



INDIAN INSTITUTE OF TECHNOLOGY
KHARAGPUR

Stamp / Signature of the Invigilator

EXAMINATION (End 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 SIX 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) Consider the following log entries for four different RAFT servers. Can these log configurations occur in a proper implementation of RAFT? Explain your answer.

Log index	1	2	3	4	5	6
Term	1	1	3	2	2	

Log index	1	2	3	4	5	6	7
Term	1	1	2	2	2	3	

Log index	1	2	3	4	5	6
Term	1	1	3	3	5	

			Missing entry					
Log index	1	2	3	4	5	6	7	8
Term	1	1		2	2	2	2	

[4 Marks]

- (b) The figure below shows the state of the logs in a cluster of five RAFT servers. Which log entries may safely be applied to state machines? Explain your answer. The values inside the box show the term values. **[4 Marks]**

Log Index	1	2	3	4	5	6	7	8
Leader for Term 4	1	1	2	2	2	2	4	
Followers	1	1	1	2				
	1							
	1	1	2	2	2			
	1	1	2	2	2	2		

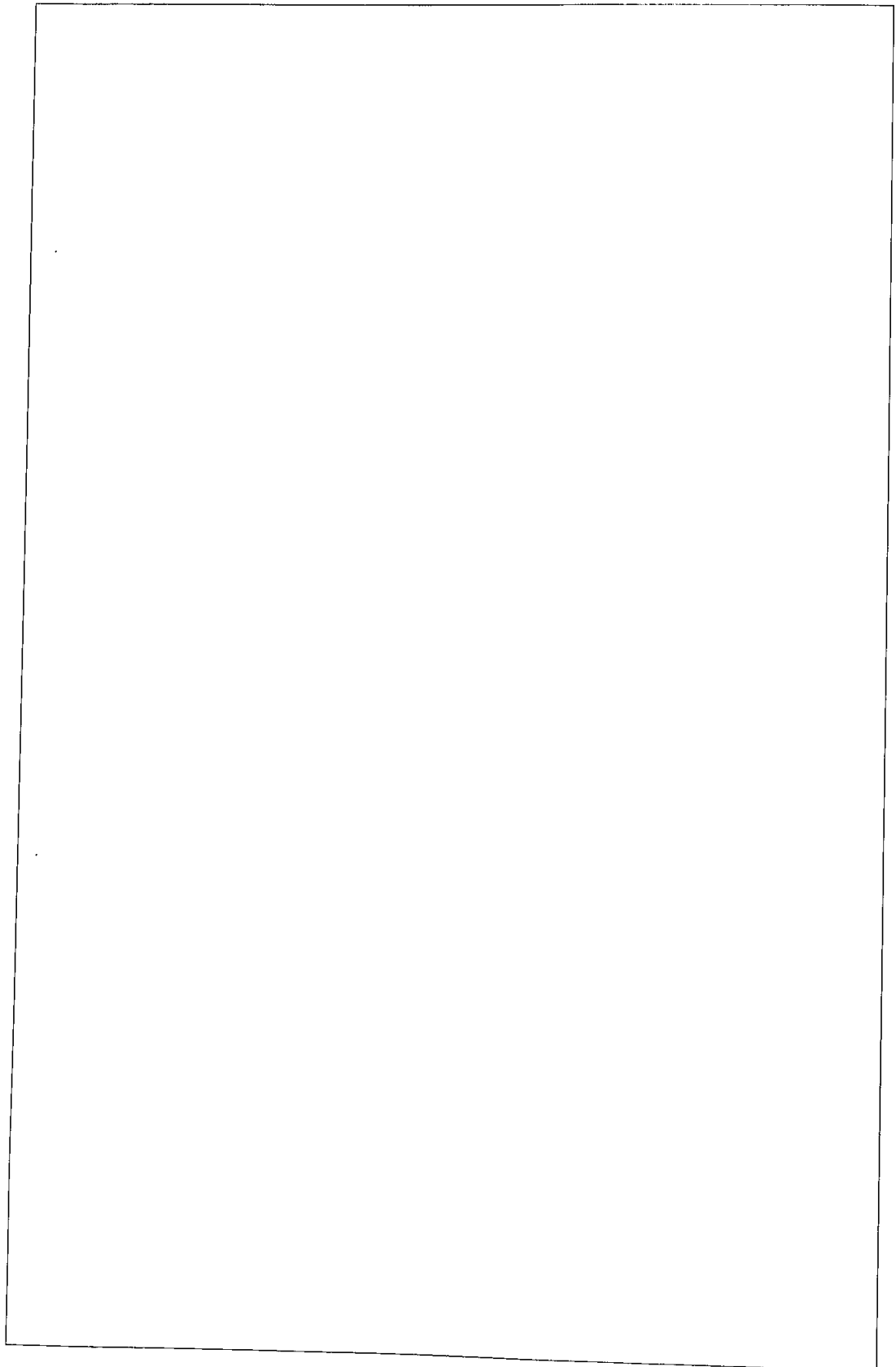
- (c) Consider a RAFT instance with 5 replicas R1 to R5. Say, the leader R1 is elected at Term 4, and the latest (index, term) for the five replicas are as follows. R1 : (11, 3), R2 : (8, 4), R3 : (5, 4), R4 : (9, 4), R5 : (4, 3). Assume that all the logs are consistent. (a) What is the first index that R1 has served as a leader? (b) What is the last index upto which the operations can be considered to be committed? [1+1 Marks]

