

**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**

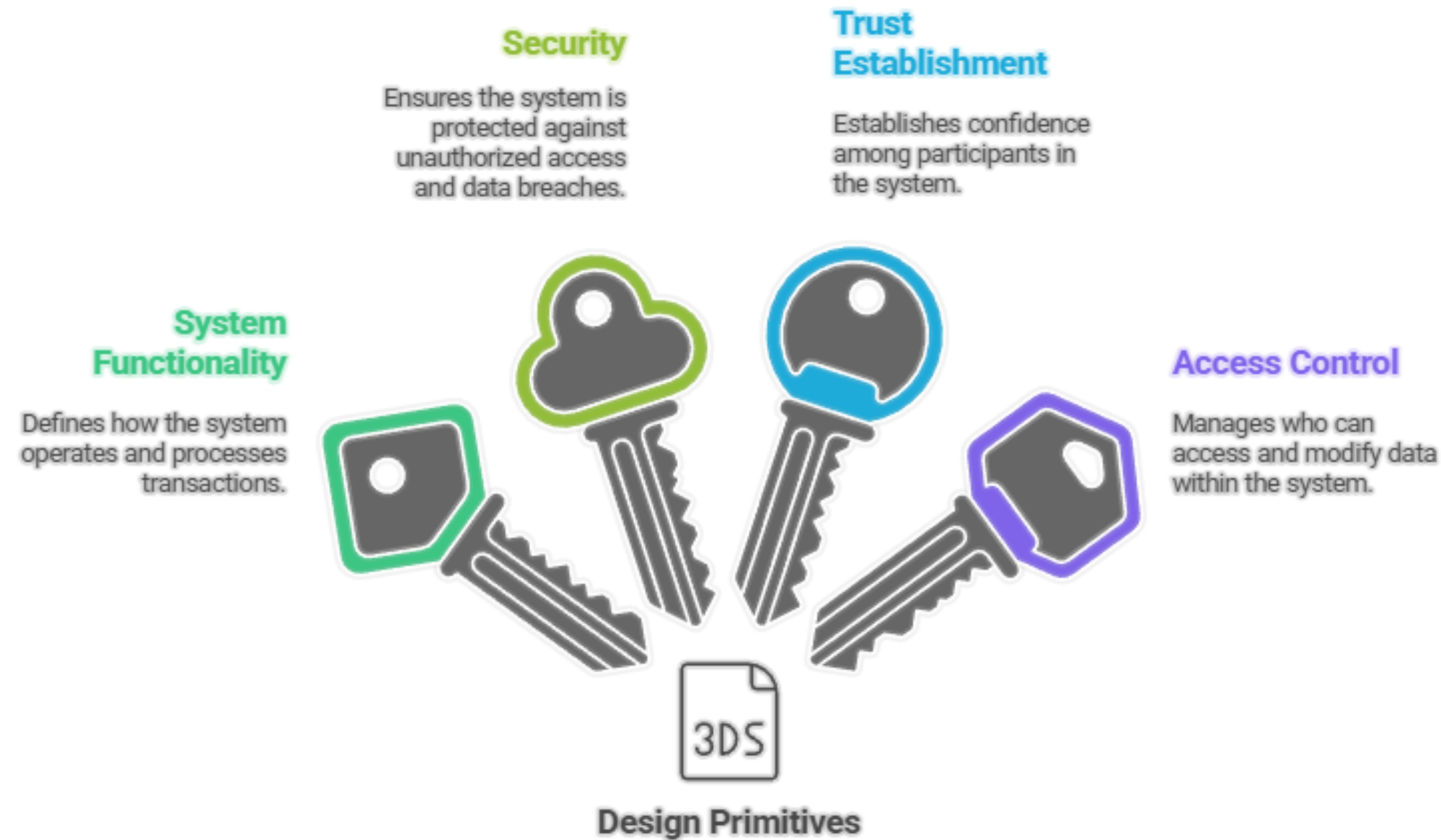
**DEPARTMENT OF COMMERCE WITH INFORMATION
TECHNOLOGY**

**21UCI505 – BLOCKCHAIN AND DISTRIBUTIVE
LEDGER**

Unit-1: Design Primitives

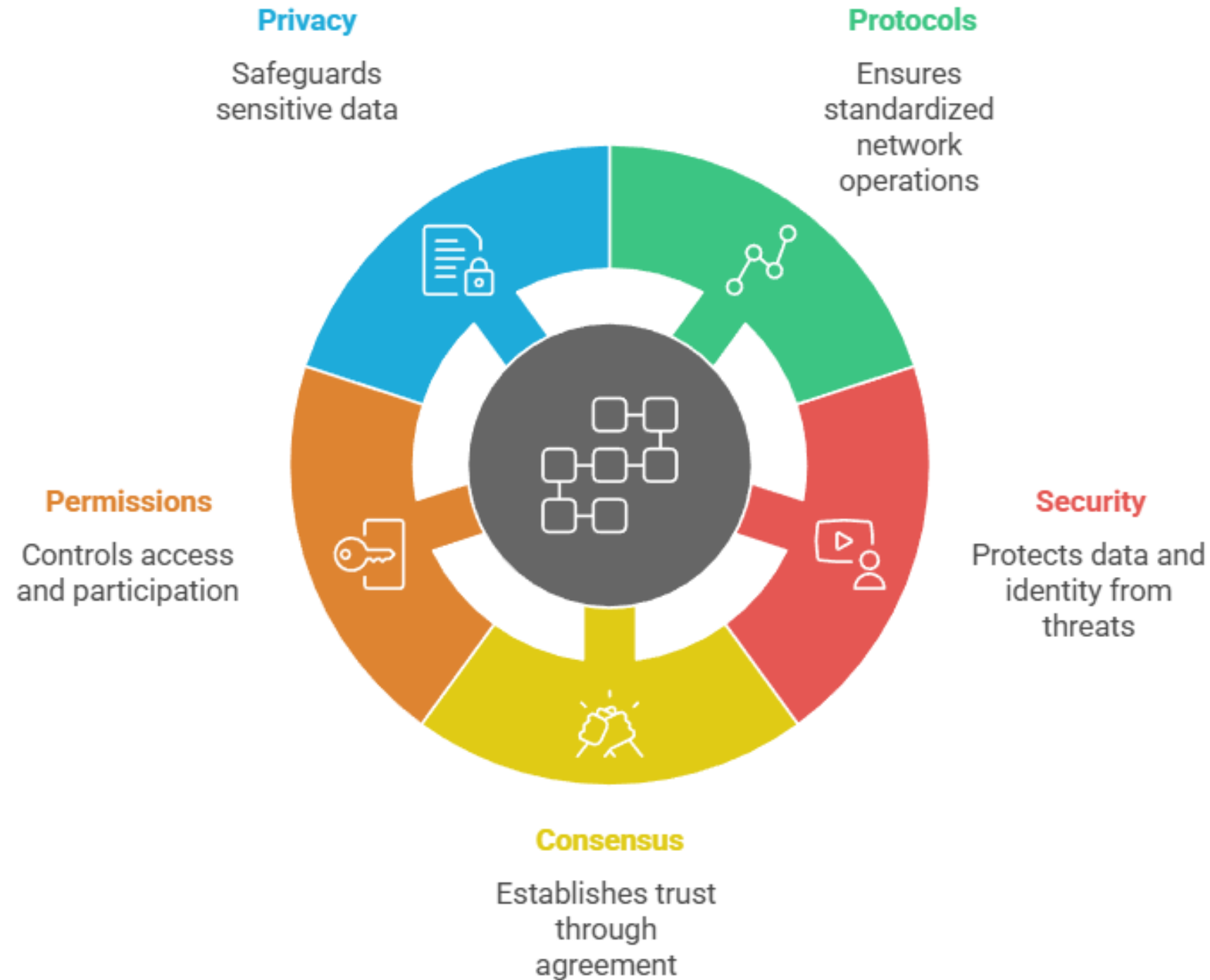
**Ms. S.Meenakshi, Assistant Professor
Department of Commerce with Information Technology**

Foundations of Distributed Ledger Systems



- ❖ fundamental building blocks used to design and operate a distributed ledger or blockchain system.
- ❖ define *how the system works, how it stays secure, how trust is established, and who can access what.*

Blockchain Design Primitives



1. Protocols

2. Security

3. Consensus

4. Permissions

5. Privacy

Meaning:

Protocols are the **rules and procedures** that define how the distributed ledger operates.

What they include:

- How nodes communicate
- How transactions are formatted
- How blocks are created & added
- How data is synchronized across nodes

Example:

Bitcoin protocol, Ethereum protocol, Hyperledger Fabric architecture.

Purpose:

Ensures **standardization and smooth coordination** among all participants.

Meaning:

Security primitives protect the ledger from **hacking, fraud, unauthorized access, and data tampering.**

Key security tools:

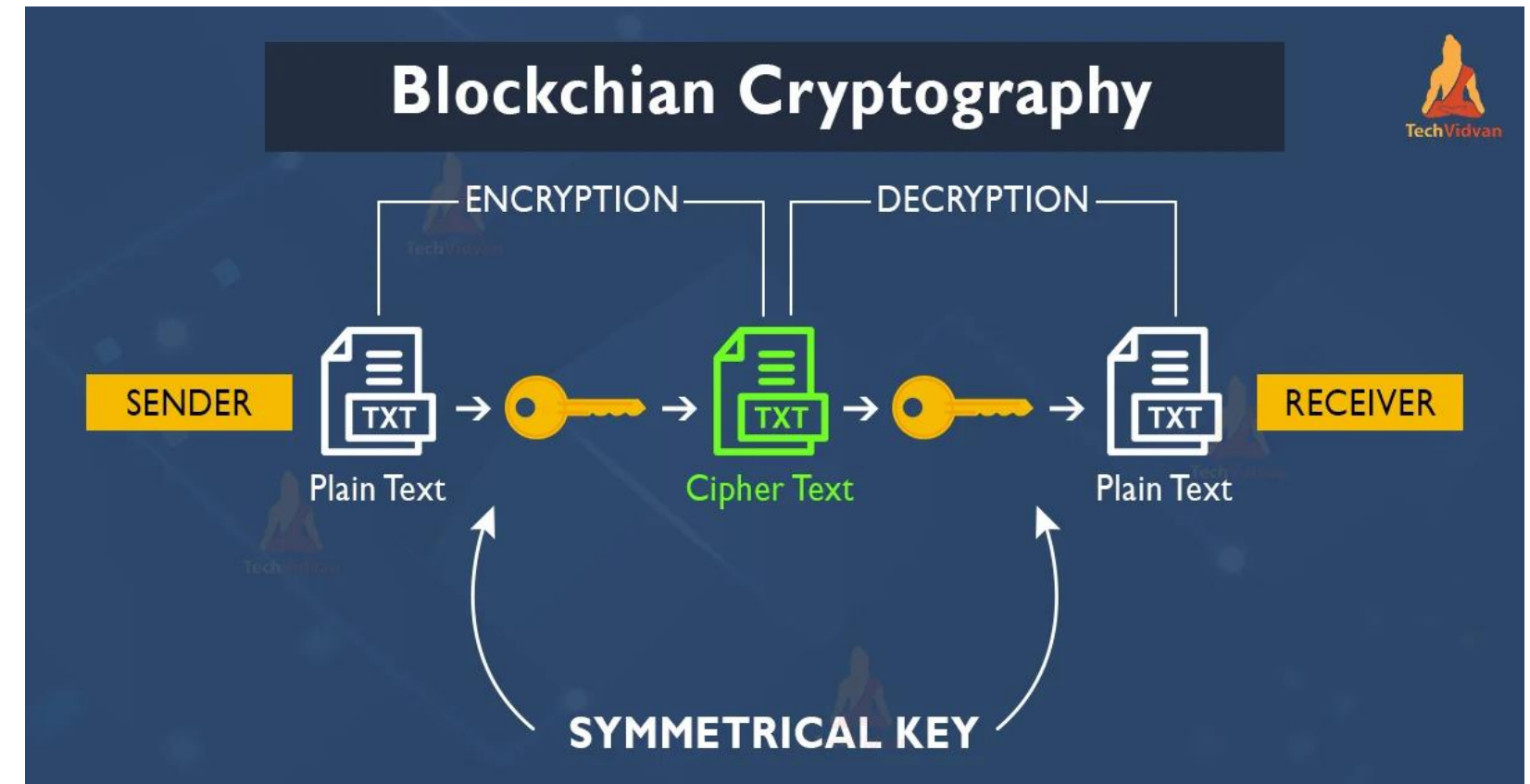
- Cryptography (public & private keys)
- Hashing (e.g., SHA-256)

Digital signatures

- Immutability of blocks
- Encryption

Purpose:

- ✓ Ensures transactions are **authentic, safe, and tamper-proof.**
- ✓ No one can alter recorded data.



Meaning:

Consensus is the **mechanism through which all nodes agree** on the validity of transactions.

Why it is needed:

- ✓ There is no central authority in DLT.
- ✓ Consensus maintains a single version of truth.

Common Consensus Algorithms:

- Proof of Work (PoW) – Bitcoin
- Proof of Stake (PoS) – Ethereum 2.0
- PBFT (Practical Byzantine Fault Tolerance) – permissioned networks
- Proof of Authority (PoA) – enterprise systems

Purpose:

Prevents-

- Double spending
- Fraud
- Conflicts between nodes
- Invalid transactions

Meaning:

Permissions define who can join the ledger, what they can view, and what actions they can perform.

Types:

1. Permissionless (Public) Blockchain

Anyone can join, read, and write. Example: Bitcoin, Ethereum.

2. Permissioned (Private/Consortium) Blockchain

Only approved members can join.

Used by banks, companies, and government. Example: Hyperledger Fabric.

Purpose:

Ensures controlled access, confidentiality, and compliance based on organization requirements.

Privacy primitives ensure that sensitive information is protected, even in a decentralized and transparent system.

