以太坊智能合约 Hello World 示例程序

欢迎加入区块链技术分享 QQ 群：群名高级乌托邦 群号 562701495

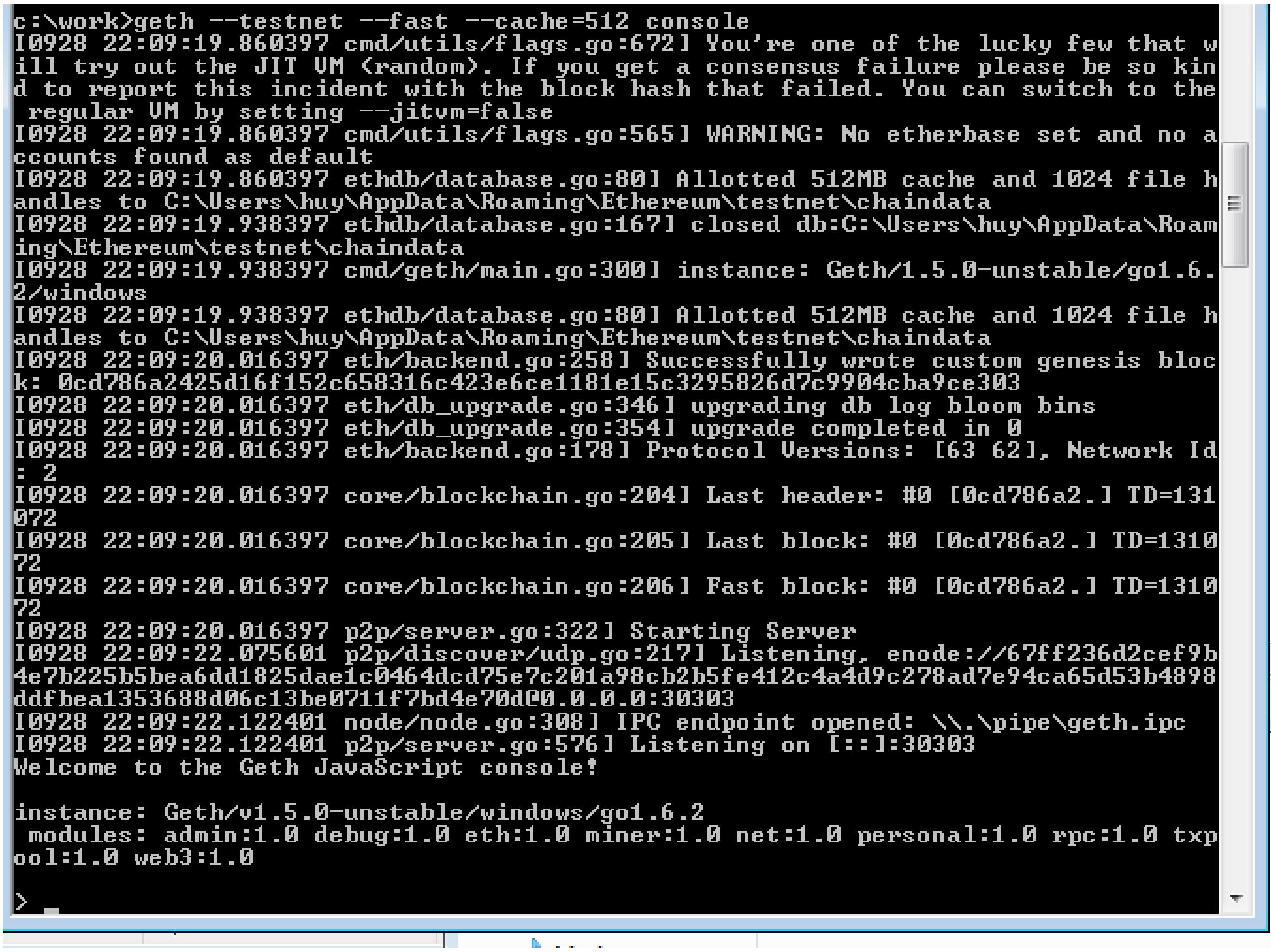
准备工作：创建开发环境

首先需要安装客户端，本文使用基于 Go 语言的 Geth，其官网为 https://github.com/ethereum/go-ethereum.

