RNT CORP

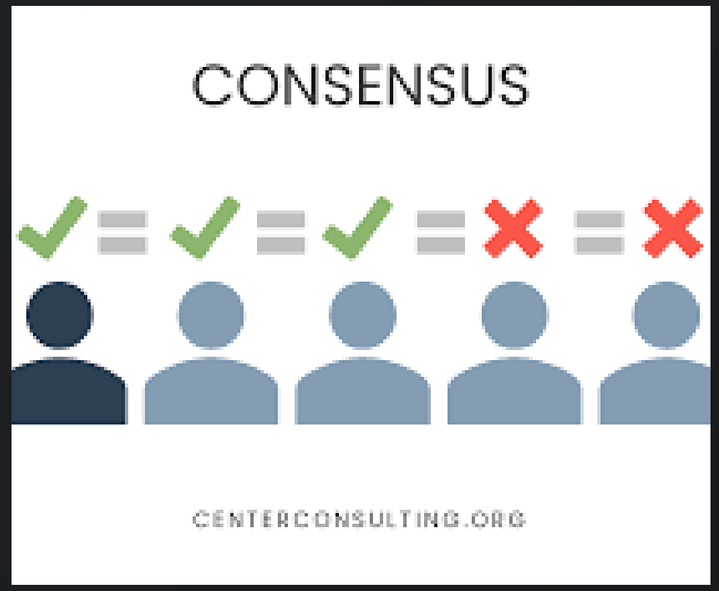
COMPARISON OF MAJOR BLOCKCHAIN CONSENSUS MODELS

PROOF OF WORK VS PROOF OF STAKE

Team: Ramazan, Nurai, Temirlan

RNT CORP

CONSENSUS IS A MECHANISM THAT ALLOWS DISTRIBUTED NODES IN A BLOCKCHAIN NETWORK TO AGREE ON A SINGLE VALID STATE OF THE LEDGER.



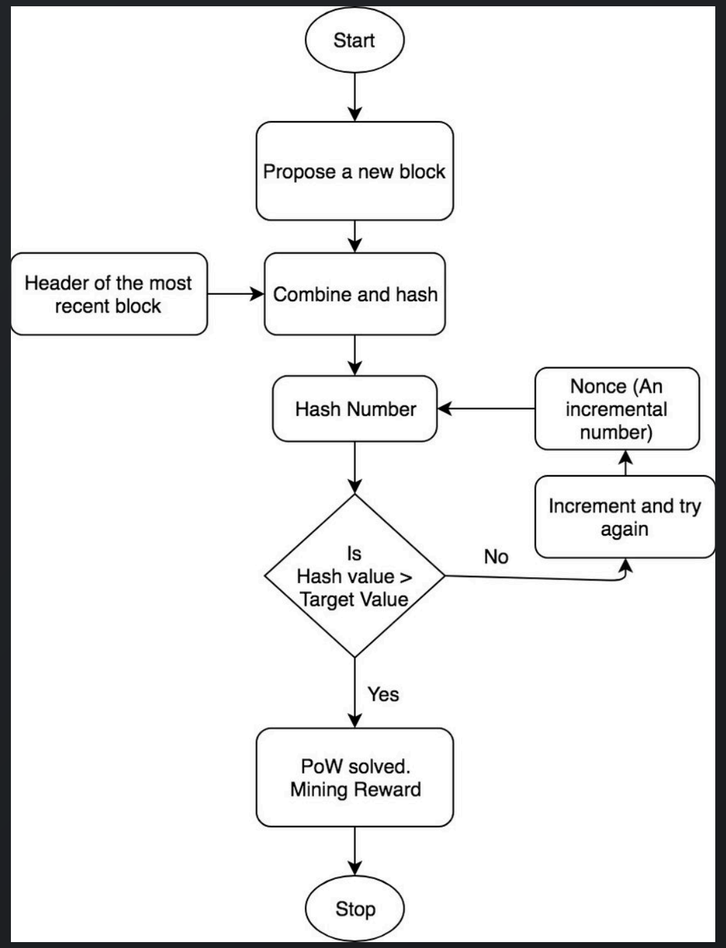
WHAT IS CONSENSUS?

It ensures:

- security
- consistency
- resistance to attacks
- trust without a central authority

RNT CORP

POW ARCHITECTURE



PROOF OF WORK ARCHITECTURE

In Proof of Work:

- transactions are broadcast to the mempool
- miners collect transactions into blocks
- miners compete by solving cryptographic hash puzzles
- the first miner to solve the puzzle adds the block to the chain

The chain with the most accumulated work is considered valid.

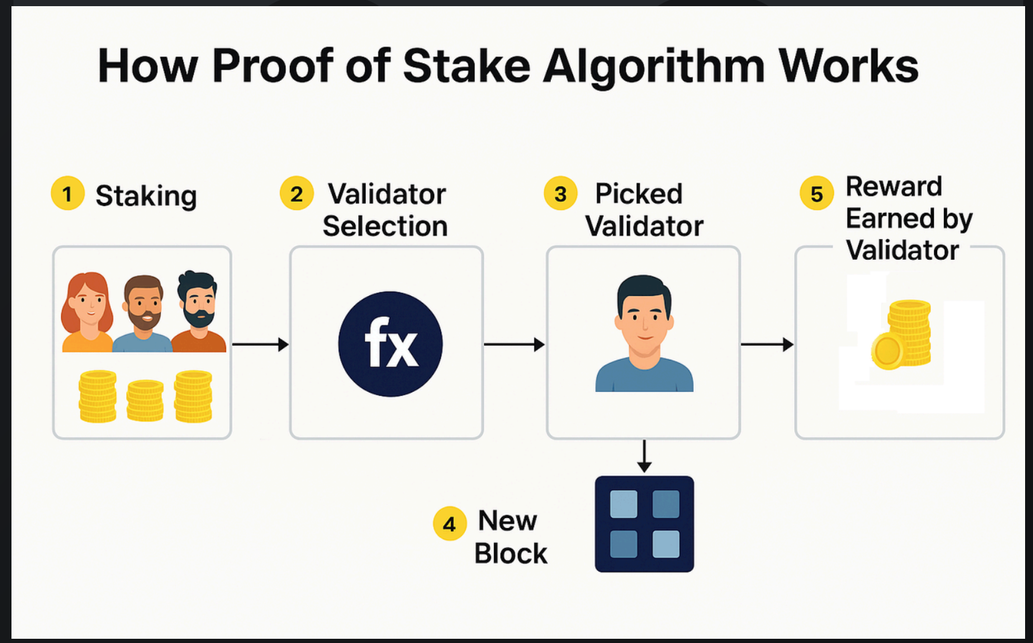
RNT CORP

POS ARCHITECTURE

PROOF OF STAKE ARCHITECTURE

In Proof of Stake:

- validators lock funds as stake
- a validator is selected to propose a block
- other validators attest to the block
- blocks are finalized using voting-based finality mechanisms
- Ethereum PoS uses proposer–attester roles and finality checkpoints.



RNT CORP

THREAT MODEL

+ POW THREATS:

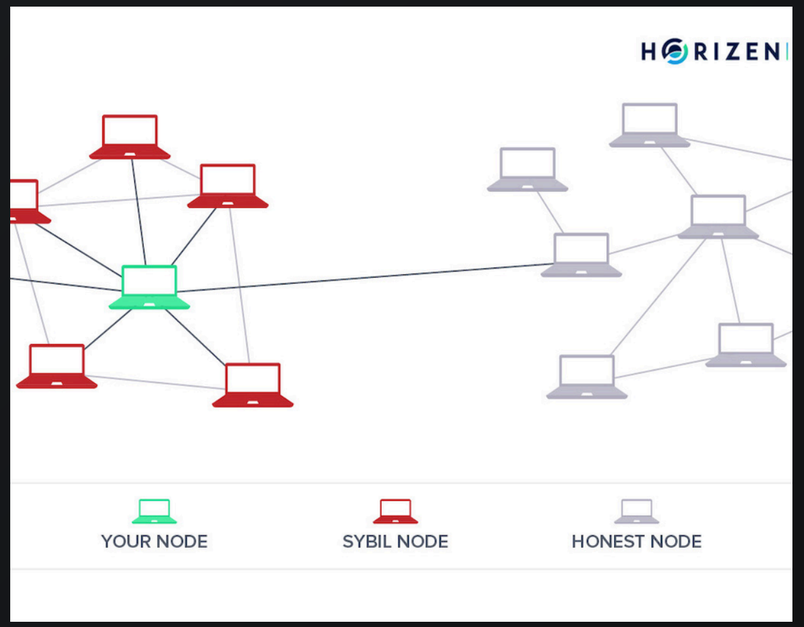
- 51% attack using majority hash power
- selfish mining
- mining pool centralization

+ POS THREATS:

- majority stake control
- validator collusion
- long-range attacks
- MEV-based manipulation

Proof of Work → Requires solving complex puzzles → very secure, but energy-heavy.

Proof of Stake → Based on ownership → efficient, faster.



