蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN

初识Solidity编程

- 蚂蚁链《区块链系统开发与应用》A认证系列课程

课程目标

- 了解介绍Solidity语言背景及基本概念
- 初识Solidity编程

01 Solidity简介

Solidity简介

Solidity语言

- Solidity是一门面向合约的、为实现智能合约而创建的高级编程语言。
- Solidity是静态类型语言，支持继承、库和复杂的用户类型定义等。
  - 静态类型语言
  - 动态类型语言
- 受到了C++、Python和Javascript语言的影响
- Solidity语言可以运行在蚂蚁链虚拟机上
  - 蚂蚁链支持EVM虚拟机

Solidity简介

Solidity特性

- ·Solidity是一个面向合约的静态类型语言，受到了C++、Python和Javascript的影响，有着高级语言共有的特性，如继承，接口，事件等。但除此之外，还有着不同于其他高级语言的独特特征：
  - 蚂蚁链等区块链平台是基于账户的，所以Solidity语言有一个特殊的identity类型(蚂蚁链独有)，用手棕识用户、定位合约等，这个类型是其他所有语言所没有的。
  - 存储是使用网络上的区块链，所以需要确定变量是存储在内存 (Memory) 还是存储在区块链 (storage)
  - 一旦出现异常，所有的执行都将会被撤回，这是为了保证合约执行的原子性，以避免中间状态出现数据不一致的情况。这个是Solidity和其他语言的一个明显不同之处。
  - 蚂蚁链支持的Solidity语言和原生Solidity有一些不同，但是绝大部分都是相同的

Solidity例子

```
pragma solidity >=0.4.0 <0.6.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

- pragma
  - 第一行的 pragma 指令，用于指定源代码的 Solidity 版本。
  - 第一行的是告诉大家源代码是为 Solidity 0.4.0以上版本编写的，但是不包括 0.6.0 及以上版本。
  - pragma 指令仅仅该源文件有效，新建另一个文件，需要重新指定。
  - pragma solidity ^0.4.0
    - 上述代码的意思是该源文件为 solidity 0.4.0 及以上版本编写，但是不包括 0.5.0 及以上版本。
    - 也就是说，该源文件是为 solidity 0.4.0 ~ 0.4.9 版本编写的。
    - 约定俗成，小版本的变化不会包含大规模的更改，更多的是 bug 修复等小规模的改动，所以我们可以使用 ^ 符号来定义源文件支持的版本号

Solidity例子

```
pragma solidity >=0.4.0 <0.6.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

- contract
  - contract 关键字用于声明一个合约
  - 例子中我们用 contract 关键字声明了一个名字叫做“SimpleStorage”的合约
- uint
  - uint 是 Solidity 语言支持的基本类型之一，叫做无符号整型（unsigned integer）
  - 例子中用 uint 关键字声明了一个名字叫做“storedData”的无符号整型

