network security
system design Lab.

Ethereum Smartcontract

KoreaAerospaceUniv.
Su. H. Kim

Ethereum Pet Shop (EPS)

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

TRUFFLE

ethereum

Setting up

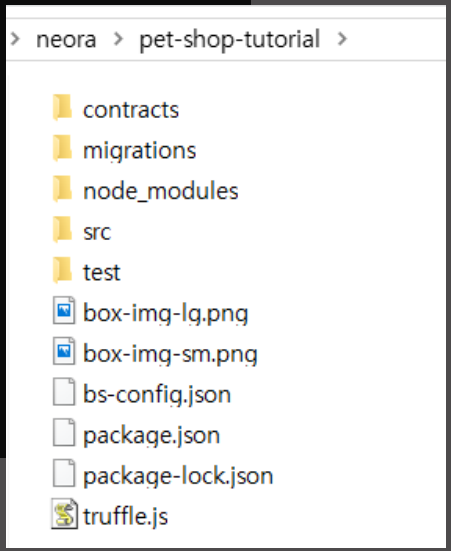
- Node.js v6+ LTS and npm : https://nodejs.org/en/
- Git : https://git-scm.com/
- Ganache : http://truffleframework.com/ganache/
- Truffle
  - 명령 프롬프트 (windows → cmd → 우클릭 → 관리자 권한으로 실행)
  > cd c:
  > npm install –g truffle

```
C:₩Users₩neora>npm install -g truffle
C:₩Users₩neora₩AppData₩Roaming₩npm₩truffle -> C:₩Users₩neora₩AppData₩Roaming₩npm₩node_mod
ules₩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>
```



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 sp
ecified. Defaulting to "public".
  function Migrations() {
  ^

Spanning multiple lines.
,/C/Users/neora/pet-shop-tutorial/contracts/Migrations.sol:15:3: Warning: No visibility s
pecified. 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 s
pecified. 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

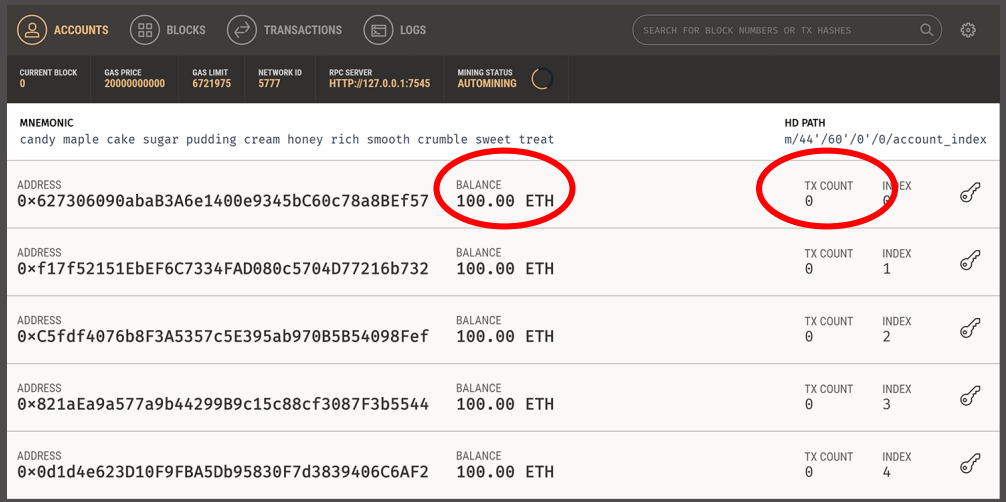
```
var Adoption = artifacts.require("Adoption");

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)



Migration

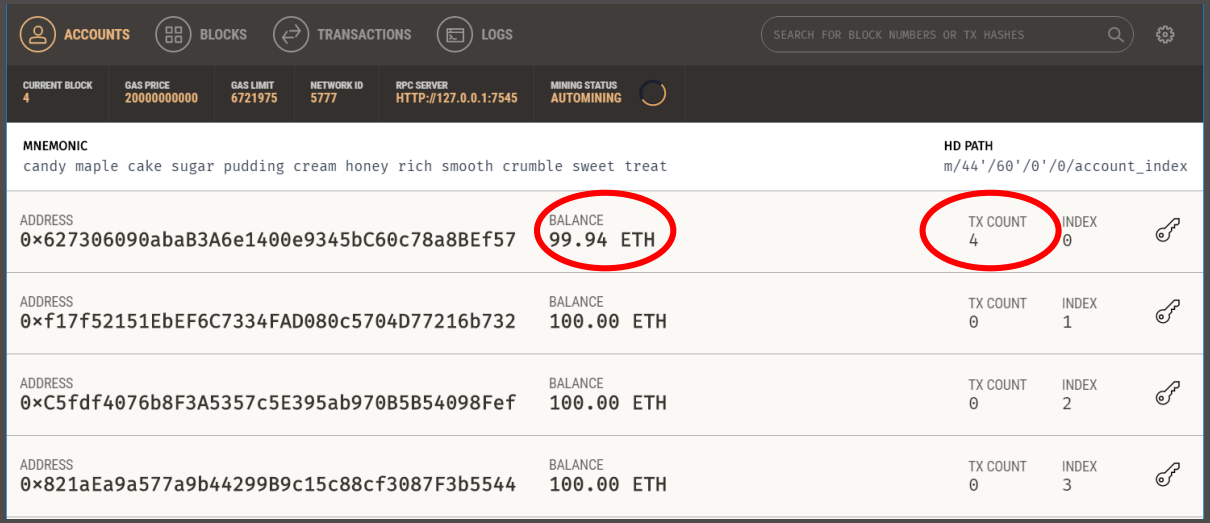
- > truffle.cmd migrate
- 에러 발생시 > truffle.cmd migrate –reset 후 다시 시도

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            Seconds: 8
   > 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            Seconds: 4
   > 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



Migration

Ganache

ACCOUNTS | BLOCKS | TRANSACTIONS | LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK	GAS PRICE	GAS LIMIT	NETWORK ID	RPC SERVER	MINING STATUS
4	20000000000	6721975	5777	HTTP://127.0.0.1:7545	AUTOMINING

BLOCK	MINED ON	GAS USED	
4	2018-04-26 16:40:28	26981	1 TRANSACTION
3	2018-04-26 16:40:28	246374	1 TRANSACTION
2	2018-04-26 16:40:27		
1	2018-04-26 16:40:27		
0	2018-04-26 16:39:34		

ACCOUNTS | BLOCKS | TRANSACTIONS | LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK	GAS PRICE	GAS LIMIT	NETWORK ID	RPC SERVER	MINING STATUS
4	20000000000	6721975	5777	HTTP://127.0.0.1:7545	AUTOMINING

TX HASH
0×917e9ac5c27d7abb7a1bdbc007c3061eadd4e7e2eb3189a5f4cda680eef386b9 — CONTRACT CALL

FROM ADDRESS	TO CONTRACT ADDRESS	GAS USED	VALUE
0×627306090abab3a6e1400e9345bc60c78a8bef57	0×8cdaf0cd259887258bc13a92c0a6da92698644c0	26981	0

TX HASH
0×1b853dfe98a6d12842bcf10bcdf4323580f78174a2447ad810b48b784995c83c — CONTRACT CREATION

FROM ADDRESS	CREATED CONTRACT ADDRESS	GAS USED	VALUE
0×627306090abab3a6e1400e9345bc60c78a8bef57	0×f12b5dd4ead5f743c6baa640b0216200e89b60da	246374	0

TX HASH
0×d7bc86d31bee32fa3988f1c1eabce403a1b5d570340a3a9cdba53a472ee8c956 — CONTRACT CALL

FROM ADDRESS	TO CONTRACT ADDRESS	GAS USED	VALUE
0×627306090abab3a6e1400e9345bc60c78a8bef57	0×8cdaf0cd259887258bc13a92c0a6da92698644c0	41981	0

TX HASH
0×55e9b7fb2d104ec4ed4ab6b28060942063e81c2133ec90bff178418146523e50 — CONTRACT CREATION

FROM ADDRESS	CREATED CONTRACT ADDRESS	GAS USED	VALUE
0×627306090abab3a6e1400e9345bc60c78a8bef57	0×8cdaf0cd259887258bc13a92c0a6da92698644c0	269607	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 – retriecal 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 – retriecal 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)

```
App = {
  web3Provider: null,
  contracts: {},

  init: function() {
    // Load pets.
    $.getJSON('../pets.json', function(data) {
      var petsRow = $('#petsRow');
      var petTemplate = $('#petTemplate');

      for (i = 0; i < data.length; i ++) {
        petTemplate.find('.panel-title').text(data[i].name);
        petTemplate.find('img').attr('src', data[i].picture);
        petTemplate.find('.pet-breed').text(data[i].breed);
        petTemplate.find('.pet-age').text(data[i].age);
        petTemplate.find('.pet-location').text(data[i].location);
        petTemplate.find('.btn-adopt').attr('data-id', data[i].id);

        petsRow.append(petTemplate.html());
      }
    });

    return App.initWeb3();
  },

  initWeb3: function() {
    /*
     * Replace me...
     */

    return App.initContract();
  },

  initContract: function() {
    /*
     * Replace me...
     */

    return App.bindEvents();
  },

  bindEvents: function() {
    $(document).on('click', '.btn-adopt', App.handleAdopt);
  },

  markAdopted: function(adopters, account) {
    /*
     * Replace me...
     */
  },

  handleAdopt: function(event) {
    event.preventDefault();

    var petId = parseInt($(event.target).data('id'));

    /*
     * Replace me...
     */
  }

};

$(function() {
  $(window).load(function() {
    App.init();
  });
});
```

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

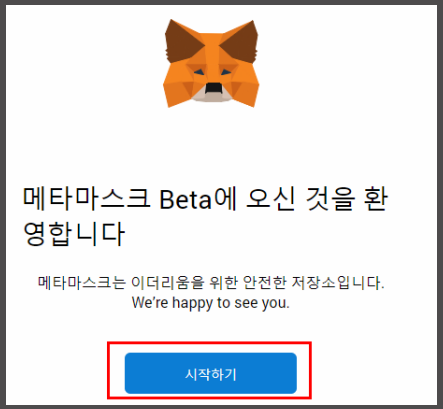

```
var adoptionInstance;
App.contracts.Adoption.deployed().then(function(instance) {
   adoptionInstance = instance;
   return adoptionInstance.getAdopters.call();
}).then(function(adopters) {

 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);
});
```

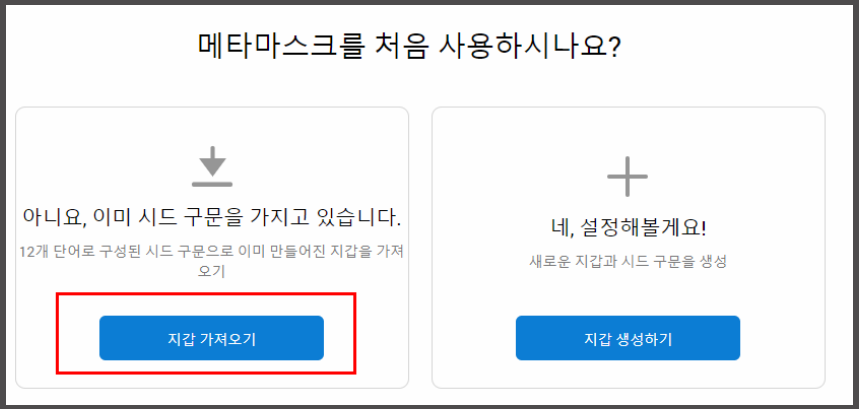
Creating UI – hadnleAdopt


```
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

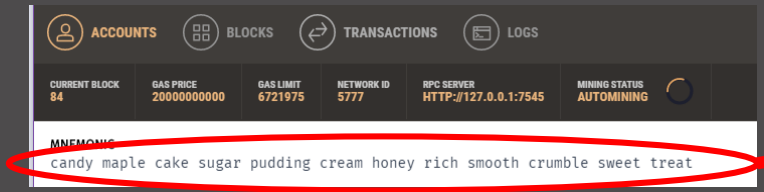
- Add Metamask to Chrome : https://metamask.io/

