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: 15th December 2023 **Time: 10:30-12:30**

Instructions

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

QUESTION ONE [30 MARKS]

a) Provide an overview of blockchain systems and their significance in the field of technology. Explain the key technical features of blockchain systems that set them apart from traditional databases. (5 Marks)

b) Explain the properties and applications of cryptographic hash functions. Describe how they are used in blockchain technology to enhance security and integrity. (4 Marks)

c) Provide an overview of the upcoming blockchain technology, Algorand. Explain its key features and potential use cases. (5 Marks)

d) Discuss the concept of permissionless consensus in blockchain networks. Explain how Proof-of-Work (PoW) functions in the Bitcoin blockchain and the role of miners. (5 Marks)

e) Identify and discuss the risks, challenges, and limitations associated with blockchain technology. Provide examples of real-world issues that blockchain systems face. (5 Marks)

f) UTXOs are locked using Bitcoin script, making sure only the intended recipient gets to spend them. Probably the simplest type of script is pay-to-public-key (P2PK). Over time, this type has been replaced by an updated version.

i. What is the successor to P2PK transactions called? Also name one reason it is superior. (2 Marks)

ii. Apart from P2PK (and its successor) there are other well-known transaction types. Briefly describe one example. (2 Marks)

iii. Bitcoin has always had a scaling problem. To decrease transaction sizes and fit more transactions into each block, the Segregated Witness update (SegWit) was introduced in 2017. SegWit separates signature data from the transactions and appends it at the end of the block. Name the two types of scripts that are concatenated for a transaction verification. Also state which one of them is shortened by SegWit. (2 Marks)

QUESTION TWO [20 MARKS]

a) Describe the system architecture of the Ethereum blockchain. Explain the components of the Ethereum network and their functions. (6 Marks)

b) Discuss the Ethereum Virtual Machine (EVM) and its significance in the Ethereum ecosystem. Explain how it enables the execution of smart contracts. (6 Marks)

c) Explain the Solidity programming language used for developing smart contracts on the Ethereum platform. Discuss its syntax, data types, and design principles with an example. (4 Marks)

d) Illustrate the concept of Ethereum decentralized applications (dApps) with a focus on current standards and frameworks. Provide examples of specific use cases for Ethereum dApps. (4 Marks)

QUESTION THREE [20 MARKS]

a) Introduce the Tezos blockchain and its advanced infrastructure. Discuss the consensus mechanism used in Tezos and explain the concept of on-chain governance. (6 Marks)

b) Compare and contrast Tezos with other blockchain systems. (4 Marks)

c)

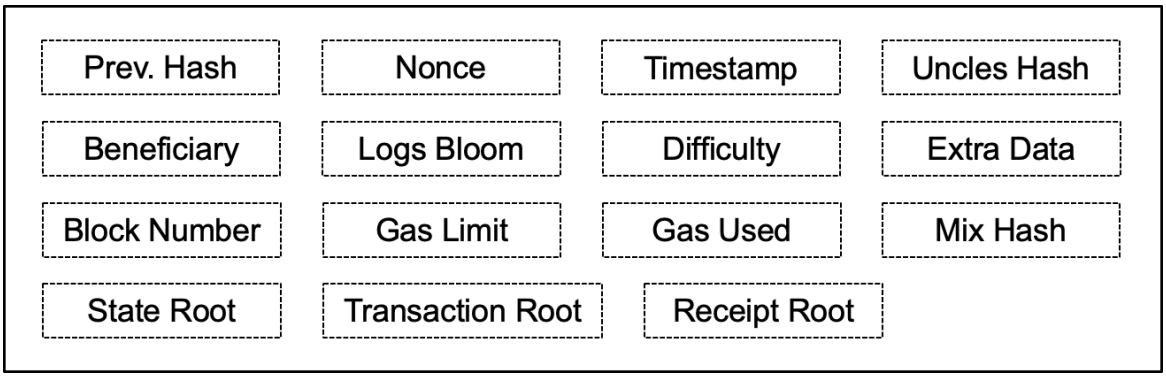

Figure 1.1: Top-Level View of a Proof-of-Work Ethereum Block Header

I. Figure 1.1 shows the top-level block header when Ethereum was still running Proof-of-Work. After "TheMerge", certain fields in the header became useless. Name two of these fields. **(2marks)**

