Medical Record

选题背景

当前社会上每个人基本上都有多个病历本，分别由不同的医院掌握，
当我们去看病时，医院可能没有或没有完全掌握我们的病史情况和医疗记录，这样就会给我们的就医造成很大的困扰，有时甚至会导致误诊，不能对症下药。

选题依据

如果能够利用区块链技术来保存我们的病历，就能保证我们每个人都
只有一个病历本，并且由我们自己掌握，需要时再由用户授权给医院查询特定的病史和医疗记录，以及添加新的就医记录，同时限制医院不能更改已有的医疗记录。这样既能保护用户的隐私，又能保证病历的不可篡改性，还能使用户未来看病或对自己健康做规划时有数据可用。

实验步骤

环境搭建

1. 安装 Node（官网下载）
2. 安装 Truffle（npm install –g truffle）
3. 安装 web3（npm install web3）
4. 安装 Ganache（官网下载）
5. 安装 lite-server（npm install –g lite-server）
6. 安装 MetaMask（浏览器扩展程序）

创建项目

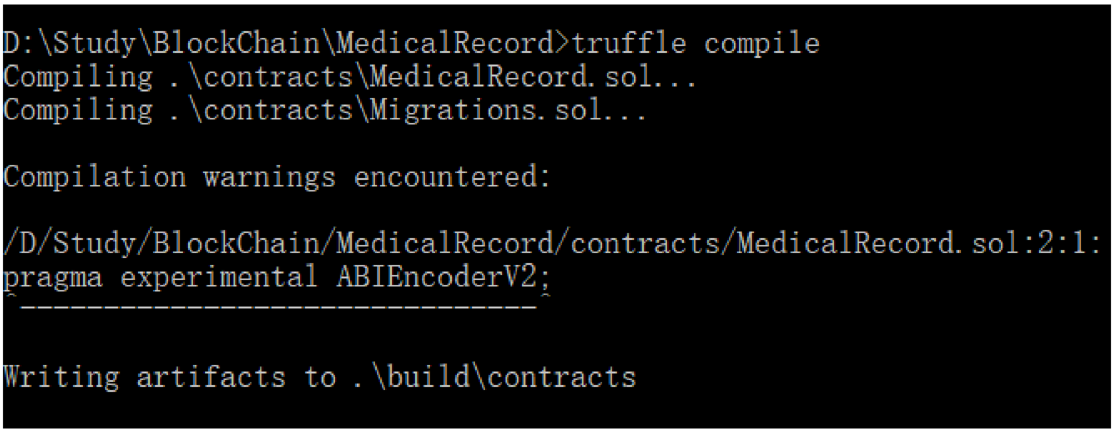
truffle init 创建全新的项目

编写智能合约

在 contracts 目录下，添加合约文件 MedicalRecord.sol

编译智能合约

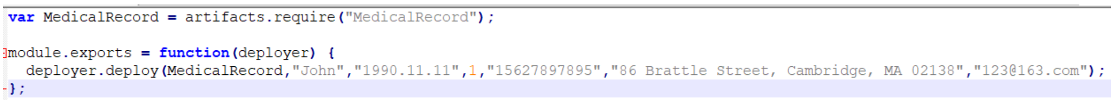
truffle compile



```
D:\Study\BlockChain\MedicalRecord>truffle compile
Compiling .\contracts\MedicalRecord.sol...
Compiling .\contracts\Migrations.sol...

Compilation warnings encountered:

/D/Study/BlockChain/MedicalRecord/contracts/MedicalRecord.sol:2:1:
pragma experimental ABIEncoderV2;
^-------------------------------^

Writing artifacts to .\build\contracts
```