2. (a) The VIEW-CHANGE message in the PBFT view change protocol contains (i) a list of previous checkpoints, (ii) a list of proposals that have been seen but not checkpointed. How are these two lists used to ensure the **safety** of the PBFT protocol? [5 Marks]

- (b) What is meant by Byzantine Dissemination Quorum? Assume that a PBFT system can tolerate a maximum of 2 crash and 1 equivocation (share different information with different peers). What is the Byzantine Dissemination Quorum for this PBFT system? Explain your answer. [2+3=5 Marks]

3. (a) Consider the Byzcoin consensus with five miners – A, B, C, D, E. The miners have collectively mined 25 key blocks with the sequence as follows: BAAEECDEBADDEDABDEBADBAED. Consider that a window size 10 is used to construct the witness co-signer tree. Let the tree is a binary search tree in order of the mining share of the individual miners (the root has the highest mining share, and so on). Construct the witness co-signer tree for signing the micro-blocks under

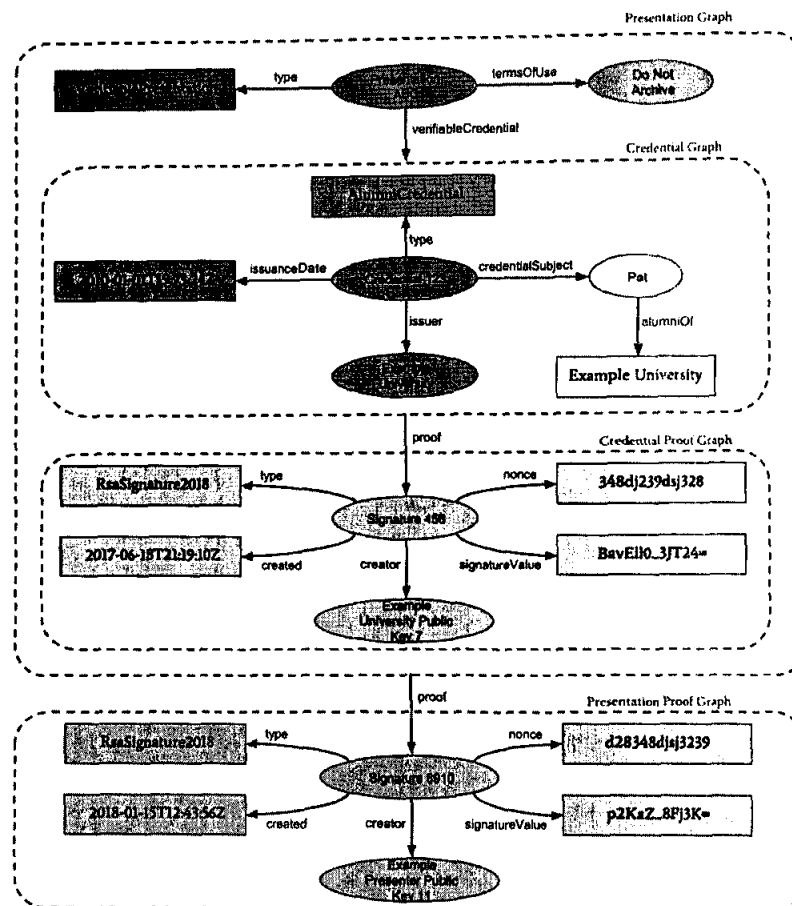
- (b) Explain how Byzcoin achieves consensus on the micro-blocks on top of the above witness co-signer tree. Consider that it uses Schnorr multisignature for this purpose. With the diagrams, clearly explain how the messages are forwarded across the witness co-signers and the final signature is obtained for a micro-block. **[5 Marks]**



4. (a) (i) Can Algorand achieve final consensus under weak synchrony assumption? Explain your answer. (ii) What is cryptographic sortition? What is the use of cryptographic sortition in Algorand? [2+2 = 4 Marks]

- (b) Suppose that IIT Kharagpur issues VCs to its students after graduation providing information about the student Roll No (R), Name (N), Major Department (D), Year of Graduation (Y), CGPA (C), and Grades (G_s) in various subjects. The student can later submit it to various employers as they change the jobs. Employers need to verify only N, D, Y and C. The student can also use it to apply for higher studies for which the universities need all the information in the VC. Identify which values will be used in the following situations for the verifiable presentations – (i) IIT Kharagpur presents (issues) the VC to the student, (ii) the student presents the VC to XYZ company to apply for a job, and (iii) the student presents the VC to BCD university. For all the above three situations, write down the values that will be used in various fields of the corresponding verifiable presentation graphs (in the form of `field_name = value`). Use

your name and roll number as the student name and roll number, if needed. You can assume any other values as needed. [Hint: The verifiable presentation graph looks as follows.]
[2+2+2 = 6 Marks]



(i) University Presents the VC to the Student:

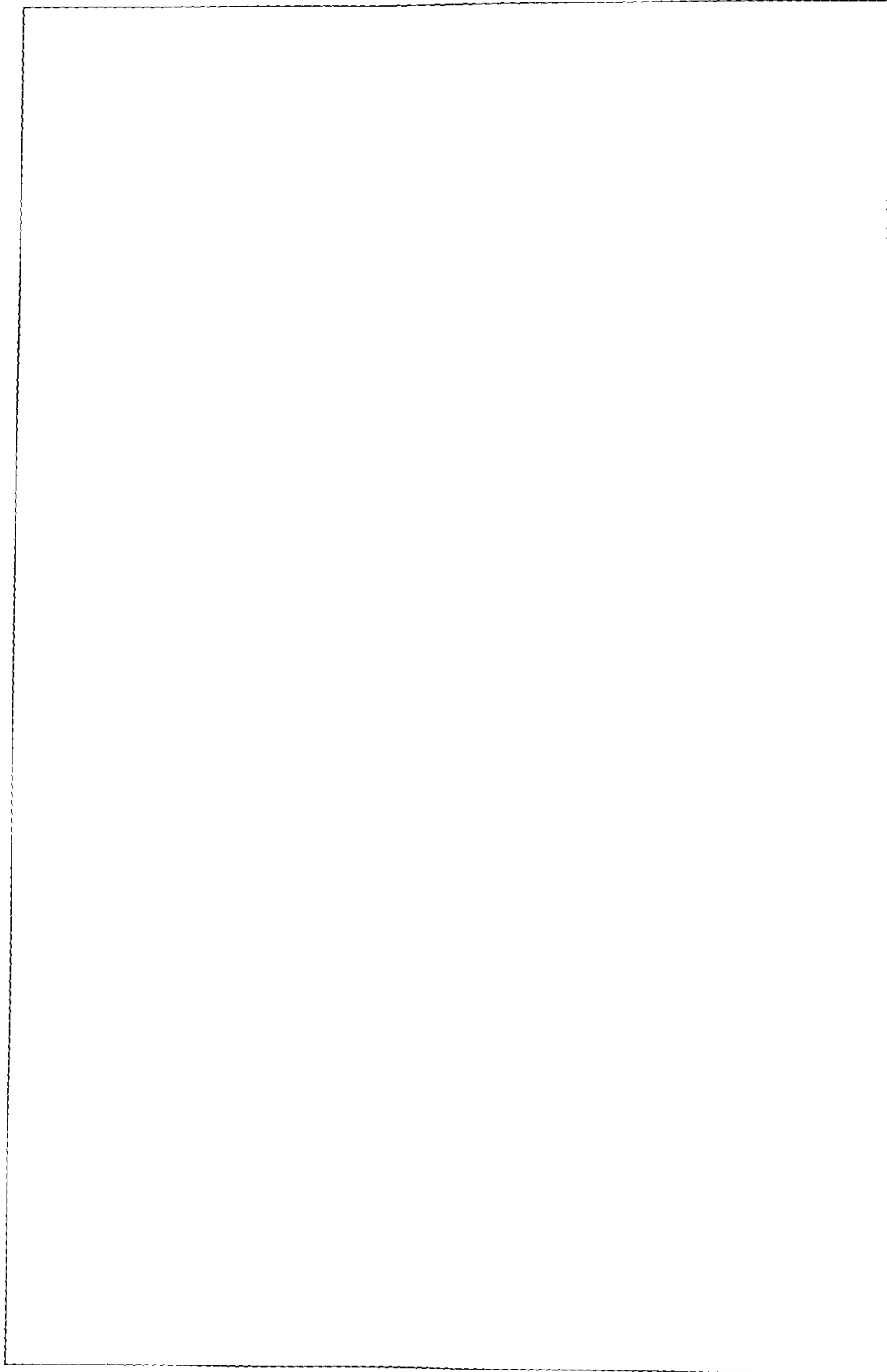
(ii) Student Presents the VC to XYZ Company:

(iii) Student Presents the VC to BCD University:

5. (a) Consider a multi-party atomic cross-chain swap between Alokesh (A), Balbir (B), Chishti (C), and David (D). Alokesh wants to buy a Cryptokitty (a digital cat in the popular Ethereum dapp game Cryptokitties) from Balbir for 1 Ether, but he does not have any Ether with him; rather, he poses some bitcoins. Chishti can trade Ethers but she can do so only through Algos. David can trade Algos through bitcoins. Consider that 1 Ether = 0.05 Bitcoins = 17,473 Algos. Write down the HTLCs that will be created for this atomic cross-chain swap. Consider that the minimum timeout duration for a HTLC is 20 mins. Assume that the key for this swap is "CRYPTOSWAP", and the corresponding hash is 2da41a3f5fa5125d61b27fe6e9a4e961 (You can write it as 2d...961). Explain, in which order, these contracts will be deployed and they will be executed. **[4+4 = 8 Marks]**

(b) Can Chishti and David form a coalition and set the contracts accordingly such that they get the bitcoins from Alokesh, but does not spend their Ethers and Algos? Explain. **[2 Marks]**

6. (a) What are the requirements that need to be ensured for verifiable data transfer across two permissioned blockchain networks. Explain with a diagram, how one can perform verifiable data transfer across two permissioned blockchain networks with the help of a relay. Clearly write down the services that the relay needs to support. **[2+3 = 5 Marks]**



- (b) With a diagram, explain how the DID controller, DID subject, DID document and Verifiable Data Registry are related to each other. Can DID subject be also a DID controller? Give examples when they are the same and different. **[3+2 = 5 Marks]**

