proof of Work (PoW)

Proof of Work is the first and most well-known consensus mechanism, introduced with Bitcoin in 2009. In PoW, miners compete to solve very complex mathematical puzzles using high computational power. The miner who solves the puzzle first gets the right to add the block to the blockchain and is rewarded with newly generated coins and transaction fees. This mechanism is highly secure and decentralized, but it requires enormous amounts of electricity and computational resources, making it less energy efficient and slower for processing transactions.

2. Proof of Stake (PoS)

Proof of Stake is an alternative to PoW that aims to reduce energy consumption. In PoS, validators are chosen to create or validate blocks based on the number of coins they stake (lock up) as collateral. The more coins a participant stakes, the higher their chances of being selected to validate the next block. If a validator acts dishonestly, they lose part of their stake, ensuring security. PoS is much more energy efficient and faster than PoW, but it is sometimes criticized because those with more wealth (larger stakes) have more power in the system.

3. Proof of Activity (PoA – Proof of Activity, not Authority)

Proof of Activity is a hybrid model that combines features of both Proof of Work and Proof of Stake. At the beginning of block creation, miners use Proof of Work to start the process. However, instead of completing it alone, validators selected through Proof of Stake must sign and verify the block. This hybrid approach increases security by making it difficult for a single party to attack the network. Although it offers better protection compared to pure PoW or PoS, it is more complex and still requires some computational energy due to the PoW component.

4. Proof of Burn (PoB)

Proof of Burn is based on the idea of sacrificing coins to demonstrate commitment to the network. In this mechanism, validators “burn” coins by sending them to an address that makes them unusable forever. By burning coins, participants prove their dedication and in return get the chance to validate new blocks and earn rewards. This reduces energy consumption compared to PoW but can decrease the liquidity of the currency since coins are permanently destroyed. Slimcoin is an example of a blockchain that uses Proof of Burn.

5. Proof of Authority (PoA – Proof of Authority)

Proof of Authority works differently from PoW and PoS because it relies on identity and reputation rather than computational power or stake. In this system, only a small group of approved validators (such as trusted companies or individuals) are allowed to validate

transactions and create new blocks. Since there are fewer validators, transactions are processed very quickly and efficiently with minimal energy usage. However, this system is less decentralized and is more suited for private or enterprise blockchains where trust among participants already exists, such as in supply chain management.

6. Proof of Importance (PoI)

Proof of Importance is a unique consensus mechanism introduced by the NEM blockchain. It is similar to Proof of Stake but with additional factors that determine a participant's importance score. Along with the number of coins staked, PoI also considers transaction frequency, network activity, and the overall contribution of a participant to the ecosystem. This encourages not only holding coins but also actively engaging in transactions and supporting the network. It provides a fairer system by rewarding active participants instead of only wealthy stakeholders, though it is more complex to implement.

7.Proof of Elapsed Time (PoET)

Proof of Elapsed Time is a consensus mechanism designed by Intel to provide a highly energy-efficient alternative to Proof of Work. Instead of requiring miners to solve difficult mathematical puzzles, PoET uses a lottery-like system based on trusted hardware. Each participant in the network is assigned a random waiting time by a secure hardware module such as Intel's Software Guard Extensions (SGX). The node with the shortest waiting time "wakes up" first and gets the right to create the next block. Other nodes can then verify that the leader was chosen fairly. This makes PoET very efficient because it avoids wasting electricity on computational puzzles, unlike Proof of Work. However, PoET depends heavily on specialized hardware, which makes it less decentralized and more suitable for private or permissioned blockchain networks. A well-known example of PoET in use is the Hyperledger Sawtooth platform developed by Intel and the Linux Foundation.

❖ What is a desktop wallet?

Desktop wallets are programs which are run from your desktop or laptop computer. They provide a streamlined, easy-to-use interface for users to interact with their crypto holdings. Unlike web or exchange wallets which are always online, desktop wallets only connect to the internet when necessary for completing transactions. They are most often non-custodial, which means the wallet owner bears sole responsibility for safeguarding their private keys.

❖ How a Desktop Wallet Works

A desktop wallet is a type of cryptocurrency wallet that you install and run directly on your personal computer or laptop. It stores your private keys (the digital keys that allow you to access and spend your crypto) locally on your hard drive rather than on a centralized server.

Here's how it works:

- Installation: You download and install the wallet software (e.g., Electrum, Exodus, Bitcoin Core).