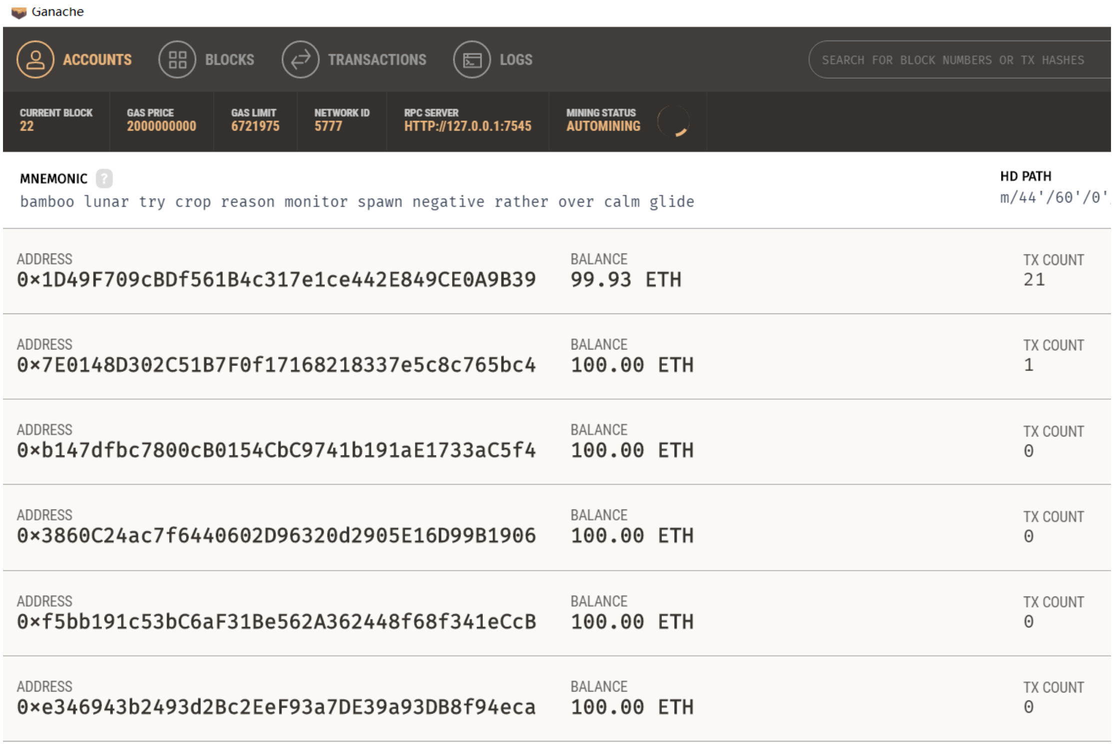
部署智能合约

1. 在 migrations 文件夹下创建部署脚本 2_deploy_contracts.js



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

module.exports = function(deployer) {
  deployer.deploy(MedicalRecord,"John","1990.11.11",1,"15627897895","86 Brattle Street, Cambridge, MA 02138","123@163.com");
};
```

2. 启动 Ganache 来开启一个私链进行开发测试



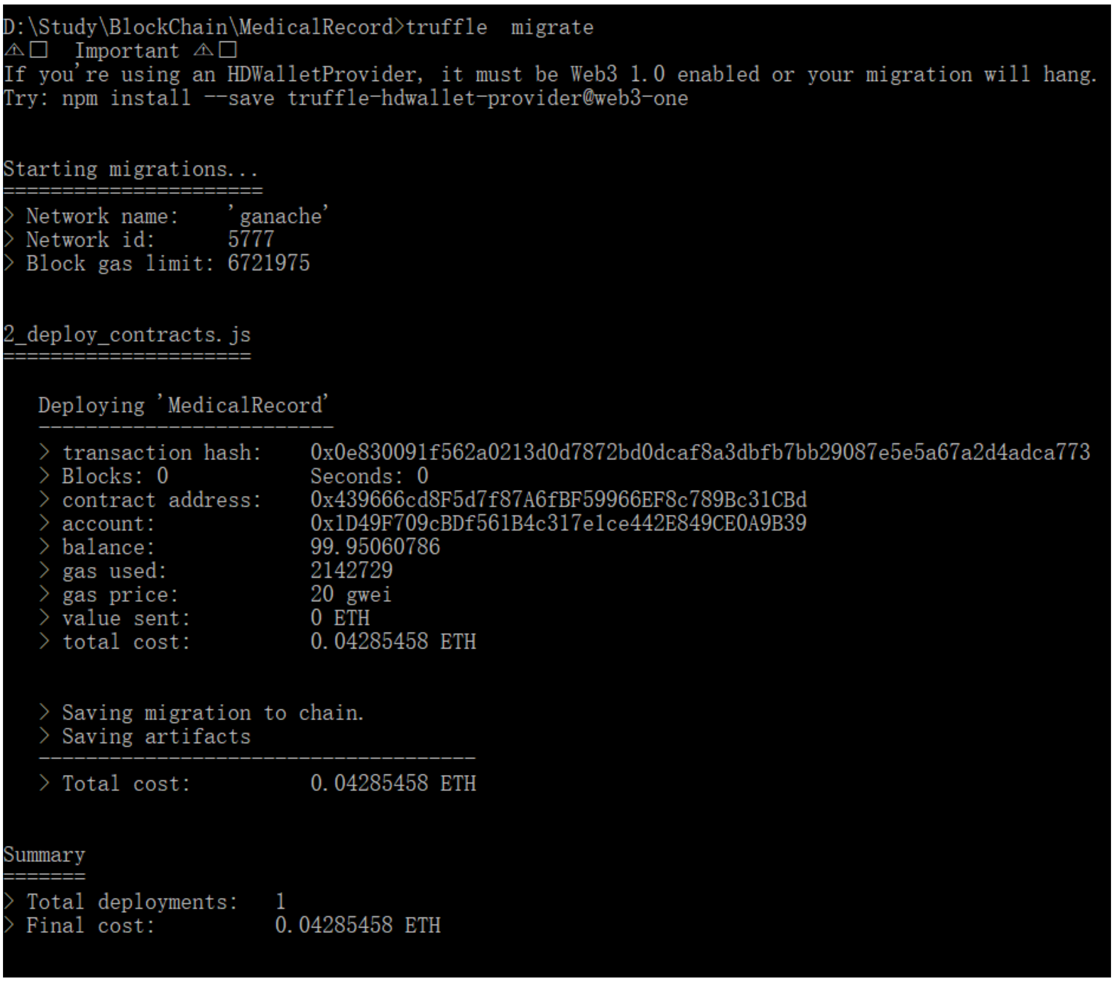
CURRENT BLOCK	GAS PRICE	GAS LIMIT	NETWORK ID	RPC SERVER	MINING STATUS
22	2000000000	6721975	5777	HTTP://127.0.0.1:7545	AUTOMINING

MNEMONIC
bamboo lunar try crop reason monitor spawn negative rather over calm glide

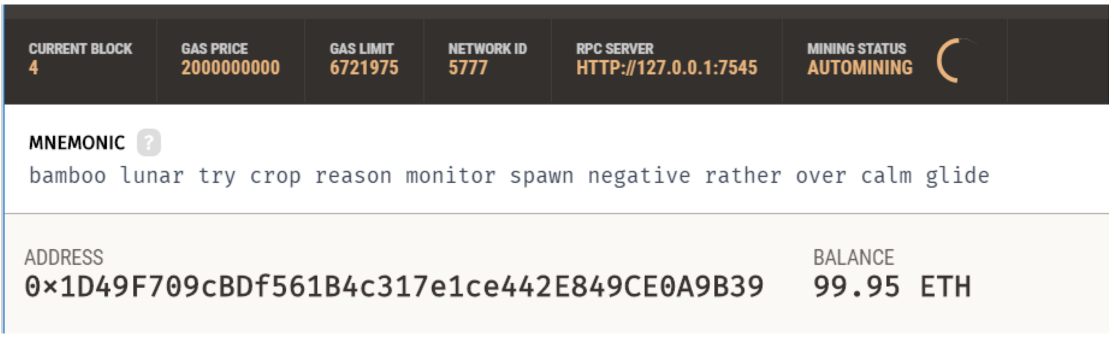
HD PATH
m/44'/60'/0'

ADDRESS	BALANCE	TX COUNT
0x1D49F709cBDf561B4c317e1ce442E849CE0A9B39	99.93 ETH	21
0x7E0148D302C51B7F0f17168218337e5c8c765bc4	100.00 ETH	1
0xb147dfbc7800cB0154CbC9741b191aE1733aC5f4	100.00 ETH	0
0x3860C24ac7f6440602D96320d2905E16D99B1906	100.00 ETH	0
0xf5bb191c53bC6aF31Be562A362448f68f341eCcB	100.00 ETH	0
0xe346943b2493d2Bc2EeF93a7DE39a93DB8f94eca	100.00 ETH	0

truffle migrate 执行部署命令



```
D:\Study\BlockChain\MedicalRecord>truffle  migrate
⚠□  Important ⚠□
If you're using an HDWalletProvider, it must be Web3 1.0 enabled or your migration will hang.
Try: npm install --save truffle-hdwallet-provider@web3-one


Starting migrations...
======================
> Network name:    'ganache'
> Network id:      5777
> Block gas limit: 6721975


2_deploy_contracts.js
=====================

   Deploying 'MedicalRecord'
   -------------------------
   > transaction hash:    0x0e830091f562a0213d0d7872bd0dcaf8a3dbfb7bb29087e5e5a67a2d4adca773
   > Blocks: 0            Seconds: 0
   > contract address:    0x439666cd8F5d7f87A6fBF59966EF8c789Bc31CBd
   > account:             0x1D49F709cBDf561B4c317e1ce442E849CE0A9B39
   > balance:             99.95060786
   > gas used:            2142729
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.04285458 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:          0.04285458 ETH


