UNIT - I

★ Blockchain

- It is a distributed database of records of all transactions or digital events that have been executed and shared among participating parties.
- Special nodes verify and validate these transaction. It contains every single record of each transactions. Ex - Bitcoin.
- This technology records transactions in Digital Ledger which is distributed over the network thus making it incorruptible.
- Land assets, Cars, etc can be recorded on Blockchain as a transaction.

★ Evolution and History of Blockchain

1991

Introduced by Stuart Haber and W. Scott Stornetta. They described a system where document timestamps could not be tampered with.

2008

Introduction of "Bitcoin : A peer-to-peer Electronic cash system" by Satoshi Nakamoto. It was the first practical implementation of BT.

2009

Bitcoin network was launched, and the first block (Genesis block) was mined.

2013

Vitalik Buterin proposed Ethereum, which expanded functionality beyond cryptocurrency.

2015

Ethereum was launched, bringing decentralized Applications (DApps) into focus.

Present

Blockchain continues to evolve with apps in finance (DeFi), supply chain, healthcare, governance, and more.

★ Characteristic / Features / Advantages

- **Decentralization** → Unlike traditional systems that rely on a central authority, blockchain relies on a distributed network of nodes, reducing control by single entity.
- **Immutability** → Once data is added to blockchain, it cannot be changed / deleted. Ensures integrity of data.
- **Transparent** → Because every node has a copy of the blockchain data, they have access to all transaction data. They themselves can verify the identities without any mediators.
- **Secure / Cryptography** → Data is encrypted, resistant to hacking or unauthorized data.
- **Consensus Mechanism** → PoW or PoS for validity of transactions across nodes.
- **Distributed Ledger** → Entire blockchain is replicated across all nodes, so that no failure exists.
- **Anonymity and Privacy** → User can remain anonymous, using cryptographic keys (no personal info).

★ Traditional database Vs Blockchain

Traditional database	Blockchain
• Uses centralized storage of data	• Use decentralized
• Needs Admin/Administrator to manage the stored data	• No administrator

• Modifying data requires permission from admin.	• Doesn't require permission. User have copy of data. Modyfying copies doesn't effect master copy. Blockchain is irresistible to modify.
• Centralized databases keeps info up-to-date	• It keeps present and past both info.

* **Blockchain Architecture / Components**

- **Blocks**
  Contains transactions, timestamp, nonce (Pow), and hash of previous block.
- **Nodes**
  These are the devices in blockchain network ~~by~~ used for validating transactions and blocks.
- **Ledger**
  A blockchain istself serves as a ledger where transactions are recorded in a decentralized manner.
  Transaction → Contract or agreement and transfer of assets b/w parties.
  Asset → typically cash or property.
  Digital Ledger → Network of computers in blockchain that stores the transactional data as a copy.
- **Consensus Algorithm**
  An algorithm that ~~agrees all blockchain~~ ensures all nodes agrees on the same version of blockchain.
- **Chain**
  It is a concept where all blocks are connected. Each block consist hash of the previous block.
- **Miners**
  Mining → Process that validates every step in transaction.
  People involved in mining are called miners.

* Distributed Ledger techno.

It is a database that is spread across various computer / nodes / institutions, accessible by multiple people.
Blockchain is one of the types of DLT in which transactions are recorded with an unchangeable cryptographic signature called a Hash.

⇒ Features

- Decentralized - solves dependency
- Immutable - no change / altered
- Fault tolerence - if one node fails, then still the data will available on other nodes.
- Transparency - Every participant can see the transactions that occures on the ledger
- Lower Costs - no intermediaries (bank) which reduces costs
- Anonymity - participant identity is anonymous
- Speed - DLT can handle larger transactions faster than the traditional method.

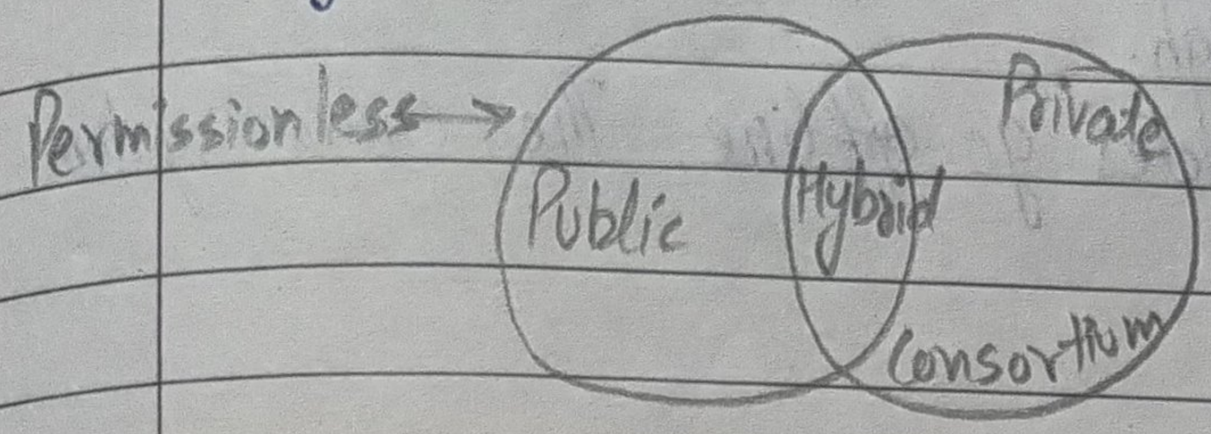
* DLT vs Blockchain

DLT	Blockchain
• Blocks can be organised in diff. forms	• Blocks are added in the form of chain.
• Doesn't need validation for each transaction.	• needs validation for each transactions.
• Doesn't require tokens or digital currencies.	• Tokens or digital cosruncies are required.
• Not sequence of data is needed.	• All blocks must be arranged in series.
• Trust among participating nodes is high.	• Higher than DLT.

Page No. _____
Date

★ Types of Blockchain

4 types are there:- Public, Private, Hybrid, Consortium.



1) Public Blockchain

- Completely open to following the idea of decentralization
- → not owned by one person
- → Anyone can participate in public blockchain
- → All the computers in the network holds the copy of other nodes or blocks.

Advantages:-

- → Secure - The blockchain is large. In a large size, there is greater distribution of records.
- → Decentralized - No single platform that maintains the network.

Disadvantages:-

- → Processing - transaction process is very slow.
- → Energy Consumption - verification of each transaction is a very high energy consuming task.

2) Private Blockchain

- only selected nodes can participate in the process.
- more secure than others.
- These blockchains are operated in a closed network
- Only few people are allowed to participate in network.

Advantages:-

- → Speed - High speed due to small size
- → Scalability - You can modify the size of the network.

Disadvantages:-

→ Security - Due to less no. of nodes, chances of manipulation are high.
→ Count - If a few nodes go offline, The entire system can be endangered.

3) Hybrid Blockchain

- Mixed of private and public blockchain
- Some part are controlled by organisation, and others are visible as public blockchain.
- Permission based and permissionless systems are used.
- User access info via Smart contracts

Advantages:-

→ Ecosystem - it cannot be hacked as 51% of users don't have access to the network.
→ Cost - Transaction are cheap as only few nodes verify the transactions.

Disadvantages:-

→ Efficiency - Not everyone can implement a hybrid blockchain.
→ Transparency - There is possibility that someone can hide info.

4) Consortium Blockchain

- Creative approach that solves the needs of the organisations
- In this types, more than one organisation manages the blockchain.

Advantages:-

→ Speed - limited no. of users make verification fast.
→ Privacy - The info of the checked blocks is unknown to the public view. but any member belonging to the blockchain can access it.

Page No.
Date

Disadvantages:-
→ Approval - All the members approve the protocol making it less flexible.
→ Transparency - Can be hacked if the organization becomes corrupt.

★ Consensus Mechanism
Since there is no central Authority, blockchain uses consensus algorithms so all nodes agree on the same version of the ledger.
Consesus ensures:-
- Agreement b/w nodes
- Cooperation
- Equal rights and paeticipation
- Only one valid version of the truth (the accepted block)

⇒ Types of Consensus Algorithms
1. Proof of Work (PoW)
→ Miners solve computational puzzles to add blocks
→ Requires high energy
→ Used by Bitcoin, earlier Ethereum

2. Proof of stake (PoS)
→ Validators are selected based on the no. of tokens they stake
→ Energy efficient.
→ Used by Ethereum 2.0, Cardano

3. Delegated Proof of stake (DPoS)
→ Users vote for delegates who validate blocks
→ Rewards are shared with voters
→ Used by EOS, TRON

4. Proof of Burn (PoB)
→ Validators burn coins to gain mining rights
→ The more coins burned, the higher the chances of block creation.

5. (PoET) Proof of Elapsed Time
→ Each node waits a random time; the shortest wait wins.
→ Ensures fairness
→ Used in Permissioned blockchains.

