Peer to Peer Systems and Blockchains
Academic Year 2019/2020
Final Term

Deadline June 5th 2020

The final term requires the solution of three assignments, one regarding the Bitcoin protocol, the second is the analysis of an Ethereum smart contract and the last requires the solution of an exercise on complex networks analysis.

1. Analysis of the Bitcoin protocol

1.a Use the **https://blockchain.info/** web site to interactively browse the Bitcoin blockchain and to solve the following questions

- examine **block number 351846** in the blockchain
    - how much in total did the miner who found this block receive for doing so?
    - locate the second transaction in this block (the one with transaction id 18b37c44...). How many inputs and outputs are there in this transaction? Give a likely explanation for why the two recipients do not receive the same amount.
        - to 6 decimal places, what is the total sum of the input for this transaction? What is the total sum of the output of this transaction? Why is there a difference?
        - What are the first 6 characters of the recipient who received the difference between the input and output for this transaction?
- examine **block number 351833** in the blockchain
    - what is odd about this block? Why do you think this occurred?
    - who owns the output address of the transaction with id 6848c…..?
    - look at all of the transactions that the miner who found that block has received. Roughly how much USD is this? How has this miner managed to win so many blocks? Describe how the miner has likely managed the rewards it received form all these transactions
    - how “hard” was the block to find? On average, how many nonces would the miners executing the PoW contemporary to the winning miner had to try before finding a satisfactory nonce?

1.b Answer the following questions

- name three typical spending conditions that are supported in Bitcoin.
- explain the three-step protocol used for exchanging new transactions/blocks in the Bitcoin P2P network.
- list at least 3 differences between Bitcoin's UTXO model and Ethereum's account-based model.
- what information is required to prove that a transaction is in a block? And how does a Bitcoin light client verify it?

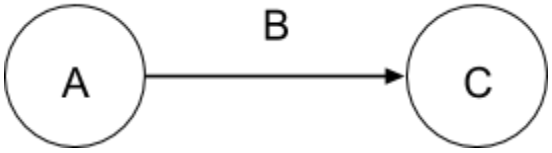
2. Pay eggs' supply chain with Ethereum smart contracts

This assignment requires you to analyze the usage of a smart contract on a simple supply chain scenario.
Every data stored on a smart contract cannot be censored, nor can be tampered. Therefore, a smart contract is suitable to be a source of trust between untrusted parties, such as the companies in the supply chain network. A company responsible for defections cannot hide the data necessary to solve conflicts (Non-Repudiation), and any party is always able to query the data (Auditability). However, we recall that a smart contract, once deployed on the network, cannot be modified (e.g. bug-fixed) and every writing operation costs the caller a fee.
The goal of this assignment consists of the assessment of the contract used by the supply chain scenario. In particular, the student needs to analyze the security issues and the cost, in gas, of the writing operations provided by the smart contract and, as consequence, the cost in fees for the companies in the scenario.

The supply chain scenario

Disclaimer: This procedure of payment does not make sense. The authors have no responsibilities if you use this contract on your company. If things go well please pay us a beer.

A consortium of companies agreed upon the utilization of the smart contract technology to track the shipment of eggs.
The consortium is composed of companies A, B and C. Eggs are produced and packed in boxes by A, and transported by B to company C.



The information of each egg box is stored in a smart contract (i.e. a smart contract per box).
The supply chain has this flow:

1. A produces the egg box, and assigns to a box an initial price, say 50€.

2. B buys the eggs from A at 50€ and wants to sell to C overpriced, say 75€. However, any bad condition influencing the egg box decreases the value of the box transported by B. For instance, every bump and every 5 minutes of temperature registered above a certain threshold decreases the price, say by 5€ and 3€ respectively as a penalty.
3. Once B reaches C, if the egg box has received enough "damage" such that the penalty is above a certain threshold, say 40€, C is allowed to reject the box of eggs; otherwise C pays B an amount equal to 75€ - (penalty).

Responsibilities of A:
After an egg box has been packed, A creates the related smart contract and deploys it on the Ethereum network.

Responsibilities of B:
After A's employee loads the egg box on B's truck, B pays X ether to A for the eggs with the smart contract, changing the status of the box in the contract from "READY" to "SHIPPING".
The shipment takes 8 hours to complete.
Each egg box has installed a set of sensors to monitor the status of the eggs during the shipment. The sensors monitor the Temperature and Bumps (e.g. with accelerometers), and produce a pair (temperature, bump) every 5 minutes[1] [2].

Responsibilities of C:
As soon as the truck reaches C, C invokes the smart contract to pay B. Based on the data stored by B the smart contract computes the amount of Ether C has to pay. If the eggs are acceptable by C, the contract pays B the proper amount (transporter price - penalty) and sets the status of the box in the contract from "SHIPPING" to "RECEIVED"; otherwise the payment will not be performed and the contract sets the status of the box in the contract from "SHIPPING" to "REFUSED". This action deactivates the contract.

Tasks

Given the zip file of the assignment, the student needs to answer to the following tasks:

1. Implement the missing portions of the *complete()* function. They need to pay the transporter and, eventually, refund the penalty to the receiver;
2. Evaluate the cost in gas of the functions provided by the smart contract;
3. Compute the fees to be paid by B to store the samples, *push_data()*, for a single shipment. Use a gas price suggested by the Ethereum gas station[3], and the current exchange Eth-Euro.
    a. Recall, the sensors produce a new pair of data (temperature, bump) every 5 minutes. The shipment lasts for 8 hours.
    b. You can evaluate the total fee whether B stores on the smart contract a new pair as soon it is produced, all the pairs only once, or a combination of the twos;

[1] This is a simplification. That value can be an aggregation of multiple samples sensed during these 5 minutes.
[2] Assume the sensors are trusted, they do not fail nor provide fake data.
[3] https://ethgasstation.info/

4. What are the security concerns to keep into consideration while developing a smart contract similar to this one? List the vulnerabilities that might arise. Use the provided articles, or any online resource.
    a. Is this contract correct, or does it present issues? (Vulnerabilities or even programming mistakes).

Files

The zip file of this assignment includes:

1. The file Box.sol: it provides the Box smart contract, where A is the **producer**, B is the **transporter** and C is the **receiver.** This contract has the complete() function not fully implemented;
2. The file PenaltyFunction.sol: it provides an abstract contract (a contract exposing a non implemented function) to compute the penalty of the input sensed data. The file includes two extensions computing the penalty using two different formulas;
3. The file test_data.json: it has a few input data to test the penalty functions;
4. A couple of articles about security concerns in Solidity.

3. Complex Network Analysis

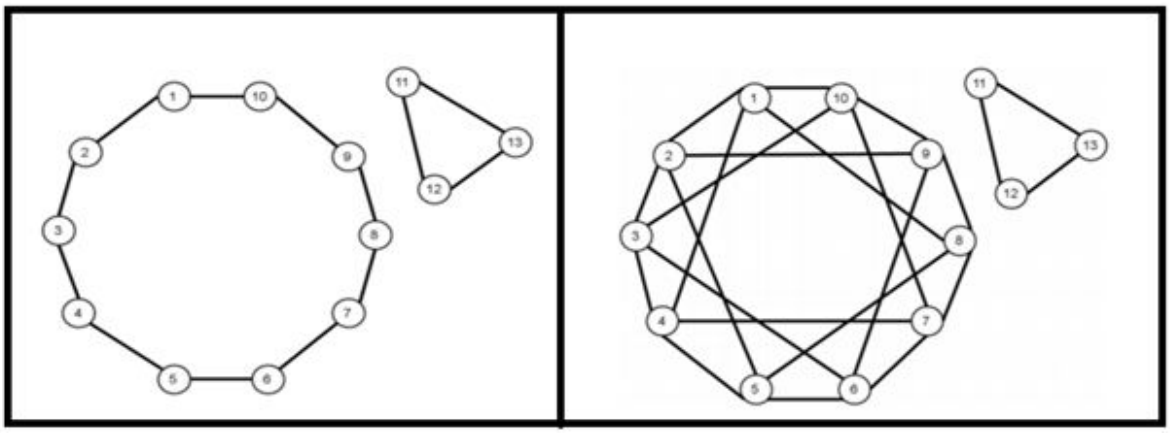


Figure 1. Two graph: differences

Compute the clustering coefficient, calculated as the average of the clustering coefficients of the single nodes of the graph, for the two graphs shown in Figure 1.

- what do you observe? Is the value of the clustering coefficient a good measure to characterize the structures of the graphs?
- describe a better way to characterize these structures.

The assignment must be done individually and its deadline is 5 June 2020. The assignment can be submitted even if the mid term has not been submitted/is not sufficient. If the evaluation of both the mid and of this final term will be positive, the student will be relieved from the oral exam. This assignment is not mandatory, if it is not presented/passed, the student will be required to pass the oral exam on the second part of the course. Submit a report including the solution of the three assignments, including also the code of the parts of the smart contract which have been modified.

Submit the assignment through Moodle. The evaluation of the assignment will be notified through Moodle. Post doubts/clarification requests on the Moodle page of the course.