**Blockchain**

**Applications of Blockchain**

**Module A**

* What is Blockchain?
* Hashing Algorithm
* Immutable Ledger
* Distributed P2P network
* Blockchain Mining
* Consensus Protocol

**Module B**

* Bitcoin
* Bitcoin vs Blockchain
* Bitcoin Monetary Policy
* miningworks
* Nonce
* CPU vs GPU vs ASCI
* Mining Pool
* mining of transaction
* UTXOs and transaction ,Transaction Fee
* Wallets
* Private Key and Public Key
* SegWit , Hierarchically Deterministic Waller

**Module C**

* Ethereum, Ethereum Nodes
* Types of Accounts in Ethereum
* Decentralized Applications (Dapps)
* Ethereum Virtual Machine(EVM)
* Ethereum Gas , Gas Price & Gas Limit
* Decentralized Autonomous Organization (DAO) Attack
* Hard Fork & Soft Fork
* Initial Coin Offering (ICO)
* Ethereum 2.0 (Serenity)
* Sharding

Block Chain is a disrupt technology

বিতরণ অপরিবর্তনীয়/ unchanged/ fixed সম্পূর্ণ স্বচ্ছ



Blockchain is a **distributed, immutable** ledger that is **completely transparent.**



Internet 🡪 communication

Block chain 🡪 Trust

Blockchain solved the trust issues

A block is like a **ledger** but **unchanged** , once a transaction is noted in the block, you can’t erase it. If a block is created & a transaction happens, every computer or device that is part of the blockchain gets it. So it’s called **distributed**.



Smart contact is likes a program

|  |  |
| --- | --- |
| A ----------------------------→ B  Product send money  Input(int(temp))  If temp <30֯ :  cancel delivery don’t Pay  else :  do delivery & transfer money | Assuming optimum temperature <30֯  If IOT detected  temperature 30֯ cancel delivery  yes don’t Pay  no  do delivery &  transfer money |



International wire transfer :



Bank1 ---------------🡪 bank2 -----------------🡪 bank3 -----------------🡪 Bank4

**Centralized Banking System:**

* **Central Control:** Managed by a central authority (e.g., government or central bank).
* **Limited Access:** Access to financial services may be restricted or dependent on location and status.
* **Trust Dependency:** Relies on trust in the central authority to manage and secure transactions.
* **Vulnerable to Fraud:** Single points of failure can be exploited by fraudsters or hackers.
* **Traditional Infrastructure:** Relies on legacy systems that can be costly to maintain and upgrade.
* **Privacy Concerns:** Centralized systems may require personal information and can potentially compromise user privacy.

**Blockchain:**

* **Decentralization:** Operates on a distributed network of computers (nodes) without a central authority.
* **Accessibility:** Anyone with internet access can participate in blockchain networks.
* **Trustless Transactions:** Uses cryptographic methods for secure and transparent transactions without relying on trust in a single entity.
* **Resilience to Fraud:** Resistant to fraud due to cryptographic security and decentralized validation.
* **Efficiency and Cost:** Lower transaction fees and faster processing times due to automated consensus mechanisms.
* **Privacy and Security:** Provides varying degrees of anonymity and security through cryptographic protocols.

Health system :

City A x- pracent City B



Data base



Blockchain technology potentially impact health systems in City A and City B:

**City A:**

* **Blockchain Integration:** A certain percentage (x%) of health data in City A could be managed and accessed through blockchain technology.
* **Decentralized Control:** Blockchain offers a decentralized approach to storing and managing health records, reducing reliance on a single centralized database.
* **Enhanced Security:** Data stored on a blockchain is encrypted and distributed across a network of computers (nodes), reducing the risk of unauthorized access and enhancing data security.
* **Patient Control:** Blockchain can empower patients with greater control over their health data, allowing them to grant access to healthcare providers as needed while maintaining privacy.

**City B:**

* **Potential Blockchain Use:** The specifics of blockchain implementation in City B are not provided, so its application could vary.
* **Hypothetical Benefits:** If City B adopts blockchain, it could potentially offer similar advantages as in City A, such as enhanced security, data transparency, and patient autonomy.
* **Considerations:** Adoption challenges, regulatory frameworks, and interoperability with existing healthcare systems would need to be addressed.

In both cities, blockchain technology could revolutionize healthcare by improving data integrity, security, and accessibility, while empowering patients with greater control over their health information. The actual implementation and benefits would depend on local policies, technological infrastructure, and healthcare system priorities.

Hashing Algorithm :

Hash is like a fingerprint (human being : every person has different identity).

Hash is generated by the help f SHA256 algorithm

**Hashing Algorithm (SHA256):**

* **Definition:** A hashing algorithm is a mathematical function that garbles data and makes it unreadable.

**Blockchain Structure:**

Blockchain organizes data into blocks, where each block contains:

* **Data:** Information such as transactions or records.
* **Previous Hash:** The hash of the previous block in the chain, creating a sequential link.
* **Hash:** The hash generated for the current block, which includes the data and the previous block's hash.
* **Output:** SHA256 produces a 256-bit (32-byte) hash value, which is commonly represented as a 64-character hexadecimal string (each character represents 4 bits).

