```
contract Test {
   uint a;
}
```

无函数

```
contract Test {
   uint public a;
}
```

```
[call] from:0xca35b7d915458ef540ade6068dfe2f44e8fa733c, to:Test.a(), data:0dbe6...e671f, return:
{
        "0": "uint256: 0"
}
```

Details Debug

```
contract Test {
   uint public a = 1;
}
```

```
[call] from:0xca35b7d915458ef540ade6068dfe2f44e8fa733c, to:Test.a(), data:0dbe6...e671f, return:
{
        "0": "uint256: 1"
}
```

Details Debug

```
contract Test {
   mapping(uint => uint) public a;

   function test () {
      a[1] = 2;
   }
}
```

```
transact to Test.test pending ...

[vm] from:0xca3...a733c, to:Test.test() 0xbde...4ddc9, value:0 wei, data:0xf8a...8fd6d, 0 logs, hash:0x473...70a55

call to Test.a

[call] from:0xca35b7d915458ef540ade6068dfe2f44e8fa733c, to:Test.a(uint256), data:f0fdf...00001, return:
{
        "0": "uint256: 2"
}
```

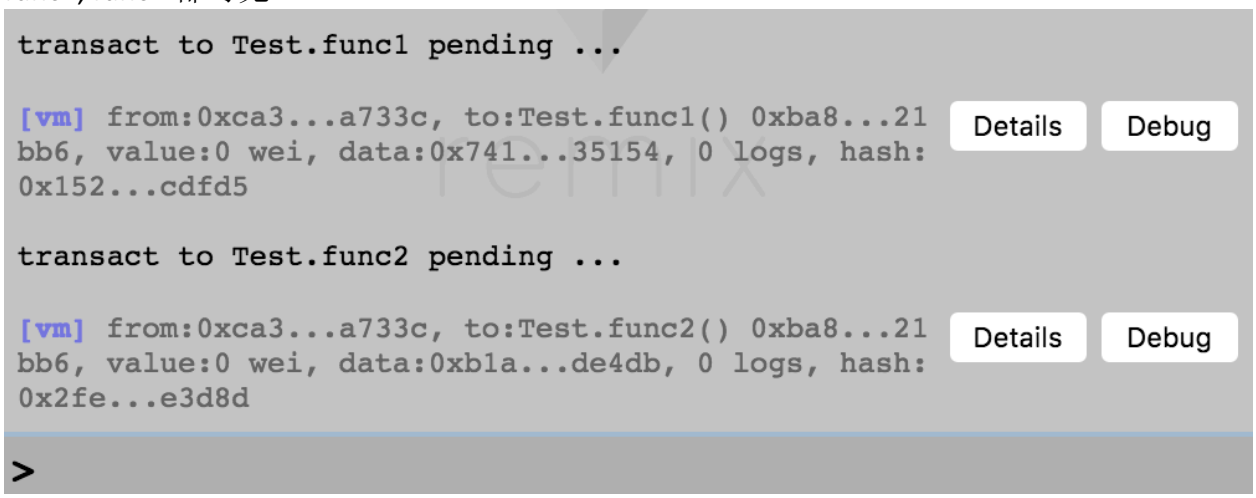
Details Debug

Details Debug

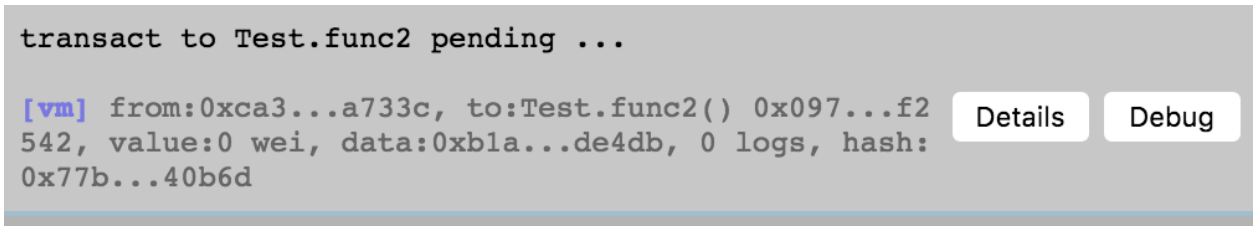
```
contract Test {
   uint private a = 1;
}
```
无函数

```
contract Test {
   uint a;
   function func1() {

   }
   function func2() {
      func1();
   }
}
```

