ASTANA IT UNIVERSITY

CONSENSUS COMPARISON

Ainur Boranova, Alikhan Amanzholov, Damir Zarkesh

What Is **a consensus?**

Blockchain systems require a consensus mechanism to ensure that all participants agree on a single, consistent state of the ledger without a central authority. Consensus determines how blocks are produced, validated, and finalized. This presentation compares two major consensus models- Proof of Work and Proof of Stake - focusing on their architecture, security assumptions, economic incentives, and real-world implications.

SALFORD & CO.

OVERVIEW
Proof of Work

Proof of Work is the original blockchain consensus mechanism, used by Bitcoin and Ethereum before the Merge. In PoW systems, miners compete to solve cryptographic hash puzzles. The first miner to solve the puzzle earns the right to add a new block to the blockchain. Security is achieved through computational difficulty and the high cost of attacking the network. As more miners participate, the network becomes more secure due to increased hash power. However, this mechanism requires significant energy consumption and specialized hardware. Over time, these factors can lead to mining centralization and environmental concerns.

SALFORD & CO.

Benefit Of **Proof of Stake**

Economic Security

Proof of Stake secures the network by requiring validators to lock cryptocurrency as stake. This creates direct financial incentives for honest behavior and penalizes attacks through slashing mechanisms.

Validator-Based Consensus

Validators are selected to propose and attest blocks based on their stake rather than computational power. This significantly reduces energy consumption and allows more predictable block production.

Modern Implementations

PoS is implemented by Ethereum after the Merge and by Cardano’s Ouroboros protocol. These systems provide improved scalability, stronger finality guarantees, and higher sustainability compared to Proof of Work.

Architecture **comparison**

Proof of Work	Proof of State
Miners compete to solve hash puzzles	Validators are selected based on stake
Security based on computational power	Security based on economic stake
Energy-intensive block production	Energy-efficient block production
Probabilistic finality	Economic finality with checkpoints

Threat **models**

PoW systems are primarily threatened by 51% attacks, selfish mining, and mining pool centralization. These attacks require large computational resources.

PoS systems face threats such as validator collusion, long-range attacks, and stake centralization. However, PoS introduces explicit penalties that make malicious behavior financially costly.

SALFORD & CO.

Mathematical **Assumptions**

PoW relies on the assumption that cryptographic hash functions are secure and that the majority of computational power is controlled by honest participants. Block selection is probabilistic.

PoS assumes that the majority of stake is controlled by rational and honest validators. It relies on digital signatures, randomness, and game-theoretic models to ensure correct behavior.

SALFORD & CO.

Economic **Assumptions**

In PoW, security is linked to external economic costs such as electricity consumption and specialized hardware. Miners must continuously spend resources to remain competitive.

In PoS, security is based on internal economic risk. Validators place their own capital at stake, and slashing ensures that dishonest behavior leads to direct financial loss.

SALFORD & CO.

CONCLUSION

Consensus mechanisms define the security, efficiency, and decentralization of blockchain systems. Proof of Work provides strong trust minimization through computational cost but suffers from scalability and sustainability limitations. Proof of Stake replaces energy-intensive mining with economic incentives, enabling improved efficiency and faster finality. There is no universally optimal consensus model; the choice depends on system goals, including security requirements, performance, and decentralization trade-offs.

Thank You