Solidity例子

```
pragma solidity >=0.4.0 <0.6.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

- function
  - function 关键字用于声明一个函数
  - 一个函数包含以下几个部分：
    - 函数名
    - 函数参数
    - 函数可见性
    - 函数返回值
    - 函数体
  - 例子中我们用 function 关键字声明了一个叫做 “set” 的函数
  - “set” 后面紧跟了一个小括号，里面的“uint x” 表示调用该函数需要传递一个 uint 类型的参数
  - public 表示该函数的可见性，public 表示该函数是一个公共函数，部署到蚂蚁链后可以被外界所访问

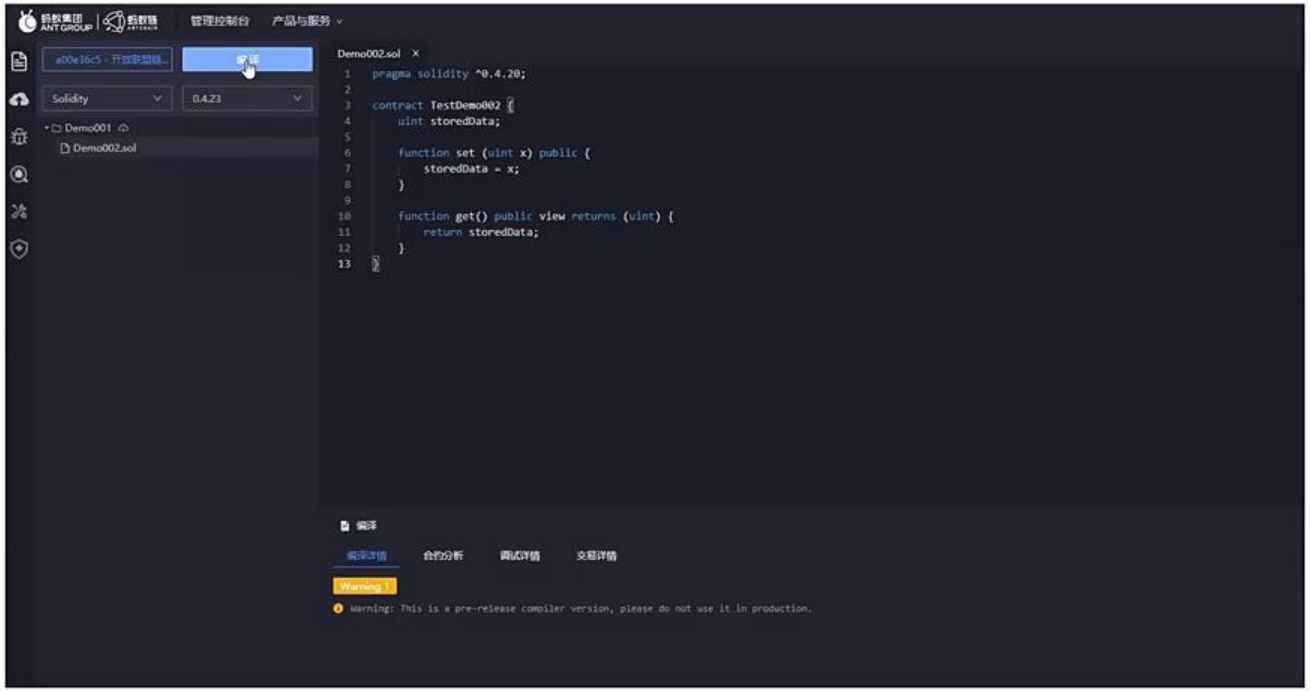
Solidity例子

```
pragma solidity >=0.4.0 <0.6.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

- function
  - 函数体需要用一对大括号括起来
  - storedData = x 语句表示讲 set 函数传递进来的 uint 类型的 x 的值赋给 storedData变量
- 同理
  - 我们用 function 关键字定义了一个叫做 get 的函数。
  - 该函数没有声明任何参数，即调用该函数无需传递任何参数
  - 该函数的可见性为 public
  - view 表示该函数不会修改状态
  - returns 表示该函数有返回值，返回值的类型在后面的小括号中表示，例子中，“get”方法需要返回一个 uint 类型的值
  - return 关键字用于函数体返回值，例子中返回了 storedData 的值
  - 注意：return 后面的变量的类型，必须和函数生命中 returns 后面声明的返回值类型一致

Solidity演示

- 演示：使用 Cloud IDE 进行编译和部署



BaaS 平台

openchain.antchain.antgroup.com/contract-edit/template/create-contract?projectId=100975&unionId=2647&bizid=a00e36c5&openchain=1

蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN | 管理控制台 | 产品与服务

a00e36c5 - 开放联盟链...

编译

Solidity | 0.4.23

Demo001

Demo002.sol

Demo003.sol

Demo003.sol

```
1  pragma solidity ^0.4.20;
2
3  contract TestDemo003 {
4      uint storedData;
5
6      function set (uint x) public {
7          storedData = x;
8      }
9
10     function get () public view returns (uint) {
11         return storedData;
12     }
13 }
```

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

openchain.antchain.antgroup.com/contract-edit/template/create-contract?projectId=100975&unionId=2647&bizid=a00e36c5&openchain=1

蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN | 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

> Demo002.sol

∨ Demo003.sol

TestDemo003

字节码 | 部署合约

0x6080604052348015610010576000080fd5b5060df8061001f6000396000f30060806040526004361060495760003357c0100000000000000

合约接口说明（ABI） | 已部署合约

[{ "constant": false, "inputs": [{ "name": "x", "type": "uint256" }], "name": "set", "outputs": [], "payable": false, "stateMutability":

保存

Demo003.sol

```
1  pragma solidity ^0.4.20;
2
3  contr
4
5
6
7
8
9
10
11
12
13 }
```

部署合约

是否正式发布

合约名称 合约名称

Gas预估 Gas预估

Gas限额 number

确定

编译

编译详情 | 合约分析 | 调试详情 | 交易详情

Warning 2

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

Demo002.sol:7:31: Warning: Decimal literal assigned to bytesXX variable will be left-aligned. Use an explicit conversion to silence this warning.

