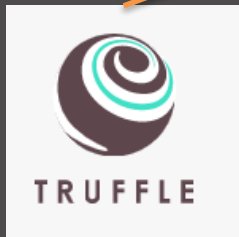


Ethereum Smartcontract

KoreaAerospaceUniv.
Su. H. Kim

Ethereum Pet Shop (EPS)

- 간단한 Dapp 예제
- Truffle을 이용하여 스마트컨트랙트 개발
- 애완동물의 분양 데이터가 블록체인에 기록



Setting up



- Node.js v6+ LTS and npm : <https://nodejs.org/en/>
- Git : <https://git-scm.com/>
- Ganache : <http://truffleframework.com/ganache/>
- Truffle
 - 명령 프롬프트 (windows → cmd → 우클릭 → 관리자 권한으로 실행)
 - > cd c:
 - > npm install -g truffle

```
C:\Users\neora>npm install -g truffle
C:\Users\neora\AppData\Roaming\npm\truffle -> C:\Users\neora\AppData\Roaming\npm\node_modules\truffle\build\cli.bundled.js
+ truffle@4.0.4
added 91 packages in 9.229s

C:\Users\neora>
```

Creating a New Truffle Project

- `>> mkdir pet-shop-tutorial`
- `>> cd pet-shop-tutorial`
- `>> truffle unbox pet-shop`

```
C:\Users\neora\pet-shop-tutorial>truffle unbox pet-shop
```

```
Downloading...
```

```
Unpacking...
```

```
Setting up...
```

```
Unbox successful. Sweet!
```

```
Commands:
```

```
  Compile:      truffle compile
```

```
  Migrate:      truffle migrate
```

```
  Test contracts: truffle test
```

```
  Run dev server: npm run dev
```

```
C:\Users\neora\pet-shop-tutorial>
```

> neora > pet-shop-tutorial >

- contracts
- migrations
- node_modules
- src
- test
- box-img-lg.png
- box-img-sm.png
- bs-config.json
- package.json
- package-lock.json
- truffle.js

Writing the Smart Contract



- contracts/ 폴더의 Migrations.sol 파일 내용 확인

```
pragma solidity ^0.5.0;
```

```
contract Migrations {  
    address public owner;  
    uint public last_completed_migration;
```

```
    modifier restricted() {  
        if (msg.sender == owner) _;  
    }
```

```
    function Migrations() {  
        owner = msg.sender;  
    }
```

```
    function setCompleted(uint completed) restricted {  
        last_completed_migration = completed;  
    }
```

```
    function upgrade(address new_address) restricted {  
        Migrations upgraded = Migrations(new_address);  
        upgraded.setCompleted(last_completed_migration);  
    }  
}
```

Writing the Smart Contract



- contracts/ 폴더에 **Adoption.sol** 파일 생성

```
pragma solidity ^0.5.0;
```

```
contract Adoption {
```

```
    address[16] public adopters;
```

// 각 강아지에 대한 입양자 명단

```
    function adopt(uint petId) public returns (uint) {
```

// 강아지 입양 신청 함수

```
        require(petId >= 0 && petId <= 15);
```

// index 확인

```
        adopters[petId] = msg.sender;
```

// 해당 강아지에 입양자 매칭

```
        return petId;
```

```
    }
```

```
    function getAdopters() public view returns (address[16] memory) {
```

```
        return adopters;
```

// 입양자 명단 확인 함수

```
    }
```

```
}
```

Compilation



- `>> truffle.cmd compile`

```
C:\Users\neora\pet-shop-tutorial>truffle.cmd compile
Compiling .\contracts\Adoption.sol...
Compiling .\contracts\Migrations.sol...

Compilation warnings encountered:

./C:/Users/neora/pet-shop-tutorial/contracts/Migrations.sol:11:3: Warning: No visibility specified. Defaulting to "public".
  function Migrations() {
  ^
Spanning multiple lines.
./C:/Users/neora/pet-shop-tutorial/contracts/Migrations.sol:15:3: Warning: No visibility specified. Defaulting to "public".
  function setCompleted(uint completed) restricted {
  ^
Spanning multiple lines.
./C:/Users/neora/pet-shop-tutorial/contracts/Migrations.sol:19:3: Warning: No visibility specified. Defaulting to "public".
  function upgrade(address new_address) restricted {
  ^
Spanning multiple lines.

Writing artifacts to .\build\contracts

C:\Users\neora\pet-shop-tutorial>
```