第一步

在命令行环境中输入以下命令，连接到以太坊测试网络

```
geth --testnet --fast --cache=512 console
```

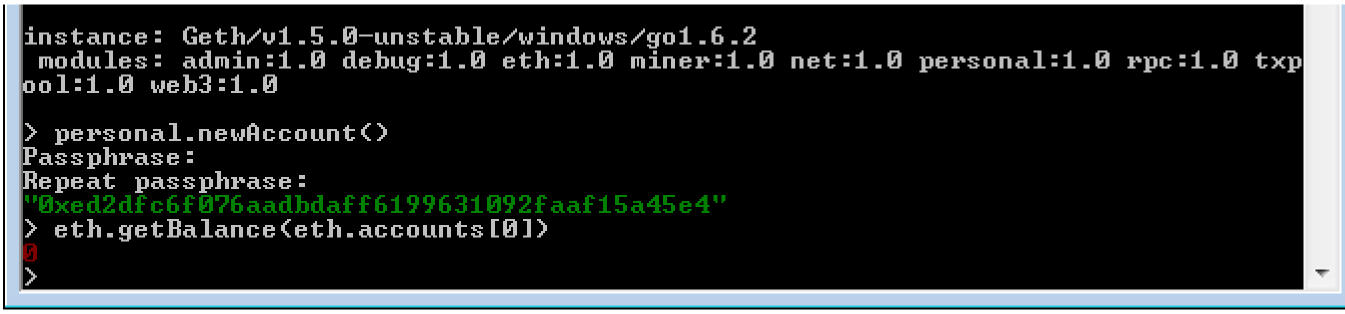


```
c:\work>geth --testnet --fast --cache=512 console
I0928 22:09:19.860397 cmd/utils/flags.go:672] You're one of the lucky few that w
ill try out the JIT VM (random). If you get a consensus failure please be so kin
d to report this incident with the block hash that failed. You can switch to the
 regular VM by setting --jitvm=false
I0928 22:09:19.860397 cmd/utils/flags.go:565] WARNING: No etherbase set and no a
ccounts found as default
I0928 22:09:19.860397 ethdb/database.go:80] Allotted 512MB cache and 1024 file h
andles to C:\Users\huy\AppData\Roaming\Ethereum\testnet\chaindata
I0928 22:09:19.938397 ethdb/database.go:167] closed db:C:\Users\huy\AppData\Roam
ing\Ethereum\testnet\chaindata
I0928 22:09:19.938397 cmd/geth/main.go:300] instance: Geth/1.5.0-unstable/go1.6.
2/windows
I0928 22:09:19.938397 ethdb/database.go:80] Allotted 512MB cache and 1024 file h
andles to C:\Users\huy\AppData\Roaming\Ethereum\testnet\chaindata
I0928 22:09:20.016397 eth/backend.go:258] Successfully wrote custom genesis bloc
k: 0cd786a2425d16f152c658316c423e6ce1181e15c3295826d7c9904cba9ce303
I0928 22:09:20.016397 eth/db_upgrade.go:346] upgrading db log bloom bins
I0928 22:09:20.016397 eth/db_upgrade.go:354] upgrade completed in 0
I0928 22:09:20.016397 eth/backend.go:178] Protocol Versions: [63 62], Network Id
: 2
I0928 22:09:20.016397 core/blockchain.go:204] Last header: #0 [0cd786a2.] TD=131
072
I0928 22:09:20.016397 core/blockchain.go:205] Last block: #0 [0cd786a2.] TD=1310
72
I0928 22:09:20.016397 core/blockchain.go:206] Fast block: #0 [0cd786a2.] TD=1310
72
I0928 22:09:20.016397 p2p/server.go:322] Starting Server
I0928 22:09:22.075601 p2p/discover/udp.go:217] Listening, enode://67ff236d2cef9b
4e7b225b5bea6dd1825dae1c0464dcd75e7c201a98cb2b5fe412c4a4d9c278ad7e94ca65d53b4898
ddfbea1353688d06c13be0711f7bd4e70d@0.0.0.0:30303
I0928 22:09:22.122401 node/node.go:308] IPC endpoint opened: \\.\pipe\geth.ipc
I0928 22:09:22.122401 p2p/server.go:576] Listening on [::]:30303
Welcome to the Geth JavaScript console!

instance: Geth/v1.5.0-unstable/windows/go1.6.2
 modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txp
ool:1.0 web3:1.0

> _
```