- Private Key Storage: The wallet generates and stores your private keys securely on your computer. These keys never leave your device, giving you full control.
- Transactions: When you want to send crypto, the wallet signs the transaction with your private key and broadcasts it to the blockchain network.
- Receiving Funds: The wallet provides you with a public address (like your account number) which others can use to send you cryptocurrency.
- Backup: Most desktop wallets give you a recovery phrase (seed phrase) that can restore your wallet if your computer is lost or damaged.

Benefits of Desktop Wallets

- Full Control: You own and control your private keys (not a third party).
- Security: More secure than online/web wallets since keys are stored locally, not on a central server.
- Convenience: Easy to use for daily transactions directly from your computer.
- Variety of Features: Many desktop wallets support multiple cryptocurrencies, portfolio tracking, and sometimes built-in exchanges.
- Offline Storage Option: Can be used in combination with cold storage methods for extra security.

Drawbacks of Desktop Wallets

- Vulnerability to Malware: If your computer is infected with a virus, keylogger, or malware, your wallet can be hacked.
- Not Portable: Only accessible on the computer where it is installed (unless you use backup/recovery).
- Dependence on Device Security: If your laptop/PC is stolen, damaged, or compromised, you risk losing your funds unless you backed up your seed phrase.
- Less Convenient than Mobile Wallets: Not ideal for payments on the go.
- Requires Updates: Wallet software needs regular updates to stay secure and compatible with blockchain networks.

❖ What is an App-Based Wallet?

An App-based wallet is a type of cryptocurrency wallet that you install as a mobile application on your smartphone (Android or iOS). It allows you to store, send, receive, and manage cryptocurrencies directly from your mobile device.

Unlike desktop wallets (installed on PCs), app-based wallets are designed for convenience and portability. Your private keys are stored securely on the mobile device itself, sometimes encrypted or protected with a password, fingerprint, or face ID.

Examples of App-Based Wallets

- Trust Wallet – A popular multi-currency wallet that supports thousands of cryptocurrencies and NFTs.
- MetaMask (Mobile App) – Mainly used for Ethereum and other EVM-compatible blockchains, supports DApps.

- Coinbase Wallet (not exchange) – A mobile wallet that lets you control your private keys and access DeFi apps.
- Exodus Mobile Wallet – Multi-currency wallet with a simple interface and built-in exchange feature.
- Mycelium Wallet – A mobile wallet known for strong Bitcoin support and advanced features.

❖ What is Browser or Web based wallet. Explain with examples. Is MetaMask a web based wallet?

A browser-based wallet or wallet service is an online account with an external provider where bitcoins can be stored. Examples include accounts on currency exchange Markets, online Services and with ecommerce transaction processors.

With 30 million users, MetaMask is a popular cryptocurrency wallet application available in both web browsers and mobile devices as an app.

❖ What is MetaMask?

MetaMask is a cryptocurrency wallet and gateway to blockchain applications (Web3).

- It is available as a browser extension (Chrome, Firefox, Edge, Brave) and a mobile app (Android, iOS)
- Mainly used for Ethereum and Ethereum-compatible blockchains (BNB Smart Chain, Polygon, Avalanche, etc.).
- It lets users store, send, and receive cryptocurrencies and tokens (ERC-20, ERC-721 NFTs, etc.).
- It also allows direct connection to Decentralized Apps (DApps) such as DeFi platforms, NFT marketplaces, and games.

In simple terms: MetaMask is like a digital wallet + login system for Web3 apps.

Steps to Create an Account in MetaMask

On Browser Extension (Desktop):

- Install Extension:

✓ Go to MetaMask official website and download the extension for Chrome/Brave/Firefox/Edge.
✓ Add it to your browser.

- Launch MetaMask:

✓ Click on the MetaMask icon in your browser toolbar.
✓ Click on "Get Started".

- Create a Wallet:

✓ Choose "Create a Wallet" (if you are new) or "Import Wallet" (if you already have one).

◆ Set a Password:

✓ Create a strong password to secure your wallet.
✓ This password protects your wallet on your device, not the blockchain.

◆ Backup Seed Phrase:

✓ MetaMask will show you a 12-word Secret Recovery Phrase (also called seed phrase).
✓ Write it down on paper and store it safely offline.
✓ Do NOT share this phrase with anyone – whoever has it can access your wallet.

◆ Confirm Seed Phrase:

✓ Re-enter the words in correct order to verify.

