

电影票务系统 Dapp

15336195 信息安全 吴立渝

- 题目:票务系统 Dapp 实现

- 工具:

Remix ide、ganache、html、javascript、ethereum

- 选题背景:

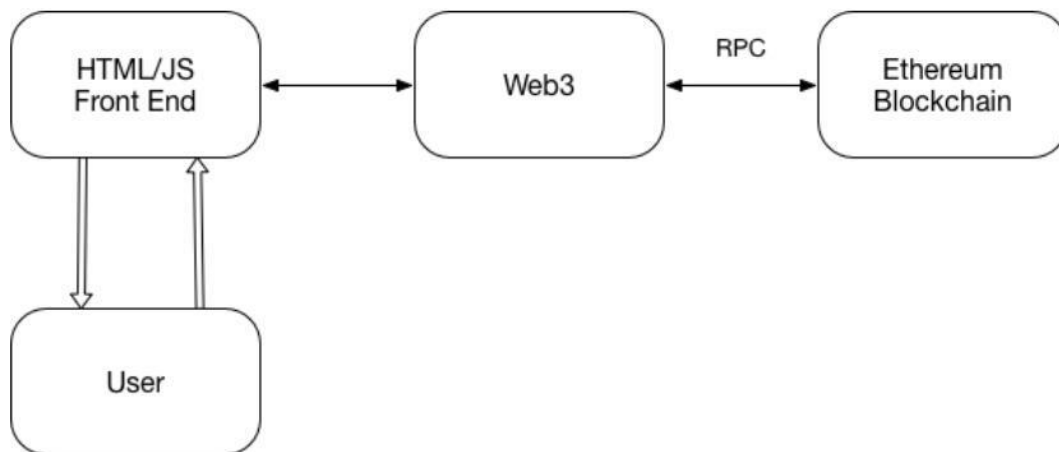
除了影院可购买电影票之外，目前也存在许多第三方平台如美团、大众点评等提供购买电影票的服务，确实也提高购票的便利性。

这样的场景可视为以第三方平台为中心进行购票业务，除了在相同影院相同电影的售价不一致之外，消费者以及购买记录分别存在相应的第三方平台可能导致数据不共享不一致，或任何中心化机构潜在的风险的发生。透过区块链智能合约的方案整合影院信息、购票记录，将其数据存储在区块链上，不仅提供数据回溯、不可篡改，导入区块链性质解决中心化的问题，也省去中介平台从中获利进而提高消费者的利益。

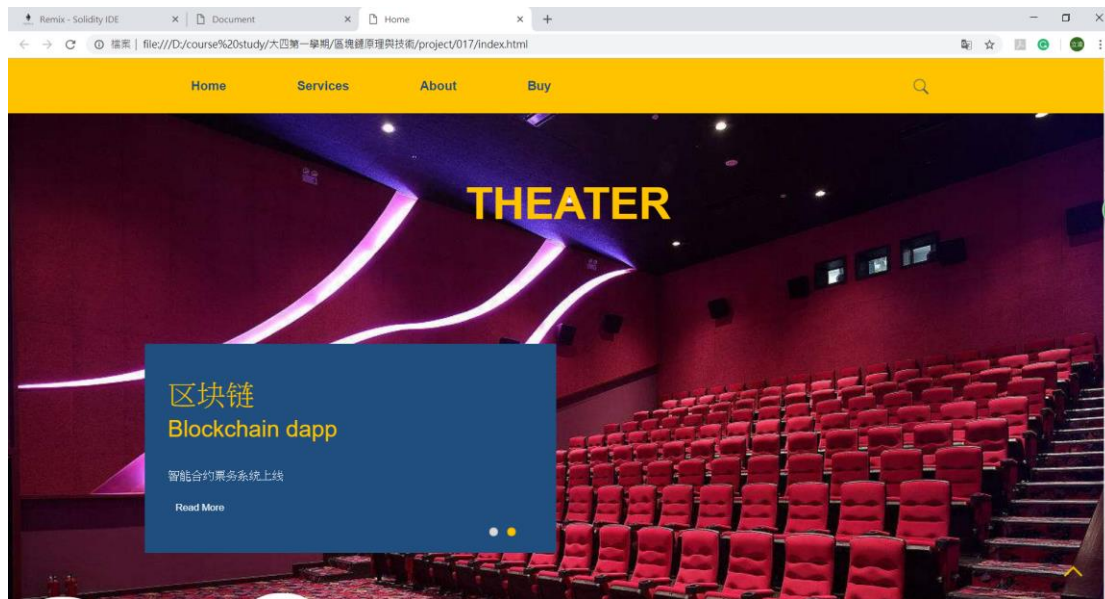
后期可加入第三方支付功能进行充值购票，如微信、支付宝，使一般用户可以不用透过以太坊进行支付，增加 Dapp 的实用性。

