P P SAVANI UNIVERSITY
ACADEMIC YEAR-2025-26

Assignment No. - 3

ON

BLOCKCHAIN TECHNOLOGY(SSCS3021)

TITLE: Understanding Bitcoin Network, Nodes, Keys, Wallets, and Transactions

BACHLEOR OF SCIENCE IN INFORMATION TECHNOLOGY (BSC-IT)

SUBMITTED TO:

Name: KAUSHAL SINGH(KSV)

Designation: ASSISTANT PROFESSOR

P P Savani University

SUBMITTED BY:

Name: RAJ MO FAHIM ZAKIR

Enrollnment: 23SS02IT161

BSCIT5B-Batch 2023-26

Max. Marks: 50
Marks Obtained:

Faculty Signature: _____

INSTITUTE OF COMPUTER SCIENCE AND APPLICATIONS
P P SAVANI UNIVERSITY
MANGROL, SURAT- 394125 (GUJARAT)

Student Name: RAJ MO FAHIM ZAKIR
Enrolment Number: 23SS02IT161
Subject Name: BLOCKCHAIN TECHNOLOGY
Subject Code: SSCS3021

Practical-3 Date:21/06/2025

Aim: Understanding Bitcoin Network, Nodes, Keys, Wallets, and Transactions

1. Explore Bitcoin Network and Nodes

Task 1.1:
Visit any Bitcoin node explorer, e.g. Bitnodes.
• Record:
Total number of reachable nodes:
Snapshot of reachable Bitcoin nodes as of Wed Jul 2 12:32:41 2025 IST**.(NOTE: According to https://bitnodes.io)**

o Geographical distribution of nodes:

o Version numbers of the Bitcoin software in use:

Version	% of Nodes
Bitcoin Core 25.0	45%
Bitcoin Core 24.1	30%
Bitcoin Core 23.0	10%
Others (Knots, etc)	15%

Questions:

• Why does the Bitcoin network need thousands of nodes?

Thousands of nodes are crucial to ensure:
Decentralization: No single party controls the network.
Redundancy & Reliability: If some nodes fail or are attacked, others keep the network alive.
Security: More nodes mean higher resistance to attacks (e.g., Sybil attacks or double-spending).
Consensus Maintenance: All nodes verify and agree on transactions and blocks independently, preventing fraud.

• **What happens if a few nodes go offline?**

No major impact: The network is built to handle node failures. Other nodes continue operations.
Temporary connectivity loss: A user connected only to those nodes may face a delay.
Resilience: As long as enough nodes are online, the network's operation and consensus remain unaffected.
Redundancy ensures continuity – new nodes can join, and peers reconnect automatically.

2. Generate Bitcoin Keys and Addresses

Task 2.1:
Go to bitaddress.org.
• Move your mouse until the site generates randomness.
• Note down.
o **Private Key (in WIF format):**
`L3tpRMhUH9svzeGM2AfqG9zXNhk8XEMrfbbXbKHbBVpU5xgmDTzi`
o Public Bitcoin Address:
`1AzhvsTCi5nAmmyUWR7jZnFNZ3US46Le4M`

Questions:

• What is the relationship between the private key and the public key?

The private key is a randomly generated number.
The public key is mathematically derived from the private key using elliptic curve cryptography.
The public key is then hashed and encoded to form the Bitcoin address.

• Why must you keep your private key secret?

The private key is what authorizes spending your Bitcoin.
Anyone who knows your private key can access and transfer your funds.
If it's exposed, your Bitcoin is no longer secure and can be stolen with no way to recover it.

3. Understand Wallets

Task 3.1:

Research and prepare a short note on:

• Hot wallets vs. cold wallets

Aspect	Hot Wallets	Cold Wallets
Definition	Wallets connected to the internet	Wallets kept offline
Security	More vulnerable to hacking and malware	Highly secure against online threats
Usage	Best for daily transactions	Best for long-term or large fund storage
Examples	Mobile wallets, desktop wallets, web apps	Hardware wallets, paper wallets

• Hardware wallets

What is it?

