Preparation Exam
Part 2 of 2

Last Name: _____

First Name: _____

HSR PID: _____

Time: 120 minutes (for both parts)
This is a closed book exam.
Using a calculator is allowed, but not necessary.

General instructions:

1. Fill out your name immediately on this title page and the title page of part 2.
2. Place you HSR ID visibly on your table with the photo side up.
3. Turn off your mobile phone and keep it concealed and not on your person during the entire exam.
4. Do not turn this page until explicitly asked to do so.
5. Make sure that you have received all parts and pages of the exam.
6. Read through the entire exam before starting.
7. You are not allowed to bring your own blank pages into the exam.
8. Write your solutions in the spaces provided.
9. In case a question is unclear, make and document your assumptions before answering it.
10. Do not use red or erasable ink.
11. Cross out unintended answers clearly. Multiple answers will be graded as being incorrect.
12. Write legibly. Unreadable answers will be marked as being incorrect.
13. You may submit your answer scripts prematurely until 15 minutes before the end of the exam.
14. After the exam is over, please remain quietly seated until all answer scripts have been collected.
15. The points per question may vary.

Nr.	Title	Max. Points	Attained Points
1.	Basics	10	
2.	P2P and Distributed Hash Tables II	17	
3.	Distributed Systems and Blockchain	8	
4.	Ethereum	10	
	Total:	45	

Question 1: Basics (10 Points)

a) (2P) What is *congestion control* and why is *congestion control* important?

What:

Why:

b) (4P) List 3 methods how to establish direct connectivity if Network Address Translation (NAT) is involved. List a 4th method that always works, but without direct connectivity.

1.

2.

3.

4.

c) (2P) Is SCTP stream or message oriented and how well is it supported in the Internet.

Stream or message oriented:

Support:

d) (2P) What is *port preservation* and why is it important for hole-punching?

What:

Question 2: P2P and Distributed Hash Tables II (17 Points)

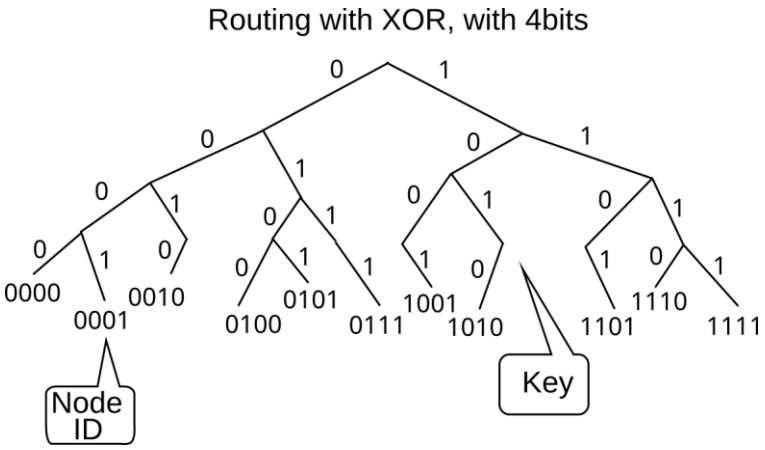
a) (5P) State whether the following statements are always completely true (**True**) or (sometimes/partially) false (**False**) by placing an X in the appropriate column in the table below.

Wrong answers do not result in negative points.

	Statement	True	False
1	Network Address Translation (NAT) enables end-to-end connectivity.		
2	A centralized P2P system can support fuzzy queries.		
3	Flooding does scale well with many nodes in the network.		
4	Peer IDs in a P2P network with 128 peers need to have a length of at least 7 bits.		
5	DHTs always needs maintenance messages for their neighbours.		

b) (13P) The following Kademlia network with an addressing space of 4 bits is given as shown below. The routing table state of each node is provided below as well. Consider the following situation:

Node 1 (binary notation 0001) starts a lookup for key 11 (binary notation 1011). Please answer in this context the questions b1), b2), and b3).



4-bit Kademlia network

Bucket Nr	1	2	3	4	node 15
Node	14	13	10	2	

Bucket Nr	1	2	3	4	node 14
Node	15	13	9	7	

Bucket Nr	1	2	3	4	node 13
Node	-	14	11	0	

Bucket Nr	1	2	3	4	node 10
Node	-	9	14	1	

Bucket Nr	1	2	3	4	node 9
Node	-	10	14	4	

Bucket Nr	1	2	3	4	node 7
Node	-	5	1	10	

Bucket Nr	1	2	3	4	node 5
Node	4	7	2	11	

Bucket Nr	1	2	3	4	node 4
Node	5	7	1	13	

Bucket Nr	1	2	3	4	node 2
Node	-	1	4	9	

Bucket Nr	1	2	3	4	node 1
Node	0	2	5	14	

Bucket Nr	1	2	3	4	node 0
Node	1	2	7	9	

Routing table of all nodes in the Kademlia network

b1) (1P) What is the distance in binary notation of node 1 to the key 11?

Distance:

b2) (9P) Fill in the dotted line (…) in the following table with the nodes that are being contacted during the routing process by node 1.