第二步

在 Geth 提示符下输入以下代码，创建一个用户并设置密码

```
personal.newAccount()
```

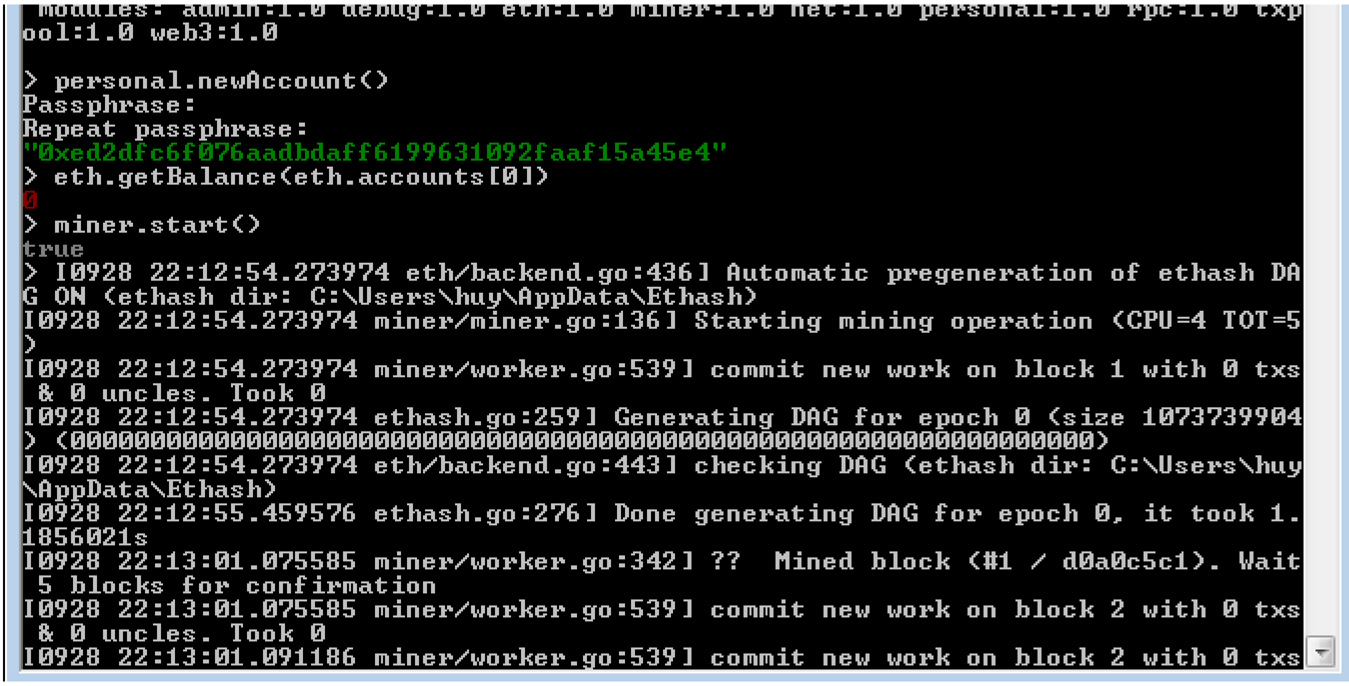


```
instance: Geth/v1.5.0-unstable/windows/go1.6.2
 modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txp
ool:1.0 web3:1.0

> personal.newAccount()
Passphrase:
Repeat passphrase:
"0xed2dfc6f076aadbdaff6199631092faaf15a45e4"
> eth.getBalance(eth.accounts[0])
0
>
```

第三步

在 Geth 提示符下输入以下代码，确认新用户的账户余额为 0，并开始”挖矿”(mine)

```
eth.getBalance(eth.accounts[0])
miner.start()
```

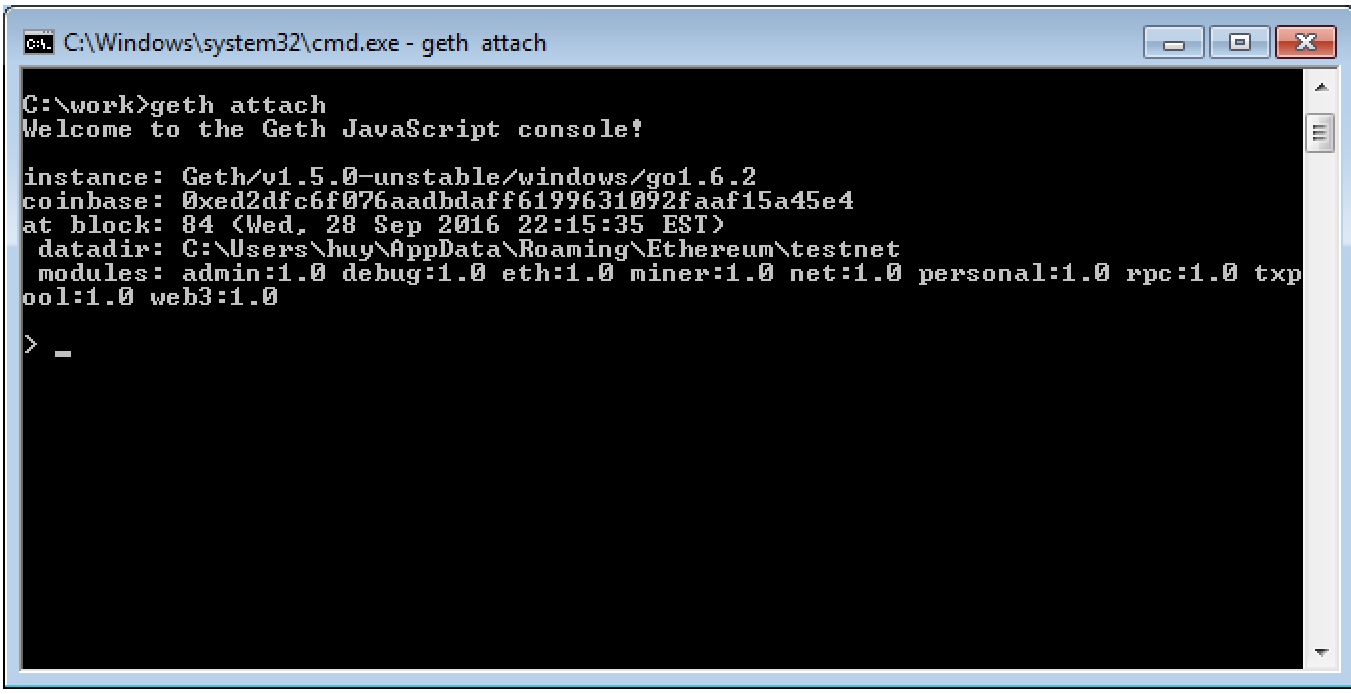


```
 modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txp
ool:1.0 web3:1.0

> personal.newAccount()
Passphrase:
Repeat passphrase:
"0xed2dfc6f076aadbdaff6199631092faaf15a45e4"
> eth.getBalance(eth.accounts[0])
0
> miner.start()
true
> I0928 22:12:54.273974 eth/backend.go:436] Automatic pregeneration of ethash DA
G ON (ethash dir: C:\Users\huy\AppData\Ethash)
I0928 22:12:54.273974 miner/miner.go:136] Starting mining operation (CPU=4 TOT=5
)
I0928 22:12:54.273974 miner/worker.go:539] commit new work on block 1 with 0 txs
 & 0 uncles. Took 0
I0928 22:12:54.273974 ethash.go:259] Generating DAG for epoch 0 (size 1073739904
) (0000000000000000000000000000000000000000000000000000000000000000)
I0928 22:12:54.273974 eth/backend.go:443] checking DAG (ethash dir: C:\Users\huy
\AppData\Ethash)
I0928 22:12:55.459576 ethash.go:276] Done generating DAG for epoch 0, it took 1.
1856021s
I0928 22:13:01.075585 miner/worker.go:342] ??  Mined block (#1 / d0a0c5c1). Wait
 5 blocks for confirmation
I0928 22:13:01.075585 miner/worker.go:539] commit new work on block 2 with 0 txs
 & 0 uncles. Took 0
I0928 22:13:01.091186 miner/worker.go:539] commit new work on block 2 with 0 txs
```

第四步

新开一个命令行窗口并输入以下命令，将这个窗口连接到正在挖矿的窗口

```
geth attach
```

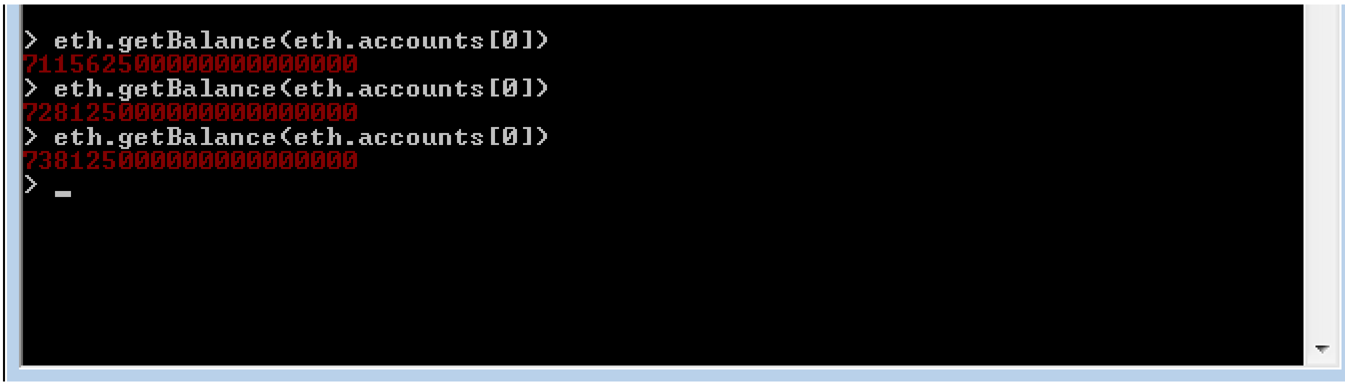


```
C:\work>geth attach
Welcome to the Geth JavaScript console!

instance: Geth/v1.5.0-unstable/windows/go1.6.2
coinbase: 0xed2dfc6f076aadbdaff6199631092faaf15a45e4
at block: 84 (Wed, 28 Sep 2016 22:15:35 EST)
 datadir: C:\Users\huy\AppData\Roaming\Ethereum\testnet
 modules: admin:1.0 debug:1.0 eth:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txp
ool:1.0 web3:1.0

> _
```

第五步

在 Geth 提示符下输入以下代码，确认新用户的账户余额有所增长

```
eth.getBalance(eth.accounts[0])
```

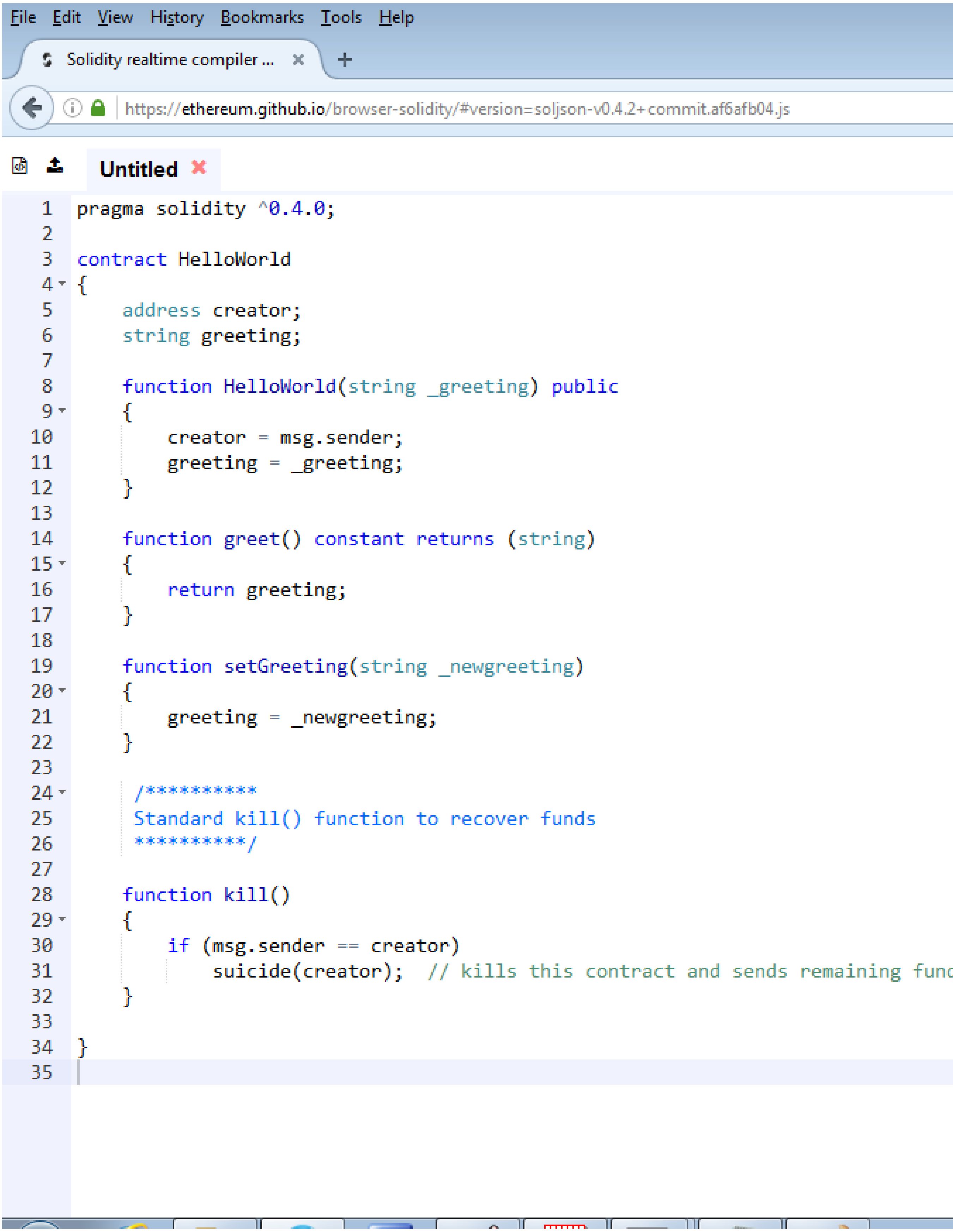


```
> eth.getBalance(eth.accounts[0])
711562500000000000000
> eth.getBalance(eth.accounts[0])
728125000000000000000
> eth.getBalance(eth.accounts[0])
738125000000000000000
> _
```

第六步

使用智能合约的在线编译器 https://ethereum.github.io/browser-solidity/编译以下代码

```
contract HelloWorld

{

    address creator;

    string greeting;



    function HelloWorld(string _greeting) public
    {
        creator = msg.sender;
        greeting = _greeting;
    }

    function greet() constant returns (string)
    {
        return greeting;
    }

    function setGreeting(string _newgreeting)
    {
        greeting = _newgreeting;
    }

     /**********
     Standard kill() function to recover funds
     **********/

    function kill()
    {
        if (msg.sender == creator)
            suicide(creator);  // kills this contract and sends remaining funds back to creator
    }
}
```


File Edit View History Bookmarks Tools Help
Solidity realtime compiler ...
https://ethereum.github.io/browser-solidity/#version=soljson-v0.4.2+commit.af6afb04.js
Untitled

```
pragma solidity ^0.4.0;

contract HelloWorld
{
    address creator;
    string greeting;

    function HelloWorld(string _greeting) public
    {
        creator = msg.sender;
        greeting = _greeting;
    }

    function greet() constant returns (string)
    {
        return greeting;
    }

    function setGreeting(string _newgreeting)
    {
        greeting = _newgreeting;
    }

     /**********
     Standard kill() function to recover funds
     **********/

    function kill()
    {
        if (msg.sender == creator)
            suicide(creator);  // kills this contract and sends remaining func
    }

}
```

