In a study group, Ramsha mentions that the term "contract" in smart contracts implies something legally binding. Sabeen corrects her by saying that in this context, the term "contract":

A. Has a specific legal meaning.
B. Implies a legally binding agreement.
C. Has no legal meaning.
D. Refers to an employment agreement.

In a blockchain class, Taha explains to Murtaza that smart contracts are deterministic. To clarify, he says this means:

A. The contract can determine legal outcomes.
B. The execution outcome is the same for everyone who runs it, given the same context and state.
C. The execution outcome is random each time it runs.
D. The contract determines the best possible outcome for users.

According to Zaema, "Smart contracts on Ethereum run in parallel like multi-threaded programs."

A. True
B. False

During a lecture, Miss Urooj asks which blockchain platform is specifically associated with the state of smart contracts. Raheel quickly responds with:

A. Ethereum
B. Bitcoin
C. Ripple
D. Litecoin

Aosaf and Zain are preparing for a finals. Aosaf asks what characteristic of smart contracts ensures that once a contract is deployed, its code cannot be altered Zain correctly answers:

A. Flexibility
B. Immutability
C. Programmability
D. Scalability

During a lecture,Miss Urooj explains how smart contracts operate on Ethereum. Abdullah is asked to summarize the key points. Abdullah says, "Smart contracts on Ethereum execute only when triggered by a transaction and cannot run in the background."

A. True
B. False

In a decentralized application (DApp) development group, Ahmad is puzzled about the aftermath of a failed transaction on the Ethereum network. He seeks input from Saad. Ahmad asks, "What is the status of a failed transaction on Ethereum?"

A. It is recorded as unsuccessful and disregarded.
B. Its effects are preserved, but the transaction is marked as failed.
C. It is recorded as attempted, and the effects are rolled back.
D. The gas spent on the transaction is refunded.

Usman is developing a smart contract to store user data that must persist between transactions. Which type of variable should Usman use to store this data permanently?

A. Local Variables
B. State Variables
C. Global Variables
D. Temporary Variables

Alina is learning about global variables in Solidity and needs to identify which one does not belong to this category. Which of the following is NOT an example of a global variable in Solidity?

A. block.number
B. msg.sender
C. tx.gasprice
D. uint storageVar

Ramish is unsure about the scope and lifetime of variables declared within functions. What would be the scope and lifetime of a variable declared within a function in Solidity according to you?

A. Global scope and permanent lifetime.
B. Local scope and permanent lifetime.
C. Local scope and temporary lifetime.
D. Global scope and temporary lifetime.

What did you do when you felt sleepy during the blockchain class?

A. Took a quick nap
B. Tried to count how many blocks were in the blockchain
C. Dreamed about becoming a blockchain millionaire
D. Imagined mining cryptocurrencies in your dreams

Mahad and Waleed are miners and are paid for their work validating transactions and adding blocks to the Ethereum blockchain in fractions of ether (ETH). These fractional units are called gwei, and comprise the gas price for the transaction.

A. True
B. False

During a blockchain class, Mizrab asks about the different places where Solidity stores data. Which place is used for storing local simple variable values defined in functions?

A. Memory
B. Storage
C. Cache
D. Stack

Shayan said to Naik that an orphan block is only created when 51% attack is successful.

A. True
B. False

Maliha is developing a decentralized application (DApp) and needs to store key-value pairs efficiently. Which data type should she use?

A. uint
B. string
C. mapping
D. array

During a discussion on Ethereum's address data type, Noor asks about its size. What is the size of an Ethereum address?