- 智能合约使用

根据下图，我们主要透过 Web3 将智能合约与 HTML 网页进行连接。



1. 前端:主要实现用户与智能合约交互的平台，目前只有购票服务，后期会在完善其他功能，如会员管理、用户登陆、提高安全性等等的功能。



About

Welcome

Intorduction

影城总投资2000多万元，影城建筑面积近2000平方米，共设计400多个座位，运用2K巴克高清晰映机、3D立体放映技术、进口音响、航空座椅，内设3个放映厅，让您享受更逼真、更舒适、更震撼的感官和视听效果。6个豪华包厢，给您一个私密的私人观影空间。

Theater Equipments

- 银幕系统
- 立体放映系统
- 特效座椅
- 特效设备
- 音响系统
- 控制系统
- 操作监控系统

Movie Express



海王

《海王》是由美国华纳兄弟影片公司出品的动作奇幻片，由华裔导演温子仁执导，杰森·莫玛、艾梅柏·希尔德、帕特里克·威尔森联合主演。《海王》根据DC漫画改编，讲述了亚瑟·库里认识到他家族血脉的真谛的过程，以及和墨拉一同对抗对人类怀有更深敌意的同母异父的兄弟——海洋领主奥姆的故事。



毒液：致命守护者

身为记者的埃迪·布洛克（汤姆·哈迪饰）在调查生命基金会老板卡尔·德雷克（里兹·阿迈德饰）的过程中，事业遭受重创，与未婚妻分离。在与卡尔·德雷克

Services

会员中心

Lorem Ipsum is that it has a more-or-less normal distribution of letters, as opposed.

[More](#)

场次查询

Lorem Ipsum is that it has a more-or-less normal distribution of letters, as opposed.

[More](#)

购票

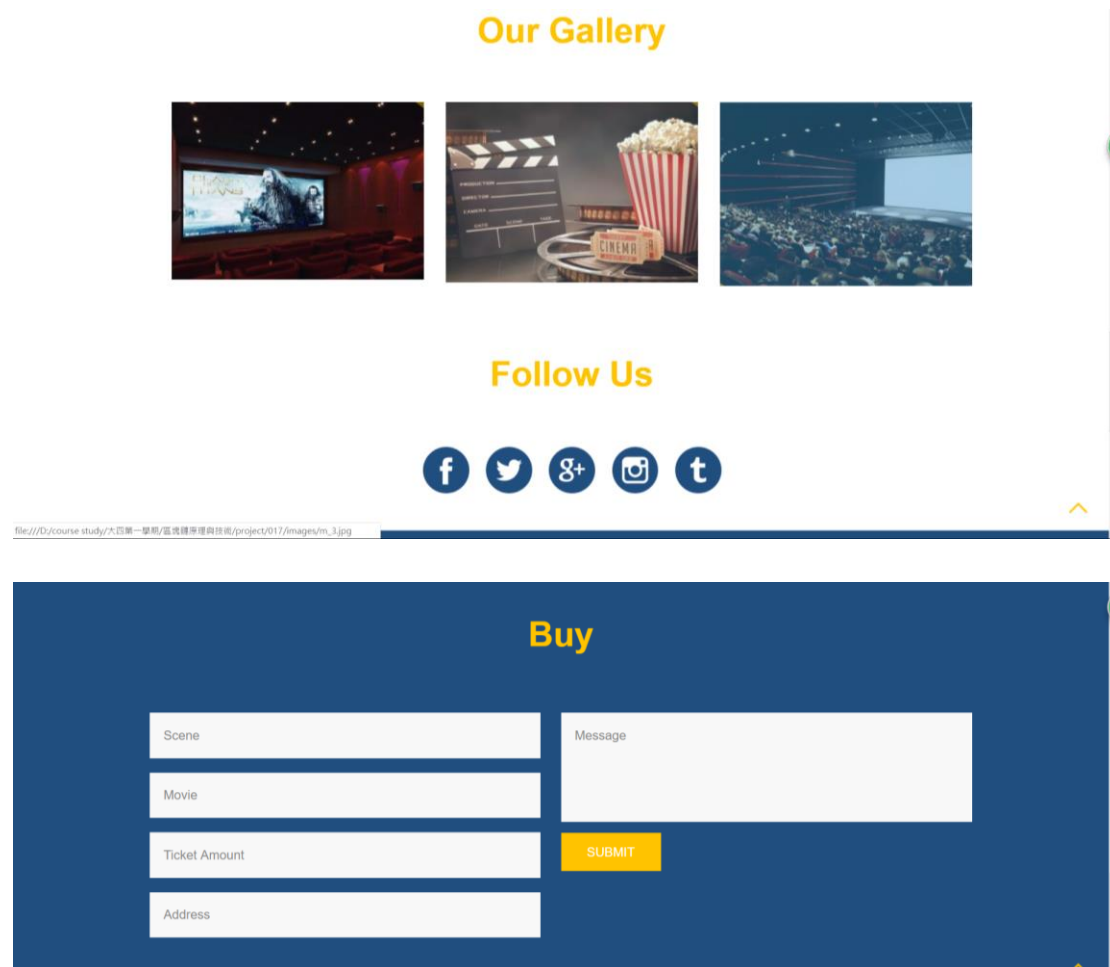
Lorem Ipsum is that it has a more-or-less normal distribution of letters, as opposed.

[More](#)

其他服务

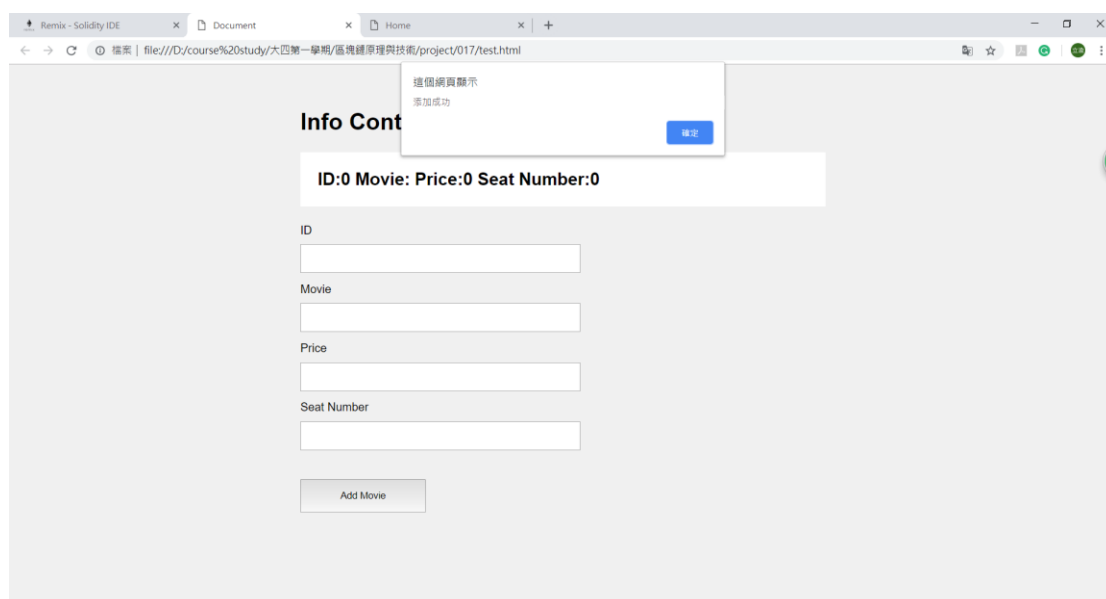
Lorem Ipsum is that it has a more-or-less normal distribution of letters, as opposed.

