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

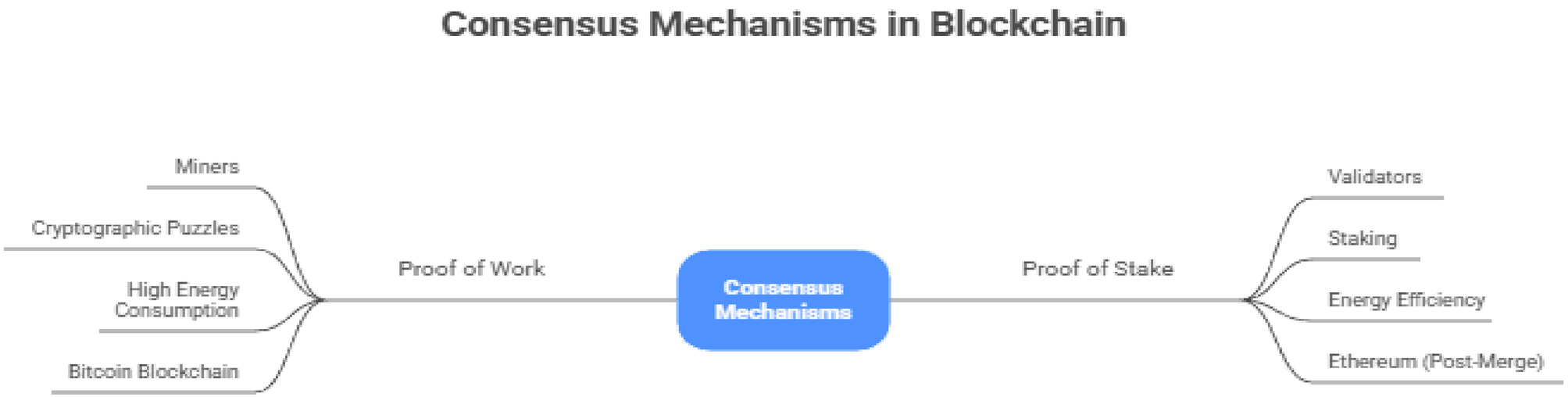
Unit-2: Consensus Mechanisms in Blockchain – Proof of Work and Proof of Stake

Ms. S.Meenakshi, Assistant Professor

Department of Commerce with Information Technology

Consensus Mechanism

A consensus mechanism is a protocol used in blockchain networks to achieve agreement among distributed nodes on the validity of transactions and the addition of new blocks. It ensures security, trust, and decentralization without a central authority. Two commonly used consensus mechanisms are Proof of Work (PoW) and Proof of Stake (PoS).



1.Proof of Work

Proof of Work (PoW) Explained

What is Proof of Work (PoW)?

It's a consensus mechanism where miners solve complex puzzles to validate transactions and add blocks to the blockchain.

How does it work?

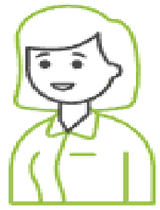
The first miner to solve the puzzle gets to validate transactions and add a block, receiving cryptocurrency and fees as a reward.

Why is it secure?

Altering data requires redoing the work for all subsequent blocks, which is practically impossible.

What are the drawbacks?

It consumes a lot of electricity and requires expensive hardware.



Case Study – Bitcoin Blockchain

Bitcoin uses the Proof of Work mechanism to maintain its decentralized network. For example, when a user transfers Bitcoin to another user, the transaction is broadcast to the network. Miners verify the transaction and compete to solve a cryptographic hash puzzle. Once a miner solves it, the transaction is added to a block and appended to the blockchain. This process prevents double spending and ensures trust without a central bank. Despite its success, Bitcoin has faced criticism due to high energy consumption and environmental impact, which has increased the search for alternative consensus mechanisms.

Simple Example – Classroom Puzzle

Imagine a classroom where the teacher asks students to solve a tough puzzle. The first student to solve it is allowed to write the answer on the board. Similarly, in PoW, the miner who solves the puzzle first adds the block. Bitcoin uses this method.

2. Proof of Stake (PoS)

What is Proof of Stake (PoS)?

It's an energy-efficient alternative to Proof of Work (PoW) where validators are selected based on the amount of cryptocurrency they stake.

How does it work?

The higher the stake, the greater the chance of being selected to validate a block. Validators earn rewards for honest behavior and may lose part of their stake if they act maliciously.

What are the benefits of PoS?

It significantly reduces energy consumption, improves scalability, and lowers entry barriers compared to PoW.

STAKE

In Proof of Stake (PoS), the term **stake** refers to the amount of cryptocurrency that a participant **locks or deposits** in the blockchain network to become a validator. This locked amount acts as a **security guarantee** and shows the validator's commitment to follow the network rules.

A higher stake increases the **chance of being selected** to validate transactions and create new blocks. Validators earn rewards for honest validation. If a validator behaves dishonestly or tries to approve invalid transactions, a **portion or all of the staked amount can be lost**. This penalty system encourages honest behavior.

Simple Example

Suppose a student deposits ₹5,000 as a refundable security to manage a college event. If the student performs the duty honestly, the deposit is returned with appreciation. If the student misuses funds, the deposit is forfeited. Similarly, in PoS, the stake is at risk if the validator acts wrongly.

In short:

Stake = Locked cryptocurrency used as **proof of trust and responsibility** in Proof of Stake.

THANK YOU