Strathmore
UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES
BACHELOR OF SCIENCE IN COMPUTER NETWORKS AND CYBER SECURITY
END OF SEMESTER EXAMINATION
CNS 4206 SPECIAL TOPICS IN SECURITY - BLOCKCHAIN TECHNOLOGY & APPLICATION

DATE: 2nd December 2024 Time: 08:00-10:00 Hours

Instructions

1. This examination consists of **FIVE** questions.
2. Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

QUESTION ONE [30 MARKS]

a) Define the following terms as used in blockchain technology: **(6 marks)**
   (i) Smart Contract
   (ii) Consensus Mechanism
   (iii) Gas Fee
   (iv) Fork
   (v) Mining Pool
   (vi) Double Spending

b) Explain three fundamental differences between permissioned and permissionless blockchains. **(6 marks)**

c) What are the key components of a blockchain block? Explain the role of each component. **(6 marks)**

d) Describe how the proof-of-work consensus mechanism ensures the security and immutability of the Bitcoin network. **(6 marks)**

e) A cryptocurrency exchange has been hacked. Using your knowledge of blockchain security:

(i) Describe three potential attack vectors that could have been exploited **(3 marks)**

(ii) Propose three security measures that could prevent such attacks **(3 marks)**

QUESTION TWO [15 MARKS]

a) Consider Ethereum's smart contract platform: **(9 marks)**

(i) Explain the concept of the Ethereum Virtual Machine (EVM)

(ii) Describe how gas pricing works

(iii) Discuss three common security vulnerabilities in smart contracts

b) Consider the following smart contract pattern. Identify its purpose, benefits, and potential risks: **(6 marks)**

```
contract Proxy {
    address public implementation;

    function upgrade(address newImplementation) public {
        implementation = newImplementation;
    }

    fallback() external payable {
        address impl = implementation;
        assembly {
            calldatacopy(0, 0, calldatasize())
            let result := delegatecall(gas(), impl, 0, calldatasize(), 0, 0)
            returndatacopy(0, 0, returndatasize())
            switch result
            case 0 { revert(0, returndatasize()) }
            default { return(0, returndatasize()) }
        }
    }
}
```

QUESTION THREE [15 MARKS]

a) In the context of blockchain scalability solutions: **(9 marks)**

(i) Explain the Lightning Network and its benefits

(ii) Describe how Layer 2 solutions work

(iii) Discuss the trade-offs between on-chain and off-chain scaling

b) Compare the following three blockchain platforms in terms of their smart contract capabilities and use cases: **(6 marks)**

(i) Tezos

(ii) Algorand

(iii) Solana

QUESTION FOUR [15 MARKS]

a) Check whether the following statements are True or False. Use the ID number to refer to a statement. If they are false, write also a correction to the solution box. Negating the statement is not accepted as a correct answer. **(8 marks)**

ID	Statement
1	There is no objectively correct number of highest unconfirmed transaction count in Bitcoin
2	Bitcoin requires a fork if transactions in the mempool are deleted after a certain time.
3	EVM refunds the spare gas of Ethereum transactions with too much gas provided.
4	Hyperledger Fabric (HLF) makes it possible to have private p2p connections within a ledger instance.
5	HLF requires at least two ordering nodes.
6	HLF makes use of the Order-Execute strategy to achieve higher throughput than otherwise possible.
7	ZK Rollups post more data on Ethereum than Optimistic Rollups for a 10,000 transaction batch.
8	Data consistency and availability are key challenges in implementing sharding.

b) Analyze the following aspects of Decentralized Identity Management: **(7 marks)**

(i) Self-Sovereign Identity principles

(ii) Verifiable Credentials

(iii) DID (Decentralized Identifier) resolution

(iv) Privacy considerations

QUESTION FIVE [15 MARKS]

Blockchain networks such as Ethereum are isolated from the external world. However, decentralized applications on them, such as financial services, require accurate price data. Oracles fill this gap by providing off-chain information to on-chain smart contracts. In this exercise, you are tasked with examining an Oracle service for feeding price data into Ethereum.

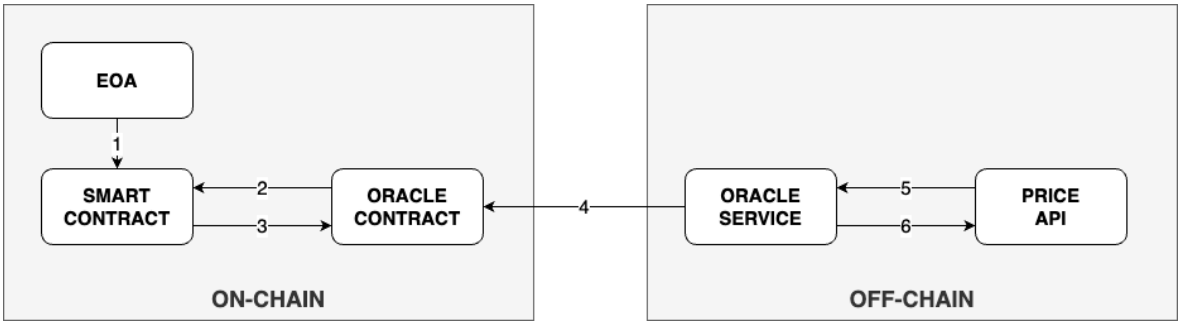

Figure 5.1: Oracle Architecture

In the initial design, the Oracle service updates the price data at every block, and every user call reads the latest available price. Figure 5.1 shows the overall architecture of this design. The calls are indexed, although they do not necessarily follow an order.

a) Of the two oracle designs we learned in the course, which one is this oracle service most similar to? (**1 mark**)

b) List the indexes of the *N* calls, which will directly incur an on-chain cost for the **Oracle service provider**. If you list more than necessary, only the first *N* answers will be considered. (**1 mark**)

c) List the indexes of the *N* calls, which are Ethereum **messages**. If you list more than necessary, only the first *N* answers will be considered. (2 marks)

d) Calculate the following metrics after the service is run for **10 minutes**. Assume the listed parameters:

- Ethereum Proof-of-Stake block time and EIP-1559 are active
- Gas Usage: 120,000
- Basefee: 30 Gwei (We consider the basefee constant for simplicity)
- Priority Fee: 1 Gwei

1. Cost per oracle service provider transaction:
2. Total burnt amount according to EIP-1559 rules: (**3 marks**)

Oracle service provider complains that the cost is too high and there is not enough demand for the service. Thus, they decide to update the price only after a user requests it and only if the last update is older than five blocks. Now, the user will see the last updated price until the new price is available. Further, the Oracle provider wants to track who makes the requests for auditing purposes. As simply checking the transactions included in the block is not efficient enough, they need to use another mechanism.

e) Answer the following questions regarding the new design: **(3 marks)**

   i. Which fundamental Solidity feature can the Oracle service provider utilize to track user requests?

   ii. Which keyword is needed to ensure the requester information can be efficiently searched off-chain?

   iii. Which Merkle-Patricia Trie (MPT) root from the Ethereum block header is specifically needed for this mechanism?

f) Briefly argue why user transactions spend more gas in the new design compared to the initial design. **(2 marks)**

   While this new design is more cost-effective for the Oracle provider, it may return a stale price for the users until the next update. To address this issue, the Oracle service provider implements a mechanism called *Honest Frontrunner*, which monitors the Ethereum public mempool and updates the price on the contract before the user request is executed.

g) How can the service provider ensure the Honest Frontrunner transaction gets executed before the user transaction **(2 marks)**