Consensus Algorithm

✅ Blockchain & Consensus

- Blockchain is a distributed ledger without a central authority
- All nodes maintain the same ledger
- Consensus algorithms determine which data is valid

Main goals:

- Data integrity
- Double-spending prevention
- Malicious behavior deterrence

✅ Byzantine Fault

- Nodes may behave maliciously by sending false or conflicting information
- Causes system inconsistency

✅ BFT vs Non-BFT

BFT Systems

- Tolerate up to f malicious nodes
- Require at least 3f + 1 nodes
- Finalize blocks with 2f + 1 agreement
- Provide **deterministic finality**

Pros:

- Strong security

Cons:

- High communication overhead

Non-BFT Systems

- Assume only node crashes

- Do not handle malicious manipulation
- Provide **probabilistic finality**

Examples:

- Paxos
- PoW blockchains

✅ Finality Types

Probabilistic Finality:

- Reversal probability decreases over time
- Used in PoW

Deterministic Finality:

- Blocks are final once committed
- Used in BFT systems

✅ PBFT

Steps:

1. Pre-prepare
2. Prepare
3. Commit

Features:

- Secure under Byzantine faults
- Inefficient at large scale

✅ Proof of Work

- Miners solve cryptographic puzzles
- Longest chain rule
- Economic security
- Probabilistic finality

✅ PoS + BFT (DPoS)

- Validators stake tokens
- Small validator set uses BFT consensus
- Fast and final

✅ Tendermint

Phases:

- Propose
- Prevote
- Precommit
- Commit

→ Provides deterministic finality

✅ Recent Trends

HotStuff:

- Improved PBFT
- Reduced communication
- Signature aggregation

DAG:

- Parallel transaction processing
- Higher throughput
- Complex conflict resolution