◆ Account Ready:

✓ Your MetaMask wallet is now created.
✓ You will see your Ethereum account address, which you can use to send/receive crypto.

❖ What is faucet in wallet? Briefly discuss the use of faucet to fund wallet.

A faucet in cryptocurrency is a platform or feature that gives out small amounts of free crypto tokens to users. It is usually used for testing purposes on blockchain test networks (testnets).

In the context of a wallet, a faucet helps users receive a little amount of cryptocurrency so they can try out transactions, test smart contracts, or interact with DApps without spending real money.

Example: On the Ethereum Goerli testnet, a faucet can give you free test ETH (not real ETH) that you can use to test smart contracts in your MetaMask wallet.

➢ Use of Faucet to Fund Wallet

◆ Testing Transactions: Developers use faucets to get free test coins and practice sending, receiving, or deploying smart contracts without risking real funds.
◆ Learning Purpose: New users can understand how a wallet works by using faucet tokens before handling real crypto
◆ DApp Development: Developers building decentralized apps (DeFi, NFTs, etc.) need testnet tokens from faucets to run experiments on blockchains like Ethereum testnets, Binance Smart Chain testnet, or Polygon testnet.
◆ Network Onboarding: Faucets make it easier for beginners to start using blockchain wallets without buying crypto from exchanges.

❖ How do you transfer your existing ETH and tokens to MetaMask?

Transferring ETH or tokens to your MetaMask wallet is similar to sending crypto from one wallet or exchange to another. The key is using your MetaMask wallet address as the destination.

Step 1: Install and Set Up MetaMask

- ✓ Ensure MetaMask is installed on your browser (Chrome, Firefox, Edge) or mobile app (Android/iOS).
- ✓ Set up your wallet and securely back up your seed phrase.

Step 2: Find Your MetaMask Wallet Address

- ✓ Open MetaMask.
- ✓ Select the account you want to use.
- ✓ Copy your public Ethereum address (it starts with 0x…).
- ✓ This is the address where you will receive ETH or tokens.

Step 3: Send ETH or Tokens from Another Wallet or Exchange

- ✓ Go to your current wallet or exchange where your ETH or tokens are stored.
- ✓ Choose the "Send" or "Withdraw" option.
- ✓ Paste your MetaMask address in the recipient field.
- ✓ Enter the amount of ETH or token you want to send.
- ✓ Review the network fees (gas fees) and make sure you are using the Ethereum network if sending ETH or ERC-20 tokens.

Step 4: Confirm the Transaction

- ✓ Confirm the transaction in your sending wallet or exchange.
- ✓ Wait for the transaction to be processed on the Ethereum blockchain. This can take a few seconds to a few minutes depending on network congestion.

Step 5: Check Your MetaMask Wallet

- ✓ Open MetaMask.
- ✓ ETH and any ERC-20 tokens sent should appear in your wallet after the transaction is confirmed.
- ✓ If a token doesn't show automatically, you may need to add the token manually by pasting its contract address under "Add Token."

❖ What is Ethereum?

Ethereum is a decentralized blockchain platform that allows developers to build and run smart contracts and decentralized applications (DApps).

- ◆ It was proposed in 2013 by Vitalik Buterin and launched in 2015.
- ◆ Unlike Bitcoin, which is primarily a digital currency, Ethereum is a platform for programmable money and applications.
- ◆ The native cryptocurrency of Ethereum is called Ether (ETH), which is used to pay for transactions, smart contract execution, and fees on the network.
- ◆ In simple terms: Ethereum is like a world computer where code runs exactly as programmed without downtime, fraud, or third-party interference.

❖ How Ethereum Works

1. Ethereum Blockchain

Ethereum has its own blockchain where all transactions and smart contracts are recorded.

- ✓ Each block contains transactions, a timestamp, and a reference to the previous block.
- ✓ Miners (or validators in Ethereum 2.0) validate and add blocks to the chain using consensus mechanisms (PoW before Ethereum 2.0, PoS after).

2. Ether (ETH)

Ether is the fuel of Ethereum:

- ✓ It is used to pay gas fees required to execute transactions and smart contracts.
- ✓ Gas ensures that network resources are used efficiently and prevents spam.

3. Smart Contracts

Smart contracts are self-executing programs stored on the blockchain.

