期末项目制品文档

所有源码Github地址：https://github.com/Runner1014/SafeOnlineShop

一、选题背景与依据

在互联网的背景下，网购因其便捷、便宜，已成为人们购物的主要方式之一。但其中还是存在一些问题。

第一，由于大数据平台对数据的贩卖，网购容易导致**泄露用户隐私**，比如刚刚浏览某个购物网站，在其他的社交平台上就会看到类似的广告弹窗。这是由于网购平台是一个**中心化**的平台，所有的用户数据都由一个中心集中管理，尽管声称会保护用户隐私，但数据毕竟掌握在中心平台手中，用户失去了对数据的自主控制权，所有的行动都要基于对第三方平台的信任。

第二，网购所有的交易也是基于对第三方支付的**信任**，一旦"第三方总是诚信的"这一基础崩塌的话，就可能会造成莫大的损失。

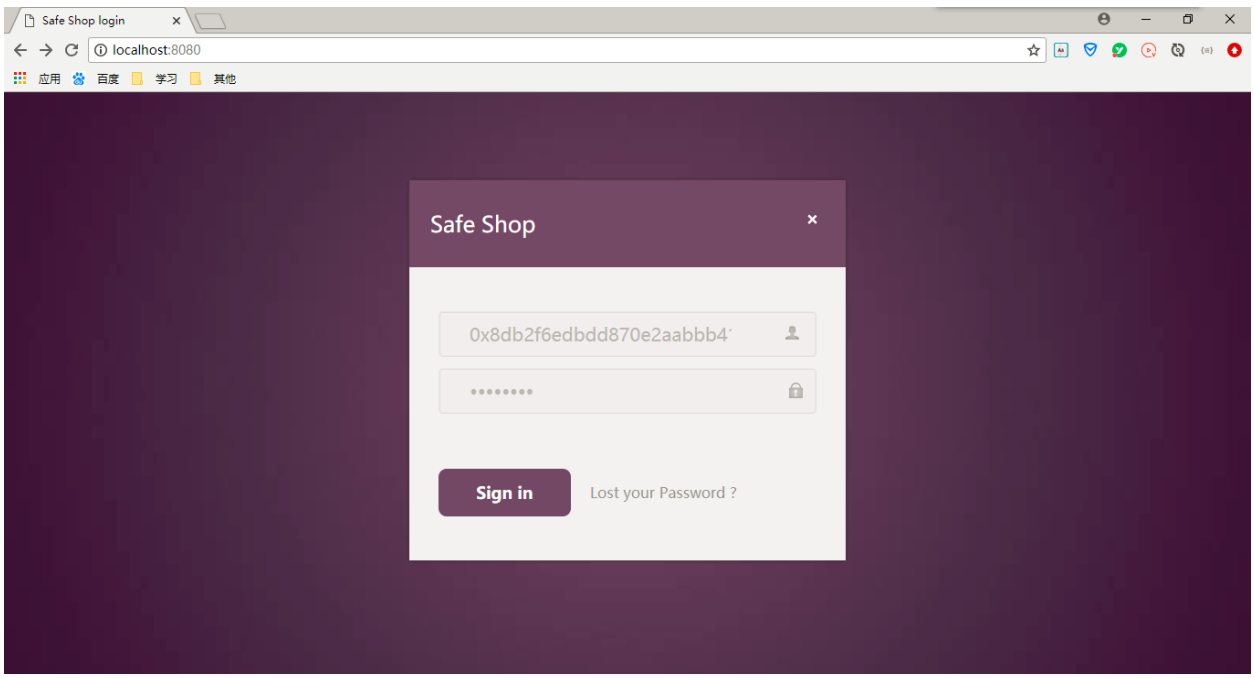
这几个问题都可以在区块链上得到解决。首先，在区块链上，用户的所有交易都是**匿名**的，不会泄露用户信息；第二，交易由哈希加密确保安全性，不用通过第三方，即**去中心化**，自然就不用担心第三方的信任问题，并且所有的交易由智能合约规定的逻辑自动执行，只要智能合约的逻辑被被接受且能抵抗攻击，则交易就是安全的，并且所有交易和购买记录可在区块链和智能合约上**追溯**，且**不可篡改**。

与一般的网购平台相比，基于区块链的网上安全商铺有以下优点：去中心化，用户不用向第三方平台泄露信息，从而**对个人信息有更大的控制权**；交易不通过第三方，**规避了第三方信任的风险**，交易记录可追溯且不可篡改。

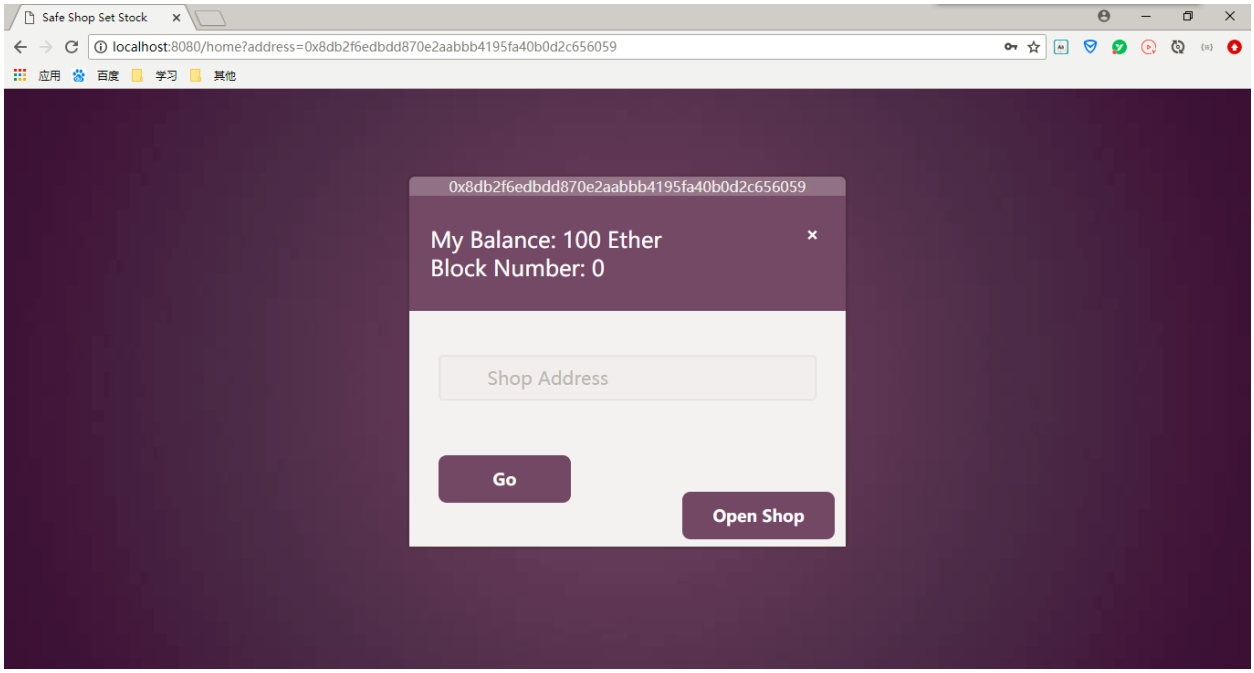
二、使用说明

- 登录

  在首页输入账户地址，点击 "Sign in" 进入个人主页。

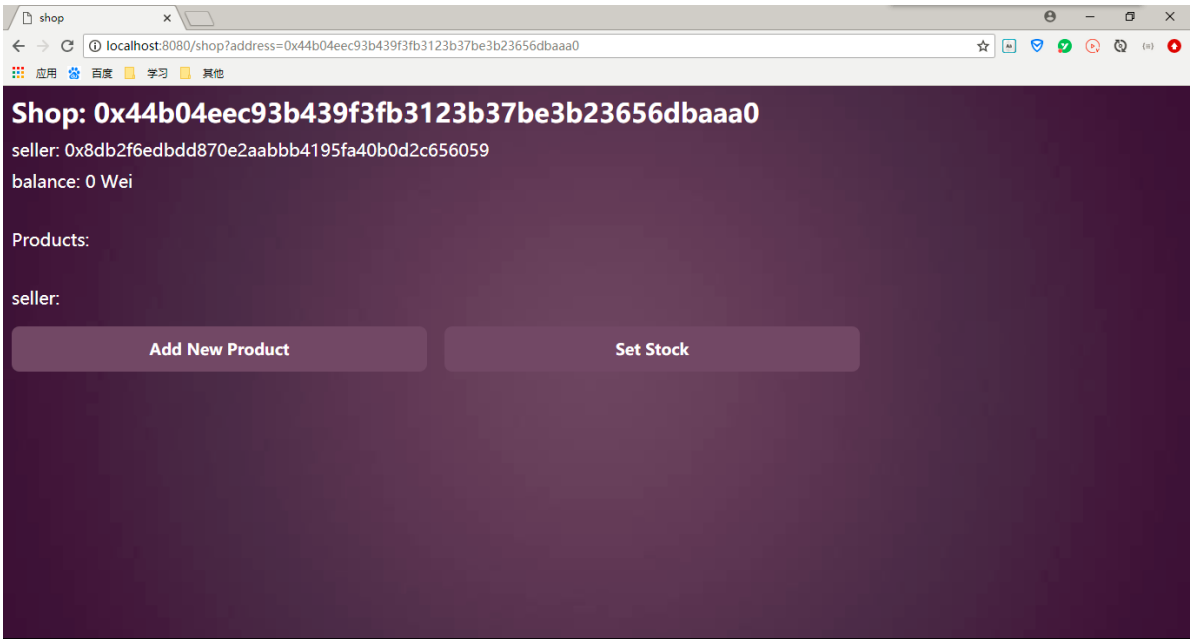


- 个人主页



  - 显示个人地址，余额，区块数
  - 点击 “Open Shop” 可以开一家属于自己的网上商铺（部署一个合约），成功后会直接跳转到商店页面；
  - 或者输入商店地址（合约地址），点击 “Go” 跳转到商店页面
- 商店页面
  - 显示商店地址，卖家账户地址，商店（合约）余额，商品列表，以及可以进行的一些操作
  - 卖家

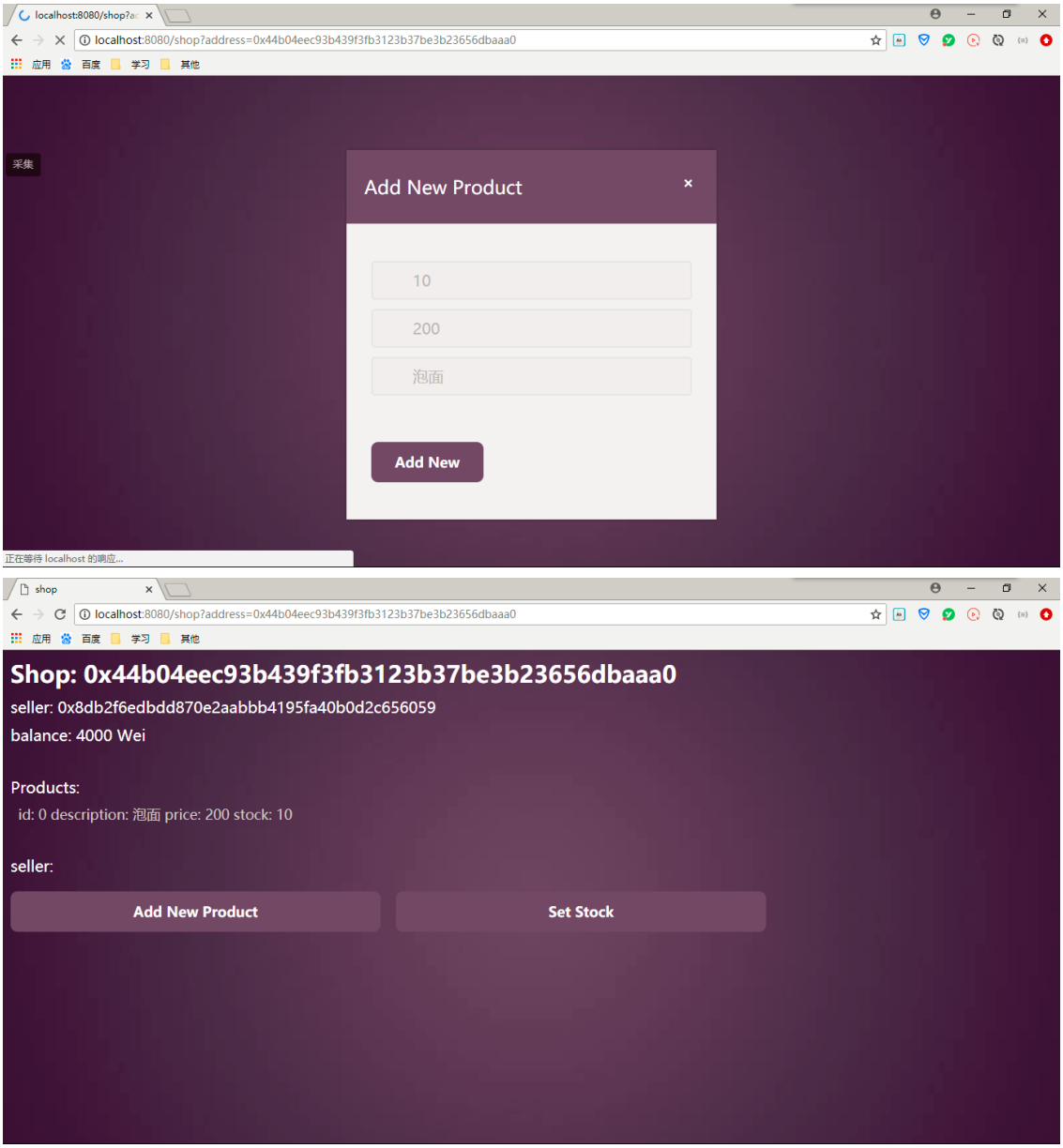
    若当前账户为商店卖家，则会显示 “Add New Product” 和 “Set Stock" 两个按钮。



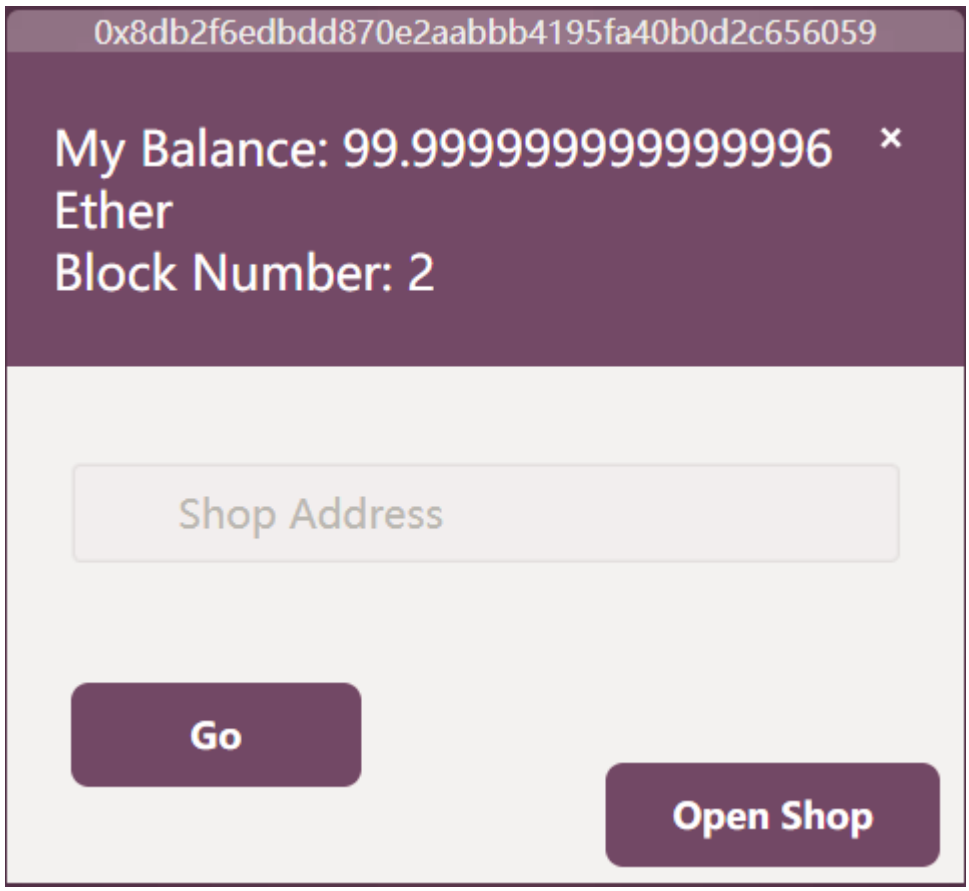
    - 添加商品

      点击 "Add New Product"，进入添加商品界面

输入个数，价格，以及商品描述，点击“Add New”，添加成功后会跳转回商店界面，商品列表新增条目，每个条目包括：商品id、描述、价格（以Wei为单位）、库存



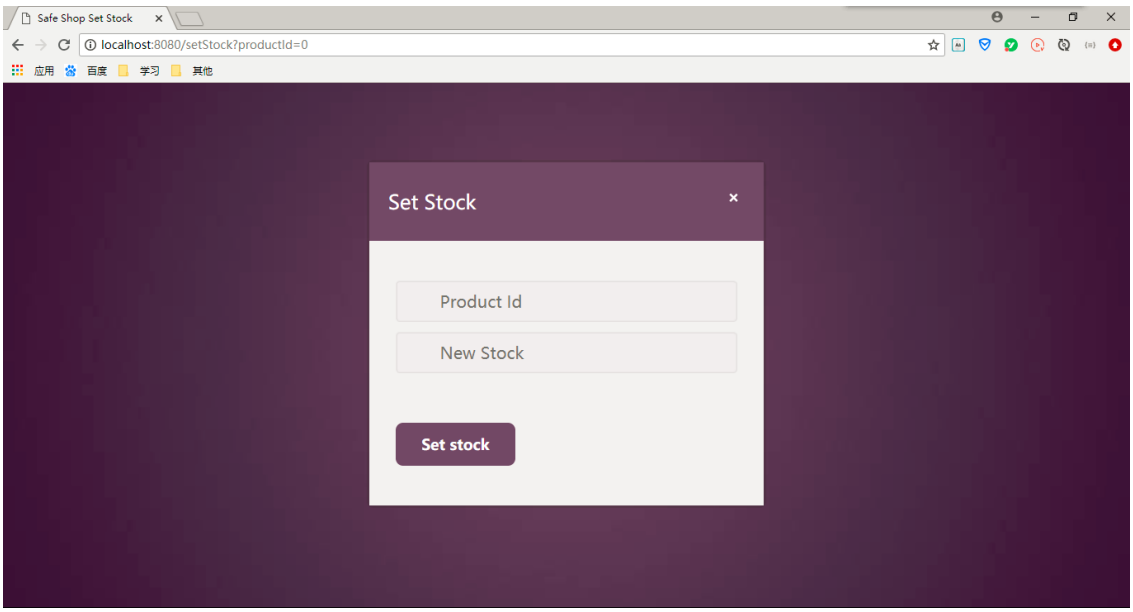
由于商家需要给商品两倍价格的保证金，所以此时商店的余额已经变为200 * 10 * 2 = 4000 Wei，返回看卖家的余额也会减少相应值：（为方便测试已将gasPrice设为0）

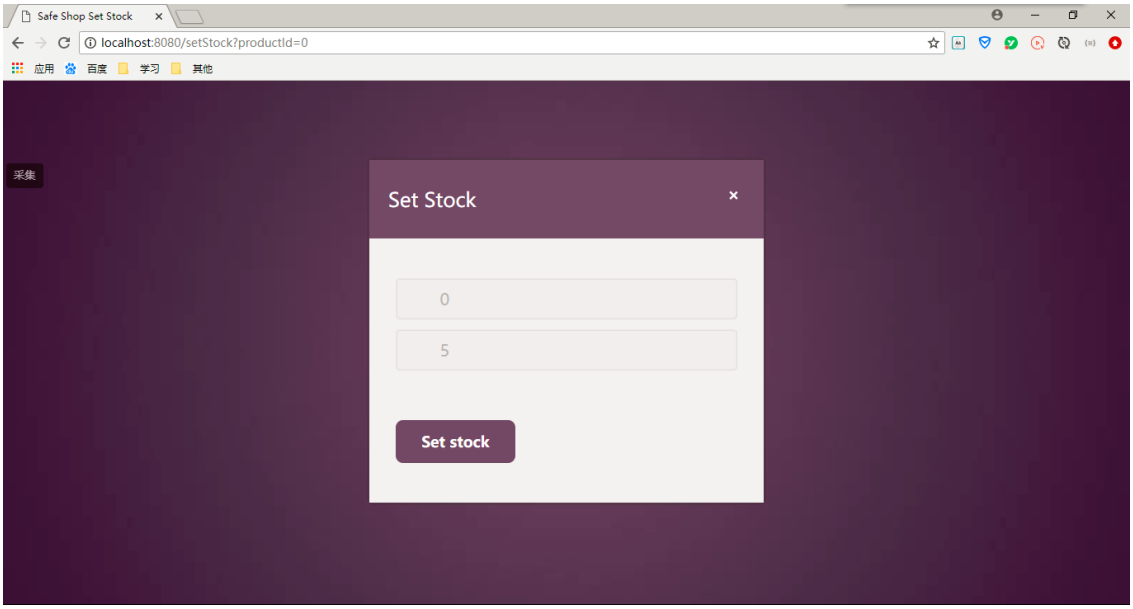


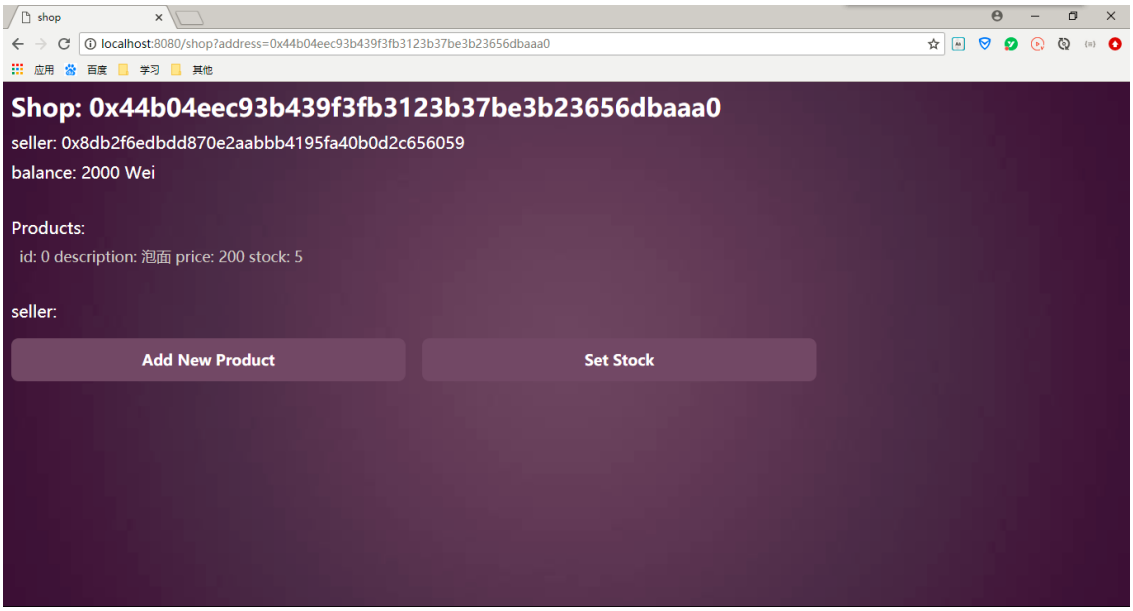
- 设置库存

  在商店界面点击 "Set Stock" 或者直接点击商品条目可以设置商品的库存。

  跳转到设置库存的界面，输入商品id（若是点击商品条目进来的，则商品id已经自动设好，不用输入）以及新的库存，点击 "Set stock"，若设置成功则会返回商店界面。





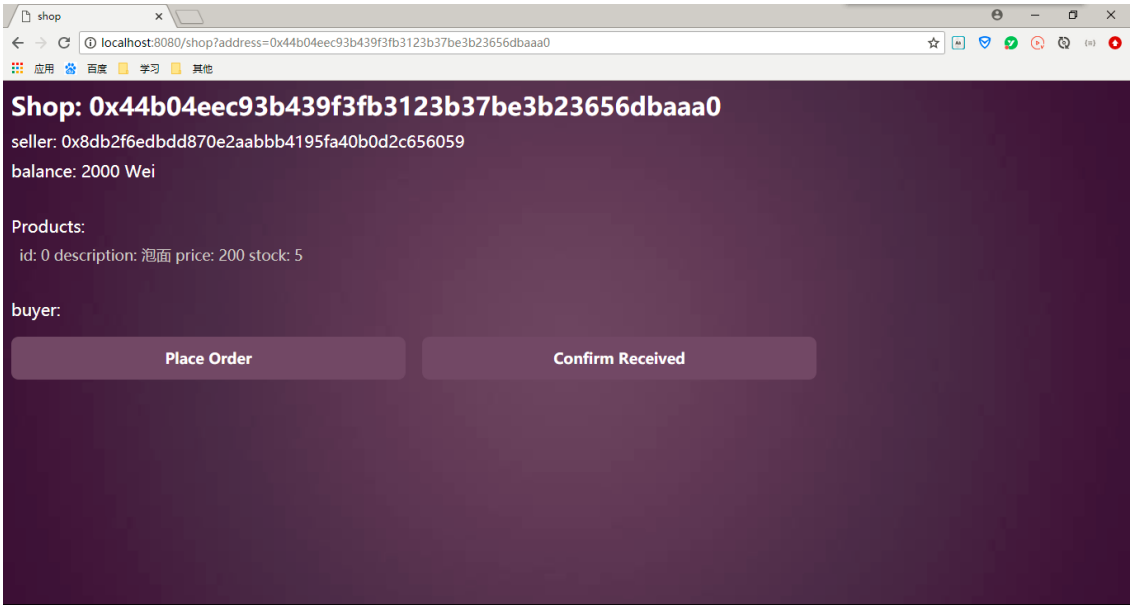


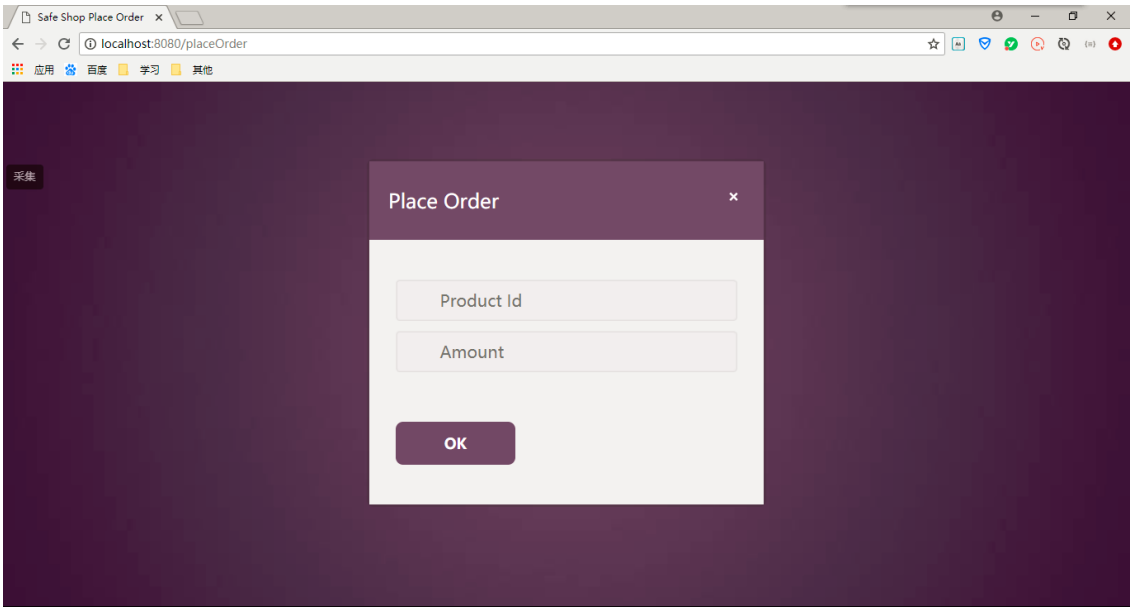
- 买家

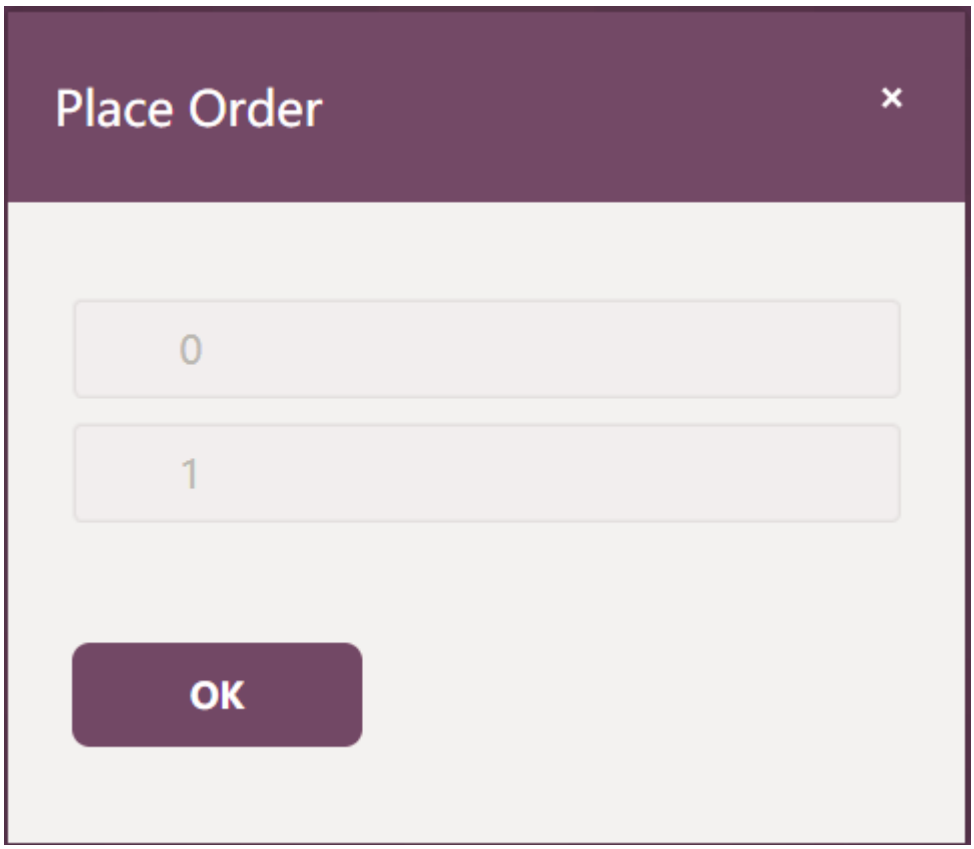
  若当前账户为不为商店卖家，即为买家，则会显示 “Place Order” 和 “Confirm Received" 两个按钮

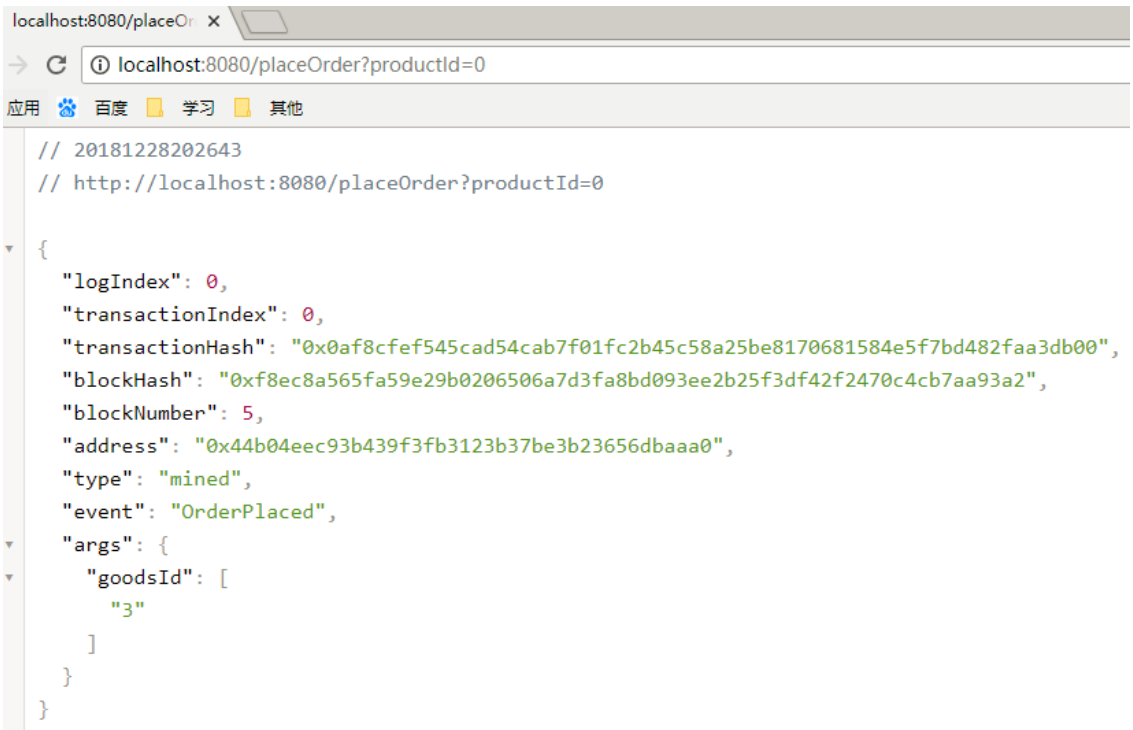
  - 下订单

    点击Place Order或者直接点击商品条目进入下订单页面，输入商品id（若是点击商品条目进来的，则商品id已经自动生成，不用输入）和购买数量，即可下订单，若下达订单成功，则会返回交易哈希和合约地址等重要数据，其中的goodsId对应商店的唯一一个具体商品实体，用来确认收货时输入，并可根据此id搜索到该商品的买家、卖家、状态等信息，是该合约的安全保障。


shop
localhost:8080/shop?address=0x44b04eec93b439f3fb3123b37be3b23656dbaaa0
应用 百度 学习 其他
Shop: 0x44b04eec93b439f3fb3123b37be3b23656dbaaa0
seller: 0x8db2f6edbdd870e2aabbb4195fa40b0d2c656059
balance: 2000 Wei
Products:
id: 0 description: 泡面 price: 200 stock: 5
buyer:
Place Order
Confirm Received


Safe Shop Place Order
localhost:8080/placeOrder
应用 百度 学习 其他
采集
Place Order
Product Id
Amount
OK



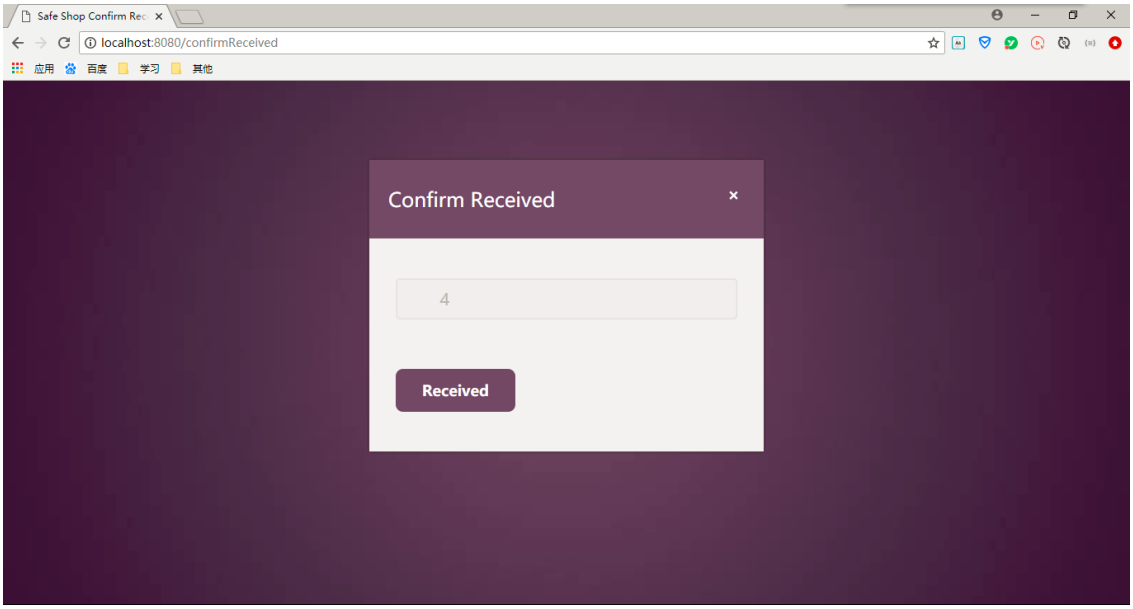


再回去看买家的余额，减少了相应金额。

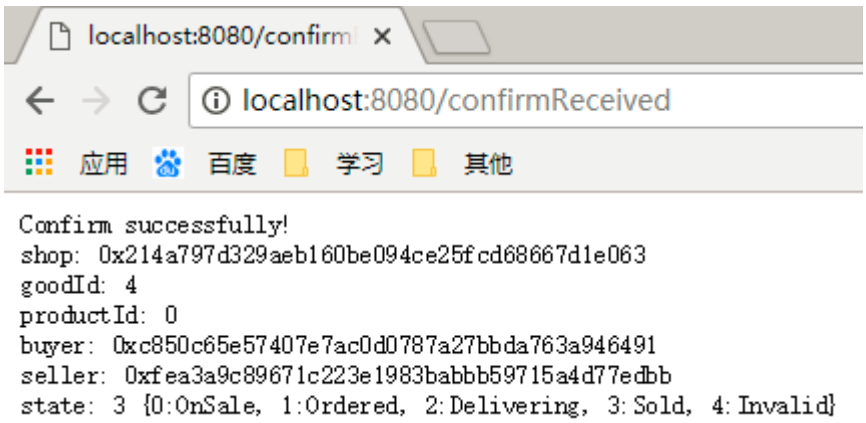
- 确认收货

  点击Confirm Received，跳转到确认收货界面，输入下订单时返回的商品唯一标识goodsId，点击Received，即可确认收货，此时商店会把该商品的价格的三倍金额返回给商家，一倍价格的金额返回给买家，这样商家就收回了保证金以及卖出的收入，买家则收回下订单时给出的多出一倍的金额。这个机制可以督促卖家发货，买家确认收货。（下图与上述操作不同步，同步的完整操作过程

见测试部分）



确认收货成功，会返回该商品的商店地址、买家地址、卖家地址、以及商品状态等信息，可以作为购买凭证。



三、测试

- 运行ganache-cli

  运行ganache-cli，生成十个账户地址，为了方便测试，将gasPrice设置为0

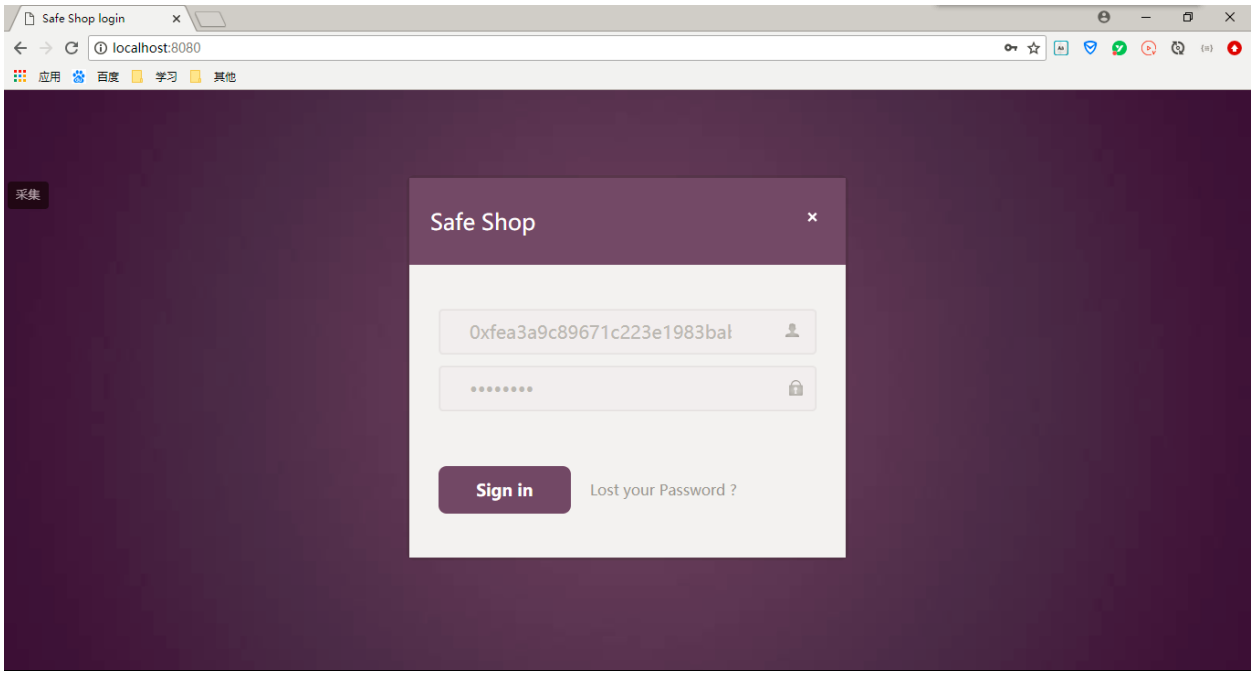
```
PS D:\program\nodejs\node_global\node_modules\.bin> .\ganache-cli -l 99999999999999 -g 0
Ganache CLI v6.2.5 (ganache-core: 2.3.3)

Available Accounts
==================
(0) 0xfea3a9c89671c223e1983babbb59715a4d77edbb (~100 ETH)
(1) 0xc850c65e57407e7ac0d0787a27bbda763a946491 (~100 ETH)
(2) 0xc67f9c0d7f0a451d1ebb9bc7e06d2f0b8b44c390 (~100 ETH)
(3) 0xc5fe5ff2ac8e01de2a97d4d1cc81e975813089c8 (~100 ETH)
(4) 0x898889ee47c0120e4e544c8b5977610337812 1d2 (~100 ETH)
(5) 0xf324dd81d1ef4459fa082a357b6cb1de7efc52cd (~100 ETH)
(6) 0xe3cd06252a7ac2dd7a41be1e49735dd977efcc55 (~100 ETH)
(7) 0x1c7983c0dd51dce214c6a9f610c87b862d5343d6 (~100 ETH)
(8) 0x2d55aaacf0355f5c114aed6b9eedd9f7f1cd60ed (~100 ETH)
(9) 0x2c6687bf2184ea626a79c6d21107c8a61d5989f9 (~100 ETH)

Private Keys
==================
(0) 0x4f6f3f4c74aca029dd4f60d3f07b9c6f435b8e8ca9778da6fc53de6b3486ed92
(1) 0x81f3d8ed879937733765d67c7a8f108f6fbc1ea19cfce560934b0f22f0660b06
(2) 0xd671967fbc0fb7126ce93f313a6bf34017b83675174083b1ec1bc03c75874612
(3) 0xe50e406356eaecad06808e497158636a71b49ed028b34024262fc4c43f7c97cc
(4) 0xdb86629c81ea4a597676c8aae302917dcb95c375318d33ddce1e8472d832b307
(5) 0x04045c1b74ce754473f54b79b97bb1505275bfcacee4485e9d1deb0563f3ba02
(6) 0x558687697e16fdc80a3318fcfa998e6e8cd0287207a49ad7897f36b439512530
(7) 0xf479a5870483c60c328cd69969cba14129101533acfc04faa5554aa22efdfb1d
>
(9) 0xce9ac1fd160c39cde9b23b5a932b71422c78c069b756bdd3dddc16cd6a9365e6
```

- 运行程序

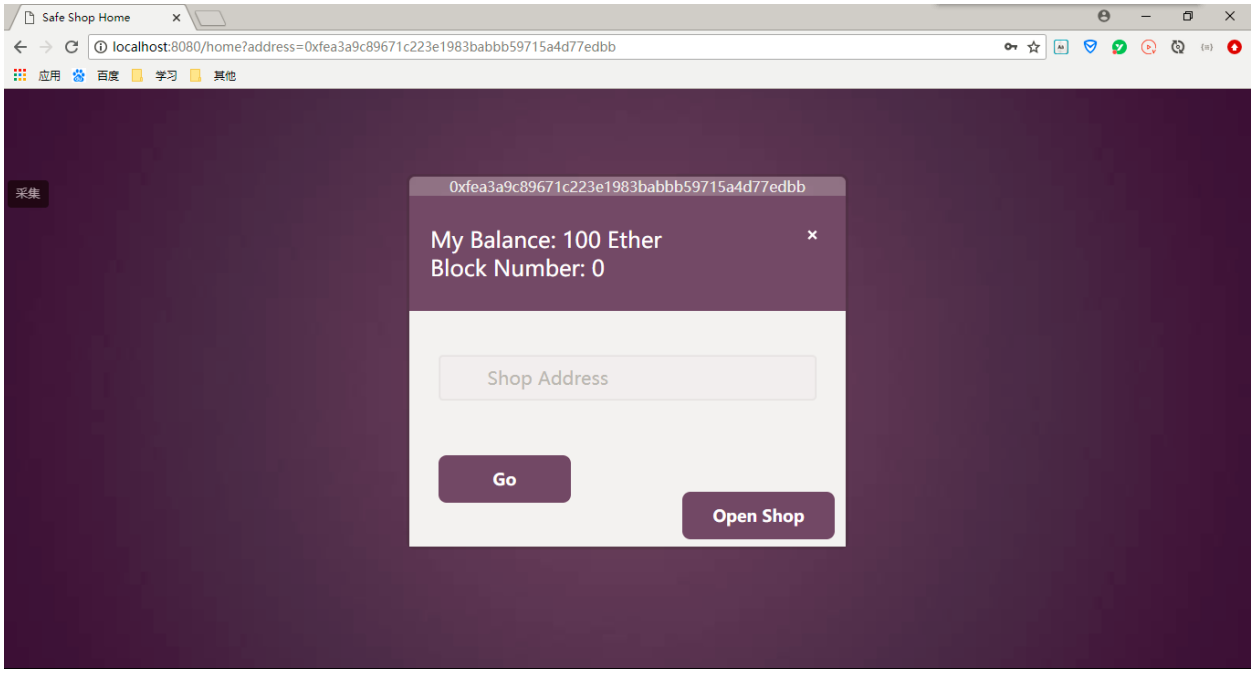
```
PS D:\nodeWorkspace\express> node .\index.js
gasPrice:  0
```

- 登录

  在首页输入第一个测试账户地址，点击 "Sign in" 进入个人主页。



- 个人主页



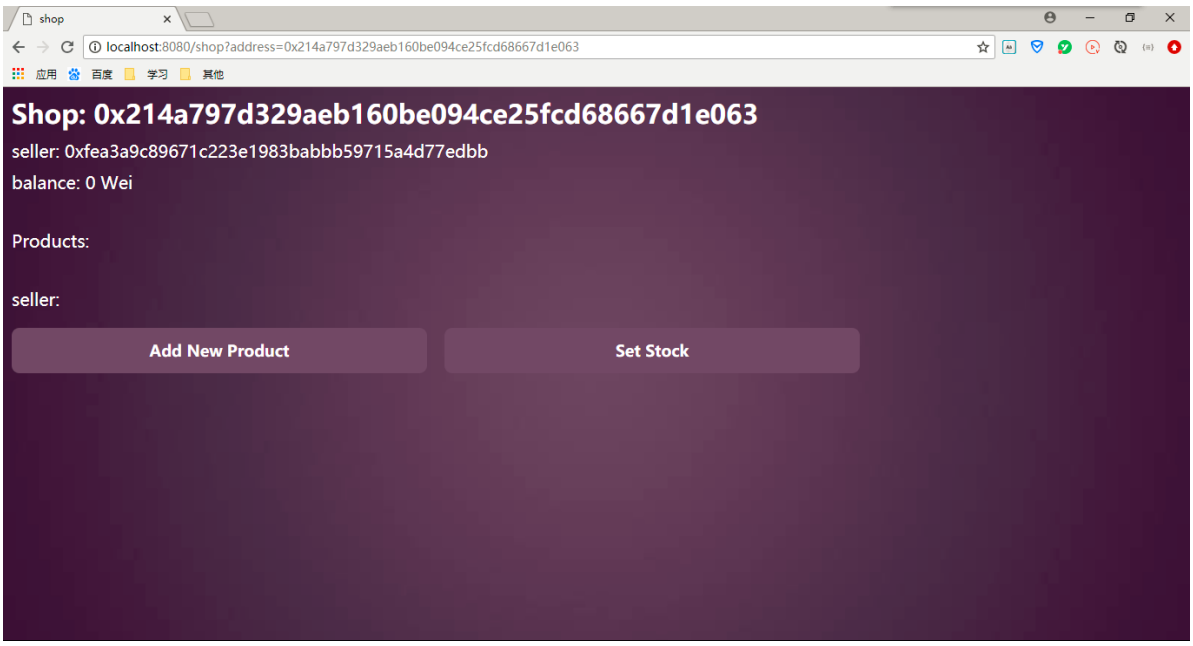
- 显示个人地址，余额，区块数
- 点击 “Open Shop” 开一家属于自己的网上商铺（部署一个合约），成功后直接跳转到商店页面；

  console：

```
account:  0xfea3a9c89671c223e1983babbb59715a4d77edbb
deploy transaction hash:0x825afb3164ef474d30bf94c60ab9691263ee9c4e5e5275bd356c31915c0f3edb
Please waiting...
deploy successfully, you shop contract address is:  0x214a797d329aeb160be094ce25fcd68667d1e063
shop:  0x214a797d329aeb160be094ce25fcd68667d1e063
seller: 0xfea3a9c89671c223e1983babbb59715a4d77edbb
```

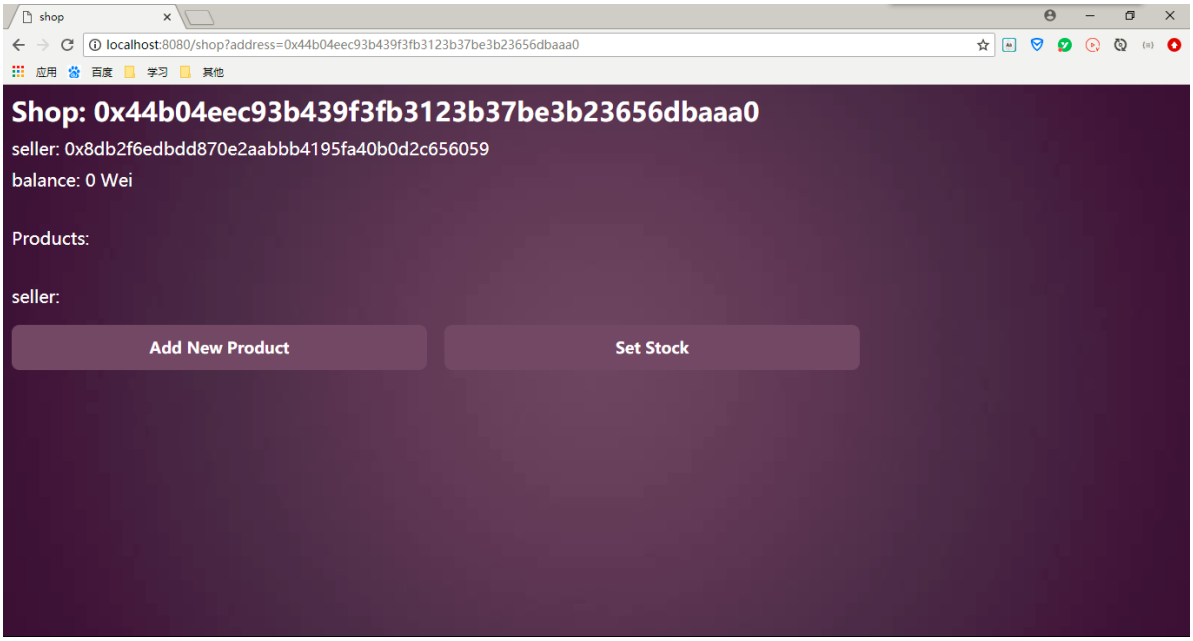
  ganache-cli:

```
eth_sendTransaction

  Transaction: 0x825afb3164ef474d30bf94c60ab9691263ee9c4e5e5275bd356c31915c0f3edb
  Contract created: 0x214a797d329aeb160be094ce25fcd68667d1e063
  Gas usage: 2400862
  Block Number: 1
  Block Time: Fri Dec 28 2018 21:18:49 GMT+0800 (中国标准时间)
```



- 商店界面显示商店地址，卖家账户地址，商店（合约）余额，商品列表，以及可以进行的一些操作
- 卖家

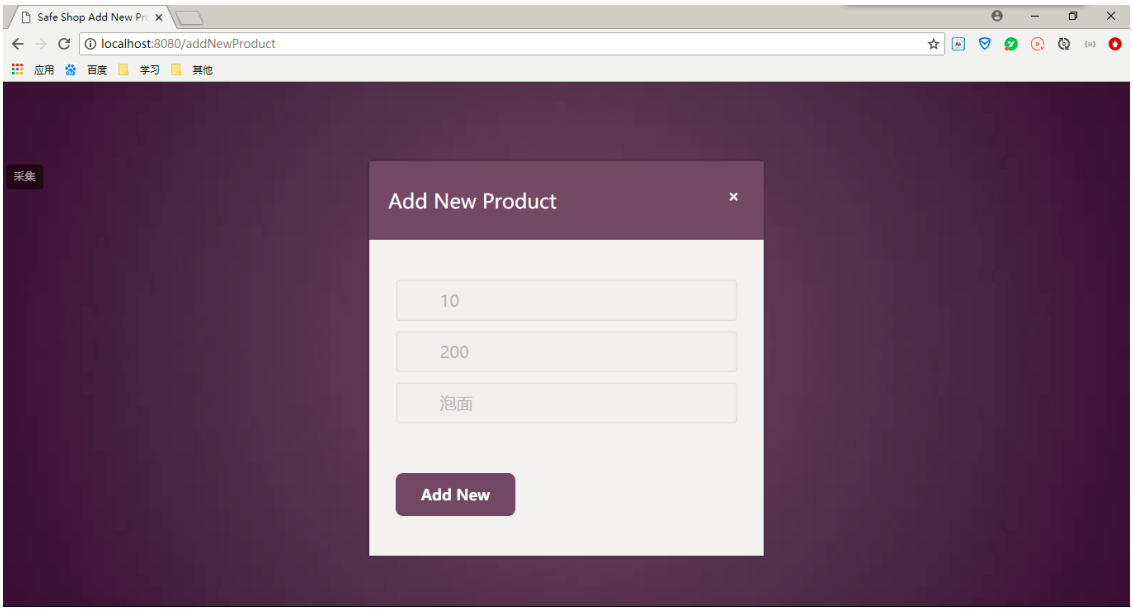
  当前账户为商店卖家，则会显示 “Add New Product” 和 “Set Stock" 两个按钮。



  - 添加商品

    点击 "Add New Product"，进入添加商品界面。

    输入个数，价格，以及商品描述，点击 “Add New”。



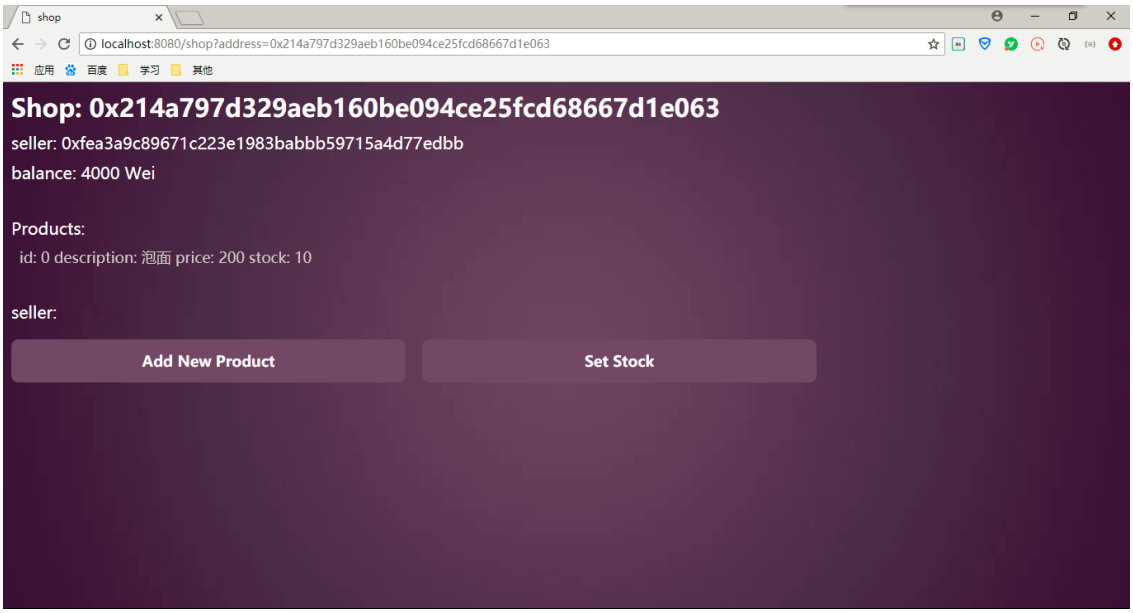
    console：

```
tx Hash: 0x9b4b1e2a476d8eb7d282c9da2ba799014c882ba316c8c95a0886c28422fb9988
add new product result:  { logIndex: 0,
  transactionIndex: 0,
  transactionHash: '0x9b4b1e2a476d8eb7d282c9da2ba799014c882ba316c8c95a0886c28422fb9988',
  blockHash: '0x643596a9210ac0c986e0594fee200334349ad52db304806d02dbb46996aae7a5',
  blockNumber: 2,
  address: '0x214a797d329aeb160be094ce25fcd68667d1e063',
  type: 'mined',
  event: 'AddNewProductOK',
  args: {} }
shop:  0x214a797d329aeb160be094ce25fcd68667d1e063
seller: 0xfea3a9c89671c223e1983babbb59715a4d77edbb
```

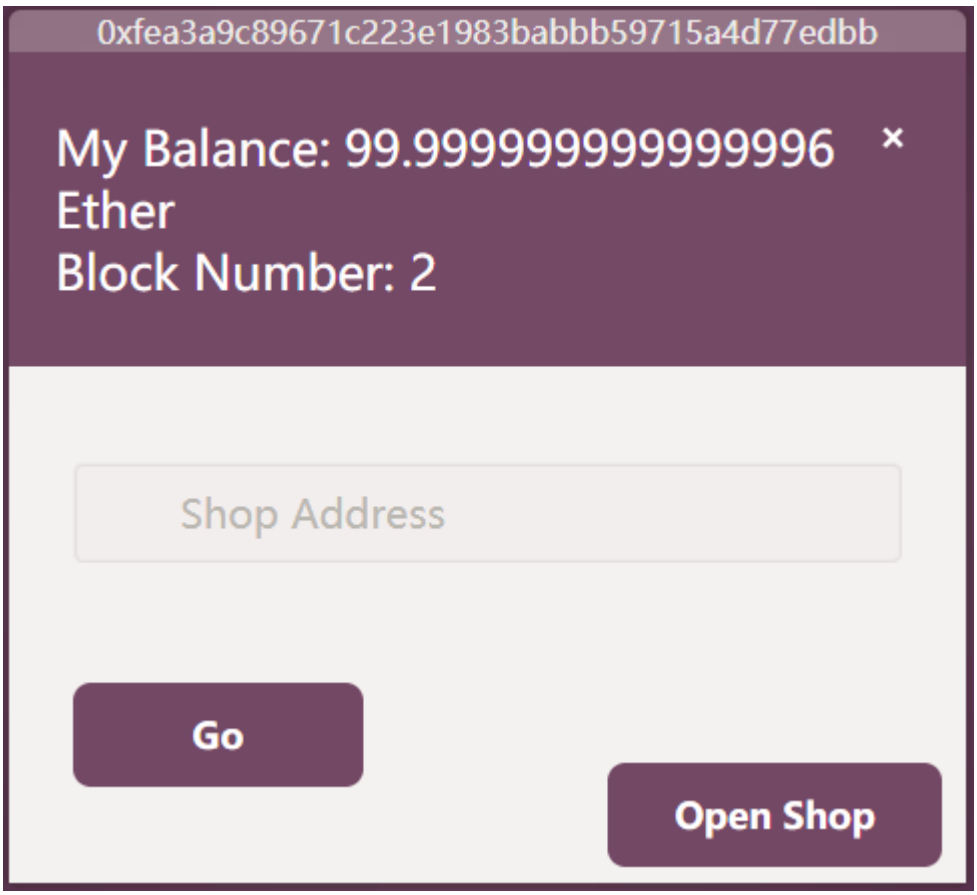
ganache-cli:

```
Transaction: 0x9b4b1e2a476d8eb7d282c9da2ba799014c882ba316c8c95a0886c28422fb9988
Gas usage: 960496
Block Number: 2
Block Time: Fri Dec 28 2018 21:25:33 GMT+0800 (中国标准时间)
```

添加成功后会跳转回商店界面，商品列表新增条目：

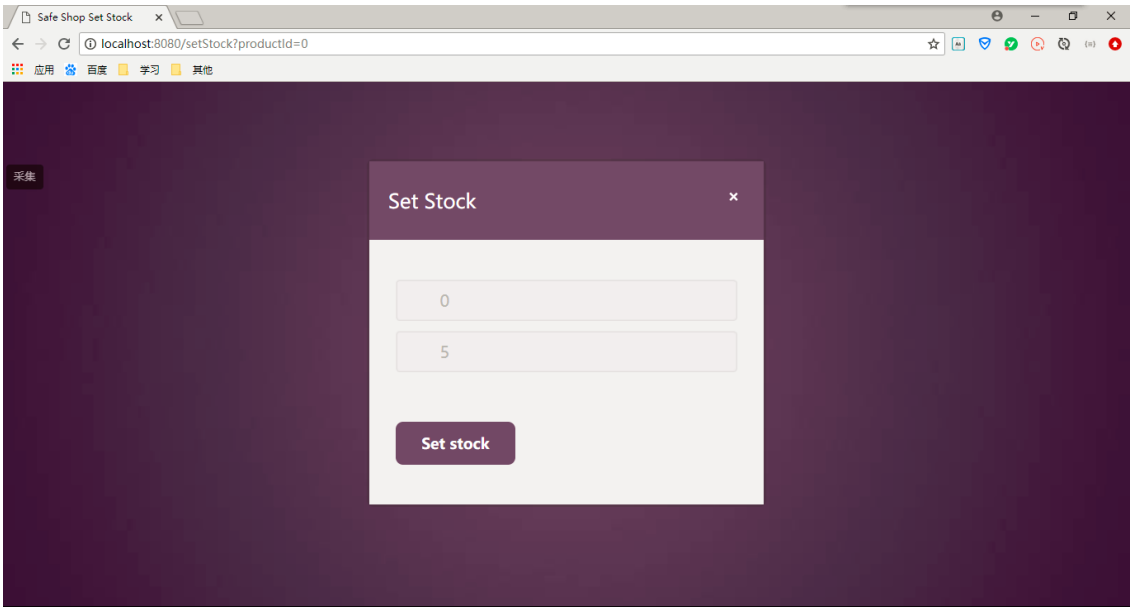


由于商家需要给商品两倍价格的保证金，所以此时商店的余额已经变为200 * 10 * 2 = 4000 Wei，返回看卖家的余额也会减少相应值：（为方便测试已将gasPrice设为0）



- 设置库存

  在商店界面直接点击商品条目设置商品的库存，设置成功返回商店界面。

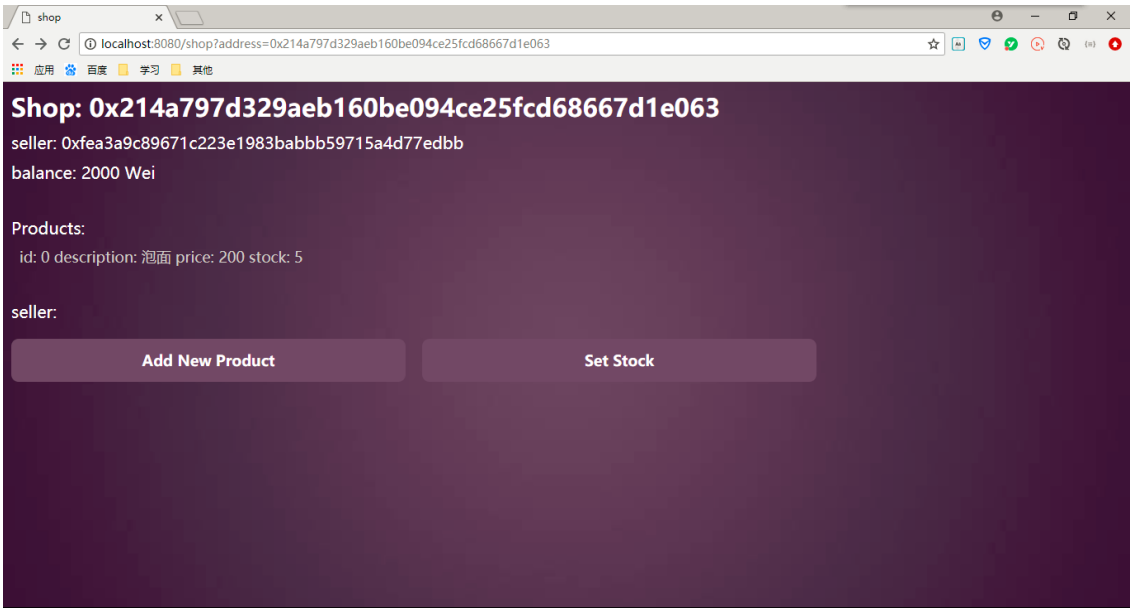


  console：

```
tx Hash: 0x62965aeb354165b4015e9af1fab49432c8cc092f1d2cda9a16c228a01efcad25
set stock result:  { logIndex: 0,
  transactionIndex: 0,
  transactionHash: '0x62965aeb354165b4015e9af1fab49432c8cc092f1d2cda9a16c228a01efcad25',
  blockHash: '0xb31790af857b4e97f3fe40d26548c8f9054774094ceb420326161b5cfd99b566',
  blockNumber: 3,
  address: '0x214a797d329aeb160be094ce25fcd68667d1e063',
  type: 'mined',
  event: 'StockSet',
  args: {} }
shop:  0x214a797d329aeb160be094ce25fcd68667d1e063
seller: 0xfea3a9c89671c223e1983babbb59715a4d77edbb
```

ganache-cli:

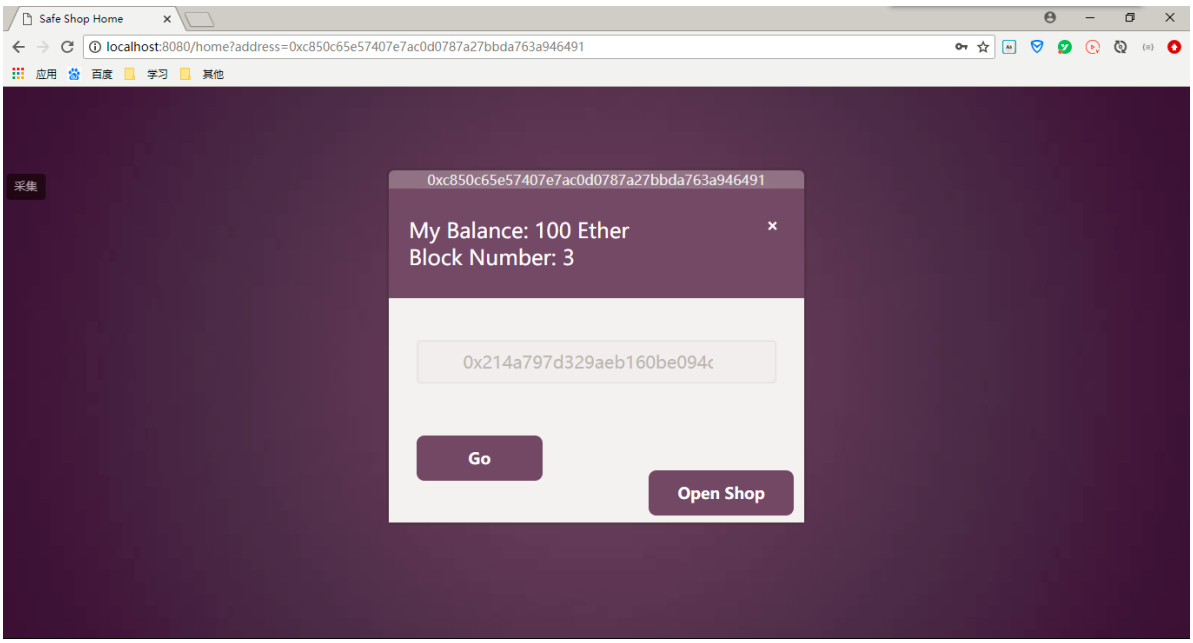
```
Transaction: 0x62965aeb354165b4015e9af1fab49432c8cc092f1d2cda9a16c228a01efcad25
Gas usage: 39231
Block Number: 3
Block Time: Fri Dec 28 2018 21:28:59 GMT+0800 (中国标准时间)
```



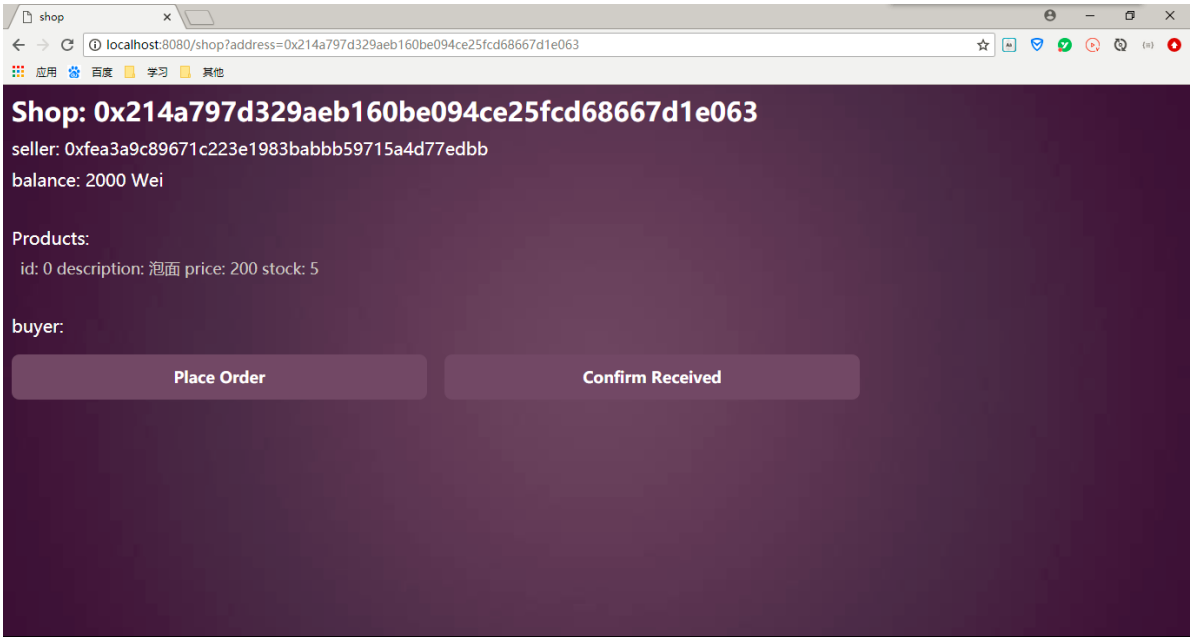
可见商品库存已经相应改变，商店余额也相应变为200 * 5 * 2 = 2000 Wei。

- 买家

  用第二个账户登录，输入以上商店的地址，点击Go，进入该商店。

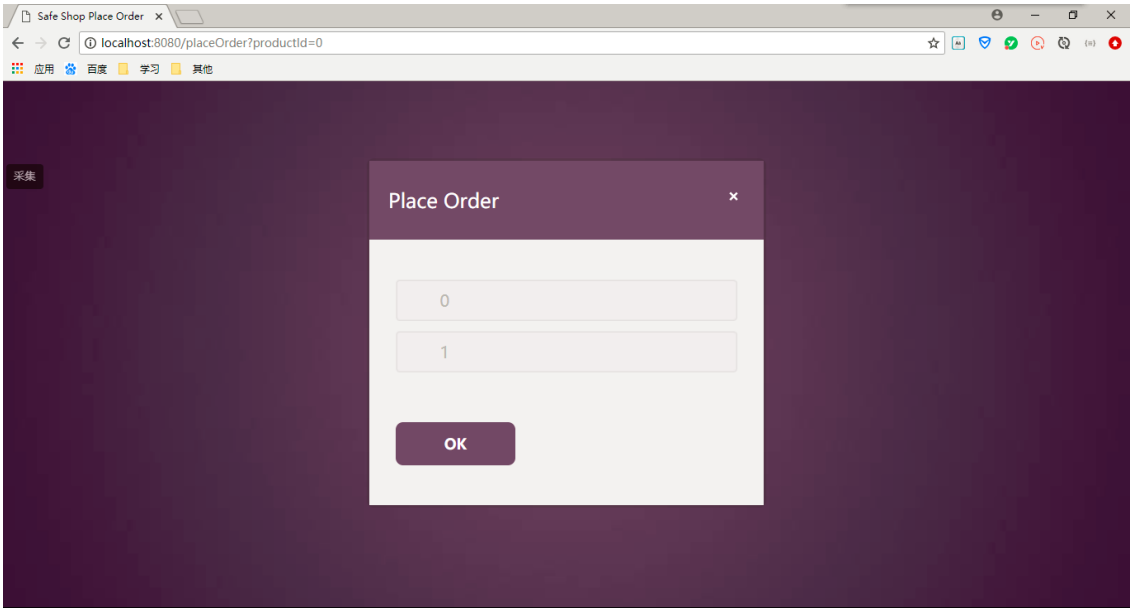


当前账户为不为商店卖家，即为买家，则会显示 “Place Order” 和 “Confirm Received" 两个按钮。

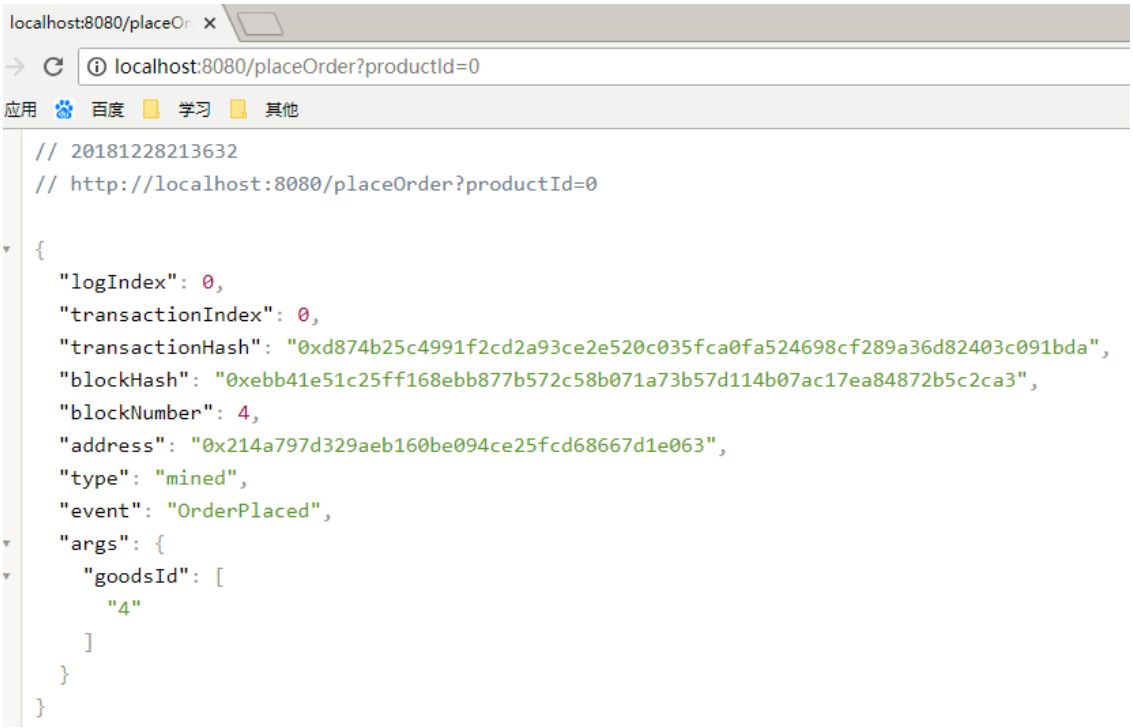


- 下订单

  直接点击商品条目进入下订单页面，输入商品id（若是点击商品条目进来的，则商品id已经自动生成，不用输入）和购买数量。



  点击OK下订单，下达订单成功，返回交易哈希和合约地址等重要数据，其中的goodsId对应商店的唯一一个具体商品实体，用来确认收货时输入，并可根据此id搜索到该商品的买家、卖家、状态等信息，是该合约的安全保障。



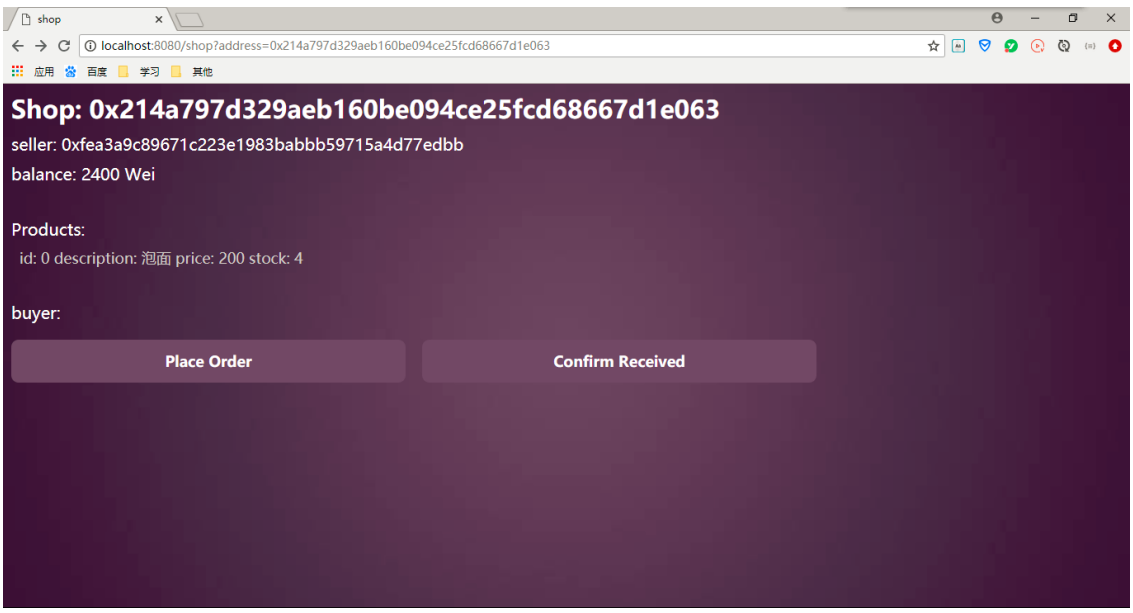
console:

```
account:  0xc850c65e57407e7ac0d0787a27bbda763a946491
shop:  0x214a797d329aeb160be094ce25fcd68667d1e063
seller: 0xfea3a9c89671c223e1983babbb59715a4d77edbb
tx Hash: 0xd874b25c4991f2cd2a93ce2e520c035fca0fa524698cf289a36d82403c091bda
result:  [ BigNumber { s: 1, e: 0, c: [ 4 ] } ]
```

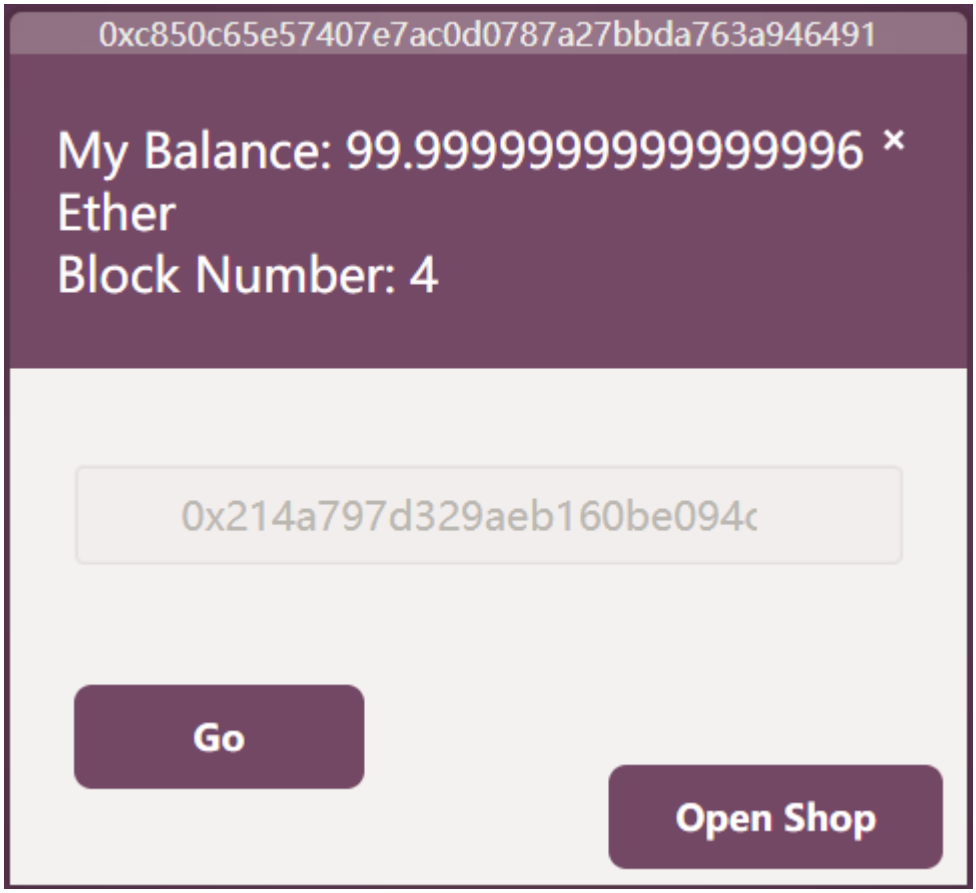
ganache-cli:

```
Transaction: 0xd874b25c4991f2cd2a93ce2e520c035fca0fa524698cf289a36d82403c091bda
Gas usage: 56337
Block Number: 4
Block Time: Fri Dec 28 2018 21:36:29 GMT+0800 (中国标准时间)
```

此时，买家需要先付两倍价格（确认收货时再退回一半），商店的余额从2000变为400，增加了200 * 1 * 2 = 400 Wei

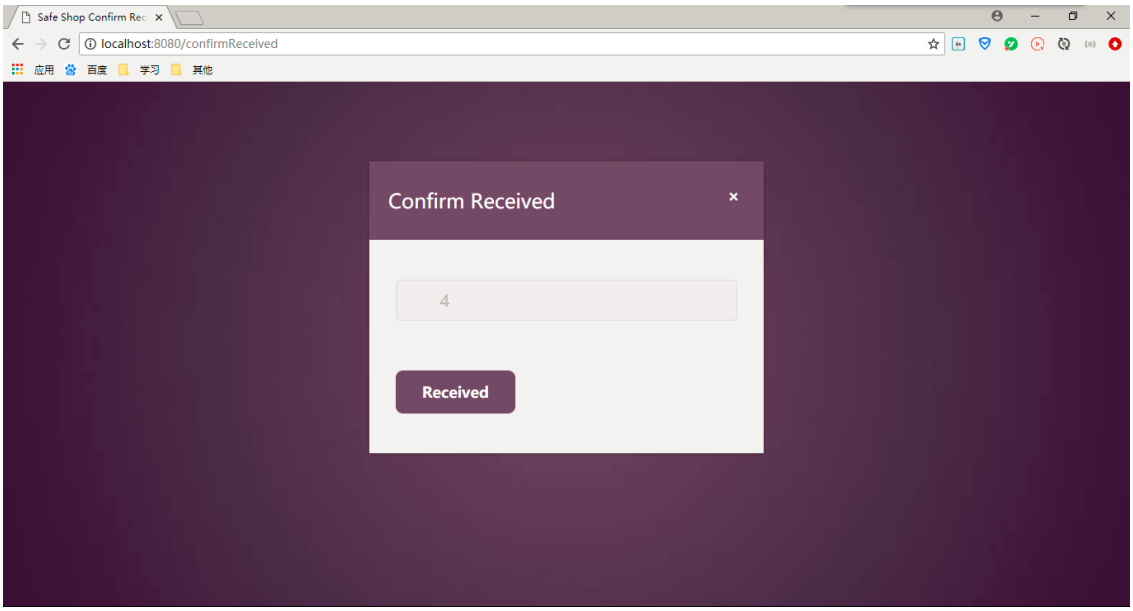


再回去看买家的余额，减少了相应金额。



- 确认收货

  点击Confirm Received，跳转到确认收货界面，输入下订单时返回的商品唯一标识goodsId，点击Received，确认收货。



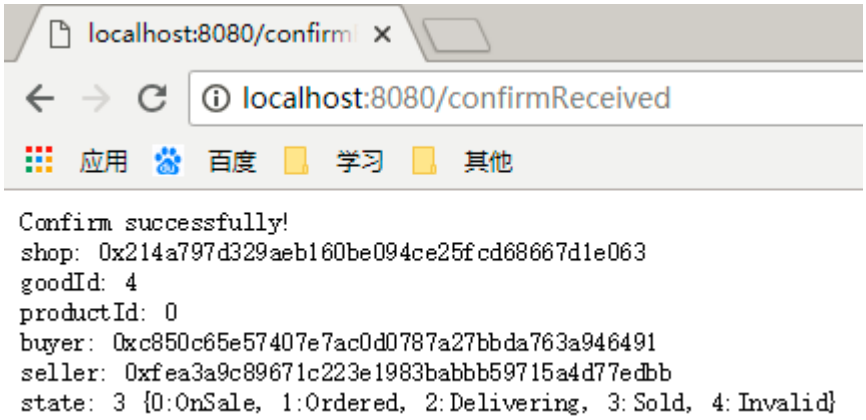
  console：

```
account:  0xc850c65e57407e7ac0d0787a27bbda763a946491
tx Hash: 0xe050b8345e92ab8dec8041d27bf5ef1afcff634839f4af240559a0b726206f2d
```

  ganache-cli：

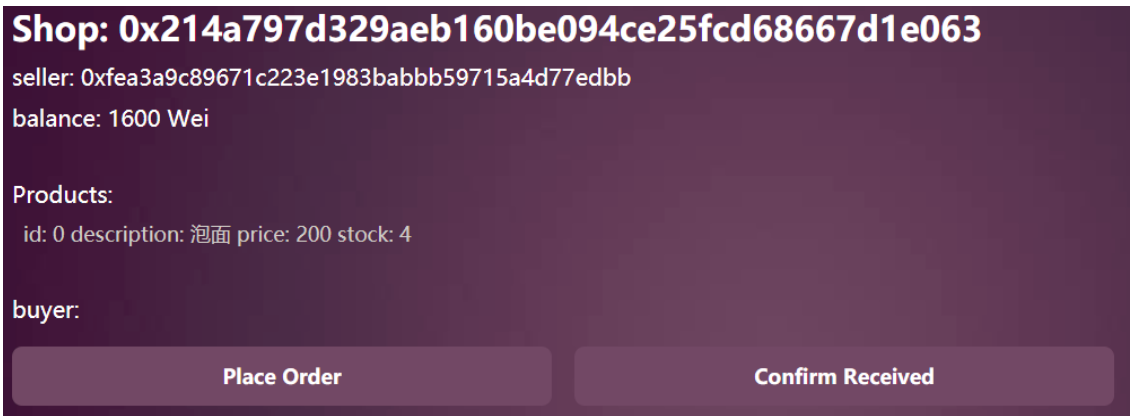
```
Transaction: 0xe050b8345e92ab8dec8041d27bf5ef1afcff634839f4af240559a0b726206f2d
Gas usage: 46105
Block Number: 5
Block Time: Fri Dec 28 2018 22:04:07 GMT+0800 (中国标准时间)
```

确认收货成功，会返回该商品的商店地址、买家地址、卖家地址、以及商品状态等信息，可以作为购买凭证。

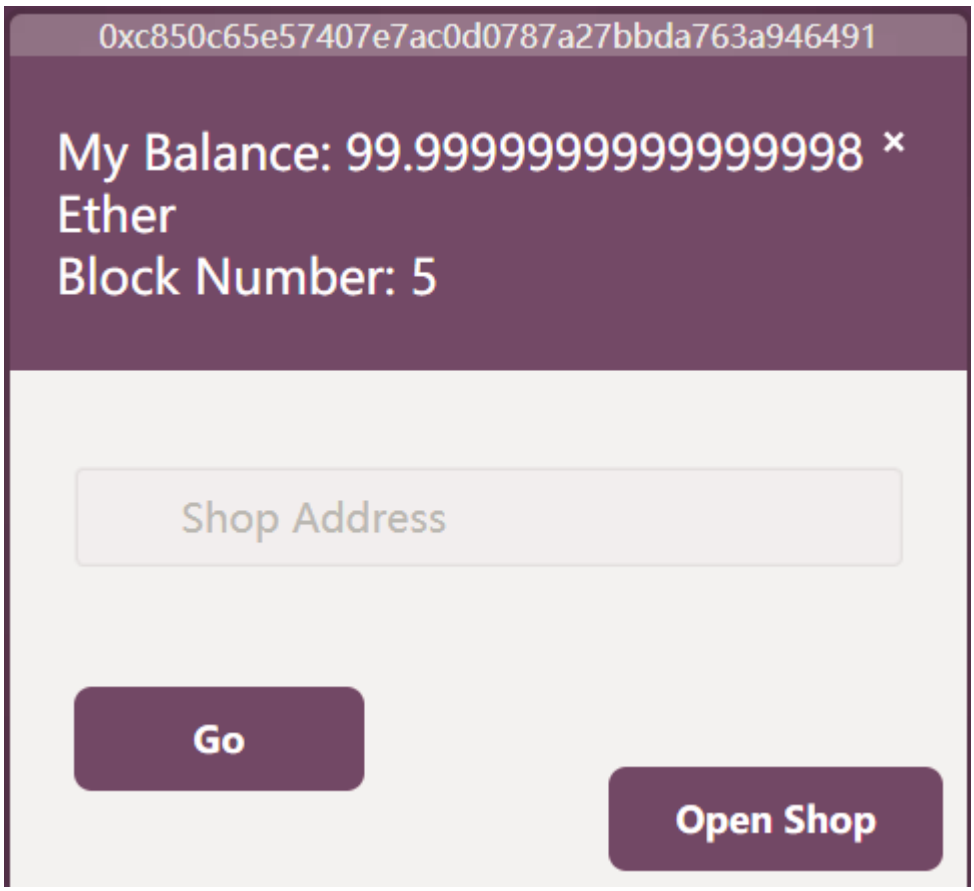


此时商店会把该商品的价格的三倍金额返回给商家，一倍价格的金额返回给买家，这样商家就收回了保证金以及卖出的收入，买家则收回下订单时给出的多出一倍的金额。这个机制可以督促卖家发货，买家确认收货。

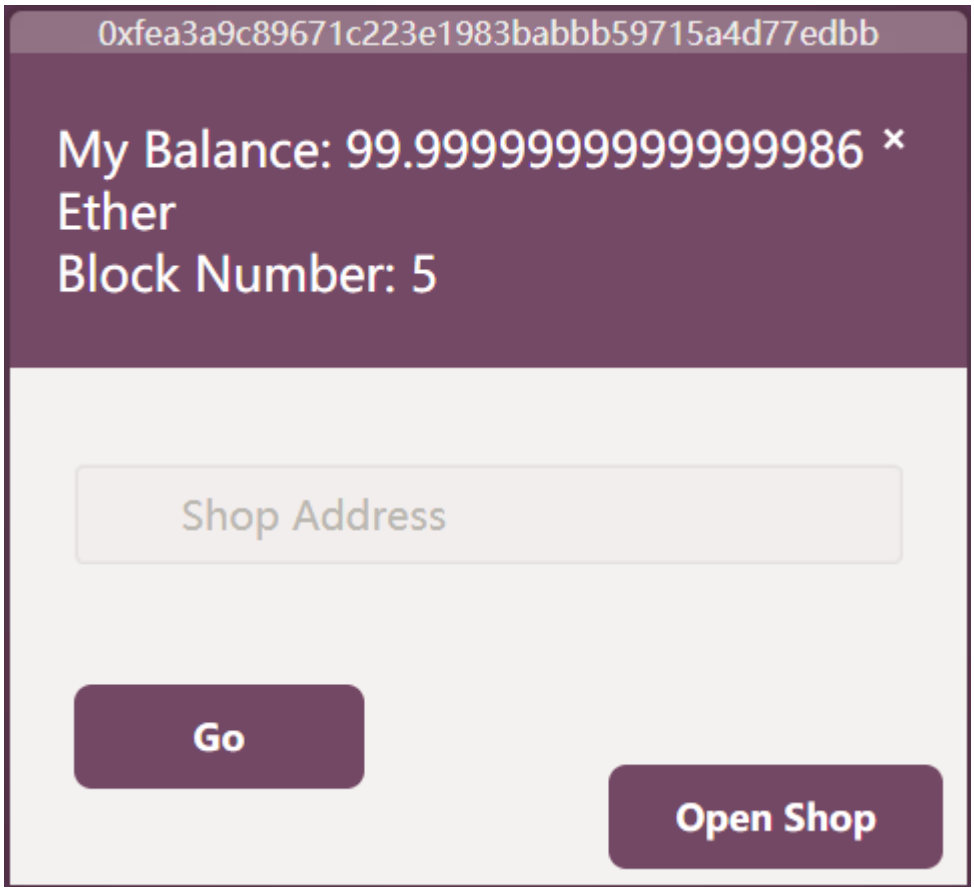
可见此时商店余额由2400变为1600，减少了 200 * 1 * 4 = 800。



买家的余额下订单时减少了400Wei，现在增加了200Wei，相当于花了200Wei：



再看买家的余额，增加了600Wei，收回了400Wei保证金，并收入200Wei：



所有源码Github地址：https://github.com/Runner1014/SafeOnlineShop

注：登录界面的模板代码来自 模板之家：http://www.cssmoban.com/cssthemes/7727.shtml