Migtaion



- migrations 폴더 아래 **2_deploy_contracts.js** 파일 생성

```
var Adoption = artifacts.require("Adoption");

module.exports = function(deployer) {
  deployer.deploy(Adoption);
};
```

- **truffle-config.js** 파일 수정

```
module.exports = {networks: {
  development: {
    host: "127.0.0.1",
    port: 8545,
    network_id: "*",
    gas: 3000000
  }
}
};
```


Migtaion

- Ganache 실행 (quick stark)

ACCOUNTS

BLOCKS

TRANSACTIONS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK0

GAS PRICE20000000000

GAS LIMIT6721975

NETWORK ID5777

RPC SERVERHTTP://127.0.0.1:7545

MINING STATUSAUTOMINING

MNEMONIC

candy maple cake sugar pudding cream honey rich smooth crumble sweet treat

HD PATH

m/44'/60'/0'/0/account_index

ADDRESS

0x627306090abaB3A6e1400e9345bC60c78a8BEf57

BALANCE

100.00 ETH

TX COUNT

0

INDEX

0

ADDRESS

0xf17f52151EbEF6C7334FAD080c5704D77216b732

BALANCE

100.00 ETH

TX COUNT

0

INDEX

1

ADDRESS

0xC5fdf4076b8F3A5357c5E395ab970B5B54098Fef

BALANCE

100.00 ETH

TX COUNT

0

INDEX

2

ADDRESS

0x821aEa9a577a9b44299B9c15c88cf3087F3b5544

BALANCE

100.00 ETH

TX COUNT

0

INDEX

3

ADDRESS

0x0d1d4e623D10F9FBA5Db95830F7d3839406C6AF2

BALANCE

100.00 ETH

TX COUNT

0

INDEX

4

Migration



- > truffle.cmd migrate
- 에러 발생시 > truffle.cmd migrate -reset 후 다시 시도

Migration

```
c:\pet-shop-tutorial>truffle.cmd migrate
```

```
Compiling your contracts...
```

```
> Everything is up to date, there is nothing to compile.
```

```
Starting migrations...
```

```
> Network name: 'development'  
> Network id: 910513  
> Block gas limit: 0x33edf4
```

```
1_initial_migration.js
```

```
Deploying 'Migrations'
```

```
> transaction hash: 0x240f6063f25741946e7e8acb71619874795e073ec0fc814a03cb71c9d5c518ca  
> Blocks: 0  
> contract address: 0xF10F1bDE9f83B4439547443EbF6Df603dC337676  
> block number: 83  
> block timestamp: 1558871242  
> account: 0x012B8Aeb9DeC52396622cbf6a091e3Dc80169673  
> balance: 415  
> gas used: 284908  
> gas price: 20 gwei  
> value sent: 0 ETH  
> total cost: 0.00569816 ETH
```

```
> Saving migration to chain.  
> Saving artifacts
```

```
> Total cost: 0.00569816 ETH
```

```
2_deploy_contracts.js
```

```
Deploying 'Adoption'
```

```
> transaction hash: 0x9cb95994a902b14c33e793638dd072b021cd5c715a  
> Blocks: 1  
> contract address: 0x781f989Ad34815C593b38C05BD0c63657440E71c  
> block number: 86  
> block timestamp: 1558871246  
> account: 0x012B8Aeb9DeC52396622cbf6a091e3Dc80169673  
> balance: 430  
> gas used: 253884  
> gas price: 20 gwei  
> value sent: 0 ETH  
> total cost: 0.00507768 ETH
```

```
> Saving migration to chain.  
> Saving artifacts
```

```
> Total cost: 0.00507768 ETH
```

```
Summary
```

```
> Total deployments: 2  
> Final cost: 0.01077584 ETH
```

Migration

- Balance and TX count must be changed

ACCOUNTS

BLOCKS

TRANSACTIONS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK
4

GAS PRICE
20000000000

GAS LIMIT
6721975

NETWORK ID
5777

RPC SERVER
HTTP://127.0.0.1:7545

MINING STATUS
AUTOMINING

MNEMONIC
candy maple cake sugar pudding cream honey rich smooth crumble sweet treat

HD PATH
m/44'/60'/0'/0'/account_index

ADDRESS
0x627306090abaB3A6e1400e9345bC60c78a8BEf57

BALANCE
99.94 ETH

TX COUNT
4

INDEX
0

ADDRESS
0xf17f52151EbEF6C7334FAD080c5704D77216b732

BALANCE
100.00 ETH

TX COUNT
0

INDEX
1

ADDRESS
0xC5fdf4076b8F3A5357c5E395ab970B5B54098Fef

BALANCE
100.00 ETH

TX COUNT
0

INDEX
2

ADDRESS
0x821aEa9a577a9b44299B9c15c88cf3087F3b5544

BALANCE
100.00 ETH

TX COUNT
0

INDEX
3

Migration

Ganache						
ACCOUNTS BLOCKS TRANSACTIONS LOGS						
SEARCH FOR BLOCK NUMBERS OR TX HASHES						
CURRENT BLOCK 4	GAS PRICE 20000000000	GAS LIMIT 6721975	NETWORK ID 5777	RPC SERVER HTTP://127.0.0.1:7545	MINING STATUS AUTOMINING	
BLOCK 4	MINED ON 2018-04-26 16:40:28				GAS USED 26981	1 TRANSACTION
BLOCK 3	MINED ON 2018-04-26 16:40:28				GAS USED 246374	1 TRANSACTION

ACCOUNTS

BLOCKS

TRANSACTIONS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK

4

GAS PRICE

20000000000

GAS LIMIT

6721975

NETWORK ID

5777

RPC SERVER

HTTP://127.0.0.1:7545

MINING STATUS

AUTOMINING

TX HASH

0x917e9ac5c27d7abb7a1bdb007c3061eadd4e7e2eb3189a5f4cda680eef386b9

CONTRACT CALL

FROM ADDRESS

0x627306090abab3a6e1400e9345bc60c78a8bef57

TO CONTRACT ADDRESS

0x8cdf0cd259887258bc13a92c0a6da92698644c0

GAS USED

26981

VALUE

0

TX HASH

0x1b853dfe98a6d12842bcf10bcd4323580f78174a2447ad810b48b784995c83c

CONTRACT CREATION

FROM ADDRESS

0x627306090abab3a6e1400e9345bc60c78a8bef57

CREATED CONTRACT ADDRESS

0xf12b5dd4ead5f743c6baa640b0216200e89b60da

GAS USED

246374

VALUE

0

TX HASH

0xd7bc86d31bee32fa3988f1c1eabc403a1b5d570340a3a9cda53a472ee8c956

CONTRACT CALL

FROM ADDRESS

0x627306090abab3a6e1400e9345bc60c78a8bef57

TO CONTRACT ADDRESS

0x8cdf0cd259887258bc13a92c0a6da92698644c0

GAS USED

41981

VALUE

0

TX HASH

0x55e9b7fb2d104ec4ed4ab6b28060942063e81c2133ec90bfff178418146523e50

CONTRACT CREATION

FROM ADDRESS

0x627306090abab3a6e1400e9345bc60c78a8bef57

CREATED CONTRACT ADDRESS

0x8cdf0cd259887258bc13a92c0a6da92698644c0

GAS USED

269607

VALUE

0

Testing



- Create a new file named 'TestAdoption.sol' in the test\ directory

```
pragma solidity ^0.4.17;
```

```
import "truffle/Assert.sol";
```

```
import "truffle/DeployedAddresses.sol";
```

```
import "../contracts/Adoption.sol";
```

```
contract TestAdoption {
```

```
    Adoption adoption = Adoption(DeployedAddresses.Adoption());
```

