INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR	
	Stamp / Signature of the Invigilator

EXAMINATION (Mid Semester)	**SEMESTER (Autumn)**

Roll Number									**Section**		**Name**	

Subject Number	C	S	6	1	0	6	5	**Subject Name**	*Theory and Applications of Blockchain*

Department / Center of the Student		**Additional sheets**	

Important Instructions and Guidelines for Students

1. You must occupy your seat as per the Examination Schedule/Sitting Plan.
2. Do not keep mobile phones or any similar electronic gadgets with you even in the switched off mode.
3. Loose papers, class notes, books or any such materials must not be in your possession, even if they are irrelevant to the subject you are taking examination.
4. Data book, codes, graph papers, relevant standard tables/charts or any other materials are allowed only when instructed by the paper-setter.
5. Use of instrument box, pencil box and non-programmable calculator is allowed during the examination. However, exchange of these items or any other papers (including question papers) is not permitted.
6. Write on both sides of the answer script and do not tear off any page. **Use last page(s) of the answer script for rough work.** Report to the invigilator if the answer script has torn or distorted page(s).
7. It is your responsibility to ensure that you have signed the Attendance Sheet. Keep your Admit Card/Identity Card on the desk for checking by the invigilator.
8. You may leave the examination hall for wash room or for drinking water for a very short period. Record your absence from the Examination Hall in the register provided. Smoking and the consumption of any kind of beverages are strictly prohibited inside the Examination Hall.
9. Do not leave the Examination Hall without submitting your answer script to the invigilator. **In any case, you are not allowed to take away the answer script with you.** After the completion of the examination, do not leave the seat until the invigilators collect all the answer scripts.
10. During the examination, either inside or outside the Examination Hall, gathering information from any kind of sources or exchanging information with others or any such attempt will be treated as **'unfair means'**. Do not adopt unfair means and do not indulge in unseemly behavior.

Violation of any of the above instructions may lead to severe punishment.

Signature of the Student

To be filled in by the examiner

Question Number	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Total**
Marks Obtained											

Marks obtained (in words)	**Signature of the Examiner**	**Signature of the Scrutineer**

Write the answers in the boxes only. You can use the designated spaces for rough works. This question has 14 pages including the space for rough works.
Note:

(i) There are FIVE questions in this paper. Answer all the questions. The answers should be precise and to-the-point. Marks will be deducted for unnecessary texts.

(ii) Write down the assumptions clearly, if any. No clarifications will be given during the exam hours.

1. (a) Let a block has 6 transactions (numbered from 1 to 6). It has so far been confirmed by 30 blocks (including the block that mined the transaction). If an attacker changes transaction number 5 in this block, determine how many hashes will have to be updated (including both Merkle tree hashes as well as block hashes) so that the change will be undetected. Assume that the attacker can determine the correct block hash in 9 minutes on an average while the rest of the network needs 10 minutes on an average to determine the correct block hash. Consider that the time to determine the Merkle root by hashing the transactions is negligible. You must briefly show your calculation. **[4 Marks]**

(b) Let Bob wants to send a long message to Alice. Alice should be able to confirm that it was indeed sent by Bob, and Bob later cannot deny that he had sent the message. They also want that nobody else should be able to see its content. Alice and Bob plan to use public key cryptography and cryptographic hashing techniques. Let the key pairs of Alice and Bob be (Pub_A, Pri_A) and (Pub_B, Pri_B), respectively. Let E, D and H be the encryption, decryption and hash functions, respectively. Let M denote the Message and $H(M)$ its digest. Briefly write the steps to be used by Alice to send the digitally signed message and the steps used by Bob to verify that the message was indeed sent by Alice while nobody else can decipher the content of the message. **[4 Marks]**

2. Let Alice wants to Pay 10 BTC to Bob in a bitcoin transaction. Let the public keys of Alice and Bob (Pub_A and Pub_B) and their hashes (pubKeyHash_A and pubKeyHash_B) are as follows: Pub_A = 6789, Pub_B = 2345, pubKeyHash_A = 56789, pubKeyHash_B = 12345.

   (a) Determine which scripts will be used by Alice and Bob for locking and unlocking the 10 BTC. You need to specify all the components of the two scripts. If you cannot determine an exact value, e.g., calculating the hash of a message, you may denote the same using an appropriate function with proper parameters. Also, show how the scripts will be executed step by step using a stack to let Bob spend the bitcoins. **[4+3 = 7 Marks]**

