

# Apply Fundamentals of Blockchain



**Lecturer 1**

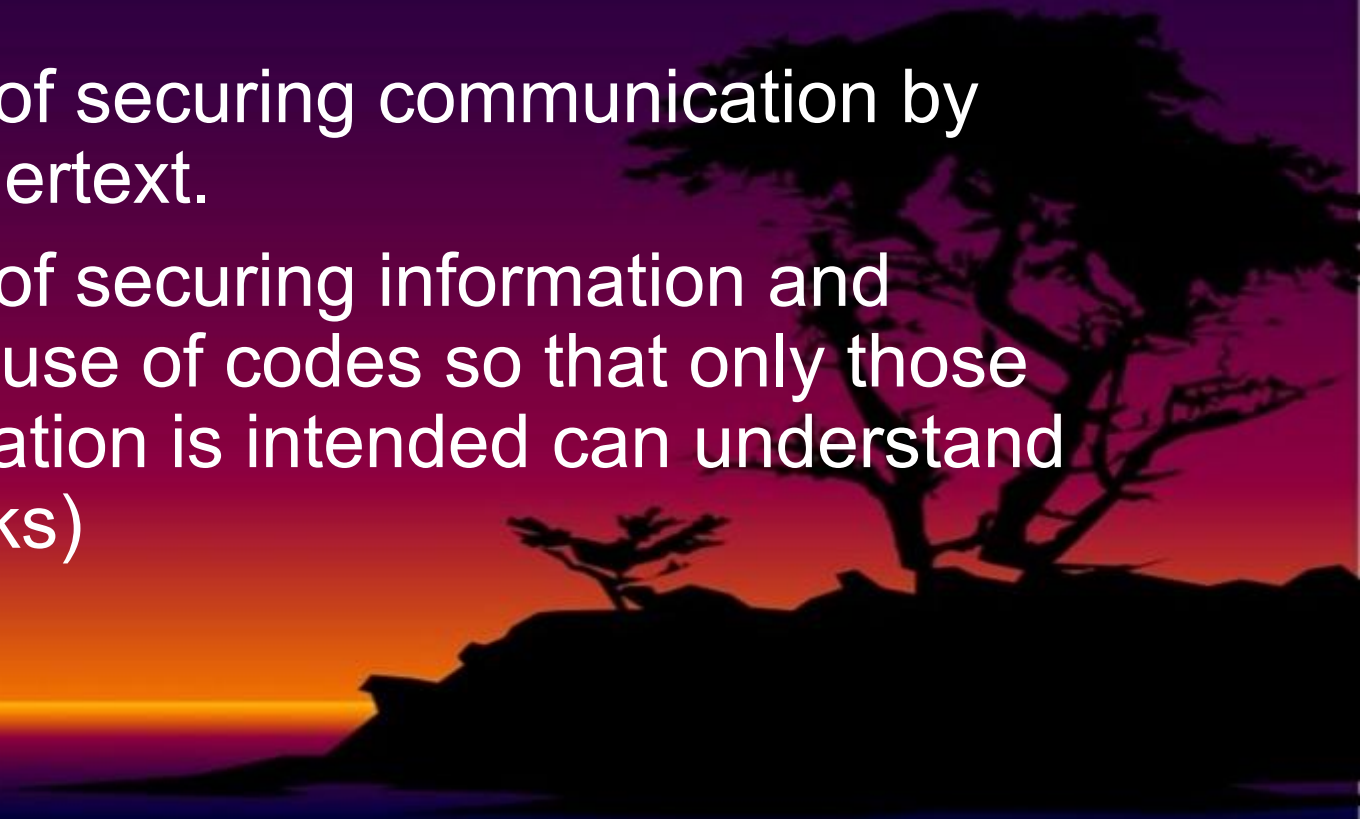
**By: Japhet Moise H.**

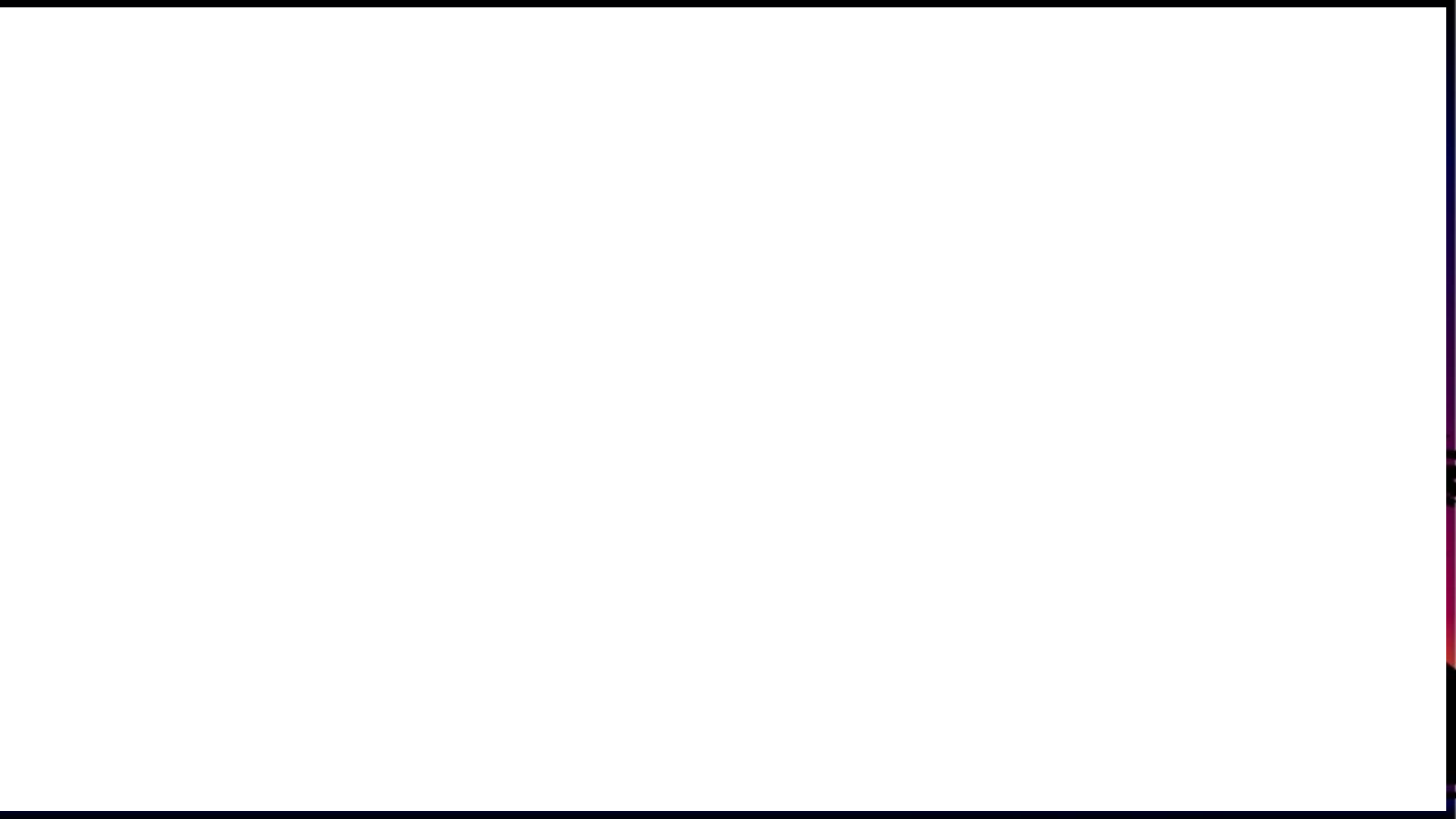
# Introduction to blockchain

- A blockchain is a distributed database or ledger shared among a computer network's nodes.
- They are best known for their crucial role in cryptocurrency systems for maintaining a secure and decentralized record of transactions, but they are not limited to cryptocurrency uses. Blockchains can be used to make data in any industry immutable—the term used to describe the inability to be altered.
- A blockchain is a distributed ledger with growing lists of records (blocks) that are securely linked together via cryptographic hashes.