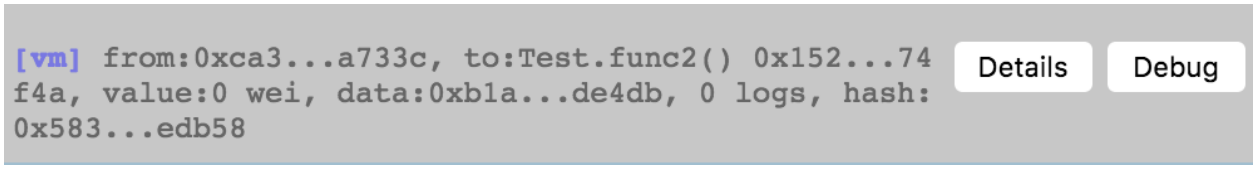
func1, func2 都可见



改为 function private func1()
只有 func2 可见

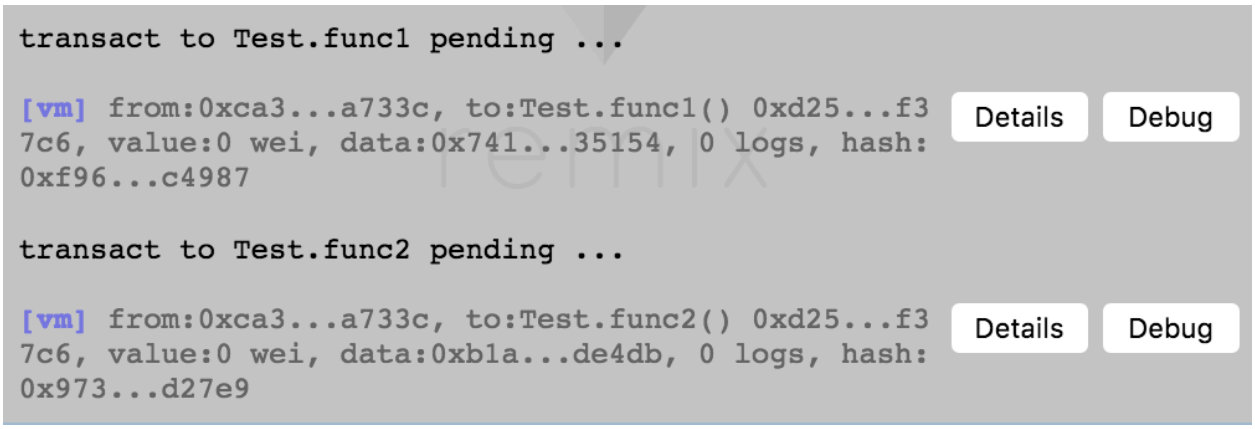


改为 function internal func1()
只有 func2 可见



```
contract Test {
   uint a;

   function func1() external {

   }

   function func2() {
      this.func1();
   }
}
```

this 把自己的合约当做外部合约来用 外部调用模式




```
pragma solidity ^0.4.14;

contract owned {

   address owner;

   function owned() {
      owner = msg.sender;
   }
}

contract Parent is owned {

   uint x;

   function Parent(uint _x) {
      x = _x;
   }
```

```
    function parentFunc1() internal {
        if (msg.sender == owner) selfdestruct(owner);
    }

    function parentFunc2() public {}

    function parentFunc3() external {}

    function parentFunc4() private {}
}

contract Child is Parent {
    uint y;
    function Child(uint _y) Parent (_y*_y) {
        y = _y;
    }

    function child() {
        parentFunc2();
        this.parentFunc3();
        parentFunc1();
    }
}

contract Child2 is Parent(666) {
    uint y;
    function Child(uint _y) {
        y = _y;
    }

    function child() {
        parentFunc1();
        parentFunc2();
        this.parentFunc3();
    }
}
```

```
creation of owned pending...

[vm] from:0xca3...a733c, to:owned.(constructor), value:0 wei, data:0x606...70029, 0 logs, hash:0x5e2...a8f17

creation of Parent pending...

[vm] from:0xca3...a733c, to:Parent.(constructor), value:0 wei, data:0x606...d0029, 0 logs, hash:0x304...2dc13

transact to Parent.parentFunc2 pending ...

[vm] from:0xca3...a733c, to:Parent.parentFunc2() 0x5b0...2aa77, value:0 wei, data:0x79a...a17ff, 0 logs, hash:0x95b...02e6d

transact to Parent.parentFunc3 pending ...

[vm] from:0xca3...a733c, to:Parent.parentFunc3() 0x5b0...2aa77, value:0 wei, data:0xc52...2d5df, 0 logs, hash:0x2d5...fc658
```

