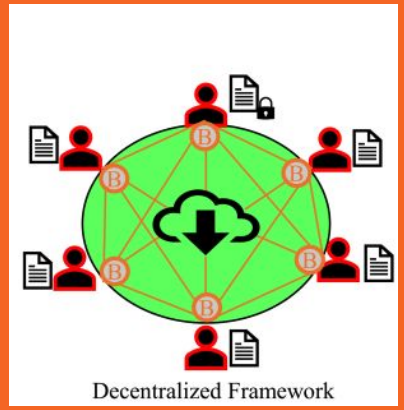
BLOCK CHAIN

-BY HARSH SAREEN

OBJECTIVES FOR THIS SESSION

To truly understand how blockchain works in practice and why individuals should consider embracing it, it’s important to explore its advantages and disadvantages. Gaining clarity on the myths versus the reality of blockchain technology can help guide informed decisions and provide valuable hands-on experience.

Introduction to Blockchain



Blockchain technology is a decentralized, distributed ledger system that records transactions across multiple computers in a way that ensures security, transparency, and immutability. Each transaction is stored in a "block," which is linked to the previous block, forming a chronological "chain." This structure prevents unauthorized modifications and eliminates the need for intermediaries, making it ideal for applications such as cryptocurrency, supply chain management, and secure data sharing.

Lets understand about hawala bazar

Key characteristics: decentralization, immutability, and transparency.

Here are the key characteristics of blockchain technology:

1. **Decentralization**: Blockchain operates on a network of distributed nodes, ensuring no single entity controls the entire system, reducing reliance on intermediaries.
2. **Immutability**: Once data is recorded on the blockchain, it cannot be altered or deleted, ensuring the integrity and trustworthiness of the information.
3. **Transparency**: Transactions on the blockchain are visible to all participants within the network, promoting accountability and openness.

Real-World Applications of Blockchain Characteristics:

Decentralization:

- **Cryptocurrencies** (e.g., Bitcoin, Ethereum): Allow peer-to-peer financial transactions without a central authority like banks.
- **Decentralized Finance (DeFi)**: Enables borrowing, lending, and trading directly between users.

Immutability:

- **Supply Chain Management**: Tracks the journey of goods (e.g., food or medicine) to ensure authenticity and reduce fraud.
- **Record-Keeping**: Secures permanent records for land titles, medical data, and certifications.

Real-World Applications of Blockchain Characteristics:

Transparency:

- **Government and Voting Systems**: Ensures fair elections and prevents tampering by making voting records auditable.
- **Charitable Donations**: Tracks how donations are used, boosting donor trust.

INDUSTRIES WHO ARE USING BLOCKCHAIN

- FINANCE
- HEALTHCARE
- SUPPLY CHAIN MANAGEMENT
- GOVERMENT AND VOTING
- ENTERTAINMENT AND ART

FINANCE

Cryptocurrencies (e.g., Bitcoin, Ethereum) enable peer-to-peer transactions without banks or intermediaries.

Decentralized Finance (DeFi) platforms allow users to lend, borrow, and trade assets without traditional banks.

Cross-border payments are faster and cheaper, reducing the need for third-party remittance services.

HEALTHCARE

Blockchain secures medical records, ensuring privacy and seamless access for authorized personnel.

Tracks the authenticity and origin of pharmaceuticals, preventing counterfeit drugs in supply chains.

SUPPLY CHAIN MANAGEMENT

Provides end-to-end visibility of goods, ensuring authenticity, especially for food, luxury items, and medicines.

Smart contracts automate processes like payment release upon delivery.

GOVERMENT AND VOTING

Blockchain-based voting systems ensure tamper-proof elections by creating transparent and verifiable records.

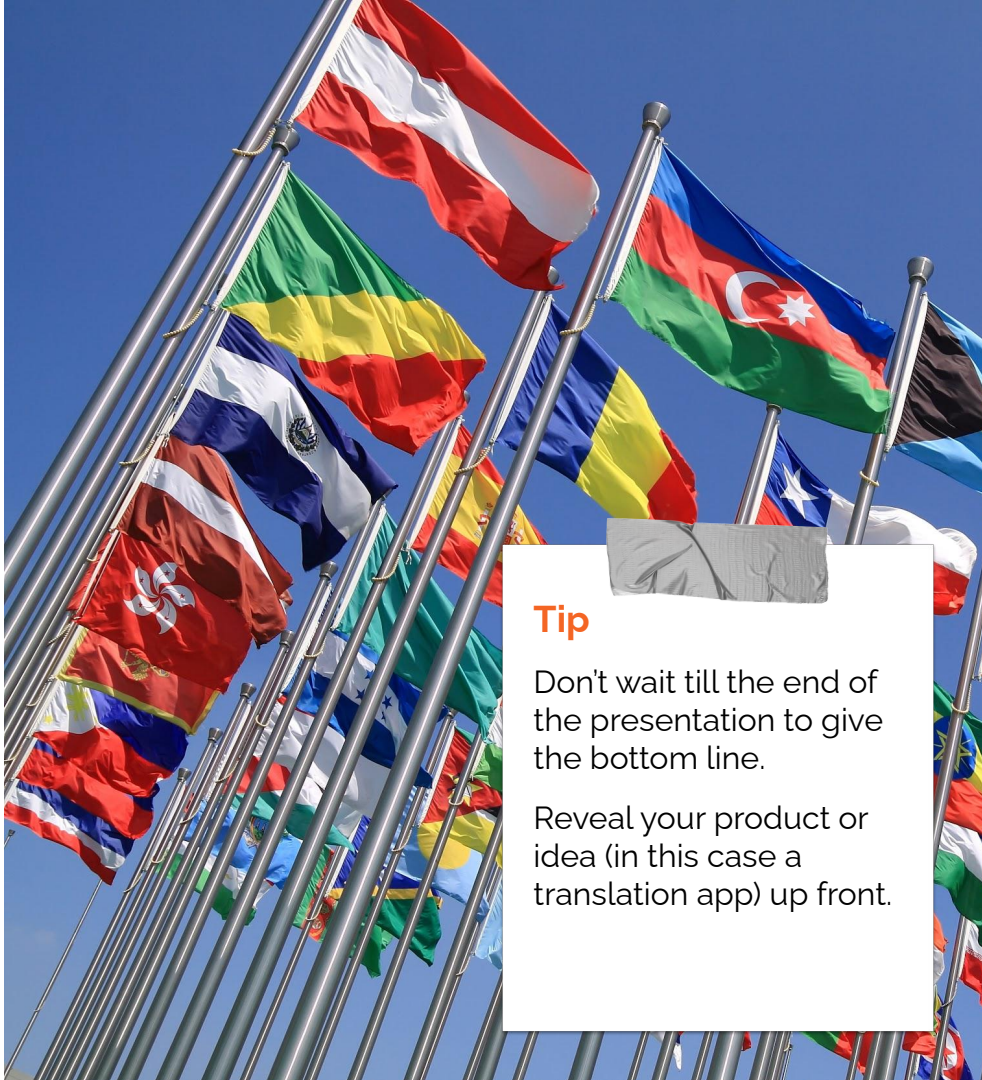
Secure identity management enables digital IDs and prevents fraud in public services.

ENTERTAINMENT AND ART

NFTs (Non-Fungible Tokens) allow artists to monetize digital works by creating unique, provable ownership.

Music streaming platforms distribute royalties transparently to artists without intermediaries.

Components of a blockchain: blocks, chains, nodes, and consensus mechanisms.



Tip

Don't wait till the end of the presentation to give the bottom line.

Reveal your product or idea (in this case a translation app) up front.

Blocks

A block is the basic unit of data storage in a blockchain.

- **Structure of a Block**:
  - **Header**: Contains metadata, including:
    - **Block hash**: A unique identifier generated using cryptographic algorithms, based on the data in the block.
    - **Previous block hash**: Links the current block to the preceding block, creating a chain.
    - **Timestamp**: Records when the block was created.
    - **Nonce**: A number used in the mining process to solve cryptographic puzzles (in Proof of Work).
  - **Transactions**: The actual data or list of transactions recorded in the block.
- **Purpose**:
  - Records all validated transactions in a tamper-proof manner.
  - Blocks are added to the blockchain sequentially, forming a chronological record.

Chains

The chain is the sequence of blocks connected in chronological order.

- **How it works**:
  - Each block contains the hash of the previous block, linking it securely to the chain.
  - This creates an immutable ledger, as altering a single block would require changing all subsequent blocks.
- **Benefits**:
  - **Immutability**: Once added, data cannot be modified or deleted.
  - **Traceability**: The chain ensures that all transactions are recorded in a verifiable sequence.

Nodes

Nodes are individual devices (computers, servers, etc.) that participate in the blockchain network.

- **Types of Nodes**:
  - **Full Nodes**: Store the entire blockchain ledger and participate in validating and relaying transactions.
  - **Light Nodes**: Store only a subset of the blockchain and rely on full nodes for verification.
  - **Mining Nodes**: Perform computational tasks to validate transactions and create new blocks (common in Proof of Work systems).
- **Role of Nodes**:
  - Verify and validate transactions.
  - Store and maintain a copy of the blockchain.
  - Ensure decentralization by distributing the ledger across multiple participants.
- **Key Features**:
  - **Decentralization**: No single node controls the network.
  - **Fault Tolerance**: Even if some nodes go offline, the blockchain remains operational.

Consensus Mechanisms

Consensus mechanisms ensure that all nodes in the blockchain network agree on the validity of transactions and the state of the ledger.

- **Types of Consensus Mechanisms**:
  - **Proof of Work (PoW)**:
    - Miners compete to solve complex mathematical puzzles to validate transactions and create new blocks.
    - Used in Bitcoin and early blockchain systems.
    - Pros: Highly secure.
    - Cons: High energy consumption.
  - **Proof of Stake (PoS)**:
    - Validators are chosen to create new blocks based on the amount of cryptocurrency they hold and are willing to "stake."
    - Used in Ethereum 2.0, Solana, and others.
    - Pros: Energy-efficient and faster.
  - **Delegated Proof of Stake (DPoS)**:
    - Participants vote to elect delegates who validate transactions on their behalf.
    - Example: EOS.
  - **Practical Byzantine Fault Tolerance (PBFT)**:
    - Nodes reach consensus by agreeing on a majority decision, even if some nodes act maliciously.
    - Example: Hyperledger Fabric.
- **Purpose**:
  - Prevent double-spending and fraud.
  - Ensure network participants trust the integrity of the blockchain without relying on a central authority.

How These Components Work Together

A transaction is initiated: A user submits a transaction, which is broadcast to the network.

Validation by nodes: Nodes verify the transaction based on the blockchain's rules (e.g., ensuring the sender has sufficient funds).

Consensus mechanism: Nodes use a consensus mechanism to decide whether to add the transaction to a block.

Block creation: Validated transactions are grouped into a block, which is then added to the chain.

Distributed ledger update: All nodes update their copy of the blockchain to reflect the new block.

Blockchain Mechanics

How Blockchain Works

Hashing

Block Creation

Linking Blocks

Hashing

- **Definition**: Hashing is the process of converting input data into a fixed-length string of characters (a hash) using a cryptographic algorithm (e.g., SHA-256).
- **Purpose**:
  - Ensures data integrity: Any change in data alters the hash completely.
  - Creates a unique identifier for each block.
- **Example**: Input: "Hello, Blockchain!" → Hash: `f4d2c3b7a5e2f9d9230...` Even a small change (e.g., adding a space) will produce a different hash.

Block Creation

- A block contains:
  - **Data**: The actual information (e.g., transactions).
  - **Hash**: A unique hash for the block's content.
  - **Previous Block Hash**: Links the current block to the previous one, forming a chain.
- Process:
  - Transactions are verified.
  - The block is created with the verified data, a timestamp, and the hash of the previous block.
  - Once the block is mined or added, it becomes immutable.

Linking Blocks

The **hash of the previous block** is stored in the current block, ensuring a sequential chain.

Tampering Prevention: If a block's data is altered, its hash changes, breaking the chain.

This makes blockchain highly secure and tamper-resistant.

Public vs. Private Blockchains

Private Blockchain

- **Definition**: A controlled network where only selected participants (nodes) have permission to validate or view data.
- **Examples**: Hyperledger, R3 Corda.
- **Characteristics**:
  - Access Control: Limited to trusted participants.
  - Fast: Fewer participants lead to quicker consensus.
  - Use Cases: Enterprises, supply chain, healthcare.

Smart Contracts

Definition

- **Smart Contracts** are self-executing contracts with the terms of the agreement directly written into code.
- They run on blockchain networks (e.g., Ethereum).

Functionality

- Automatically enforce agreements when predefined conditions are met.
- Examples:
  - A payment is released when goods are delivered.
  - Insurance claims are automatically processed based on trigger events.

Examples of Use Cases

- **Decentralized Finance (DeFi)**: Loans, lending, and trading.
- **Supply Chain**: Tracking shipments and ensuring payments.
- **Real Estate**: Automating property ownership transfers.

Consensus Mechanisms

Proof of Work (PoW)

- **Definition**: Miners compete to solve a complex mathematical problem (hashing) to validate transactions and add a new block.
- **Key Features**:
  - Energy-intensive: Requires high computational power.
  - Secure: Difficult to tamper with the network.
- **Example**: Bitcoin.
- **Drawbacks**:
  - High energy consumption.
  - Slower transaction speeds.

Consensus Mechanisms

Proof of Stake (PoS)

- **Definition**: Validators are chosen based on the amount of cryptocurrency they "stake" as collateral.
- **Key Features**:
  - Energy-efficient: Eliminates the need for mining.
  - Faster: Transactions are validated more quickly.
- **Example**: Ethereum 2.0.
- **Drawbacks**:
  - Potential centralization: Wealthier participants have more influence.

THANKYOU!!!!