Okay, here are 2 scenario-based questions for each week, covering the most important points from an exam perspective:

Week 1: The Model of Decentralization

1. **Scenario:** A company wants to improve transparency and reduce fraud in its supply chain. Currently, tracking goods involves multiple intermediaries, each with their own records, leading to inefficiencies and potential for tampering.
    - **Question:** How can blockchain technology be applied to this supply chain to address these issues? Explain the specific benefits of decentralization, immutability, and transparency in this context.
2. **Scenario:** A local community wants to create a digital platform for residents to vote on local issues and manage community funds. They need a system that is secure, transparent, and prevents any single entity from controlling the process.
    - **Question:** How can a blockchain-based solution help this community achieve its goals? Discuss the advantages of using a distributed ledger and the role of consensus mechanisms in ensuring trust and security.

Week 2: Basic Cryptographic Primitives

1. **Scenario:** A company wants to secure its online communication and ensure that sensitive documents are only accessible to the intended recipients. They are considering using both symmetric and asymmetric encryption.
    - **Question:** Explain how symmetric and asymmetric cryptography can be used in conjunction to achieve both efficiency and security in this scenario. Specifically, address how they can secure key exchange and document encryption.
2. **Scenario:** A software company wants to distribute software updates to its users, ensuring that the updates are authentic and have not been tampered with.
    - **Question:** How can digital signatures be used to verify the authenticity and integrity of these software updates? Explain the process and the security benefits.

Week 3: Bitcoin

1. **Scenario:** A business is considering accepting Bitcoin as a payment method. They are concerned about the irreversibility of Bitcoin transactions and the potential for fraud.
    - **Question:** Explain how Bitcoin transactions are verified and added to the blockchain. Discuss the measures that can be taken to mitigate the risks associated with irreversible transactions and potential fraud.
2. **Scenario:** A developer wants to create a smart contract on the Bitcoin network

with specific conditions for fund release.
    - **Question:** How can Bitcoin Script be used to define the conditions for this smart contract? What are the limitations of Bitcoin Script in implementing complex smart contract logic?

Week 4: Attacks on Bitcoin

1. **Scenario:** A new cryptocurrency exchange is handling a high volume of Bitcoin transactions. They are concerned about the possibility of double-spending attacks by malicious users.
    - **Question:** Explain how a double-spending attack works in the context of Bitcoin transactions. What measures can the exchange implement to detect and prevent such attacks?
2. **Scenario:** A group of miners is suspected of attempting to gain control of a significant portion of the Bitcoin network's mining power.
    - **Question:** Describe the 51% attack and its potential consequences for the Bitcoin network. What are the long-term implications of such an attack on the trust and security of the cryptocurrency?

Week 5: Beyond PoW

1. **Scenario:** An organization wants to implement a blockchain-based supply chain tracking system but is concerned about the high energy consumption associated with Proof of Work (PoW).
    - **Question:** Compare and contrast Proof of Work (PoW) with Proof of Stake (PoS) in terms of energy consumption and scalability. How can PoS or other consensus mechanisms address the organization's concerns?
2. **Scenario:** A developer is tasked with creating a decentralized application (dApp) that automates the terms of a financial agreement between two parties.
    - **Question:** Explain how smart contracts can be used to implement this agreement. What are the key steps involved in writing, deploying, and executing the smart contract?

Week 6: Consensus for Permissioned Models

1. **Scenario:** A consortium of banks wants to use blockchain technology to streamline interbank transactions. They require a system where all participants are known and authenticated.
    - **Question:** Explain why a permissioned blockchain is more suitable for this scenario than a public blockchain. How does a Membership Service Provider (MSP) contribute to the security and efficiency of the network?
2. **Scenario:** A distributed system needs to maintain a consistent state across multiple nodes, even in the presence of node failures.

- **Question:** Explain the concept of State Machine Replication. How do consensus algorithms ensure that all nodes in the system agree on the sequence of state transitions?

Week 7: Byzantine Agreement Protocols

1. **Scenario:** An aviation company wants to implement a distributed system for controlling unmanned aerial vehicles (UAVs). The system must be highly reliable and fault-tolerant, even if some UAVs provide incorrect or conflicting data.
   - **Question:** Why is Byzantine Fault Tolerance (BFT) important in this scenario? Explain how the Practical Byzantine Fault Tolerance (PBFT) algorithm can be used to ensure consensus and prevent a single faulty UAV from disrupting the system.
2. **Scenario:** A company wants to implement a distributed database with strong consistency guarantees. They need to ensure that all replicas of the database remain consistent, even if some servers crash or become unresponsive.
   - **Question:** How does the PBFT algorithm ensure both safety and liveness in a distributed database system? Explain the roles of the different phases (PRE-PREPARE, PREPARE, COMMIT) in achieving consensus.

Week 8: Scalability Solutions

1. **Scenario:** A decentralized application (dApp) is experiencing slow transaction speeds and high fees due to the limited throughput of the underlying blockchain.
   - **Question:** How can sharding, as implemented in Zilliqa, help to improve the scalability of the blockchain and address these performance issues? Explain the concept of network sharding and its benefits.
2. **Scenario:** A financial institution wants to use blockchain technology to process a high volume of cross-border payments. They need a solution that can provide fast transaction confirmation times and high throughput.
   - **Question:** How does the Bitcoin-NG protocol improve upon the original Bitcoin protocol in terms of transaction throughput? Explain the roles of key blocks and microblocks in achieving faster transaction processing.

Week 9: Blockchain Interoperability

1. **Scenario:** A company uses a permissioned blockchain for its supply chain management and wants to share data with another company that uses a different permissioned blockchain.
   - **Question:** Explain the challenges of interoperability between permissioned blockchains. How can Verifiable Data Transfer be used to enable secure and trusted data sharing between these two companies?
2. **Scenario:** A user has assets on two different blockchain networks (e.g., Bitcoin

and Ethereum) and wants to exchange them directly without using a centralized exchange.
    - **Question:** Describe the concept of an atomic swap. How do Hashed Timelock Contracts (HTLCs) ensure that the exchange is executed in a trustless manner, preventing either party from cheating?

Week 10: Hyperledger Indy

1. **Scenario:** A university wants to issue digital transcripts to its students that can be easily verified by employers and other institutions.
    - **Question:** How can Hyperledger Indy be used to create and manage these verifiable credentials? Explain the roles of Decentralized Identifiers (DIDs) and verifiable presentations in this process.
2. **Scenario:** A government agency wants to create a secure and privacy-preserving system for citizens to manage their digital identities and access various online services.
    - **Question:** What are the key features of Hyperledger Indy that make it suitable for this scenario? Discuss the roles of Stewards and Trust Anchors in the Indy network and how they contribute to identity management.

Week 11: Blockchain Security

1. **Scenario:** A blockchain network is experiencing a significant increase in transaction delays. It is suspected that a malicious entity is attempting to disrupt the network by controlling a large portion of the network's resources.
    - **Question:** Describe the 51% attack and how it can be used to disrupt a blockchain network. What measures can be taken to mitigate the risk of such an attack and protect the network's integrity?
2. **Scenario:** A decentralized exchange (DEX) is experiencing a series of suspicious transactions where some users are able to exploit the timing of transactions to their advantage.
    - **Question:** Explain how front-running attacks can occur on a DEX. What are the potential consequences of these attacks, and what countermeasures can be implemented to prevent them?

Week 12: Use Cases

1. **Scenario:** A company is considering using blockchain technology to manage its intellectual property (IP) and ensure that ownership and licensing agreements are transparent and immutable.
    - **Question:** How can blockchain technology be applied to manage intellectual property rights? What are the potential benefits in terms of reducing disputes, streamlining licensing, and improving transparency?

2. **Scenario:** A group of cloud service providers wants to create a federated system where they can share resources and allocate them to customers in a fair and transparent manner.
    - **Question:** How can blockchain technology be used to implement a fair scheduling algorithm for resource allocation in this cloud federation scenario? What are the advantages of using a distributed ledger to manage resource allocation and track usage?