Routing Steps	1	2	3	4
Node	1	…	…	…

b3) (2P) Which closest node does the node at step 4 return?

Node at step 4 returns the following closest node:

Question 3: Distributed Systems and Blockchains (8 Points)

State whether the following statements are always completely true (**True**) or (sometimes/partially) false (**False**) by placing an X in the appropriate column in the table below.

Wrong answers do not result in negative points.

	Statement	True	False
1	Paxos describes the following roles: client, acceptor, proposer, learner, and leader		
2	Paxos can be divided into 3 phases: prepare/promise, accept/accepted, commit/validate.		
3	The main goal of Range Queries in DHTs is to quickly access an interval of key / values.		
4	Blockchains such as Ethereum or Bitcoin can be attacked with a 51% attack in order to delete transactions from the blockchain.		
5	TOR uses 3 random relays for anonymous Internet communication.		
6	TOR onion (hidden) services are used to provide services (such as web-sites) without revealing the provider's IP address.		
7	Message queues can be used for inter-process communication (IPC).		
8	Message queues can be used to build scalable distributed systems.		

Question 4: Ethereum (10 Points)

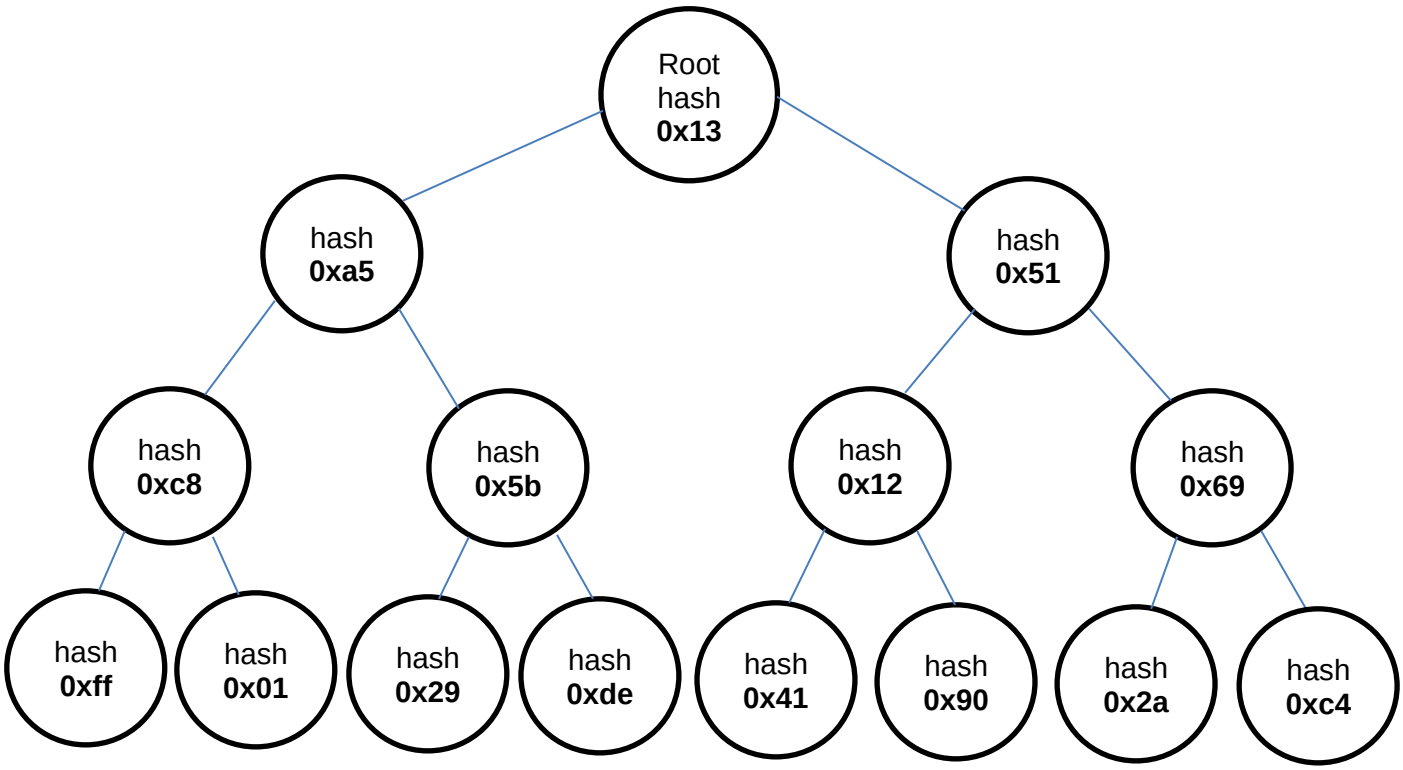
a) (3P) What is the main difference between the proof-of-work and proof-of-stake?

Main difference:

b) (4P) What happens if some miners change *e.g.,* the block reward and some miner do not?

What happens:

c) (3P) Consider the following Merkle tree. An incomplete Merkle proof was received: **0x13**, **0xa5**, **0x12**. Which transaction(s) could potentially be verified if the complete Merkle proof is received?



Given information: **0x13**, **0xa5**, **0x12** Potential transaction(s) for verification: