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-3: Requirements for Consensus Protocols

Ms. S.Meenakshi, Assistant Professor

Department of Commerce with Information Technology

Consensus Protocol

A **consensus protocol** is a set of rules used in distributed systems (especially blockchain networks) to help all participating nodes agree on a single version of data or transactions without a central authority.

In simple words, it ensures that **everyone in the network agrees on what is true**, even if some participants are faulty or malicious.

Requirements for Consensus Protocols

A **consensus protocol** in distributed systems (especially blockchain) must satisfy certain essential requirements to ensure that all participating nodes agree on a single, correct version of data. These requirements are fundamental in platforms like Bitcoin and Ethereum.

1. Agreement (Consistency)
Definition:
All honest (non-faulty) nodes must agree on the same value or transaction.
Explanation:
If one node confirms a transaction as valid, all other honest nodes must also confirm the same transaction as valid.
Example:
If ₹10,000 is transferred from A to B, every node in the network must record the same transaction. There should not be two different versions.
Why Important?
Prevents conflicting records and double spending.

Requirements for Consensus Protocols

2. Validity (Correctness)

Definition:

If all honest nodes propose the same value, the final decision must be that value.

Explanation:

The protocol must ensure that only valid transactions are accepted.

Example:

If a user has ₹5,000 but tries to send ₹10,000, the system must reject it.

Why Important?

Ensures integrity and prevents fraud.

Requirements for Consensus Protocols

3. Termination (Liveness)

Definition:

All honest nodes must eventually reach a decision.

Explanation:

The consensus process should not run forever. It must complete within a reasonable time.

Example:

A blockchain transaction should be confirmed within minutes (like in Bitcoin) or seconds (like modern blockchains).

Why Important?

Ensures the system remains usable and efficient.

Requirements for Consensus Protocols

4. Fault Tolerance

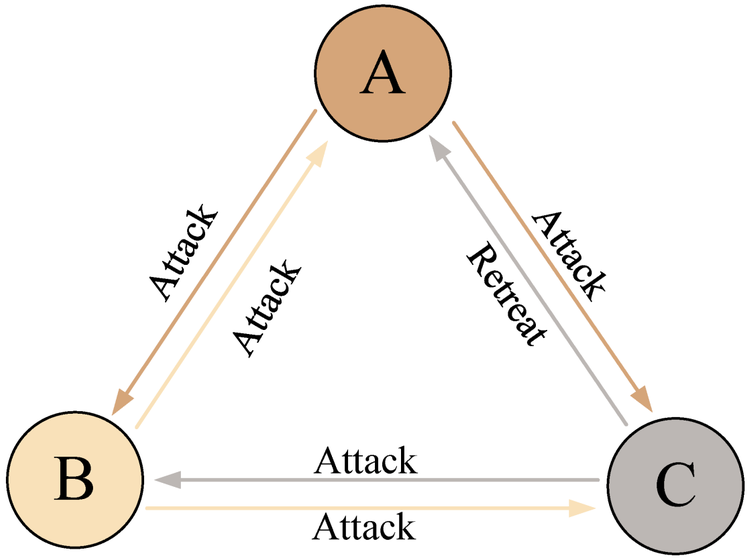
Definition:

The system must continue functioning even if some nodes fail or act maliciously.

Types of Faults:

Crash faults (node stops working)

Byzantine faults (node sends incorrect/malicious data)



Requirements for Consensus Protocols

5. Decentralization

Definition:

No single authority controls the decision-making process.

Explanation:

Decision power is distributed among many nodes.

Why Important?

Prevents monopoly, corruption, and central point of failure.

Requirements for Consensus Protocols

6. Security

Definition:

The protocol must protect against attacks like:

Double spending

51% attack

Sybil attack

Explanation:

It should be computationally or economically expensive to attack the system.

Why Important?

Maintains trust in the network.

Requirements for Consensus Protocols

7. Scalability

Definition:

The protocol must support growth in the number of nodes and transactions.

Explanation:

As users increase, performance should not degrade drastically.

Why Important?

Essential for real-world financial and enterprise applications.

Requirements for Consensus Protocols

8. Efficiency

Definition:

The protocol should use minimum resources (energy, time, computation).

Example:

Proof of Work consumes high electricity, while Proof of Stake is energy efficient (used in Ethereum after upgrade).

Why Important?

Reduces operational costs.

Requirements for Consensus Protocols

9. Transparency and Auditability

Definition:

All decisions and transactions should be verifiable.

Explanation:

Participants can independently check transaction history.

Why Important?

Enhances trust and compliance in financial systems.

Requirements for Consensus Protocols

10. Immutability

Definition:

Once consensus is reached, data cannot be altered easily.

Explanation:

Changing past records requires enormous computational or economic power.

Why Important?

Ensures permanent and tamper-proof records.

THANK YOU