Summary
=======
> Total deployments:   1
> Final cost:          0.04285458 ETH
```



CURRENT BLOCK 4 | GAS PRICE 2000000000 | GAS LIMIT 6721975 | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING

MNEMONIC

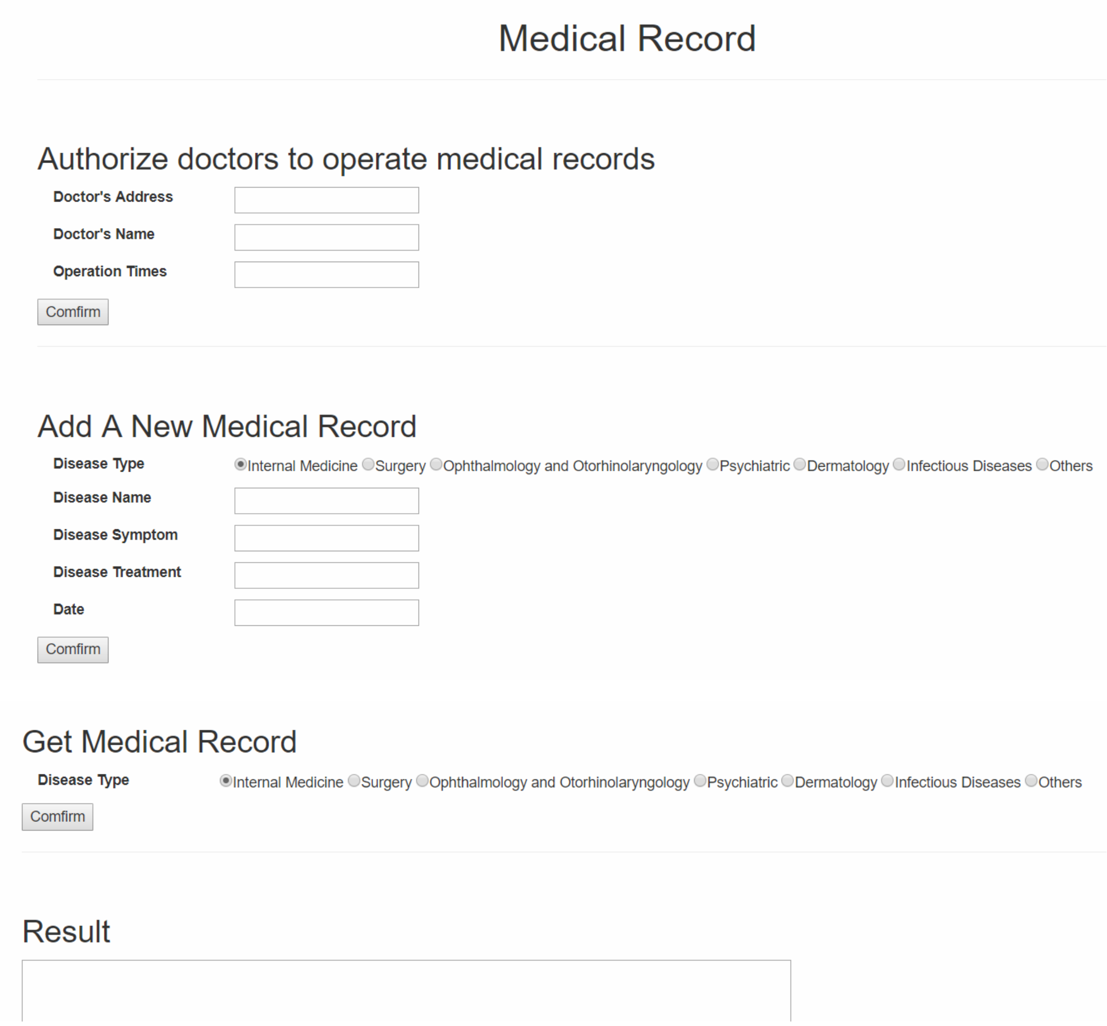
bamboo lunar try crop reason monitor spawn negative rather over calm glide

ADDRESS 0x1D49F709cBDf561B4c317e1ce442E849CE0A9B39

BALANCE 99.95 ETH

产生了四个区块说明部署成功

编辑 HTML 文件创建布局



Medical Record

Authorize doctors to operate medical records

Doctor's Address

Doctor's Name

Operation Times

Comfirm

Add A New Medical Record

Disease Type ● Internal Medicine ○ Surgery ○ Ophthalmology and Otorhinolaryngology ○ Psychiatric ○ Dermatology ○ Infectious Diseases ○ Others

Disease Name

Disease Symptom

Disease Treatment

Date

Comfirm

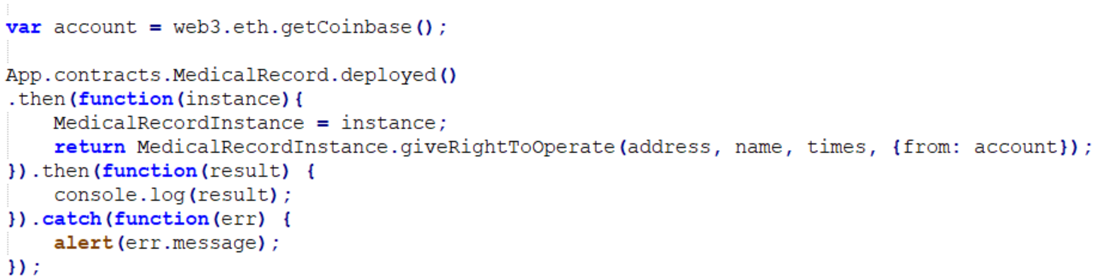
Get Medical Record

Disease Type ● Internal Medicine ○ Surgery ○ Ophthalmology and Otorhinolaryngology ○ Psychiatric ○ Dermatology ○ Infectious Diseases ○ Others

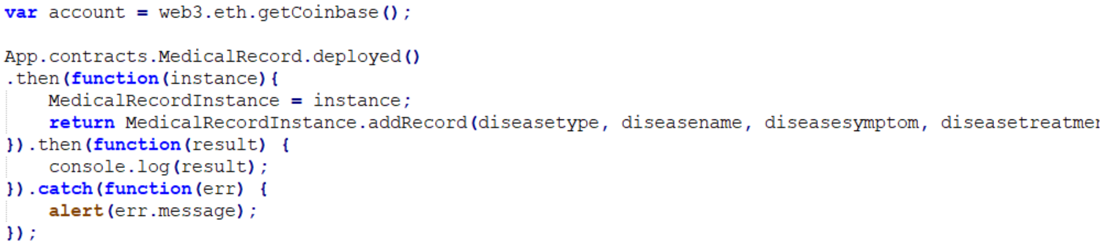
Comfirm

Result

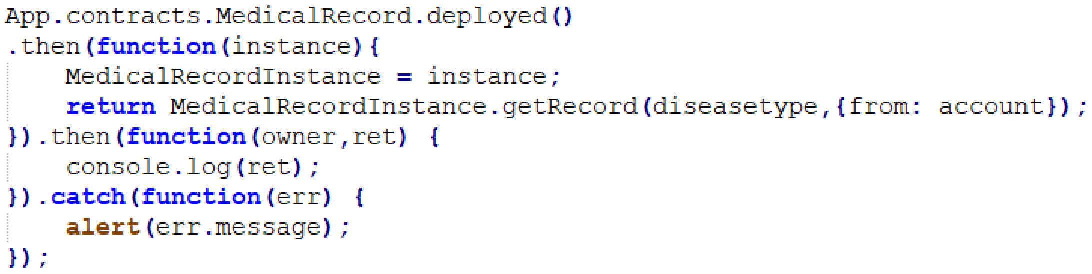
创建用户接口和智能合约交互



```
var account = web3.eth.getCoinbase();

App.contracts.MedicalRecord.deployed()
.then(function(instance){
    MedicalRecordInstance = instance;
    return MedicalRecordInstance.giveRightToOperate(address, name, times, {from: account});
}).then(function(result) {
    console.log(result);
}).catch(function(err) {
    alert(err.message);
});
```



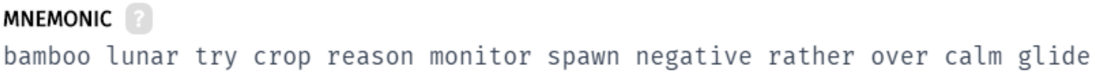
```
var account = web3.eth.getCoinbase();

App.contracts.MedicalRecord.deployed()
.then(function(instance){
    MedicalRecordInstance = instance;
    return MedicalRecordInstance.addRecord(diseasetype, diseasename, diseasesymptom, diseasetreatme
}).then(function(result) {
    console.log(result);
}).catch(function(err) {
    alert(err.message);
});
```



```
App.contracts.MedicalRecord.deployed()
.then(function(instance){
    MedicalRecordInstance = instance;
    return MedicalRecordInstance.getRecord(diseasetype,{from: account});
}).then(function(owner,ret) {
    console.log(ret);
}).catch(function(err) {
    alert(err.message);
});
```

运行测试

复制 Ganache 助记词

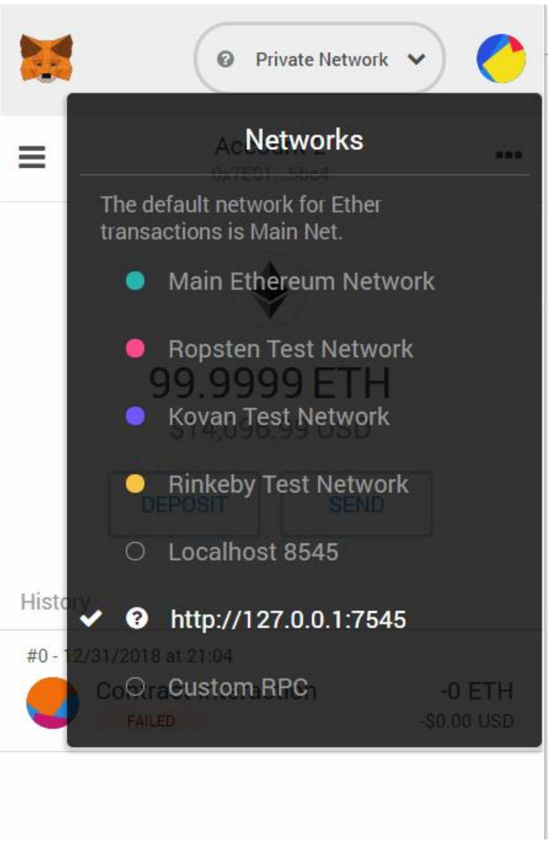


MNEMONIC

bamboo lunar try crop reason monitor spawn negative rather over calm glide

输入自定义密码进入 MetaMask

选择 Custom RPC 添加新网络 http://127.0.0.1:7545



The default network for Ether transactions is Main Net.

✓ http://127.0.0.1:7545

配置 lite-server

bs-config.json 指示了 lite-server 的工作目录。