Data: document/ audio/ video ---🡪 SHA256 --------🡪 encrypted data ;

64 hexadecimal char , each char = 4 bits . 64 x 4 = 256 bits encrypted data

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | Block no : 01 | | Data | | Prev hash :0000000 | | hash : 00D8C42 | | |  | | --- | | Block no : 02 | | Data | | Prev hash : 00D8C42 | | hash : 003445 | | |  | | --- | | Block no : 03 | | Data | | Prev hash : 003445 | | hash : 002D45F | | |  | | --- | | Block no : 04 | | Data | | Prev hash : 002D45F | | hash 9984GH5 | |

Requirements of a hashing algorithm:

* **One-way Functionality:** It's easy to turn data into a hash, but extremely hard to turn a hash back into the original data.
* **Deterministic**: Ensures that identical input data always generates the same hash, critical for maintaining consistency in blockchain transactions and blocks.
* **Fast Computation**: Essential for handling the high transaction volumes of blockchain networks swiftly and efficiently.
* **Uniformity**: Distributes hash values evenly to minimize the likelihood of different blocks having the same hash, ensuring data integrity in blockchain.
* **Pre-image Resistance**: Makes it highly impractical to reverse-engineer original data from its hash, safeguarding the immutability of recorded transactions.
* **Collision Resistance**: Minimizes the chance that different blocks produce identical hash values, preserving the uniqueness and reliability of blockchain's chronological chain.
* **Avalanche Effect**: Guarantees that any change in block data results in a significantly different hash value, enabling detection of even minor tampering attempts.
* **Non-Reversible**: Ensures that once data is hashed, it cannot be feasibly reconstructed back to its original form, ensuring privacy and permanence in blockchain transactions and records.

"SHA-256, a widely used hashing algorithm in blockchain, exemplifies the requirements:

* **One-way Functionality**: Easily converts data to a hash but computationally impractical to reverse.
* **Deterministic**: Identical blockchain data always yields the same SHA-256 hash, ensuring transaction consistency.
* **Fast Computation**: Efficiently handles vast blockchain transaction volumes.
* **Uniformity**: Distributes hashes evenly, reducing the chance of identical hashes for different blocks.
* **Pre-image Resistance**: It's nearly impossible to derive original data from its SHA-256 hash, securing transaction integrity.
* **Collision Resistance**: SHA-256 minimizes the likelihood of different transactions producing the same hash, crucial for blockchain reliability.
* **Avalanche Effect**: Even slight changes in blockchain data drastically alter SHA-256 hashes, promptly detecting tampering.
* **Non-Reversible**: Once data is hashed with SHA-256, it cannot feasibly be reversed, ensuring transaction privacy and permanence.

**Immutable ledger** :

An immutable ledger is a record-keeping system where the data entered can't be altered, tampered with, or deleted. It ensures that all transactions or entries made in the ledger are permanently recorded and maintained in their original state, creating a transparent and trustworthy record of events.



A 🡨 B 🡨 C 🡨 D 🡨 E 🡨 F



If C block hacked or little bit changed , because of Avalanche effect D will be corrupt & all corrupted

benefits of immutability in blockchain:

1. **Data Integrity**: Once information is recorded in a blockchain, it cannot be altered or deleted, ensuring that transactions and data remain accurate and trustworthy. This guarantees the reliability of records and prevents manipulation.
2. **Trust and Transparency**: Immutability enhances trust in blockchain networks by providing a secure and tamper-proof record of transactions. Participants can rely on the authenticity of the data, fostering transparency in operations.
3. **Security**: Blockchain's immutability makes it highly secure against cyber threats. The use of cryptographic hashing and consensus mechanisms ensures that any attempt to alter the blockchain is easily detectable, maintaining the network's integrity and safeguarding against unauthorized changes.
4. **Auditability**: The inability to alter blockchain data facilitates easy auditing and regulatory compliance. Auditors and regulators can easily trace transaction histories, verify records, and detect fraud without extensive manual effort.
5. **Dispute Resolution**: Immutable records in blockchain provide conclusive evidence in case of disputes. Parties can verify transactions independently, reducing the need for third-party intermediaries and legal proceedings.
6. **Efficiency and Cost Savings**: By ensuring data validity and reducing the need for manual verification, blockchain improves operational efficiency. This efficiency translates into cost savings by minimizing errors, enhancing trust, and streamlining processes.

The Bitcoin blockchain's immutable ledger works:

* **Transaction Records**: Each Bitcoin transaction is recorded as a block in the blockchain.
* **Block Formation**: Transactions are grouped into blocks, and each block contains a hash code that links it to the previous block.
* **Immutability**: Once added, a block cannot be altered without changing all subsequent blocks, due to the cryptographic hash linking.
* **Decentralization and Consensus**: Bitcoin operates on a decentralized network where multiple nodes maintain copies of the blockchain. Changes require consensus among nodes.
* **Security and Trust**: The immutable nature of the blockchain ensures secure and trustworthy transactions, allowing participants to verify transactions independently.

distributed P2P network in blockchain

A "distributed P2P network in blockchain" refers to a network architecture where multiple computers (nodes) across a blockchain system operate as peers ,meaning each node has equal power and responsibility to maintain a copy of the shared ledger, allowing for direct transactions between participants without a central authority, making the network decentralized and highly secure , essentially, every node acts as both a client and a server, communicating directly with other nodes to verify and validate transactions .

**Centralized Network:**

* **Single Hub:** Like a single main office where all decisions are made.
* **Issues:**
  + If the main office shuts down, the whole network stops working.
  + If many people need help at once, it can get slow.
  + Sometimes, it's easier for bad guys to break in.

**Peer-to-Peer (P2P) Network:**

* **Everyone Helps:** Like a big group where everyone shares and helps each other.
* **Good Things:**
  + If one person stops helping, others can still share and work.
  + **Security**: The decentralized nature makes it difficult to tamper with data as any changes would need to be validated by a majority of nodes.
  + **Transparency**: Anyone can view the transaction history on the blockchain.
  + **Reliability**: No single point of failure, as the network continues to function even if some nodes go offline

peer-to-peer (P2P) network handles a hacked block:

1. **Consensus Protocols:** P2P networks use rules that all nodes must agree on before accepting new blocks. This ensures everyone checks if a block is valid.
2. **Block Verification:** Each node checks new blocks to see if they follow the rules. If one node finds a hacked block (not following the rules), it rejects it.
3. **Network Resilience:** P2P networks keep working even if one node is hacked. Other nodes have copies of the correct data and ignore the hacked information.
4. **Reorganizing:** If a hacked block gets through, nodes can fix it by reorganizing the data to remove the bad block and keep the good ones.
5. **Rollback:** Some networks can go back to a point before the hack to fix things and keep the data correct.
6. **Security:** P2P networks use strong security like codes and shared data to stop hacks before they cause big problems.

In simple terms, P2P networks use rules and teamwork to spot and fix hacked blocks, keeping the whole network safe and working right.

Blockchain mining :

Blockchain mining is a process that involves verifying and adding transactions to a blockchain, a public ledger that documents cryptocurrency transactions. Miners are rewarded with digital currency for their work, which incentivizes them to maintain the blockchain's integrity. The reason ,the block chain mining create an environment of trust & security .

 blockchain mining works:

* **Collect transactions** : Miners' computers, called nodes, collect transactions from the past ten minutes.
* **Create a block** : The transactions are bundled into a block, which includes information from the previous block.
* **Solve a puzzle** : Miners compete to solve a complex mathematical puzzle to validate the block.
* **Broadcast the solution** :The first miner to find the correct solution broadcasts it to the network.
* **Add to the blockchain** : If the other nodes confirm the solution, the new block is added to the blockchain.

Byzantine Generals Problem :

The Byzantine Generals Problem is a game theory problem, which describes the difficulty decentralized parties have in arriving at consensus without relying on a trusted central party.

* **The challenge** : The generals must coordinate their actions, but they have no secure communication channels. Messages could be intercepted or tampered with by the enemy.
* **The goal** : The generals must come to an agreement on a strategy. If they attack at the same time, they'll win, but if they attack at different times, they'll lose.

consensus protocol :

A consensus protocol in blockchain ensures all network nodes agree on transactions and the blockchain state. It prevents fraud by verifying and adding new blocks, ensuring all nodes reach agreement on stored data.

Proof of Work

* Validation is done by a network of miners
* Bitcoin paid as a reward and for transaction fees
* Competitive nature uses lots of energy and computational power

Proof of Stake

* Validation is done by participants who offer ether as collateral
* Ether is paid for transaction fees only
* Less computational power and energy used
* Consensus is reached faster because there is no difficulty

Cryptocurrency :

Cryptocurrency is a digital way to pay for things without needing banks. Transactions are just digital entries in a public online record. When you transfer cryptocurrency, it gets recorded in a public ledger.

** Technology:** The tools and infrastructure used to build and run blockchain networks, like software and hardware.

* **Example:** Ethereum's software and nodes that execute smart contracts.

** Protocol**: Rules that govern how blockchain networks operate, including data validation and consensus mechanisms**.**

* **Example**: Bitcoin's protocol defines how transactions are verified and added to its blockchain.

The main difference of coin & token is that **crypto coins** have their own independent blockchain, whereas **tokens** are built on an existing blockchain.

the types of cryptography:

1. **Symmetric Key Cryptography:**
   * Uses a single shared key for both encryption and decryption.
   * Fast and efficient.
   * Key exchange between sender and receiver must be secure.
   * Examples include DES (Data Encryption Standard) and AES (Advanced Encryption Standard).
2. **Hash Functions:**
   * No key is used; a fixed-length hash value is generated from plaintext.
   * One-way function: cannot be reversed to obtain plaintext.
   * Commonly used in securing passwords in operating systems.
3. **Asymmetric Key Cryptography:**
   * Uses a pair of keys: a public key and a private key.
   * Public key is used for encryption, private key for decryption.
   * Public key can be shared openly, private key is kept secret.
   * Ensures secure communication without needing a prior exchange of keys.
   * RSA (Rivest-Shamir-Adleman) is a popular algorithm for asymmetric cryptography.

**Bitcoin eco-system :**

 **Bitcoin Blockchain:** A decentralized, distributed ledger that records all Bitcoin transactions. It ensures transparency and immutability by using cryptographic techniques.

 **Miners:** Individuals or groups who validate transactions and secure the network by solving complex mathematical puzzles. They are rewarded with newly minted bitcoins and transaction fees.

 **Wallets:** Software or hardware used to store, send, and receive bitcoins. Wallets manage private keys necessary for accessing and managing Bitcoin holdings.

 **Exchanges:** Platforms where users can buy, sell, and trade bitcoins and other cryptocurrencies. They provide liquidity and price discovery within the market.

 **Developers:** Individuals and teams who contribute to Bitcoin's protocol development, improving its functionality, security, and scalability.

 **Nodes:** Computers that maintain a full copy of the Bitcoin blockchain and participate in validating and relaying transactions. Nodes help ensure the network's decentralization and security.

 **Merchants and Adoption:** Businesses and individuals who accept Bitcoin as payment for goods and services, promoting its use as a medium of exchange.

 **Regulation and Legal Framework:** Various jurisdictions have different regulatory approaches to Bitcoin, impacting its adoption and use globally.

 **Mining Pools:** Groups of miners who collaborate to increase their chances of solving blocks and earning rewards collectively.

 **Bitcoin Improvement Proposals (BIPs):** Proposals for technical improvements to Bitcoin's protocol, governance, and ecosystem, allowing for community input and evolution.

two key concepts related to Bitcoin's monetary policy and blockchain operation:

1. **Bitcoin Halving:**
   * Bitcoin halving refers to the reduction in the reward given to miners for validating transactions and securing the Bitcoin network.
   * This event occurs approximately every four years (specifically, every 210,000 blocks).
   * Initially, when Bitcoin started, miners received 50 bitcoins as a reward for adding a new block to the blockchain. After the first halving event, the reward was reduced to 25 bitcoins, then to 12.5 bitcoins, and so on.
   * The most recent halving event took place in May 2020, reducing the reward from 12.5 bitcoins to 6.25 bitcoins per block.
   * The halving is programmed into Bitcoin's protocol as a way to control its inflation rate and ensure a predictable issuance schedule, ultimately aiming to limit the total number of bitcoins that will ever be created to 21 million.
2. **Block Frequency:**
   * Block frequency refers to the average time it takes for miners to discover and add a new block to the Bitcoin blockchain.
   * Bitcoin's protocol adjusts the difficulty of mining every 2016 blocks (approximately every two weeks) to maintain an average block discovery time of about 10 minutes.
   * The block frequency can vary slightly due to fluctuations in computational power (hash rate) dedicated to mining.
   * A consistent block frequency helps ensure the stability and predictability of Bitcoin's transaction processing and issuance of new bitcoins.

Mining : Mining is the process by which networks of specialized computers generate and release new Bitcoin and verify new transactions

Nonce : the nonce is the number that blockchain miner are solving for …

Target : Target is a number used in mining . it is a number that a block hash must be below to the block to be added . target adjust every 2016 bocks to try & ensure that block are mining once every 10 minutes on average.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | Block no : 01 | Block no : 02 | Block no : 03 | | Nonce : 15119  Data | Nonce : 14594  Data | Nonce : 97739  Data | | Prev hash : 00000 | Prev hash : 002D45F | Prev hash : 003445 | | hash : 002D45F | hash : 003445 | hash : 000E | | Nonce : 97739  **Target 000 (hash)**  **Matched at block 03** |

**The most important** think is , which miner solve first is depends on how first it can generate hashes

**Mining Works:**

* **Block Formation**: Miners gather transactions into a block and then create a block header. This header includes details like the previous block hash, timestamp, and a nonce.
* **Hashing**: Miners hash the block header using the SHA-256 algorithm to generate a hash value. This hash is a unique digital fingerprint of the block data.
* **Adjustment and Validity**: The miner checks if the resulting hash is below the target value. If not, they increment the nonce and hash again. This process repeats until a valid hash (below the target) is found.
* **Proof of Work**: Finding a valid hash (one that meets the target criteria) is proof that the miner has expended computational effort, known as Proof of Work (PoW). This valid block can then be added to the blockchain.
* **Difficulty Adjustment**: Every 2016 blocks, the network adjusts the target based on how quickly blocks are being mined. If blocks are being mined too quickly, the target decreases to increase difficulty, and vice versa.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **CPU**: General-purpose, slow for mining, less efficient  10MH/s [10million hashes] | GPU: Specialized for graphics, good for mining due to parallel processing, more efficient than CPUs.  1GH/s [1billion hashes] | **ASIC**: Highly specialized, very efficient for mining, but limited to specific algorithms.  1000GH/s [1 trillion] |

1. **CPU (Central Processing Unit)**:
   * **Role**: General-purpose processor found in most computers.
   * **Mining Capability**: Initially used for early cryptocurrency mining (e.g., Bitcoin). However, CPUs are relatively slow and inefficient compared to GPUs and ASICs.
   * **Efficiency**: Less energy-efficient for mining due to their general-purpose design.
   * **Versatility**: Suitable for various tasks beyond mining, but not cost-effective for large-scale cryptocurrency mining.
2. **GPU (Graphics Processing Unit)**:
   * **Role**: Specialized for rendering graphics in computers.
   * **Mining Capability**: Became popular for cryptocurrency mining (e.g., Ethereum) due to their parallel processing power.
   * **Efficiency**: More energy-efficient than CPUs for mining, offering higher hash rates per watt.
   * **Versatility**: Can be used for gaming, AI, and other parallel processing tasks besides mining.
3. **ASIC (Application-Specific Integrated Circuit)**:
   * **Role**: Custom-built chip designed specifically for one task, such as cryptocurrency mining.
   * **Mining Capability**: Highly efficient and specialized for mining specific cryptocurrencies (e.g., Bitcoin ASICs for SHA-256 hashing).
   * **Efficiency**: Most energy-efficient option for mining, offering significantly higher hash rates per watt compared to CPUs and GPUs.
   * **Versatility**: Limited to the specific algorithm it's designed for, making it less versatile than CPUs and GPUs.

mining pool :

A mining pool is a group of cryptocurrency miners who work together to solve the cryptographic problems required by a blockchain.

