

MAJOR PROJECT 1 PRESENTATION 1 IS SCHEDULED ON 12/09/25 FOR ALL APPROVED PROJECT GROUPS.

FOR THE PRESENTATION 1 THE EMPHASIS IS ON ANALYSIS PHASE. EACH GROUP WILL GET 12 MINS FOR PRESENTATION AND 05 MINUTES FOR Q & A SESSION

EXPLAINING THE FOLLOWING -

- 1. PROBLEM STATEMENT**
- 2. OBJECTIVES AND SCOPE**
- 3. FEASIBILITY STUDY**
- 4. SOFTWARE AND HARDWARE REQUIREMENT**
- 5. LITERATURE SURVEY (DETAILED STUDY)**
- 6. SUMMARIZATION OF ANALYSIS PHASE**

EVERY PROJECT GROUP SHOULD FOLLOW THE ABOVE MINIMUM REQUIREMENT. SHOULD COMPLETE THE PRESENTATION SESSION WITH INTERNAL GUIDE PRIOR TO FINAL PRESENTATION ON 12/09/25. FOLLOW THE SUGGESTIONS OF INTERNAL GUIDE FOR ANY ADDITION TO ABOVE.

**PROF D V CHANDRAN
DEPT PROJECT COORDINATOR**

Add class comment





Smt. Indira Gandhi College of Engineering, Navi Mumbai

(An Autonomous Institute Accredited by NAAC with Grade "A")



Computer Science & Engineering Department

2. Energy Consumption

- **Explanation:** Blockchains using Proof of Work (PoW) require massive computational power to validate transactions.
- **Impact:** High electricity usage, environmental concerns, and increased operational costs.
- **Example:** Bitcoin mining consumes electricity comparable to small countries.

3. Security and Privacy Concerns

- **Explanation:** While blockchain is secure against data tampering, it still faces threats like:
 - **51% attack** (if majority controls mining/validation power).
 - **Smart contract bugs** leading to hacks.
 - **Privacy issues** since transactions are transparent.
- **Impact:** Financial losses, reduced trust.
- **Example:** The 2016 Ethereum DAO hack due to smart contract vulnerability.

4. Regulatory and Legal Uncertainty

- **Explanation:** Many governments lack clear laws on blockchain and cryptocurrencies.
- **Impact:** Businesses face risks due to unclear taxation, compliance, and cross-border transaction rules.
- **Example:** Different countries have banned, restricted, or taxed cryptocurrencies differently.

5. Integration with Legacy Systems

- **Explanation:** Traditional businesses (banks, supply chain, healthcare) still rely on centralized databases and legacy IT systems. Integrating blockchain into these systems is complex and costly.
- **Impact:** High implementation costs, slow adoption, and technical challenges in interoperability.
- **Example:** Supply chain companies struggle to connect blockchain platforms with their old ERP systems.



Q1. A) What is a Merkle tree? Explain the structure of a Merkle tree

What is a Merkle Tree?

A **Merkle Tree** (also called **Hash Tree**) is a **binary tree structure** used in computer science and cryptography to verify **data integrity** efficiently.

It is widely used in:

- **Blockchain (Bitcoin, Ethereum, etc.)**
- **Peer-to-Peer networks (BitTorrent, IPFS)**
- **File verification systems**

The main idea: Instead of storing or verifying entire data, a **hash (digital fingerprint)** of the data is stored at each node, making verification faster and secure.

Structure of a Merkle Tree

1. Leaf Nodes (Bottom Level):

- Each leaf node contains the **hash of a data block** (e.g., a transaction in blockchain).
- Example: Hash(Transaction 1), Hash(Transaction 2) ...

2. Intermediate Nodes (Middle Levels):

- Each non-leaf node contains the **hash of the concatenation** of its child nodes.
- Example:
- Parent = Hash(LeftChildHash + RightChildHash)

3. Root Node (Top Level):

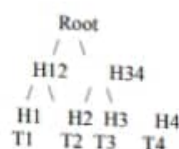
- The **Merkle Root** is the single hash at the top of the tree.
- It represents the **entire dataset**.
- If even a single transaction changes → Merkle Root changes.

✓ Example of a Merkle Tree

Suppose we have 4 transactions: T1, T2, T3, T4

1. Compute hashes of each transaction:
2. $H1 = \text{Hash}(T1)$
3. $H2 = \text{Hash}(T2)$
4. $H3 = \text{Hash}(T3)$
5. $H4 = \text{Hash}(T4)$
6. Combine pairs and hash them:
7. $H12 = \text{Hash}(H1 + H2)$
8. $H34 = \text{Hash}(H3 + H4)$
9. Compute Merkle Root:
10. $\text{Root} = \text{Hash}(H12 + H34)$

So, the structure looks like:



Why Merkle Trees are Useful?

- **Efficient Verification:** You don't need the entire dataset, just the hashes along the path to the root.
- **Integrity Check:** If one transaction is modified, its hash changes → propagates up to the root.
- **Scalability:** Used in blockchains to handle thousands of transactions securely.

b) List and explain the components of blockchain technology with examples

Main Components of Blockchain Technology

A blockchain system has several key components that work together to provide **security, transparency, decentralization, and immutability**.





Computer Science & Engineering Department

- **Access Control:** No restrictions; permissionless.
- **Consensus Mechanism:** Typically Proof of Work (PoW) or Proof of Stake (PoS).
- **Transparency:** Fully transparent, all transactions are visible to anyone.
- **Examples:** Bitcoin, Ethereum.
- **Use Cases:** Cryptocurrencies, decentralized finance (DeFi), public record systems.
- **Advantages:**
 - High transparency and trust.
 - Censorship-resistant.
 - Decentralized control.
- **Disadvantages:**
 - Slower transaction speed.
 - High energy consumption (in PoW).
 - Scalability issues.

2. Private Blockchain

- **Definition:** A blockchain where only a single organization has control. Participation is restricted and permissioned.
- **Access Control:** Controlled by one authority; only authorized participants can join.
- **Consensus Mechanism:** Can use simpler, faster methods (e.g., Practical Byzantine Fault Tolerance, Raft).
- **Transparency:** Limited; only participants approved by the central authority can see data.
- **Examples:** Hyperledger Fabric (when deployed by one organization), Corda.
- **Use Cases:** Supply chain management, internal auditing, enterprise data management.
- **Advantages:**
 - Faster transactions.
 - More privacy and confidentiality.
 - Efficient and scalable.
- **Disadvantages:**
 - Centralized control → less trustless.
 - Vulnerable to corruption by the controlling authority.

3. Consortium (Federated) Blockchain

- **Definition:** A blockchain governed by a group of organizations rather than a single entity. It is partially decentralized.