```
{
   "server": {
      "baseDir": ["./src", "./build/contracts"]
   }
}
```

package.json 文件的 scripts 中添加了 dev 命令

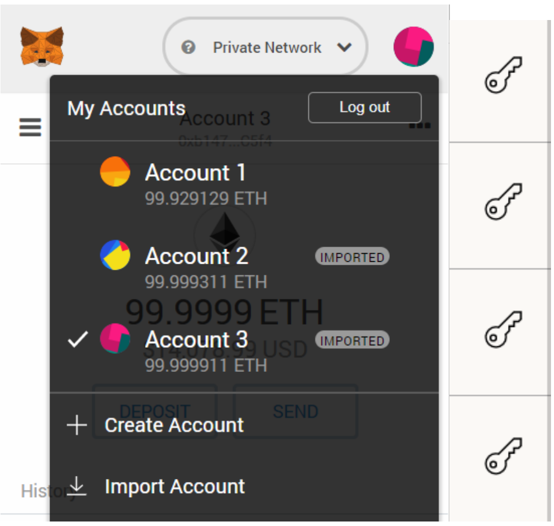
```
"scripts": {
   "dev": "lite-server",
   "test": "echo \"Error: no test specified\" && exit 1"
},
```

使用指令 npm run dev 启动 lite-server 运行并测试 DAPP

使用说明

1. 通过 MetaMask 可以实现多个账户对合约交互，合约拥有者为 Account 1

   添加账户可以点击右上角，Import Account，复制 Ganache 中其中一个用户的密钥并粘贴



Private Network

My Accounts　Log out

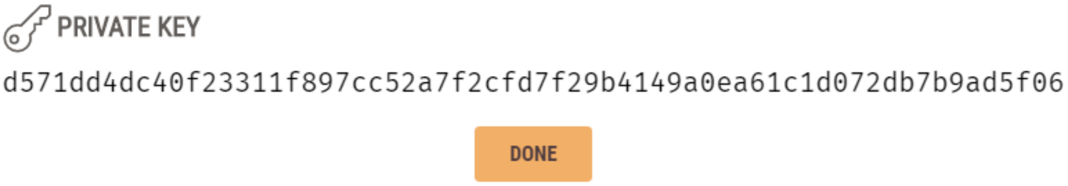
Account 1
99.929129 ETH

Account 2　IMPORTED
99.999311 ETH

✓ Account 3　IMPORTED
99.999911 ETH

＋ Create Account

Import Account



PRIVATE KEY

```
d571dd4dc40f23311f897cc52a7f2cfd7f29b4149a0ea61c1d072db7b9ad5f06
```

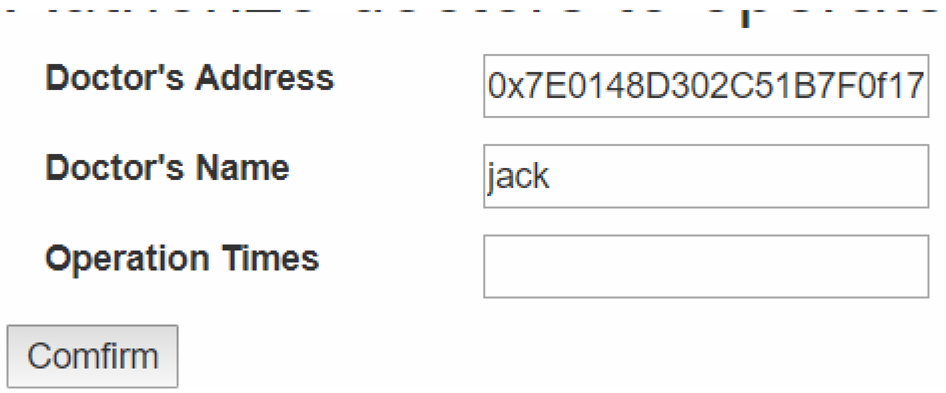
DONE

2. 使用 Account 1 可以给其他账户授权操作他的病历

3. Account 1 和被授权的账户可以查询和添加 Account 1 的病历记录

测试

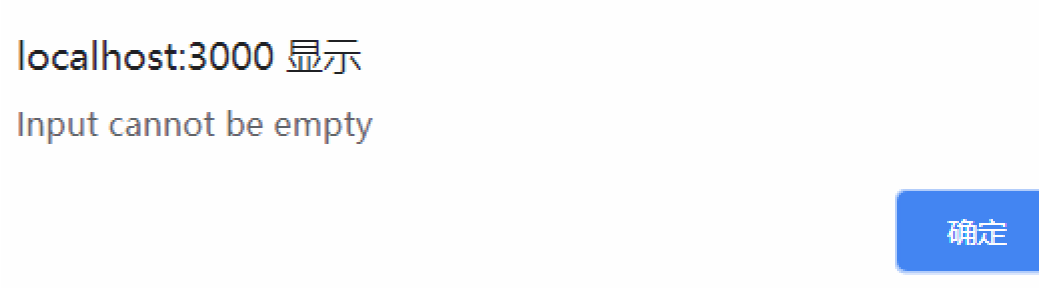
输入存在空



Doctor's Address 0x7E0148D302C51B7F0f17

Doctor's Name jack

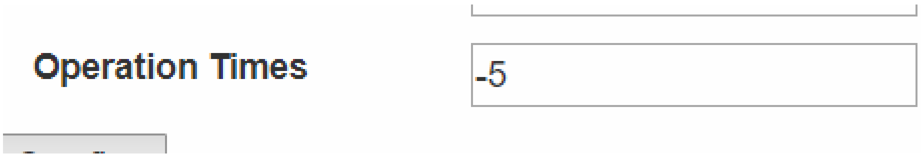
Operation Times



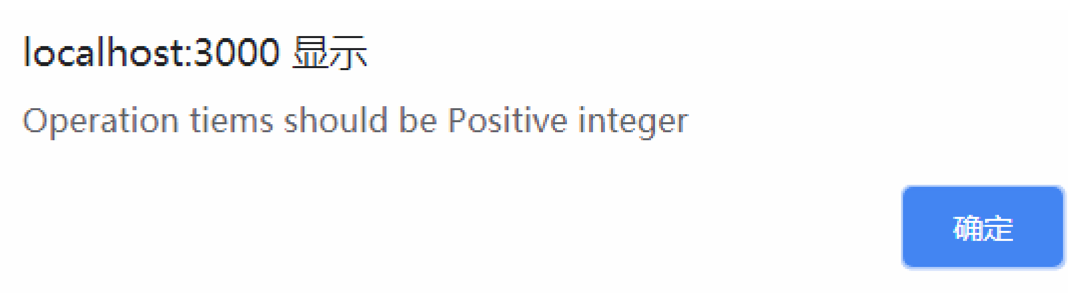
localhost:3000 显示

Input cannot be empty

操作次数不为正整数



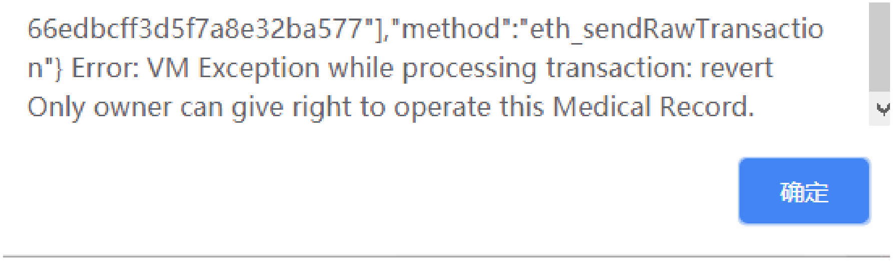
Operation Times -5



localhost:3000 显示

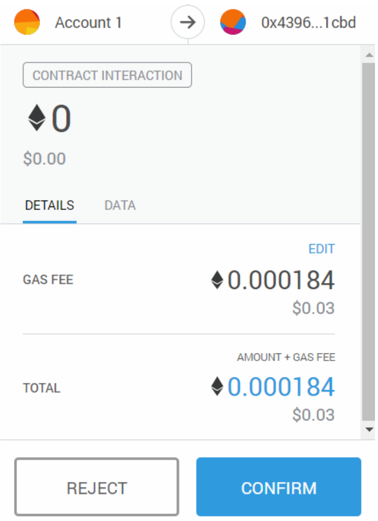
Operation tiems should be Positive integer

授权者不是合约的持有者



