LESSON 7: NODES, NETWORKS, AND CONSENSUS

A Prison Professors Self-Directed Course

Estimated time: 65–100 minutes

Educational Boundary:

> *This lesson explains technology. It does not recommend any network, company, product, or digital asset. It does not provide individualized financial, investment, legal, or tax advice. You do not need internet access, an account, a wallet, or a digital asset to complete the lesson.*

OPENING GUIDANCE

Lesson 6 explained how transactions can enter blocks and how hashes can connect one block to the next. That explanation leads to another question: If many computers hold copies of a blockchain, how do they decide which new information belongs in the accepted record?

When I study a system that involves many participants, I find it useful to separate the people, the tools, and the rules. Who participates? What work does each participant perform? Which rules guide the group when messages arrive at different times or when participants disagree? I encourage you to use those questions throughout this lesson.

You do not need to become a miner, operate a validator, or run a node. Your objective is to understand the roles well enough to evaluate claims. Words such as decentralized and consensus can sound as if a network reaches perfect agreement without leadership, cost, or conflict. A responsible learner asks what the rules actually require, who has practical influence, and what tradeoffs follow.

PURPOSE AND ESSENTIAL QUESTION

Lesson 7 explains how a network of computers communicates, checks information, and reaches agreement under a set of rules.

Essential Question:

» What can make a shared system trustworthy when no single participant controls the entire record?

LEARNING OBJECTIVES

After completing this lesson, you should be able to:

- Define node and consensus mechanism.
- Explain the problem consensus mechanisms are designed to address.
- Compare proof of work and proof of stake at an introductory level.
- Identify security, concentration, energy, speed, and participation tradeoffs.
- Distinguish a node from a miner or validator.

KEY TERMS

NODE

Definition: A computer running software that connects to a blockchain network and performs one or more network functions, such as receiving, relaying, storing, or checking data.

Sample sentence: The node checked the proposed block against the network's rules before accepting it.

VALIDATOR

Definition: A participant or node authorized by a proof-of-stake or related system to propose, check, or vote on blocks according to the network's rules.

Sample sentence: The validator reviewed the proposed block and submitted a vote under the protocol.

MINER

Definition: A participant in a proof-of-work system that uses computing power to compete for the opportunity to propose a block.

Sample sentence: The miner searched for a valid proof of work that other nodes could verify.

CONSENSUS MECHANISM

Definition: The collection of rules, processes, and incentives that helps distributed participants agree on an accepted blockchain history.

Sample sentence: The consensus mechanism told nodes how to evaluate competing versions of the latest block.

PROOF OF WORK

Definition: A method used in some blockchain consensus systems in which miners perform computational work to compete for the right to propose blocks.

Sample sentence: Bitcoin uses proof of work as part of the process for adding blocks and selecting an accepted chain.

PROOF OF STAKE

Definition: A method used in some blockchain consensus systems in which validators commit value, called stake, and may face rewards or penalties as they propose or check blocks.

Sample sentence: In a proof-of-stake system, dishonest validator behavior may put staked value at risk.

MAIN LESSON

A BLOCKCHAIN IS ALSO A NETWORK

A blockchain is more than a chain of records. It is also a network of computers running software. Those computers exchange transactions, blocks, and other messages. Each computer that participates through the network software is commonly called a node.

Nodes do not all perform the same job. Depending on the network and configuration, a node may keep a full copy of the blockchain, keep only selected information, relay messages, check blocks, help an application read data, or participate directly in consensus. A computer does not become a miner or validator merely because it is a node. Miner and validator describe more specialized roles.

This distinction matters because statements such as “the nodes voted” may hide important details. Which nodes were eligible to participate? Did every node vote, or did only a selected group propose and attest to blocks? Could ordinary full nodes independently reject a block that violated protocol rules? Accurate analysis begins by identifying the actual role.

THE AGREEMENT PROBLEM

Imagine that several record keepers maintain copies of the same journal. New entries travel between them, but messages do not always arrive in the same order. Two proposed pages may appear at nearly the same time. One computer may go offline. Another may send incorrect information. A dishonest participant might create many false identities to appear more influential than one person should be.

The group needs rules for at least four questions:

1. Validity: What makes a transaction or block acceptable under the protocol?
2. Proposal: Who may propose the next block, and how is that participant selected?
3. Chain choice: If competing versions appear, which history should nodes follow?
4. Finality: When should participants treat a block as sufficiently settled that reversal is unlikely or prohibited by the rules?

A consensus mechanism addresses these questions through software rules, cryptography, communication, incentives, and sometimes penalties. It is not simply an informal vote. It also does not require every participant to agree at every instant. Networks may briefly have different views because messages take time to travel. The rules provide a method for those views to converge on an accepted history.

TEMPORARY DISAGREEMENT AND FINALITY

Suppose two valid block proposals reach different parts of a network almost simultaneously. Some nodes may see the first proposal before the second, while other nodes see them in the opposite order. For a short period, honest participants can hold different views of the newest accepted block.

The network's chain-choice rules tell nodes how to resolve that conflict as more information arrives. One proposed branch may become the accepted history while the other is left behind. This temporary division is often called a fork, although the word fork can also describe a deliberate change in software rules. Context determines which meaning applies.

Finality describes the point at which a network treats a block as settled under its design. Some systems provide increasing confidence as more blocks accumulate. Others use validator votes to mark a block final after defined conditions are met. Final does not mean that software, governance, or social decisions can never affect a network. It describes a technical status under the current protocol rules.

CONSENSUS DOES NOT PROVE TRUTH

Consensus can establish that network participants accepted a transaction under their technical rules. It cannot prove that every statement about the outside world was true.

Suppose an authorized organization records that a learner completed a course. Nodes may verify the format, digital signature, and other protocol conditions. The network may reach consensus that the record belongs in a block. Those checks do

not independently prove that the learner actually completed the work. The quality of outside information still depends on people, source records, authorization, audits, and accountability.

Consensus should therefore be understood as agreement about the network's record and state, not universal agreement about reality.

PROOF OF WORK AND THE MINER'S ROLE

In a proof-of-work system, miners compete by repeatedly performing a computational task. A miner assembles a proposed block and searches for a result that satisfies the network's difficulty rules. Finding a valid result can require substantial computation, while other nodes can check the result much more quickly.

When multiple valid chains exist, the protocol applies a chain-selection rule based on accumulated work. A block usually becomes harder to reverse as additional proof-of-work blocks build on top of it. Settlement is therefore often described in terms of confirmations and increasing confidence rather than an immediate promise that reversal is impossible.

Proof of work makes attempted manipulation costly because an attacker may need extensive computing equipment and energy to compete with the honest network. It also creates tradeoffs:

- Mining can consume substantial electricity.
- Specialized hardware and access to inexpensive energy may influence who can compete effectively.
- Miners may combine resources in pools, creating concentration concerns.
- Block times and confirmation practices can affect how quickly users treat a transaction as settled.
- Security depends on the network's total honest computing power, software, incentives, and distribution—not on hashing alone.

Bitcoin is the best-known proof-of-work network. Ethereum also used proof of work historically, but it changed to proof of stake in 2022. That history is a reminder that a network's consensus design can change through an organized protocol upgrade.

PROOF OF STAKE AND THE VALIDATOR'S ROLE

In a proof-of-stake system, validators commit an asset as stake according to the network's rules. The system selects or assigns validators to propose blocks and to check or vote on proposed blocks. Honest participation may earn rewards. Cer-

tain provably dishonest behavior may lead to penalties, including the loss of some staked value, often called slashing.

Proof of stake replaces the proof-of-work competition for computing power with a security model built around committed value, validator messages, and penalties. It generally requires far less energy for block production than proof of work because validators are not racing through the same kind of repeated computational search.

Proof of stake also creates tradeoffs:

- Greater stake may bring greater influence or a greater chance of selection, depending on the design.
- Large holders, custodians, staking services, or coordinated operators may create concentration concerns.
- Penalties can punish dishonest conduct, but software mistakes, configuration errors, or downtime may also create losses under some rules.
- The details of proposer selection, voting, chain choice, and finality can be complex.
- Participation requirements differ across networks and may include minimum stake, technical equipment, continuous operation, or delegation.

The phrase proof of stake describes a broad family of designs. Ethereum's system, BNB Smart Chain's system, and another proof-of-stake network may use different validator sets, voting procedures, finality rules, and penalties. Knowing the label is only the beginning of the analysis.

COMPARING THE TWO APPROACHES CAREFULLY

Proof of work and proof of stake aim to make dishonest control expensive, but they place the cost in different resources. Proof of work relies heavily on computing power and energy. Proof of stake relies on committed economic value and the threat of penalties.

Neither method automatically guarantees decentralization. A proof-of-work network can become concentrated among large mining operations or pools. A proof-of-stake network can become concentrated among large stakeholders, service providers, or a limited validator set. The important questions include how participation is distributed, how easily independent participants can verify the chain, how upgrades occur, and what happens when powerful actors coordinate.

Speed also requires careful wording. A consensus design may permit shorter block times or faster finality, but performance depends on the entire network architecture. Faster processing may involve tradeoffs in validator count, hardware requirements,

communication demands, or decentralization. The name of a consensus method alone does not prove that one network is faster, safer, cheaper, or more decentralized than another.

APPLIED EXAMPLE: BNB SMART CHAIN

As of July 20, 2026, BNB Chain's official documentation describes BNB Smart Chain as using Proof of Staked Authority, commonly shortened to PoSA. The design combines stake-based validator selection with an active set of validators that takes turns proposing and voting on blocks. Its rules also include penalties for conduct such as double signing, certain malicious votes, and extended downtime.

This example shows why labels require investigation. BNB Smart Chain uses stake, but its operation is not identical to Ethereum's proof-of-stake system. Its active validator design may support short block times and fast finality, while a limited block-producing set also raises questions about concentration and participation. Those are design tradeoffs to examine, not reasons to praise or reject the network automatically.

Mentioning BNB Smart Chain is an educational example. It is not an endorsement, an invitation to acquire BNB, or a request to operate a validator or conduct a transaction.

WHAT CREATES PRACTICAL TRUST

People sometimes describe blockchains as "trustless." A more careful explanation is that a blockchain can reduce dependence on one central record keeper by distributing verification across participants and enforcing shared rules. Trust does not disappear. It shifts.

Participants still rely on protocol design, software implementation, network communication, cryptography, economic incentives, operator behavior, governance, and access to independent verification. They may also rely on developers, hardware, internet providers, custodians, data sources, and legal institutions.

A shared system becomes more worthy of confidence when its rules are clear, independent participants can verify compliance, dishonest behavior is difficult or costly, failures are detectable, software is reviewed, and power is not dangerously concentrated. No single feature proves trustworthiness. Responsible evaluation looks at the system as a whole.

APPLIED SCENARIO: COMPETING RECORD KEEPERS

Seven community organizations maintain a shared record of donated textbooks. Each organization runs software that receives new entries and checks whether the submitting organization signed them correctly.

Two proposed blocks arrive close together. One records a delivery of 100 books. The other records 80. Both have a valid technical format, and each refers to a different source report. The organizations need a rule for choosing which proposed block becomes part of the shared history.

Under one possible design, participants who perform verifiable computational work compete to propose the block, and the network follows the valid chain with the most accumulated work. Under another design, selected participants place value at risk, propose or vote on a block, and may lose that value for provably conflicting conduct.

Reasoned conclusion: Either rule may help the network settle on one technical history. Neither rule proves whether 100 or 80 books actually arrived. The organizations still need delivery receipts, authorized submitters, correction procedures, and audits. Consensus can organize agreement about the record; outside evidence establishes whether the record reflects reality.

BENEFITS, LIMITATIONS, RISKS, AND MISCONCEPTIONS

POSSIBLE BENEFITS

- Shared rules can help independent computers converge on one accepted history.
- Nodes can verify transactions and blocks instead of relying entirely on one record keeper.
- Incentives and penalties can make certain dishonest behavior costly.
- Multiple copies and independent verification can improve resilience.
- Public protocols can make decision rules available for inspection.

IMPORTANT LIMITATIONS AND RISKS

- Consensus does not prove that outside information was truthful or lawfully obtained.
- Network delays, software defects, attacks, or configuration errors can disrupt agreement.
- Mining power, stake, validator operation, software development, or infrastructure can become concentrated.
- Proof of work may require substantial energy and specialized equipment.

» Proof of stake may expose committed value to penalties and may concentrate influence among large stakeholders or services.
» Governance decisions can change rules, divide communities, or create separate chains.

COMMON MISCONCEPTIONS

» "Every node is a miner or validator." Many nodes relay or verify information without proposing blocks.
» "Consensus means every node agrees instantly." Networks can have temporary disagreement and use rules to converge.
» "Consensus proves the recorded claim is true." It shows acceptance under network rules, not proof of every outside fact.
» "Proof of work is secure because it uses hashes." Its security depends on accumulated work, network distribution, incentives, software, and honest participation.
» "Proof of stake is simply one person, one vote." Voting weight and selection depend on the network's protocol and stake rules.
» "One consensus method is always superior." Security, energy, speed, concentration, access, and governance involve tradeoffs.
» "Trustless means no trust is required." Trust shifts from one central keeper to a broader technical and social system.

OFFLINE EXERCISE: COMPARE THREE AGREEMENT RULES

Estimated time: 20–25 minutes

Materials: Separate paper and a pencil.

Imagine that seven record keepers maintain identical paper logs. Two conflicting entries arrive for the same delivery. The group must choose one entry for the next page.

RULE A: ONE COORDINATOR

One designated coordinator checks the entries and chooses the official version. Everyone copies that choice.

