Universität Zürich[UZH]

1312 - Blockchains and Overlay Networks

Exercise 2

7 March 2019

Due: 13 March 2019

Assistants: Eder Scheid, Christian Killer

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

ifi

Students must send their solutions to **p2p@lists.ifi.uzh.ch** up until the deadline. The solutions will be discussed the day after the deadline. Handing in all exercises is mandatory to receive credits and will be very useful for preparing the final exam. We encourage students to solve the exercises on their own and actively participate in the exercise discussions.

1 Distributed Ledgers and Blockchain

1 Tick the box with the right answer True (T), or Flase (F)::

A block in the blockchain can contain one or more transactions	T ☐	F ☐
If a change occurs in a leaf of a Merkle tree, then the Merkle root does not change, because the change only happened in the leaf	T ☐	F ☐
The SHA-256 hash function produces a fixed string of 256 bytes	T ☐	F ☐
Bitcoin miners are not able to select which transactions to include in a block	T ☐	F ☐
In Bitcoin, a private key of an address can be found by hashing its public key using the double SHA-256 method	T ☐	F ☐

2 What is the main difference between public and private blockchains?

3 How Bitcoin ensures that a new block will be created every approximate 10 minutes?

4 Why the Proof-of-Work (PoW) consensus algorithm is said to be a waste of energy?

5 Can a private blockchain be considered a blockchain?

2 Challenge Task Preparation

1 To familiarize yourself with the Ethereum Blockchain you must transfer some Ether to our address. For this exercise we use the testing network (**Ropsten**).
   → Install the Geth client: https://www.ethereum.org/cli, make sure you use the "--syncmode fast", "--testnet" and "console" options when starting the client.
   → Create an Account: > personal.newAccount()
   → Get some Ether through mining or from a faucet (e.g., http://faucet.ropsten.be:3001/)

→ Transfer 0.<matriculation_number> Ether to our address: **0x7547A14fe390f54dCe90Cfbf1c1d231Fb9308922**

→ Send the transaction ID and your matriculation number with the other solutions to **p2p@lists.ifi.uzh.ch**

P.S.: Remember to use the Ropsten testnet. Don't buy ether, in the testnet it is easy to get it for free. The Ropsten testnet may need some time to sync, so it is good to leave it syncing overnight. There is also the option to add instead of "--syncmode fast" you can change it "--syncmode light". The light option downloads less data but it is still experimental.