[More](#)



2. 面向开发者

连接智能合约、提供企业添加电影、服务等操作端，后期将完善其他操作。



确认刚添加的电影信息，表示添加成功。

Info Contract

ID:1 Movie:Aquaman Price:36 Seat Number:150

ID

Movie

Price

Seat Number

Add Movie

3. 其他功能

目前仍在各个功能上进行相应的前端开发，具体功能可以透过 remix ide 进行调适。

● 智能合约部属

1. Ganache

为了方便测试，使用 Ganache Gui 作为部属工具。创建 10 位用户并默认分别拥有 100ETH，使用 ganache 可以方便我们在 remix ide 上部属智能合约并，此外 ganache 可以看到每次调用智能合约的交易以及交易的相关信息，助于我们进行代码调适。

ACCOUNTS

BLOCKS

TRANSACTIONS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK
3

GAS PRICE
2000000000

GAS LIMIT
6721975

NETWORK ID
72

RPC SERVER
HTTP://127.0.0.1:7545

MINING STATUS
AUTOMINING

MNEMONIC

language ticket muffin village mandate total elephant birth humble until skill sport

HD PATH

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

ADDRESS

0x60E637042c8E93Fd7810F89825404A3215713570

BALANCE

100.00 ETH

TX COUNT

3

INDEX

0

ADDRESS

0xd2cA239268cacB2B2a00F15Af0b79c94d12d0C5F

BALANCE

100.00 ETH

TX COUNT

0

INDEX

1

ADDRESS

0xF7dafcacD6A59c7356816FdA49992439a47818F7

BALANCE

100.00 ETH

TX COUNT

0

INDEX

2

ADDRESS

0x1287de539F99e3b09102Ca074F97CBd9073a0403

BALANCE

100.00 ETH

TX COUNT

0

INDEX

3

ADDRESS

0x3F4143783C6FbEc7DfAC52D16AEce96D808BDB20

BALANCE

100.00 ETH

TX COUNT

0

INDEX

4

ADDRESS

0x0eDDC5CaFEa364d12891EA5e1f5dd85Cc4A3E862

BALANCE

100.00 ETH

TX COUNT

0

INDEX

5

ADDRESS

0x6bEa77ce084e91dd1e9Ded87a1c875A64272D717

BALANCE

100.00 ETH

TX COUNT

0

INDEX

6

Ganache

ACCOUNTS

BLOCKS

TRANSACTIONS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK

3

GAS PRICE

2000000000

GAS LIMIT

6721975

NETWORK ID

72

RPC SERVER

HTTP://127.0.0.1:7545

MINING STATUS

AUTOMINING

TX HASH

0×acd67448eac90e4e6b376a29c3428b4f001486c1d9f5ebfc5aaf2f0f58e5bfb2

CONTRACT CALL

FROM ADDRESS

0×60E637042c8E93Fd7810F89825404A3215713570

TO CONTRACT ADDRESS

0×6Df01fb9d6C608B88404e37e1570166B6ee26213

GAS USED

195422

VALUE

0

TX HASH

0×144081a0283afdbb113a8ed49fd730b1c1812d0c7c57f1c0d564f82f7dc2dfd3

CONTRACT CALL

FROM ADDRESS

0×60E637042c8E93Fd7810F89825404A3215713570

TO CONTRACT ADDRESS

0×6Df01fb9d6C608B88404e37e1570166B6ee26213

GAS USED

74584

VALUE

0

TX HASH

0×fd42a1bd0c78a0be15cd07a51bd51d380a199f97a1a3dcb8d02b3e7bad77f889

CONTRACT CREATION

FROM ADDRESS

0×60E637042c8E93Fd7810F89825404A3215713570

CREATED CONTRACT ADDRESS

0×6Df01fb9d6C608B88404e37e1570166B6ee26213

GAS USED

1346512

VALUE

0

Ganache

ACCOUNTS

BLOCKS

TRANSACTIONS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK
3

GAS PRICE
2000000000

GAS LIMIT
6721975

NETWORK ID
72

RPC SERVER
HTTP://127.0.0.1:7545

MINING STATUS
AUTOMINING

BLOCK
3

MINED ON
2018-12-23 21:20:36

GAS USED
195422

1 TRANSACTION

BLOCK
2

MINED ON
2018-12-23 21:19:51

GAS USED
74584

1 TRANSACTION

BLOCK
1

MINED ON
2018-12-23 21:19:28

GAS USED
1346512

1 TRANSACTION

BLOCK
0

MINED ON
2018-12-23 21:19:05

GAS USED
0

NO TRANSACTIONS

2. Remix ide 与 ganache 具体连接:

在 Environment 切换到 Web3 Provider, 并输入我们的测试链的地址
http://127.0.0.1:7545, 这里对这三个选项做一简单说明:

- Javascript VM: 简单的 Javascript 虚拟机环境。
- Injected Web3: 连接到嵌入到页面的 Web3, 如连接到 MetaMask
- Web3 Provider: 连接到自定义的节点, 如私有的测试网络。

如果连接成功, Account 的选项会默认选择 Ganache 创建的第一个账户地址。接下来我们点击 Deploy 将智能合约部署到测试网中。在后面编写前端代码时还要用到合约的地址以及 ABI 信息。

● Web3 与智能合约交互:

首先创建 Web3.js 的实例, 代码参考

<https://github.com/ethereum/web3.js/>

```
if (typeof web3 !== 'undefined') {
  web3 = new Web3(web3.currentProvider);
} else {
  // set the provider you want from Web3.providers
  web3 = new Web3(new Web3.providers.HttpProvider("http://localhost:7545"));
}
```

设置默认以太坊账户:

```
web3.eth.defaultAccount = web3.eth.accounts[0];
```

将合约的 ABI 黏贴进 js 中:

```
var infoContract = web3.eth.contract(PASTE ABI HERE!);
```

合约地址

```
var info = InfoContract.at('PASTE CONTRACT ADDRESS HERE');
```

- 总结:

对于第一次编写 Dapp, 在整个项目进程中碰到不少麻烦, 有些在与老师、同学的交流找到解决方案, 部分问题仍在尝试不同的解决方法。

整体来说, 我认为本次的实作中仍有很大的进步空间, 从合约构想、功能设计、前端整合都有改进之处。在前端的部分, 本次是采用动态网页的方式进行展示, 由于对 html、js 了解的程度较初步, 所以目前还无法在前端设计上完整整合智能合约的各项功能, 使得合约也无法实现较复杂的农, 未来会在前端设计的短处加大学习力度并很好整合智能合约。

在合约调用中碰到最大的难题是在 address 类型中调用 balance 属性返回值为空, 这导致合约在有交易、金钱流动的地方会执行失败, 关于该问题目前还没找到适当的解答, 因此, 我采用充值的概念为替代方案, 在合约中加入 mapping (address=>uint) 的类型纪录充值金额, 再利用该金额进行交易。

未来可以加入第三方支付机构进行充值, 使更广大的用户可以不需透过以太币才能进行消费, 增加 Dapp 的实用性。

- Reference:

1. Interacting with Smart Contract through Web3.js
[https://coursetro.com/posts/code/99/Interacting-with-a-Smart-Contract-through-Web3.js-\(Tutorial\)](https://coursetro.com/posts/code/99/Interacting-with-a-Smart-Contract-through-Web3.js-(Tutorial))
2. Web3.js API Document
<http://web3.tryblockchain.org/>
3. 以太坊详解与实战
4. Javascript 教程
<https://www.liaoxuefeng.com/wiki/001434446689867b27157e896e74d51a89c25cc8b43bdb3000>