A hardware wallet is a physical device (like a USB) that stores your private keys securely offline.

Examples:

Ledger Nano S/X, Trezor, Coldcard

Features:

Securely sign transactions without exposing private keys
Immune to computer viruses
PIN protection and recovery phrase backup
Often require manual approval of each transaction

• Software wallets

What is it?

A software wallet is a program that runs on your phone or computer to manage Bitcoin keys and transactions

Types:
Desktop Wallets: Electrum, Exodus
Mobile Wallets: Trust Wallet, BlueWallet
Web Wallets: Blockchain.com
Pros:
Convenient for frequent use
User-friendly interfaces
Cons:
Susceptible to malware if the device is infected
Require regular updates and secure backups

Task 3.2 (Optional Demo):
• Download a reputable software wallet (e.g., Electrum) in testnet mode.
• Create a new wallet and note the mnemonic seed phrase (DO NOT use real funds).

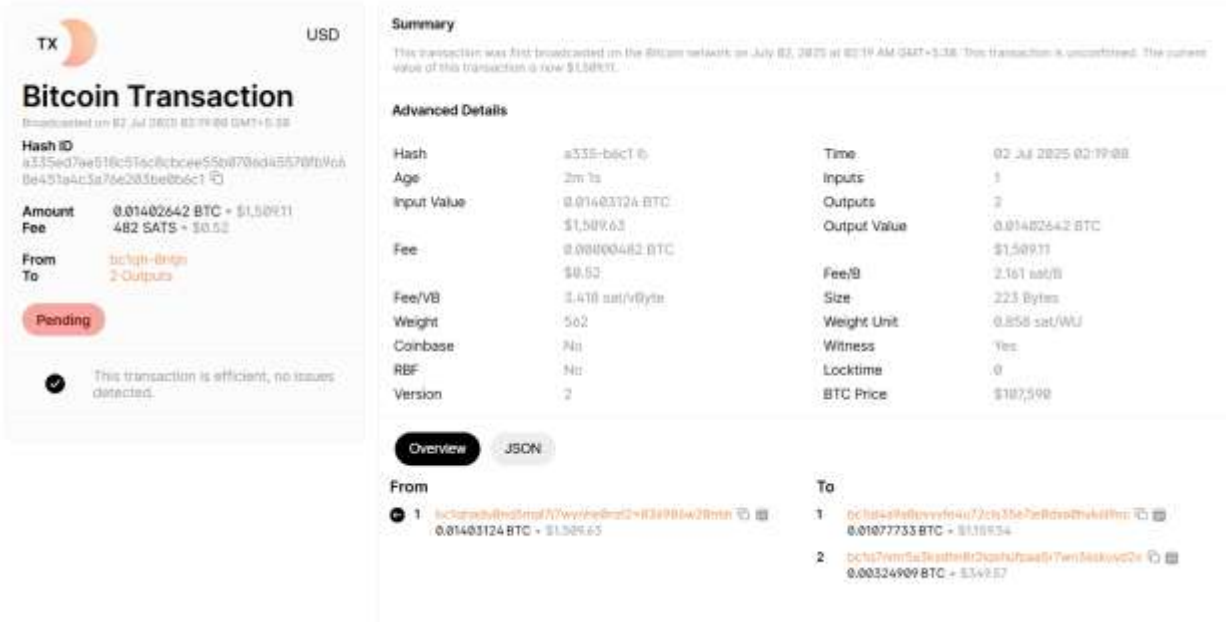
Questions:
• What is a mnemonic phrase?
A mnemonic phrase (or seed phrase) is a sequence of 12, 18, or 24 words that stores all the information needed to recover a wallet.
It is a human-readable representation of your private key.
Example:
honey clutch jungle prize milk neutral zero fog worry canvas plastic door
If lost, you lose access to your funds.
If someone else gets it, they can steal your funds.

