Kulliyyah of Information and Communication Technology

CSC 4608 - Blockchain & Applications

Project: Part 1

Semester 1 2020/2021

Mohamad Faiq Bin Mohd Shahrul Munir 1718235
Ahmad Zaidan Bin Adnan 1718733

Instructor:
Prof. Dr. Norbik Bashah bin Idris

Introduction

In this project, we are required to write, compile, deploy a smart contract which assumes the basic role of a cryptocurrency regulator. Some examples of cryptocurrency regulators are Bank Negara, Central Bank and Securities Commission). A regulator must be able to detect suspicious transactions and the suspects involved, as well as report them.There are sets of functions that regulator need to take care of. In this project, there are 3 actors or parties that consist of regulator, depositor and withdrawer.

The workloads for this project are distributed evenly to get the best result. Ahmad Zaidan is the main person who worked with the code and did some part of project writing. Mohamad Faiq assists the code writing and the one who wrote the report.

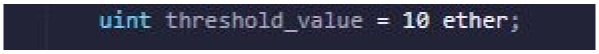
Project Code

For the project, we are using **solidity** and **remix** to code the smart contract. The full source codes are shown below.

```
pragma solidity ^0.5.8;

contract Regulator {

    mapping(address => uint) private balances;
    address public owner;

    event LogDeposit(address indexed _accountOwner, uint _amount);
    event LogWithdraw(address indexed _accountOwner, uint _amount);
    event LogSuspicious(address indexed _accountOwner, uint _amount);
    event LogMessage(address indexed _accountOwner, string _message);

    constructor() public payable {
        owner = msg.sender;
        balances[msg.sender] = 10 ether;
    }

    function set_threshold(uint value, uint balance) internal {
        uint threshold_value = 10 ether;

        if (value > threshold_value) {
            emit LogMessage(msg.sender, "Huge transaction is being made.");
        }

        if (balance > 50 ether) {
            emit LogMessage(msg.sender, "Suspicious activity in this smart contract.");
        }

         emit LogSuspicious(msg.sender, value);

    }

    function deposit(uint deposit_amount) public payable returns (uint) {
        balances[msg.sender] += deposit_amount;
        emit LogDeposit(msg.sender, deposit_amount);
        set_threshold(deposit_amount, balances[msg.sender]);
        return balances[msg.sender];
    }

    function withdraw(uint withdraw_amount) public returns (uint) {
        if (withdraw_amount <= balances[msg.sender]) {
            balances[msg.sender] -= withdraw_amount;
            emit LogWithdraw(msg.sender, withdraw_amount);
            set_threshold(withdraw_amount, balances[msg.sender]);
        }
        return balances[msg.sender];
    }

    function check_balance() public view returns (uint) {
        return balances[msg.sender];
    }

}
```

The screenshot of the requirements fulfillment is shown below.

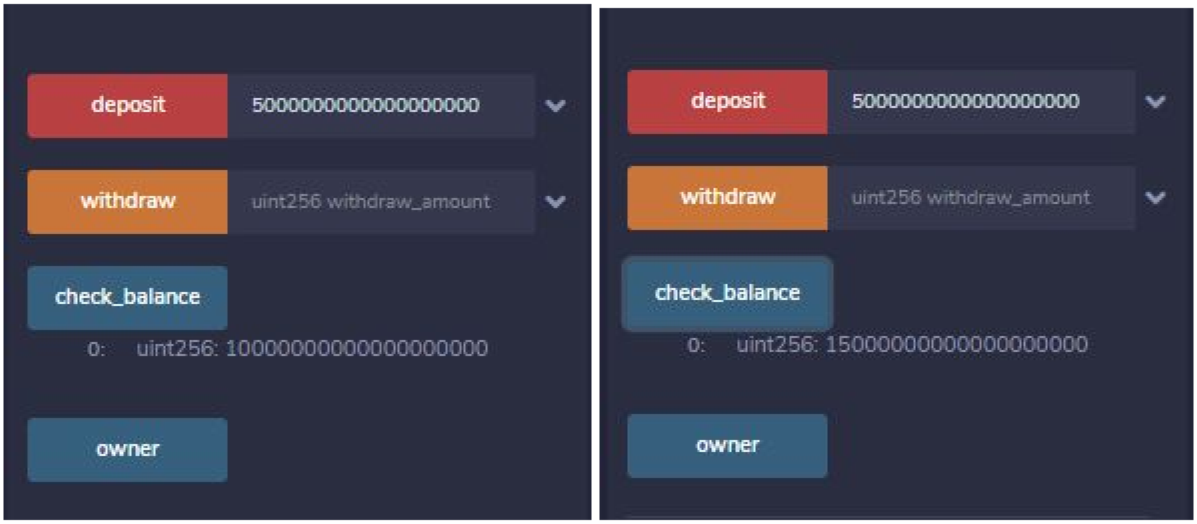
a. Set the Threshold value of the fund transacted. Example of latest threshold value = 10 Ether.



```
uint threshold_value = 10 ether;
```

