Unit-I Introduction

Blockchain technology revolutionizes digital transactions by providing a decentralized, secure, and transparent framework for recording data. This distributed ledger system underpins cryptocurrencies like Bitcoin and enables innovations such as smart contracts while ensuring data integrity through cryptographic principles and consensus mechanisms. Below is a structured overview of blockchain fundamentals and related concepts.

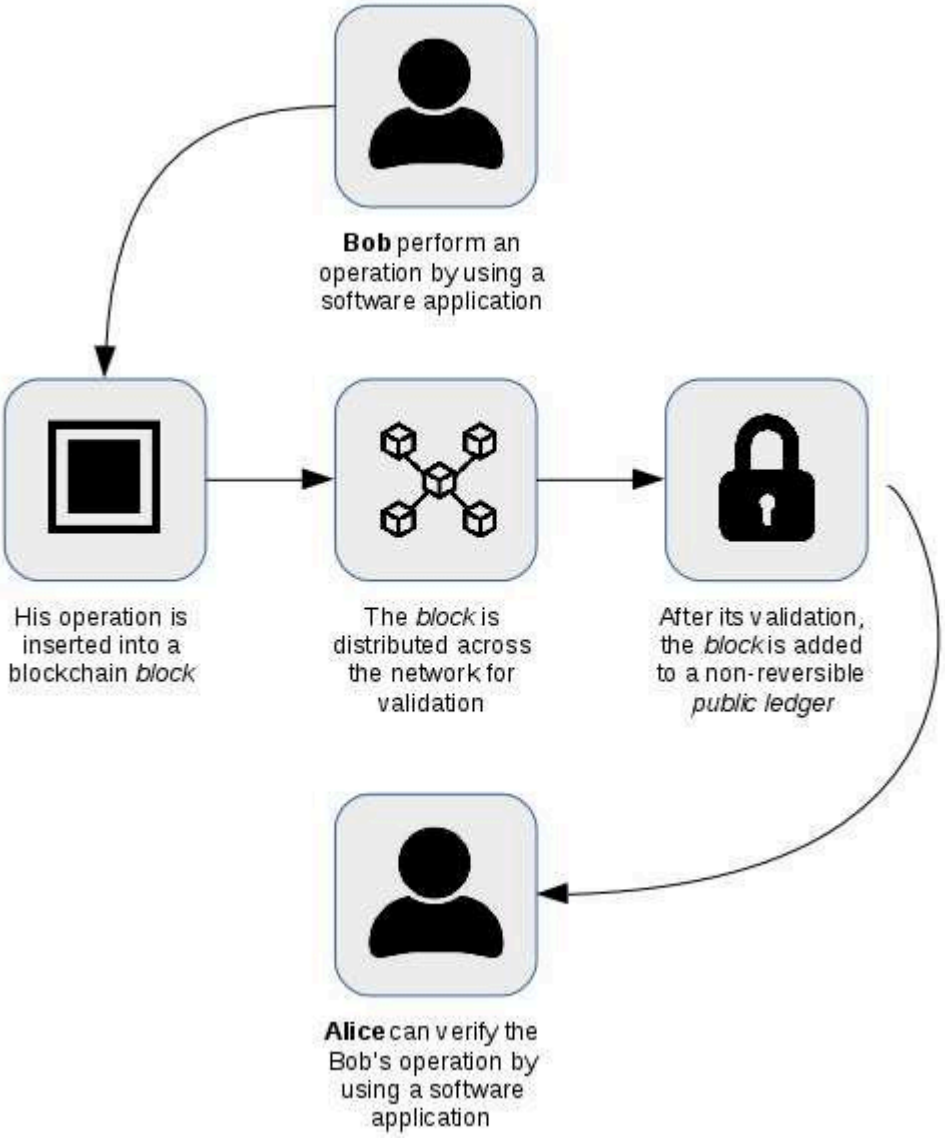
Introduction to Blockchain

Blockchain is a **shared, immutable digital ledger** that records transactions and tracks assets across a decentralized network[1]. It operates as a distributed database where data is stored across multiple computers, making it tamper-resistant[1]. Each transaction is grouped into blocks, cryptographically linked to form a chain, ensuring data integrity and transparency[15]. This structure eliminates the need for traditional intermediaries (e.g., banks), reducing fraud risks and streamlining processes in industries like finance and healthcare[16].

Public Ledgers

A **cryptocurrency public ledger** is a decentralized record-keeping system that uses cryptography to secure transaction data while allowing public visibility. Key features include:

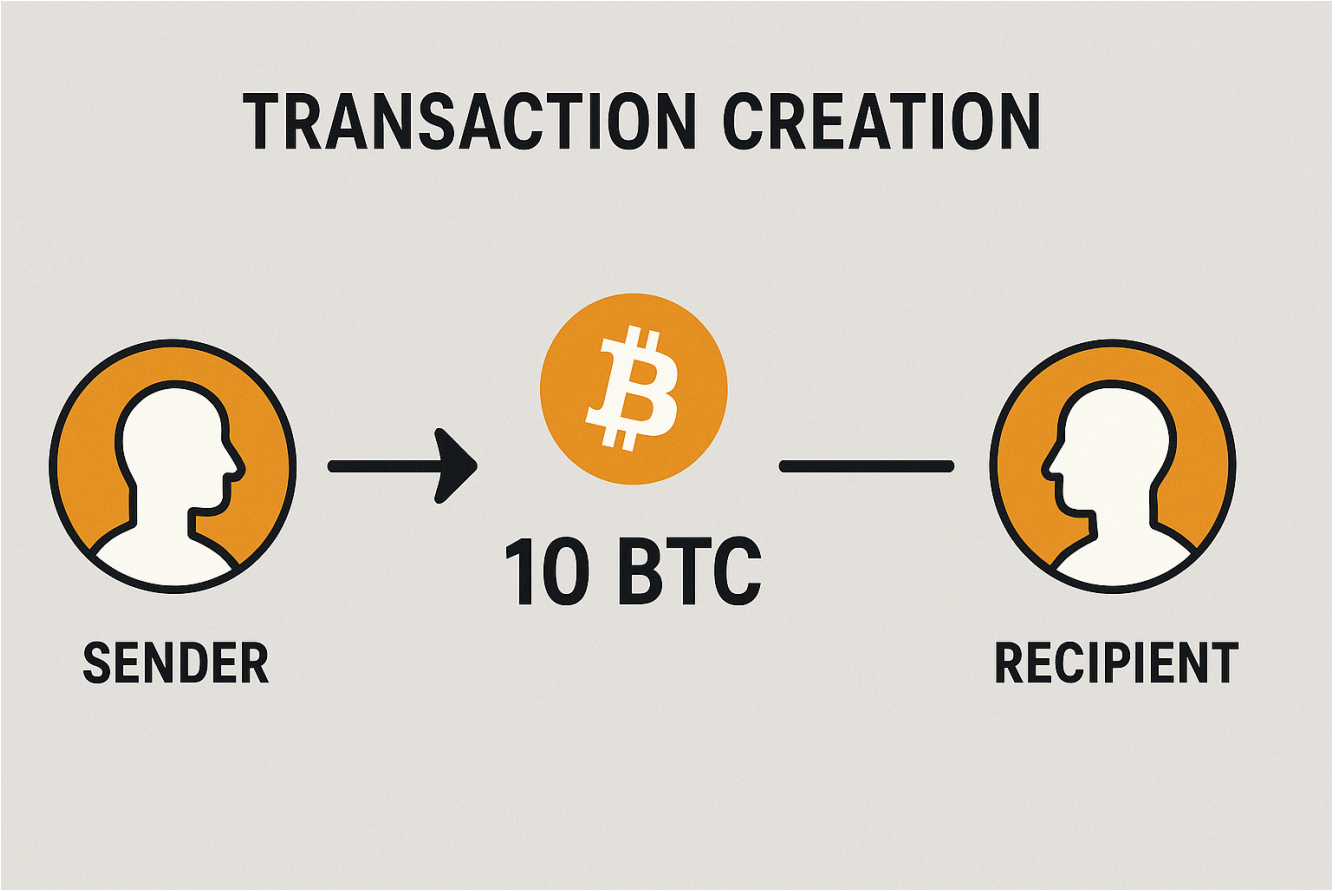
- **Pseudo-anonymization** of participant identities
- **Automated verification** of token ownership and transfers
- **Distributed consensus protocols** to maintain ledger security[2].
  These ledgers—commonly called blockchains—remove human auditing, reducing errors and corruption.



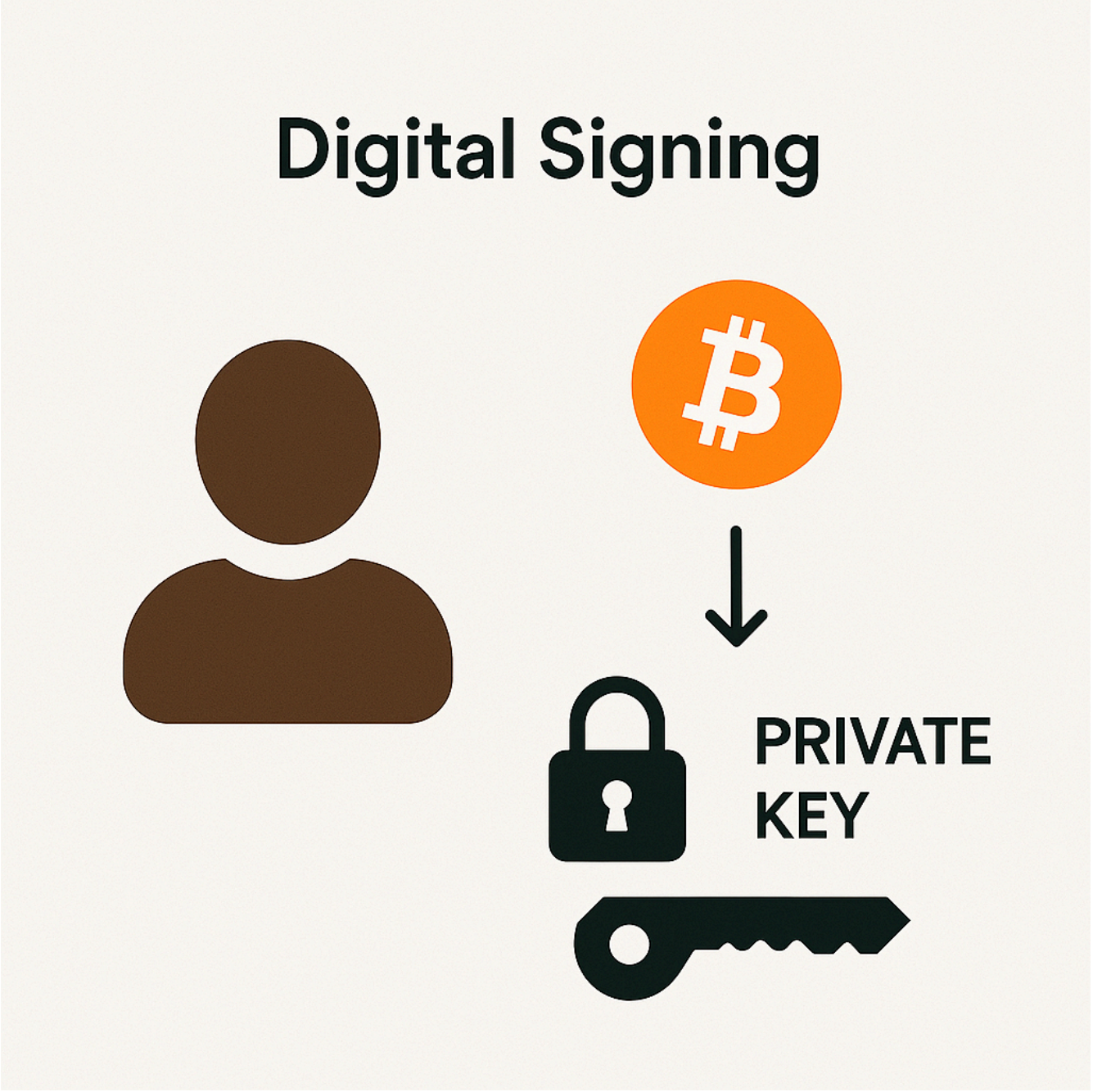
Bitcoin

Bitcoin is a **peer-to-peer digital currency** operating without central authority. Its workflow involves:

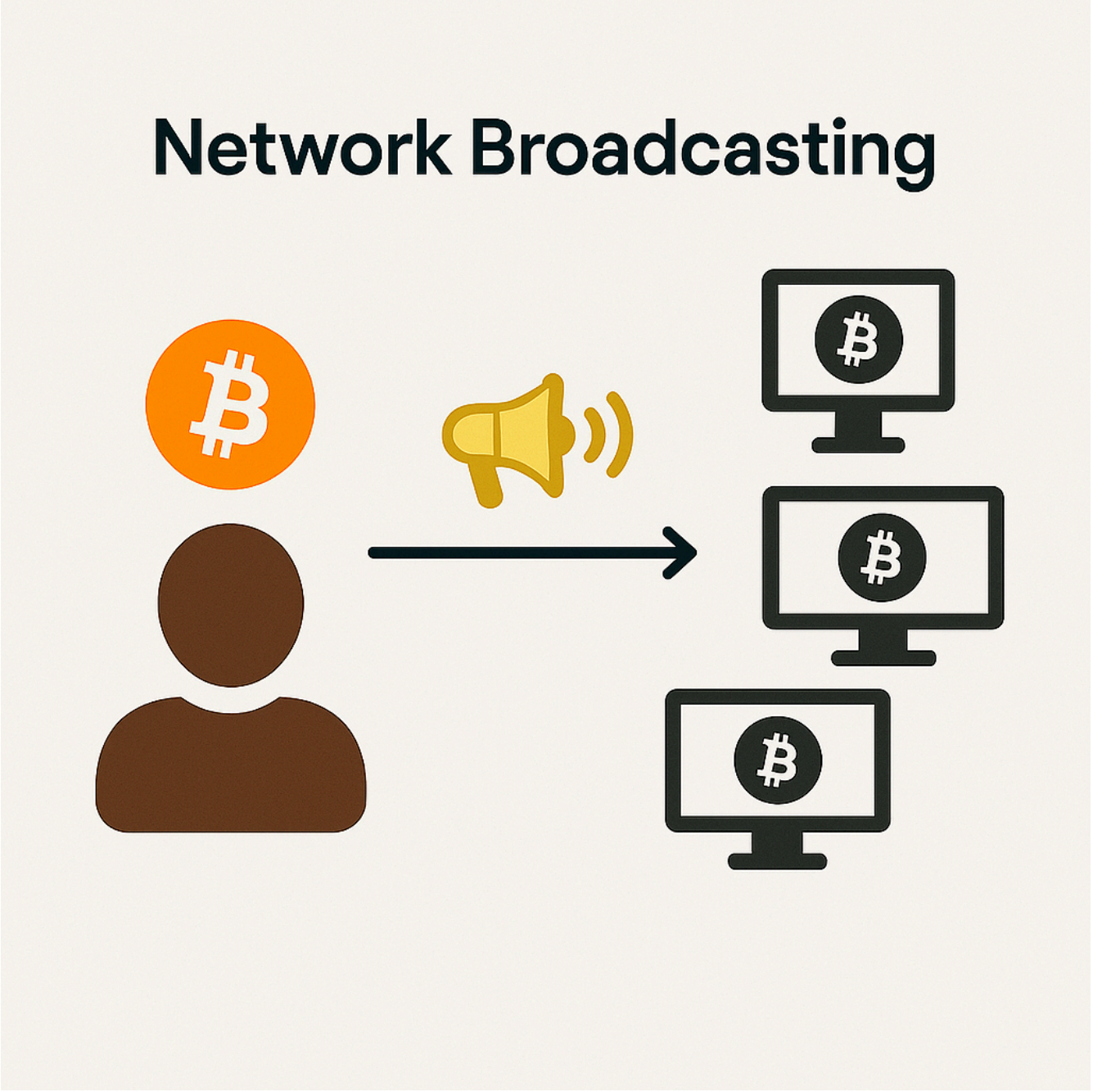
1. **Transaction creation**: Sender specifies recipient and amount.



