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: Consensus Protocols – Proof of Stake (PoS) Mechanism

Ms. S.Meenakshi, Assistant Professor

Department of Commerce with Information Technology

Proof of Stake (PoS) Mechanism

- a consensus mechanism used in blockchain networks (like Bitcoin)
- To validate transactions and
- To add new blocks securely.

Example:

- ❑ Imagine a lottery where the first person to guess a number that makes a lock open wins a prize.
- ❑ Guessing takes time and effort, but once someone wins, everyone can instantly check that the lock is open. That effort is **Proof of Work**.

Proof of Work (PoW) Mechanism

1. Transaction Collection

Users initiate transactions (e.g., sending cryptocurrency). These transactions are broadcast to the blockchain network and collected into a *block*.

2. The Cryptographic Puzzle

To add the block to the blockchain, *miners* must solve a complex mathematical puzzle.

The puzzle requires finding a **nonce** (a random number).

When the nonce is combined with the block data and hashed, the resulting **hash** must meet a specific condition (e.g., start with a certain number of zeros).

3. Mining (Trial-and-Error Process)

Miners repeatedly change the nonce and compute the hash until one miner finds a valid solution.

This process requires significant **computational power**.

There is no shortcut—only brute-force guessing.

Proof of Work (PoW) Mechanism

4. Block Verification

Once a miner finds a valid hash:

The solution is broadcast to the network.

Other nodes quickly verify the hash (verification is easy compared to solving).

5. Block Addition to the Chain

After verification, the block is added to the blockchain.

Each block contains the hash of the previous block, forming a secure, tamper-resistant chain.

