蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN

Solidity 函数-下

- 蚂蚁链《区块链系统开发与应用》A认证系列课程

课程目标

- 了解函数返回值与命名参数
- 了解函数可见性
- 了解View 函数

01 函数返回值与命名参数

函数参数

函数返回值

- 返回值的定义与参数类似，使用 returns 关键字来标识要返回值的类型；
- 返回值类型可以省略变量名称；
- 在函数体中，使用 return 关键字来返回值；
- 返回值的类型必须和函数定义中的返回值类型一致；
- Solidity 中可以返回任意数量的参数作为输出；

```
pragma solidity ^0.4.0;

contract Simple {
   // 函数入参的定义与变量定义类似
   function InputPara(uint a, uint) {
     // 省略未使用的参数
     a = a + 1;
   }
}
```

BaaS 平台

BaaS 平台

openchain.cloud.alipay.com/contract-edit/template/create-contract?projectId=101040&unionId=2647&bizid=a00e36c5&openchain=1

蚂蚁集团 ANT GROUP | 金融科技

管理控制台 产品与服务

a00e36c5 - 开放联盟链...

编译

Solidity

0.4.23

SolidityBasicCourse002

TimeUnitDemo15.sol

FunctionDemo16.sol

FunctionDemo17.sol

FunctionDemo17.sol

```
1  pragma solidity ^0.4.20;
2
3  contract FunctionDemo17 {
4      // 定义一个有返回变量的函数
5
6  }
```

1 发 2 分 3 放 4 法 5 非 6 方 7 风

保存

在这里输入你要搜索的内容

英 17:42 2020/12/20

BaaS 平台

BaaS 平台

openchain.cloud.alipay.com/contract-edit/template/create-contract?projectId=101040&unionId=2647&bizid=a00e36c5&openchain=1

蚂蚁集团 ANT GROUP | 金融科技 | 管理控制台 | 产品与服务

a00e36c5 - 开放联盟链...

编译

Solidity

0.4.23

SolidityBasicCourse002

TimeUnitDemo15.sol

FunctionDemo16.sol

FunctionDemo17.sol

FunctionDemo17.sol

```
1  pragma solidity ^0.4.20;
2
3  contract FunctionDemo17 {
4      uint public testA = 1;
5      // 定义一个有返回变量的函数
6      function functionTest001() public returns(uint) {
7          return testA;
8      }
9  }
```

编译

编译详情 | 合约分析 | 调试详情 | 交易详情

Warning 7

Warning: This is a pre-release compiler version, please do not use it in production.

TimeUnitDemo15.sol:13:28: Warning: Using "years" as a unit denomination is deprecated.
uint public yearUint = 1 years;
^-----^

FunctionDemo16.sol:5:5: Warning: Function state mutability can be restricted to pure
function functionTest001() public {
^ (Relevant source part starts here and spans across multiple lines).

FunctionDemo16.sol:10:5: Warning: Function state mutability can be restricted to pure

保存

08:16

在这里输入你要搜索的内容

英 17:42 2020/12/20

函数参数

函数返回值

- 与其他高级语言不同，Solidity 语言可以返回任意数量的参数作为输出，有两种返回方式：
  - 方式一：使用返回参数名来返回参数；
  - 方式二：使用 return 关键字来返回多个值，这种情况下，函数参数变量名可以省略；

```
pragma solidity ^0.4.20;

contract Simple {
   function arithmetics(uint _a, uint _b) public returns (uint o_sum, uint o_product) {
      o_sum = _a + _b;
      o_product = _a * _b;
   }
}
```

BaaS 平台

BaaS 平台

openchain.cloud.alipay.com/contract-edit/template/create-contract?projectId=101040&unionId=2647&bizid=a00e36c5&openchain=1

蚂蚁集团 ANT GROUP | 金融科技 | 管理控制台 | 产品与服务

a00e36c5 - 开放联盟链...

编译

Solidity

0.4.23

SolidityBasicCourse002

TimeUnitDemo15.sol

FunctionDemo16.sol

FunctionDemo17.sol

FunctionDemo17.sol

```
1  pragma solidity ^0.4.20;
2
3  contract FunctionDemo17 {
4      uint public testA = 1;
5      // 定义一个有返回变量的函数
6      function functionTest001() public returns(uint) {
7          return testA;
8      }
9  }
```

编译

编译详情 | 合约分析 | 调试详情 | 交易详情

Warning 7

Warning: This is a pre-release compiler version, please do not use it in production.

TimeUnitDemo15.sol:13:28: Warning: Using "years" as a unit denomination is deprecated.
uint public yearUint = 1 years;
^-----^

FunctionDemo16.sol:5:5: Warning: Function state mutability can be restricted to pure
function functionTest001() public {
^ (Relevant source part starts here and spans across multiple lines).

FunctionDemo16.sol:10:5: Warning: Function state mutability can be restricted to pure

保存

08:16

在这里输入你要搜索的内容

英 17:42 2020/12/20

BaaS 平台

BaaS 平台

openchain.cloud.alipay.com/contract-edit/template/create-contract?projectId=101040&unionId=2647&bizid=a00e36c5&openchain=1

蚂蚁集团 ANT GROUP | 金融科技 | 管理控制台 | 产品与服务

a00e36c5 - 开放联盟链...