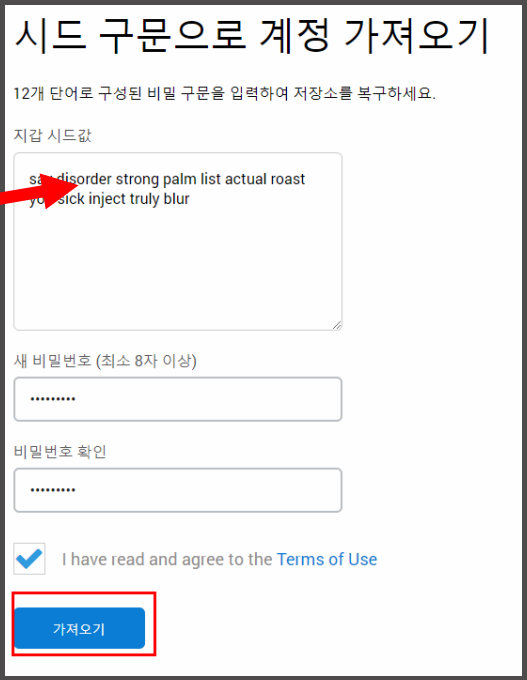




MetaMask

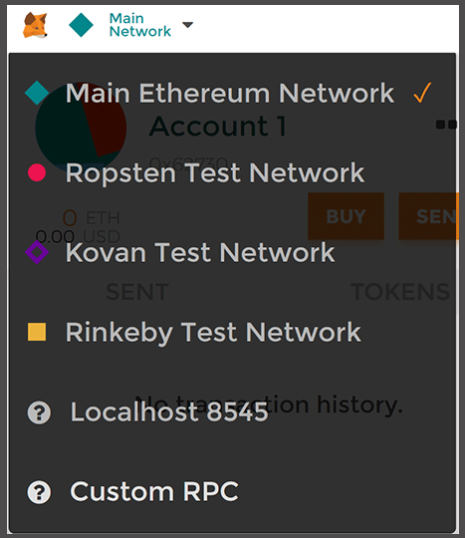
- 시드 구문으로 계정 가져오기

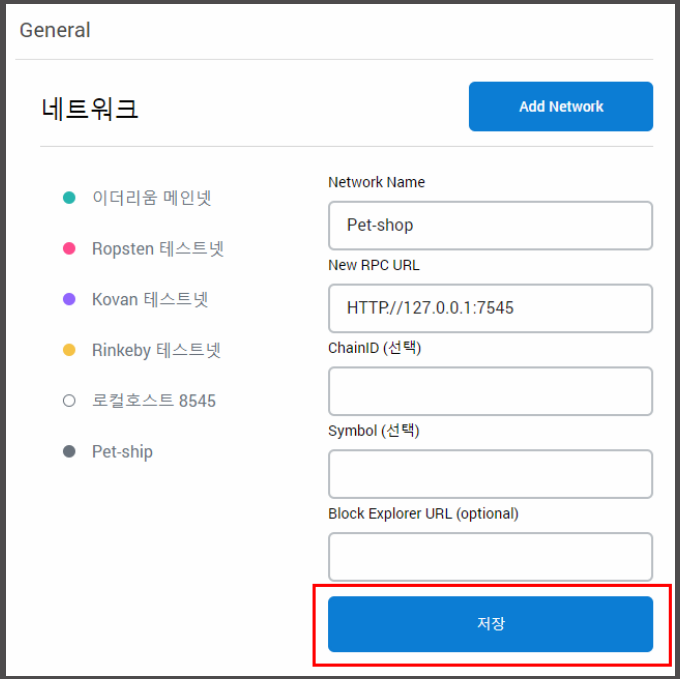




MetaMask

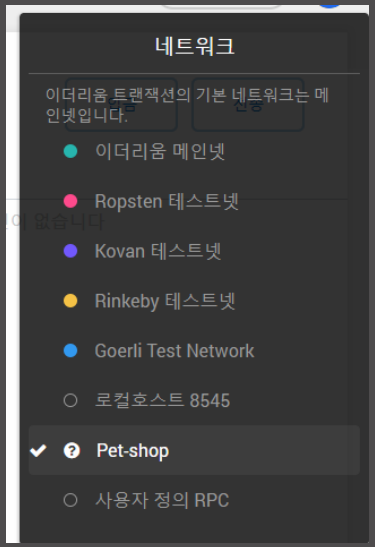
- 이더리움 메인넷에서 Custom RPC 로 네트워크 변경
- Set network as private local test server