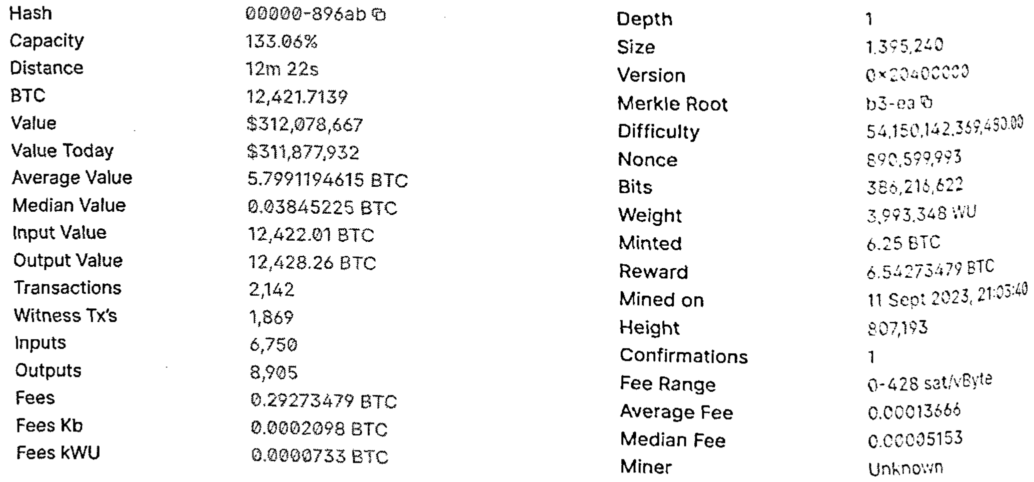
(b) Next, assume Cathy could capture the transaction sent by Alice and is now trying to use the 10 BTC from that transaction. Show which script processing step(s) will prevent her from doing so under various assumptions of the knowledge of Cathy. **[3 Marks]**

3. (a) Suppose we start a bitcoin like cryptocurrency (Called KGPCoin) today with initial block reward of 100 KGPCoins. Block reward is reduced by a factor of 3 every 1800 days. Average block mining time is 20 minutes. Determine (i) the total KGPCoins that will be "minted" in such a network, and (ii) the approximate date by which 90% of total KGPCoins will get minted.

[4+4 = 8 Marks]

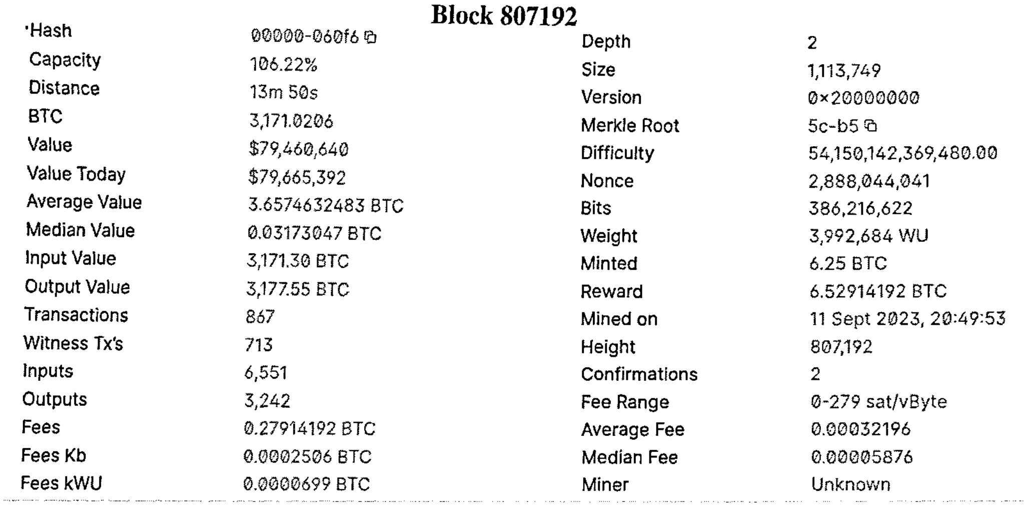
(b) Consider that we want to verify if the block hash for Bitcoin Block Number 807192 is correct or not. Based on the following three figures, identify the values that will be required for the verification. [4 Marks]