- ✓ They automatically execute actions when predefined conditions are met.
- ✓ No intermediaries are needed, reducing cost and increasing trust.
- ✓ Example: A decentralized crowdfunding contract can automatically release funds to a project only when a target is reached.

4. Ethereum Virtual Machine (EVM)

The EVM is a decentralized computer that executes smart contracts.

- ✓ Every node in the Ethereum network runs the EVM to verify transactions
- ✓ This ensures that contracts execute the same way on all nodes, maintaining consistency.

5. Decentralized Applications (DApps)

Ethereum allows developers to build DApps, which are applications that run on the blockchain.

- ✓ Examples include DeFi platforms (Uniswap, Aave), NFT marketplaces (OpenSea), and games (Axie Infinity).

❖ How Does Ethereum Make Money? Is Ethereum a Cryptocurrency?

Ethereum is not a centralized organization that makes money. Validators who participate in the Ethereum network earn ETH rewards for their contributions.
The Ethereum platform has a native cryptocurrency, known as ether, or ETH. Ethereum itself is a blockchain technology platform that supports a wide range of decentralized applications (dApps), including cryptocurrencies. The ETH coin is commonly called Ethereum, although the distinction remains that Ethereum is a blockchain-powered platform, and ether is its cryptocurrency.

❖ How do you write a smart contract in Hyperledger fabric?

A smart contract in Hyperledger Fabric is a program, called chaincode. Chaincode can be written in Go, JavaScript (node. js), and eventually other programming languages such as Java that implement a prescribed interface. Chaincode runs in a secured Docker container isolated from the endorsing peer process.

❖ How the transaction validation takes place in Hyperledger Fabric?.

In the validation phase, a transaction is considered valid if the version of each key present in the read set of the transaction matches the version for the same key in the world state – assuming that all the preceding valid transactions, including the preceding transactions in the same block, are committed.

❖ What is Hyperledger?

Hyperledger is an open-source collaborative effort hosted by the Linux Foundation, aimed at advancing cross-industry blockchain technologies. It is designed to support the collaborative development of blockchain-based solutions, focusing primarily on enterprise needs. Unlike public blockchains like Bitcoin or Ethereum, Hyperledger frameworks enable the creation of permissioned blockchains, which offer greater privacy, scalability, and control over data.

Key Features

1. **Modular Architecture**: Hyperledger offers a modular framework, allowing developers to customize their blockchain solutions based on specific business requirements.
2. **Multiple Frameworks**: It includes several frameworks like **Hyperledger Fabric**, **Hyperledger Sawtooth**, and **Hyperledger Iroha**, each catering to different use cases and industries.
3. **Permissioned Networks**: Hyperledger allows organizations to create permissioned networks where participants can be verified, enhancing security and privacy.
4. **Smart Contracts**: The platform supports smart contracts (or chaincode) that automate processes and enable complex business logic within transactions.

❖ What is Ethereum?

Ethereum is a decentralized, open-source blockchain platform that enables developers to build and deploy smart contracts and decentralized applications (DApps). Launched in 2015 by Vitalik Buterin and others, Ethereum extends the capabilities of blockchain beyond simple transactions by allowing programmable contracts that automatically execute when predefined conditions are met.

Key Features

1. **Smart Contracts**: These self-executing contracts with the terms directly written into code facilitate trustless transactions without intermediaries, allowing for automation and efficiency.
2. **Decentralized Applications (DApps)**: Ethereum provides a framework for building DApps that run on a peer-to-peer network, eliminating reliance on central authorities.
3. **Ethereum Virtual Machine (EVM)**: The EVM enables the execution of smart contracts and ensures that all transactions are executed consistently across the network.
4. **Cryptocurrency (Ether)**: Ether (ETH) is the native cryptocurrency of the Ethereum network, used to pay for transaction fees and computational services on the platform.

Hyperledger vs Ethereum

Here are the differences between Hyperledger and Ethereum:

	Hyperledger	Ethereum
Definition	An open-source collaborative framework for enterprise blockchain solutions.	A decentralized platform for building smart contracts and decentralized applications (DApps).
Type of Network	Permissioned (private) networks for businesses and organizations.	Permissionless (public) network allowing anyone to participate.
Consensus Mechanism	Supports multiple consensus algorithms (e.g., Raft, PBFT) tailored for enterprise needs.	Uses Proof of Work (PoW) and is transitioning to Proof of Stake (PoS) for security and scalability.
Smart Contracts	Known as "chaincode," they can be written in multiple programming languages.	Written in Solidity, a specialized programming language for Ethereum.
Privacy	Offers fine-grained privacy and data confidentiality for transactions.	Limited Privacy
Scalability	Highly scalable due to its permissioned architecture and modular design.	Scalability is a challenge, though solutions like Layer 2 (e.g., rollups) are being developed.