2. **Digital signing**: Sender uses a private key to authorize the transfer.



3. **Network broadcasting**: Miners verify and include the transaction in a block.



4. **Mining**: Miners solve cryptographic puzzles to add blocks to the blockchain.

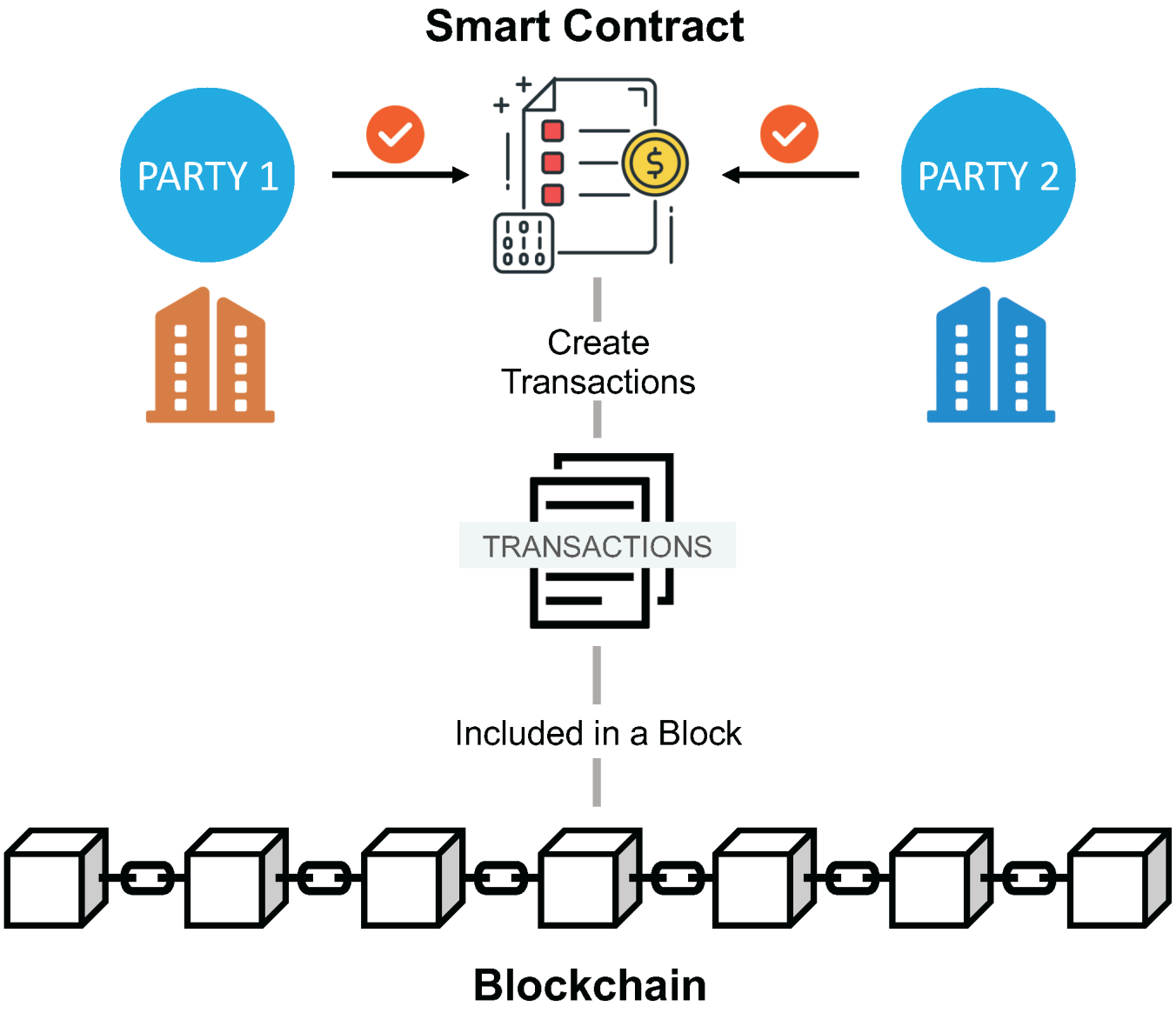
5. **Confirmation**: Immutable recording after block addition.

Users need only a crypto wallet (with public/private keys), internet access, and an exchange for acquisition.

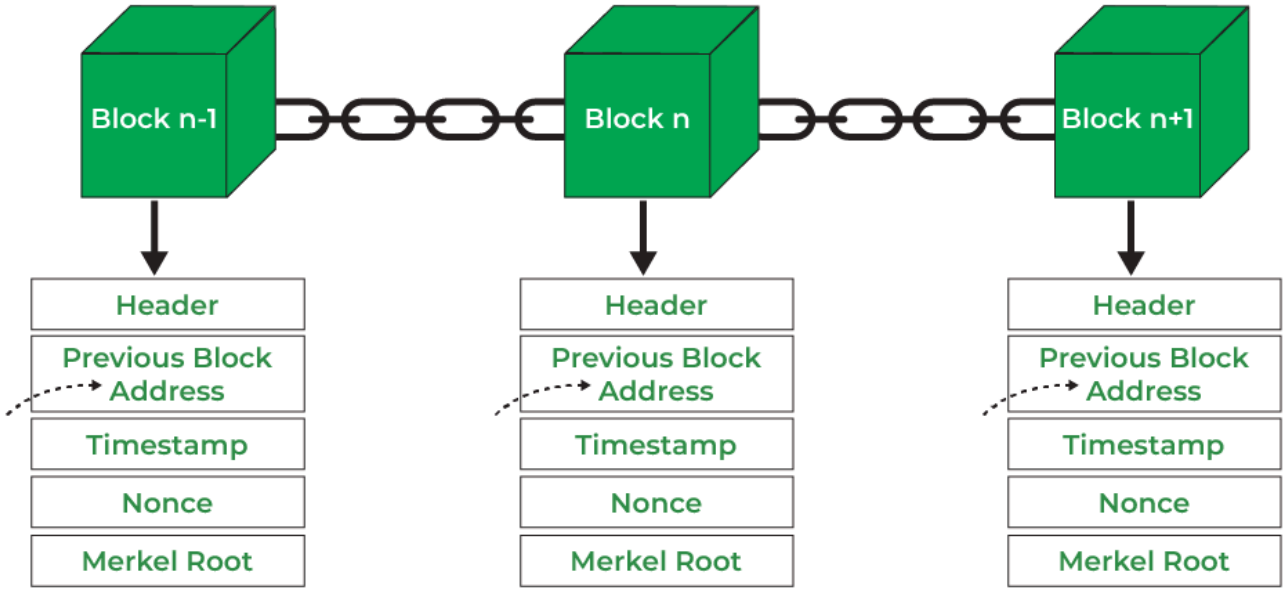
Smart Contracts

Self-executing digital contracts stored on blockchains automate agreements when predefined conditions are met. They:

- Use "if/when...then..." coded logic to trigger actions (e.g., fund releases or notifications).
- Eliminate intermediaries, ensuring immediate, tamper-proof outcomes.
- Require participants to define terms, exceptions, and dispute-resolution frameworks before deployment.



Block in a Blockchain



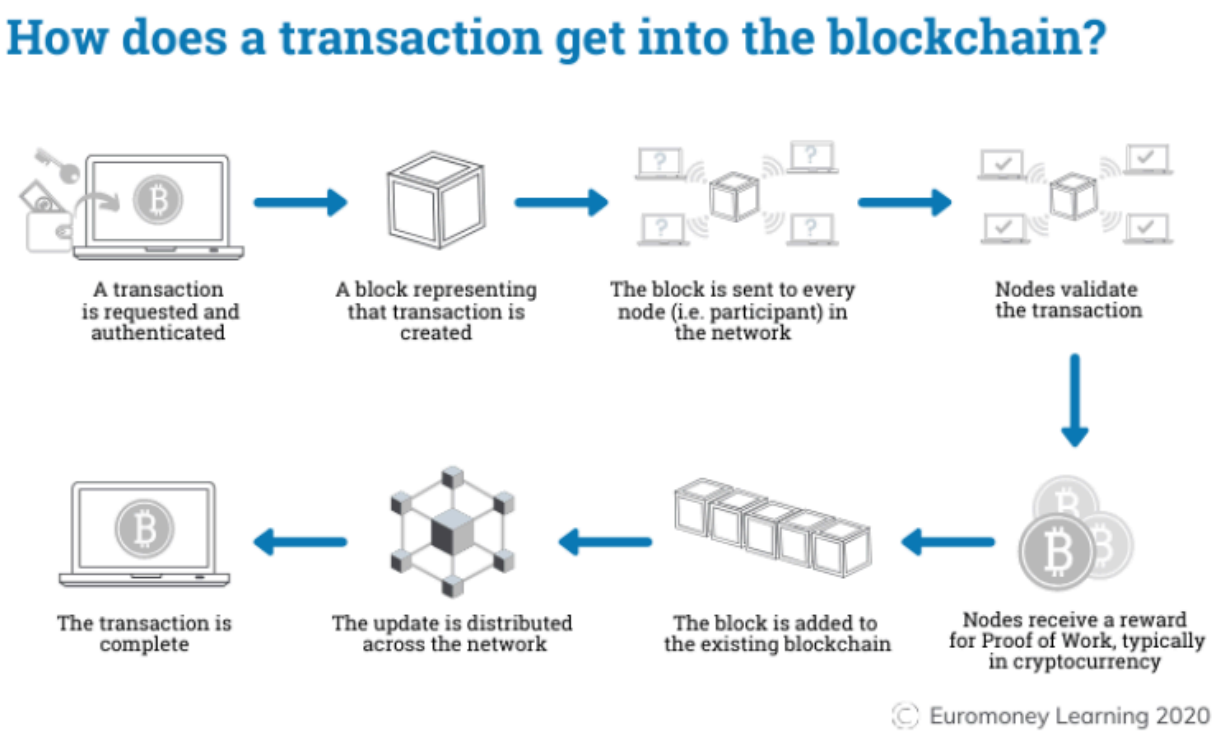
A **block** is a digital container storing verified transaction data. Its structure includes:

- **Header**: Version, previous block's hash, timestamp, and nonce (PoW) or validator list (PoS).
- **Body**: Transaction records.
  Blocks are validated via consensus (e.g., Proof-of-Work mining or Proof-of-Stake validation) and chained using cryptographic hashes, ensuring immutability.

Transactions

Transactions represent **asset transfers** recorded on the blockchain. Each includes:

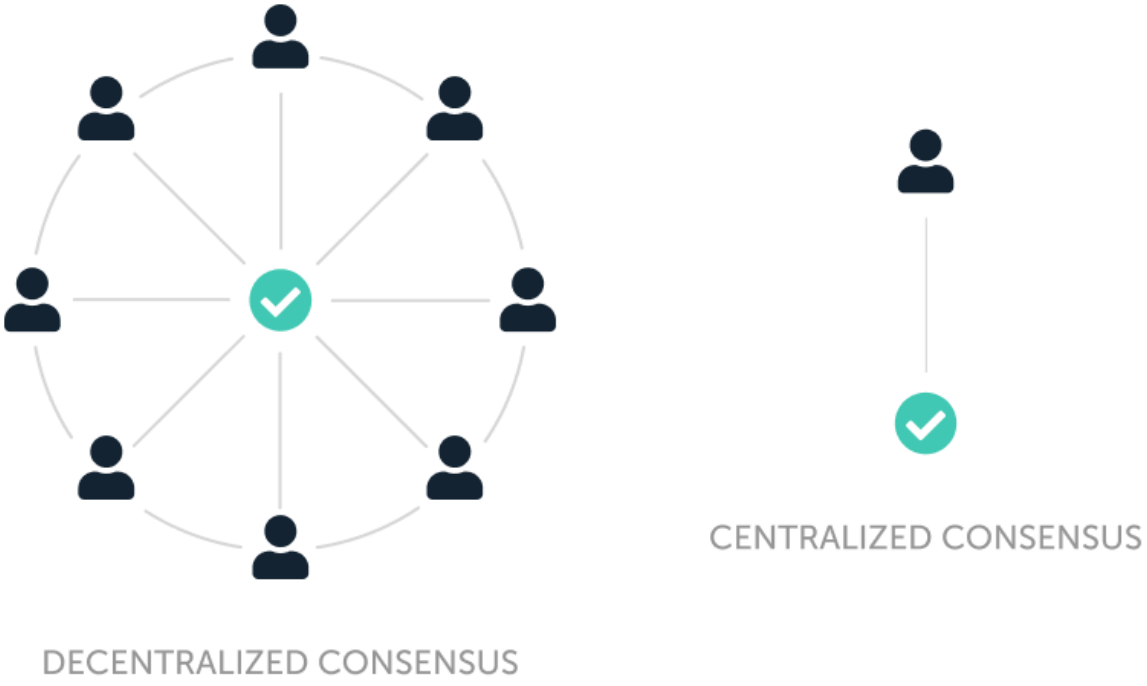
- Involved parties
- Asset quantity
- Timestamp and location
- Preconditions.
  Consensus among network participants validates transactions before permanent recording.



Distributed Consensus(A general agreement)

Agreement protocols validate transactions without central authority:

- **Proof-of-Work (PoW)**: Miners compete to solve cryptographic puzzles (used by Bitcoin).
- **Proof-of-Stake (PoS)**: Validators stake tokens to participate in verification (e.g., Ethereum).
  Both methods ensure transaction legitimacy and ledger consistency.



Iska matlab sab nodes (computers) ka **agreement hona** ki kaun sa block sahi hai. Common consensus methods:

Proof of Work (PoW) and **Proof of Stake (PoS)** are consensus mechanisms used in blockchain networks to agree on the state of the ledger and secure the network. But they go about it quite differently:

🛠 Proof of Work (PoW)

Think of this like a race to solve a super difficult puzzle.

- **How it works:** Participants (miners) compete to solve complex cryptographic problems. The first one to succeed gets to validate the transaction block and is rewarded.
- **Energy use:** Very high—because it requires immense computational power.
- **Security:** Extremely secure, but resource-intensive.
- **Used by:** Bitcoin, for example.

⛏️ It's kind of like having a global math competition every 10 minutes just to keep things honest.

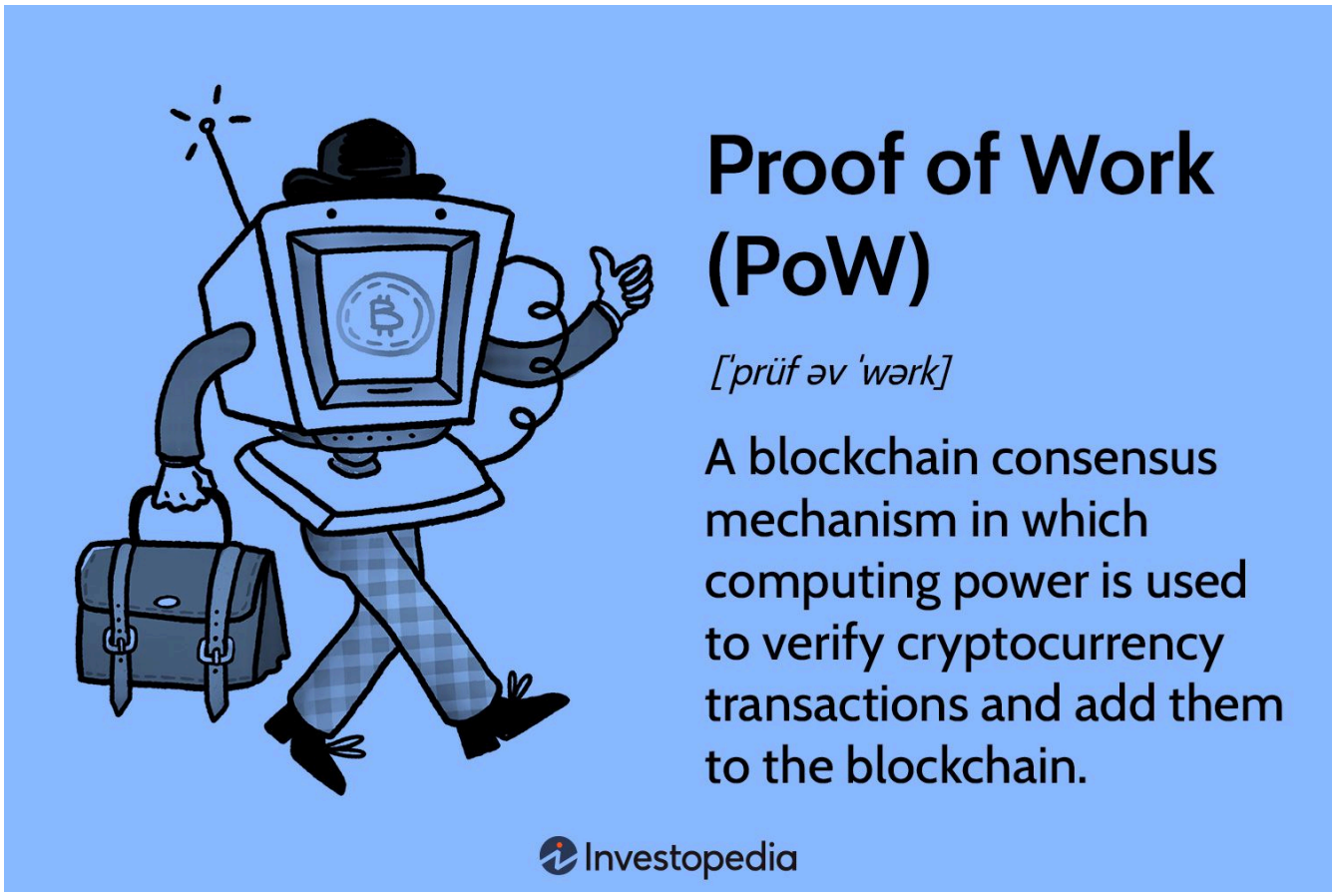
💰 Proof of Stake (PoS)

Instead of computing power, it's based on trust and financial stake.

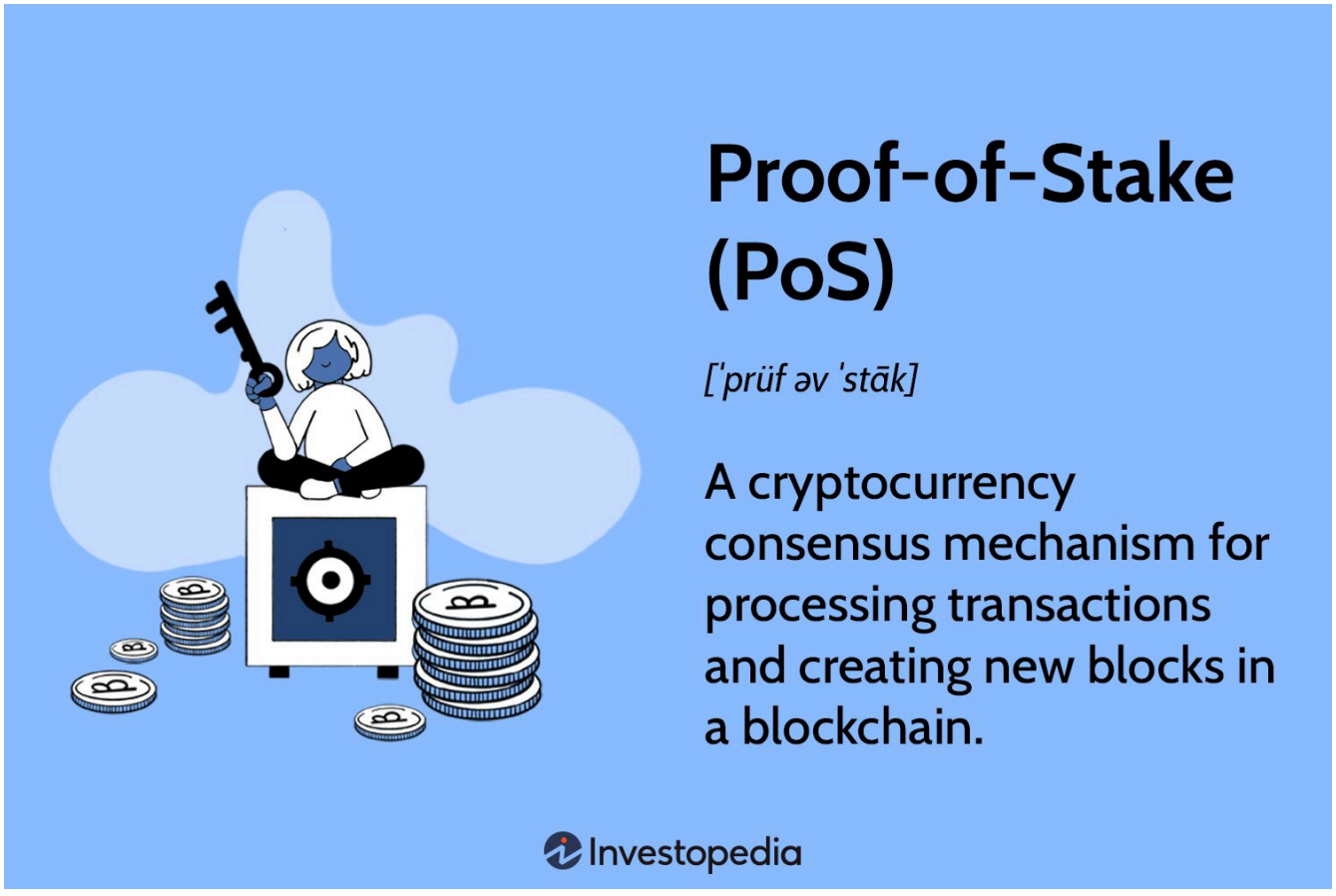
- **How it works:** Validators are chosen based on the amount of cryptocurrency they "stake" or lock up. The more you stake, the better your chances to validate the next block.
- **Energy use:** Much lower—no heavy computing needed.
- **Security:** Still strong, with mechanisms like slashing to penalize bad actors.
- **Used by:** Ethereum (since it transitioned from PoW), Cardano, Solana, and others.

 It's more like putting your money where your mouth is—and getting rewarded for being honest.

- Proof of Work (PoW)



- Proof of Stake (PoS)



Yeh ensure karta hai ki blockchain me sirf valid data hi add ho.

Public vs Private Blockchain

Feature	Public Blockchain	Private Blockchain
Access	Permissionless (anyone can join)	Permissioned (restricted access)
Control	Decentralized	Centralized entity
Use Cases	Cryptocurrencies (Bitcoin)	Enterprise applications
Consensus	PoW/PoS	Varied (e.g., voting-based)
Public blockchains prioritize transparency; private blockchains optimize for efficiency and control[16].		

Understanding Cryptocurrency to Blockchain

Cryptocurrencies rely on blockchain as their **foundational infrastructure**. The relationship enables:

- **Decentralization**: Peer-to-peer transactions without banks.
- **Security**: Tamper-proof transaction recording.
- **Transparency**: Publicly verifiable ledgers[6].
  Blockchain's immutability solves issues like double-spending, making cryptocurrencies viable[16].

Permissioned Model of Blockchain

In **permissioned blockchains**, access is restricted to authorized participants. This model:

- Enhances privacy for sensitive data (e.g., supply chains).
- Uses tailored consensus mechanisms (e.g., voting).
- Balances decentralization with regulatory compliance.

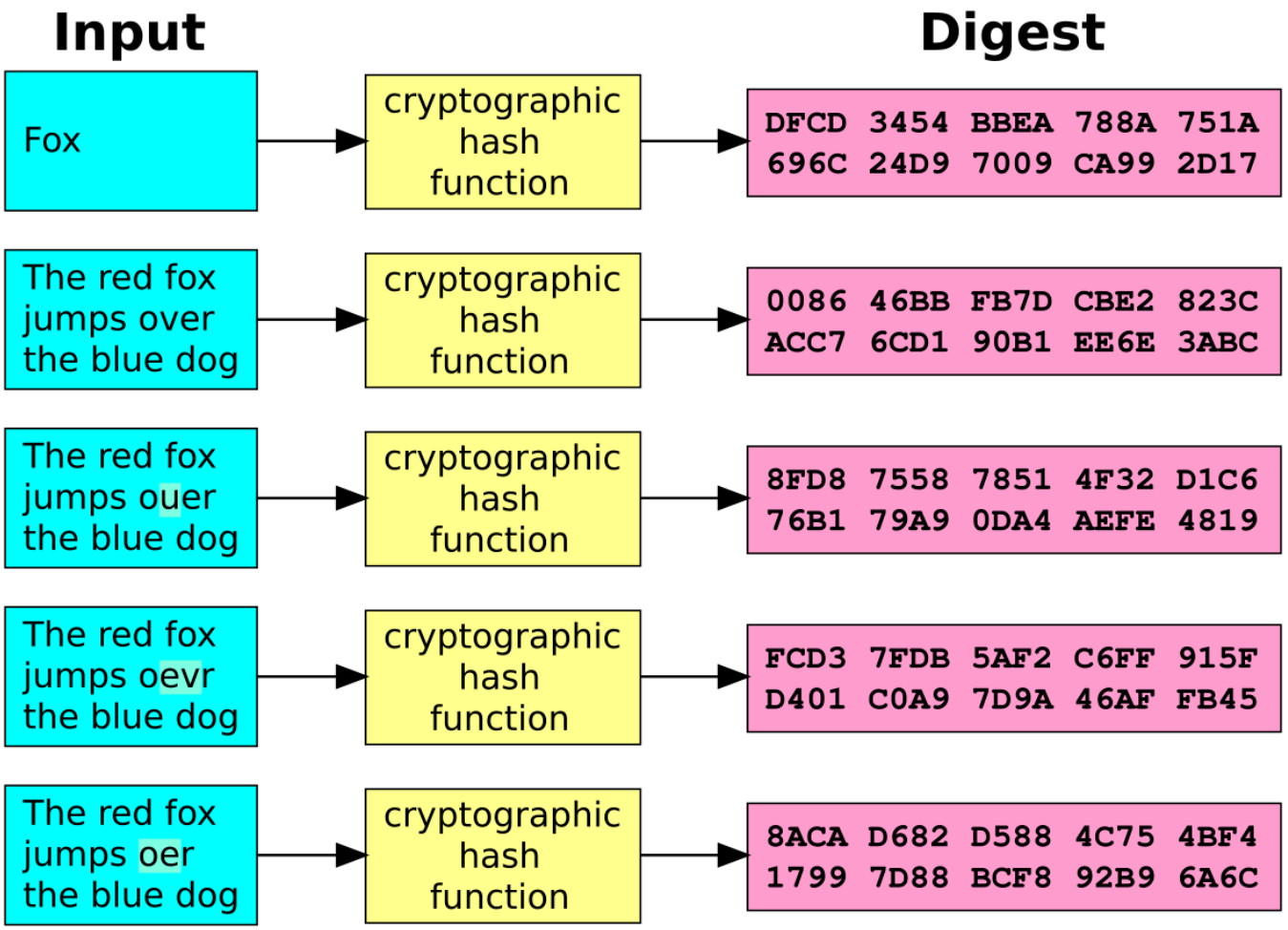
Security Aspects of Blockchain

Key security features include:

- **Immutability**: Transactions cannot be altered post-consensus.
- **Cryptographic hashing**: Each block links to the prior via unique hashes, preventing tampering.
- **Transparency**: Public ledgers enable real-time auditing.
  Challenges include scalability and maintaining decentralization-security tradeoffs.

Basic Cryptographic Primitives

Cryptographic Hash Function



A **one-way function** converting input to a fixed-size output (hash).

Properties:

- **Deterministic**: Same input → same hash.
- **Preimage resistance**: Hash cannot reveal input.
- **Collision resistance**: Unique inputs → unique hashes.

Hash Pointer and Merkle Tree

- **Hash pointer**: Stores data location and its hash, enabling tamper detection1.
- **Merkle tree**: Hierarchical hash structure verifying data integrity in blocks (e.g., Bitcoin transactions)15.

Digital Signature and Public Key Cryptography

- **Digital signature**: Proves authenticity using a sender's private key, verifiable via public key34.
- **Public key cryptography**: Asymmetric encryption for secure transactions (e.g., Bitcoin transfers)36.

Basic Cryptocurrency

A **decentralized digital currency** using:

- Blockchain for transaction recording.
- Cryptographic hashing and digital signatures for security.
- Consensus for validation (e.g., Bitcoin's PoW)[36].

Blockchain's fusion of cryptography, decentralization, and consensus creates a paradigm shift in secure digital interactions, extending beyond cryptocurrencies to supply chains, identity management, and automated contracts.

- 2️⃣ **Consensus Protocols**

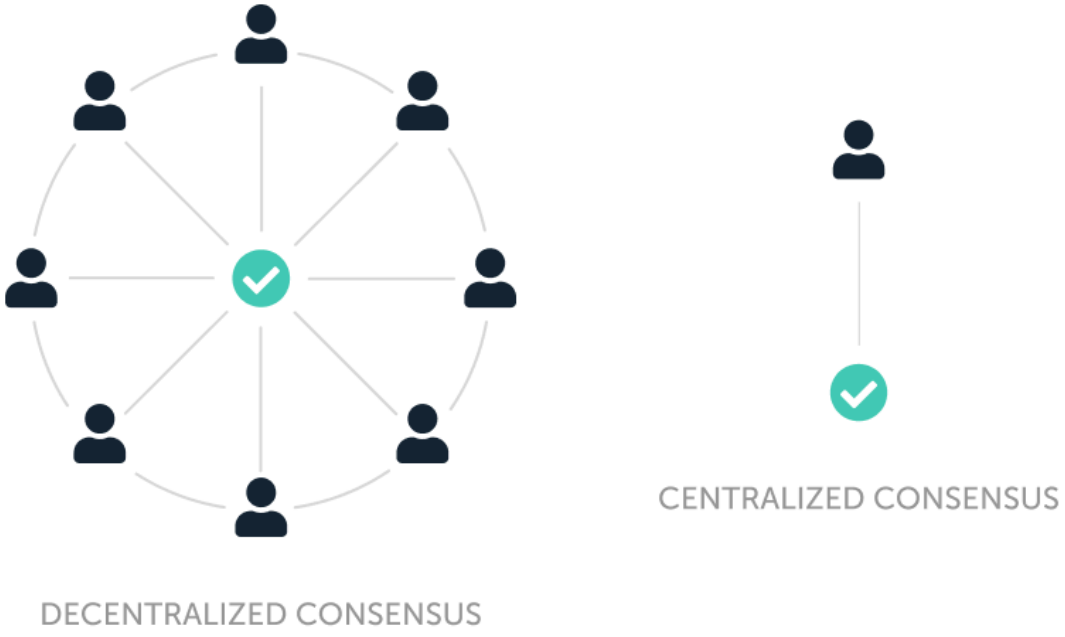
  Definition:
  Consensus protocol ek set of rules hota hai jisme **blockchain ke sare nodes (computers)** agree karte hain ki kaunsa transaction valid hai.

  Popular Types:

  - 🔨 **Proof of Work (PoW)** – Mining kar ke problem solve karna padta hai (Bitcoin ka method)
  - □ **Proof of Stake (PoS)** – Jitna zyada coin hold, utna zyada power to validate

  Purpose:

  - Double spending se bachata hai
  - Fraudulent transaction reject karta hai
  - Decentralized agreement banata hai (no single boss)



  -

3️⃣ Immutability

Definition:
Immutability ka matlab hota hai **ek baar data blockchain pe chala gaya, toh use delete ya change nahi kiya ja sakta**.

Kaise kaam karta hai?

- Har block ka link uske pehle block ke hash se hota hai (hash pointer)
- Agar koi ek block me data change kare, toh uske baad ke sab blocks ka hash change ho jaayega → easily detect ho jaata hai

Result:

- Data tamper-proof hota hai
- Pure ledger trusted rehta hai

Isse data tamper-proof aur trustable hota hai.

🔒 Basic Crypto Primitives

🔷 1. Cryptographic Hash Function

Ye ek mathematical function hota hai jo kisi bhi data ko **fixed-size hash value** mein convert karta hai.

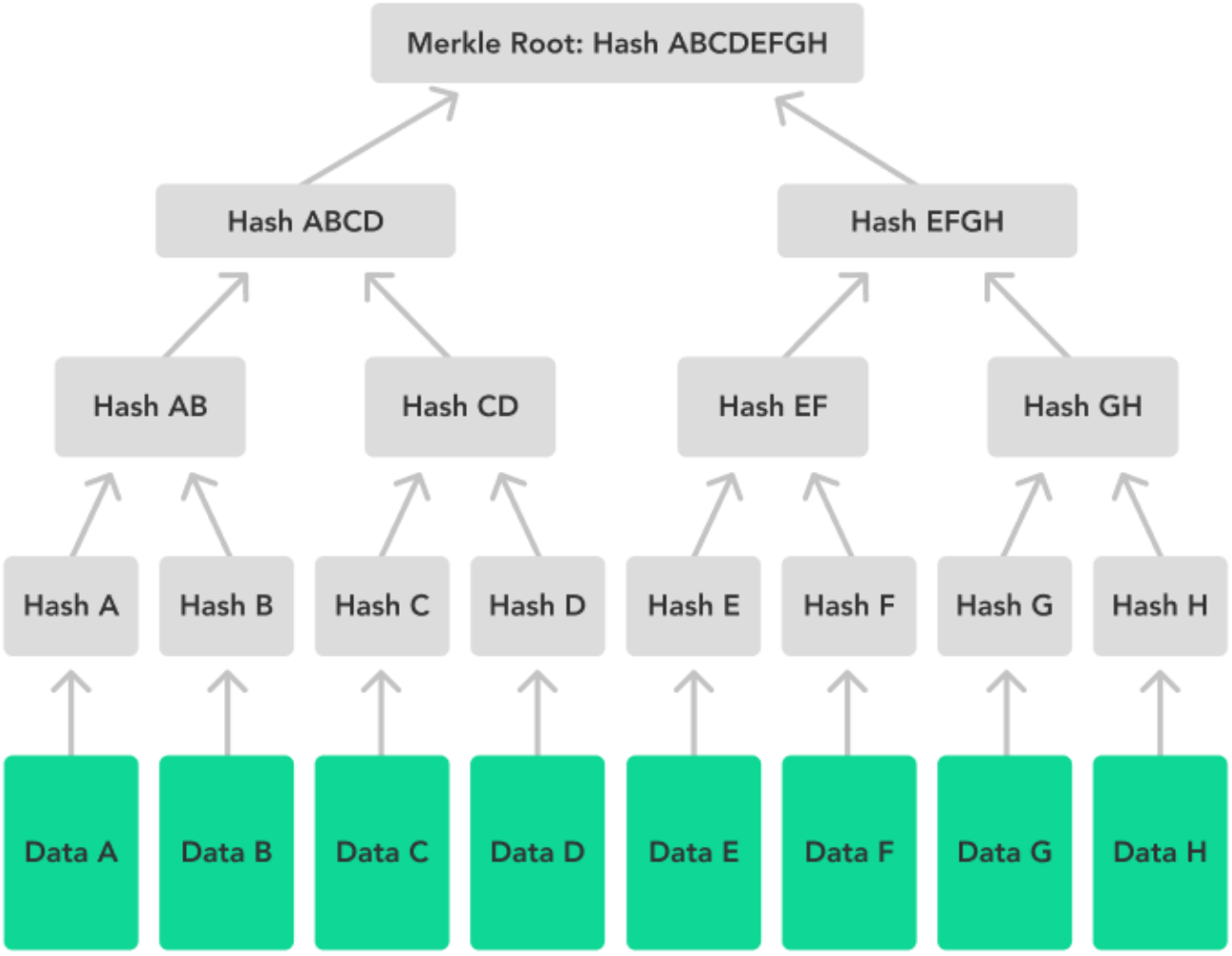
Example: SHA-256 → 64-character hexadecimal hash banata hai.

🔷 2. Properties of a Hash Function

- **Deterministic** – Same input = same output
- **Quick Computation**
- **Pre-image resistance** – Output se input guess nahi kar sakte
- **Collision resistance** – 2 inputs ka same output nahi ho sakta
- **Avalanche Effect** – Thoda input change → bada output change

---

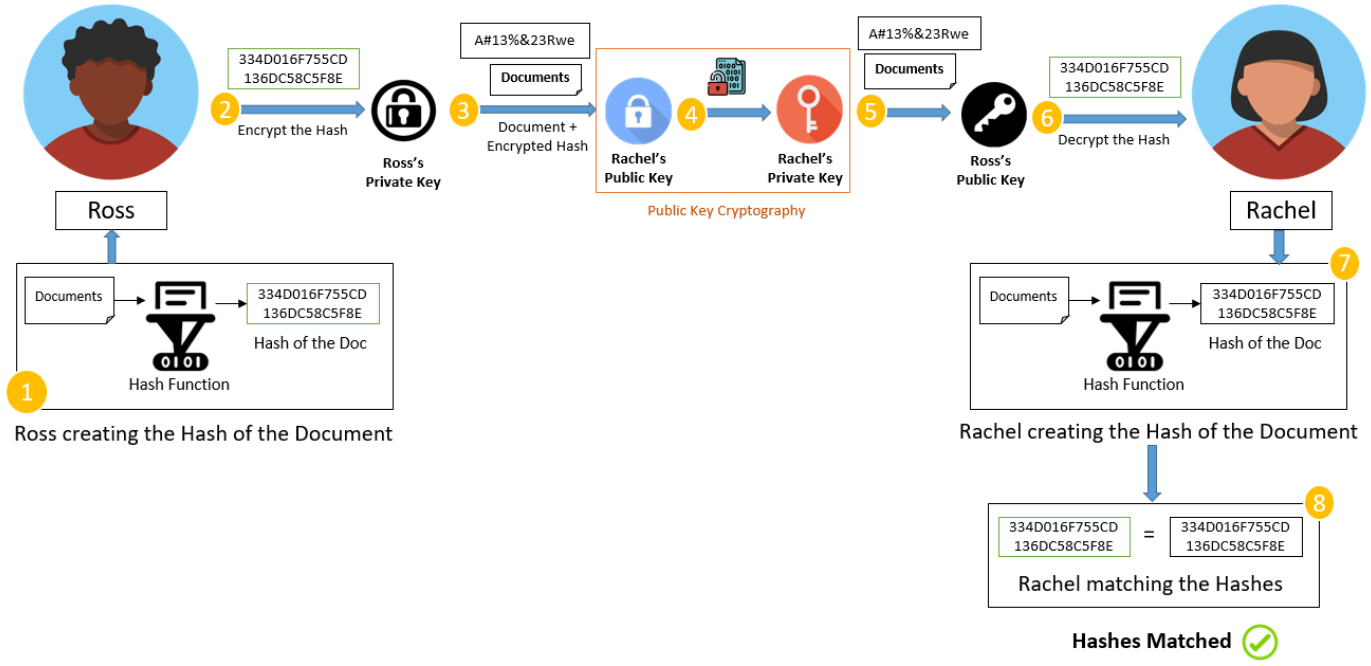
🔷 3. Hash Pointer and Merkle Tree



- **Hash Pointer**: Ek pointer jo kisi data aur uske hash ko refer karta hai.
- **Merkle Tree**: Tree structure where leaves are hashes of transactions, and each parent is a hash of its children. Root hash se pura data verify hota hai.

🔷 4. Digital Signature

Ye ek cryptographic technique hai jisse **sender ki identity verify hoti hai** aur data ka tampering detect hota hai. Sender apni private key se sign karta hai, aur receiver uski public key se verify karta hai.



💼 Scene:

Ross ek document bhejna chahta hai Rachel ko, aur vo chahta hai Rachel trust kare ki:

1. Document **waaqai Ross ne bheja hai**
2. **Bina ched-chaad ke** mila hai

🔢 Step-by-Step Explanation:

✅ STEP 1:

🔁 Ross ne document ka hash banaya

- Jaise tu ek fingerprint nikalta hai kisi cheez ka — waise hi **document ka ek short unique hash** banaya.
- Ye hash function se nikalta hai (e.g., SHA256).

> 📄 → 🧮 → `334D016F755CD136DC58C5F8E`

✅ STEP 2:

🔐 Ross ne apni private key se hash ko encrypt kiya

- Ye ban gaya **Digital Signature**.
- Sirf Ross ke paas hoti hai private key = prove karta hai **"main hi hoon bhai, fake nahi."**

✅ STEP 3:

📦 **Ross ne Document + Encrypted Hash (signature)** ko send kiya Rachel ko

✅ STEP 4 & 5:

🔒 Rachel ne document receive kiya, ab vo verify karegi ki sach me Ross ne sign kiya tha ya nahi.

✅ STEP 6:

🔓 **Ross ki public key se encrypted hash decrypt kiya**

- Public key sabke paas hoti hai
- Agar isse decrypt kar paayi to **iska matlab ye hash Ross ki private key se encrypt hua tha**
- ✅ Identity verified!

✅ STEP 7:

🧮 **Rachel ne bhi wahi document ka hash banaya** (same process as Ross did in Step 1)

✅ STEP 8:

✅ Rachel ne dono hash compare kiya:

- Decrypted hash (from Ross's signature)
- Freshly generated hash (from received doc)

Agar dono match karte hain 👉
🔒 **Document me koi changes nahi hue + Ross ne hi bheja tha** ✅

🔚 Final Result:

🎉 **Hashes Matched** =

- 📦 Document original hai
- ✍️ Sign Ross ka hai
- 🔒 Bina tampering ke mila

🔷 5. Public Key Cryptography

Ismein do keys hoti hain:

- **Public Key**: Sabko diya ja sakta hai
- **Private Key**: Secret rakha jaata hai
  Ye pair milke encryption-decryption aur digital signature mein use hota hai.

🔷 6. A Basic Cryptocurrency

Cryptocurrency ek **digital asset** hai jo blockchain pe based hota hai, aur jiska use value transfer ke liye hota hai.
Key features:

- Uses blockchain
- No central authority
- Secured by cryptography
- Eg: Bitcoin, Ethereum