A. 20 bytes
B. 32 bytes
C. 64 bytes
D. 40 bytes

```
pragma solidity ^0.8.0;

contract Lottery {
    address public manager;
    address[] public players;

    constructor() {
        manager = msg.sender;
    }

    function enter() public payable {
        require(msg.value > 0.01 ether);

        players.push(msg.sender);
    }

    function random() private view returns (uint) {
                        return    uint(keccak256(abi.encodePacked(block.difficulty,    block.timestamp,
players.length)));
    }

    function pickWinner() public restricted {
        require(players.length > 0, "No players in the lottery");

        uint index = random() % players.length;
        payable(players[index]).transfer(address(this).balance);

        players = new address ; // Resetting the players array
    }

   modifier restricted() {
            require(msg.sender == manager, "Unauthorized access. Only authorized personnel can
call this function.");
        _;
    }

    function getPlayers() public view returns (address[] memory) {
        return players;
    }
}
```

Consider the given smart contract in which two friends, Faizan and Mujeeb decided to organize a fun lottery game using a smart contract called Lottery. Answer the MCQs 16-20 considering this contract.

What is the minimum amount of ether required for a participant to enter the lottery?

A. 0.001 ether
B. 0.01 ether
C. 0.1 ether
D. 1 ether

In the Lottery contract, what happens if the pickWinner() function is called when there are no players in the lottery?

A. The contract self-destructs
B. The manager becomes the winner
C. An error is thrown, and the function reverts
D. The contract transfers its balance to a predefined address

Which of the following statements regarding the restricted modifier is true?

A. It restricts access to the pickWinner() function based on the number of participants.
B. It restricts access to the random() function based on the current block timestamp.
C. It restricts access to the getPlayers() function to only non-participants.
D. It restricts access to the enter() function to only the manager.

What does the keccak256(abi.encodePacked(block.difficulty, block.timestamp, players.length)) expression in the random() function of the Lottery contract do?

A. It generates a random number based on the current block's timestamp, difficulty, and the number of players.
B. It calculates the average number of participants in the lottery based on the current block's timestamp, difficulty, and the number of players.
C. It selects a winner based on the number of participants based on the current block's timestamp, difficulty, and the number of players.
D. It computes the total gas consumed by the contract based on the current block's timestamp, difficulty, and the number of players.

What is the purpose of declaring the getPlayers() function as public view in the Lottery contract?

A. It allows external parties to modify the state of the contract.
B. It prevents external parties from accessing the list of players.
C. It enables external parties to retrieve data from the contract without modifying its state.
D. It restricts access to the function only to the contract owner.

In a decentralized file storage system, Shahbano uses Merkle trees for efficient data verification. Which of the following accurately describes the role of Merkle trees in this scenario?

A. They optimize data packet routing across the network.
B. They provide direct access to individual files.
C. They maintain the sequential ordering of data blocks.
D. They ensure quick and secure verification of large datasets.

Zyena and Eesha are racing against the clock to create efficient smart contracts. They're strategizing ways to minimize gas costs for function calls, aiming for maximum performance and cost-effectiveness. Which practice should they avoid to achieve this?

A. Utilizing extensive event logging
B. Making frequent calls to external contracts
C. Using dynamic data structures like mappings
D. Implementing complex mathematical calculations

Suleman needs to accurately estimate gas costs for executing methods of a smart contract and decides to use a specific function. Which function did Suleman use to estimate gas costs?

A. web3.eth.estimateGas()
B. instance.myFunction.estimateGas()
C. contract.methods.myFunction.estimateGas()
D. web3.eth.getTransactionReceipt()

In a blockchain development environment, Ali is exploring built-in functions for contract operations. Which built-in function should Ali use if he wants to delete the current contract and send any remaining ether to a specified recipient address?

A. selfdestruct(recipient_address)
B. selfdestruct(recipient)
C. selfdestruct(address payable recipient_address)
D. selfdestruct(address receiver)

When the blockchain lecture ran longer than expected, what did you and your friend do to stay awake?

A. Played a quiet game of tic-tac-toe on a piece of paper
B. Whispered jokes to each other to stay alert
C. Took turns drawing funny doodles in each other's notebooks
D. What kind of MCQ is this? I'll complain to Dr. Hammad!

In a blockchain development scenario, Muqeem is considering constructors for his smart contract design. Muqeem wants to clarify the limitation regarding constructors in Solidity. Which statement accurately reflects the situation?

A. Muqeem can use multiple constructors in his contract to handle different scenarios.
B. Only one constructor is allowed in a contract, as overloading is not supported.
C. Muqeem can work around the constructor limitation by using function overloading.
D. Muqeem can deploy separate contracts for different initialization scenarios.

Human said to Zukhraf that In blockchain technology, a hard fork is a change to the software protocol where only previously valid transaction blocks are made invalid. Because old nodes will recognize the new blocks as valid, a hard fork is backwards-compatible.

A. True
B. False

Nouman asked Youneeb, "What is the term applied for splits in a blockchain network?" Youneeb responds with:

A. Mergers
B. Divisions
C. Forks
D. None of the above

Bitcoin central server is located in?

A. Washington DC
B. Undisclosed location
C. London
D. None of the above

In a decentralized application (DApp) ecosystem, Dayyan has deployed a smart contract to manage token transfers. Another user, Saifullah, wants to create a new DApp that interacts with Dayyan's contract. What is the possibility of Alice's DApp invoking Dayyan's contract?

A. Yes, it's possible; smart contracts can be invoked by other contracts.
B. No, it's not possible; smart contracts can only be invoked by external users.
C. None of the above.

In Ethereum, Noor and Maliha are miners, they create competing blocks simultaneously, resulting in orphan blocks. What happens to the miner who created the orphan block?

A. I am not sure, needs no points for this one
B. Yes

C. No
D. None of the above

Umais wants to delete items from the array. Can the items of a Solidity array be deleted?

A. Unfortunately no, this is the limitation of blockchain.
B. No, this is the beauty of blockchain.
C. Yes, a new contract needs to be deployed.
D. None of the above.

Why is the contract used to donate ethers (such as the one used for Ganache) named as a 'faucet'?

A. It dispenses ethers for testing.
B. It controls ether flow.
C. It regulates ether usage.
D. None of the above

Haider is handling errors in Solidity smart contracts, which function he will use to evaluate a condition and stop execution with an error if the condition is false?

A. assert, used when the outcome is expected to be true.
B. require, used when testing inputs like function arguments.
C. revert, used to specify a custom error message.
D. None of the above.

Najmus is creating a fundraising smart contract. To receive ethers, what approach should be implemented?

A. Donators pay ethers to Najmus's personal wallet.
B. Najmus manually transfers ethers to the contract.
C. The contract includes a payable function.
D. Donators transfer ethers directly to the contract's address.

Haris is setting up a local blockchain development environment using Ganache. What is the default port used by Ganache for local blockchain development?

A. 7544
B. 7545
C. 7546
D. 7547

How is resiliency defined in the context of DApps?

A. Continuous availability ensured by high transaction fees.
B. Downtime prevention through regular maintenance windows.
C. No downtime, available as long as the blockchain network is operational.
D. Availability limited by dependence on centralized servers.

Mohid is developing a cross-platform application and considering using ReactJS and React Native. Which statement best describes the relationship between ReactJS and React Native?

A. ReactJS for web, React Native for mobile.
B. React Native for web, ReactJS for mobile.
C. Both for web applications.
D. ReactJS for components, React Native for mobile.

What is the default port number where the CLI version typically listens at?

A. 6545
B. 7545
C. 8545
D. 9545

Umer is exploring the Ganache interface and notices a key icon. What does this key icon represent?

A. Private key
B. Public key
C. Blockchain encryption key
D. Transaction key

Ahmad is writing tests for his smart contracts using Truffle. Which file is used to configure network settings in a Truffle project?

A. config.js
B. truffle-network.js
C. truffle-config.js
D. truffle-settings.js

During the blockchain class, what did Sabeen do when she couldn't understand a complex concept?

A. Asked a thoughtful question to clarify
B. Nodded along, pretending to understand
C. Searched for memes related to blockchain

D. Imagined explaining it to herself

In the context of the following constructor in a Solidity smart contract, what does the **this** keyword refer to?

```
constructor() {
   owner = msg.sender;
   donutBalances[address(this)] = 100;
}
```

A. The Ethereum address of the contract itself
B. The address of the owner of the contract
C. The address of the person deploying the contract
D. The address of the most recent sender

During a Solidity lecture, Hamza is learning about contract inheritance. He wants to clarify a point about Solidity's contract inheritance feature. Which statement best addresses his query?

A. Solidity does not support contract inheritance.
B. Inheritance can only occur from a single parent contract.
C. Solidity allows for single-level and multiple-level inheritance using the **'is'** keyword.
D. Inheritance in Solidity can only be achieved by importing external libraries.

In the provided Solidity code snippet, what modification should be made by Huzaifa to the onlyOwner modifier to correct the error introduced

```
modifier onlyOwner {
   require(msg.sender == owner);
 }
```

A. Add an underscore (_) at the end of the modifier.
B. Remove the require statement from the modifier.
C. Change msg.sender == owner to msg.sender != owner.
D. Add a semicolon (;) after the require statement.

During class, Ammar is confused about function visibility in smart contracts. He encounters a function marked as **internal** and wonders about its accessibility. What explanation would best clarify the situation for him?

A. It can be called by other contracts or externally owned accounts (EOA) transactions.
B. It is only accessible from within the contract and can be called by derived contracts.
C. It is like internal functions but cannot be called by derived contracts.
D. It cannot be called from within the contract unless explicitly prefixed with the keyword this.

What is a characteristic of the receive function in Solidity?

A. It can have arguments but cannot return anything.
B. It cannot have arguments or return anything.
C. It can have arguments and return values.
D. It must be marked as external to be callable.

What happens if a contract written by Aizaz receives ether but doesn't have a receive Ether function defined?

A. Reverts the transaction.
B. Transfers the ether to the contract creator.
C. Discards the received ether.
D. Executes its fallback function if one is defined.

For permissioned blockchains, which consensus algorithm(s) are typically designed?

A. Proof of Work (PoW)
B. Proof of Stake (PoS)
C. Practical Byzantine Fault Tolerance (PBFT)
D. Delegated Proof of Stake (DPoS)

Moonis is exploring blockchain technology and asks for a concise definition. Which option best describes blockchain?

A. A centralized transactional state machine.
B. A transactional decentralized state machine.
C. A centralized data storage system.
D. A decentralized data storage system.

Which of the following keys are required for generating a signature?

A. Public key
B. Private key
C. Both public and private
D. None of the above

Abdul Musawir is studying Bitcoin's scripting language and its characteristics. Which statement best describes Bitcoin's scripting language?

A. It was inspired by Python programming language.
B. It is designed to be complex and versatile.

C. It is inspired by Forth and built specifically for Bitcoin.
D. It allows for extensive looping and iteration.

Shaheer is studying the halting problem in computer science. What does it entail?

A. Determining if a program will terminate or run indefinitely.
B. Finding the fastest algorithm to solve a computational problem.
C. Identifying errors in a program's code during debugging.
D. Predicting the output of a program based on its input.

In lecture 12 **"Introduction to Ethereum"**, you learned about Ethereum's gas mechanism. What best describes its purpose and function

A. It allows smart contracts to execute without any limits.
B. It accounts for the cost of each instruction executed in a smart contract.
C. It determines the amount of Ethereum needed to deploy a smart contract.
D. It restricts the number of transactions that can be included in a block.

What term is used to describe the process of acquiring cryptocurrency before it is made available to the public?

A. Post-mining
B. Pre-mining
C. Early-mining
D. Advanced-mining

Hammad is exploring different types of wallet software for managing cryptocurrencies. What is a key benefit of using a separate address/key for each coin in wallet software?

A. It improves transaction speed.
B. It enhances security against cyberattacks.
C. It benefits privacy, making it appear as if each coin has a separate owner.
D. It reduces transaction fees.

Sheraz wants to personalize his cryptocurrency address to include the alphanumeric sequence **'20I-0965'**. Which type of address would Sheraz generate to achieve this?

A. Standard address
B. Vanity address
C. Green address
D. Exchange address

What best describes hot storage in cryptocurrency?

A. Convenient and risky
B. Offline and safe
C. Ideal for long-term storage
D. Involves separate keys

Shahbaz is exploring solutions for using a new address (and key) for each coin sent to cold storage, even when the cold wallet is offline. What solution is suggested in the lecture?
Hint: I ask this in quiz as well if you remember :D

A. Generate a batch of addresses/keys for the hot wallet beforehand.
B. Keep the cold wallet online to synchronize with the hot wallet.
C. Use a hierarchical wallet system.
D. Manually generate new addresses for each transaction.

How do you feel when you see 80 MCQs waiting for you on a Blockchain exam paper?

A. Slightly nervous, but up for the challenge.
B. Overwhelmed, but determined to do your best.
C. Instant regret for not studying more.
D. I don't have feelings, I have multiple-choice questions!

Khuzaima is considering using an online wallet for his cryptocurrency. Which description best fits an online wallet?

A. Like a local wallet but stored on a USB drive.
B. Similar to a physical wallet but with virtual coins.
C. Functions in the cloud and runs in your browser.
D. Stored on a hardware device for added security.

What port does the Bitcoin P2P network typically run on?

A. TCP port 80
B. TCP port 443
C. TCP port 8333
D. UDP port 123

Asad is studying the Bitcoin P2P network and its topology. What best represents the topology of the Bitcoin P2P network?

A. Hierarchical
B. Centralized
C. Random
D. Star

In the Bitcoin P2P network, how are all nodes treated?

A. Nodes with higher computational power are given priority.
B. Nodes are ranked based on geographic location.
C. All nodes are considered equal.
D. Nodes are classified based on their transaction history.

Hissam is studying the dynamics of the Bitcoin P2P network. How frequently are non-responding nodes forgotten in the Bitcoin P2P network?

A. 1 hour
B. 2 hours
C. 3 hours
D. 4 hours

When can new nodes join the Bitcoin P2P network?

A. At any time
B. Only during specific time windows
C. Only when approved by existing nodes
D. Only after passing a security check

Zaid is learning about race conditions in blockchain transactions. What is the default behavior when transactions or blocks conflict?

A. Accept the transaction or block with the highest transaction fee.
B. Accept the transaction or block that arrives first.
C. Accept the transaction or block with the most recent timestamp.
D. Reject all conflicting transactions or blocks.

Is it possible to purchase gas using an Ethereum exchange in Pakistan?

A. Yes
B. No

How many satoshis are there in one bitcoin?

A. 1 million
B. 10 million
C. 100 million
D. 1 billion

Ahsan is studying the average block creation time in a blockchain network. What is the average creation time per block in a network?

A. 5 minutes
B. 10 minutes
C. 15 minutes
D. 20 minutes

If Umair successfully mined a block on the Bitcoin network, how much reward will he get?

A. 6.25 BTC
B. 12.5 BTC
C. 25 BTC
D. 50 BTC

What is the term for when the blockchain splits?

A. Hard Fork
B. Soft Fork
C. All of the above
D. A spoon

Raheel and Zyena are discussing the reasons why people consider Bitcoin and blockchain technology more trustworthy than traditional currencies and contracts. Which of the following is NOT a common reason?

A. Transparency and immutability of transaction records.
B. Decentralization and lack of a central authority.
C. Guaranteed high value and price stability.
D. Enhanced security through cryptographic techniques.

Taha suggested that Bitcoin is like gold, while Murtaza says that Ethereum is like oil. In this context, which statement is true?

A. Bitcoin is valuable due to its limited supply, similar to gold.
B. Ethereum is valuable because it fuels decentralized applications, similar to how oil fuels engines.
C. Both statements are true.
D. Neither statement is true.

Nouman is explaining how a block size decrease can be implemented in a blockchain network. Which method would allow this change without requiring all nodes to upgrade?

A. Hard-forking
B. Soft-forking
C. No-forking

D. Chain-splitting

Centralization in public blockchain is often undesirable. How does Bitcoin address this aspect?

A. Bitcoin is not a true public blockchain; no one knows who Satoshi is.
B. Rewarding orphan blocks can make Bitcoin somewhat better in this regard but not much.
C. All of the above
D. None of the above

Why does Bitcoin not use the concept of gas?

A. Because gas is a complex concept that only Ethereum users understand.
B. Because Bitcoin transactions do not require computational resources to execute.
C. Because gas fees are not efficient for managing transaction fees in Bitcoin.
D. Because Bitcoin operates on a different blockchain protocol compared to Ethereum.

Proof-of-Elapsed-Time (PoET) relies on trusted code provided by which technology?

A. Intel Software Guard Extensions (SGX)
B. Advanced Encryption Standard (AES)
C. Secure Hash Algorithm (SHA)
D. Rivest–Shamir–Adleman (RSA)

Congratulations on reaching the 80th mcq 🙂 How do you feel after attempting 79 MCQs?

A. Ready for part B!
B. Kamal ka saffar tha.
C. Yeh toh hona hi tha
D. Aakhir kar, mission accomplished!

Question 1: **(25 Marks)**

Write a smart contract in solidity to manage the alumni network for batch 20 students who are expected to graduate from FAST-NUCES after the Spring 2024 semester. Below are the updated specifications you need to follow:

Contract Name: [2 Mark]

- AlumniNetwork

Variables to Declare: [2 x 4 = 8 Marks]

- **alumniList:** stores the addresses of alumni from batch 20
- **flexStatus:** to track the Flex status of each alumni (true if active, false if removed)
- **graduationDate:** to store the graduation date of each alumni
- **owner:** the contract owner address

Constructor: [2 Mark]

- Write a constructor to initialize the contract owner.

Modifier: [3 Mark]

Implement a modifier named **onlyOwner** to restrict access to certain functions to the contract owner only. Additionally, specify that only the contract owner **(Sir Amir)** can modify certain aspects of the contract.

Functions to Implement: [5 x 2 = 10 Marks]

- Implement a function named **addAlumni** to add alumni addresses and graduation dates to the network.

- Implement a function named **removeFromFlex** to mark alumni as removed from the Flex program after their graduation.

Instructions:

- Ensure that your Solidity code is clear, well-commented, and follows best practices for readability and maintainability.
- Use appropriate naming conventions for variables, functions, and modifiers.

Question 2: **(10 Marks)**

The smart contract, named FriendCounterBatch20, is designed to keep track of the number of friends each student of batch 20 has. It utilizes a mapping called friendCounts, which associates each student's address with an unsigned integer representing their friend count.
The contract provides three main functions:

addFriend: This function allows a student to increment their friend count by one. It takes the address of the student as an argument and increases their friend count in the friendCounts mapping.

removeFriend: This function enables a student to decrement their friend count by one, but it first checks if the student has any friends to remove. It prevents reducing the friend count below zero to ensure accuracy.

getFriendCount: This function allows anyone to query the friend count of a specific student by providing their address. It returns the current friend count associated with that address from the friendCounts mapping.

```
1  | pragma solidity ^0.8.0;
 2 |
 3 | contract FriendCounterBatch20 {
 4 |     mapping(address => uint250) friendCounts;
 5 |
 6 |     function addFriend(address _student) public {
 7 |         friendCounts[–student]++;
 8 |     }
 9 |
10 |     function removeFriend(address _student) public payable {
11 |         require(friendCounts[_student] < 0, "Student has no friends to remove");
12 |         friendCounts[_student]--;
13 |     }
14 |
15 |     function getFriendCount(address _student) public view {
16 |         return friendCounts[_student];
17 |     }
18 | }
```

Identify and correct the errors in the provided smart contract. Create a table on your answer sheet indicating the line number containing the error and the corrected line. Below is the header of the table for your reference.

Line No	Error	Corrected Line

Question 3: **(4 x 5 = 20 Marks)**

a. Sabeen and Ramsha both want to execute a smart contract simultaneously. What approach should they take? **[5 Marks]**

b. Taha has deployed a smart contract on the Ethereum blockchain and now wishes to delete it. How can he achieve this, and what happens after the deletion? **[5 Marks]**

c. Huzaifa, Umais and Moonis are working on a project together. They need to ensure compatibility with different versions of Ethereum. To manage this, they decide to follow Ethereum's versioning model. How is Ethereum's versioning model structured? **[5 Marks]**

d. How does censorship resistance help Mahad when using a decentralized application (DApp)? **[5 Marks]**