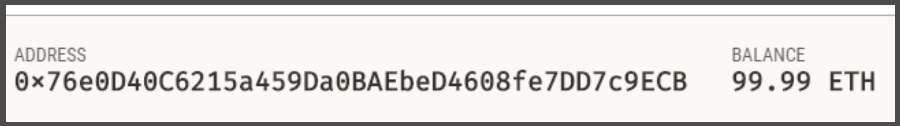


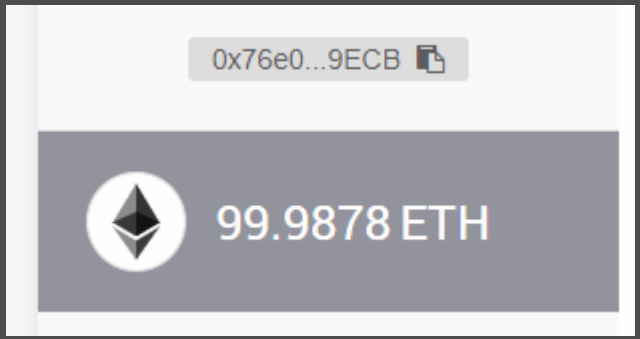


MetaMask

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

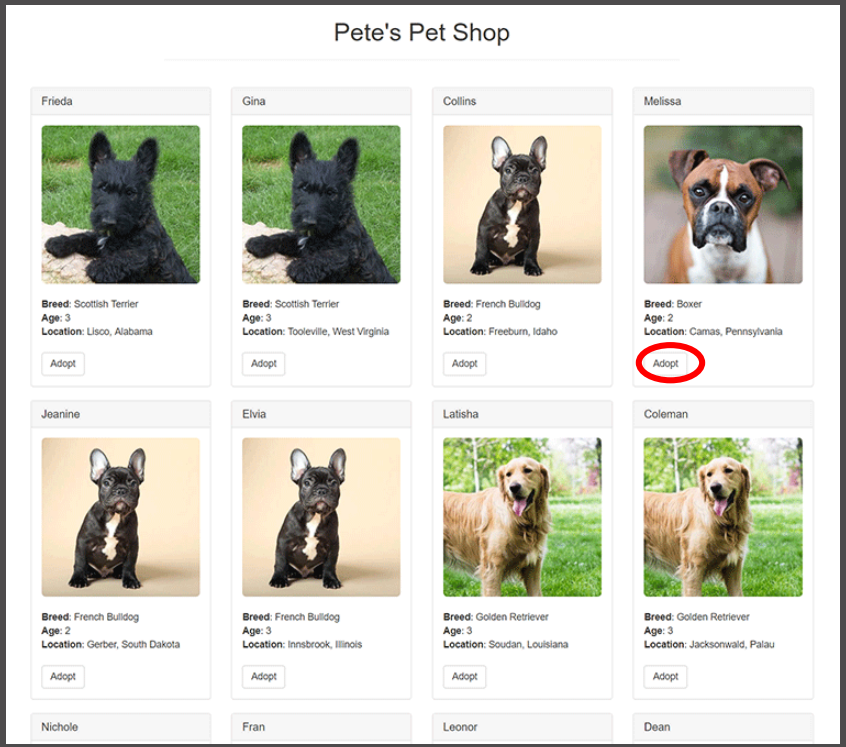


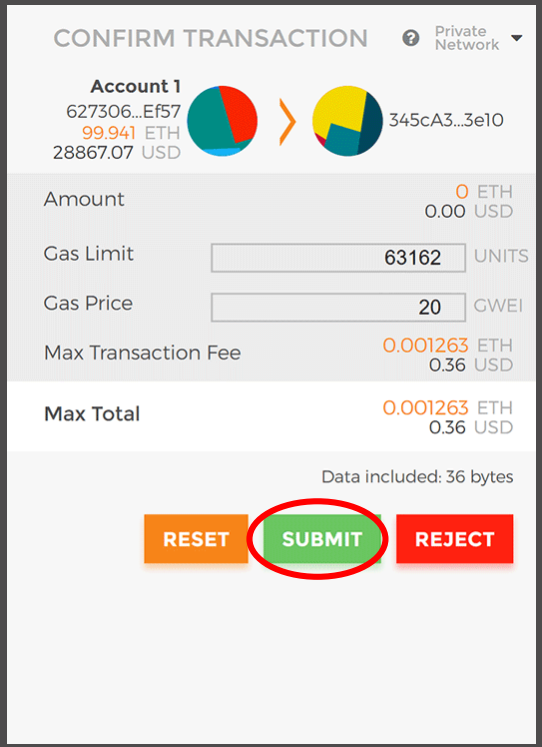




Pet Shop 실행

>> npm run dev





Pet Shop 실행

← BACK

TX 0×7c365c829303b2129c82fdbf999036c3d6ccd9eaf57d6a00f32eee1a04bf2dd7

SENDER ADDRESS
0×627306090abab3a6e1400e9345bc60c78a8bef57

TO CONTRACT ADDRESS
0×345ca3e014aaf5dca488057592ee47305d9b3e10

CONTRACT CALL

VALUE	GAS USED	GAS PRICE	GAS LIMIT	MINED IN BLOCK
0.00 ETH	42138	100000000000	63207	15

TX DATA
0×8588b2c50000000000000000000000000000000000000000000000000000000000000003

Collins

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

Adopt

Melissa

Breed: Boxer
Age: 2
Location: Camas, Pennsylvania

Success

network security
system design Lab.

THANK YOU

FOR YOUR ATTENTION