Understanding Smart Contracts

Jan-Erik Sandberg

COO

WWW.JAN-ERIK.COM

Making Smart Contracts

Write

Compile

Deploy

Interact

Solidity

```
contract MyContract
{
    uint myData;

    function setData(uint value)
    {
        myData = value;
    }

    function getData() returns (uint returnData)
    {
    return myData;
    }
}
```

Supported Data Types

bool

string

int/uint

int8 → int256

address

ufixed
ufixed8x8

Access Modifiers

public

internal

private

external

Basic Structure

```
contract HelloWorld
{
    string greeting;
    function Hello() public returns (string)
    {
        greeting= "Hello World!";
        return greeting ;
    }
}
```

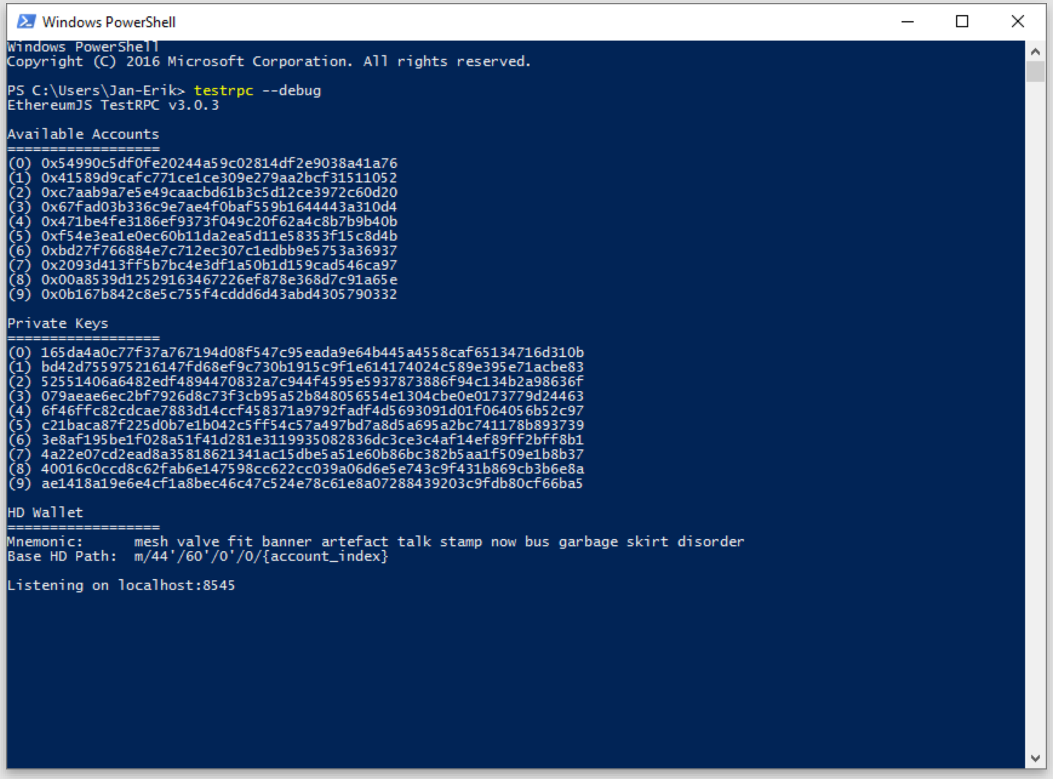
Truffle

Compile and build

Testing

Deployment

Interaction



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Jan-Erik> testrpc --debug
EthereumJS TestRPC v3.0.3

Available Accounts
==================
(0) 0x54990c5df0fe20244a59c02814df2e9038a41a76
(1) 0x41589d9cafc771ce1ce309e279aa2bcf31511052
(2) 0xc7aab9a7e5e49caacbd61b3c5d12ce3972c60d20
(3) 0x67fad03b336c9e7ae4f0baf559b1644443a310d4
(4) 0x471be4fe3186ef9373f049c20f62a4c8b7b9b40b
(5) 0xf54e3ea1e0ec60b11da2ea5d11e58353f15c8d4b
(6) 0xbd27f766884e7c712ec307c1edbb9e5753a36937
(7) 0x2093d413ff5b7bc4e3df1a50b1d159cad546ca97
(8) 0x00a8539d12529163467226ef878e368d7c91a65e
(9) 0x0b167b842c8e5c755f4cddd6d43abd4305790332

Private Keys
==================
(0) 165da4a0c77f37a767194d08f547c95eada9e64b445a4558caf65134716d310b
(1) bd42d755975216147fd68ef9c730b1915c9f1e614174024c589e395e71acbe83
(2) 52551406a6482edf4894470832a7c944f4595e5937873886f94c134b2a98636f
(3) 079aeae6ec2bf7926d8c73f3cb95a52b848056554e1304cbe0e0173779d24463
(4) 6f46ffc82cdcae7883d14ccf458371a9792fadf4d5693091d01f064056b52c97
(5) c21baca87f225d0b7e1b042c5ff54c57a497bd7a8d5a695a2bc741178b893739
(6) 3e8af195be1f028a51f41d281e3119935082836dc3ce3c4af14ef89ff2bff8b1
(7) 4a22e07cd2ead8a35818621341ac15dbe5a51e60b86bc382b5aa1f509e1b8b37
(8) 40016c0ccd8c62fab6e147598cc622cc039a06d6e5e743c9f431b869cb3b6e8a
(9) ae1418a19e6e4cf1a8bec46c47c524e78c61e8a07288439203c9fdb80cf66ba5

HD Wallet
==================
Mnemonic:      mesh valve fit banner artefact talk stamp now bus garbage skirt disorder
Base HD Path:  m/44'/60'/0'/0/{account_index}

Listening on localhost:8545
```

Test RPC

In-memory

Implements ethereumjs

Test Accounts

Demo

TestRPC

Truffle

Solidity Hello World

```
struct Person
{
    uint age;
    bool isCool;
    address accountAddress;
}
```

```
struct Parents
{
    Person father;
    Person mother;
}
```

Structs

Custom defined types

```
enum Gender { Male, Female, Non-Specified}
```

Enum

List of finite set of values.

```
string[] names;
Person[] persons;
Person[10] topTenAuthors;
topTenAuthors[3] = persons[5];
```

Arrays

Structure for grouping of elements

Data Locations

memory

storage

calldata

```
mapping(address => uint) public balances;

return balances[account.Address];
```

Mappings

Table of values

```
selfdestruct(msg.sender);

delete(objectArray);
```

Selfdestruct & delete

Killing a contract or deleting the content

```
throw();
```

Throwing Exceptions

Stop all operations and return unspent ether

Commenting

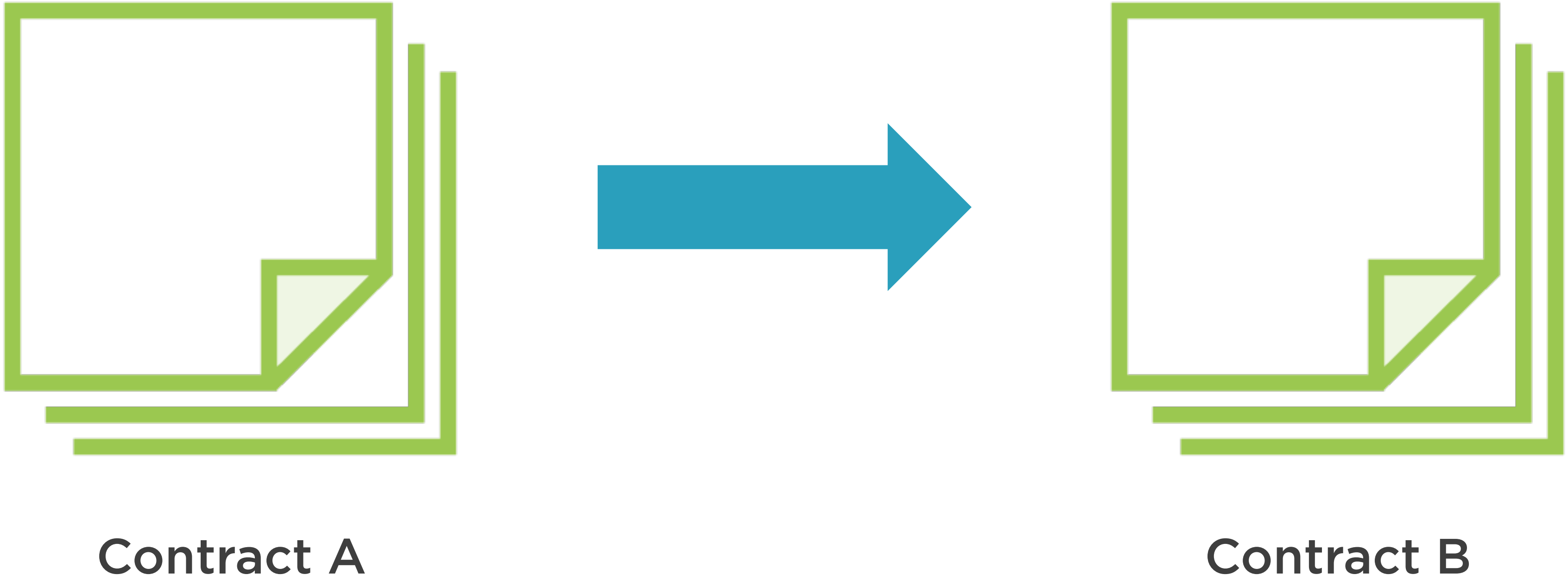
tspec comment

Demo

Simple contract for storage

Deploying to private Ethereum

Calling External Functions



Contract A

Contract B

Demo

Creating a second contract

Calling external contracts

Summary

Solidity basics

“Hello World”

Function contract

External contract