Block 807193



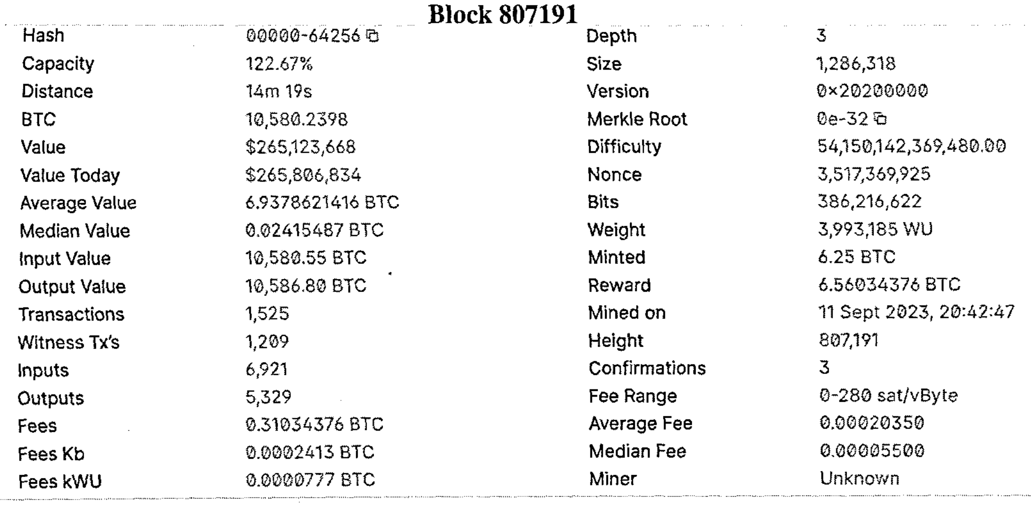
Hash	00000-896ab	Depth	1
Capacity	133.06%	Size	1,395,240
Distance	12m 22s	Version	0×20400000
BTC	12,421.7139	Merkle Root	b3-ea
Value	$312,078,667	Difficulty	54,150,142,369,480.00
Value Today	$311,877,932	Nonce	890,599,993
Average Value	5.7991194615 BTC	Bits	386,216,622
Median Value	0.03845225 BTC	Weight	3,993,348 WU
Input Value	12,422.01 BTC	Minted	6.25 BTC
Output Value	12,428.26 BTC	Reward	6.54273479 BTC
Transactions	2,142	Mined on	11 Sept 2023, 21:03:40
Witness Tx's	1,869	Height	807,193
Inputs	6,750	Confirmations	1
Outputs	8,905	Fee Range	0-428 sat/vByte
Fees	0.29273479 BTC	Average Fee	0.00013666
Fees Kb	0.0002098 BTC	Median Fee	0.00005153
Fees kWU	0.0000733 BTC	Miner	Unknown

Block 807192



Hash	00000-060f6	Depth	2
Capacity	106.22%	Size	1,113,749
Distance	13m 50s	Version	0x20000000
BTC	3,171.0206	Merkle Root	5c-b5
Value	$79,460,640	Difficulty	54,150,142,369,480.00
Value Today	$79,665,392	Nonce	2,888,044,041
Average Value	3.6574632483 BTC	Bits	386,216,622
Median Value	0.03173047 BTC	Weight	3,992,684 WU
Input Value	3,171.30 BTC	Minted	6.25 BTC
Output Value	3,177.55 BTC	Reward	6.52914192 BTC
Transactions	867	Mined on	11 Sept 2023, 20:49:53
Witness Tx's	713	Height	807,192
Inputs	6,551	Confirmations	2
Outputs	3,242	Fee Range	0-279 sat/vByte
Fees	0.27914192 BTC	Average Fee	0.00032196
Fees Kb	0.0002506 BTC	Median Fee	0.00005876
Fees kWU	0.0000699 BTC	Miner	Unknown

Block 807191



Hash	00000-64256	Depth	3
Capacity	122.67%	Size	1,286,318
Distance	14m 19s	Version	0x20200000
BTC	10,580.2398	Merkle Root	0e-32
Value	$265,123,668	Difficulty	54,150,142,369,480.00
Value Today	$265,806,834	Nonce	3,517,369,925
Average Value	6.9378621416 BTC	Bits	386,216,622
Median Value	0.02415487 BTC	Weight	3,993,185 WU
Input Value	10,580.55 BTC	Minted	6.25 BTC
Output Value	10,586.80 BTC	Reward	6.56034376 BTC
Transactions	1,525	Mined on	11 Sept 2023, 20:42:47
Witness Tx's	1,209	Height	807,191
Inputs	6,921	Confirmations	3
Outputs	5,329	Fee Range	0-280 sat/vByte
Fees	0.31034376 BTC	Average Fee	0.00020350
Fees Kb	0.0002413 BTC	Median Fee	0.00005500
Fees kWU	0.0000777 BTC	Miner	Unknown

4. (a) (i) Why does Ethereum PoS use pseudorandom functions rather than directly considering the stake contribution, to determine a block proposer from the activated validator set? (ii) Explain how does Ethereum use RANDAO for selecting the block proposers at each slot. (iii) Is there a possibility of fork in PoS (consider Ethereum PoS as an example), apart from the planned forks (like for version update, etc.)? **[2+4+2 = 8 Marks]**

(b) What do you think would be a major challenge in adopting PoS in Bitcoin blockchain, particularly from the perspective of the miners? Explain your answer **[2 Marks]**

5. (a) (i) What are the two important criteria that needs to be satisfied for a perfect distributed consensus? Explain those two criteria. (ii) Write down the factors that prevents applying majority voting-based distributed consensus protocols for a permissionless blockchain networks.

[3+2=5 Marks]

(b) What is double spending in the context of blockchain transactions? In PoS blockchains, the block proposers do not need to find out the nonce value for a block; then how do we prevent double spending in a PoS blockchain?

[2+3 = 5 Marks]