Exercise
for Lecture “P2P Systems”

Prof. Dr. David Hausheer
Dipl.-Wirtsch.-Inform. Matthias Wichtlhuber, Leonhard Nobach, M. Sc., Dipl.-Ing. Fabian Kaup, Christian Koch, M. Sc., Dipl.-Wirtsch.-Inform. Jeremias Blendin

Summer Term 2015
Exercise No. 12
Published at: 07.07.2015, Submission date: 14.07.2015
Submission only via the Moodle platform in PDF, plain text, or JPG/PNG.
Contact: [mwichtlh|lnobach|fkaup|ckoch|jblendin]@ps.tu-darmstadt.de
Web: http://www.ps.tu-darmstadt.de/teaching/p2p/

Surname (Nachname):	
First name (Vorname):	
ID# (Matrikelnummer):	

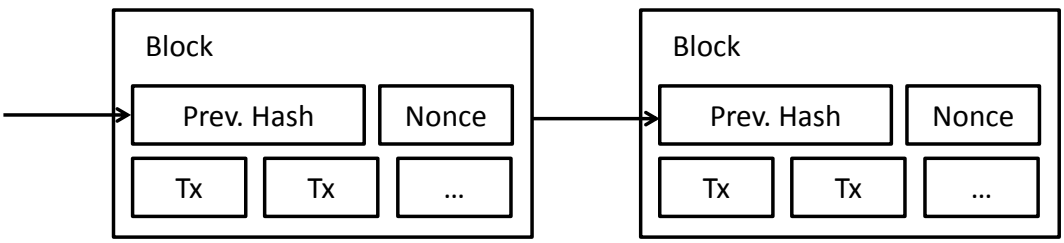
Problem 12.1 - BitTorrent

A) In the lecture, you have learnt about the incentive applied by BitTorrent. Assume two peers having the choice to cooperate or defect. Uploading data has a cost of $C_F = 1$ and downloading has a slightly higher value $U_F = 1 + \epsilon$, as the peer receives content. Derive the payoff matrix, taking the properties of the unchoking algorithm into account. What is the dominant strategy?

B) Discuss the trade-off between piece overlap and the number of distributed copies in a swarm. How does BitTorrent maintain a good balance?

C) Derive a formula for the average number of requests needed to receive a new chunk out of n pieces, if you already possess $m \leq n$ pieces. Use this formula as a base to define the average number of requests for receiving all pieces. Calculate the average number of requests needed for $n = 7$ pieces.

Problem 12.2 - Bitcoin



A) Bitcoin applies a cryptographic puzzle as a proof of work. The peer guesses a nonce in a hash function H, until the following (slightly refined) condition holds: $H(H(\text{previous hash}), \text{transactions}, \text{nonce}) \leq 2^n$. Assume the length of the hash to be 128

bits and the difficulty $n = 120$. Calculate the average number of guesses needed to solve the block with a probability of 99%.

B) Discuss the scalability of Bitcoin with respect to the block chain concept and the way new transactions and solved blocks are spread in the network.