

Lecture 25 - More on Solidity Contracts

Videos

<https://youtu.be/D9sFU0yLQ2A> - Lect-25-4010-5010-pt1.mp4

<https://youtu.be/CoVTXA6v4WQ> - Lect-25-4010-5010-pt2.mp4

<https://youtu.be/G6pF7X7o-vY> - Lect-25-4010-5010-pt3.mp4

From Amazon S3 - for download (same as youtube videos)

<http://uw-s20-2015.s3.amazonaws.com/Lect-25-4010-5010-pt1.mp4>

<http://uw-s20-2015.s3.amazonaws.com/Lect-25-4010-5010-pt2.mp4>

<http://uw-s20-2015.s3.amazonaws.com/Lect-25-4010-5010-pt3.mp4>

How Solidity Works

Get A Receipt

```
curl \
-H "Content-Type: application/json" \
-X POST \
--data '{"jsonrpc":"2.0", "method":"eth_getTransactionReceipt","params":\
    ["0x3f3aa792dd4a76d6feea51d57fc6543e97031cb4fb53e76642243eab0dfdb343"],"id":1}' \
http://192.168.0.199:8545/
```

Get an Account Balance

```
curl \
-H "Content-Type: application/json" \
-X POST \
--data '{"jsonrpc":"2.0", "method":"eth_getBalance", "params":[\
    "0x6ffba2d0f4c8fd7961f516af43c55fe2d56f6044", "latest"], "id":1}' \
http://192.168.0.199:8545
```

Unlock an Account

```
#!/bin/bash
```

```
# UTC--2018-03-11T01-56-42.511489695Z--9a6446d642d76a3ac1baf6c6d8c1e5179c58d87f
```

```
geth attach "http://192.154.97.75:8545/" <<XXxx
personal.unlockAccount( "0x9a6446d642d76a3ac1baf6c6d8c1e5179c58d87f", "xtwHdVIsKNFdM0cI
exit
XXxx
```

Storage & Events

A simple PayFor contract that will accept payments and create events.

```
1 pragma solidity >=0.4.21 <0.6.0;
2
3 import "openzeppelin-solidity/contracts/ownership/Ownable.sol";
4
5 contract PayFor is Ownable {
6
7     address payable owner_address;
8     event ReceivedFunds(address sender, uint256 value, uint256 application, uint256 l
9     event Withdrawn(address to, uint256 amount);
10
11     uint256 internal nPayments;
12     uint256 internal paymentID;
13
14     address[] private listOfPayedBy;
15     uint256[] private listOfPayments;
16     uint256[] private payFor;
17
18     mapping (address => uint256) internal totalByAccount;
19
20     constructor() public {
21         owner_address = msg.sender;
22         nPayments = 0;
23     }
24
25     function ReceiveFunds(uint256 forProduct) public payable returns(bool) {
26         nPayments++;
27         uint256 pos;
28         pos = listOfPayments.length;
29         listOfPayedBy.push(msg.sender);
30         listOfPayments.push(msg.value);
31         payFor.push(forProduct);
32         uint256 tot;
33         tot = totalByAccount[msg.sender];
```

```
34     totalByAccount[msg.sender] = tot + msg.value;
35     emit ReceivedFunds(msg.sender, msg.value, forProduct, pos);
36     return true;
37 }
38
39 function getNPayments() public onlyOwner payable returns(uint256) {
40     return ( nPayments );
41 }
42
43 function getPaymentInfo(uint256 n) public onlyOwner payable returns(address, uint
44     return ( listOfPayedBy[n], listOfPayments[n], payFor[n] );
45 }
46
47 function withdraw( uint256 amount ) public onlyOwner returns(bool) {
48     require(amount <= address(this).balance, "Insufficient funds for withdrawl");
49     address(owner_address).transfer(amount);
50     emit Withdrawn(owner_address, amount);
51     return true;
52 }
53
54 function getBalanceContract() public view onlyOwner returns(uint256){
55     return address(this).balance;
56 }
57 }
```

Testing for Contract

Dennis Ritchie: "Software that is not tested is broken."

Overview

1. How do you know that your results are correct?
2. What will testing tell you
3. What will it not tell you
4. Code Review
5. Testing and the real world
6. Different ways of testing
 1. Think Testing
 2. Unit Testing
 3. TDD - Test Driven Development
 4. Integration Testing
 5. Formally Proven

Solidity

```
1  pragma solidity >=0.4.21 <0.6.0;
2
3  import "truffle/Assert.sol";
4  import "truffle/DeployedAddresses.sol";
5  import "../contracts/PayFor.sol";
6
7  contract PayFor_Test {
8
9      PayFor token = new PayFor();
10
11      function testGetNPayments() public {
12          uint tmp = token.getNPayments();
13          Assert.equal(0, tmp, "No Payments Yet.");
14      }
15      function testGetBalanceContract() public {
16          uint tmp = token.getBalanceContract();
17          Assert.equal(0, tmp, "Random address has 0 tokens.");
18      }
19
20  }
```

Mocha / Web3 / JS

```
1
2  const PayFor = artifacts.require('./PayFor.sol');
3
4  contract('PayFor', function(accounts) {
5
6      let payForItem,
7          account_two = accounts[1];
8
9      beforeEach(async () => {
10          payForItem = await PayFor.new();
11      });
12
13      it("should pay for an item", async function() {
14          // event ReceivedFunds(address sender, uint256 value, uint256 application, uint
15          // emit ReceivedFunds(msg.sender, msg.value, forProduct, pos);
16          const ReceivedFunds = payForItem.ReceivedFunds();
17
18          await payForItem.ReceiveFunds( 42, {from: account_two, value:1000});
19          ReceivedFunds.get(function(error, result){
20              assert.equal(result[0].event, 'ReceivedFunds', "ReceivedFunds event should oc
21          });
22
23          var nPayments = await payForItem.getNPayments();
```

```
24     assert.equal(nPayments, 1, "Shoudl be 1 Payment Made.");
25
26     let [addr_to, amount, for] = await payForItem.getPaymentInfo(0);
27     assert.equal(amount, 1000, "Shoudl be 1000 Payed Made.");
28
29   });
30
31 });
```

Truffle Test

```
$ truffle test
```

Test Output

Using network 'development'.

```
Compiling ./contracts/PayFor.sol...
Compiling ./test/PayFor_Test.sol...
Compiling ./test/helpers/ThrowProxy.sol...
Compiling openzeppelin-solidity/contracts/ownership/Ownable.sol...
Compiling truffle/Assert.sol...
Compiling truffle/DeployedAddresses.sol...
```

PayFor_Test

- ✓ testGetNPayments (62ms)
- ✓ testGetBalanceContract (54ms)

Contract: PayFor

- ✓ should pay for an item (86ms)

3 passing (4s)