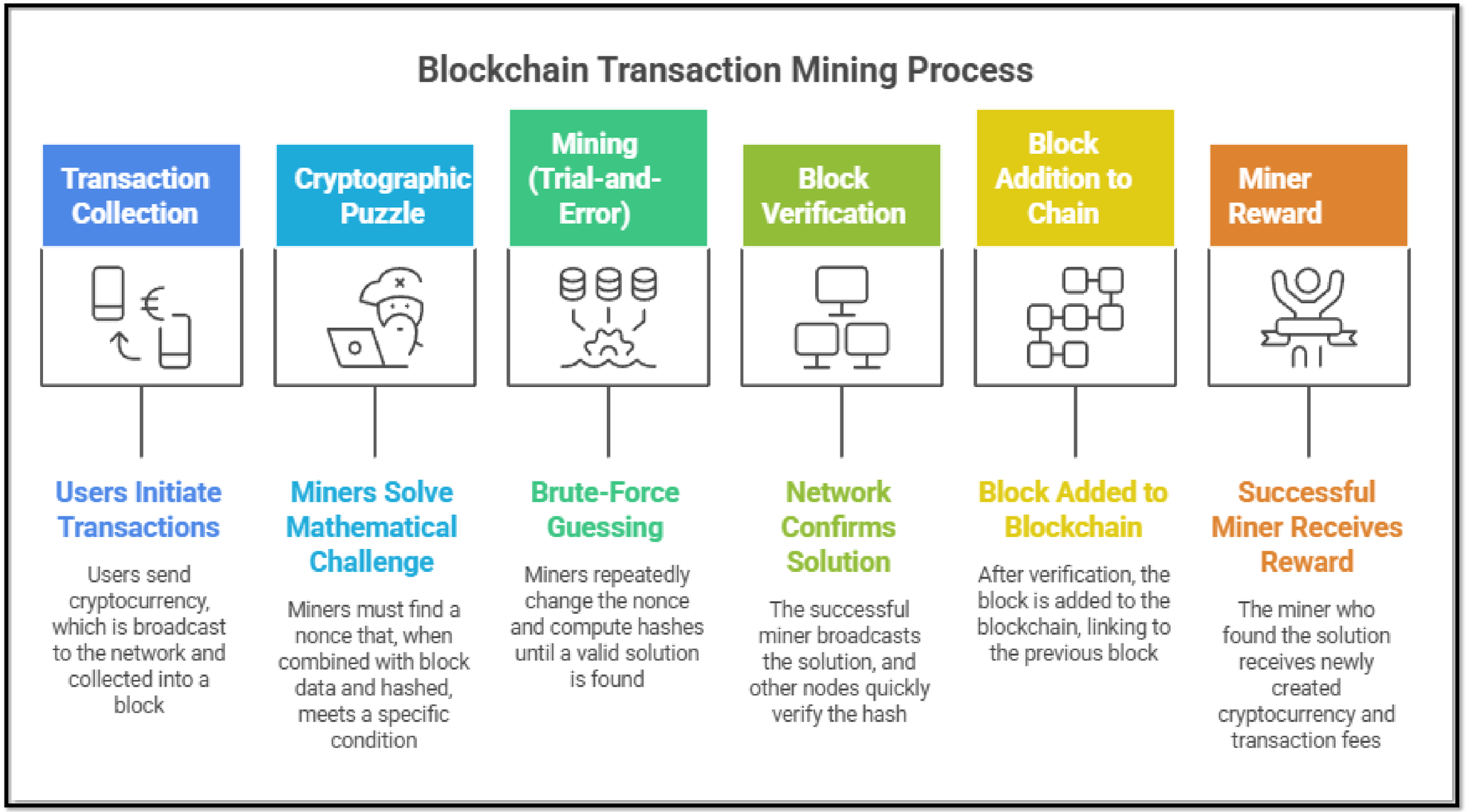
6. Miner Reward

The successful miner receives:

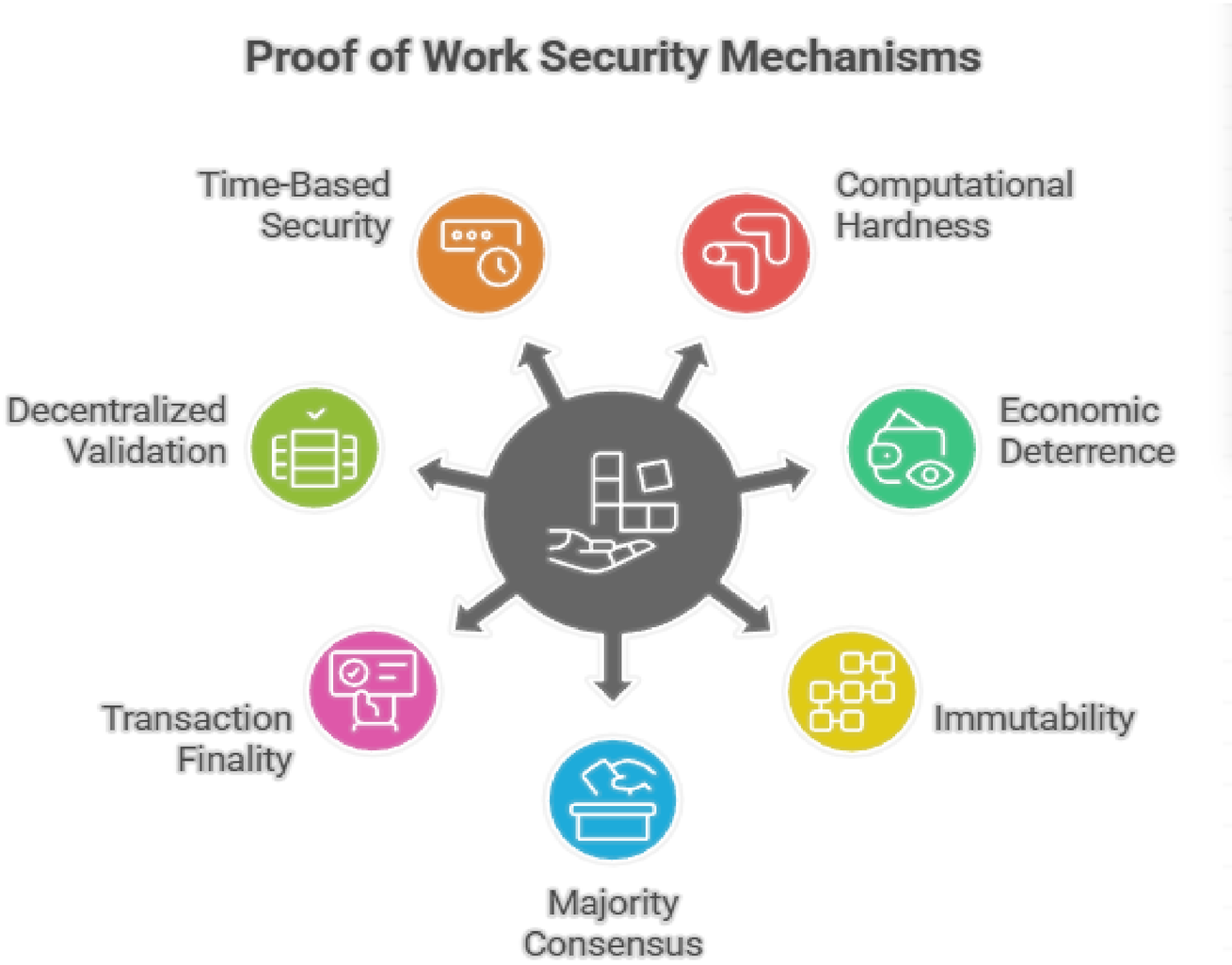
Block reward (newly created cryptocurrency)