// add the code of following slide hear

```
}
```

Testing – adopt() function



- Recall the upon success it returns the given petId

```
function testUserCanAdoptPet() public {  
    uint returnedId = adoption.adopt(8);  
  
    uint expected = 8;  
  
    Assert.equal(returnedId, expected, "Adoption of pet ID 8 should be recorded.");  
}
```

Testing – retrieval of single owner



- Retrieve the address stored by adoption test above

```
function testGetAdopterAddressByPetId() public {  
    // Expected owner is this contract  
    address expected = this;  
  
    address adopter = adoption.adopters(8);  
  
    Assert.equal(adopter, expected, "Owner of pet ID 8 should be recorded.");  
}
```


Testing – retrieval of all owner



- Getter for the entire array

```
function testGetAdopterAddressByPetIdInArray() public {  
    // Expected owner is this contract  
    address expected = this;  
  
    // Store adopters in memory rather than contract's storage  
    address[16] memory adopters = adoption.getAdopters();  
  
    Assert.equal(adopters[8], expected, "Owner of pet ID 8 should be recorded.");  
}
```

Testing



- >> truffle.cmd test

```
C:\Users\Suhan\pet-shop-tutorial>truffle.cmd test
Using network 'development'.

Compiling .\contracts\Adoption.sol...
Compiling .\test\TestAdoption.sol...
Compiling truffle\Assert.sol...
Compiling truffle\DeployedAddresses.sol...

TestAdoption
  ✓ testUserCanAdoptPet (63ms)
  ✓ testGetAdopterAddressByPetId (52ms)
  ✓ testGetAdopterAddressByPetIdInArray (128ms)

3 passing (659ms)

C:\Users\Suhan\pet-shop-tutorial>_
```

- Ganache에 추가로 만들어진 TX이 보임

Creating UI

- Open \src\js\app.js (워드패드)

```
1 App = {
2   web3Provider: null,
3   contracts: {},
4
5   init: function() {
6     // Load pets.
7     $.getJSON('../pets.json', function(data) {
8       var petsRow = $('#petsRow');
9       var petTemplate = $('#petTemplate');
10
11     for (i = 0; i < data.length; i++) {
12       petTemplate.find('.panel-title').text(data[i].name);
13       petTemplate.find('img').attr('src', data[i].picture);
14       petTemplate.find('.pet-breed').text(data[i].breed);
15       petTemplate.find('.pet-age').text(data[i].age);
16       petTemplate.find('.pet-location').text(data[i].location);
17       petTemplate.find('.btn-adopt').attr('data-id', data[i].id);
18
19       petsRow.append(petTemplate.html());
20     }
21   });
22
23   return App.initWeb3();
24 },
25
26 initWeb3: function() {
27   /*
28    * Replace me...
29    */
30
31   return App.initContract();
32 },
33
34 initContract: function() {
35   /*
36    * Replace me...
37    */
38
39   return App.bindEvents();
40 },
```

```
41
42 bindEvents: function() {
43   $(document).on('click', '.btn-adopt', App.handleAdopt);
44 },
45
46 markAdopted: function(adopters, account) {
47   /*
48    * Replace me...
49    */
50 },
51
52 handleAdopt: function(event) {
53   event.preventDefault();
54
55   var petId = parseInt($(event.target).data('id'));
56
57   /*
58    * Replace me...
59    */
60 }
61
62 };
63
64 $(function() {
65   $(window).load(function() {
66     App.init();
67   });
68 });
69
```

Creating UI – initWeb3



```
if (window.ethereum) {  
  App.web3Provider = window.ethereum;  
  try {  
    await window.ethereum.enable();  
  } catch (error) {  
    console.error("User denied account access")  
  }  
}  
  
else if (window.web3) {  
  App.web3Provider = window.web3.currentProvider;  
}  
  
else {  
  App.web3Provider = new Web3.providers.HttpProvider('http://localhost:7545');  
}  
  
web3 = new Web3(App.web3Provider);
```

Creating UI – initContract



```
$.getJSON('Adoption.json', function(data) {  
  
  var AdoptionArtifact = data;  
  App.contracts.Adoption = TruffleContract(AdoptionArtifact);  
  App.contracts.Adoption.setProvider(App.web3Provider);  
  
  // Use our contract to retrieve and mark the adopted pets  
  return App.markAdopted();  
});
```