6. Proof of Authority (PoA)
→ Re-approved validators create blocks
→ Efficient but more centralized.
→ Used in VeChain, private Ethereum networks

* Cryptographic Foundations in Blockchain
BT is built on key cryptographic principles that ensures the security, integrity, and authenticity of data

1. Hash Function
It takes an input of any size and produces a fixed-size output called a hash value. It is used to map large data into a smaller, manageable format.

Key properties:-
→ Deterministic - Same input always gives the same output
→ Fixed output size - Hash value length doesn't depend on input size.
→ Efficient - Should compute the hash quickly.

Applications:-
→ Hash Tables - Fast data storage and retrieval.

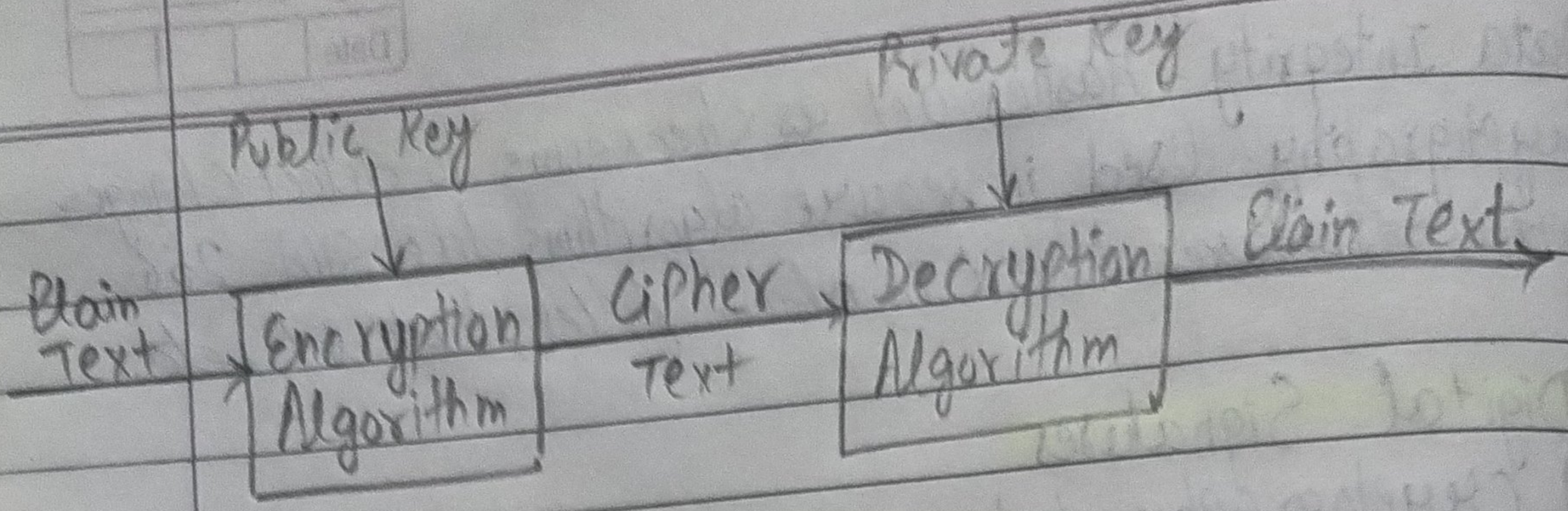
→ Data Integrity - Hashes act as checksums to detect changes
→ Cryptography - Used in secure algorithms like SHA-256
→ Data Structures - Used in bloom filters, hash sets, etc.

2. **Digital Signatures**
A cryptographic technique used to verify the authenticity and integrity of a transaction.
How it works:-
- A user signs a message with their private key, producing a digital signature
- Anyone with the user's public key can verify that the signature was created with the corresponding private key.

Applications of digital signatures:-
- Healthcare
- Legal
- Manufacturing
- Cryptocurrencies

3. **Public Key Cryptography**
It ~~used~~ uses two keys:-
→ a public key (shared with everyone) (encrypt) (locking)
→ a private key (kept secret) (decrypt) (unlocking)
These keys are mathematically linked and are used to encrypt, decrypt, and verify data securely.
Applications:-
→ Wallets & Addresses
→ Transaction security

⇒ So in one line we can summarize that public key cryptography secures blockchain by using a public key for identification and a private key for ownership and transaction authorization.



4. Merkle Trees

It is a tree based data structure used to verify and maintain the integrity of large datasets.

