

CST4125: Blockchain Development

Week: 22

Title: Case Study

Dr Ian Mitchell



smerf.net
Bedfordshire,
UK

January 2023

Contact and Office Hours

Contact Details

- Name: Dr Ian Mitchell
- Room: TG10
- Address: Middlesex University, Computer Science, London, NW4 4BT
- email: smerf.net

Contact and Office Hours

Contact Details

- Name: Dr Ian Mitchell
- Room: TG10
- Address: Middlesex University, Computer Science, London, NW4 4BT
- email: smerf.net

Office Hours

- During term time only
- When: Autumn Term: Mondays 1100-1300hrs
- Please read notifications or emails
- There are occasions that these could be arranged online, e.g., due to industrial action or inclement weather

Deadlines

Description	Submission	Weight	Deadline	Feedback	
				Formative	Summative
1. Hyperledger	MyLearning	50%	18 th December 2022	LW11-12	12/01/2023
2. Ethereum	MyLearning	50%	2 nd April 2023	LW23-24	24/04/2023
Resits	MyLearning	50-100%	1 st July 2023	None	None
Deferrals	MyLearning	50-100%	1 st July 2023	None	None

Lecture Objectives

- Web3
- ABI
-
-

Application Binary Interface

- Similar to API
- High-level of abstraction
- EVM - compiled to bytecode
- bytecode is:
 - stored on blockchain
 - associated with contract address
- Bytecode
 - parseable
 - precise/consistent
 - translatable
- ABI identifies the caller of the function
- Contract ABI is represented in JSON
- Clear spec. on encode and decoding a contract ABI
- Where:
../contracts/artifacts/*.js

Solidity Code

Raw

```
1 //SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.0;
3
4 contract simple{
5     uint public x;
6
7     function incrementX() public {
8         x++;
9     }
10
11    function decrementX() public {
12        x--;
13    }
14 }
```

smerf.net

CST4125:L22

March 1, 2023

6 / 23

ABI

Raw

```
7  "abi": [
8  {
9  "inputs": [],
10 "name": "decrementX",
11 "outputs": [],
12 "stateMutability": "nonpayable",
13 "type": "function"
14 },
15 {
16 "inputs": [],
17 "name": "incrementX",
18 "outputs": [],
19 "stateMutability": "nonpayable",
20 "type": "function"
21 },
22 {
23 "inputs": [],
24 "name": "x",
25 "outputs": [
26 {
27 "internalType": "uint256",
28 "name": "",
29 "type": "uint256"
30 }
31 ]
32 }
33 ]
```

smerf.net

CST4125:L22

March 1, 2023

7 / 23

ABI

- inputs: parameters
- outputs: returns
- type: function, constructor, fallback or receiver
- name: identity of function
- stateMutability: Mutability of function: pure, view, nonpayable or payable

smerf.net

CST4125:L22

March 1, 2023

8 / 23

Project

- ABI file associated with SC
- Address of smart contract
- `npx create-react-app simple`
- `truffle init`
- `truffle compile & quit`
- Generates ABI
- Open Ganache, add new project and enter ABI file
- Migrate, create a new file `2_simple.sol`
- `truffle migrate`

smerf.net

CST4125:L22

March 1, 2023

9 / 23

Simple.sol

```
1 //SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.0;
3
4 contract simple{
5     uint public x;
6
7     function incrementX() public {
8         x++;
9     }
10
11    function decrementX() public {
12        x--;
13    }
14 }
```

smerf.net

CST4125:L22

March 1, 2023

10 / 23

Migrate

```
1 const simple = artifacts.require("simple");
2
3 module.exports = function (deployer) {
4     deployer.deploy(simple);
5 };
```

smerf.net

CST4125:L22

March 1, 2023

11 / 23

Migrate



```
networks: {
  // Useful for testing. The 'development' name is special - truffle uses it by default
  // if it's defined here and no other network is specified at the command line.
  // You should run a client (like ganache-cli, geth or parity) in a separate terminal
  // tab if you use this network and you must also set the 'host', 'port' and '
  network_id'
  // options below to some value.
  //
  development: {
    host: "127.0.0.1",      // Localhost (default: none)
    port: 7545,            // Standard Ethereum port (default: none)
    network_id: "*",      // Any network (default: none)
  },
}
```

smerf.net

CST4125:L22

March 1, 2023

12 / 23

Web3.0/truffle setup



- [Web3.0 JS](#)
- Open Ganache simple project (linked to truffle-config.js)
- `truffle migrate`
- `truffle console`

smerf.net

CST4125:L22

March 1, 2023

13 / 23

Web3.0

Owner



```
1 owner = web3.eth.getCoinbase()
2 owner
3 <<owner address>>
```

smerf.net

CST4125:L22

March 1, 2023

14 / 23

Web3.0

Accounts



```
5 accounts = await web3.eth.getAccounts()
6 accounts
7 [
8   <<address>>,
9   <<address>>,
10  <<address>>,
11  <<address>>,
12  .
13  .
14  <<address>>
15 ]
```

smerf.net

CST4125:L22

March 1, 2023

15 / 23

Web3.0

Balance



```
17 web3.eth.getBalance(accounts[0])
18 <<balance>>
```

smerf.net

CST4125:L22

March 1, 2023

16 / 23

Web3.0

Current Provider



```
20 web3.eth.currentProvider
21 <<network details>>
```

smerf.net

CST4125:L22

March 1, 2023

17 / 23

Web3.0

Block Number



```
23 bn = await web3.eth.getBlockNumber()
24 bn
25 << Block Number >>
```

smerf.net

CST4125:L22

March 1, 2023

18 / 23

Web3.0

Solidity Function



```
27 simple = await simple.deployed()
28 simple.address
29 <<contract address>>
30 simple.abi
31 << abi >>
32 simple.incrementX()
33 simple.incrementX()
34 simple.decrementX()
35 simple.x()
```

smerf.net

CST4125:L22

March 1, 2023

19 / 23

Testing



- Chai Assertion Library

```
1
2 const Simple = artifacts.require('./simple.sol')
3
4 contract('Simple', (accounts) =>{
5   let simple
6
7   before(async () =>{
8     simple=await Simple.deployed();
9   })
10
11  describe('deployment', async () =>{
12    it('deploys successfully', async ()=>{
13      const address = await simple.address
14      assert.notEqual(address, 0x0)
15      assert.notEqual(address, '')
16      assert.notEqual(address, null)
17      assert.notEqual(address, undefined)
18    })
19
20    it('x has value', async ()=>{
21      const targetX = simple.x();
22      simple.incrementX();
23      simple.decrementX();
24      assert.notEqual(targetX, simple.x())
25    })
26  })
27 })
```

smerf.net

CST4125:L22

March 1, 2023

20 / 23

Summary



- React
- Solidity
- Web3

smerf.net

CST4125:L22

March 1, 2023

21 / 23

Reading



- Read Ch.2 in [1]

smerf.net

CST4125:L22

March 1, 2023

22 / 23

References I



- [1] Santiago Palladino. *Ethereum for Web Developers*. Springer, 2020.

smerf.net

CST4125:L22

March 1, 2023

23 / 23