编译

FunctionDemo17.sol

字节码

部署合约

0x6080604052600160005534801561001557600080fd5b506103dd806100256000396000f3006080604052600436106100835760003560

合约接口说明（ABI）

已部署合约

[{ "constant": false, "inputs": [], "name": "functionTest003", "outputs": [{ "name": "", "type": "uint256" }, { "name": "", "type":

functiondemo106

合约ID:0xec8cec224d6ebfc0a6b6f24fde4e...

TX Hash:0x400dff362e623f309a6ea61c01...

function functionTest003

调用合约

function functionTest006

调用合约

function functionTest001

调用合约

function functionTest004

调用合约

保存

合约接口说明（ABI）

```
[
  {
    "constant": false,
    "inputs": [],
    "name": "functionTest003",
    "outputs": [
      {
        "name": "",
        "type": "uint256"
      },
      {
        "name": "",
        "type": "uint256"
      },
      {
        "name": "",
        "type": "string"
      }
    ],
    "payable": false,
    "stateMutability": "nonpayable",
    "type": "function"
  },
  {
    "constant": false,
    "inputs": [],
    "name": "functionTest006",
    "outputs": [
      {
        "name": "",
        "type": "uint256"
      }
    ],
```

uint, string) {

returns(uint) {

) {

4a4c81d23698b49da

5b83f38c7ca0c477a9

8462696c0ef884f6af

906da449cbd6ab2818

08:16

在这里输入你要搜索的内容

英 17:42 2020/12/20

02 函数可见性

函数可见性

简单回顾一下

- Solidity 有两种函数调用方式
  - 内部函数调用：这种调用方式使用的是 EVM 虚拟机内部的简单跳转，不会产生消息调用；
  - 外部函数调用：与内部函数不同，外部函数调用会产生消息调用；
- 针对以上两种函数调用方式，函数存在四种可见性：
  - Public
  - External
  - Internal
  - Private

函数可见性

函数可见性

- Public
  - public 函数是合约接口的一部分，可以在内部或通过消息调用。
- External
  - 外部函数作为合约接口的一部分，意味着我们可以从其他合约和交易中调用。 一个外部函数 f 不能从内部调用（即 f 不起作用，但 this.f() 可以）。 当收到大量数据的时候，外部函数有时候会更有效率。
- Internal
  - 这些函数和状态变量只能是内部访问（即从当前合约内部或从它派生的合约访问），不使用 this 调用。
- Private
  - private 函数和状态变量仅在当前定义它们的合约中使用，并且不能被派生合约使用。

BaaS 平台

BaaS 平台

openchain.cloud.alipay.com/contract-edit/template/create-contract?projectId=101040&unionId=2647&bizid=a00e36c5&openchain=1

蚂蚁集团 ANT GROUP | 金融科技 | 管理控制台 | 产品与服务

a00e36c5 - 开放联盟链...

编译

合约部署与调用

编译合约之后，可以部署到配置选中的远端环境，也可以链接已部署的合约，部署或链接成功后，可以对合约方法进行调用测试。

部署记录

保存

FunctionDemo17.sol

```
21          string memory z = "abc";
22          return (x, y, z);
23      }
24
25      // 加法
26      function functionTest004(uint x, uint y) public returns(uint) {
27          uint z = x + y;
28          return z;
29      }
30
31      // 使用普通方式来调用函数
32      function functionTest005() public returns(uint) {
33          uint z = functionTest004(1, 2);
34          return z;
35      }
36
37      // 使用命名参数调用函数
38      function functionTest006() public returns(uint) {
39          uint z = functionTest004({y: 3, x: 5});
40          return z;
41      }
42  }
```

08:16

在这里输入你要搜索的内容

英 17:42 2020/12/20

函数可见性

函数可见性

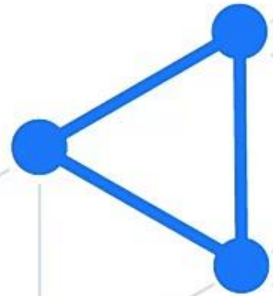
- Public
  - public 函数是合约接口的一部分，可以在内部或通过消息调用。
- External
  - 外部函数作为合约接口的一部分，意味着我们可以从其他合约和交易中调用。 一个外部函数 f 不能从内部调用（即 f 不起作用，但 this.f() 可以）。 当收到大量数据的时候，外部函数有时候会更有效率。
- Internal
  - 这些函数和状态变量只能是内部访问（即从当前合约内部或从它派生的合约访问），不使用 this 调用。
- Private
  - private 函数和状态变量仅在当前定义它们的合约中使用，并且不能被派生合约使用。

函数可见性

注意事项

- 我们知道，智能合约拥有“透明性”特征，也就是说，智能合约一旦部署到区块链上，其源码对所有人可见，所以，我们设置“private”类型只能阻止其他合约访问和修改这些信息，但是对于区块链外的整个世界它仍然是可见的；
- 可见性标识符的定义位置，对于状态变量来说是在类型后面，对于函数是在参数列表和返回关键字中间。

03 View 函数



View 函数

View 函数

- 可以将函数声明为 view 类型，这种情况下要保证不修改状态。
- 下面的语句被认为是修改状态：
  - 修改状态变量；
  - 产生事件；
  - 创建其它合约；
  - 使用 selfdestruct；
  - 调用任何没有标记为 view 的函数；
  - 使用低级调用；
  - 使用包含特定操作码的内联汇编；
- 编译器没有强制 view 方法不能修改状态。

BaaS 平台

BaaS 平台

openchain.cloud.alipay.com/contract-edit/template/create-contract?projectId=101040&unionId=2647&bizid=a00e36c5&openchain=1

蚂蚁集团 ANT GROUP | 金融科技 | 管理控制台 | 产品与服务

a00e36c5 - 开放联盟链...

编译

0130060806040526004361061008357600003

合约接口说明（ABI）

已部署合约

[{ "constant": true, "inputs": [], "name": "functionTest007", "outputs": [{ "name": "", "type": "uint256" }], "payable": false,

functiondemo120

合约ID:0xded0148d0ee18037809cc55d52...

TX Hash:0x935cede96461b8e52d3ac37c9...

function functionTest007

调用合约

function functionTest003

调用合约

function functionTest006

调用合约

function functionTest001

调用合约

function functionTest002

调用合约

保存

FunctionDemo17.sol

```
37      /**
38      1. 使用命名参数调用函数
39      2. public 可见性：外部调用和内部调用均可；
40      3. external 可见性：外部调用可以，但是内部调用不可以；
41      4. internal 可见性：外部调用不可以，但是内部调用可以；
42      5. private 可见性：外部调用不可以，内部调用可以；
43      */
44      function functionTest006() public returns(uint) {
45          uint z = functionTest004({y: 3, x: 5});
46          return z;
47      }
48
49      function functionTest007() public view returns(uint) {
50          // 修改状态变量；
51          testA = 2;
52          // 创建其他合约和使用selfdestruct，这两个目前蚂蚁链不支持；
53          // 调用任何没有标记为 view 的函数；
54
```

编译

编译详情 | 合约分析 | 调试详情 | 交易详情

Filter

txhash: 0x47a6a01e23a2c8ab3c4d984f9c7c27cf9ee1a5e6ddb5f10976eb87ccb19c3b19


```
{
  "msg_type": "63",
  "block_number": 43729506,
  "receipt": {
    "result": 0,
    "output": "0x0000000000000000000000000000000000000000000000000000000000000001",
```


08:16

在这里输入你要搜索的内容

英 17:42 2020/12/20

BaaS 平台

BaaS 平台

openchain.cloud.alipay.com/contract-edit/template/create-contract?projectId=101040&unionId=2647&bizid=a00e36c5&openchain=1

蚂蚁集团 ANT GROUP | 金融科技 | 管理控制台 | 产品与服务

编译成功

自动保存

a00e36c5 - 开放联盟链...

编译

合约部署与调用

编译合约之后，可以部署到配置选中的远端环境，也可以链接已部署的合约，部署或链接成功后，可以对合约方法进行调用测试。

部署记录

> FunctionDemo16.sol

FunctionDemo17.sol

FunctionDemo17

字节码

部署合约

0x6080604052600160005534801561001557600080fd5b506103d7806100256000396000f3006080604052600436106100835760003560e0

合约接口说明（ABI）

已部署合约

[{ "constant": true, "inputs": [], "name": "functionTest007", "outputs": [{ "name": "", "type": "uint256" }], "payable": false,

> TimeUnitDemo15.sol

保存

FunctionDemo17.sol

```
43      */
44      function functionTest006() public returns(uint) {
45          uint z = functionTest004({y: 3, x: 5});
46          return z;
47      }
48
49      function functionTest007() public view returns(uint) {
50          // 修改状态变量：
51          // testA = 2;
52          // 创建其他合约和使用selfdestruct，这两个目前蚂蚁链不支持；
53          // 调用任何没有标记为 view 的函数；
54          uint z = functionTest004(1, 2);
55          return testA;
56      }
57  }
```

编译

编译详情 | 合约分析 | 调试详情 | 交易详情

在这里输入你要搜索的内容

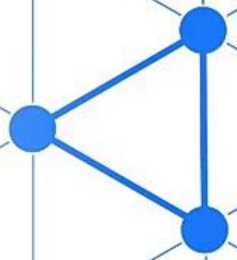
英 17:42 2020/12/20

View 函数

View 函数

- 可以将函数声明为 view 类型，这种情况下要保证不修改状态。
- 下面的语句被认为是修改状态：
  - 修改状态变量；
  - 产生事件；
  - 创建其它合约；
  - 使用 selfdestruct；
  - 调用任何没有标记为 view 的函数；
  - 使用低级调用；
  - 使用包含特定操作码的内联汇编；
- 编译器没有强制 view 方法不能修改状态。

谢 谢



蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN