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

Date: 05.11.2022 **Weightage: 30%** **Duration: 1 hr 30 min.** **Type: Closed Book**

Instructions: Answer all questions. All parts of a question should be answered consecutively. No.of pages: 2

Q1. (a) This problem pertains to the cryptographic hash functions in blockchains. (i) If a hash function H produces an n-bit output, what is the number of operations (in terms of n) an attacker needs to carry out on a random input to search for the second match of the output? (ii) As applied to the bitcoin blockchain, what is the number of operations in this context?

(b)Let H be a hypothetical cryptographic hash function used in the blockchain context with M as the input and h as the hash value generated. H(M) is M mod n with n being a large integer. The hash value h ranges from 0 to n-1. (i) Is H a pre-image resistant function? (ii) Is H strongly collision-free? Reason your answer in both the cases.

(5 + 5 = 10 marks)

Q2. (a) Merkle trees help us encode blockchain data in an efficient and secure manner. Consider a merkle tree construction for a block b1 comprising 8 transactions. User B suspects that the User A has not included Transaction #6 (TX6) and hence wishes to check its inclusion in the block b1. (i) Show how B checks the presence of TX 6? (ii) What pieces of information B requires from A so that it can check TX6's presence in b1. Show the pictorial representation of the Merkle tree construction while you answer this.

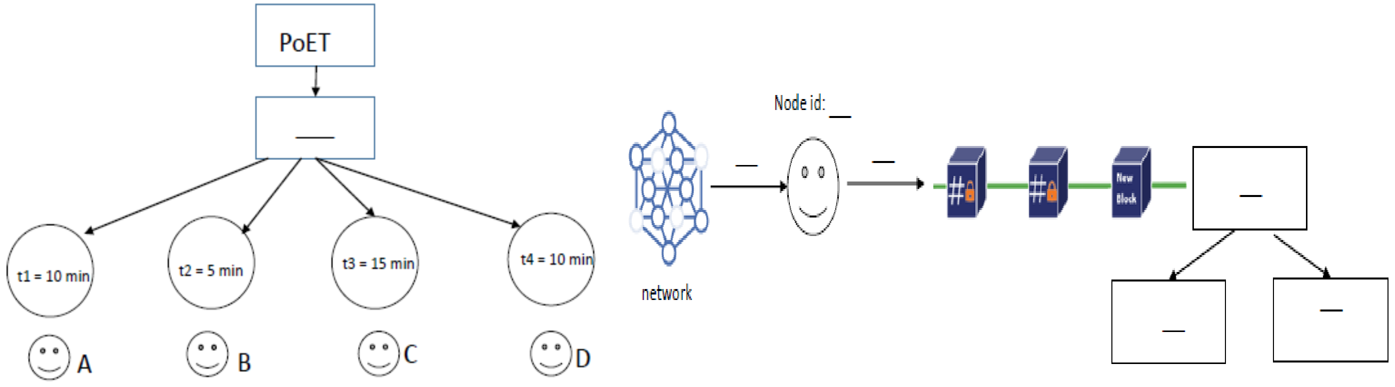
(b) Let us consider a blockchain BC1 with over 5 lakh blocks in it. Let the root hash of the block #492919 be the value H: e045b18e7a3d708d686717b4f44db2099aabcad9bebf968de5f7271b458f71c8. Fill in the blanks in the following table:

The block header of #492919 comprises the fields ______; _______; _______; ______; ______; ______. For block #492919, let its unique hash value H1 be: 000000000000000000bfc767ef8bf28c42cbd4bdbafd9aa1b5c3c33c2b089594. The cryptographic pointer value ______ of #492919 is stored in the block #______.

(6 + 4 = 10 marks)

Q3. Blockchain networks rely on consensus protocols to establish agreement among the nodes in the network. Answer the following with regard to blockchain consensus algorithms.

(a) The following is a depiction of the Proof of Elapsed Time (PoET) consensus algorithm. Fill in the blanks depicted in the diagrams to complete the flow of the algorithm. A, B, C and D are the nodes and t1, t2, t3 and t4 their respective waiting time.



(b) Following is the snapshot of one round of execution of DPoS. Fill in the blanks.

Let n = 51 be the number of block producers who get selected from a pool of block producer candidates. The ith block producer signs the _____ block until i = _____. A block is finalized when it is voted by _____ number of block producers. Otherwise the _____ rule is followed. The block validators verify that the created blocks follow the _____ rule.

PTO

(c) Assume that a blockchain network uses the Proof of Stake (PoS) consensus protocol. Let N = 100 be the number of nodes in the blockchain network; let h = 399999 be the current block height; let C = 1000 be the number of coins present in the system; let the number of coins owned by a node n1 in the network be 100. Compute the number of new blocks the node n1 can get to mine.

(5 + 5 + 2 = 12 marks)

Q4. As you are aware, Script is a stack-based programming language that enables the processing of transactions on the Bitcoin blockchain.

(a) Complete the P2PKH transaction.

Basic P2PKH transaction (user A wants to send 1BTC to B)
A does not know B's ___ key; A only knows B's address which is a ____ encoded cryptographic hash of B's ___ key. A can create the transaction by decoding B's address to his "___ hash." When A sends 1 BTC to B, a locking script called ___ is placed on the funds. At that point, the only person who can spend this 1 BTC is the person that supplies the input (___) that produces the ___ hash to which A sent the funds, along with a digital signature from the corresponding Bitcoin ____ key. 1 BTC now belongs to B, but only if B can prove that he is the owner of the BTC address that he provided to A.

(b) The following table shows some of the opcodes used for flow control in the Bitcoin script language. Write the table in the answer script and complete the tabular description of the opcodes.

Opcode (word)	Input	Output	Description
OP_VERIFY			
OP_RETURN			

(8 + 2 =10 marks)

Q5. (a) Block header hash and block height help us understand the structure of a blockchain. (i) Given that the block header hash of the first bitcoin block ever created is: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f, what is its height? (ii) If the block height on January 1, 2014, for the bitcoin network was approximately 278,000, what is the length of the blockchain? (iii) Does the block height always identify a single block? Reason your answer.

(b) This problem pertains to assembling and selecting chains of blocks. Fill in the blanks.

A new block # 277,316 will have a reference to the hash of the block #___. Most nodes that receive the block #____ will already have the block #_____ as the tip of their main chain and will therefore link the new block and extend that chain.

(c) Consider the bitcoin forks and longest chain rule. Assume that two nodes A and B succeed in resolving the PoW challenge and both add a new block to their local blockchain. They, then propagate the new blockchains to other nodes. If another node P receives first the blockchain from A, and it approves it, will it reject the chain it receives from B? Reason your answer.

(3 + 3 + 2 = 8 marks)

Q6. (a) As applied to the bitcoin blockchain network, answer the following: (i) why the network difficulty value is readjusted after every 2016 blocks? (ii) what is the difficult level of the very first block in bitcoin network? (iii) it has been observed that in the bitcoin network, what is the reason that the first difficulty adjustment did not take place until block #32,256**?**

(b) Consider the double spending attacks in bitcoin networks. For the given descriptions for each of the three types of double spending attacks, match the description with the type of attack.

Description	Type of double spending attack
(i) The attacker is a miner who uses the same coins in a second transaction and then releases the pre-mined block	
(ii)The attacker may send the same coin to different vendors in rapid succession, probably by using two different machines	
(iii)The attacker mines a private blockchain where he double-spends the coins	

(7 + 3 = 10 marks)