Creating UI – markAdopted



```
var adoptionInstance;
App.contracts.Adoption.deployed().then(function(instance) {
  adoptionInstance = instance;
  return adoptionInstance.getAdopters.call();
}).then(function(adopters) {

  for (i = 0; i < adopters.length; i++) {
    if (adopters[i] !== '0x0000000000000000000000000000000000000000') {
      $('panel-pet').eq(i).find('button').text('Success').attr('disabled',true);
    }
  }
}).catch(function(err) {
  console.log(err.message);
});
```

Creating UI – hadnleAdopt



```
var adoptionInstance;
web3.eth.getAccounts(function(error, accounts) {
  if (error) {
    console.log(error);
  }
  var account = accounts[0];
  App.contracts.Adoption.deployed().then(function(instance) {
    adoptionInstance = instance;
    return adoptionInstance.adopt(petId, {from: account});
  }).then(function(result) {
    return App.markAdopted();
  }).catch(function(err) {
    console.log(err.message);
  });
});
```

dapp 실행



- Add Metamask to Chrome : <https://metamask.io/>



메타마스크 Beta에 오신 것을 환영합니다

메타마스크는 이더리움을 위한 안전한 저장소입니다.
We're happy to see you.

시작하기

메타마스크를 처음 사용하시나요?



아니요, 이미 시드 구문을 가지고 있습니다.

12개 단어로 구성된 시드 구문으로 이미 만들어진 지갑을 가져오기

지갑 가져오기



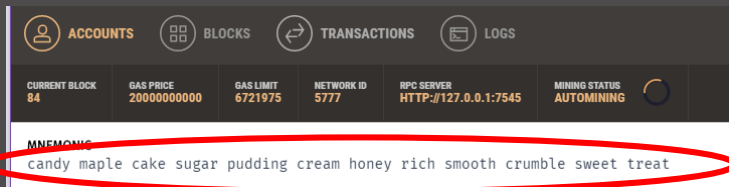
네, 설정해볼게요!

새로운 지갑과 시드 구문을 생성

지갑 생성하기

MetaMask

- 시드 구문으로 계정 가져오기



시드 구문으로 계정 가져오기

12개 단어로 구성된 비밀 구문을 입력하여 저장소를 복구하세요.

지갑 시드값

sa disorder strong palm list actual roast
yo sick inject truly blur

새 비밀번호 (최소 8자 이상)

비밀번호 확인

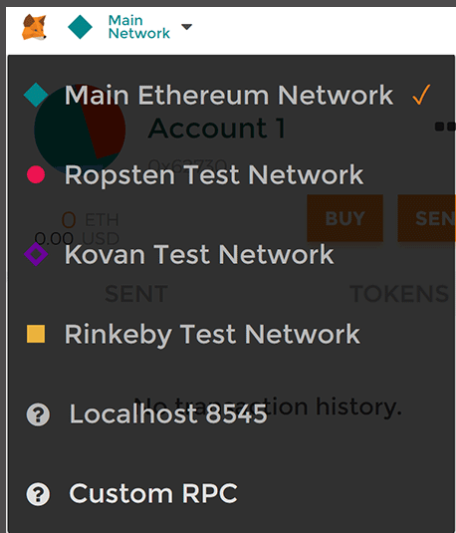


I have read and agree to the [Terms of Use](#)

가져오기

MetaMask

- 이더리움 메인넷에서 Custom RPC 로 네트워크 변경
- Set network as private local test server



General

네트워크

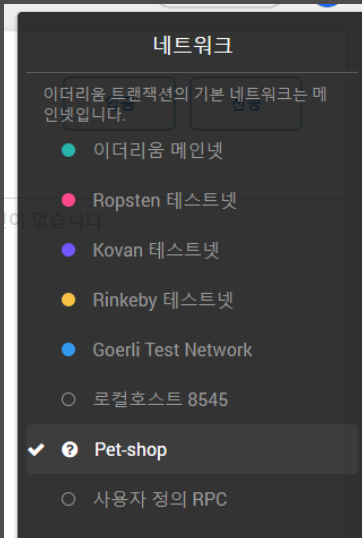
[Add Network](#)

<input checked="" type="radio"/> 이더리움 메인넷	Network Name <input type="text" value="Pet-shop"/>
<input type="radio"/> Ropsten 테스트넷	New RPC URL <input type="text" value="HTTP://127.0.0.1:7545"/>
<input type="radio"/> Kovan 테스트넷	ChainID (선택) <input type="text"/>
<input type="radio"/> Rinkeby 테스트넷	Symbol (선택) <input type="text"/>
<input type="radio"/> 로컬호스트 8545	Block Explorer URL (optional) <input type="text"/>
<input type="radio"/> Pet-shop	

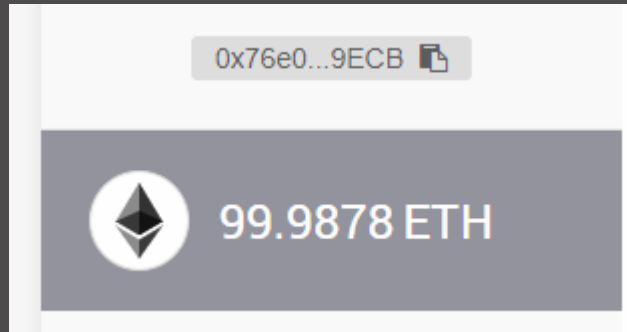
[저장](#)

MetaMask

- Now MetaMask interact with Ganache
- You have get some ETH



ADDRESS	BALANCE
0x76e0D40C6215a459Da0BAEbeD4608fe7DD7c9ECB	99.99 ETH



Pet Shop 실행

>> npm run dev

Pete's Pet Shop

Frieda



Breed: Scottish Terrier
Age: 3
Location: Lisoo, Alabama

Adopt

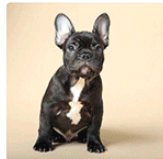
Gina



Breed: Scottish Terrier
Age: 3
Location: Tooleville, West Virginia

Adopt

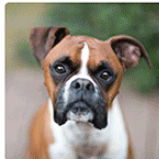
Collins



Breed: French Bulldog
Age: 2
Location: Freeburn, Idaho

Adopt

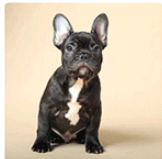
Melissa



Breed: Boxer
Age: 2
Location: Camas, Pennsylvania

Adopt

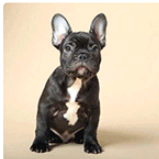
Jeanine



Breed: French Bulldog
Age: 2
Location: Gerber, South Dakota

Adopt

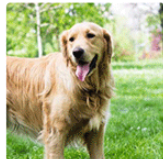
Elvia



Breed: French Bulldog
Age: 3
Location: Innsbrook, Illinois

Adopt

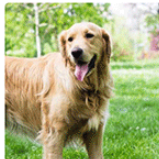
Latisha



Breed: Golden Retriever
Age: 3
Location: Soudan, Louisiana

Adopt

Coleman



Breed: Golden Retriever
Age: 3
Location: Jacksonwald, Palau

Adopt

Nichole

Fran

Leonor

Dean

CONFIRM TRANSACTION

Private Network

Account 1

627306...EF57
99.941 ETH
28867.07 USD



345cA3...3e10

Amount

0 ETH
0.00 USD

Gas Limit

63162 UNITS

Gas Price

20 GWEI

Max Transaction Fee

0.001263 ETH
0.36 USD

Max Total

0.001263 ETH
0.36 USD

Data included: 36 bytes

RESET

SUBMIT

REJECT

A close-up photograph of a computer keyboard. A single, ornate golden key is placed on the 'Enter' key, which is marked with a white arrow pointing to the right. The key is positioned diagonally across the frame, with its head resting on the 'Enter' key and its shaft extending towards the top left. The keyboard keys are dark grey or black, and the lighting creates highlights on the keys and the golden key.

[illegible]

Adopt

Breed: Boxer
Age: 2
Location: Camas, Pennsylvania

Success



THANK YOU
FOR YOUR ATTENTION