

**Dr.SNS RAJALAKSHMI COLLEGE OF ARTS AND SCIENCE  
(Autonomous)**

**Accredited by NAAC - UGC with 'A+ Grade (Cycle IV)  
( Recognized by UGC, Approved by AICTE & Affiliated to Bharathiar University)  
Coimbatore- 49**

**DEPARTMENT OF COMMERCE WITH INFORMATION  
TECHNOLOGY**

**21UCI505 – BLOCKCHAIN AND DISTRIBUTIVE  
LEDGER**

**Unit-2: From Hash Chain to Blockchain**

**Ms. S.Meenakshi, Assistant Professor  
Department of Commerce with Information Technology**

# What is a Hash Chain

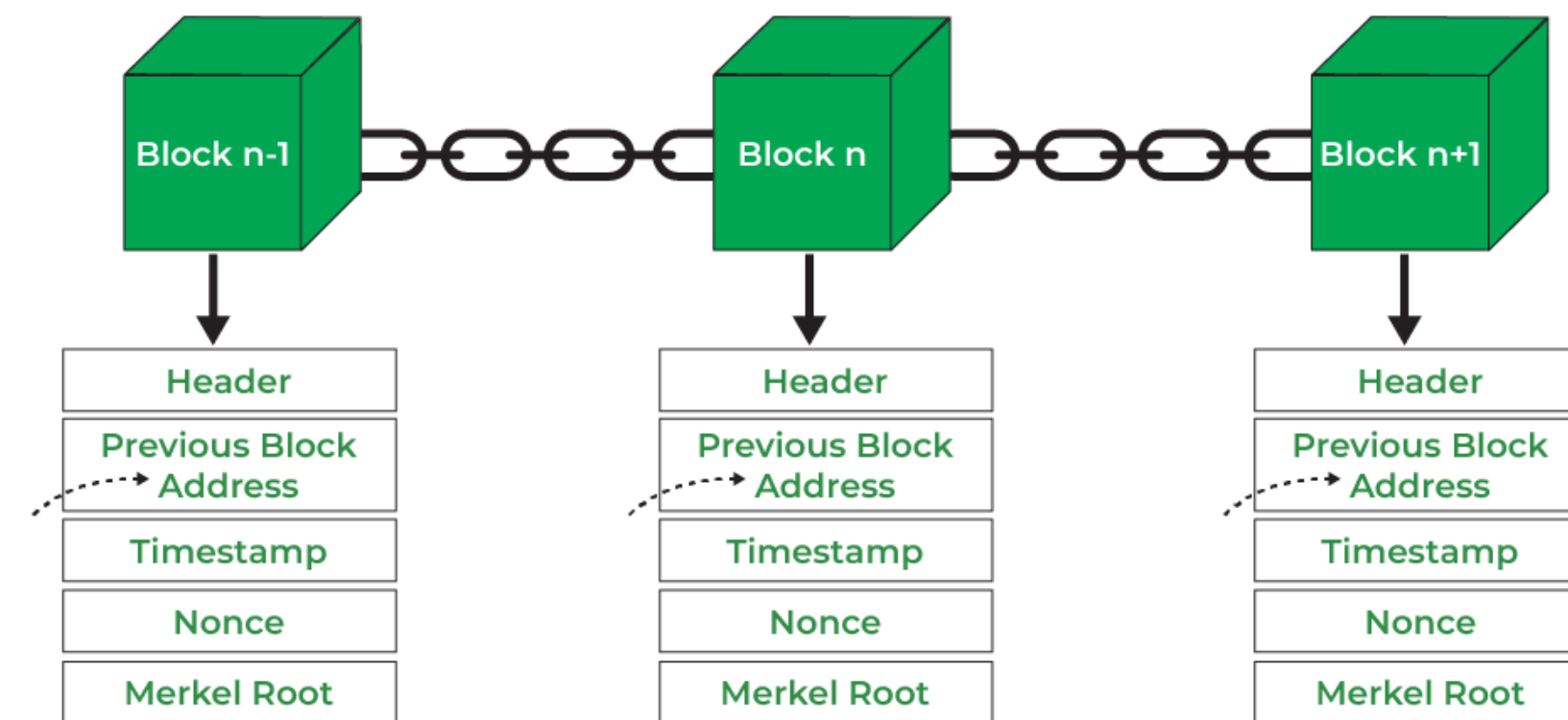
A hash chain is a sequence of data blocks where each block contains the hash of the previous block.

### Structure:

Block 1 → Hash → Block 2 → Hash → Block 3 → Hash → ...