Structure:-

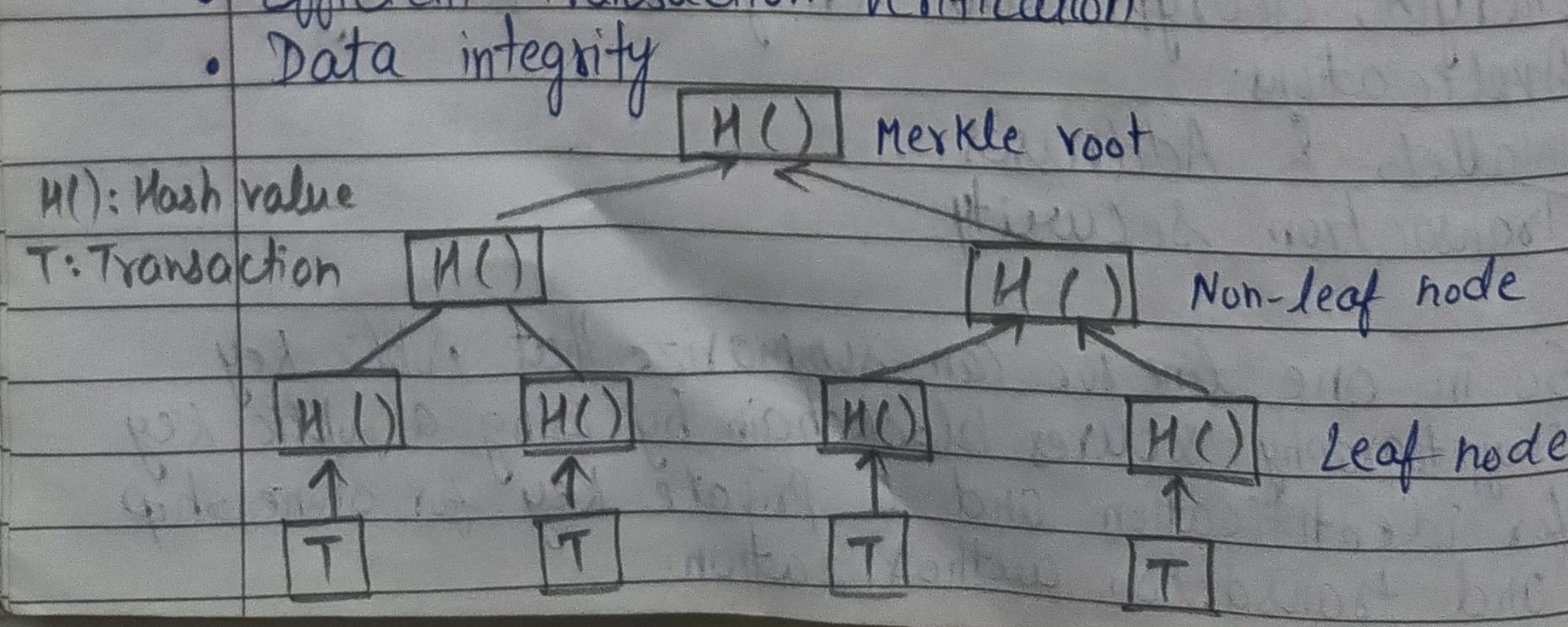
- Leaf nodes - Hashes of individual transactions
- Non-leaf nodes - Hashes of their child nodes
- Merkle root - The single top most hash representing all transactions in the block.

How it works:-

- Each transaction is hashed and placed in leaf nodes.
- Hashes are paired and combined upward until the merkle root is formed.
- To verify a single transactions, only.
  → the merkle root
  → and a few intermediate hashes (merkle proof) are needed.

Applications in Blockchain:-

- Efficient transaction verification
- Data integrity



★ Zero Knowledge Roofs (ZKPs)

It is a cryptographic technique where a prover can prove to a verifier that a statement is true without revealing the actual info.

Key prities Properties:-

- Completeness - If the statement is true, an honest prover convinces the verifier.
- Soundness - If the statement is false, no fake prover can convince the verifier.
- Zero Knowledge - The verifier learns nothing except that the statement is true.

Types of ZKPs

1. Interactive ZKPs
   - Prover and verifier exchange multiple messages
   - More rounds → higher confidence

2. Non-Interactive ZKPs
   - Only one proof is generated by the prover
   - No interaction needed; verifier checks it anytime

Applications in Blockchain

1. Privacy Reserving Transactions
   Used in Zcash (zK-SNARKs):- validates transactions without revealing sender, reveceiver or amount
2. Authentication
3. Verifiable Computation (off chain computation)
4. Voting systems

Advantages	Challenges
• High privacy	• Complex Implementation
• Secure Authentication	• Trusted setup issues.
• Efficiency	