bytes2 public byteTest3 = 23; // 十进制 23 转换为十六进制为：17

^^

08:16

在这里输入你要搜索的内容

英 17:42 2020/12/20

BaaS 平台

openchain.antchain.antgroup.com/contract-edit/template/create-contract?projectId=100975&unionId=2647&bizid=a00e36c5&openchain=1

蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN | 管理控制台 | 产品与服务

部署成功

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

> Demo002.sol

v Demo003.sol

TestDemo003

字节码 部署合约

0x6080604052348015610010576000080fd5b5060df8061001f6000396000f30060806040526004361060495760003357c01000000000

合约接口说明（ABI） 已部署合约

[{ "constant": false, "inputs": [{ "name": "x", "type": "uint256" }], "name": "set", "outputs": [], "payable": false,

TestDemo015

合约ID:0xae634f851ae4993c96ac28cc5bcc...

TX Hash:0x0f5e3894cc3b1c5a0a6e4b138e...

function set 调用合约

保存

Demo003.sol

```
1  pragma solidity ^0.4.20;
2
3  contract TestDemo003 {
4      uint storedData;
5
6      function set (uint x) public {
7          storedData = x;
8      }
9
10     function get () public view returns (uint) {
11         return storedData;
12     }
13 }
```

编译

编译详情 合约分析 调试详情 交易详情

Filter

txhash: 0x2a19c5f95d95cbbc1728beb93fdc0c7dee228139e3ca9bd13125da43f7c56e08

txhash: 0x0f5e3894cc3b1c5a0a6e4b138e7c854df54d04a487f98522567aefd7340e213d

08:16

在这里输入你要搜索的内容

英 17:42 2020/12/20

BaaS 平台

openchain.antchain.antgroup.com/contract-edit/template/create-contract?projectId=100975&unionId=2647&bizid=a00e36c5&openchain=1

蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN | 管理控制台 | 产品与服务

a00e36c5 开放联盟链... | 编译

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

> Demo002.sol

v Demo003.sol

TestDemo003

字节码 | 部署合约

0x6080604052348015610010576000080fd5b5060df8061001f6000396000f30060806040526004361060495760003357c01000000000

合约接口说明（ABI） | 已部署合约

[{ "constant": false, "inputs": [{ "name": "x", "type": "uint256" }], "name": "set", "outputs": [], "payable": false,

TestDemo015

合约ID:0xae634f851ae4993c96ac28cc5bcc...

TX Hash:0x0f5e3894cc3b1c5a0a6e4b138e...

function set | 调用合约

function get | 调用合约

保存

Demo003.sol

```
1  pragma solidity ^0.4.20;
2
3  contr
4
5
6
7
8
9
10
11
12
13 }
```

调用合约

Gas预估 | Gas预估

Gas限额 | number

确定

编译

编译详情 | 合约分析 | 调试详情 | 交易详情

Filter

txhash: 0x2a19c5f95d95cbbc1728beb93fdc0c7dee228139e3ca9bd13125da43f7c56e08

txhash: 0x0f5e3894cc3b1c5a0a6e4b138e7c854df54d04a487f98522567aefd7340e213d

08:16

在这里输入你要搜索的内容

英 17:42 2020/12/20

BaaS 平台

openchain.antchain.antgroup.com/contract-edit/template/create-contract?projectId=100975&unionId=2647&bizid=a00e36c5&openchain=1

蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN | 管理控制台 | 产品与服务

a00e36c5 - 开放联盟链...

编译

Demo003.sol

TestDemo003

字节码 部署合约

0x6080604052348015610010576000080fd5b5060df8061001f6000396000f30060806040526004361060495760003357c01000000000

合约接口说明（ABI） 已部署合约

[{ "constant": false, "inputs": [{ "name": "x", "type": "uint256" }], "name": "set", "outputs": [], "payable": false,

TestDemo015

合约ID:0xae634f851ae4993c96ac28cc5bcc...

TX Hash:0x0f5e3894cc3b1c5a0a6e4b138e...