```
66edbcff3d5f7a8e32ba577"],"method":"eth_sendRawTransactio
n"} Error: VM Exception while processing transaction: revert
Only owner can give right to operate this Medical Record.
```

正常授权


Account 1 → 0x4396...1cbd

CONTRACT INTERACTION

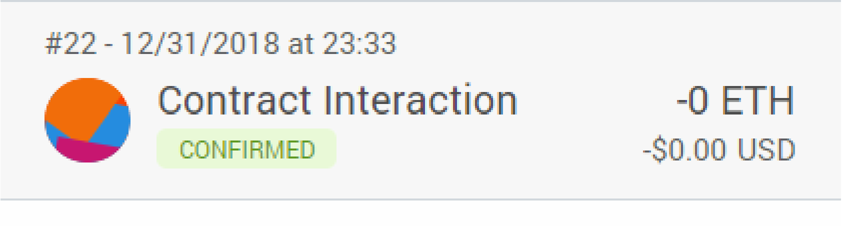
0

$0.00

DETAILS DATA

GAS FEE	EDIT 0.000184 $0.03
TOTAL	AMOUNT + GAS FEE 0.000184 $0.03

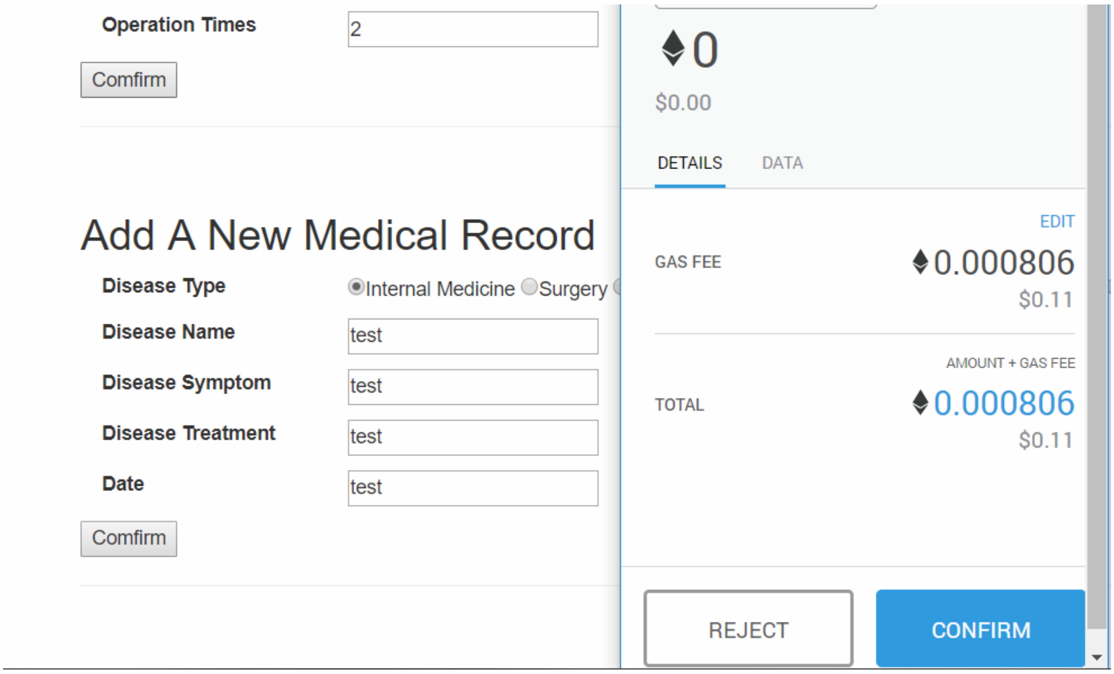
REJECT CONFIRM


#22 - 12/31/2018 at 23:33

Contract Interaction -0 ETH

CONFIRMED -$0.00 USD

授权用户添加记录


Operation Times	2

Comfirm

Add A New Medical Record

Disease Type	● Internal Medicine ○ Surgery
Disease Name	test
Disease Symptom	test
Disease Treatment	test
Date	test

Comfirm

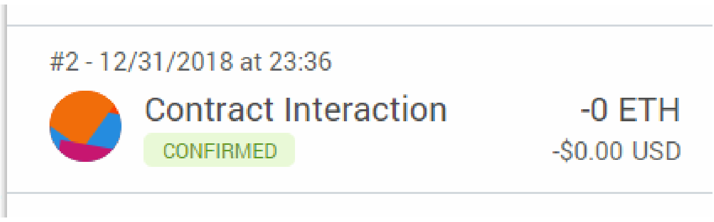
0

$0.00

DETAILS DATA

GAS FEE	EDIT 0.000806 $0.11
TOTAL	AMOUNT + GAS FEE 0.000806 $0.11

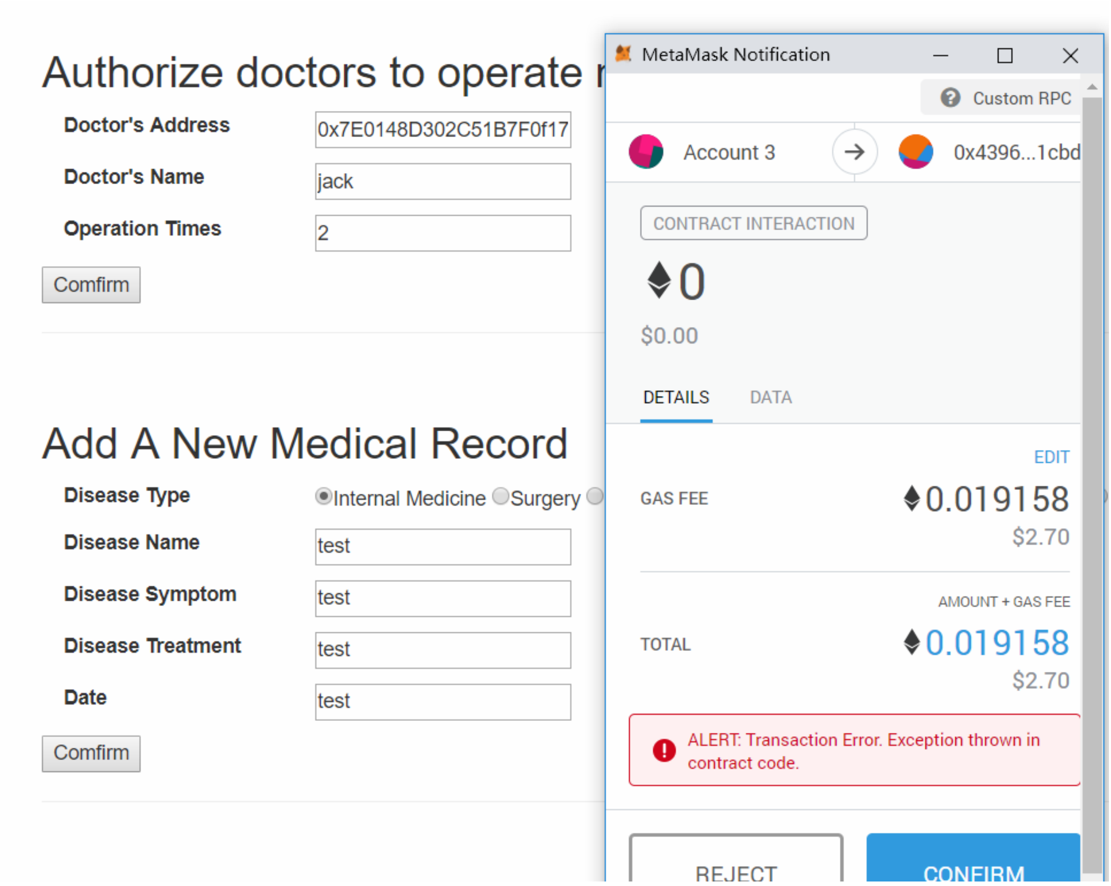
REJECT CONFIRM


#2 - 12/31/2018 at 23:36

Contract Interaction -0 ETH

CONFIRMED -$0.00 USD

未授权用户添加记录



Authorize doctors to operate r

Doctor's Address 0x7E0148D302C51B7F0f17

Doctor's Name jack

Operation Times 2

Add A New Medical Record

Disease Type ● Internal Medicine ○ Surgery ○

Disease Name test

Disease Symptom test

Disease Treatment test

Date test

MetaMask Notification

Account 3 → 0x4396...1cbd

CONTRACT INTERACTION

0

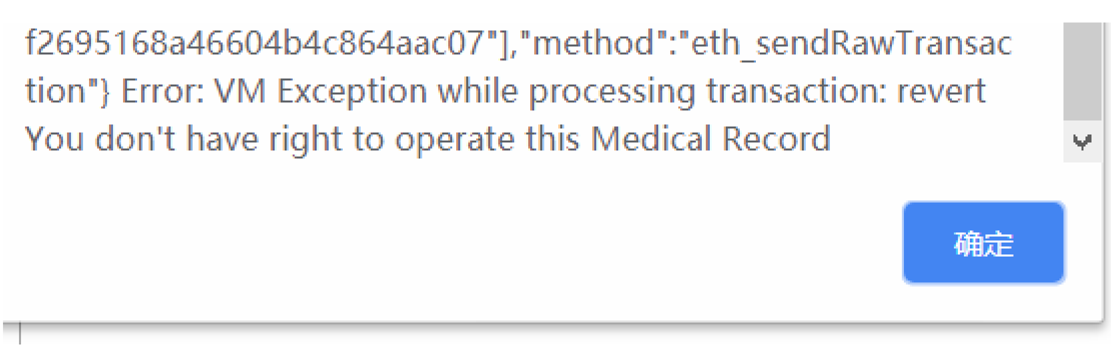
$0.00

GAS FEE 0.019158 $2.70

AMOUNT + GAS FEE

TOTAL 0.019158 $2.70

ALERT: Transaction Error. Exception thrown in contract code.