Details Debug

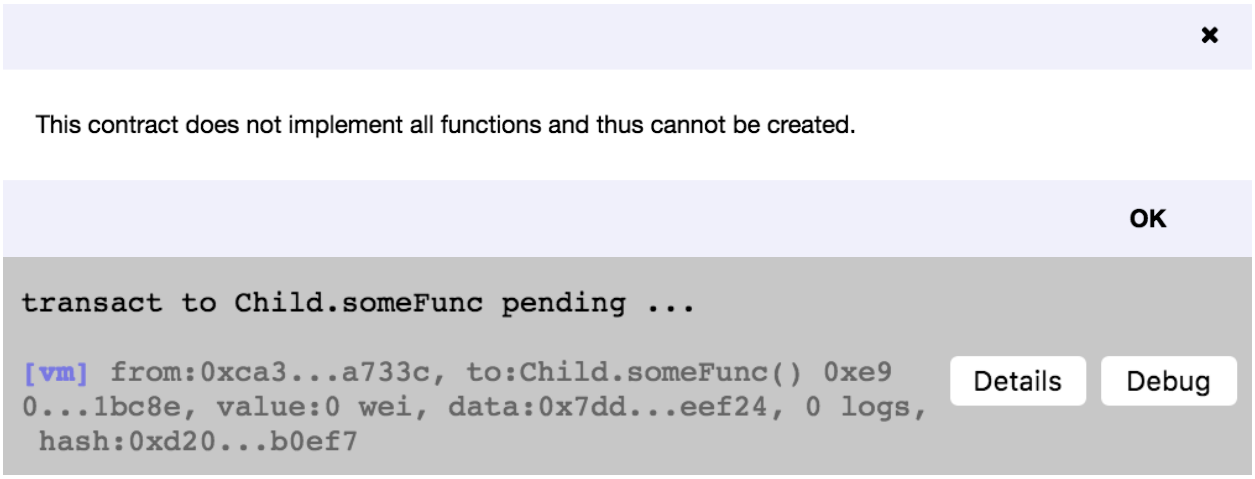
Details Debug

Details Debug

Details Debug

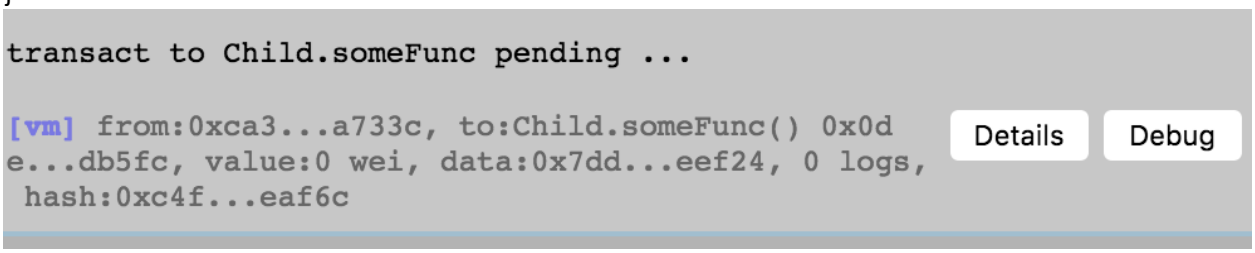
抽象合约 无法部署在区块链上

```
contract Parent {
   function someFunc() returns (uint);
}

contract Child is Parent {
   function someFunc() returns (uint) {
      return 1;
   }
}
```



INTERFACE 类似于 java 中概念，只是一个告诉我们之后编程的框架，告诉我们实现什么功能，只有 function 定义，子类要求没有实现方法的实现。如果没完成，则无法部署。

```
interface Parent{
   function someFunc() returns (uint);
}

contract Child is Parent {
   function someFunc() returns (uint) {
      return 1;
   }
}
```



```
contract Base1 {
   function func1() {}
}

contract Base2 {
   function func2() {}
}

contract Final is Base1, Base2 {
}
```

```
creation of Base1 pending...

[vm] from:0xca3...a733c, to:Base1.(constructor), value:0 wei, data:0x606...80029, 0 logs, hash:0x03a...13ccd

transact to Base1.func1 pending ...

[vm] from:0xca3...a733c, to:Base1.func1() 0x692...77b3a, value:0 wei, data:0x741...35154, 0 logs, hash:0x51c...bf9e5

creation of Base2 pending...

[vm] from:0xca3...a733c, to:Base2.(constructor), value:0 wei, data:0x606...30029, 0 logs, hash:0xa1c...204fd

transact to Base2.func2 pending ...

[vm] from:0xca3...a733c, to:Base2.func2() 0x0dc...97caf, value:0 wei, data:0xb1a...de4db, 0 logs, hash:0xc8d...3c7df

transact to Final.func1 pending ...

[vm] from:0xca3...a733c, to:Final.func1() 0x089...659fb, value:0 wei, data:0x741...35154, 0 logs, hash:0x72f...72c38

transact to Final.func2 pending ...

[vm] from:0xca3...a733c, to:Final.func2() 0x089...659fb, value:0 wei, data:0xb1a...de4db, 0 logs, hash:0xa47...3c2d3
```

