BLOCKCHAIN

Overview of Blockchain   Unit-1

What is Blockchain?

“Blockchain is a decentralized, distributed ledger technology that records transactions across multiple computers securely and transparently. Each record (called a block) is linked to the previous one, forming a chain of blocks—hence the name "blockchain.”

- **Key Features of Blockchain:**

1. **Decentralization:** No central authority; data is distributed across a network.
2. **Immutability:** Once data is recorded, it cannot be altered.
3. **Transparency:** All transactions are visible to participants.
4. **Security:** Uses cryptographic hashing to ensure data integrity.
5. **Consensus Mechanism:** Transactions are validated by the network (e.g., Proof of Work, Proof of Stake).

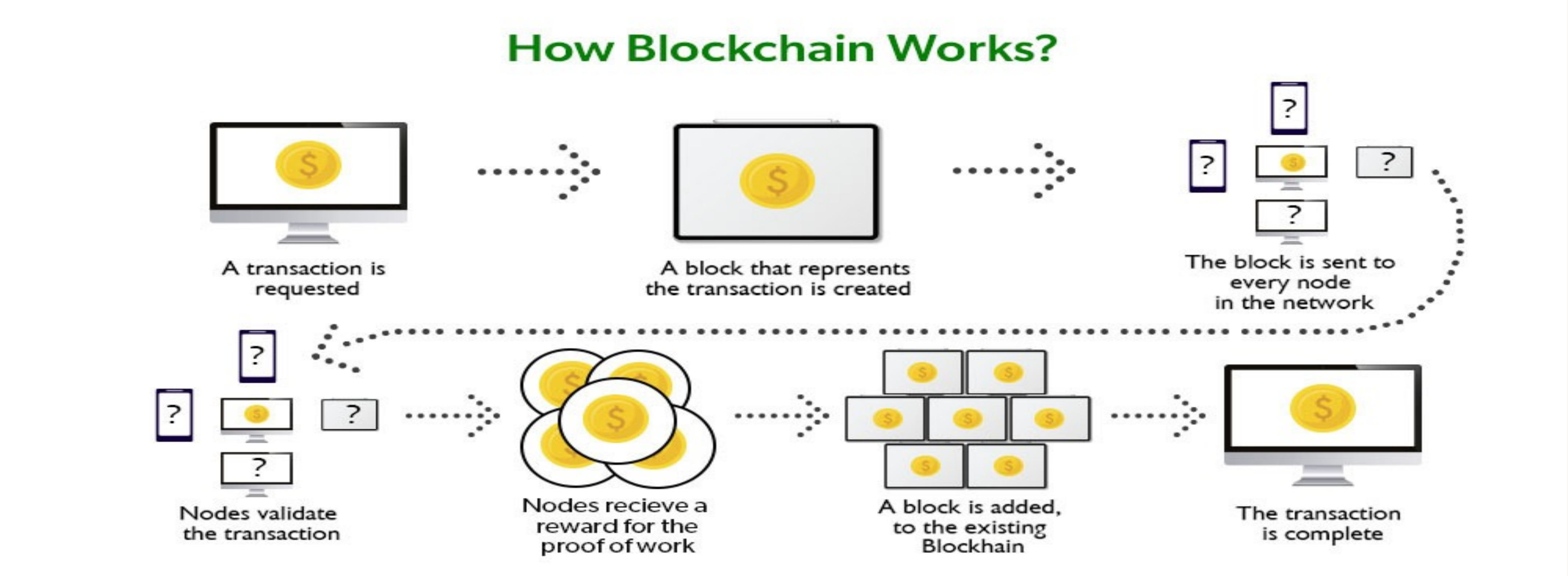
Example of Blockchain:

Imagine a digital ledger shared among a group of friends tracking expenses. If one friend buys groceries, the transaction is recorded, and everyone has a copy. Once verified, it cannot be changed, ensuring trust without a middleman.

- Example Transaction Flow:

1. Alice sends 2 Bitcoins to Bob.
2. Transaction is broadcast to the network.
3. Network nodes validate the transaction.
4. The transaction is added to a new block.
5. The block is linked to the previous one, creating a chain.
6. The updated blockchain is shared across all nodes.

Diagram to Understand Blockchain:


How Blockchain Works?
A transaction is requested
A block that represents the transaction is created
The block is sent to every node in the network
Nodes validate the transaction
Nodes recieve a reward for the proof of work
A block is added, to the existing Blockhain
The transaction is complete

- It illustrates the structure of blocks, how transactions are processed, and how they are linked together in a secure, decentralized manner.