Transaction fees from the transactions included in the block

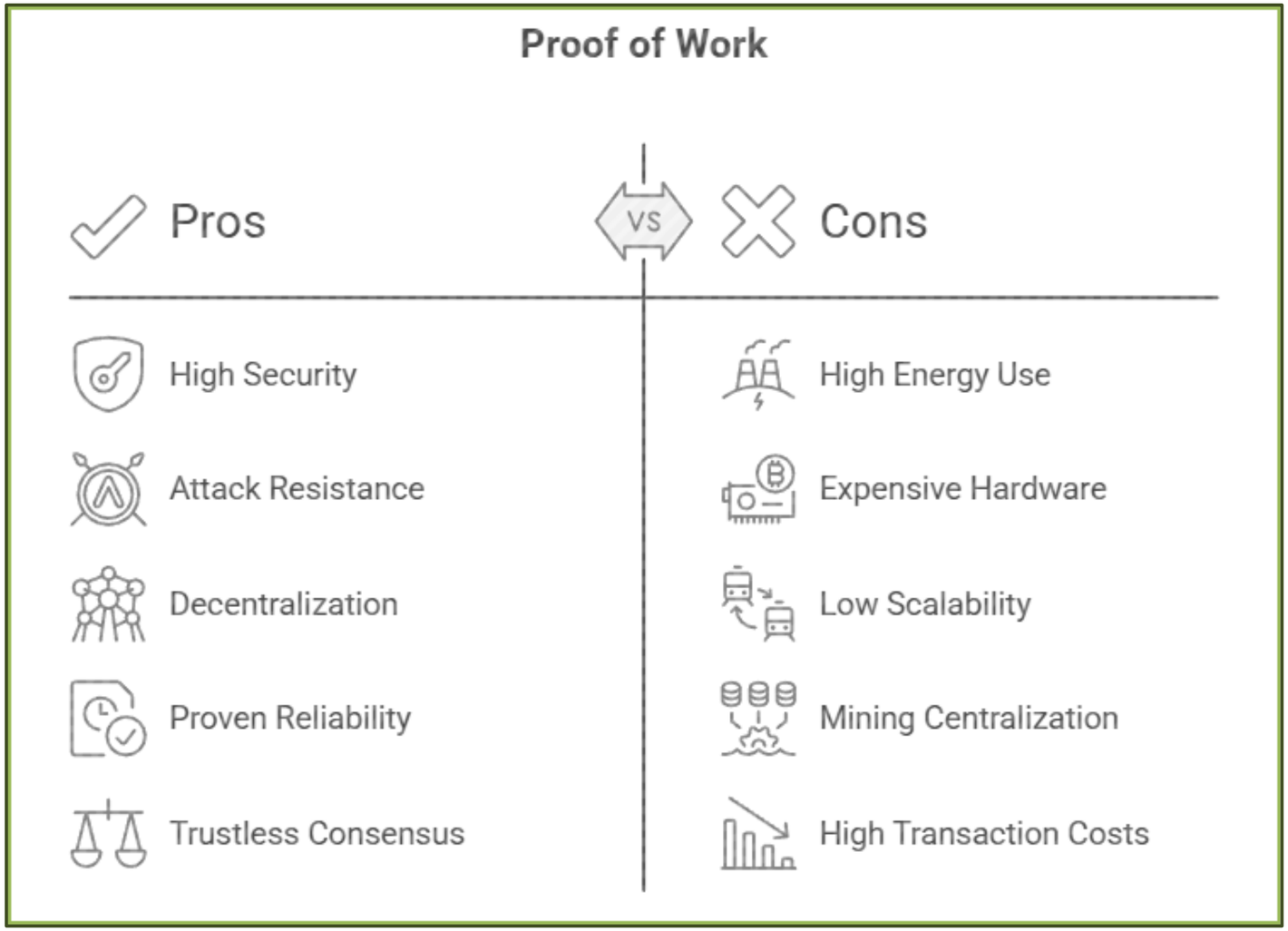
Proof of Work (PoW) Mechanism



Security Principles of Proof of Work (PoW) Mechanism



Advantages and Limitations



THANK YOU