第七步

编译器生成的代码如下

```
var _greeting = /* var of type string here */ ;
var helloworldContract =
web3.eth.contract([{"constant":false,"inputs":[],"name":"kill","outputs
":[],"payable":false,"type":"function"},{"constant":false,"inputs":[{"n
ame":"_newgreeting","type":"string"}],"name":"setGreeting","outputs":[]
,"payable":false,"type":"function"},{"constant":true,"inputs":[],"name"
:"greet","outputs":[{"name":"","type":"string"}],"payable":false,"type"
:"function"},{"inputs":[{"name":"_greeting","type":"string"}],"type":"c
onstructor"}]);
var helloworld = helloworldContract.new(
   _greeting,
   {
     from: web3.eth.accounts[0],
     data:
'6060604052604051610 44e38038061044e833981016040528080518201919060200150
505b33600060006101000a81548173ffffffffffffffffffffffffffffffffffffffff0
2191690830217905550806001600050908051906020019082805460018160011615610 1
00020316600290049060005260206000209060 1f016020900481019282601f1061009e5
7805160ff1916838001178555 56100cf565b82800160010185558215 6100cf579182015b
828111156100ce578251826000505591602001919060010190 6100b0565b5b509050610
0fa91906100dc565b808211156100f65760008181506000905550600101 6100dc565b50
90565b50505b50610342806101 0c6000396000f3606060405260003 57c0100000000000
0000000000000000000000000000000000000000009004806341c0e1b51461005257
8063a413686214610066578063cfae3217146100c15761004d565b610002565b3461000
257610064600480505061014 1565b005b34610002576100bf600480803590602001908 2
01803590602001919190808060 1f0160208091040260200160405190810160405280939
29190818152602001838380828437820191505050505050909091905050610 1d5565b00
5b34610002576100d36004805050610286565b604051808060200182810382528381815
18152602001915080519060200190808383829060006004602084601f0104600302600f
01f150905090810190601f16801561013357808203805160018360200361 01000a03191
68152602001915 05b509250505060405180910390f35b600060009054906101000a9004
73ffffffffffffffffffffffffffffffffffffffff1673fffffffffffffffffffffffff
fffffffffffffff163373ffffffffffffffffffffffffffffffffffffffff161415610 1
d257600060009054906101000a900473fffffffffffffffffffffffffffffffffffffff
f1673ffffffffffffffffffffffffffffffffffffffff16ff5b5b565b80600160005090
80519060200190828054600181600116156101000203166002900490600052602060002
090601f016020900481019282601f106102245780516 0ff191683800117855561025556
5b82800160010185558215610255579182015b828111156102545782518260005055916
02001919060010190610236565b5b50905061028091906102625 65b8082111561027c57
6000818150600090555060010161026256 5b5090565b50505b50565b602060405190810
16040528060008152602001506001600050805460018160011615610100020316600290
0480601f016020809104026020016040519081016040528092919081815260200182805
46001816001161561010002031660029004801561033357806 01f1061030857610100 80
83540402835291602001916103335 65b82019190600052602060002090 5b81548152906
00101906020018083116103165782900 3601f168201915b5050505050905061033f565b
9056',
     gas: 4700000
   }, function (e, contract){
    console.log(e, contract);
    if (typeof contract.address !== 'undefined') {
         console.log('Contract mined! address: ' + contract.address + '
transactionHash: ' + contract.transactionHash);
    }
 })
```

设置显示的字符串以及减少费用(gas)

```
var _greeting = "Hello World" ;
gas: 300000
```

第九步

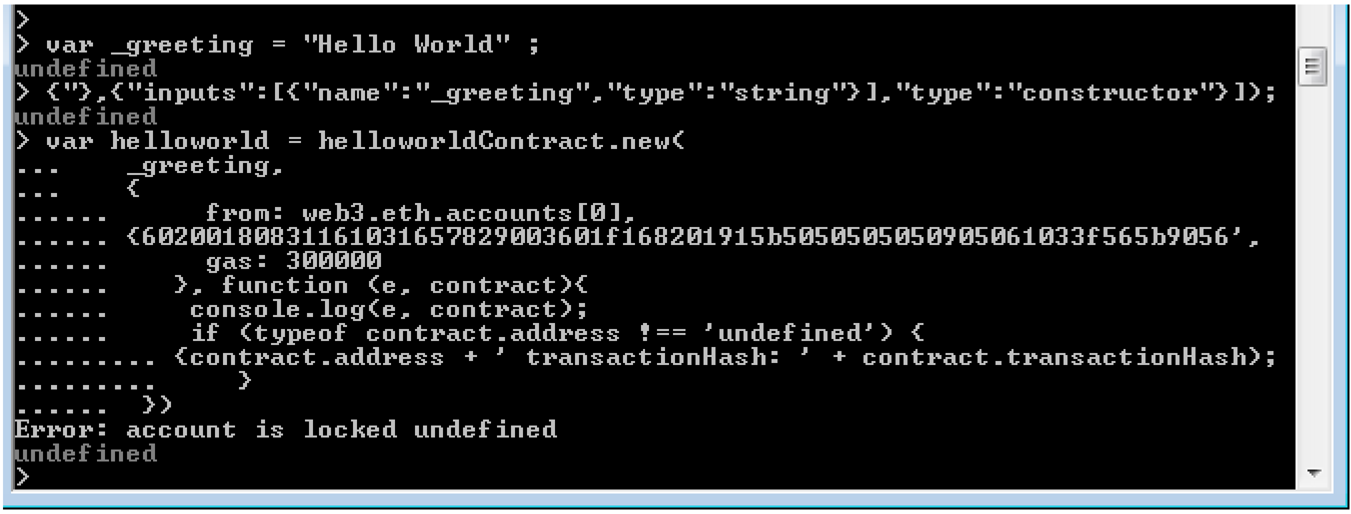
将修改完的代码复制到第四步的窗口中，如果出现

`Error: account is locked undefined`

错误的话，则使用

`personal.unlockAccount(eth.accounts[0], 'password')`

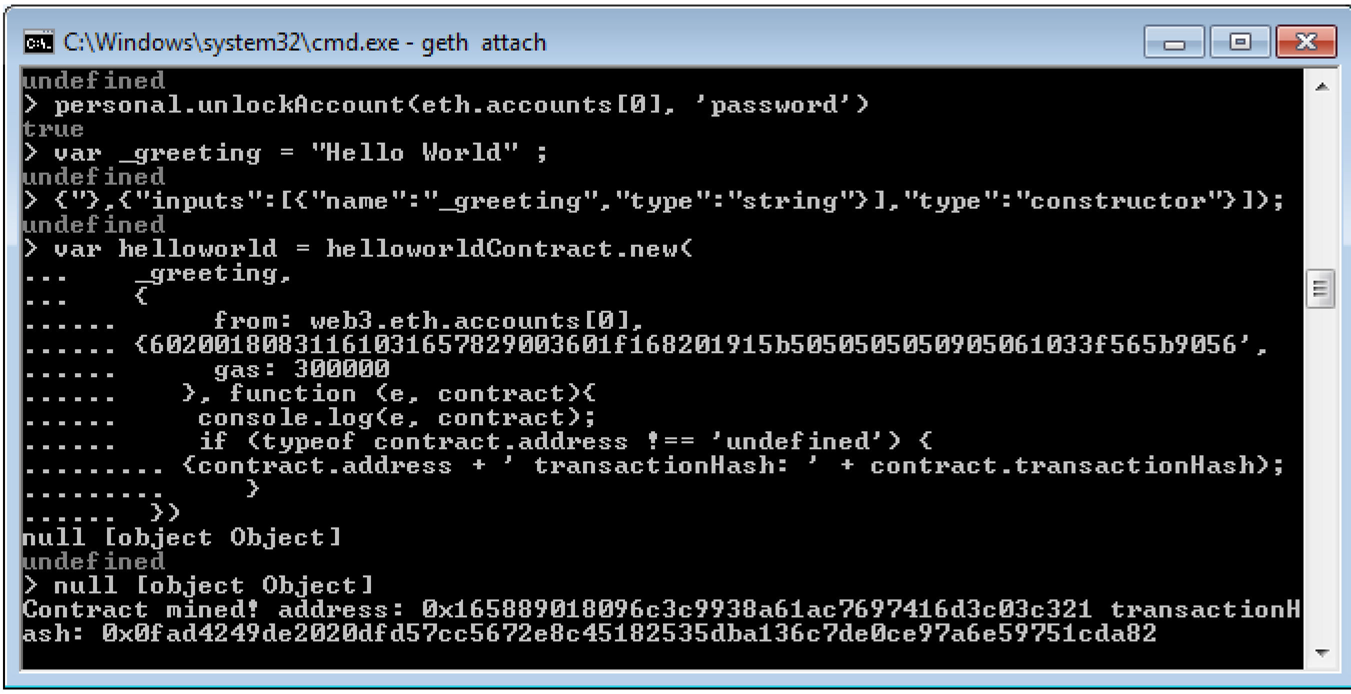
命令将用户解锁.



```
>
> var _greeting = "Hello World" ;
undefined
> {"},{"inputs":[{"name":"_greeting","type":"string"}],"type":"constructor"}]);
undefined
> var helloworld = helloworldContract.new(
...     _greeting,
...     {
......       from: web3.eth.accounts[0],
...... {6020018083116103165782900360 1f168201915b5050505050905061033f565b9056',
......       gas: 300000
......     }, function (e, contract){
......      console.log(e, contract);
......      if (typeof contract.address !== 'undefined') {
......... {contract.address + ' transactionHash: ' + contract.transactionHash);
.........      }
......  })
Error: account is locked undefined
undefined
>
```

第十步

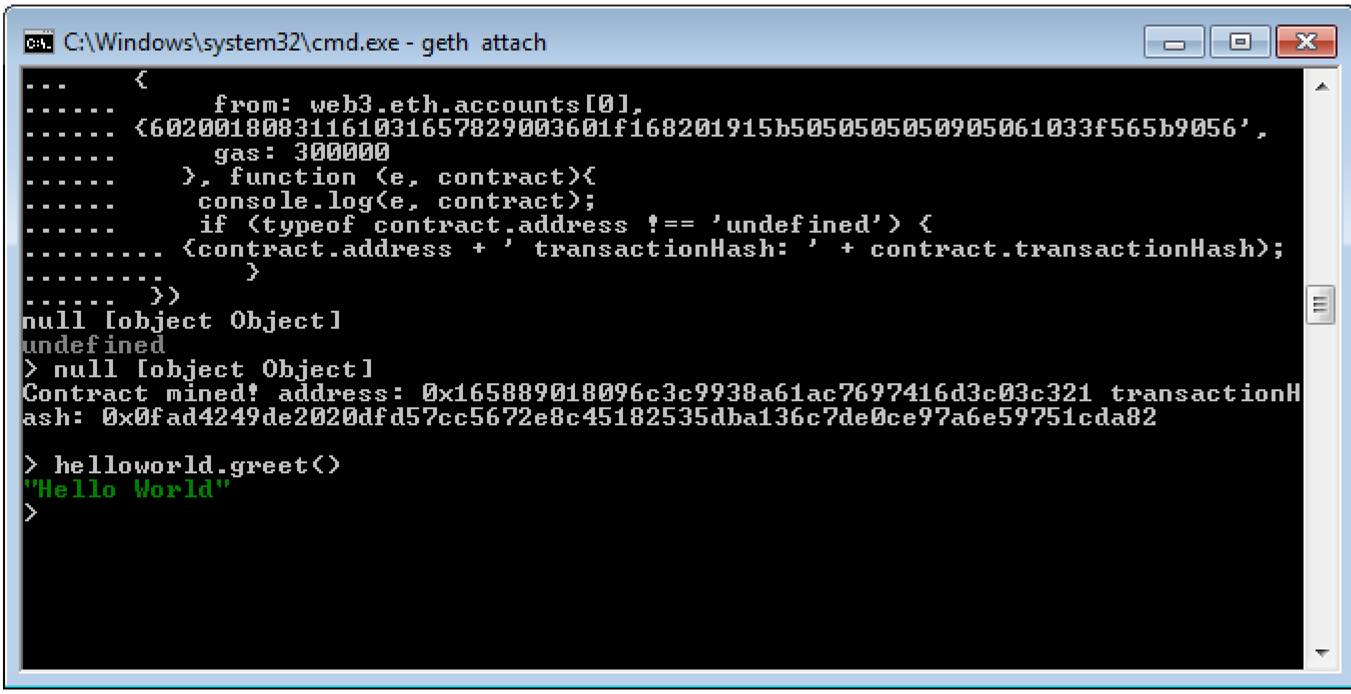
等候一段时间之后, geth 窗口就会出现`Contract mined! address...`, 表明合约代码发布成功



```
undefined
> personal.unlockAccount(eth.accounts[0], 'password')
true
> var _greeting = "Hello World" ;
undefined
> {"},{"inputs":[{"name":"_greeting","type":"string"}],"type":"constructor"}]);
undefined
> var helloworld = helloworldContract.new(
...     _greeting,
...     {
......       from: web3.eth.accounts[0],
...... {6020018083116103165782900360 1f168201915b5050505050905061033f565b9056',
......       gas: 300000
......     }, function (e, contract){
......      console.log(e, contract);
......      if (typeof contract.address !== 'undefined') {
......... {contract.address + ' transactionHash: ' + contract.transactionHash);
.........      }
......  })
null [object Object]
undefined
> null [object Object]
Contract mined! address: 0x165889018096c3c9938a61ac7697416d3c03c321 transactionH
ash: 0x0fad4249de2020dfd57cc5672e8c451825 35dba136c7de0ce97a6e59751cda82
```

第十一步

使用 `helloworld.greet()`命令来运行该合约



```
...    {
......      from: web3.eth.accounts[0],
...... (6020018083116103165782900360 1f168201915b50505050509050610 33f565b9056',
......      gas: 300000
......    }, function (e, contract){
......     console.log(e, contract);
......     if (typeof contract.address !== 'undefined') {
......... (contract.address + ' transactionHash: ' + contract.transactionHash);
.........       }
......  })
null [object Object]
undefined
> null [object Object]
Contract mined! address: 0x165889018096c3c9938a61ac7697416d3c03c321 transactionH
ash: 0x0fad4249de2020dfd57cc5672e8c45182535dba136c7de0ce97a6e59751cda82

> helloworld.greet()
"Hello World"
>
```