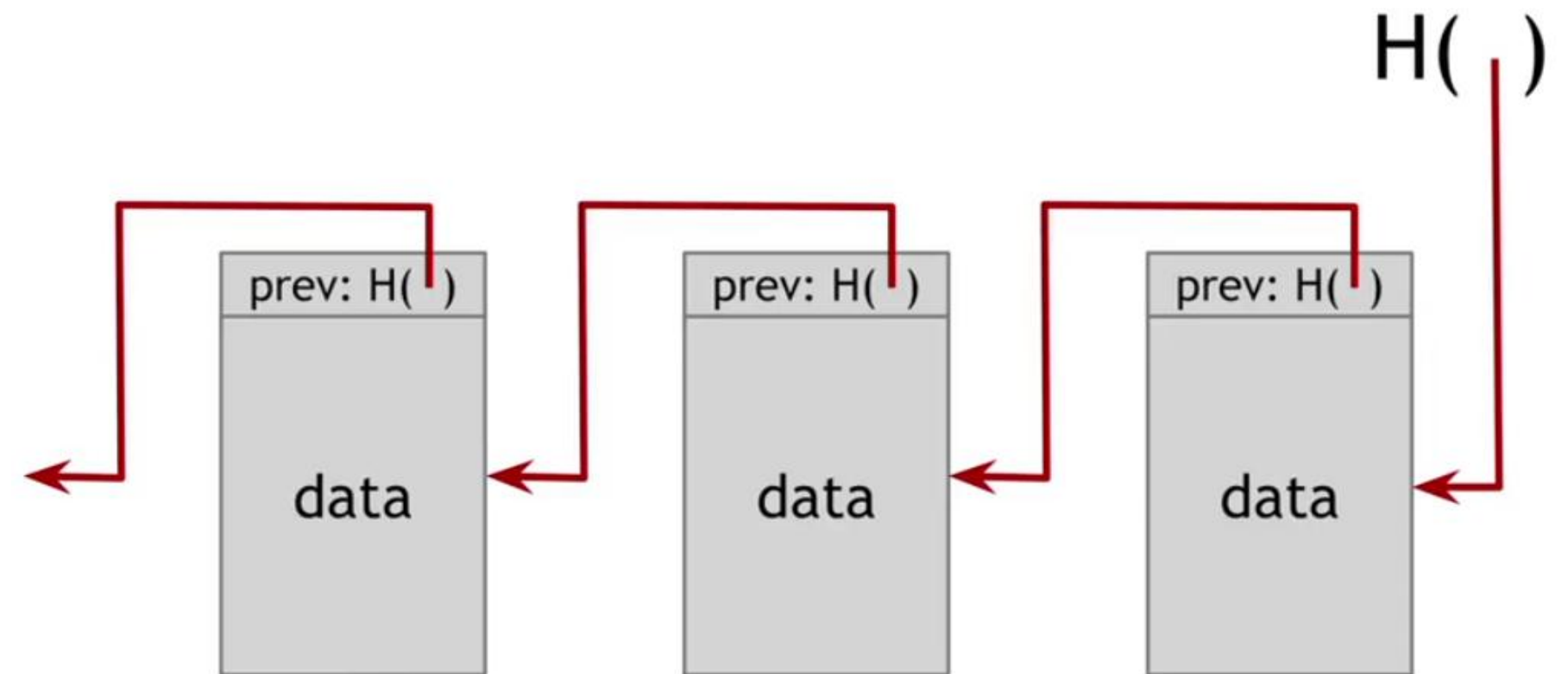
### Key Idea

- ✓ Every block depends on the previous block's hash
- ✓ If one block is altered, all subsequent hashes change
- ✓ Ensures data integrity and tamper detection



## Limitation of Hash Chain

1. No user identity
2. No ownership verification
3. No transaction authorization
4. Works well for integrity, but not for trust in multi-user systems



## Role of Digital Signature

A digital signature ensures authentication, integrity, and non-repudiation using asymmetric cryptography.