	Hyperledger	Ethereum
Use Cases	Primarily targeted at industries such as finance, supply chain, healthcare, and government.	Popular in decentralized finance (DeFi), gaming, NFTs, and general-purpose DApps.
Governance	Governed by the Hyperledger community and managed by the Linux Foundation.	Governed by the Ethereum community, with decisions often made through community proposals (EIPs).
Transaction Speed	Generally faster due to reduced node participation in consensus.	Slower transaction speeds due to public consensus requirements, though improvements are being made.
Native Cryptocurrency	Does not have a native cryptocurrency; focuses on enterprise use cases.	Ether (ETH) is the native cryptocurrency, used for transaction fees and network participation.

❖ What is Hyperledger Fabric? Is Hyperledger Fabric a private blockchain? Explain.

Hyperledger Fabric platform is an open source blockchain framework hosted by The Linux Foundation. It has an active and growing community of developers. Permissioned-Fabric networks are permissioned, meaning all participating member's identities are known and authenticated.

Hyperledger Fabric is one of the blockchain projects within Hyperledger. Like other blockchain technologies, it has a ledger, uses smart contracts, and is a system by which participants manage their transactions. Where Hyperledger Fabric breaks from some other blockchain systems is that it is private and permissioned.

❖ How blockchain can be used in cross border payments? Explain

Blockchain can significantly improve cross-border payments, which are traditionally slow, expensive, and dependent on multiple intermediaries like banks and payment processors. By using a decentralized ledger, blockchain allows all participants in the network to access the same transaction records in real time, eliminating the need for intermediaries to verify transactions. Payments can be made using cryptocurrencies such as Bitcoin or Ether, or stablecoins like USDT and USDC, which can be converted back to local currencies as needed. Smart contracts further enhance the system by automating payments once predefined conditions are met, such as releasing funds automatically when goods are shipped. Blockchain enables cross-border transactions to settle in minutes instead of days, while providing transparency, security through cryptography, and reduced transaction fees. Platforms like Ripple (XRP), Stellar (XLM), and JPM Coin are examples of blockchain-

based systems facilitating fast, secure, and low-cost international payments. In essence, blockchain simplifies international money transfers, making them faster, cheaper, and more transparent, while also promoting financial inclusion for people without traditional banking access.

❖ How blockchain can be used for efficient implementation of know your customers (KYC) process?

Blockchain can make the Know Your Customer (KYC) process more efficient, secure, and cost-effective for financial institutions. Traditionally, KYC involves collecting, verifying, and storing customer information for each bank or service provider separately, which is time-consuming, redundant, and prone to errors. By using blockchain, customer identity data can be stored on a shared, tamper-proof distributed ledger, where authorized institutions can access and verify the information with the customer's consent. Once a customer's identity is verified and recorded on the blockchain, other banks or financial services can reuse this verified data without repeating the process. This reduces duplication, speeds up onboarding, and lowers operational costs. Additionally, blockchain ensures data integrity and security, as the information is encrypted and immutable, minimizing the risk of fraud or identity theft. Several platforms are exploring blockchain-based KYC solutions, allowing seamless, transparent, and customer-controlled identity verification across multiple institutions.

❖ How blockchain can be used in food security and agriculture?

Blockchain can play a significant role in improving food security and agriculture by providing transparency, traceability, and accountability across the supply chain. In traditional systems, it is often difficult to track the origin of food, verify its quality, or monitor storage conditions, which can lead to contamination, fraud, or wastage. By recording each step of the agricultural supply chain on a blockchain—such as planting, harvesting, processing, transportation, and sale—stakeholders can trace food products from farm to table. This ensures consumers know exactly where their food comes from and whether it meets safety standards. Farmers can also benefit by gaining fair pricing and faster payments through smart contracts, while governments and organizations can monitor food distribution efficiently. Additionally, blockchain can help reduce fraud, prevent counterfeit agricultural products, and improve crop insurance processes by providing immutable records of production and delivery. Platforms like IBM Food Trust and TE-FOOD are already using blockchain to enhance food traceability and safety globally.