COMM.NET.500 P2P Systems and Blockchain Technologies
Blockchain laboratory:
Instruction sheet (2022-11-03)

Blockchain laboratory: Instruction sheet (2022-11-03)

1 Introduction

In this laboratory, you will work in pairs going through an example Python implementation of a generic blockchain and try out some of its functions, such as mining and transactions.

You should follow the instructions given in this paper in order and take notes/prepare answers for any questions presented. Questions do not have to be answered during the lab session, but the answers should be included in the post-lab report. Short answers with some key points are enough. More detailed information about the post-lab report and submission can be found on the course Moodle page.

Whenever the instructions tell you to do something related to the PCs, it should be done on both PCs, unless stated otherwise.

After the teaching assistant has accepted your work at the final checkpoint, you have passed the laboratory session.

If you have any questions at any time, please feel free to ask the teaching assistant.

2 Initial preparations

For the purposes of this laboratory, you have been assigned two PCs, which have IP addresses from the network 130.230.83.0/25 pre-configured on the *eth0* interface. Log in as the `student` user, whose password is simply `tc403`. On your desktop, you should have a shortcut for the terminal - open two of them.

On one terminal, start up the client: `python3 blockchain/client/blockchain_client.py` . By default, the web GUI of the client is accessible on port 8080. Open a browser and connect to `localhost:8080`. Create a wallet, and store the public and private keys in a text file, e.g. with `gedit`.

On the second terminal, start up the miner and link it with your wallet by giving your public key as an argument: `python3 blockchain/miner/blockchain.py -k PUBLIC_KEY` . Open up the web GUI of the miner, which is accessible on `localhost:5000`.

3 Joining the blockchain

In this section, your task is to join the existing blockchain and examine the past transactions of the blockchain.

Launch **Wireshark** and start capturing on the *loopback and eth1* interfaces. In the `Configure` tab of the miner web GUI, add 130.230.83.113:5000 and your group's other PC (130.230.83.???:5000) as nodes. Including the port is important.

Go back to the `Mining` tab and refresh the transactions in the blockchain by clicking the small blue button next to the *Transactions on the Blockchain* header.

In Wireshark, find and examine the existing blockchain data you received from node 130.230.83.113 (Filter hint: ip.addr == 130.230.83.113), and answer the following questions.

1. What kind of information is stored in the blockchain? (Hint: http://localhost:5000/chain)
2. How many blocks are already in the blockchain?
3. What transactions were made in block number 5?
4. Could you edit a past transaction and then pass off the chain as a newer valid one? Why or why not?

4 Mining

As your wallet does not contain any currency at the moment, your task is to "mine" some currency. Go back to the `Mining` tab in the miner web GUI (top right corner) and click the *mine* button. Observe the terminal outputs and the source code to find out what happens behind the scenes and then answer the following questions.

1. What mining actually is, i.e. what happens when a block is being mined?
2. What is the function of *nonce*?
3. When a block is considered to be valid and mined?
4. What do the other nodes do when they receive a new mined block from you?

5 Transactions

In this section, your task is to perform various transactions and observe in Wireshark and the source code what happens behind the scenes. Go to the `Make transaction` tab in the client web GUI. Fill in the requested information. Address means public key in this context. Try to make an invalid transaction and a valid transaction, which you then mine to the blockchain.

1. How does the blockchain network know that it was really this person that sent out the transaction?
2. How does the blockchain network know whether you have enough currency to perform the transaction?
3. Can you somehow find out how much currency anyone else has?

6 Double spending

In this section, you will perform double spending. On one of the PCs, make two transactions which both use all of your available currency. Submit one of them to the node running on the other PC (**Blockchain Node URL** in the confirmation dialog) and the other one to the node running on localhost.

Check that the transactions are going to be added to the next block in the miner web GUI on each PC by clicking the small blue button next to the *Transactions to be added to the next block* header. Mine the blocks on both of your PCs *at the same time*. Examine the resulting blockchains on your nodes.

1. What happened? What is this situation generally called?
2. How will this situation be resolved? What will happen to the other chain at that point?
3. What should be done to avoid negative consequences from situations like this?

Ask the teaching assistant to verify your results before starting to clean up.

7 Clean Up instructions

Simply shutdown both of the PCs you have used.