History of Blockchain

- 1. The Idea (1991-2008)
- **1991** – Stuart Haber and W. Scott Stornetta proposed a cryptographically secured chain of blocks to prevent document tampering.
- **1998** – Nick Szabo created "Bit Gold," a decentralized digital currency concept, but it was never implemented.
- 2. Bitcoin and the Birth of Blockchain (2008-2009)
- **2008** – Satoshi Nakamoto published the Bitcoin whitepaper, describing a decentralized ledger system called blockchain.
- **2009** – Bitcoin launched as the first practical application of blockchain.

History of Blockchain

- **3. Growth Beyond Bitcoin (2010-2014)**
- **2010** – The first real-world Bitcoin transaction: 10,000 BTC for two pizzas! 🍕
- **2011** – Other cryptocurrencies like Litecoin and Namecoin emerged.
- **2013** – Vitalik Buterin proposed **Ethereum**, a blockchain with smart contract functionality.
- **2014** – Blockchain technology expanded beyond cryptocurrency (e.g., supply chain, healthcare, and finance).
- **4. Blockchain 2.0: Smart Contracts (2015-2017)**
- **2015** – **Ethereum** launched, introducing smart contracts—self-executing agreements on blockchain.
- **2017** – Initial Coin Offerings (ICOs) surged, raising billions for blockchain startups.

History of Blockchain

- 5. Enterprise Adoption and Expansion (2018-Present)

- 2018 – Companies like IBM, Microsoft, and banks began using blockchain for business solutions.
- 2020 – DeFi (Decentralized Finance) and NFTs (Non-Fungible Tokens) gained popularity.
- 2023+ – Governments explore Central Bank Digital Currencies (CBDCs), and industries widely adopt blockchain for secure record-keeping.

Future of Blockchain

Web3 & Metaverse – Decentralized internet applications.

AI & Blockchain – Combining AI with blockchain for automation.

Regulations – Governments working on blockchain laws and compliance.

1. Public Ledgers

- A public ledger is an open, decentralized digital record where transactions are stored and accessible to everyone. It ensures transparency and trust without a central authority. Blockchain is an example of a public ledger.
- Example:
  Imagine a shared online spreadsheet where anyone can see and verify transactions but cannot change past records.

2. Bitcoin

- Bitcoin is a decentralized digital currency that uses blockchain technology to allow peer-to-peer transactions without intermediaries like banks. Transactions are recorded on a public ledger, ensuring transparency and security.
- **Key Features:**
- No central control (decentralized)
- Secure through cryptographic hashing
- Limited supply (21 million Bitcoins)
- Transactions verified by miners
- **Example:**
  Alice sends 1 Bitcoin to Bob. The transaction is verified by the network and added to the blockchain, making it permanent and visible to all.

3. Smart Contracts

- A smart contract is a self-executing program stored on a blockchain that runs when predefined conditions are met. It automates agreements without intermediaries.
- **Key Features:**

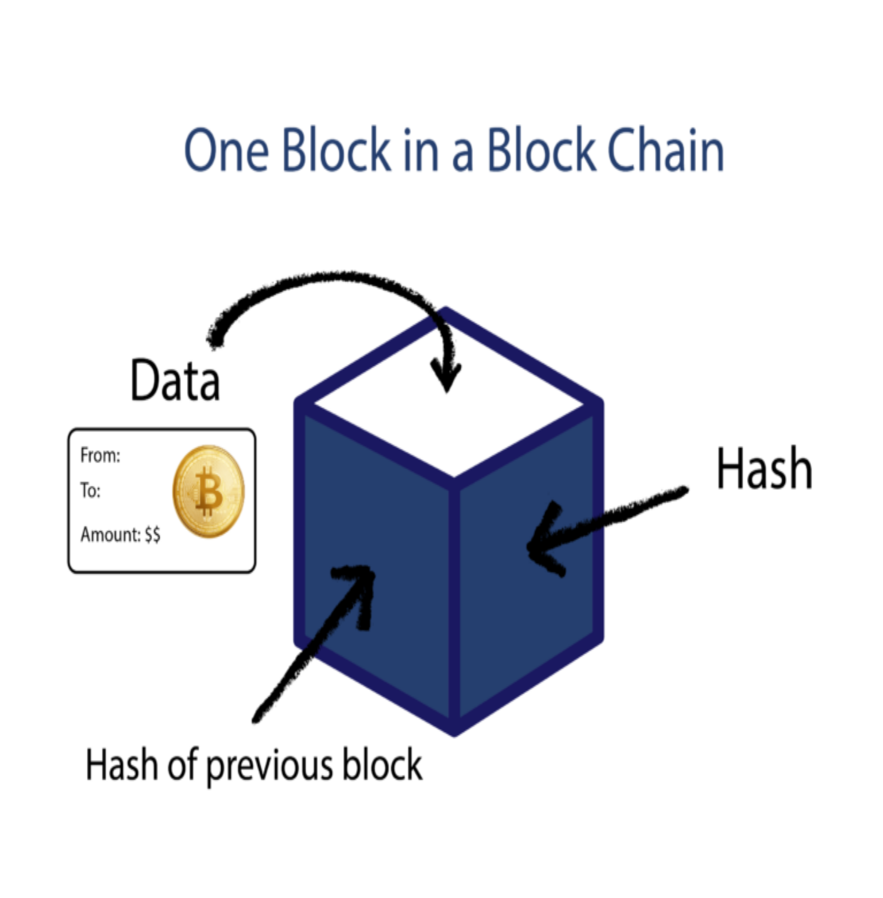
- Automatic execution
- Trustless and tamper-proof
- Reduces costs and speeds up processes

- **Example:**
  A vending machine works like a smart contract. You insert money, select an item, and the machine automatically delivers it if conditions are met.

Block in a Blockchain

- A **block** in a blockchain is a container that holds data (such as transactions), a unique identifier (hash), and a reference to the previous block. These blocks are linked together to form a secure and unchangeable chain.
- **Structure of a Block:**
- Each block typically contains:

1. **Data:** Transaction details (e.g., sender, receiver, amount).
2. **Hash:** A unique identifier for the block.
3. **Previous Hash:** Links to the previous block in the chain.
4. **Timestamp:** Records when the block was created.
5. **Nonce:** A number used in the mining process to validate the block.



Example to Understand:

- Imagine a notebook where each page (block) records financial transactions. Each page references the previous one, ensuring no page can be altered without affecting the entire notebook.
- Example transaction in a block:
- Sender: Alice
- Receiver: Bob
- Amount: 2 BTC
- Timestamp: 24-Jan-2025

What is a Transaction?

- A **transaction** is a record of an exchange of value between two parties. In blockchain, a transaction represents the transfer of digital assets (e.g., cryptocurrency, tokens, or smart contract executions) from one address to another.
- **Example of a Transaction in Blockchain**
- Imagine Alice wants to send 2 Bitcoins to Bob. The transaction process involves:

1. **Alice initiates the transaction** – She enters Bob’s Bitcoin address and specifies 2 BTC.
2. **Transaction is broadcast** – The network nodes receive and verify the transaction.
3. **Miners validate the transaction** – Miners confirm it using a consensus mechanism (e.g., Proof of Work).
4. **Transaction is added to a block** – Once verified, the transaction is recorded in a block.
5. **Block is added to the blockchain** – The updated ledger is shared across all nodes.
6. **Bob receives 2 BTC** – The transaction is completed and permanently stored.

Distributed consensus

- **Distributed consensus** is a way of ensuring that all participants in a network agree on the same data or transaction, even if they are spread across different locations. This is crucial for blockchain and other decentralized systems where there is no central authority.
- **Example:**
- Imagine you and your friends are playing a game, and you all need to agree on the score. You each write down the score on a piece of paper. After each round, everyone compares their score with others. If everyone agrees on the same score, then it's accepted as the official score. If one person has a different score, you figure out why and correct it.

Distributed consensus (Conti...)

- In a **blockchain network**, the participants (called nodes) work the same way. They compare their version of the data (like a transaction) and ensure that everyone agrees. If one node tries to cheat or send incorrect information, the majority of nodes will reject it.
- **Example in blockchain:**
- Alice sends Bob 1 Bitcoin.
- All nodes (computers) on the Bitcoin network check and agree that Alice has enough Bitcoin to send, and they all record the same transaction.
- This consensus process prevents fraud and ensures everyone has the same version of the blockchain.

Distributed consensus (Conti…)

- Example: Forming a Government After an Election (Like PM Voting in India)
- Election Results:
  - *In a general election, different parties contest for seats. Let's say BJP wins the most seats but doesn't have a majority on its own.*
  - *BJP might get 200 seats, but 300 seats are needed for a majority (out of 545).*
- Forming a Coalition:
  - *To form a government, BJP needs to collaborate with other smaller parties or alliances that have some seats but are not enough to form a majority alone.*
  - *After discussions, BJP decides to form a coalition with, say, Party X (which has 50 seats) and Party Y (which has 60 seats). Now, BJP + Party X + Party Y = 310 seats, which is enough for a majority.*

Distributed consensus (Conti…)

- Voting and Consensus:
  - *These parties (like nodes in a blockchain) all agree on who will be the Prime Minister, which party will take which position, and what policies they will support.*
  - *Just like in a distributed consensus (where different nodes need to agree on the same data), in politics, the coalition parties need to agree on the formation of the government. If the majority of parties agree (consensus), the government is formed.*
- Result:
  - *The coalition now has more than 300 seats, which is the majority. They form the new government, and the leader of the largest party, usually the BJP, becomes the Prime Minister.*

Distributed consensus (Conti…)

In this case, like a blockchain, each party is a "node," and their "vote" is part of the consensus process to decide who forms the government. If most parties agree (like most nodes in a blockchain), the decision is finalized.

Public Blockchain:

- A public blockchain is open to everyone. Anyone can join the network, participate in transactions, and view the data stored on the blockchain. It's decentralized, meaning no single entity controls it.
- Example:
  - *Bitcoin is a public blockchain. Anyone can join the Bitcoin network, send or receive Bitcoin, and see all transactions happening on the network. It's like a public ledger where everyone has equal access.*

Private blockchain

- A **private blockchain** is a closed network where only specific, authorized participants can join and see the data. It's often used by businesses or organizations for secure internal use. It's controlled by a central authority or a group of trusted entities.
- **Example:**
  - *A **bank** may use a private blockchain to handle internal transactions and records between its branches. Only authorized employees and systems can participate in this blockchain, and the data is kept private within the organization.*

- **Public Blockchain:** Open to everyone (like Bitcoin).
- **Private Blockchain:** Restricted access for specific users (like a bank's internal ledger).

Understanding Cryptocurrency and Blockchain

- Cryptocurrency is digital money that uses blockchain technology to record transactions. Unlike traditional money, it doesn’t rely on banks or governments.
- **Example:** Bitcoin is a cryptocurrency. If you send Bitcoin to a friend, the transaction gets recorded on the blockchain and is verified by many computers in the network. Once verified, it is permanently stored and cannot be changed.

How Cryptocurrency Uses Blockchain?

- **Transactions are recorded on the blockchain.**
- **No central authority** (like a bank) is needed to process payments.
- **Secure & transparent**—everyone in the network can verify transactions.

■ **Example:**
Imagine you want to send **1 Bitcoin** to your friend:

1. You enter your friend's Bitcoin wallet address and send 1 BTC.
2. The transaction is verified by multiple computers (miners).
3. Once approved, the transaction is added to a block on the blockchain.
4. Your friend receives 1 BTC in their wallet.

Understanding Cryptocurrency and Blockchain

- **Final Connection:**

Blockchain = Technology that records transactions securely.
Cryptocurrency = Digital money that runs on blockchain.

Permissioned Model of Block chain

- A **permissioned blockchain** is a type of blockchain where only approved participants can join the network, validate transactions, and maintain the ledger. It offers more control, security, and efficiency compared to public blockchains.
- **Example:**
- A bank consortium creates a **permissioned blockchain** for secure interbank transactions. Only authorized banks can join the network, validate transactions, and access records. This ensures privacy and faster processing while maintaining trust among participants.
- **Key Features:**
  ✓ Controlled access
  ✓ Higher security
  ✓ Faster transactions
  ✓ Suitable for businesses and organizations

Security Aspects of Blockchain

- Blockchain is designed to be **secure** through various mechanisms that protect data, prevent fraud, and ensure trust.
- **1. Cryptography (Encryption & Hashing)**
- Transactions are **encrypted** and linked using **hash functions**, making data tamper-proof.
  Example: If a hacker tries to change one block, its hash changes, breaking the chain and exposing the tampering.
- **2. Decentralization**
- No single entity controls the blockchain; multiple nodes verify transactions, making it harder to attack.
  Example: A hacker would need to control **51%** of all nodes to manipulate the blockchain, which is nearly impossible in large networks.

Security Aspects of Blockchain

- 3. Consensus Mechanisms (Proof of Work/Stake)
- Transactions must be validated by multiple participants (miners/stakers) before they are added to the blockchain.
  Example: In Bitcoin, miners solve complex puzzles (Proof of Work) to validate transactions, preventing fraud.
- 4. Immutability (Data Cannot Be Changed)
- Once recorded, transactions cannot be altered, ensuring a **trustworthy** history of events.
  Example: If someone tries to modify a past transaction, the network will reject it because all copies must match.

Security Aspects of Blockchain

- **5. Smart Contract Security**
- Self-executing contracts automate agreements but must be **audited** to avoid loopholes.
  Example: A buggy smart contract in Ethereum's DAO hack (2016) led to a **$60M loss** due to an exploit.
- **6. Private & Permissioned Blockchain Security**
- Restricted access ensures only **trusted participants** can join and validate transactions.
  Example: Banks use **Hyperledger Fabric**, a permissioned blockchain, to keep transactions private.

Cryptographic Hash Function

- A Cryptographic Hash Function is a special type of function that takes an input (any data) and produces a fixed-length string (hash) that uniquely represents the input. It is one-way, meaning you cannot reverse it to get the original data.
- https://andersbrownworth.com/blockchain/hash

Cryptographic Hash Function

- Imagine you put a sentence into a hash function:
- **Input:** "Hello, World!"
SHA-256 Hash Output:
64EC88CA00B268E5BA1A35678A1B5316D212F4F366B2477237E3EE4C5AEB6B92
- Even a small change in input creates a completely different hash:
- **Input:** "hello, World!" (lowercase 'h')
SHA-256 Hash Output:
3A28B7B79B36852D4E67287079D95E63FA295BB72A56DE28C5B62882F354D129
- This property makes hash functions useful in **password storage**, **data integrity verification**, and **blockchain technology** (like Bitcoin).

Properties of a hash function

- A cryptographic hash function has five main properties that make it secure and useful:

1. Deterministic
    - *The same input will always produce the same output.*

- Example:
    - *Input: "Hello" → Hash: 2CF24DBA5FB0A30E26E83B2AC5B9E29E1B161E5C1FA7425E73043362938B9824*
    - *Input: "Hello" (again) → Same Hash: 2CF24DBA...*

2. Fast Computation
    - *It should quickly generate a hash for any input.*

- Example:
    - *Even a large document should be hashed in milliseconds.*

Properties of a hash function

3. Preimage Resistance (One-way Property)

  – *Given a hash, you cannot find the original input.*

- Example:
  – *If you see the hash 5D41402ABC4B2A76B9719D911017C592, you cannot easily determine the input was "hello".*

4. Small Change, Big Difference (Avalanche Effect)

  – *A tiny change in input creates a completely different hash.*

- Example:
  – *"Hello" → 2CF24DBA5FB0A...*
  – *"hello" → 5D41402ABC4B2...*
  (Just changing H to h results in a totally different hash.)

Properties of a hash function

5. Collision Resistance

  - *No two different inputs should produce the same hash.*

- Example:
  - *If "apple" and "orange" both had the same hash, the function would be insecure.*
  - *These properties make hash functions essential for password hashing, digital signatures, and blockchain security.*

Hash Pointer

- A hash pointer is a data structure that stores a hash of some data along with a pointer to the data’s location. It helps in ensuring data integrity and security by detecting any changes to the original data.

Hash Pointer

- A hash pointer is like a regular pointer, but instead of just storing the memory address of some data, it also stores the hash of that data. This ensures data integrity, meaning if someone tries to change the data, the hash will no longer match, making tampering detectable.

Example:

Think of a linked list where each node contains:

Data

A hash pointer to the previous node (which includes the hash of that node's data)

🔗 Node 3 → Hash Pointer to Node 2
🔗 Node 2 → Hash Pointer to Node 1
🔗 Node 1 → First Node (No pointer)

If someone tries to modify Node 2’s data, its hash will change, which will break the hash pointer in Node 3, revealing the tampering.

Merkle Tree

- A Merkle Tree is a data structure that organizes multiple data blocks using hashes, forming a tree-like structure. It helps efficiently verify large sets of data, used in blockchain and file integrity verification.

Example:

Imagine you have 4 transactions (A, B, C, D).

- **Compute hashes of each transaction:**

  Hash(A), Hash(B), Hash(C), Hash(D)

- **Pair them and hash again:**

  Hash(AB) = Hash(A) + Hash(B)

  Hash(CD) = Hash(C) + Hash(D)

Merkle Tree

- **Pair the results to get the root hash:**

  Hash(ABCD) = Hash(AB) + Hash(CD)

- The final hash at the top is the Merkle Root, which uniquely represents all transactions. If any transaction changes, the root hash will change, making tampering easily detectable.

- Uses:
  ✅ Bitcoin and Blockchain verification
  ✅ Secure file verification
  ✅ Efficient data validation in distributed systems

Digital Signature

- A digital signature is like an electronic fingerprint that ensures a document or message is authentic and untampered. It uses cryptography to prove that a message was created by a specific sender and hasn't been changed.
- How It Works (Simple Explanation)

A digital signature involves two keys:

Private Key – Used to sign the message (kept secret).

Public Key – Used to verify the signature (shared with everyone).

Digital Signature

- **Example:**

  Imagine Alice wants to send a secure message to Bob:

Alice Signs the Message:

- *Alice writes: "Hello, Bob!"*
- *She applies a hash function to the message.*
- *She then encrypts the hash with her private key (this is the digital signature).*
- *She sends (Message + Signature) to Bob.*

Bob Verifies the Signature:

- *Bob receives the message and signature.*
- *He decrypts the signature using Alice's public key, revealing the original hash.*
- *He hashes the received message himself and compares it with the decrypted hash.*
- ✅*If both hashes match → The message is authentic and untampered.*
- ❌*If they don't match → Someone tampered with the message.*

Digital Signature

- Uses of Digital Signatures:
- ✓ Secure online transactions
  ✓ Digital contracts & legal documents
  ✓ Blockchain & cryptocurrency transactions
  ✓ Software updates verification
- It’s like signing a document with a unique, unforgeable seal!

Public Key Cryptography

- Public Key Cryptography (also called Asymmetric Cryptography) is a method of encrypting and securing data using two keys:
  - ***Public Key*** *– Shared with everyone (used for encryption).*
  - ***Private Key*** *– Kept secret by the owner (used for decryption).*
- This system ensures secure communication, as only the intended recipient can decrypt the message.
- **Example:**
- Imagine **Alice** wants to send a secret message to **Bob** using public key cryptography.

  Bob Generates Two Keys:
  - *Bob creates a* ***Public Key*** *and a* ***Private Key.***
  - *He shares the* ***Public Key*** *with everyone but keeps the* ***Private Key*** *secret.*

Public Key Cryptography

- Alice Encrypts the Message:
  - *Alice takes Bob’s Public Key and encrypts "Hello, Bob!".*
  - *She sends the encrypted message to Bob.*
- Bob Decrypts the Message:
  - *Bob uses his Private Key to decrypt the message.*
  - *Now he can read "Hello, Bob!" securely.*

Public Key Cryptography

- **Why Is It Useful?**
- ✓ Secure online transactions (like credit card payments)
  ✓ Digital signatures for authentication
  ✓ Secure email and messaging (PGP encryption)
  ✓ Blockchain and cryptocurrency transactions
- It's like **a locked mailbox:**

- **Public Key = Mailbox address (anyone can send letters)**
- **Private Key = The key to open the mailbox (only the owner can read messages)**

Basic cryptocurrency

- A cryptocurrency is a digital currency that uses cryptography for security and operates on a decentralized network (usually blockchain). Unlike traditional money, cryptocurrencies are not controlled by banks or governments.
- Example of Cryptocurrency
- Bitcoin (BTC) – The First Cryptocurrency
  - *Alice wants to send 1 BTC to Bob.*
  - *The transaction is recorded on the blockchain (a public digital ledger).*
  - *Miners (special computers) verify the transaction using cryptography.*
  - *Once verified, the transaction is added to a block and becomes permanent & unchangeable.*
  - *Bob receives 1 BTC, and Alice's balance is reduced.*

Key Features of Cryptocurrency

- **Decentralized** – No central authority like a bank.
- **Secure** – Uses cryptography to prevent fraud.
- **Transparent** – Transactions are recorded on a public blockchain.
- **Global & Fast** – Can be sent anywhere, anytime, with low fees.

Other Examples: Ethereum (ETH), Binance Coin (BNB), Solana (SOL), Dogecoin (DOGE).

Thank you