### Key Components

Private Key: Used to create the signature (kept secret by the sender)

Public Key: Used to verify the signature (shared openly)

### Process

- Transaction data is hashed
- Hash is signed using the sender's private key
- Network verifies signature using sender's public key

**A blockchain is an enhanced hash chain with added features:**

<b>Feature</b>	<b>Hash Chain</b>	<b>Blockchain</b>
Hash Linking	Yes	Yes
Digital Signature	No	Yes
Decentralization	No	Yes
Consensus Mechanism	No	Yes
Tamper Resistance	Partial	Very Strong

## Structure of a Blockchain Block

### Each block contains:

- Transaction data
- Hash of previous block (hash chain property)
- Digital signatures of transactions
- Timestamp
- Nonce (for consensus like Proof of Work)

### This makes blockchain:

- Immutable (hash chain)
- Trustworthy (digital signatures)
- Decentralized (consensus)

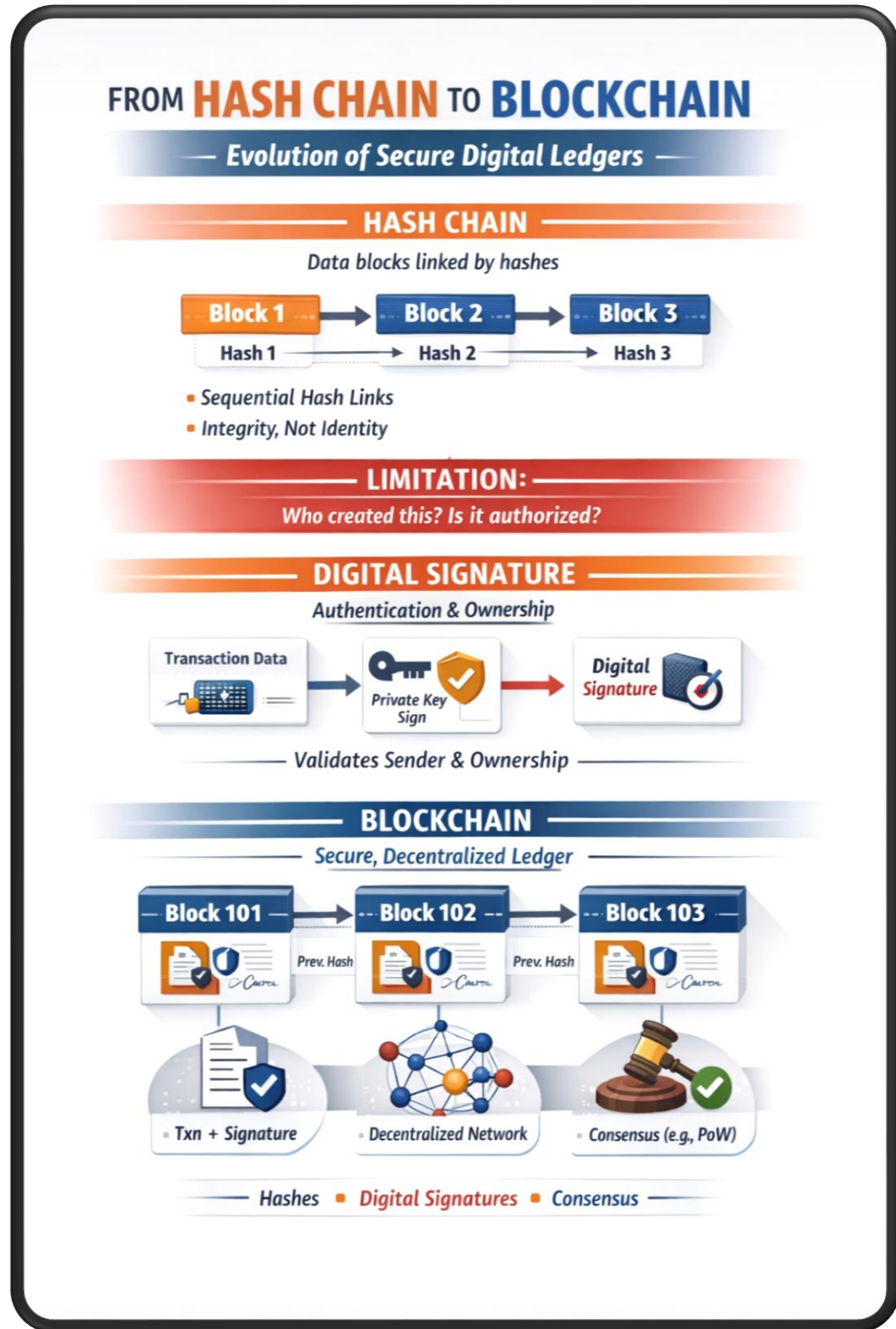
# Simple Evolution Summary

Hash Function → Ensures data integrity

Hash Chain → Links records securely

Digital Signature → Verifies sender and ownership

Blockchain → Secure, decentralized, trusted ledger



**THANK YOU**