0xae634f851ae4993c96ac28cc5bcc355b414f3bb199b15ec358e77c2d79ce8a81

function get 调用合约

tx hash

0x0de338085373852366c2f88c4e4e...

input

output

uint256: 0

保存

Demo003.sol

```
1  pragma solidity ^0.4.20;
2
3  contract TestDemo003 {
4      uint storedData;
5
6      function set (uint x) public {
7          storedData = x;
8      }
9
10     function get () public view returns (uint) {
11         return storedData;
12     }
13 }
```

编译

合约分析 调试详情 交易详情

Filter

txhash: 0x2a19c5f95d95cbbc1728beb93fdc0c7dee228139e3ca9bd13125da43f7c56e08

txhash: 0x0f5e3894cc3b1c5a0a6e4b138e7c854df54d04a487f98522567aefd7340e213d

txhash: 0x0de338085373852366c2f88c4e4e6f751ced877b0536f07769c937fb62e67885

08:16

在这里输入你要搜索的内容

英 17:42 2020/12/20

BaaS 平台

openchain.antchain.antgroup.com/contract-edit/template/create-contract?projectId=100975&unionId=2647&bizid=a00e36c5&openchain=1

蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN | 管理控制台 | 产品与服务

a00e36c5 开放联盟链... | 编译 | 部署合约

字节码

0x6080604052348015610010576000080fd5b5060df8061001f6000396000f30060806040526004361060495760003357c01000000000

合约接口说明（ABI） | 已部署合约

[{ "constant": false, "inputs": [{ "name": "x", "type": "uint256" }], "name": "set", "outputs": [], "payable": false,

TestDemo015

合约ID:0xae634f851ae4993c96ac28cc5bcc...

TX Hash:0x0f5e3894cc3b1c5a0a6e4b138e...

function set | 调用合约

function get | 调用合约

tx hash

0x0de338085373852366c2f88c4e4e...

input

output

uint256: 0

log

Demo003.sol

```
1  pragma solidity ^0.4.20;
2
3  contr
4
5
6
7
8
9
10
11
12
13 }
```

调用合约

Gas预估 | Gas预估

Gas限额 | number

确定

编译

编译详情 | 合约分析 | 调试详情 | 交易详情

Filter

txhash: 0x2a19c5f95d95cbbc1728beb93fdc0c7dee228139e3ca9bd13125da43f7c56e08

txhash: 0x0f5e3894cc3b1c5a0a6e4b138e7c854df54d04a487f98522567aefd7340e213d

txhash: 0x0de338085373852366c2f88c4e4e6f751ced877b0536f07769c937fb62e67885

txhash: 0x8218499826db0704073cfece7ea277b80e19c984d3c459cfd98fa0e4dc28741f

保存

08:15

在这里输入你要搜索的内容

英 17:42 2020/12/20

BaaS 平台

openchain.antchain.antgroup.com/contract-edit/template/create-contract?projectId=100975&unionId=2647&bizid=a00e36c5&openchain=1

蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN | 管理控制台 | 产品与服务

a00e36c5 - 开放联盟链... | 编译

字节码 | 部署合约

0x6080604052348015610010576000080fd5b5060df8061001f6000396000f30060806040526004361060495760003357c01000000000

合约接口说明 (ABI) | 已部署合约

[{ "constant": false, "inputs": [{ "name": "x", "type": "uint256" }], "name": "set", "outputs": [], "payable": false,

TestDemo015

合约ID:0xae634f851ae4993c96ac28cc5bcc...

TX Hash:0x0f5e3894cc3b1c5a0a6e4b138e...

function set | 调用合约

function get | 调用合约

tx hash

0x049f7ccf618e8f7f7da32e2486a5ea...

input

output

uint256: 123

123

log

保存

Demo003.sol

```
1  pragma solidity ^0.4.20;
2
3  contract TestDemo003 {
4      uint storedData;
5
6      function set (uint x) public {
7          storedData = x;
8      }
9
10     function get () public view returns (uint) {
11         return storedData;
12     }
13 }
```

编译

编译详情 | 合约分析 | 调试详情 | 交易详情

Filter

txhash: 0x2a19c5f95d95cbbc1728beb93fdc0c7dee228139e3ca9bd13125da43f7c56e08

txhash: 0x0f5e3894cc3b1c5a0a6e4b138e7c854df54d04a487f98522567aefd7340e213d

txhash: 0x0de338085373852366c2f88c4e4e6f751ced877b0536f07769c937fb62e67885

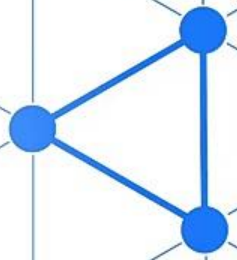
txhash: 0x8218499826db0704073cfece7ea277b80e19c984d3c459cfd98fa0e4dc28741f

08:15

在这里输入你要搜索的内容

英 17:42 2020/12/20

谢 谢



蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN