区块链最终报告

16340008 蔡梓珩

1. 所有源码 Github 地址：
   https://github.com/c980129/Blockchain-FinalProject

2. 选题背景、依据：
   项目的主题是利用区块链编写一个用于博彩的 Dapp。目前市面上的博彩应用大多高度中心化。中奖机制对于彩民而已就是一个黑盒子，彩民将赌资送入黑盒子，黑盒子反馈中奖情况并返回奖金（假如有的话）。我们大多难以知道中奖概率的真实情况，因为我们不知道其是否真的随机，或是否如数据公布一样。庄家很多时候可以根据彩民的选择分布选择一个对庄家而言最高收益的中奖号码，此时彩民的利益就会受到损害。类似的，如刮刮乐这种我们无法知道奖池内的中奖率是否真的属实（如同公布的一样），因为没有验证的方法，于是就给了庄家更多的操作空间。
   而如果开奖的操作依赖区块链（这可能需要智能合约的代码公开以获取玩家的信任），就可以避免庄家对奖池或者中奖号码的暗箱操作了。每个人都能知道智能合约的内容，并放心的调用智能合约，每个人都存储一份操作记录以及开奖记录，这样就能尽可能杜绝作弊的可能（虽然可能引入了矿工作弊的可能性）。

3. 使用说明：
   先在 dapp 目录下输入 truffle compile 执行，对 solidity 代码进行编译

```
C:\Users\azu\OneDrive\Course\blockchainprj\dapp>truffle compile
Compiling .\contracts\Migrations.sol...
Compiling .\contracts\gambling0.sol...
Compiling .\contracts\gambling1.sol...
Writing artifacts to .\build\contracts
```

   然后输入 truffle migrate 部署

```
C:\Users\azu\OneDrive\Course\blockchainprj\dapp>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


1_initial_migration.js
======================

   Deploying 'Migrations'
   ----------------------
   > transaction hash:    0x8a5a94b8d5d3d2fca6d677d39e0f469a715fa9c10bb28c424ed07b06bcdc6350
   > Blocks: 0            Seconds: 0
   > contract address:    0x7905Ce9B8aD77cccc314F042DDD4102e81F3B4a9
   > account:             0x939582533400Aa154669041fDB866112d7832400
   > balance:             9999.99430312
   > gas used:            284844
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.00569688 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:          0.00569688 ETH
```

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

   Deploying 'gambling1'
   ---------------------
   > transaction hash:    0xfd64c9c0334da7cc3d712d02972f29ce70ebdb1f90651fe06c295e2c515965e3
   > Blocks: 0            Seconds: 0
   > contract address:    0x4862079Ef7B3cA67B14D71390D002584e1cDE223
   > account:             0x939582533400Aa154669041fDB866112d7832400
   > balance:             9999.98437138
   > gas used:            454553
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.00909106 ETH


   Deploying 'gambling0'
   ---------------------
   > transaction hash:    0xa980665b3051ab776d7c6fc7090098d0837489f1228e8a0273acb7a4fddf9125
   > Blocks: 0            Seconds: 0
   > contract address:    0x1fFE65807b401769f8394F4de956BceA73d3681B
   > account:             0x939582533400Aa154669041fDB866112d7832400
   > balance:             9999.97353386
   > gas used:            541876
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.01083752 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:          0.01992858 ETH


Summary
=======
> Total deployments:   3
> Final cost:          0.02562546 ETH
```

最后输入 npm run dev 即可。

```
C:\Users\azu\OneDrive\Course\blockchainprj\dapp>npm run dev

> truffle-init-webpack@0.0.2 dev C:\Users\azu\OneDrive\Course\blockchainprj\dapp
> webpack-dev-server

i ｢wds｣: Project is running at http://localhost:8080/
i ｢wds｣: webpack output is served from /
i ｢wdm｣: Hash: 2243ab33f18c02280169
Version: webpack 4.28.2
Time: 13781ms
Built at: 2018-12-31 00:42:45
     Asset       Size  Chunks                    Chunk Names
    app.js   870 KiB       0  [emitted]  [big]  main
app.js.map  2.77 MiB       0  [emitted]         main
index.html  1.58 KiB          [emitted]
Entrypoint main [big] = app.js app.js.map
 [31] ./node_modules/url/url.js 22.8 KiB {0} [built]
 [95] multi (webpack)-dev-server/client?http://localhost:8080 ./app/scripts/index.js 40 bytes {0} [built]
 [96] (webpack)-dev-server/client?http://localhost:8080 7.78 KiB {0} [built]
[102] ./node_modules/strip-ansi/index.js 161 bytes {0} [built]
[104] ./node_modules/loglevel/lib/loglevel.js 7.68 KiB {0} [built]
[105] (webpack)-dev-server/client/socket.js 1.05 KiB {0} [built]
[107] (webpack)-dev-server/client/overlay.js 3.58 KiB {0} [built]
[112] (webpack)/hot sync nonrecursive ^\.\/log$ 170 bytes {0} [built]
[114] (webpack)/hot/emitter.js 75 bytes {0} [built]
[115] ./app/scripts/index.js 7.42 KiB {0} [built]
[116] ./app/styles/app.css 1.18 KiB {0} [built]
[121] ./node_modules/web3/index.js 193 bytes {0} [built]
[199] ./node_modules/truffle-contract/index.js 437 bytes {0} [built]
[310] ./build/contracts/gambling0.json 214 KiB {0} [built]
[311] ./build/contracts/gambling1.json 191 KiB {0} [built]
    + 297 hidden modules

WARNING in asset size limit: The following asset(s) exceed the recommended size limit (244 KiB).
This can impact web performance.
Assets:
  app.js (870 KiB)

WARNING in entrypoint size limit: The following entrypoint(s) combined asset size exceeds the recommended limit (244 KiB). This can impact web performance.
Entrypoints:
  main (870 KiB)
      app.js


WARNING in webpack performance recommendations:
You can limit the size of your bundles by using import() or require.ensure to lazy load some parts of your application.
For more info visit https://webpack.js.org/guides/code-splitting/
i ｢wdm｣: Compiled with warnings.
```

然后在浏览器输入蓝字部分 http://localhost:8080/访问即可进入 Dapp 界面。

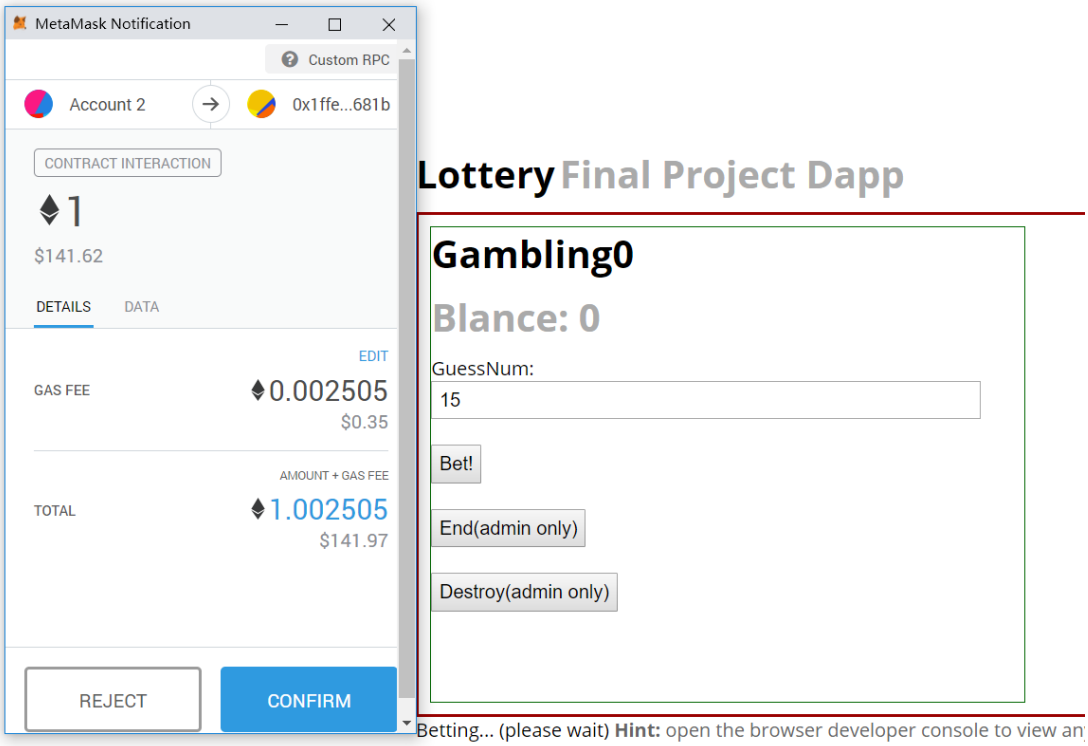
共有两个智能合约。
其中左边是类似彩票形式，输入任意数字，点击 Bet!可参与竞猜（投入 1ether）。
有 1%的几率中奖（会取模）。
End 为开奖（即公布中奖数字）并分发奖励（中奖数字在下方公布）。
Destroy 为摧毁智能合约。摧毁后左半边将消失（即使刷新页面也会消失，除非重新部署智能合约）。
右边类似刮刮乐形式，点击 Bet!即可参与（投入 1ther），即可开奖。
右边需要合约创造者先点击 Initialize 为奖池投入奖金，才可进行竞猜。
Take 将摧毁智能合约，与左边同理。

4. 测试：
在部署项目和运行 demo 中，可能由于各种差异，导致从 unbox 直到 npm run dev 都遇到各种文件确实、依赖确实，与教程中的各种一键部署一键运行的畅顺截然不同。光是配置环境就花了很长时间，因此 UI 十分简陋。

测试链与账户使用 Ganache。

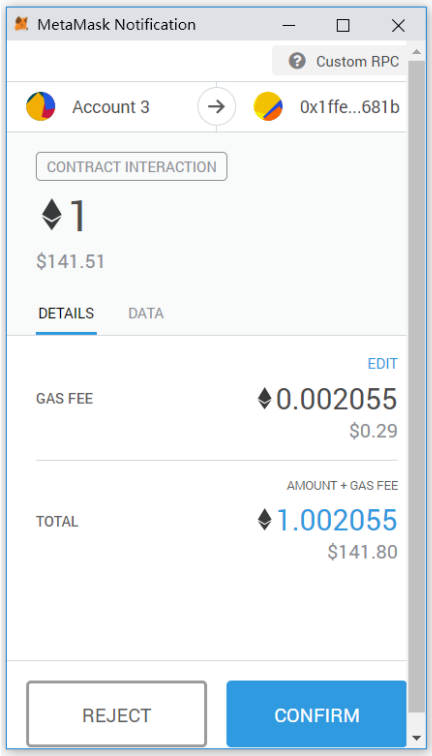
ADDRESS	BALANCE	TX COUNT	INDEX
0x939582533400Aa154669041fDB866112d7832400	9999.97 ETH	5	0
0xbC2D626D5571BFd17f4BDD76C9Bd0056525AB8f1	10000.00 ETH	0	1
0x94E905d62861947427d71B615D44784552d7Bd4D	10000.00 ETH	0	2

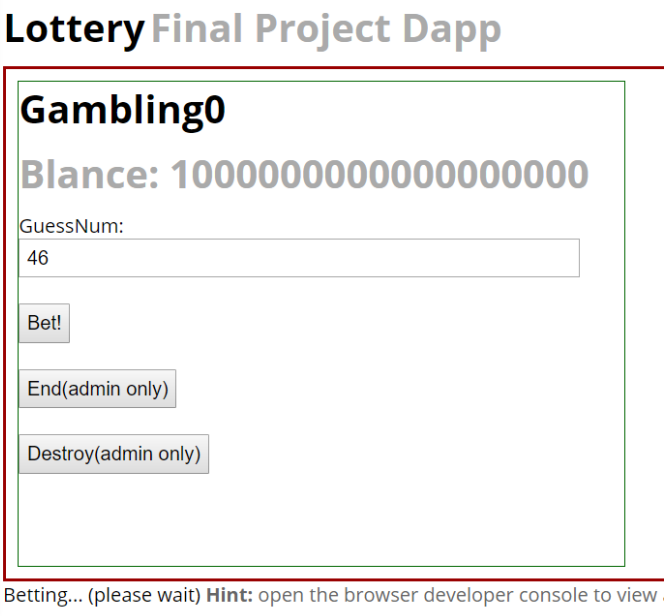
Account1 为合约创造者，Account2 与 Account3 为测试玩家。
先使用账号 2 购买竞猜数字 5（若报错请尝试执行 MetaMask 的 Restart）



Bet 后合约 Blance 将增加。

然后切换到 Account3 再执行类似的操作：





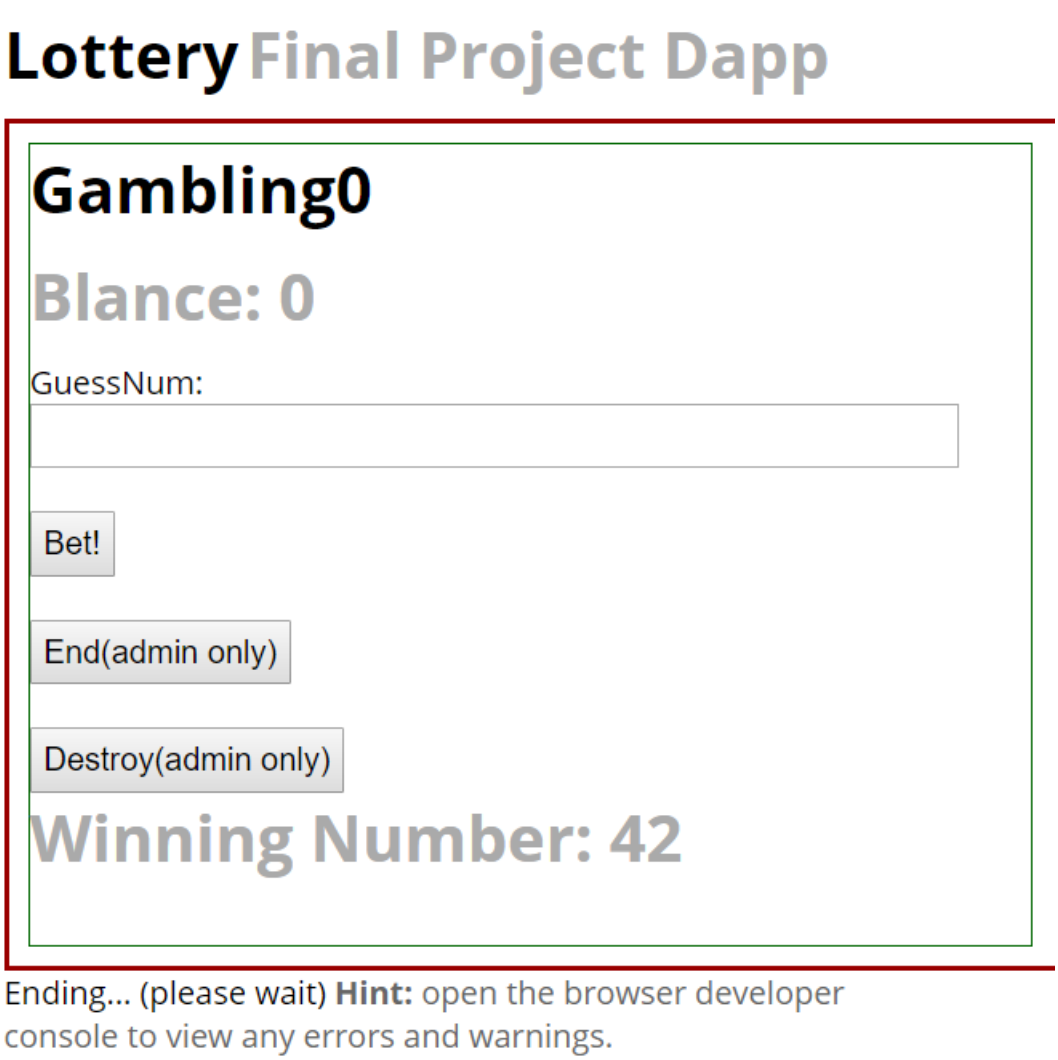
Blance: 20000000000000000000

ADDRESS	BALANCE	TX COUNT	INDEX
0×939582533400Aa154669041fDB866112d7832400	9999.97 ETH	5	0
0×bC2D626D5571BFd17f4BDD76C9Bd0056525AB8f1	9999.00 ETH	1	1
0×94E905d62861947427d71B615D44784552d7Bd4D	9999.00 ETH	1	2

此时切换回 Account1 执行 End。

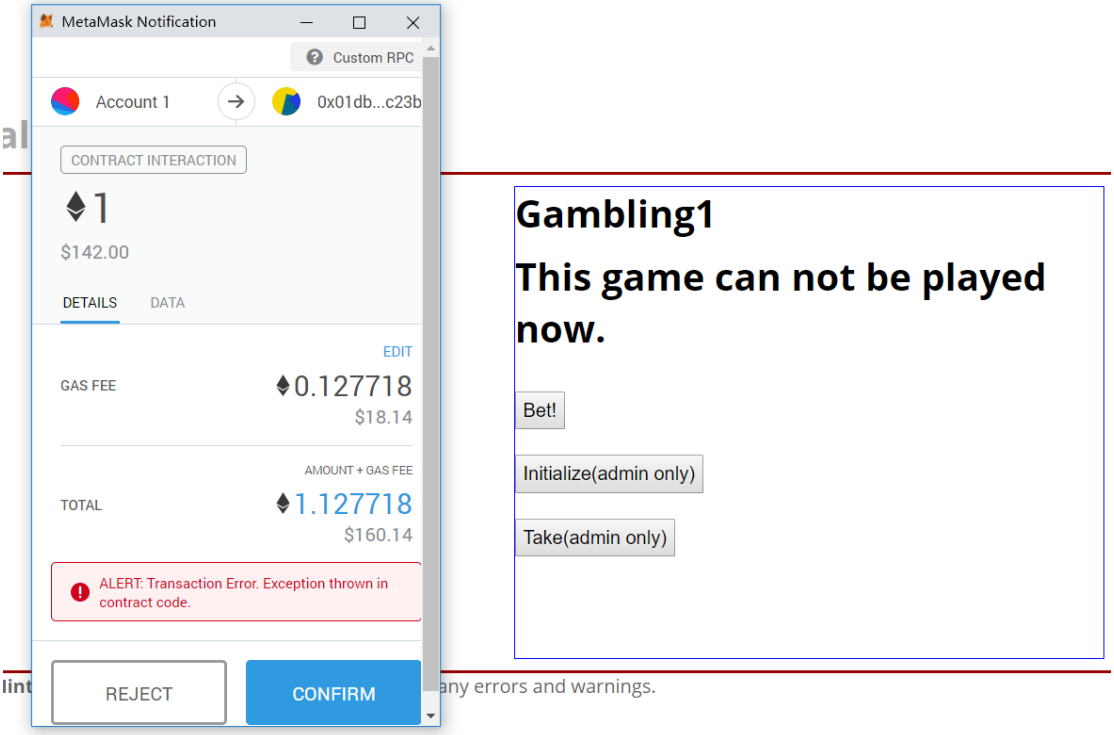
ADDRESS	BALANCE	TX COUNT	INDEX
0×939582533400Aa154669041fDB866112d7832400	10001.95 ETH	11	0
0×bC2D626D5571BFd17f4BDD76C9Bd0056525AB8f1	9999.00 ETH	1	1
0×94E905d62861947427d71B615D44784552d7Bd4D	9999.00 ETH	1	2

很遗憾两位都没中奖，被创建者全拿走了。
Balance 清空，中奖数公布。

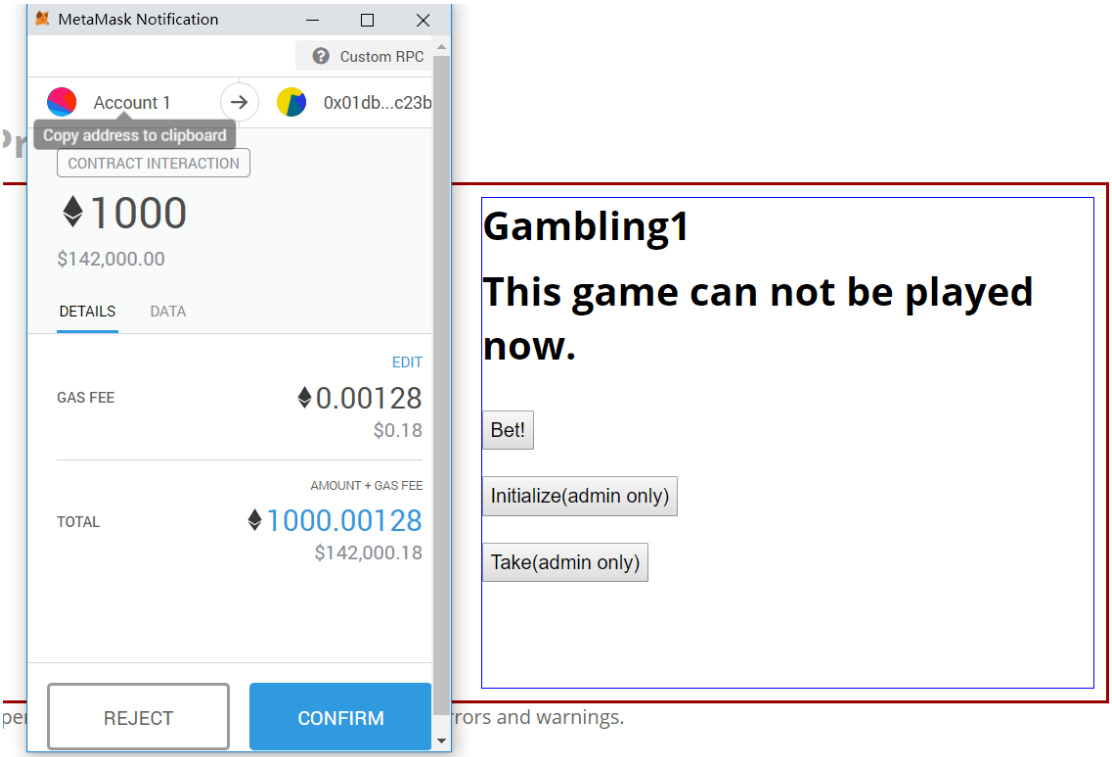


Destroy 后:

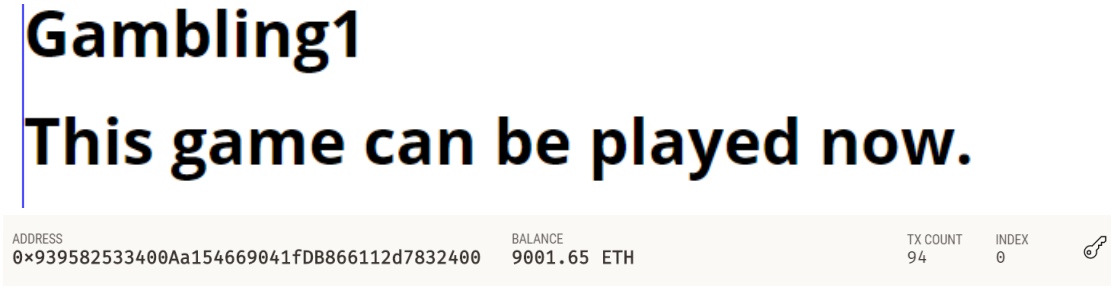
未初始化就 Bet 会抛出异常:


MetaMask Notification
Custom RPC
Account 1
0x01db...c23b
CONTRACT INTERACTION
1
$142.00
DETAILS
DATA
EDIT
GAS FEE
0.127718
$18.14
AMOUNT + GAS FEE
TOTAL
1.127718
$160.14
ALERT: Transaction Error. Exception thrown in contract code.
REJECT
CONFIRM
Gambling1
This game can not be played now.
Bet!
Initialize(admin only)
Take(admin only)
any errors and warnings.

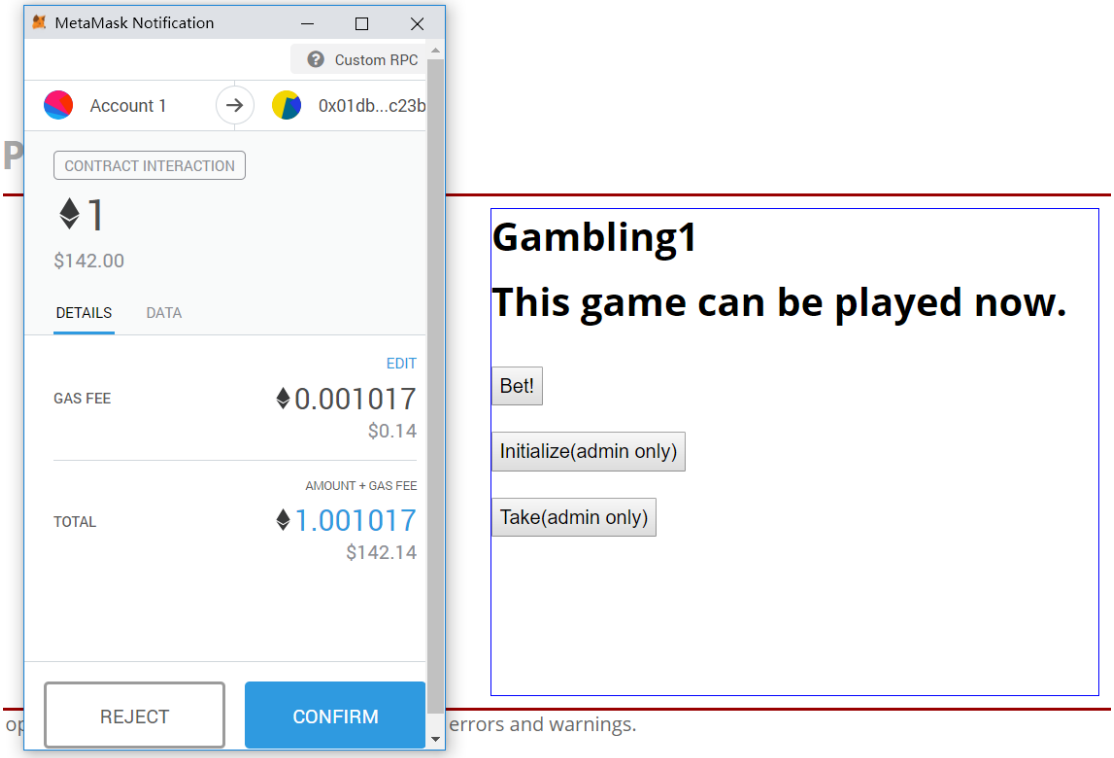
初始化:


MetaMask Notification
Custom RPC
Account 1
0x01db...c23b
Copy address to clipboard
CONTRACT INTERACTION
1000
$142,000.00
DETAILS
DATA
EDIT
GAS FEE
0.00128
$0.18
AMOUNT + GAS FEE
TOTAL
1000.00128
$142,000.18
REJECT
CONFIRM
Gambling1
This game can not be played now.
Bet!
Initialize(admin only)
Take(admin only)
rors and warnings.

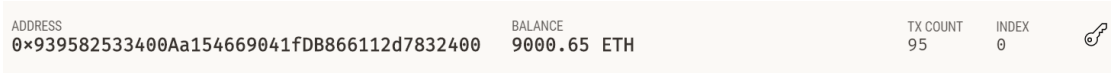
初始化后:



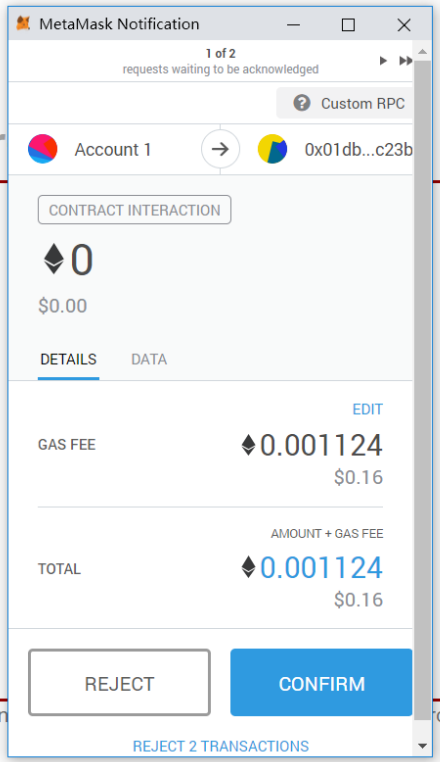
Bet:



中奖率为 1%，奖金为 99ether，一次下注 1ether。



Take 将取走所有钱并销毁合约（同时隐藏）：



Gambling1

This game can be played now.

Bet!

Initialize(admin only)

Take(admin only)

ors and warnings.

Lottery Final Project Dapp

Contract has been destroyed; see log. **Hint:** open the browser developer console to view any errors and warnings.

ADDRESS	BALANCE	TX COUNT	INDEX
0×939582533400Aa154669041fDB866112d7832400	10001.65 ETH	96	0