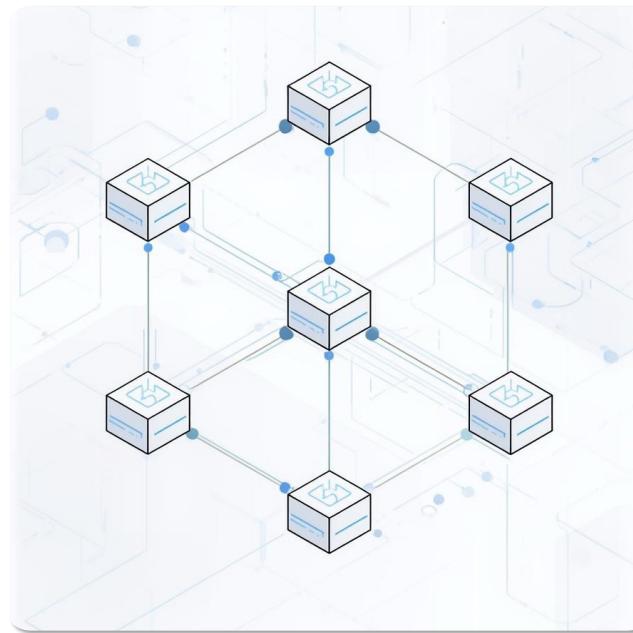


# Blockchain Transaction Validation Using Trees!

By Team Innovibe:

Harshitha [22EG107B45],  
Yashhwanth [25EG506D02],  
Surya [25EG507J05],  
Sanvi [25EG507J03],  
Sathwik [23EG107C48].



BLOCKCHAIN

# Executive Summary

## Understanding Blockchain Validation Using Trees

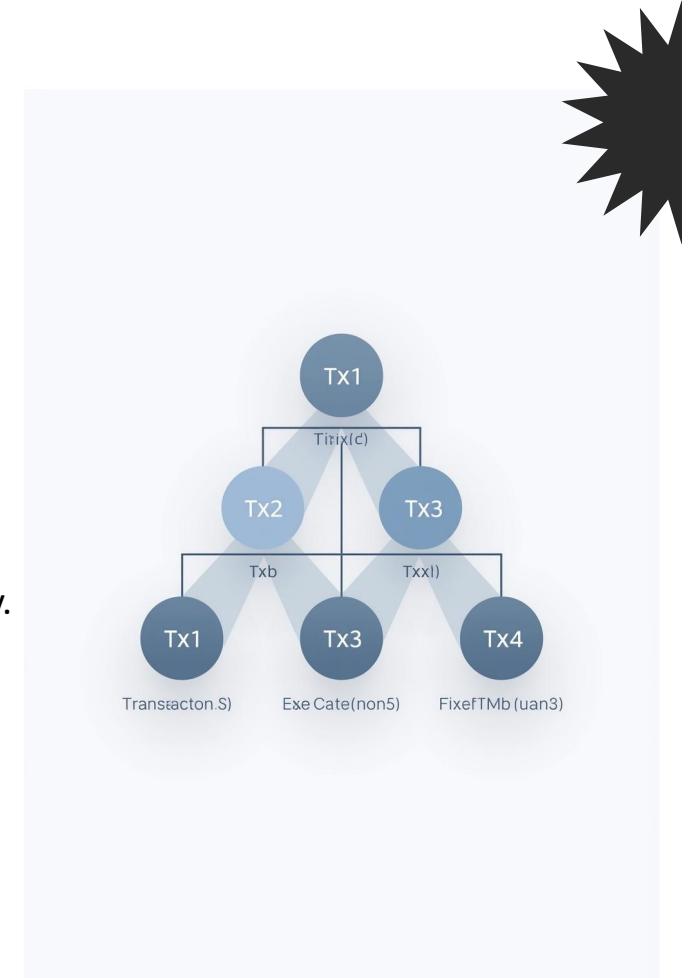
Blockchain transaction validation ensures security and trust. This presentation explains how Merkle Trees use unique hash structures to validate transactions efficiently. By combining many transactions into one root hash, any tampering can be quickly detected, ensuring data integrity.

### What is Blockchain?

- A **distributed digital ledger** that stores transactions securely and transparently.
- Each block is linked to the previous one, forming a **chain of records**.
- Commonly used in **cryptocurrencies, supply chains, and smart contracts**.

### Why Transaction Validation?

- Ensures every transaction is **authentic and tamper-proof**.
- Prevents **double spending** and fraud.
- Builds **trust** in a decentralized network.



# Data Structures in Blockchain

## What are Trees in Computer Science?

A hierarchical structure with a root and branches (nodes).

Used to organize and access data efficiently.

## Merkle Tree Concept:

A binary hash tree used in blockchain.

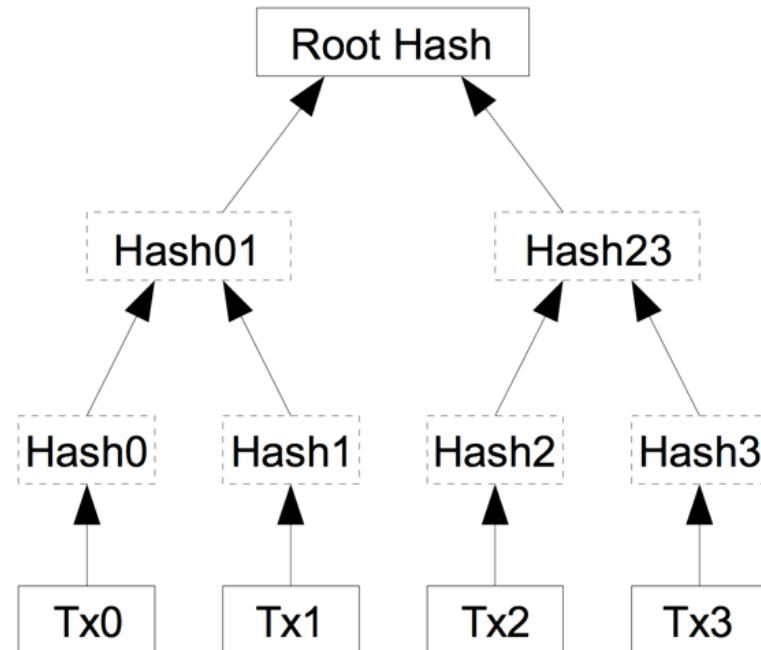
Each leaf node contains the hash of a transaction.

Parent nodes contain the hash of their children, and the topmost node is the Merkle Root.

## Why Trees in Blockchain?

To quickly verify large sets of data.

To detect any tampering in transactions efficiently.

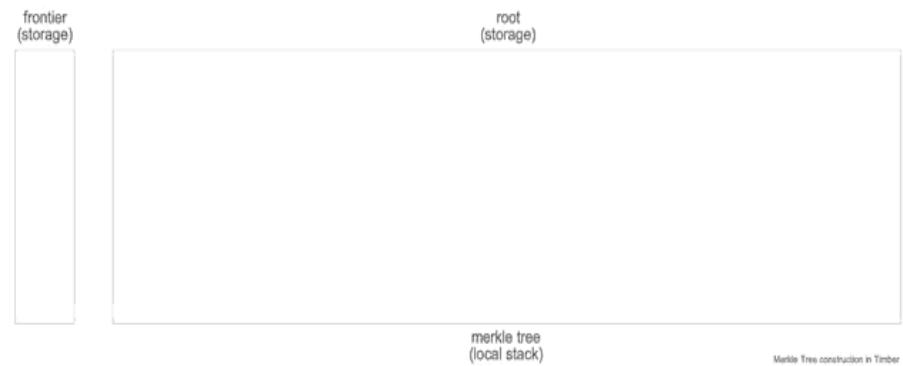


sanvi

## How Transactions Are Validated Using Trees

### Step-by-Step Validation Process:

1. Each transaction is hashed (converted into a unique digital signature).
2. Hashes are paired and re-hashed to form parent nodes.
3. The process continues until a single Merkle Root hash remains.
4. The root hash represents all transactions in that block.
5. When verifying a transaction, only a few hashes (proof path) are needed - not the entire dataset.

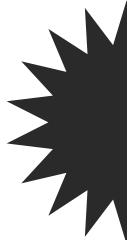


### Example:

If one transaction changes, its hash changes, altering all parent hashes up to the root — revealing tampering.



sathwik



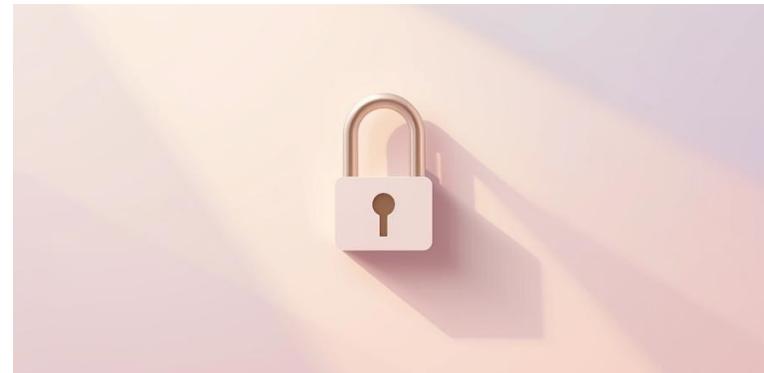
## Security and Efficiency

### Security Benefits:

Integrity: Any modification in transaction data changes the Merkle root.

Tamper Detection: Easy to detect malicious changes.

Transparency: Everyone can independently verify transactions.



### Efficiency Benefits:

Faster Verification: Only a small subset of hashes is needed.

Reduced Storage: No need to store full data for validation.

Scalability: Works efficiently even as blockchain grows.

## Real-World Use & Future Outlook

### Where It's Used:

Bitcoin: Uses Merkle Trees for transaction verification.

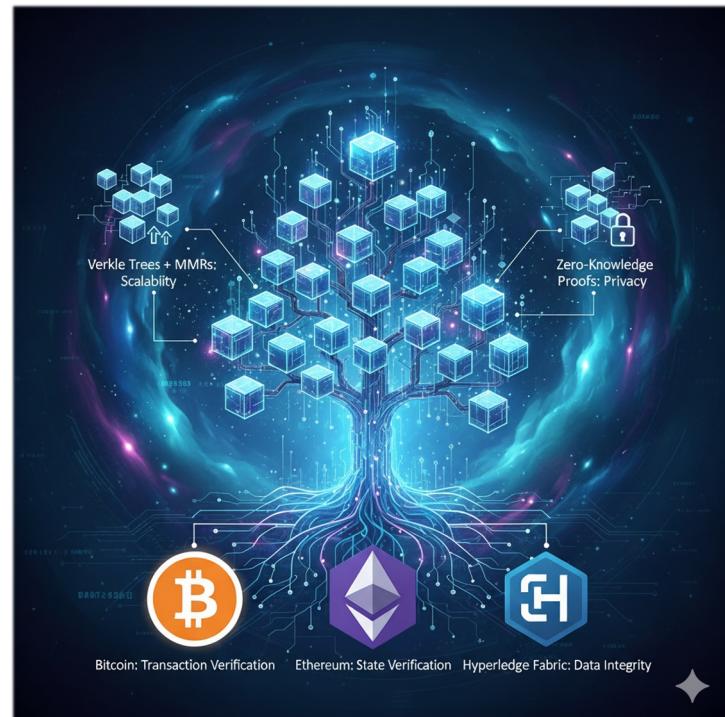
Ethereum: Uses modified Merkle Patricia Trees for state verification.

Hyperledger Fabric: Uses Merkle-based structures for secure data integrity.

### Future Outlook:

Introduction of Verkle Trees and Merkle Mountain Ranges (MMRs) for scalability.

Enhanced privacy with Zero-Knowledge Proofs integrated with trees.



# Sources and Resources!

**Frontiers in Blockchain Journal** — “Blockchain Transaction Validation using Merkle Trees”

🔗 <https://www.frontiersin.org/articles/10.3389/fbloc.2020.00003/full>

**ResearchGate Articles** — “Comparison of Transactions in Traditional vs Merkle Tree Validation”

🔗 [https://www.researchgate.net/figure/a-The-comparison-of-transactions-in-the-traditional-Merkle-tree-TMT-and-Merkle-Trim fig5 363888842](https://www.researchgate.net/figure/a-The-comparison-of-transactions-in-the-traditional-Merkle-tree-TMT-and-Merkle-Trim_fig5_363888842)

“Flow Diagram of Blockchain Validation Process”

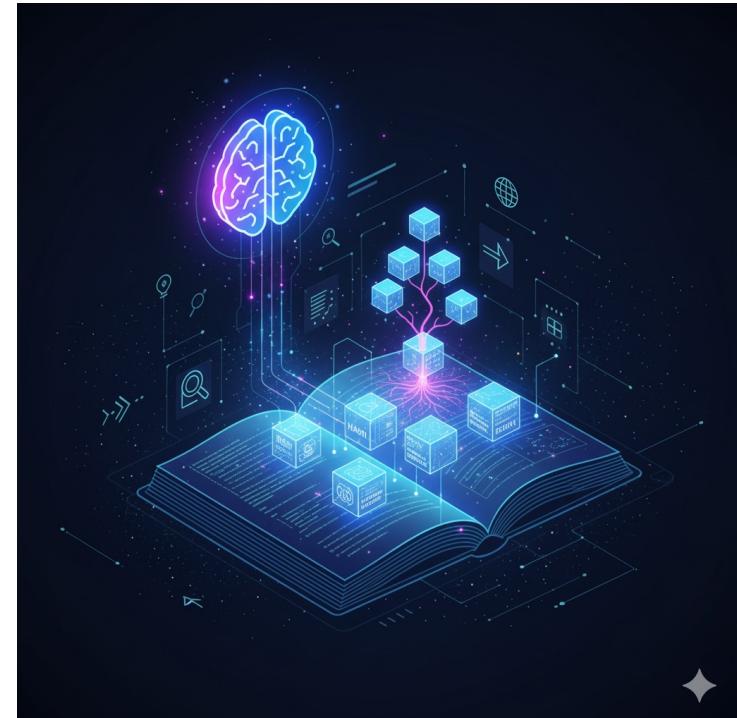
🔗 [https://www.researchgate.net/figure/Flow-Diagram-of-Blockchain-validation-process-towards-education-system fig4 365348751](https://www.researchgate.net/figure/Flow-Diagram-of-Blockchain-validation-process-towards-education-system_fig4_365348751)

**GeeksforGeeks** — “Validation Based Protocols in Blockchain”

🔗 <https://www.geeksforgeeks.org>

**Github** — “Validation Based implementation and inspirations”

🔗 <https://www.github.com>





## Conclusion

Trees like Merkle Trees make blockchain secure, fast, and verifiable.

Validation using trees ensures data integrity and transparency.

As blockchain evolves, new tree structures will make validation even more efficient and scalable.

anyone

