



# **SNS COLLEGE OF ENGINEERING**

Kurumbapalayam (Po), Coimbatore – 641 107 An Autonomous Institution Accredited by NBA – AICTE and Accredited by NAAC  
UGC wit‘A’ Grade Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

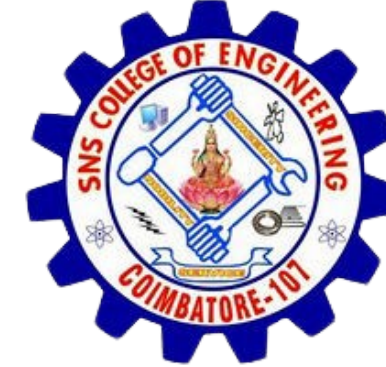
**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING IOT Including CS&BCT**  
**COURSE NAME : DISTRIBUTED LEDGER TECHNOLOGY**

**TOPIC: Transaction in Bitcoin Network**



## Introduction to Bitcoin Transactions

Bitcoin transactions are the backbone of the Bitcoin network. Each transaction involves the transfer of ownership of a certain amount of bitcoins from one party to another. These transactions are recorded in the blockchain, a decentralized ledger that ensures the transparency and immutability of the Bitcoin network. The process is designed to be secure, fast, and transparent, enabling peer-to-peer transactions without the need for intermediaries like banks.



## Components of a Bitcoin Transaction

A Bitcoin transaction consists of several key components:

### **Input:**

The input refers to the source of the bitcoins being spent. It typically references a previous transaction's output, indicating where the bitcoins are coming from.

### **Output:**

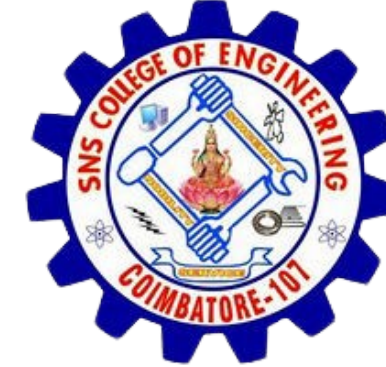
The output specifies the recipient's Bitcoin address and the amount of bitcoins being transferred. A transaction can have multiple outputs.

### **Signature:**

The signature is created using the sender's private key. It verifies that the sender has authorized the transaction and that the transaction hasn't been altered.

### **Transaction Fee:**

A transaction fee is optional but encouraged. It incentivizes miners to include the transaction in the next block and ensures faster processing. The fee is typically calculated based on the transaction size (in bytes).



## How Bitcoin Transactions Work

### **Creating a Transaction:**

The sender creates a transaction by specifying the input (previous transaction's output), the output (recipient's address), and the amount to send. The transaction is then signed with the sender's private key.

### **Broadcasting the Transaction:**

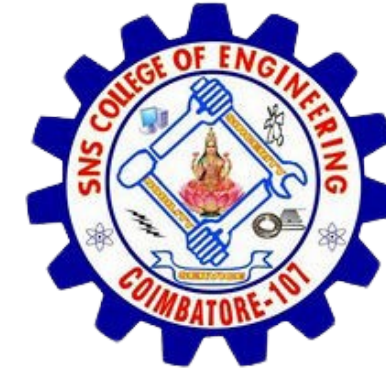
Once signed, the transaction is broadcast to the Bitcoin network. It is propagated through the network to various nodes (computers) that validate it.

### **Transaction Validation:**

Nodes verify that the transaction is valid by checking the sender's signature, ensuring there are no double-spends, and confirming that the inputs are unspent.

### **Mining the Transaction:**

Valid transactions are grouped into blocks by miners. Once a miner successfully solves the cryptographic puzzle (Proof of Work), the block is added to the blockchain, and the transaction is considered confirmed.



## Transaction Confirmation and Security

### Transaction Confirmation:

- A Bitcoin transaction is considered confirmed once it has been added to a block and that block is appended to the blockchain. Subsequent blocks are mined on top of this block, increasing the number of confirmations.
- Generally, 6 confirmations are considered secure for a transaction to be irreversible.

### Security Features:

- Public-Private Key Cryptography: Transactions are secured using a combination of the sender's private key and the recipient's public key. This ensures that only the owner of the private key can authorize the transaction.
- Decentralization: Bitcoin's decentralized nature ensures that no central authority can alter or reverse transactions. Once a transaction is recorded on the blockchain, it becomes part of the permanent, immutable ledger.
- Transaction Privacy: While Bitcoin is transparent, meaning all transactions are visible on the blockchain, the identities of the participants remain pseudonymous.

### Transaction Fees:

- Miners prioritize transactions with higher fees, so the fee paid can affect the speed at which a transaction is included in a block. The more congested the network, the higher the transaction fee required for timely inclusion.