RNT CORP

MATHEMATICAL ASSUMPTIONS

HOW THE NETWORK DECIDES WHAT'S TRUE

PoW assumes:

- honest majority of computational power
- cryptographic hash functions are secure
- block creation is probabilistic

PoS assumes:

- honest majority of staked capital
- digital signatures are secure
- network eventually reaches synchrony

RNT CORP

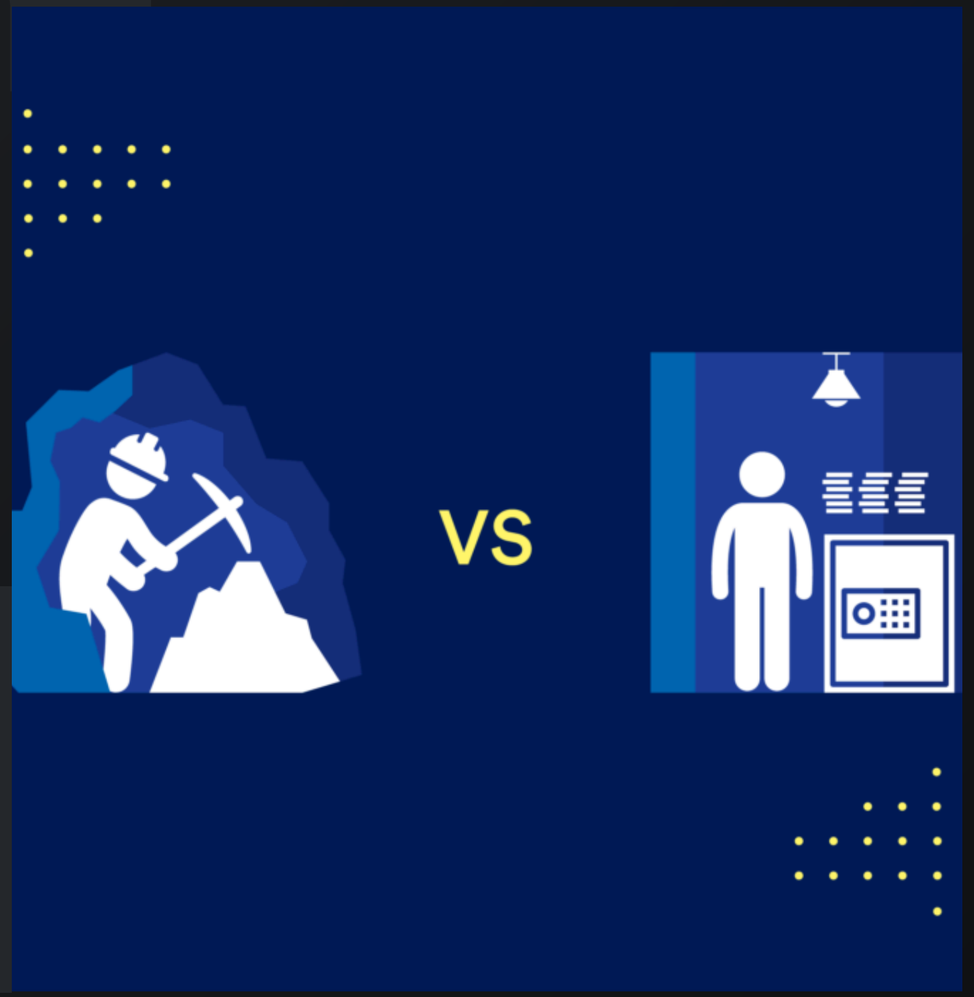
ECONOMIC ASSUMPTIONS

PoS security relies on:

- capital at risk (stake)
- slashing penalties for misbehavior
- economic disincentives for attacks

PoW security relies on:

- high energy and hardware costs
- continuous operational expenses



RNT CORP

REAL-WORLD ATTACKS

PoW examples:

- 51% attacks on small PoW blockchains
- mining pool concentration risks

PoS examples:

- validator centralization
- MEV attacks (transaction reordering)
- slashing incidents due to misconfiguration

Each model achieves consensus through different security and incentive structures.

RNT CORP

CRITICAL COMPARISON OF POW AND POS

+ Proof of Work

- Security is based on computational power and energy expenditure
- Resistant to some economic attacks but vulnerable to mining centralization
- Provides probabilistic finality, allowing temporary chain reorganizations

+ Proof of Stake

- Security is based on economic stake and validator incentives
- Reduces energy consumption significantly
- Provides faster finality through validator voting and slashing mechanisms

CRITICAL EVALUATION

RNT CORP

CONCLUSION

- Proof of Work and Proof of Stake represent two fundamentally different approaches to achieving consensus in blockchain networks.
- Proof of Work secures the network through computational effort and energy expenditure, while Proof of Stake relies on economic incentives, validator participation, and penalty mechanisms.
- Both models involve trade-offs between security, decentralization, efficiency, and scalability.
- The choice of a consensus mechanism depends on the specific goals and constraints of the blockchain system.

TEAM: RAMAZAN, NURAI, TEMIRLAN