RULE B: PROOF-OF-EFFORT SIMULATION

Each proposed writer must complete a difficult paper puzzle. The first writer to produce a correct solution earns the opportunity to propose the page. The others

can check the solution quickly. Later pages build on the accepted page, and the group follows the valid history with the most accumulated puzzle work.

RULE C: STAKE-AT-RISK SIMULATION

Eligible writers place ten paper points at risk. The rules select one writer to propose the page. Other selected participants check it and record approval or rejection. A writer who signs conflicting pages loses the paper points under the exercise rules.

On separate paper, create four headings for each rule:

1. Who proposes the record?
2. What discourages dishonest behavior?
3. What concentration or participation risk exists?
4. What can the rule prove, and what can it not prove?

THEN ANSWER THESE QUESTIONS:

» Which rule depends most directly on one trusted decision-maker?
» Which rule makes repeated computational effort the scarce resource?
» Which rule makes committed value and penalties the scarce resource?
» How might power become concentrated under each rule?
» Why would none of the three rules prove how many books actually arrived?
» What additional evidence would the record keepers need?

Important limitation of the simulation: Real consensus mechanisms use software, cryptography, network messages, precise validity rules, proposer selection, chain-choice procedures, and incentives. Proof of work is not simply any difficult puzzle, and proof of stake is not simply a majority vote among people holding points. This activity compares broad resource and decision tradeoffs only.

KNOWLEDGE CHECK

MULTIPLE CHOICE

1. Which statement best describes a blockchain node?
   a. Every person who owns a digital asset
   b. A computer running network software that performs one or more blockchain functions
   c. Only the company that designed the blockchain
   d. A paper record that cannot communicate with other systems

2. What problem is a consensus mechanism designed to address?
    a. How distributed participants can agree on an accepted blockchain history
    b. How to guarantee that every outside statement is true
    c. How to eliminate all energy use and all concentration
    d. How to provide individualized investment advice
3. Which comparison is most accurate?
    a. Proof of work uses committed stake, while proof of stake uses only electricity.
    b. Proof of work uses computational effort, while proof of stake uses committed value and validator rules.
    c. Both systems require every node to be a professional miner.
    d. Both systems prove that outside records are accurate.

TRUE OR FALSE

» Every node on a blockchain network necessarily proposes blocks and participates directly as a miner or validator.

SHORT EXPLANATION

» In two or three sentences, explain why reaching consensus about a blockchain record does not prove that every outside fact in the record is true.

SUMMARY AND PRACTICAL TAKEAWAYS

» A node is a computer running blockchain network software, but nodes can perform different roles.
» Miners are block-producing participants in proof-of-work systems; validators perform defined roles in proof-of-stake or related systems.
» A consensus mechanism helps distributed participants evaluate blocks, select an accepted history, and manage disagreement.
» Proof of work makes computing power and energy central to block competition.
» Proof of stake makes committed value, validator selection, voting, rewards, and penalties central to its security model.
» Both approaches involve security, concentration, speed, energy, access, and governance tradeoffs.
» Consensus establishes agreement under network rules; it does not independently prove outside truth.

The practical skill is learning to ask who participates, what each participant verifies, how block producers are selected, how competing histories are resolved, and where power could become concentrated.

PROFILE JOURNAL ASSIGNMENT

Write one coherent journal entry of approximately 300–400 words. Do not submit a disconnected list of answers. Use the prompts below to organize a beginning, middle, and conclusion:

- Define a node and distinguish it from a miner or validator.
- Explain the problem a consensus mechanism is designed to address.
- Compare proof of work and proof of stake in your own words.
- Identify one strength and one tradeoff associated with each approach.
- Explain why consensus about a record does not prove every outside fact is true.
- Describe what would make you trust a shared system when no single participant controls the entire record.
- Connect this lesson to the critical-thinking, communication, or self-directed-learning skills you are developing.

Your response should demonstrate your reasoning. You are not being asked to operate a node, mine a block, stake an asset, create an account, open a wallet, purchase an asset, or conduct a transaction.

SUBMISSION REMINDER

Write your response on separate paper or in an approved institutional messaging system. Include your name or approved Profile identifier, Lesson 7: Nodes, Networks, and Consensus, and the date you completed the entry.

Use one of the established Prison Professors Profile methods, subject to your facility's rules:

1. Send it by institutional email to Playbook@PrisonProfessors.org. Suggested subject: Web3 Lesson 7 — [date completed].
2. Send it by postal mail to: Prison Professors, 1205 BMC Drive, Suite 706, Cedar Park, TX 78613.
3. Send it to an approved family member or supporter who can enter it on your Profile at PrisonProfessors.org.

Keep a copy when circumstances permit. Never include passwords, private keys, seed phrases, authentication codes, account numbers, real wallet addresses, or other sensitive credentials.