Tools Used:

Zero-knowledge proofs (ZKP)

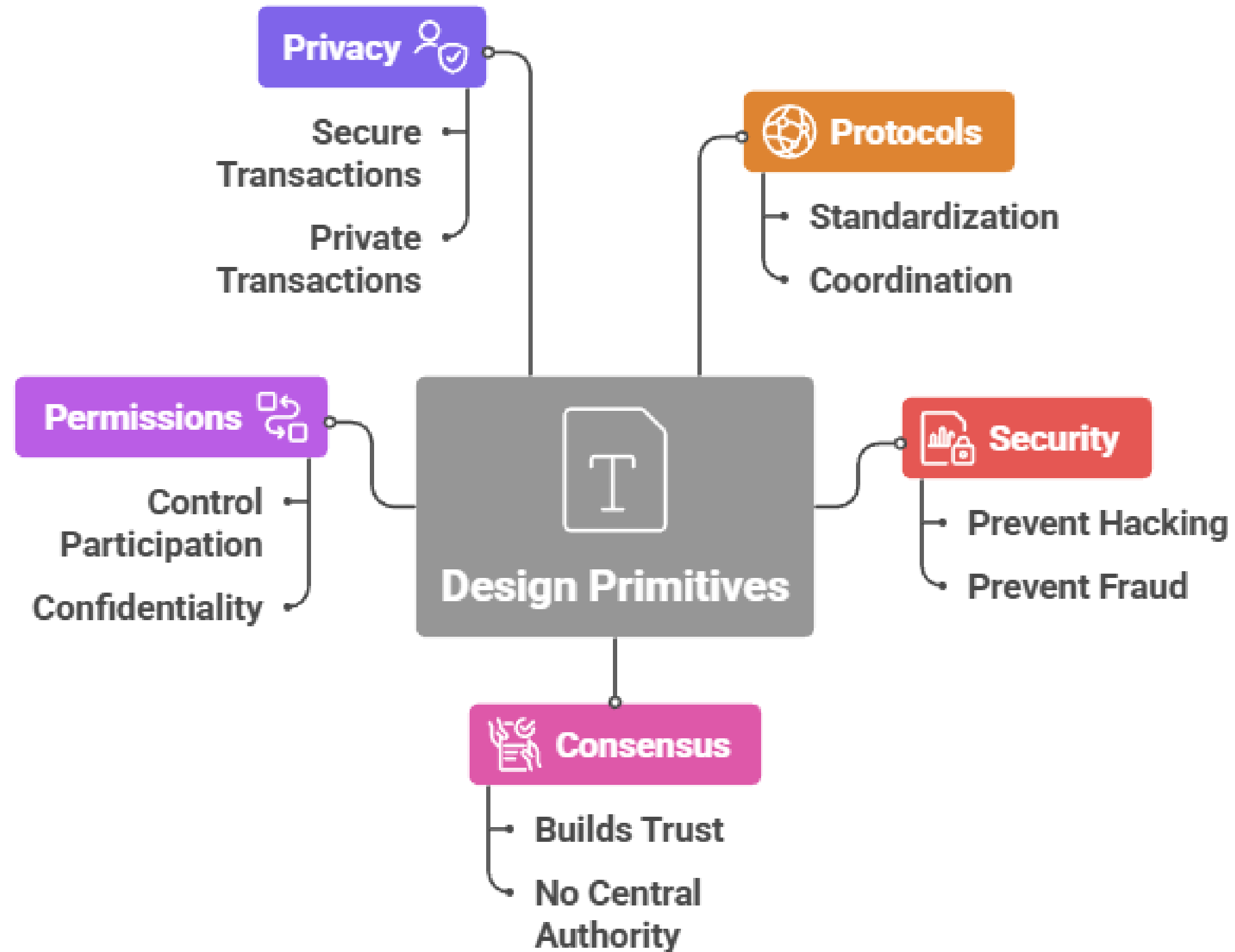
- Private channels (Hyperledger)
- Data encryption
- Off-chain data storage

Purpose:

Protects:

- Customer data
- Business secrets
- Transaction details
- Regulatory compliance (e.g., GDPR, banking regulations)

Design Primitives in Decentralized Systems



Assessment Questions & Answers

What is the mechanism nodes use to agree on a single version of truth?

Consensus

What are the rules that define how a distributed ledger operates?

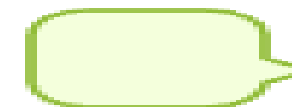
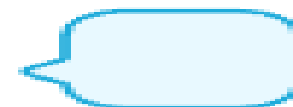
Protocols

What is the technique that protects data using keys and hashing?

Security

What control decides who can join or access a blockchain network?

Permissions



THANK YOU