Birla Institute of Technology & Science – Pilani
Hyderabad Campus
1st Semester 2022-2023
Blockchain Technology (BITS F452) – Comprehensive Examination (Regular)

Date: 31.12.2022 Weightage: 40% Duration: 3 hrs. Type: Closed Book

Instructions: Answer all questions. All parts of a question should be answered consecutively. No of pages: 4

Q1.(a) This problem pertains to the Ethereum blockchain platform. The pre-upgrade computation of Ethereum gas fees is different from the post-upgrade. Given: pre-upgrade gas limit = 21000 units; gas price is 200 gwei. Fill in the blanks in the table below.

The maximum gas fee is ___ ETH. Now user1 sends 2 ETH to user2. The amount which comes from user1's Ethereum wallet is ___ ETH. At the end of this transaction, user2 receives ___ ETH. An Ethereum miner would receive ___ ETH.

(b) As you are aware, there is a standard limit on Ethereum gas consumption. However, the ether gas limit varies from transactions to transactions. Fill in the blanks in the following table.

(i) User A places an Ether gas limit of 65000 units for an ETH transfer which involves smart contracts. The EVM consumes ___ units and refunds ____. (ii) User B sets a gas limit of 20,000 whereas the actual transaction required 21000 units and the transaction is to send 1 ETH to another user C. The EVM consumes ___ units. The transaction status is ___. The amount of ETH received at user C is ___. The gas units at user B is ____. The amount of ETH which user B will hold on to is ____. The gas units lost by user B is ____

(c) This scenario talks about the post-upgrade transactions in Ethereum which introduced the notion of variable -size blocks and transaction-fee mechanism to Ethereum. Given block number 6; its base fee is 160.2 gwei; the base fee increases by a maximum of 12.5% per block if the target block size is exceeded. Compute the maximum base fee to be added to create a transaction on block number 9.

(2 + 4 + 4 = 10 marks)

Q2. (a) A snippet of a bitcoin transaction with one input and one output is given below: Fill in the blanks in the subsequent table.

Input: Previous TX: f5d8ee39a430901c91a5917b9 f2dc19d6d1a0e9cea205b009ca73dd04470b9a6 Index: 0	Output: Value: 5000000000 scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35 549d OP_EQUALVERIFY OP_CHECKSIG
ScriptSig: 304502206e21798a42fae0e854281abd38bacd1a eed3ee3738d9e1446618c4571d1090db022100e2 ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5f dd7d5d6cc8d25c6b241501	

In the given transaction, the input imports ___ BTC from output #____ in transaction #____ The output sends ____ BTC to the bitcoin address ____ (expressed here in hexadecimal form) instead of the regular ____ form. When the recipient wants to spend this money, the recipient will reference the output # ____ of this transaction in an input of its own ____.

(b) Bitcoin networks use a scripting system for transactions. The script words are also known as commands, opcodes or functions and there are different categories of script words. Given a few script words, correctly map them to their respective categories. Ex: **A => 1**

Script words	Script word categories	Script word-Category mapping
A: OP_1NEGATE B: OP_NOP C: OP_IFDUP D: OP_EQUALVERIFY E: OP_NEGATE	1. Arithmetic 2. Stack 3. Bitwise logic 4. Constant 5. Flow control	

(c) Given the following steps of a transaction execution as applied to the bitcoin environment, summarize the steps as a **one-line P2PKH transaction script.**

1. The original public key is duplicated using OP_DUP. 2.It is then hashed using the OP_HASH160. 3. The hashed value is compared with the hashed public key in the locking script (scriptPubKey) using OP_EQUALVERIFY. This makes sure that they are similar. 4. If it is a match, the script proceeds to check the digital signature against the public key using the OP_CHECKSIG.

(4 + 5 + 1 = 10 marks)

Q3. (a) Cryptographic hash functions play a very important role in various aspects of blockchain technology. Also, in blockchain protocols, we need to test securely and efficiently and then prove that a transaction indeed belongs to a block. Assume that we have a set of four transactions T1, T2, T3 and T4 in a block b1 in the bitcoin environment. Prove that a Merkle tree for these transactions can be thought of as a collision resistant hash function to test the membership of a transaction in the block by providing the authentication path. Show the steps and the diagrams (Merkle tree) clearly.

(b) As you are aware, for a Merkle tree construction with odd number of transactions, we need to duplicate the last transaction since the Merkle tree has to be a full binary tree. According to the collision resistant property of the hash function, this would mean that the two leaf nodes represent exactly the same content. Show by Merkle tree construction and by proof how the Bitcoin network can avoid the dishonest nodes from intentionally recording exactly the same two transactions inside the same block and thereby prevent the possibility of double-spending attack? For illustration purpose take the number of transactions in the block as 5.

