



Universität
Zürich^{UZH}

3041 - Blockchains and Overlay Networks — CSG, Prof. Dr. Burkhard Stiller

3041 - Blockchains and Overlay Networks

Exercise 4

25 March 2021

Optional Exercise

Assistants: Eder John Scheid, Christian Killer

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH—8050 Zürich, Switzerland



This exercise is optional and it **will not be** discussed in class. Students may send **questions** to **scheid@ifi.uzh.ch** and **killer@ifi.uzh.ch**. Some questions were taken from old exams.

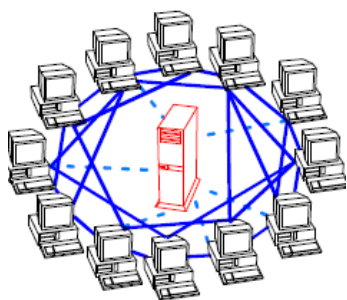
1 Dual-Choice Exercises

Choose for each statement either true or false. Please mark the correct answer with a cross. For each statement there is only one correct answer.

	Statement	True	False
a)	If a flooding-based search is executed in a P2P system, the requested file will always be found as long as it resides in the network.		
b)	Napster and Kademia are examples of structured P2P systems.		
c)	A Client/Server system is not an example of a P2P system.		
d)	In DHTs the identifier space for peers has to be the same as the identifier space for content.		
e)	No routing information is required to execute a flooding-based search in a P2P system.		
f)	The Bitcoin mining process allows the creation of an arbitrary amount of Bitcoins.		
g)	Flooding scales well in large networks.		
h)	In DHTs, nodes are only responsible for content with an ID equal to their node ID.		

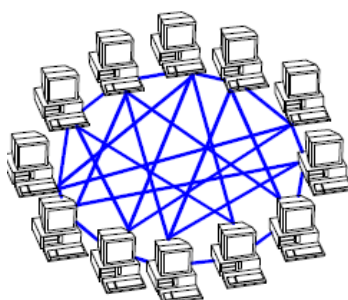
2 P2P Architectures

Provide the name of the corresponding 3 P2P architectures based on the figures below. Also, name an example application for each one of these architectures. Use these six boxes respectively to place your answer.



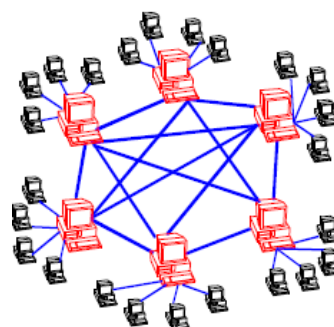
Name:

Example:



Name:

Example:



Name:

Example:

3 P2P Lookup

Fill in the blanks in the table below regarding lookup approaches. The blank cells listed in the second and third column shall be defined in the big-O notation; the remaining columns four to six are to be ticked with either a “yes” or a “no” answer.

Lookup Approach	Per Node State	Communication Overhead	Support of Fuzzy Queries	False Negatives Possible	Single Point of Failure Present
Centralized			<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Flooding			<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
DHT			<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No

4 Comprehension and Discussion

Answer to following questions with a maximum of 4 sentences each.

a)	What is peer churn in the context of P2P Systems?
Answer:	
b)	How is double spending avoided in the Bitcoin system?
Answer:	

c)	In DHTs, the content can be stored in the participant nodes using two different strategies: Direct Storage and Indirect Storage. Describe both and present one advantage and one drawback of each strategy.
Direct:	
Indirect:	
d)	What is a Blockchain? What are the differences between public and private Blockchains?
Definition:	
Public:	
Private:	

5 Ethereum

Choose for each statement either true or false. Please tick the box for the correct answer.

	Statement	True	False
a)	Ethereum smart contracts can have repetition structures (e.g., loops).		
b)	While Bitcoin is Account-based, Ethereum is UTXO-based.		
c)	In a 51% attack you need to control 51% of the nodes.		
d)	ERC-20 is a technical standard used for smart contracts on the Ethereum blockchain for implementing tokens.		
e)	Oracles can be used to provide random values.		