A mining pool in cryptocurrency:

1. **Combines Resources**: Miners pool their computational resources together.
2. **Increases Efficiency**: Increases chances of earning rewards by collectively solving blocks.
3. **Shares Rewards**: Distributes rewards proportionally based on contributed computational power.
4. **Manages Operations**: Pool operator handles distribution of work and reward management.
5. **Reduces Variability**: Smoothers out income variability compared to solo mining.

Nonce Range :

Nonce is finite number 32 bit , range 0 to -1 = 0 to **4x**

4 billion hashes can be produce with the help of 4 billion nonce

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx 🡪 each character ha 16 hexadecimal possibilities

SHA256 produce , Total no of possible hashes = 16x16\*\*\*\*\*x16 = =

**Total** valid hashes =  **Total** no of nonce = **4x**

Ther are not enough nonce to generate the valid hash .

A modest does  **hashes per secund .** so **4x nence** will be covered = **4x**/ **= 40sec**

When a miner runs out of nonces without finding a valid block (hitting the target hash), they simply increment the block timestamp and start trying new nonces again

* When a miner exhausts all possible nonces without finding a valid block, they increment the block timestamp.
* This resets the nonce counter and changes the data slightly, including the updated timestamp.
* By doing this, miners expand the search space for finding a valid block, increasing the chances of success.

**timestamp :**

The timestamp is a small data stored in each block as a unique serial and whose main function is to determine the exact moment in which the block has been mined and validated by the blockchain network.

* **Identification**: The timestamp uniquely identifies when a block was created and validated on the blockchain.
* **Chronological Order**: It ensures transactions and blocks are arranged in the correct sequence, maintaining the integrity of the blockchain's history.
* **Network Consensus**: Nodes in the network use timestamps to agree on the order of transactions and blocks, crucial for consensus mechanisms like Proof of Work or Proof of Stake.
* **Precision**: Timestamps provide precise timing information, allowing participants to verify the timing of transactions and events within the blockchain network.

Current hash rate is 180Millin Trillion hashes per sec

so **4x nence** will be covered = **4x**/ **x = 4x second**

mempool :

 A mempool is an important component of blockchain transactions. Mempools serve as a temporary holding area for unconfirmed transactions.

mining of transactions takes place:

1. **Transaction Propagation**: Transactions are broadcasted across the blockchain network by participants.
2. **Verification**: Miners collect and verify these transactions to ensure they are valid according to the blockchain's rules (e.g., sufficient funds, correct signatures).
3. **Block Formation**: Valid transactions are grouped into a block. Miners compete to solve a cryptographic puzzle (Proof of Work) by finding a nonce that, when combined with other block data, produces a hash meeting certain criteria.
4. **Consensus**: Once a miner finds a valid hash (meets the target difficulty), they broadcast the new block to the network.
5. **Inclusion in Blockchain**: Other nodes validate the block and, if accepted, add it to their own copy of the blockchain.
6. **Reward**: The miner who successfully mines the block typically receives a reward (e.g., cryptocurrency) for their effort and contribution to securing the network.

The mempool enables miners to see which transactions are pending and decide which ones to include in the next block based on factors like transaction fees and the size of the transactions. Miners collect transactions from the mempool and bundle them into a block.

**Transactions in Blockchain:**

1. **What is a Transaction?**
   * A transaction in blockchain is a fundamental unit of data that records the transfer of value between participants on the network. It can involve the transfer of cryptocurrency (like Bitcoin) or other assets.
2. **Components of a Transaction:**
   * **Inputs:** These are references to previous transaction outputs (UTXOs) that are being spent to fund the new transaction.
   * **Outputs:** These are the new UTXOs created as a result of the transaction, specifying the amount and the recipient.

**Transaction Process:**

* **Signing:** Alice signs the transaction with her private key to prove ownership of the input UTXO.
* **Broadcasting:** Once signed, the transaction is broadcast to the network.
* **Verification:** Nodes in the network validate the transaction to ensure it meets consensus rules

**UTXOs (Unspent Transaction Outputs):**

1. **What are UTXOs?**
   * UTXOs represent the outputs of previous transactions that have not been spent yet.
   * In simpler terms, they are like the balance of an account in traditional banking systems but fragmented into distinct, spendable amounts.

The transaction fee in a blockchain context refers to a small amount of cryptocurrency that is included in a transaction and collected by miners or validators as a reward for processing that transaction and including it in a block on the blockchain. A transaction fee is composed of:

* **Base Fee:** This is a minimum fee required for a transaction to be processed by the network.
* **Priority Fee:** An optional fee paid by the sender to prioritize their transaction.

A transaction fee is based on several factors:

* **Network Congestion:** Higher congestion can lead to higher fees as users compete to have their transactions processed quickly.
* **Transaction Size:** Larger transactions (in terms of data size, not necessarily amount) may require higher fees to prioritize them in the queue.
* **Desired Speed:** Users can choose to pay higher fees for faster confirmation times.

**A cryptocurrency wallet** is a digital tool that allows users to securely store, send, and receive cryptocurrencies .

**Key Aspects of Cryptocurrency Wallets:**

1. **Private Keys:**
   * A cryptocurrency wallet stores your private keys, which are crucial for authorizing transactions and accessing your funds. Private keys are generated securely and should be kept confidential.
2. **Public Addresses:**
   * Each cryptocurrency wallet has a public address associated with it. This address is like a bank account number and is used to receive funds. It is derived from your wallet's public key.
3. **Security Features:**
   * **Encryption:** Wallets often use strong encryption to protect private keys and transactions from unauthorized access.
   * **Backup:** It's important to securely back up your wallet's seed phrase or private keys. Losing access to these can mean losing access to your funds permanently.
4. **Types of Cryptocurrency Wallets:**
   * **1. Software Wallets:**
     + **Desktop Wallets:** Installed on a computer and accessible only from that device. Examples include Electrum (Bitcoin) and Exodus (multi-currency).
     + **Mobile Wallets:** Apps installed on smartphones, offering convenience for everyday transactions. Examples include Trust Wallet and Coinbase Wallet.
     + **Online/Web Wallets:** Accessed via a web browser, they are convenient but may be less secure than other types. Examples include MyEtherWallet (for Ethereum).
   * **2. Hardware Wallets:**
     + Physical devices (USB-like) designed to securely store cryptocurrency offline. They provide a high level of security by keeping private keys offline and require physical interaction to authorize transactions. Examples include Ledger Nano S and Trezor.
   * **3. Paper Wallets:**
     + A physical paper or document containing your public and private keys, often printed as QR codes. It's considered very secure because it's completely offline, but care must be taken to protect it from physical damage and theft.
   * **4. Cold Storage Wallets:**
     + Refers to any wallet where private keys are stored offline, away from internet-connected devices. This includes hardware wallets and paper wallets.
   * **5. Custodial Wallets:**
     + Managed by a third party (like exchanges) who store your private keys on your behalf. While convenient, they pose security risks as you don't have full control over your keys.

**Using a Cryptocurrency Wallet:**

* **Receiving Funds:** Share your public address with others to receive cryptocurrency.
* **Sending Funds:** Input the recipient's public address and authorize the transaction with your private key.
* **Security Practices:** Always use strong passwords, enable two-factor authentication (2FA), and regularly back up your wallet.

**Segregated Witness (SegWit):**

* **Definition:** SegWit is a protocol upgrade implemented in some blockchain networks, such as Bitcoin and Litecoin.
* **Purpose:** It separates (or segregates) transaction data (witness data) from the transaction ID (txid) and moves it to a new structure.

**Benefits of Segregated Witness (SegWit):**

1. **Increased Transaction Capacity:**
   * SegWit reduces the size of transaction data stored on the blockchain, allowing more transactions to fit into each block.
   * This helps alleviate network congestion and reduces transaction fees.
2. **Enhanced Security:**
   * Fixes transaction malleability issues by separating digital signatures from transaction data.
   * Improves the security and reliability of transactions.
3. **Compatibility and Future Upgrades:**
   * SegWit provides a foundation for implementing further scaling solutions and upgrades in blockchain networks.
   * It supports the development of second-layer scaling solutions like the Lightning Network.

Ethereum is an open source block chain based platform . Ethereum provide ether.

Ethereum has 3 types of node 🡪 Full Node , Light Node , Archive Node

**Types of Ethereum Nodes:**

1. **Full Node:**
   * **Function:** A full node stores the entire blockchain and validates every transaction and smart contract on the network.
   * **Features:**
     + Maintains a complete copy of the Ethereum blockchain.
     + Participates in consensus by validating and relaying transactions.
     + Supports network security and decentralization by independently verifying all data.
2. **Light Node (or Light Client):**
   * **Function:** A light node downloads only block headers, not the entire blockchain. It relies on full nodes for transaction information.
   * **Features:**
     + Requires less storage space and bandwidth compared to full nodes.
     + Can send and receive transactions but doesn't validate them independently.
     + Suitable for resource-constrained devices like smartphones, providing quicker access to the blockchain.
3. **Archive Node:**
   * **Function:** An archive node stores all historical data and state changes on the blockchain, including past transaction details.
   * **Features:**
     + Provides access to complete transaction history, smart contract states, and account balances since the genesis block.
     + Consumes significant storage space due to storing extensive blockchain data.
     + Essential for developers, researchers, and projects needing deep historical analysis of Ethereum's state.

**Use Cases:**

* **Full Nodes:** Ideal for users requiring full blockchain security and independence, such as miners, developers, and businesses handling large transaction volumes.
* **Light Nodes:** Suitable for everyday users and applications needing quick access to Ethereum's network without extensive resource requirements.
* **Archive Nodes:** Critical for developers building decentralized applications (dApps), conducting blockchain research, or requiring comprehensive historical data.

Ethereum account is an entity with an ether (ETH) balance that can send or receive transection on Ethereum .

**1. Externally Owned Account (EOA):**

* **Definition:** An Externally Owned Account is a basic Ethereum account controlled by a private key and associated with an Ethereum address.
* **Characteristics:**
  + **Control:** Owned and controlled by an individual or entity via a private key.
  + **Capabilities:** Can hold Ether (ETH) and initiate transactions (send and receive ETH) on the Ethereum network.
  + **Interaction:** Used by individuals to participate in transactions, interact with dApps (decentralized applications), and manage personal funds.
* **Usage:** Commonly used by:
  + Individual users for managing personal funds and conducting transactions.
  + Wallets and exchanges to facilitate ETH transfers on behalf of users.

**2. Contract Account:**

* **Definition:** A Contract Account, also known as a smart contract, is a type of Ethereum account that holds both code and Ether (ETH).
* **Characteristics:**
  + **Code Execution:** Contains Ethereum Virtual Machine (EVM) bytecode, enabling it to execute predefined operations when triggered by transactions.
  + **Autonomous:** Operates autonomously based on predefined rules and conditions encoded in its smart contract code.
  + **Interaction:** Can receive and store Ether (ETH), initiate transactions, and interact with other smart contracts and EOAs.
* **Usage:** Commonly used for:
  + Deploying decentralized applications (dApps) that execute complex logic and automated functions.
  + Token contracts (e.g., ERC-20 tokens) that manage token issuance, transfers, and other functionalities on Ethereum.

**Decentralized application (dApp):** A dApp on Ethereum leverages smart contracts—self-executing code on the blockchain—to offer decentralized functionality.

**Characteristics:**

* **Decentralization:** Operates on a decentralized network of computers (nodes), ensuring transparency, security, and censorship resistance.
* **Smart Contracts:** Core components written in languages like Solidity, managing business logic and interactions within the Ethereum ecosystem.
* **Immutable:** Once deployed, dApps' code and data reside on the blockchain, making them resistant to tampering and ensuring historical transparency

**Centralized Network:**

* **Control:** Controlled by a single entity or organization that manages all operations, data, and decision-making.
* **Architecture:** Typically uses a client-server model where clients (users) connect to a central server to access services or data.
* **Examples:** Traditional banking systems, social media platforms (e.g., Facebook, Twitter), and centralized cloud services (e.g., AWS, Google Cloud).

**Decentralized Network:**

* **Control:** Operates without a central authority, distributing control and decision-making across multiple nodes or participants.
* **Architecture:** Nodes communicate directly with each other, often using peer-to-peer (P2P) protocols, and share resources (e.g., processing power, data storage).
* **Examples:** Blockchain networks like Ethereum and Bitcoin, peer-to-peer file sharing networks (e.g., BitTorrent), and decentralized applications (dApps).

**Key Differences:**

* **Security:** Decentralized networks are more resilient to single points of failure and censorship due to their distributed nature.
* **Trust:** Centralized networks require users to trust the central authority, while decentralized networks rely on cryptographic mechanisms and consensus algorithms for trustless interactions.
* **Scalability:** Centralized networks can scale more easily but may face bottlenecks and issues with trust and control. Decentralized networks often face scalability challenges but offer enhanced security and censorship resistance.

**Ethereum Virtual Machine (EVM):** The Ethereum Virtual Machine (EVM) is a decentralized computing environment that runs on all nodes in the Ethereum network.

**Functionality:**

* **Execution:** It executes bytecode from smart contracts deployed on the Ethereum blockchain.
* **Turing-Complete:** The EVM is Turing-complete, meaning it can compute any algorithm given enough resources, enabling complex computations and logic within smart contracts.
* **State Transitions:** Manages state transitions and maintains the integrity of the Ethereum blockchain by processing transactions and smart contract interactions.

The Ethereum Virtual Machine (EVM) protects against hackers and viruses through:

* **Deterministic Execution:** Ensures consistent results across all nodes.
* **Gas Mechanism:** Prevents resource abuse with transaction cost.
* **Sandboxed Environment:** Isolates smart contracts to limit interactions.
* **Immutability:** Code and state are unalterable once deployed.
* **Formal Verification:** Mathematically verifies smart contract correctness.
* **Community Vigilance:** Promotes best practices and security audits.

**Gas on Ethereum:**

* **Definition:** Gas is a measurement of computational work required to perform operations or execute smart contracts on the Ethereum blockchain.

**Gas Price:**

* **Definition**: Gas price is the amount of Ether (ETH) paid per unit of gas.
* **Denomination:** Gas prices are denoted in **gwei, where 1 gwei = ETH.**
* **Function:** Higher gas prices prioritize transactions by offering incentives to miners, resulting in faster transaction confirmations.

**Gas Limit:**

* **Definition**: Gas limit is the maximum amount of gas a transaction is willing to consume.
* **Purpose**: Prevents transactions from exceeding specified resource limits, ensuring predictable costs and preventing abuse.
* **Adjustment**: Users set the gas limit based on the complexity of operations and desired transaction execution.

**Gas Limit < Gas Used**: Transaction fails and reverts changes.

**Gas Limit = Gas Used**: Transaction executes successfully.

**Gas Limit > Gas Used**: Transaction executes successfully with unused gas refunded.

**decentralized autonomous organization (DAO)** : A decentralized autonomous organization (DAO) is an emerging form of organizational structure with no central governing body and whose members share a common goal of acting in the best interest of the entity.

**Decentralized Autonomous Organization (DAO):**

1. **Decentralization:**
   * **Structure:** Operates without a central authority or hierarchical management structure.
   * **Decision-Making:** Governance and decision-making processes are decentralized, typically through voting mechanisms executed on a blockchain.
   * **Blockchain Technology:** Relies on blockchain's cryptographic security and consensus mechanisms to secure funds and operations.
   * **Trustless Interactions:** Minimizes the need for trust between participants through automated, transparent protocols.

**The DAO:**

1. **Concept:**
   * **Purpose:** Designed as a decentralized venture capital fund governed by smart contracts and DAO principles.
   * **Structure:** Operated autonomously based on code and decisions made through token holder voting.

| **Aspect** | **DAO** | **Traditional Organization** |
| --- | --- | --- |
| **Fully Democratized** | Yes | No |
| **Voting Required** | Yes | May or may not be required |
| **No Trusted Intermediary for Vote Count** | Yes | Outcome of voting must be handled manually |
| **Services Handled Automatically** | Yes | Requires human handling or central control |
| **Activity Transparency** | All activity is transparent and fully public | Activity is typically private and limited |
| **Structure** | Decentralized | Usually hierarchical |

timeline of the DAO attack and related events in 2016:

* **30.04.16:** The DAO is launched on the Ethereum blockchain, aiming to operate as a decentralized venture capital fund.
* **15.05.16:** The DAO starts to raise significant funds through Ethereum (ETH) investments, showcasing the potential of decentralized autonomous organizations (DAOs).
* **16.06.16:** Exploiting a recursive call vulnerability in its smart contracts, an attacker drains approximately one-third of The DAO's funds, leading to a loss of millions of dollars worth of ETH.
* **17.06.16:** The Ethereum community begins discussing the implications of the attack and potential responses, including a hard fork to recover the stolen funds.
* **20.07.16:** Following community debate and consensus-building, Ethereum executes a controversial hard fork to reverse the attack and recover the stolen ETH, leading to the split of Ethereum into Ethereum (ETH) and Ethereum Classic (ETC).

Hard Fork

* During a hard fork, software implementing a protocol and its mining procedures is upgraded.
* Once a user upgrades their software, that version rejects all transactions from older software, effectively creating a new branch of the blockchain.
* However, those users who retain the old software continue to process transactions.

Soft Fork

* Soft forks are a change to the protocol, but the end product remains unchanged.
* A soft fork is a backward-compatible upgrade, meaning that the upgraded nodes can still communicate with the non-upgraded ones.
* .Old nodes(not upgraded nodes) could still validate blocks and transactions (the formatting didn't break the rules), but they just wouldn't understand them.

**IPO (Initial Public Offering):**

* **Definition:** An IPO is the process through which a private company offers shares to the public for the first time, raising capital by selling ownership stakes in the company.
* **Regulation:** IPOs are heavily regulated by financial authorities in the country where they are offered (e.g., SEC in the United States).
* **Investment:** Investors in IPOs receive shares of the company, representing ownership and potential dividends based on company performance.
* **Purpose:** Typically used by established companies looking to raise funds for growth, expansion, debt repayment, or shareholder liquidity.

**ICO (Initial Coin Offering):**

* **Definition:** An ICO is a fundraising method in which a company or project sells digital tokens (cryptocurrencies) to investors in exchange for funds, usually Ether (ETH) or Bitcoin (BTC).
* **Regulation:** ICOs were initially less regulated, leading to varying levels of investor protection and legal scrutiny globally. Regulations have since tightened in many jurisdictions.
* **Investment:** Investors in ICOs receive tokens that may have utility within the project's ecosystem (utility tokens) or represent a share in future profits (security tokens).
* **Purpose:** Used by blockchain startups and projects to fund development, often for decentralized applications (dApps) or platforms built on blockchain technology.

**Ethereum 2.0 (Serenity):**

* **Purpose:** Ethereum 2.0 aims to address scalability, security, and sustainability issues faced by the current Ethereum blockchain (Ethereum 1.0).
* **Components:**
  + **Proof of Stake (PoS):** Transition from Proof of Work (PoW) to PoS consensus mechanism to improve energy efficiency and scalability.
  + **Sharding:** Introduce sharding to Ethereum, allowing the network to process multiple transactions simultaneously, enhancing scalability.
  + **Beacon Chain:** Introduce the Beacon Chain as the backbone of Ethereum 2.0, coordinating PoS consensus and managing validators.
* **Benefits:**
  + **Scalability:** Increased transaction throughput and reduced fees.
  + **Security:** Enhanced network security through PoS consensus and decentralized validator system.
  + **Sustainability:** Lower energy consumption compared to PoW, supporting long-term network sustainability.

| **Aspect** | **Proof of Work (PoW)** | **Proof of Stake (PoS)** |
| --- | --- | --- |
| **Validation Mechanism** | Miners compete to solve complex mathematical puzzles. | Validators create and validate blocks based on their stake in the network. |
| **Consensus Strategy** | Chain with the most accumulated computational work (longest chain wins). | Validators are chosen deterministically to create new blocks. |
| **Security** | Robust due to high computational power required to attack. | Relies on economic incentives (staked assets) rather than computational power. |
| **Decentralization** | Initially promotes decentralization by allowing participation with hardware. | Potentially enhances decentralization by reducing hardware requirements. |
| **Energy Consumption** | Energy-intensive due to competition and high computational requirements. | Generally more energy-efficient than PoW due to reduced computational needs. |