Sheet 3, WS 2018/19
Cryptocurrencies and Blockchain
Published 25.01.2019
Deadline 10.02.2019

Katinka Wolter
Larissa Zech
Inst. für Informatik
Freie Universität Berlin

Assignment. Ethereum Blockchain and Smart Contracts

The objective of this assignment is to gain some hands-on experience with the Ethereum blockchain and smart contracts. We have selected Ethereum rather than Bitcoin because this allows you to work with smart contracts which are much more powerful than simple transactions. We have decided against hyperledger and for Ethereum because hyperledger is much more complex and difficult to learn.

Below, you can find an explanation of how to use the private Ethereum blockchain number 1234 running on the ubuntu-PC rhea.imp.fu-berlin.de with IP address 160.45.38.66.

The objective of this assignment will be that you include a smart contract in the blockchain and issue some transactions that will run the smart contract.

You can either use a pre-fab smart contract, e.g. from the instructions at at Contract-Tutorial or Ethereum token, or you can modify the given examples or design your own smart contract which could for example make delayed payments.

You should submit the following:

1. a short text describing the functionality of your smart contract
2. your documented contract code
3. a specification of where your contract is on the blockchain (which block)
4. a specification of how your contract can be used
5. a documentation of your usage in at least one transaction, such that your transaction can be found on the blockchain.

You may make additional transactions or *play with the blockchain* in other ways. You can use a public test network as long as it is accessible to us, or you can use the private ethereum blockchain which we have set up.

Below is a description of how to use the private blockchain:

- each group will obtain an account, distributed during the lecture on Monday, 28th of January. The accounts are on a machine running ubuntu linux, so log in using

  ```
  ssh user<i>@rhea.imp.fu-berlin.de
  ```

  the initial password is `user<i>`. Please change the password upon your first login. We will check this and disable accounts with the original password on the 31st of January.

- you will find a script `startGeth.sh` which you should run to start your geth node.
- in a second terminal you should run `geth attach /home/user<i>/ethdata/geth.ipc` to start the geth console
- you will have access to one account, the public key of which is shown when you call `eth.coinbase` in the console.
- please generate a new account (which will not be your coinbase) using `personal.newAccount()` and store public key and password.
- your first transaction should transfer 1000 Ether from the coinbase account to your own new account. This will allow you to fuel later transactions with gas.

Our ethereum nodes are running on rhea, IP address 160.45.38.66 Ports 30301 and 30302.

Starting Monday evening, at least one of those nodes will be permanently mining, so you do not have to start a mining process for your transactions to propagate.

We do not know whether a full list of geth commands exists, but some information can be found here.

Remark: please note that geth1.7 turned out to be stable, while other versions are not, even if they are more recent. On rhea geth1.7 is preinstalled in /usr/bin and you should not download any other version of geth to your home directory.

For a bit of fun and on related matters I can recommend a Bitcoin explainer that has been generated using AI, i.e. it has been trained on other Bitcoin explainers.