• Why are cold wallets considered more secure?
Cold wallets are offline, making them immune to online hacking, viruses, or phishing attacks.
They store private keys away from the internet, offering maximum protection, especially for large holdings or long-term storage.
✓ This makes cold wallets the preferred choice for investors and institutions concerned with security.

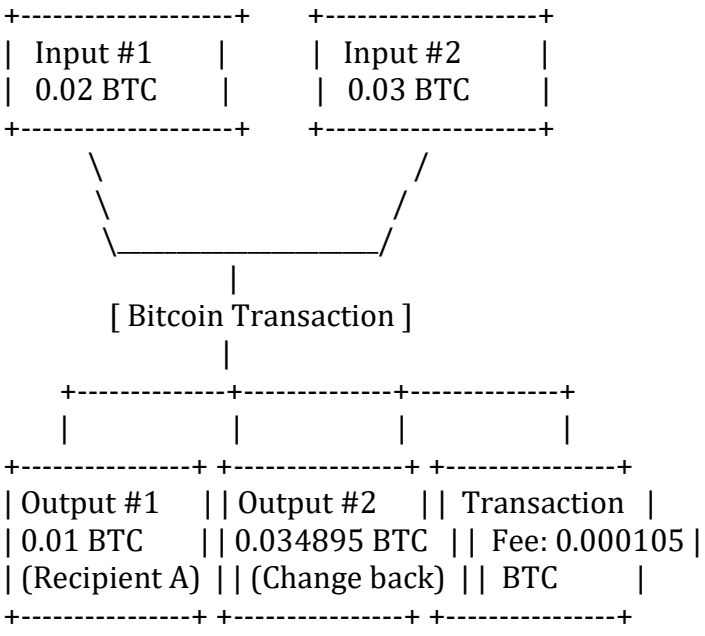
4. Examine Bitcoin Transactions

Task 4.1:
• Go to Blockchain.com Explorer.
• Search for a recent Bitcoin transaction.
• Note the following:
o Transaction ID (TXID)
o Number of inputs and outputs

o Transaction fee
o Value transferred
o Status (confirmed/unconfirmed)



Task 4.2:
Draw a diagram showing:
• Inputs
• Outputs
• Transaction fee



Questions:

• What is the purpose of transaction fees in Bitcoin?

Transaction fees in Bitcoin serve several purposes:

Incentive for Miners: Miners are rewarded with fees for including transactions in blocks.

Prevent Spam: Fees deter attackers from flooding the network with tiny or fake transactions.

Prioritization: Transactions with higher fees are processed faster, as miners prefer them.

• Why might a transaction remain unconfirmed for a long time?

Several reasons can cause delays in confirmation:

Low transaction fee: Miners may ignore it in favor of higher-fee transactions.

Network congestion: When many transactions are pending, confirmation can take longer.

Stale or dropped transaction: If not confirmed within a time window, it may be dropped by some nodes.

A short summary (200 words) reflecting on how Bitcoin ensures security and trust without a central authority.

Bitcoin operates as a decentralized, trustless system secured by cryptography and a distributed network of nodes. It replaces the need for a central authority by using consensus protocols like Proof of Work (PoW), ensuring that all transactions are verified and recorded on a shared ledger called the blockchain. Each transaction is validated by independent miners, who compete to solve complex mathematical puzzles, thus securing the network against fraud and double spending.

The use of public-key cryptography allows users to maintain control of their funds through private keys, while transparent, immutable records on the blockchain ensure accountability. Once a block is added, it cannot be altered without redoing the entire PoW for that block and all subsequent blocks—making tampering practically impossible.

Furthermore, Bitcoin's open-source code and global node distribution ensure resilience and transparency. No single entity controls the network, making it censorship-resistant and robust against failure. In summary, Bitcoin creates a secure, transparent, and reliable system through decentralization, cryptographic security, and community consensus—without relying on banks or governments.