

# Lesson 3.2 Exercises: Consensus Mechanisms and Blockchain Architecture

## Module 3: The Trust Problem

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

## Exercise 1: Byzantine Generals and Real Networks

**Scenario:** A consortium of 7 central banks is building a shared settlement system. Intelligence reports suggest that up to 2 of the banks' IT systems may be compromised by state-sponsored hackers who could inject fraudulent settlement messages.

### Tasks:

- a) Using the BFT bound  $n > 3f$ , determine whether the system can tolerate 2 Byzantine nodes out of 7. Show your calculation.
- b) If the consortium grows to 10 banks, what is the maximum number of compromised nodes the system can tolerate?
- c) Explain in plain language why the  $\frac{1}{3}$  bound exists. Why can't a BFT system tolerate, say, 49% faulty nodes the way Proof of Work can tolerate up to 49% of hash power?
- d) A junior engineer proposes: "If we suspect Bank X is compromised, let's just remove them from the validator set." Evaluate this proposal — what are the benefits and risks?

*Difficulty: Introductory — tests understanding of BFT bounds and their practical meaning.*

## Exercise 2: Bitcoin Mining Profitability Analysis

**Scenario:** You are evaluating a Bitcoin mining investment. Use these parameters:

| Parameter             | Value                              |
|-----------------------|------------------------------------|
| Mining rig hash rate  | 100 TH/s (terahashes per second)   |
| Rig power consumption | 3,000 W                            |
| Electricity cost      | \$0.06 per kWh                     |
| Current block reward  | 3.125 BTC                          |
| Network hash rate     | 600 EH/s ( $6 \times 10^{20}$ H/s) |
| BTC price             | \$60,000                           |
| Blocks per day        | 144                                |

### Tasks:

- Calculate your rig's share of the total network hash rate.
- Calculate your expected daily BTC earnings (share  $\times$  total daily rewards).
- Calculate your daily electricity cost (power  $\times$  hours  $\times$  rate).
- Is the operation profitable? What BTC price would make it break-even?
- After the next halving (reward drops to 1.5625 BTC), recalculate. Is the operation still viable?

*Difficulty: Intermediate — requires arithmetic and economic reasoning.*

## Exercise 3: Simulating Difficulty Adjustment

**Scenario:** A new PoW blockchain targets 5-minute block times and adjusts difficulty every 100 blocks. Use the data below:

| Period | Actual Time for 100 Blocks | Difficulty |
|--------|----------------------------|------------|
| 1      | 500 min (on target)        | 1,000      |
| 2      | 400 min (too fast)         | ?          |
| 3      | ?                          | ?          |

### Tasks:

- Calculate the new difficulty for Period 2 using:  $\text{new} = \text{old} \times \frac{\text{target\_time}}{\text{actual\_time}}$ .
- With the Period 2 difficulty, the network produces 100 blocks in 600 minutes. Calculate the Period 3 difficulty.
- Plot the three difficulty values. Is the system converging toward the 5-minute target?
- What happens if 50% of miners suddenly leave the network (e.g., due to a government ban) before the next adjustment? How long would blocks take on average? How does this compare to Bitcoin's experience after China's 2021 ban?

*Difficulty: Intermediate — requires iterative calculation and critical analysis.*

## Exercise 4: Analyzing a Blockchain Fork

**Scenario:** At block height 500, two miners (A and B) simultaneously find valid blocks. The network splits:

- 55% of hash power builds on Miner A's block
- 45% of hash power builds on Miner B's block

Assume average block time is 10 minutes and the fork is resolved by the longest chain rule.

### Tasks:

- What is the probability that Miner A's chain is extended first (i.e., one of the 55% miners finds block 501 before a 45% miner does)?
- After 3 blocks are built on Miner A's chain and only 2 on Miner B's chain, what happens to the transactions that were in Miner B's blocks but not in Miner A's?
- A merchant accepted a 10 BTC payment in Miner B's block 500. After the fork resolves in favor of Miner A's chain, has the merchant been paid? What should the merchant have done differently?
- Calculate the probability that Miner B's chain catches up after falling behind by 1 block, 2 blocks, and 3 blocks. Use the formula  $P = (q/p)^k$  where  $p = 0.55$ ,  $q = 0.45$ ,  $k = \text{deficit}$ .

*Difficulty: Advanced — requires probability reasoning and understanding of fork mechanics.*

## Exercise 5: Comparing Attack Costs

**Scenario:** You are a security consultant comparing the cost of attacking two networks:

### Network X (PoW):

- Total hash rate: 500 EH/s
- Cost of hash power: \$0.05 per TH/s per day (rental)
- A 51% attack requires controlling  $\geq 250$  EH/s

### Network Y (PoS):

- Total staked: 30 million ETH at \$2,000/ETH
- A 34% attack requires controlling  $\geq 10.2$  million ETH

### Tasks:

- Calculate the daily cost of a 51% attack on Network X.
- Calculate the capital required to acquire 34% of Network Y's stake on the open market. Why would the actual cost be even higher than this calculation suggests?
- Compare the two attack costs. Which network is more expensive to attack?
- In Network Y, after a successful attack, the attacker's stake is slashed. What is the attacker's total loss? Does PoW have an equivalent "slashing" mechanism?

*Difficulty: Advanced — requires quantitative security analysis across paradigms.*

## Exercise 6: Designing for the Trilemma

**Scenario:** Three blockchain projects approach you for advice. Each has a specific priority and asks how to configure their system:

- 1 **Project A — Global remittance platform:** Must handle 10,000 TPS with sub-5-second finality. Willing to sacrifice decentralization.
- 2 **Project B — Censorship-resistant digital gold:** Maximum decentralization and security. Throughput is secondary.
- 3 **Project C — Government digital identity system:** Must be highly secure and scalable, but can be centrally managed.

### Tasks:

- a For each project, identify which two trilemma properties are prioritized and which is sacrificed.
- b Recommend a specific consensus mechanism for each project. Justify your choice.
- c For Project A, the team later demands “but we also want full decentralization.” Explain why this is infeasible with current technology and propose a Layer 2 compromise.
- d Draw a trilemma triangle and plot all three projects on it, showing their position.

*Difficulty: Advanced — requires synthesis of trilemma trade-offs and mechanism selection.*

## Exercise 7: Evaluating a DeFi Protocol's Consensus Choice

**Scenario:** A DeFi lending protocol operates on three different blockchains and must choose which to prioritize:

|            | Chain P (PoW) | Chain Q (PoS) | Chain R (BFT) |
|------------|---------------|---------------|---------------|
| Finality   | ~60 min       | ~13 min       | ~3 sec        |
| TPS        | 7             | 30            | 5,000         |
| Validators | 10,000+       | 800,000+      | 21            |
| Gas fees   | \$15–\$50     | \$0.50–\$5    | \$0.001       |

### Tasks:

- a. For a **liquidation engine** that must execute within seconds to prevent bad debt, which chain is best? Justify.
- b. For a **long-term savings vault** where security matters most and speed is irrelevant, which chain is best?
- c. Chain R has only 21 validators. A competitor bribes 8 of them. What attack is now possible? Would this attack be feasible on Chain Q?
- d. The protocol decides to deploy on all three chains. Propose a strategy that uses each chain's strengths (e.g., liquidations on R, long-term storage on P). Justify.

*Difficulty: Advanced — requires multi-criteria evaluation and practical system design.*

## Exercise 8: Design a Cross-Border Payment Network

**Scenario:** The Central Bank of Euroland commissions you to design a blockchain-based cross-border payment system connecting 50 banks across 20 countries. Requirements:

- Finality within 10 seconds (irreversible settlements)
- Throughput: 500 transactions per second at peak
- Must tolerate up to 5 compromised banks
- Full auditability by regulators
- No single country should control the network

### Tasks:

- a) Select a consensus mechanism. Justify why PoW, PoS, or BFT is most appropriate. Verify that the BFT bound  $n > 3f$  is satisfied.
- b) Design the validator set: how many validators, how are they selected, what are the hardware requirements?
- c) Define the finality rule: when exactly is a transaction considered settled?
- d) Describe what happens when 6 banks (exceeding the tolerance threshold) go offline during a network partition. How does the system recover?
- e) Identify two risks that your consensus choice introduces and propose mitigations.

*Difficulty: Advanced–Integrative — combines all lesson concepts in a complete system design.*