```
f2695168a46604b4c864aac07"],"method":"eth_sendRawTransac
tion"} Error: VM Exception while processing transaction: revert
You don't have right to operate this Medical Record
```

获取病历记录还存在一点问题，改进和测试见 Github

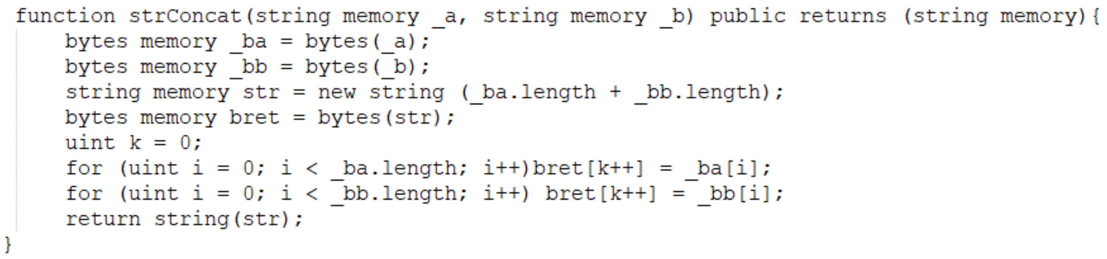
Github 地址：https://github.com/Zhanggen-sysu/MedicalRecord

参考资料：https://learnblockchain.cn/2018/01/12/first-dapp/#more

报告补充

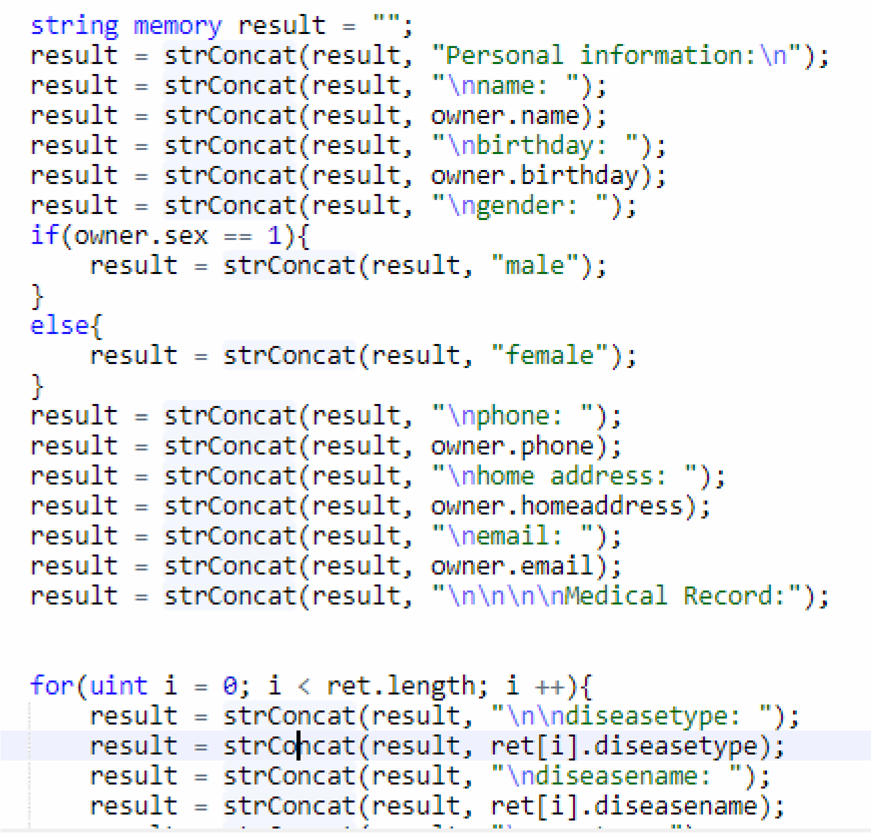
由于之前合约查询返回的是一个结构体和一个结构体数组，处理极为复杂，所以修改了合约，将返回变成一个字符串，但最后的效果是一样的。

Solidity 语言不支持加法字符串拼接，所以手动实现：



```
 function strConcat(string memory _a, string memory _b) public returns (string memory){
     bytes memory _ba = bytes(_a);
     bytes memory _bb = bytes(_b);
     string memory str = new string (_ba.length + _bb.length);
     bytes memory bret = bytes(str);
     uint k = 0;
     for (uint i = 0; i < _ba.length; i++)bret[k++] = _ba[i];
     for (uint i = 0; i < _bb.length; i++) bret[k++] = _bb[i];
     return string(str);
}
```

返回字符串的代码如下

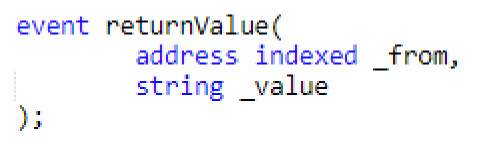


```
string memory result = "";
result = strConcat(result, "Personal information:\n");
result = strConcat(result, "\nname: ");
result = strConcat(result, owner.name);
result = strConcat(result, "\nbirthday: ");
result = strConcat(result, owner.birthday);
result = strConcat(result, "\ngender: ");
if(owner.sex == 1){
    result = strConcat(result, "male");
}
else{
    result = strConcat(result, "female");
}
result = strConcat(result, "\nphone: ");
result = strConcat(result, owner.phone);
result = strConcat(result, "\nhome address: ");
result = strConcat(result, owner.homeaddress);
result = strConcat(result, "\nemail: ");
result = strConcat(result, owner.email);
result = strConcat(result, "\n\n\n\nMedical Record:");


for(uint i = 0; i < ret.length; i ++){
    result = strConcat(result, "\n\ndiseasetype: ");
    result = strConcat(result, ret[i].diseasetype);
    result = strConcat(result, "\ndiseasename: ");
    result = strConcat(result, ret[i].diseasename);
```

使用 return 返回，返回的是交易的 Hash，所以修改为利用事件返回：

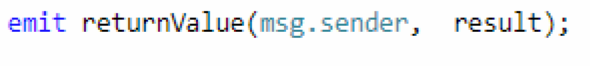
参考资料：https://www.tuicool.com/articles/J7JbUvq

定义事件



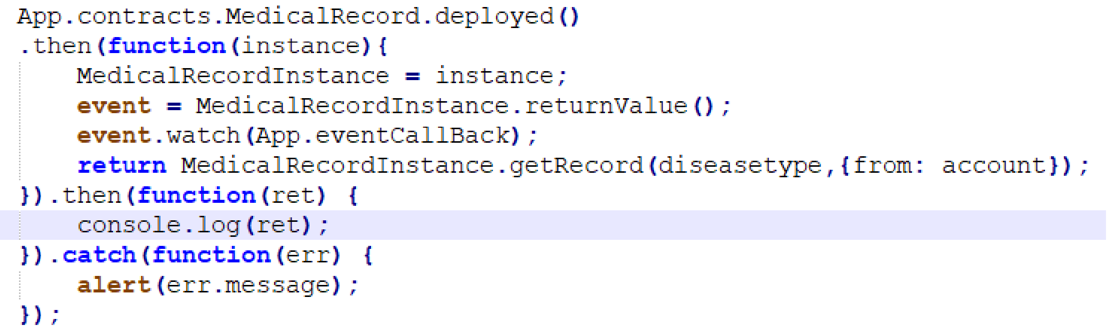
```
event returnValue(
        address indexed _from,
        string _value
);
```

触发事件

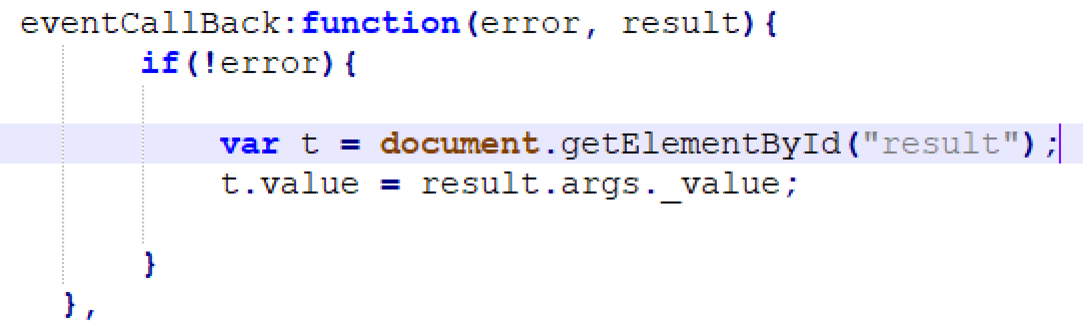


```
emit returnValue(msg.sender,  result);
```

在 js 中:



```
App.contracts.MedicalRecord.deployed()
.then(function(instance){
    MedicalRecordInstance = instance;
    event = MedicalRecordInstance.returnValue();
    event.watch(App.eventCallBack);
    return MedicalRecordInstance.getRecord(diseasetype,{from: account});
}).then(function(ret) {
    console.log(ret);
}).catch(function(err) {
    alert(err.message);
});
```



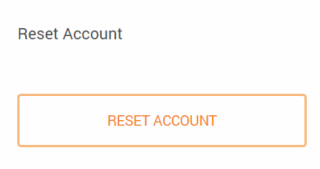
```
eventCallBack:function(error, result){
        if(!error){

            var t = document.getElementById("result");
            t.value = result.args._value;

        }
   },
```

利用回调函数更新 UI

其他补充

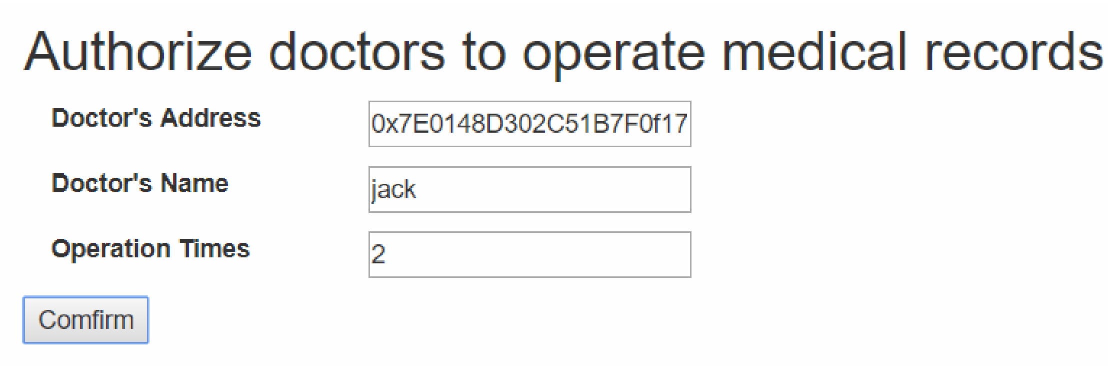
重新编译合约后再次部署需要 truffle network –clean 清理原来的部署

使用 MetaMask 出现 nonce 错误需要先重置账户



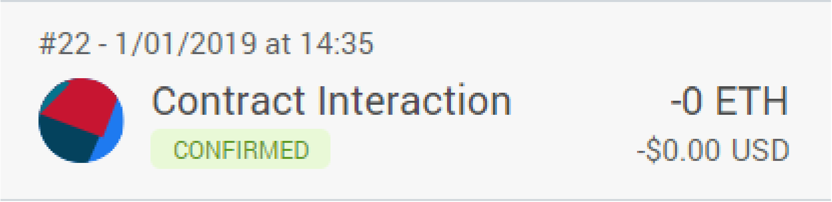
Invalid address 可以通过刷新页面解决

测试补充



Authorize doctors to operate medical records

Doctor's Address	0x7E0148D302C51B7F0f17
Doctor's Name	jack
Operation Times	2



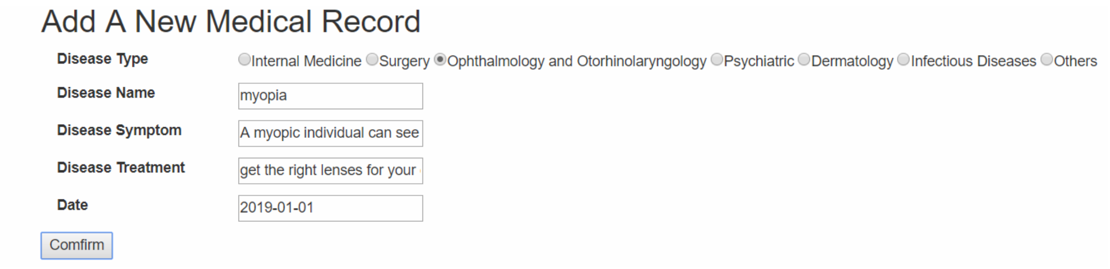
#22 - 1/01/2019 at 14:35

Contract Interaction

CONFIRMED

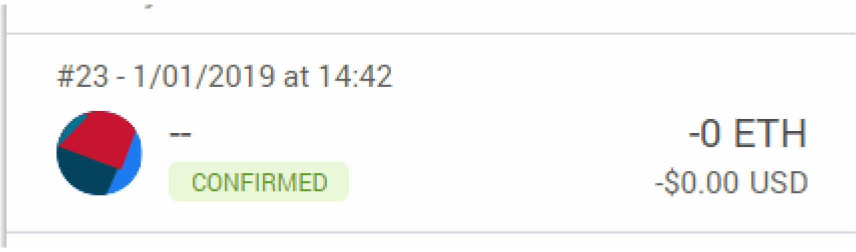
-0 ETH

-$0.00 USD



Add A New Medical Record

Disease Type	○Internal Medicine ○Surgery ●Ophthalmology and Otorhinolaryngology ○Psychiatric ○Dermatology ○Infectious Diseases ○Others
Disease Name	myopia
Disease Symptom	A myopic individual can see
Disease Treatment	get the right lenses for your
Date	2019-01-01



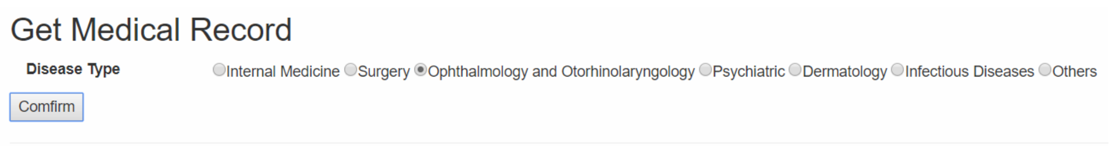
#23 - 1/01/2019 at 14:42

--

CONFIRMED

-0 ETH

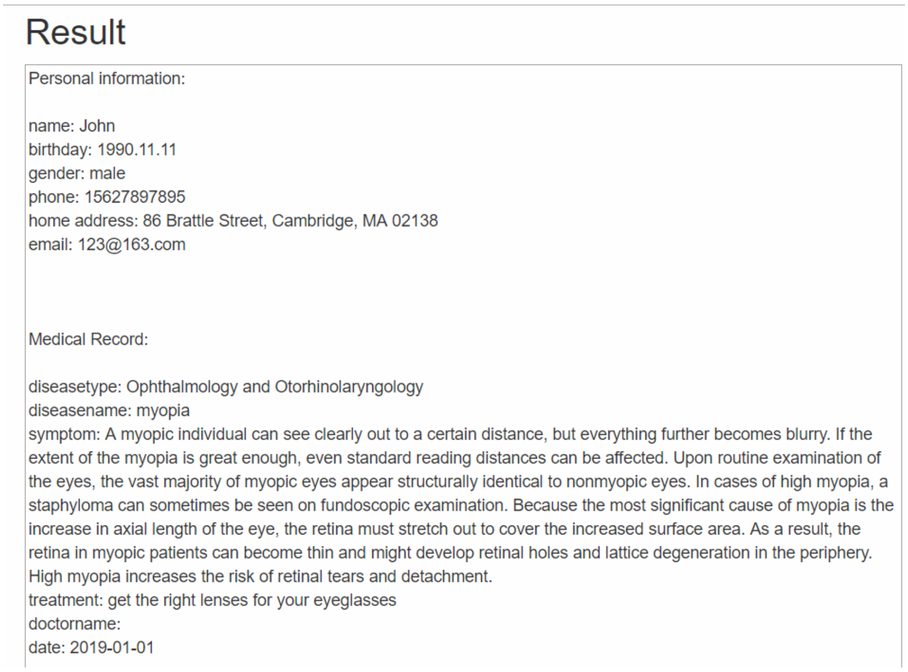
-$0.00 USD



Get Medical Record

Disease Type ○Internal Medicine ○Surgery ●Ophthalmology and Otorhinolaryngology ○Psychiatric ○Dermatology ○Infectious Diseases ○Others