(7.5 + 7.5 = 15 marks)

Q4. (a) The following table gives a snapshot of various blockchain consensus protocols and the type of attacks which they can resist. Give the closest mapping of the consensus algorithm and the type of attack which it can possibly prevent.

Blockchain consensus algorithm	Type of attack which it can resist	Consensus – attack prevention mapping
(i) Proof of Work	1. network preservation attack	
(ii) Proof of Stake	2. node malfunction attack	
(iii) Delegated Proof of Stake	3. DDoS attack	
(iv) Proof of Elapsed Time	4. Double spending attack	
(v) Proof of Burn	5. 51% attack	

(b) The Ethereum blockchain has moved to the Proof of Stake consensus mechanism since it is more secure and less energy-intensive. Answer the following with regard to PoS implementation in Ethereum.
(i) What is the amount in ETH, which a user has to deposit into a deposit contract so that it can participate as a validator?
(ii) The time in Proof of Stake is divided into slots of duration (_seconds) and epochs (_ #slots)
(iii) Atleast what fraction of the total staked ETH is required to declare a transaction's finality using PoS?
(iv) What fraction of the total staked ETH is required to be committed to be lost by an attacker to revert a finalized block in PoS?
(v) In PoS, can a honest validator decide to forcibly remove the attacker from the network and destroy their staked ETH? Reason your answer.

(5 + 5 = 10 marks)

Q5. (a) In Ethereum platform, the mining difficulty is calculated from the time difference between blocks. Also the difficulty is calculated differently for different implementations of the Ethereum projects.
(i) Give the exact formula for computing the mining difficulty in Ethereum Frontier project.
(ii) Give the exact formula for computing the mining difficulty in Ethereum Homestead project.
(iii) What way the Homestead computation is superior to the Frontier computation?
(b) Answer the following in the context of bitcoin blockchain networks.
(i) If the number of guesses per second on the bitcoin blockchain network as on May 2011 was 10^{12}, what was the corresponding the hash rate?
(ii) Fill in the blanks in the following table.

The Bitcoin difficulty value started at ___. For every ___ blocks that are found, the timestamps of the blocks are compared to find out how much time it took to find the blocks; let it be T. We want ___ # blocks to take ___ weeks. If T is different, then we multiply the difficulty by (___) . As an example, if it took only 10 days, it means the difficulty is too ___ and thus will be increased by ____%. Generally, the difficulty will decrease after the network ___drops. If the correction factor is greater than ___ (or less than ___), then the factor ___ or the factor ___ are used instead, to prevent the change to be too abrupt.

(5 + 7 = 12 marks)

Q6. (a) Smart contract is an important feature of the Ethereum platform. Consider the multi-sig smart contracts used for simple DAO governance. (i) If there are 123 possible acceptable

signatures, how many signatures we can afford to be lost and still the funds being retrievable? (ii) What is the minimum number of key holders who must agree and sign in order for the multi-sig contract to execute?

(b) Ethereum, the state machine model based environment, uses a Merkle-Patricia tree data structure unlike the bitcoin blockchain networks. (i) Illustrate, how the Merkle Patricia tree saves the states in Ethereum. (ii) Draw the taxonomy of the different types of nodes in a Merkle Patricia tree. (iii) Given the following key value pairs {(0x0, null), (0x1, null), (0x9, null), (0xA, 2000), (0xB, null), (0xC, null), (0xD, null), (0xE, 3000), (0xF, null)} as the leaf nodes and 0XBE as the root node, construct the Merkle Patricia tree. What is the value in the key 0XBEA? What is the value in the key 0XBEE?

(5 + 8 = 13 marks)

Q7. (a) The bitcoin blockchain network follows the longest chain rule. As you are aware, the longest chain is measured by the chain work. Given a blockchain BC1 with 3 blocks mined with a difficulty target of 1 and 2 blocks mined with an increased difficulty target of 4. Compute the total chain work for this blockchain.
(b) The Ethereum platform uses the Greedy Heaviest Observed Sub Tree (GHOST) chain selection rule. Given below is a partial depiction of the simplified version of GHOST protocol which goes through seven levels. Complete the protocol.

- A block must specify a parent, and it must specify 0 or more ___ blocks
- A ___ block included in block B must have the following properties:
  - It must be a direct child of the kth generation ancestor of B, where ___ <= k <= ___.
  - It cannot be an ancestor of ____
  - A ___ block must have a valid block header, but does not need to be a previously verified or even valid block
  - A ___ block must be different from all uncles included in previous blocks and all other uncles included in the ____ block (non-double-inclusion)
- For every uncle block U in block B, the miner of B gets an additional ____% added to its coinbase reward and the miner of U gets ____% of a standard coinbase reward.

(5 + 5 = 10 marks)