II. Due to the advanced state structure, Ethereum can be considered more as a distributed state machinethan a simple distributed ledger. To maintain the state, Ethereum utilizes Merkle-Patricia Tries (MPT) and stores the roots of the MPTs on the block header. For each use case listed below, **list the set of MPT roots needed**. If you list more than the necessary number of roots, we will only consider your first *N* roots which match the solution size. **Note**: MPT roots are not limited to the ones listed in Figure 1.1. **(4 Marks)**

i. Calculating the transaction fee paid by a certain transaction

ii. Checking if any ERC-20 token was transferred (without going through the transactions)

iii. Checking Ether and ERC-20 token balances of an address

iv. Checking the liquidity available in an on-chain Automated Market Maker (AMM) pool

III. The London Hard Fork in 2021 relaxed the maximum Gas Limit field from 15M to 30M gas, while the target gas limit remained at 15M. This change was a part of the newly introduced transaction fee mechanism EIP-1559. Briefly explain how these values are relevant for EIP-1559. (4 marks)

QUESTION FOUR [20 MARKS]

a) Discuss alternative approaches to distributed ledger technologies in the enterprise space. (6 Marks)

b) Explain the key features and advantages of Hyperledger Fabric in the context of enterprise blockchain solutions. (6 Marks)

c) Analyze the role of blockchain technology in the Self-Sovereign Identity (SSI) and Decentralized Identity Management. Discuss the potential benefits of SSI and its challenges. (4 Marks)

d) Describe the concept of Decentralized Finance (DeFi) and its significance in the blockchain ecosystem. Provide examples of DeFi applications and platforms. (4 Marks)

QUESTION FIVE [20 MARKS]

a) Explain the concept of Automated Market Makers (AMM) in the context of decentralized exchanges and liquidity provision. Discuss their role in the DeFi ecosystem. (6 Marks)

b) Discuss the concept of Maximal Extractable Value (MEV) in blockchain networks. Explain how MEV can impact transactions and miners' behavior. (4 Marks)

c) Carrie has the following transaction which is included in the last confirmed block. Table 2.1 displays thedetails of this transaction and its input data (calldata).

Sender	Recipient	Nonce	Value	Gas Limit	Gas Used	Base Fee	Tip
0xaa22...	0xdd44...	51	0 ETH	500,000	420,550	18 Gwei	0.2 Gwei
Calldata							
[0]: 0x23B872DD							
[1]:	000000000000000000000000CC6295B8B5E9DAD2D3BA15EF4CD4C47A4C0AE2FA						
[2]:	000000000000000000000000BB8F95DBC639621DBAF48A472AE8FCE0F6F56A6E						
[3]:	0000000000000000000000000000000000000000000000000000000000000FF						

Table 2.1: Details of Carrie's Transaction

Function Signature	Keccak Hash
allowance(address owner, address spender)	dd62ed3e90e97b3d417db9c0c7522647811bafca5afc6694f143588d255fdfb4
approve(address spender, uint256 value)	095ea7b334ae44009aa867bfb386f5c3b4b443ac6f0ee573fa91c4608fbadfba
burn(address account, uint256 value)	9dc29fac0ba6d4fc521c69c2b0c636d612e3343bc39ed934429b8876b0d12cba
mint(address account, uint256 value)	16267c0d056579491157dd84f60a063a564dc2160bb7ebeb4396e7481bc609ea
transfer(address to, uint256 value)	a9059cbb2ab09eb219583f4a59a5d0623ade346d962bcd4e46b11da047c9049b
transferFrom(address from, address to, uint256 value)	23b872dd7302113369cda2901243429419bec145408fa8b352b3dd92b66c680b
update(address from, address to, uint256 value)	8ce516dafdf7e6222dd04731d0a2cd3b2d9f3c9c62b3bf2c97db3b87615b98b8

Table 2.2: Function Signature Lookup Table

i. Use the provided function signature lookup table to decode the calldata of Carrie's transaction in Table Specify the function signature and arguments with their value. Note: Hex bytes you skip are assumed to be 0. The least significant byte is the right-most one. (3 marks)

ii. Carrie's transaction is executing a call to an ERC-20 contract. For this transaction to not revert, another specific call to a function of the same contract must have **already been made**. Use the lookup table and fill in the calldata of **that call** to the function. **(5 marks. Note**: Fields below are provided for your convenience. It does not mean all have to be filled.

[0]:
[1]:
[2]:
[3]:

iii. Calculate the fee from Carrie's transaction that the proposer of the block got to keep.

Note: It is accepted if you only write the closed form of the equation with the correct numbers. (2marks)

iv. Briefly explain what happens to the fee that the validator does not get to keep and name the macroeconomic influence of this action on the Ethereum blockchain. (2 marks)