自己添加的所以 doctorname 为空



Result

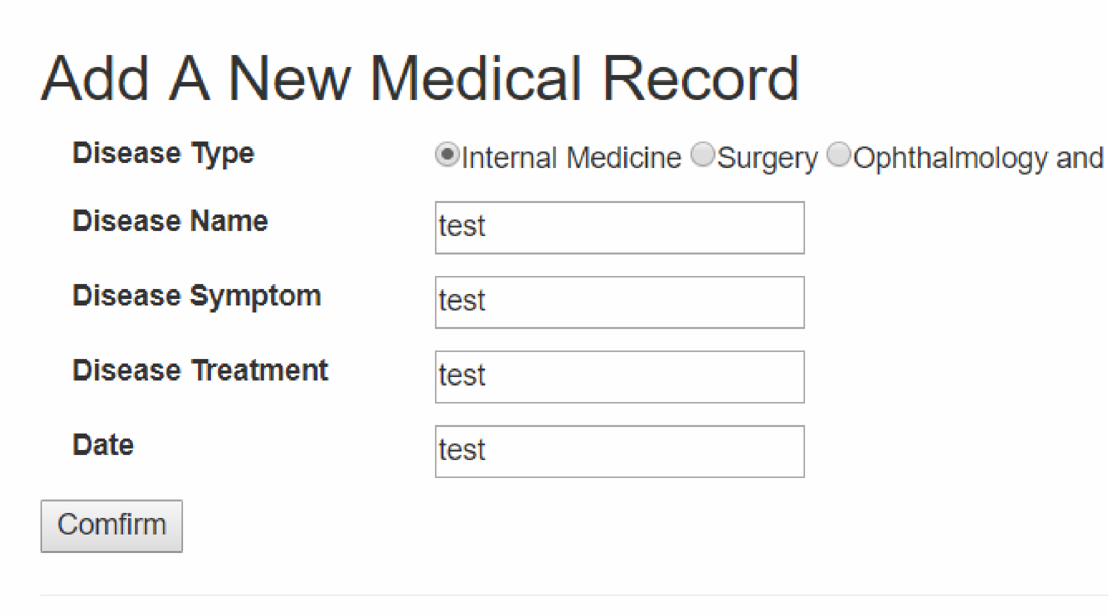
Personal information:

name: John
birthday: 1990.11.11
gender: male
phone: 15627897895
home address: 86 Brattle Street, Cambridge, MA 02138
email: 123@163.com

Medical Record:

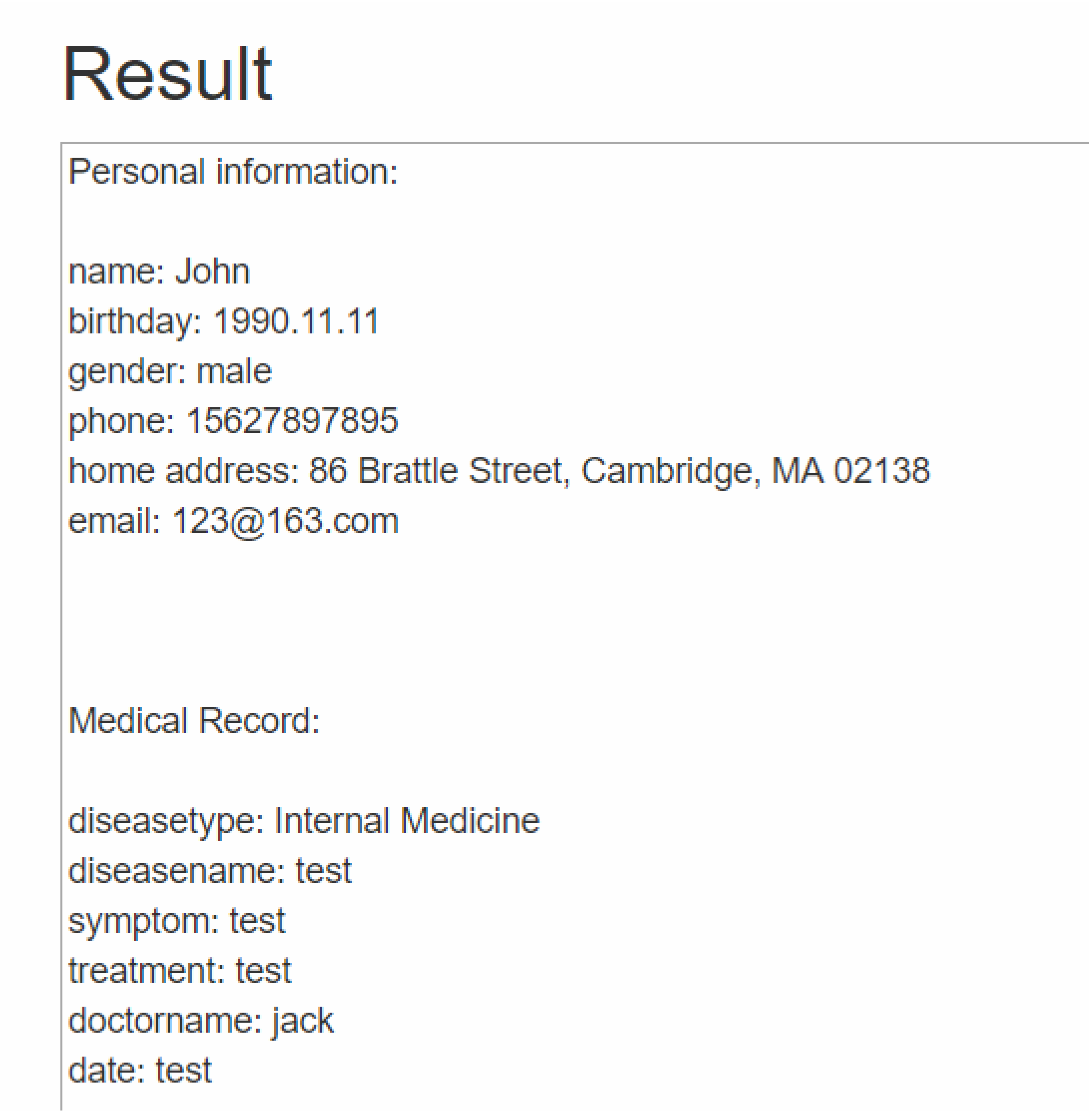
diseasetype: Ophthalmology and Otorhinolaryngology
diseasename: myopia
symptom: A myopic individual can see clearly out to a certain distance, but everything further becomes blurry. If the extent of the myopia is great enough, even standard reading distances can be affected. Upon routine examination of the eyes, the vast majority of myopic eyes appear structurally identical to nonmyopic eyes. In cases of high myopia, a staphyloma can sometimes be seen on fundoscopic examination. Because the most significant cause of myopia is the increase in axial length of the eye, the retina must stretch out to cover the increased surface area. As a result, the retina in myopic patients can become thin and might develop retinal holes and lattice degeneration in the periphery. High myopia increases the risk of retinal tears and detachment.
treatment: get the right lenses for your eyeglasses
doctorname:
date: 2019-01-01

使用 Account 2 添加并查询



Add A New Medical Record

Disease Type ● Internal Medicine ○ Surgery ○ Ophthalmology and
Disease Name test
Disease Symptom test
Disease Treatment test
Date test



Result

Personal information:

name: John
birthday: 1990.11.11
gender: male
phone: 15627897895
home address: 86 Brattle Street, Cambridge, MA 02138
email: 123@163.com

Medical Record:

diseasetype: Internal Medicine
diseasename: test
symptom: test
treatment: test
doctorname: jack
date: test