Figure 1: Threshold value is set inside the set_threshold function.

b. A valid account holder may transact (deposit/withdraw) any amount of fund into/from the smart contract.



deposit 5000000000000000000

withdraw uint256 withdraw_amount

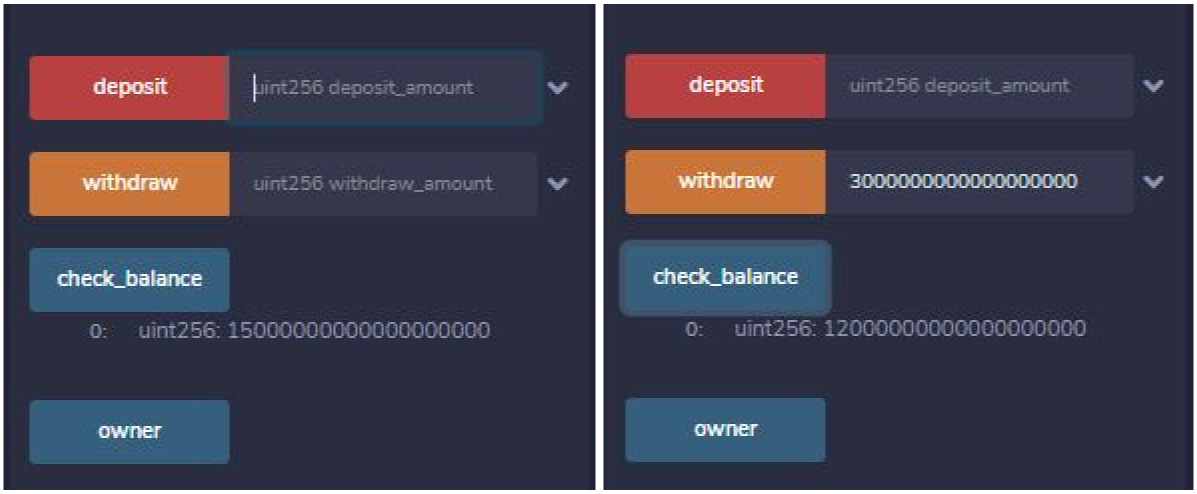
```
0:    uint256: 10000000000000000000
```

deposit 5000000000000000000

withdraw uint256 withdraw_amount

```
0:    uint256: 15000000000000000000
```

Figure 2: The deposit process of the transaction.



deposit uint256 deposit_amount

withdraw uint256 withdraw_amount

```
0:    uint256: 15000000000000000000
```

deposit uint256 deposit_amount

withdraw 3000000000000000000

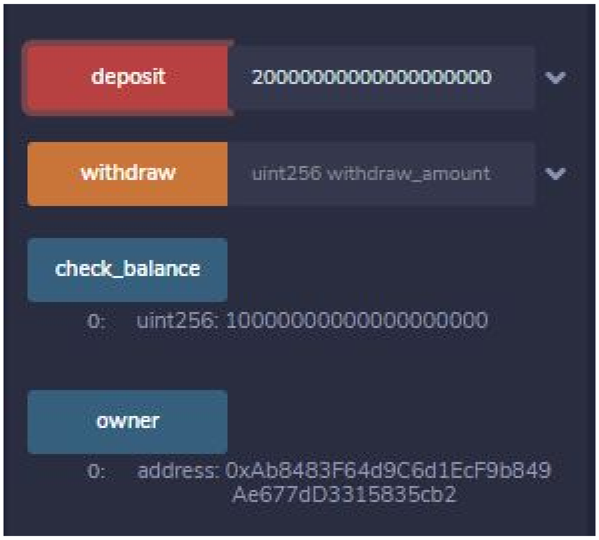
```
0:    uint256: 12000000000000000000
```

Figure 3: The withdrawal process of the transaction.

c. However, if the fund transacted is > the Threshold value set by Bank-Negara:

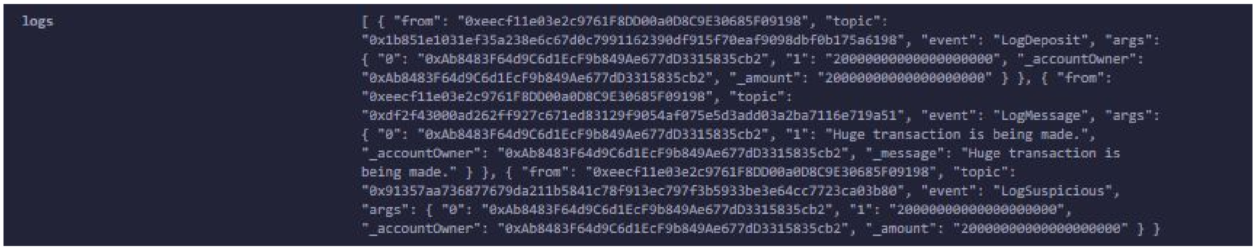
   i. An alert (ie message) must be raised to report such a huge transaction.

   ii. The alert must include the address of the Account involved, and the amount involved.



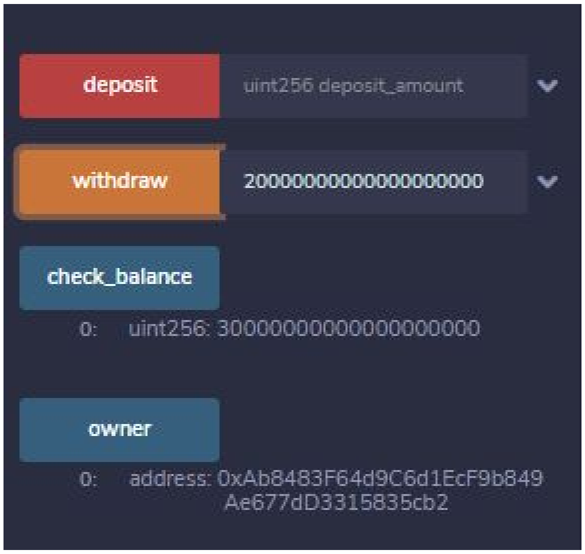
```
deposit        20000000000000000000
withdraw       uint256 withdraw_amount
check_balance
  0:   uint256: 10000000000000000000
owner
  0:   address: 0xAb8483F64d9C6d1EcF9b849
                Ae677dD3315835cb2
```

Figure 4: 20 ethers which is more than the threshold value is transferred into the smart contract.



```
[ { "from": "0xeecf11e03e2c9761F8DD00a0D8C9E30685F09198", "topic":
"0x1b851e1031ef35a238e6c67d0c7991162390df915f70eaf9098dbf0b175a6198", "event": "LogDeposit", "args":
{ "0": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2", "1": "20000000000000000000", "_accountOwner":
"0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2", "_amount": "20000000000000000000" } }, { "from":
"0xeecf11e03e2c9761F8DD00a0D8C9E30685F09198", "topic":
"0xdf2f43000ad262ff927c671ed83129f9054af075e5d3add03a2ba7116e719a51", "event": "LogMessage", "args":
{ "0": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2", "1": "Huge transaction is being made.",
"_accountOwner": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2", "_message": "Huge transaction is
being made." } }, { "from": "0xeecf11e03e2c9761F8DD00a0D8C9E30685F09198", "topic":
"0x91357aa736877679da211b5841c78f913ec797f3b5933be3e64cc7723ca03b80", "event": "LogSuspicious",
"args": { "0": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2", "1": "20000000000000000000",
"_accountOwner": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2", "_amount": "20000000000000000000" } }
```

Figure 5: The log alerts about the large transaction by mentioning the account address, the amount transacted and an alert message, “Huge transaction is being made.”



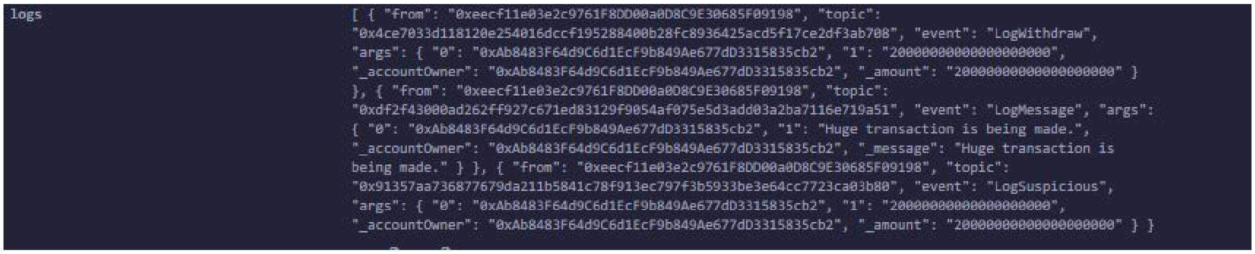
uint256 deposit_amount

20000000000000000000

0: uint256: 30000000000000000000

0: address: 0xAb8483F64d9C6d1EcF9b849
Ae677dD3315835cb2

Figure 6: 20 ethers which is more than the threshold value is being withdrawn from the smart contract.



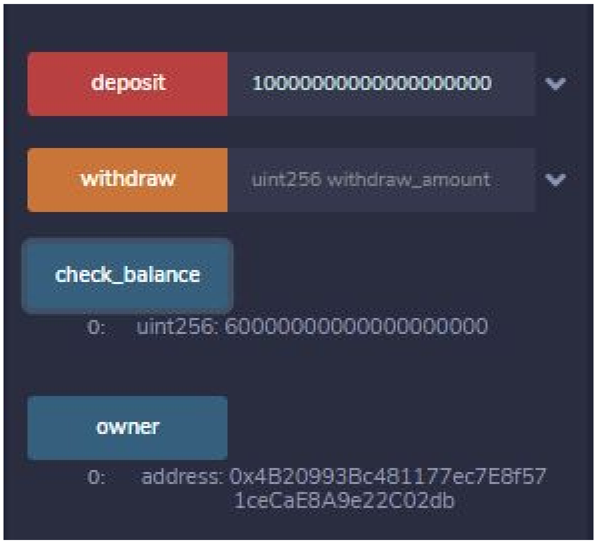
```
logs                                    [ { "from": "0xeecf11e03e2c9761F8DD00a0D8C9E30685F09198", "topic":
                                        "0x4ce7033d118120e254016dccf195288400b28fc8936425acd5f17ce2df3ab708", "event": "LogWithdraw",
                                        "args": { "0": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2", "1": "20000000000000000000",
                                        "_accountOwner": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2", "_amount": "20000000000000000000" }
                                        }, { "from": "0xeecf11e03e2c9761F8DD00a0D8C9E30685F09198", "topic":
                                        "0xdf2f43000ad262ff927c671ed83129f9054af075e5d3add03a2ba7116e719a51", "event": "LogMessage", "args":
                                        { "0": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2", "1": "Huge transaction is being made.",
                                        "_accountOwner": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2", "_message": "Huge transaction is
                                        being made." } }, { "from": "0xeecf11e03e2c9761F8DD00a0D8C9E30685F09198", "topic":
                                        "0x91357aa736877679da211b5841c78f913ec797f3b5933be3e64cc7723ca03b80", "event": "LogSuspicious",
                                        "args": { "0": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2", "1": "20000000000000000000",
                                        "_accountOwner": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2", "_amount": "20000000000000000000" } }
```

Figure 7: The log alerts about the large transaction by mentioning the account address, the amount transacted and an alert message, “Huge transaction is being made.”

d. At any time, after any successful transaction, if the balance of fund in the smart contract is more than 50 Ether, the Bank-Negara must also be alerted via an appropriate message that the smart contract may have been used as a place to launder cryptocurrency.

i. The Bank-Negara must be alerted of ALL the Account Holders which have deposited funds into the smart-contract (in real life these are suspects for money launderers).

ii. The Bank-Negara must be alerted of ALL the Account Holders which have withdrawn funds from the smart-contract (in real life these are also suspects for money launderers).



deposit 10000000000000000000

withdraw uint256 withdraw_amount

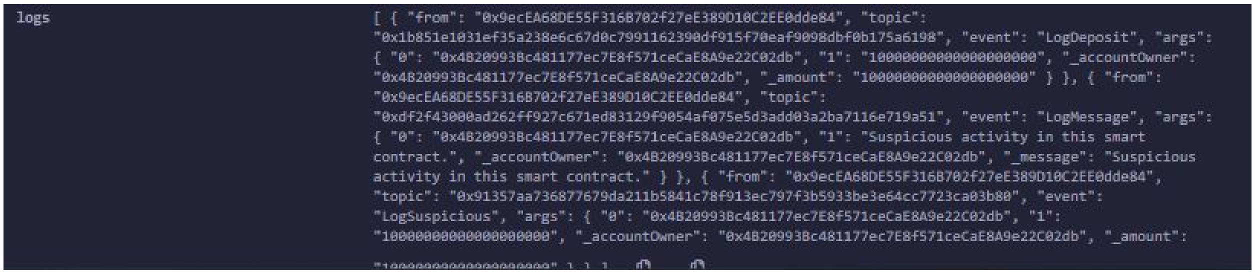
check_balance

0: uint256: 60000000000000000000

owner

0: address: 0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db

Figure 8: The remaining balances in the smart contract have reached more than 50 ethers.



logs

```
[ { "from": "0x9ecEA68DE55F316B702f27eE389D10C2EE0dde84", "topic":
"0x1b851e1031ef35a238e6c67d0c7991162390df915f70eaf9098dbf0b175a6198", "event": "LogDeposit", "args":
{ "0": "0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db", "1": "10000000000000000000", "_accountOwner":
"0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db", "_amount": "10000000000000000000" } }, { "from":
"0x9ecEA68DE55F316B702f27eE389D10C2EE0dde84", "topic":
"0xdf2f43000ad262ff927c671ed83129f9054af075e5d3add03a2ba7116e719a51", "event": "LogMessage", "args":
{ "0": "0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db", "1": "Suspicious activity in this smart
contract.", "_accountOwner": "0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db", "_message": "Suspicious
activity in this smart contract." } }, { "from": "0x9ecEA68DE55F316B702f27eE389D10C2EE0dde84",
"topic": "0x91357aa736877679da211b5841c78f913ec797f3b5933be3e64cc7723ca03b80", "event":
"LogSuspicious", "args": { "0": "0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db", "1":
"10000000000000000000", "_accountOwner": "0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db", "_amount":
"10000000000000000000" } } ]
```

Figure 9: The log alerts about the funds that have reached beyond the limit set by the regulator by mentioning the account address, the remaining balances and the alert message, “Suspicious activity in this smart contract.