# cryptography

- Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. (Forbinet)
- Cryptography is a technique of securing communication by converting plain text into ciphertext.
- Cryptography is a technique of securing information and communications through the use of codes so that only those persons for whom the information is intended can understand and process it.( geeksforgeeks)





# Types of Blockchain

- **1. Public Blockchains:**

- Anyone can participate in the network and create or validate blocks.
- Examples: Bitcoin, Ethereum, Litecoin

- **2. Private Blockchains:**

- Only authorized participants can join the network.
- Examples: Hyperledger Fabric, Corda

- **3. Hybrid Blockchains:**

- Combine elements of public and private blockchains, allowing for both public and private transactions.
- Examples: R3 Corda, IBM Blockchain Platform



## 4. Sidechains:

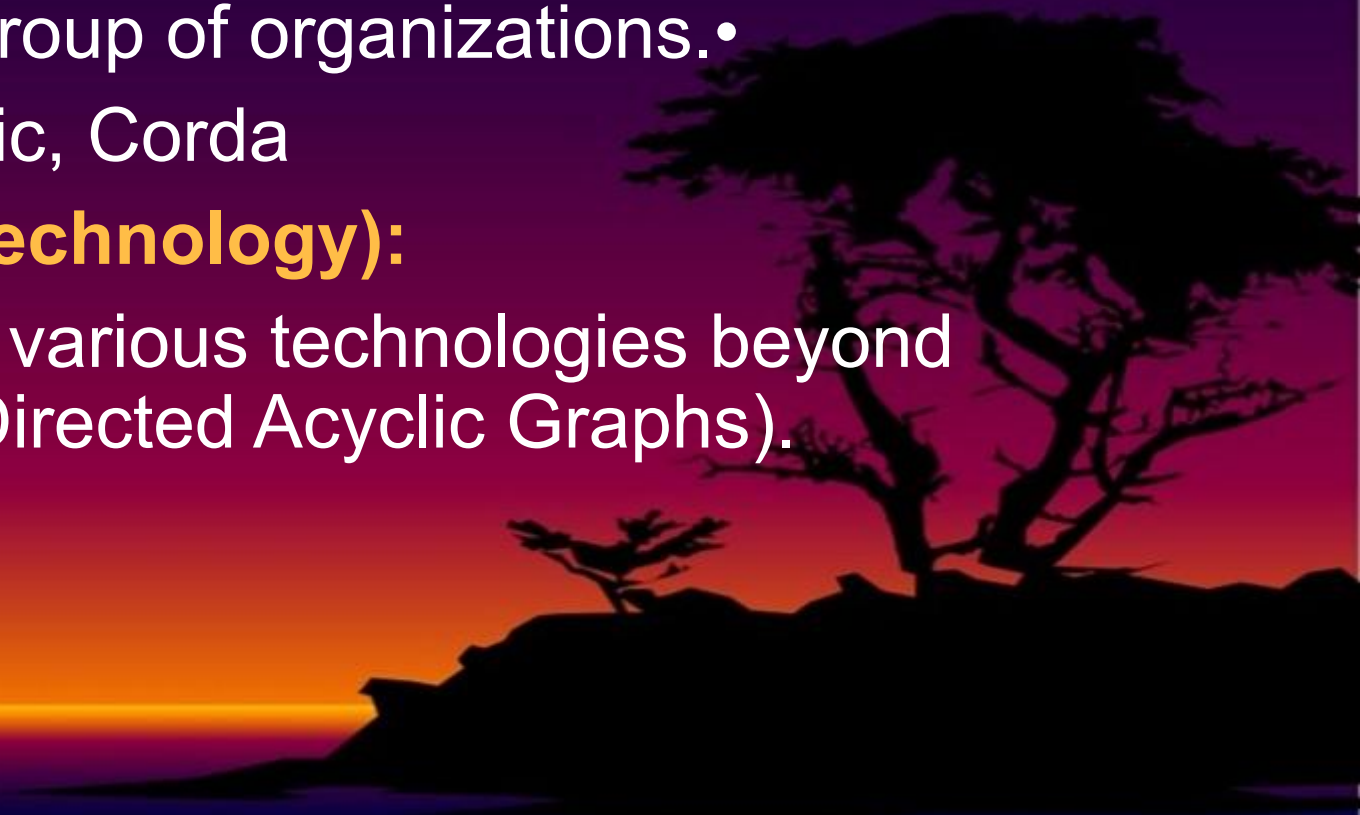
- **Separate:** Operate as separate blockchains but are connected to a mainchain.
- Examples: Liquid Network (Bitcoin), Polkadot parachains

## 5. Consortium Blockchains:

- Multi-party: Controlled by a group of organizations.
- Examples: Hyperledger Fabric, Corda

## 6. DLT (Distributed Ledger Technology):

- Broader term: Encompasses various technologies beyond blockchain, such as DAGs (Directed Acyclic Graphs).
- Examples: IOTA, Hashgraph





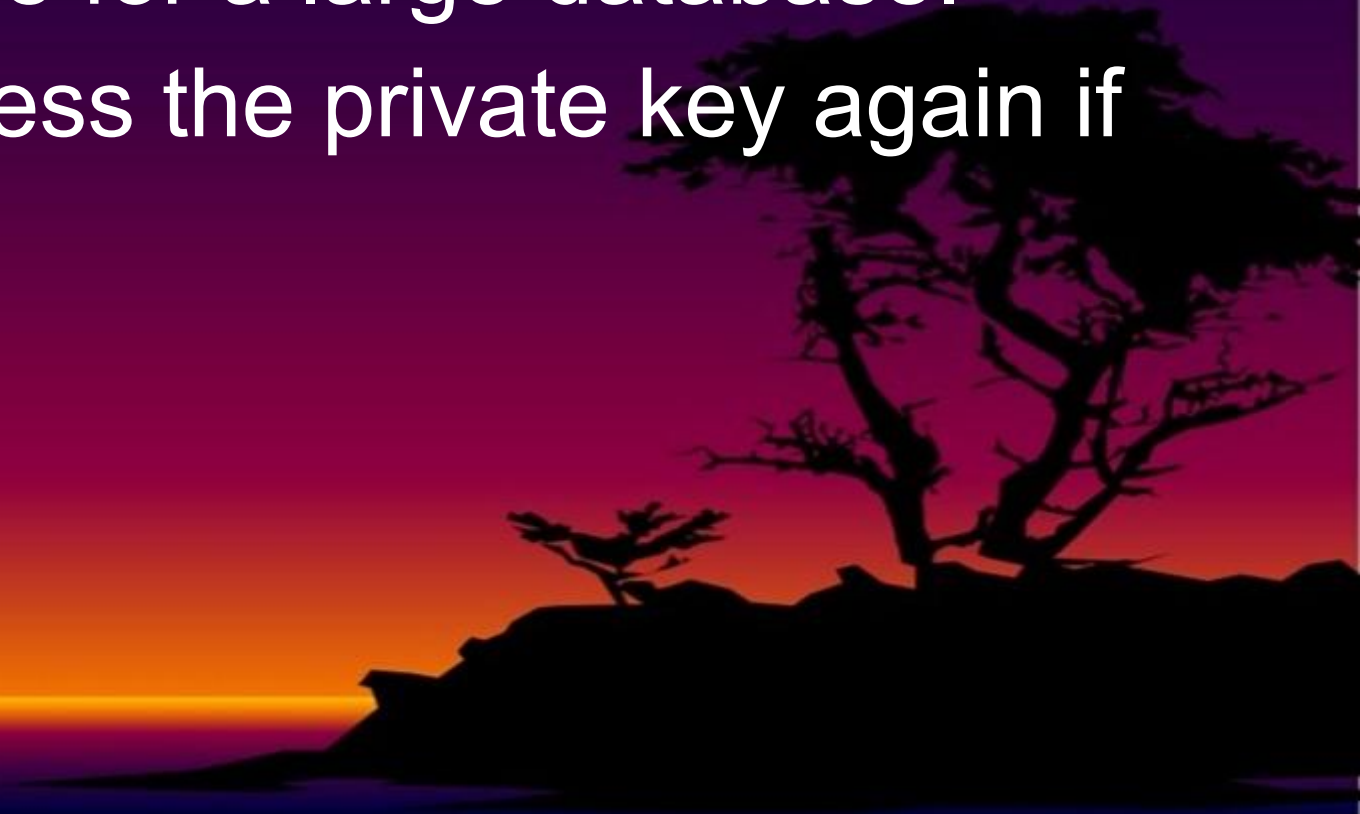
# Advantage using blockchain

1. It provides greater trust among users.
2. It provides greater security among data.
3. Reduce the cost of production.
4. Improve Speed.
5. Invocation and tokenization.
6. It provides immutable records.
7. Smart contracts




# Disadvantages using blockchain :

- Data modification is not possible.
- It requires large storage for a large database.
- The owner cannot access the private key again if they forget or lose it.





# Blockchain principles

- **Immutability:** Transactions are recorded and cannot be changed.
  - **Cryptographic hashing:** Data is secured using cryptographic algorithms.
  - **Distributed consensus:** Multiple participants verify and agree on transactions.
  - **Transparency:** The ledger is visible to all participants.
  - **Decentralization:** Eliminates the need for intermediaries like banks or governments.
- 
- A silhouette of a tree is visible on the right side of the slide, set against a background of a sunset or sunrise with a gradient from orange to purple.

# Blockchain Company Solutions

## 1. Supply Chain Management:

- **Transparency and Traceability:** Blockchain can provide end-to-end visibility into supply chains, ensuring product authenticity and reducing fraud.
- **Efficiency:** Smart contracts can automate processes, streamline logistics, and reduce costs.
- **Sustainability:** Blockchain can track the sustainability of products and materials throughout the supply chain.

## 2. Financial Services:

- **Cross-Border Payments:** Blockchain can facilitate faster and more cost-effective cross-border payments.
- **Remittances:** Blockchain can reduce the cost and time associated with sending remittances.
- **Tokenization:** Assets can be tokenized on the blockchain, enabling fractional ownership and improved liquidity.





### • **3. Healthcare:**

- Electronic Health Records (EHRs): Blockchain can provide a secure and tamper-proof way to store and share EHRs.
- Supply Chain Management: Blockchain can track the movement of pharmaceuticals and medical supplies to prevent counterfeiting and ensure quality.
- Clinical Trials: Blockchain can streamline the process of clinical trials by securely storing and sharing patient data.

### • **4. Identity and Access Management:**

- Decentralized Identity: Blockchain can enable individuals to control their own identity data and share it securely with organizations.
- Anti-Fraud: Blockchain can help prevent identity theft and fraud by providing a tamper-proof record of identity information.

## • **5. Real Estate:**

- **Property Records:** Blockchain can provide a secure and transparent way to record property ownership and transactions.
- **Fractional Ownership:** Blockchain can enable fractional ownership of real estate, making it more accessible to investors.

## **6. Gaming:**

- **Non-Fungible Tokens (NFTs):** Blockchain can be used to create and trade unique digital assets, such as in-game items or collectibles.
- **Decentralized Autonomous Organizations (DAOs):** Blockchain can enable communities of gamers to collectively own and manage virtual worlds.



## 7. Energy:

- Renewable Energy Trading: Blockchain can facilitate the trading of renewable energy credits and certificates.
- Smart Grids: Blockchain can enable secure and efficient communication between energy producers, consumers, and the grid.





# What is a Blockchain Wallet?

- A blockchain wallet is a cryptocurrency wallet that allows users to manage different kinds of cryptocurrencies—for example, Bitcoin or Ethereum.
- A blockchain wallet helps someone exchange funds easily.
- The wallet is accessible from web devices, including mobile ones, and the privacy and identity of the user are maintained





# components of wallet

## 1. Private Key:

- In the Private key, the same key (secret key) is used for encryption and decryption. In this key is symmetric because the only key is copied or shared by another party to decrypt the cipher text. It is faster than public-key cryptography.

## 2. Public Key:

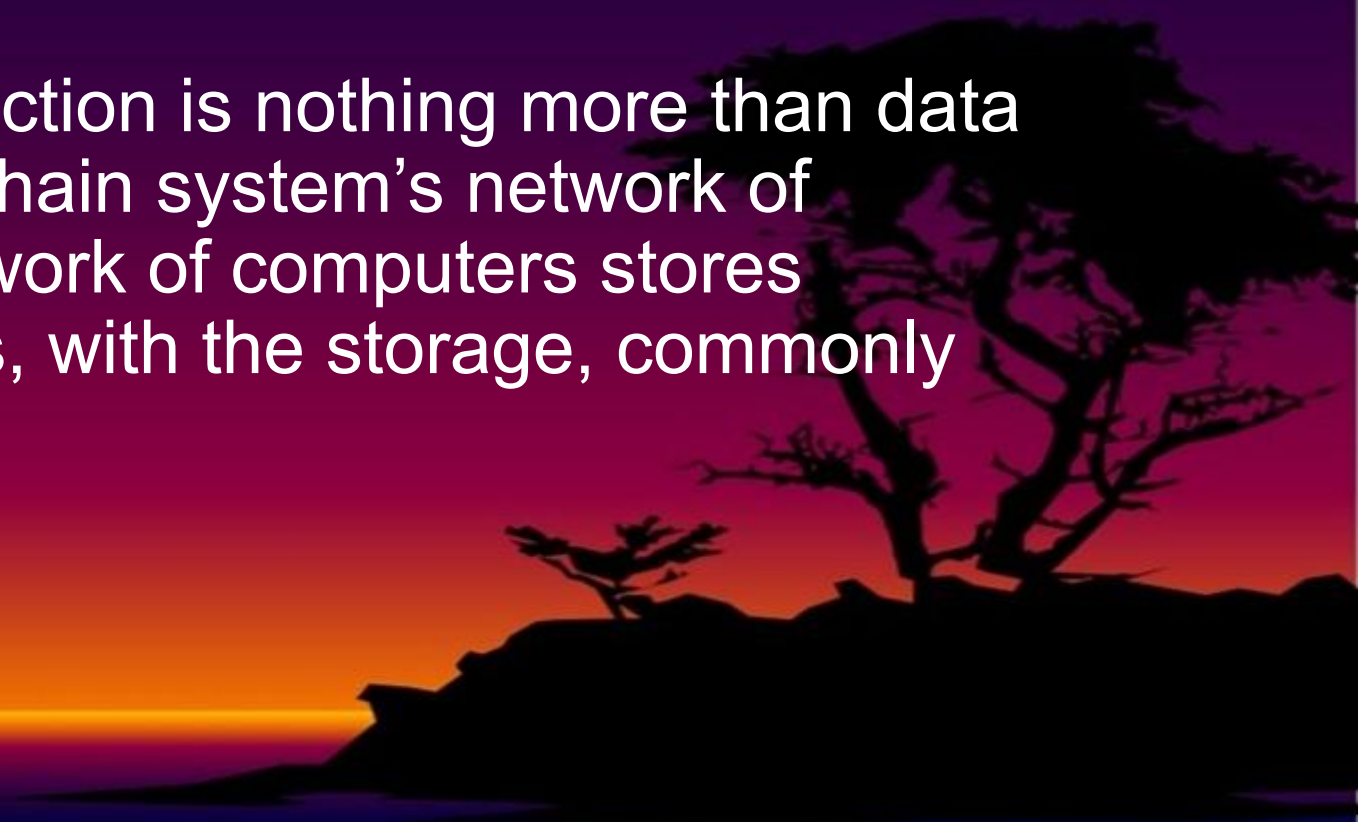
- Two keys are used one key is used for encryption and another key is used for decryption. One key (public key) is used to encrypt the plain text to convert it into cipher text and another key (private key) is used by the receiver to decrypt the cipher text to read the message.

## 3. Addresses:

- A wallet address in blockchain is a unique identifier that acts as your public key. It's like a postal address for your cryptocurrency holdings. When you send someone cryptocurrency, you send it to their wallet address.
- Wallet address is like your bank account number. People can use it to send you money, but they can't access your account without the private key (like your PIN).

# Transactions:

- A contract, agreement, transfer, or exchange of assets between two or more parties is referred to as a transaction. Typically, the asset is cash or property.
- Similarly, a blockchain transaction is nothing more than data transmission across a blockchain system's network of computers. A blockchain network of computers stores transactional data as replicas, with the storage, commonly referred to as a digital ledger.



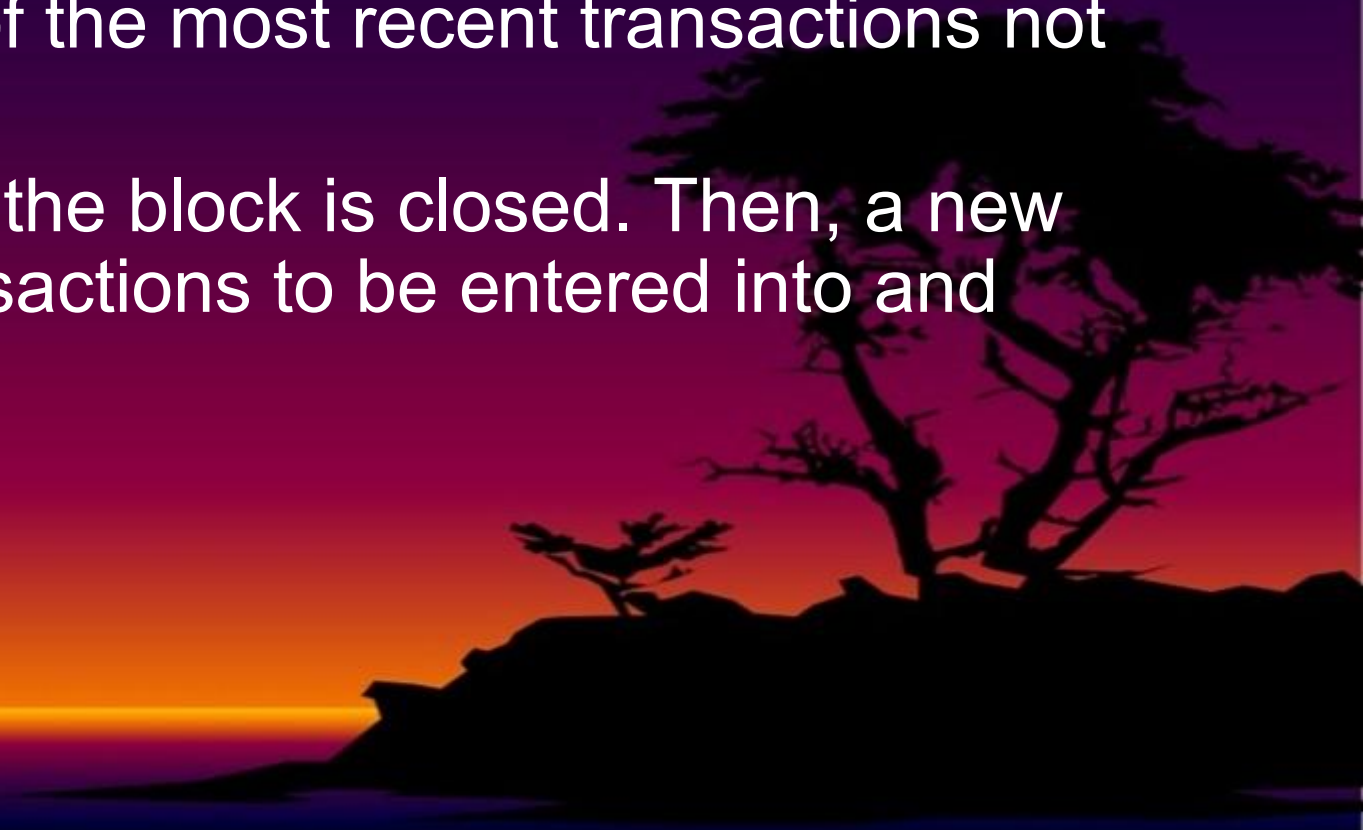
# Markle trees

- **Merkle trees** are a structured way of encoding data for easy verification and better security.
- Blockchains use Merkle trees to generate hashes that are used to verify transactions and secure the blocks.
- Visual representations of Merkle trees resemble upside-down trees with the root at the top.
- The repeated hashing technique used in blockchain Merkle trees is one of the mechanics that contribute to their immutability.



# Blocks

- **Blocks** are files stored by a blockchain, where transaction data are permanently recorded.
- A block records some or all of the most recent transactions not yet validated by the network.
- Once the data are validated, the block is closed. Then, a new block is created for new transactions to be entered into and validated.



Thank you!!!