Details Debug

Details Debug

Details Debug

Details Debug

Details Debug

Details Debug

```
contract Base1 {
   function func1() {}
}

contract Base2 {
   function func1() {}
}

contract Final is Base1, Base2 {
}

contract test {
   function test() {
      Final f = new Final();
      f.func1();
   }
}
```
contract test 没有函数显示

```
contract Base1 {
   function func1() returns (uint){
      return 1;
   }
}

contract Base2 {
   function func1() returns (uint){
      return 2;
   }
}

contract Final is Base1, Base2 {
}

contract test {
   function test() {
      Final f = new Final();
      f.func1();
   }
}
```

优化后测试 Final 继承顺序

```
transact to Final.func1 pending ...

[vm] from:0xca3...a733c, to:Base2.func1() 0x860...24b9b, value:0 wei, data:0x741...35154, 0 logs, hash:0x32c...7ac96
```

Details Debug

status	0x1 Transaction mined and execution succeed
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	Base2.func1() 0x8609a0806279c94bcc5432e36b57281b3d524b9b
gas	3000000 gas
transaction cost	21466 gas
execution cost	194 gas
hash	0x32c536512d7bce086dd99751ed9d63093f3551858eff21f55e12c4a5a057ac96
input	0x74135154
decoded input	{}
decoded output	{ "0": "uint256: 2" }
logs	[]
value	0 wei

```
pragma solidity ^0.4.14;

contract foundation {
   function func1() {
   }
}
contract Base1 is foundation{
   function func1() {
      super.func1();
   }
}

contract Base2 is foundation{
   function func1() {
      super.func1();
   }
}

contract Final is Base1, Base2 {
}

contract test {
   function test() {
      Final f = new Final();
      f.func1();
   }
}
```

```
transact to foundation.func1 pending ...

[vm] from:0xca3...a733c, to:foundation.func1() 0x0d
c...97caf, value:0 wei, data:0x741...35154, 0 logs,
 hash:0x99f...dcf51

transact to Base1.func1 pending ...

[vm] from:0xca3...a733c, to:Base1.func1() 0x5e7...2
6e9f, value:0 wei, data:0x741...35154, 0 logs, has
h:0x9b2...9ae0f

transact to Base2.func1 pending ...

[vm] from:0xca3...a733c, to:Base1.func1() 0x089...6
59fb, value:0 wei, data:0x741...35154, 0 logs, has
h:0xbe3...076e9

transact to Final.func1 pending ...

[vm] from:0xca3...a733c, to:Final.func1() 0xef5...4
6e41, value:0 wei, data:0x741...35154, 0 logs, has
h:0x721...ad05d
```

Details Debug

Details Debug

Details Debug

Details Debug

```
pragma solidity ^0.4.14;

contract Parent {
   uint public a = 2;
   modifier someModifier(){
      _;
      a = 1;
   }

   function parentFunc2(uint value) someModifier public returns (uint) {
      a = value;
      return a;
   }

   function parentFunc3(uint value) public returns (uint) {
      a = value;
      return a;
      a = 1;
   }
}
```

此处与老董讲的有出入

transact to Parent.parentFunc2 pending ...

[vm] from:0xca3...a733c, to:Parent.parentFunc2(uint256) 0x35e...450cf, value:0 wei, data:0x62b...00005, 0 logs, hash:0xe38...36a5c Details Debug

status	0x1 Transaction mined and execution succeed
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	Parent.parentFunc2(uint256) 0x35ef07393b57464e93deb59175ff72e6499450cf
gas	3000000 gas
transaction cost	31969 gas
execution cost	10505 gas
hash	0xe381035bb5a327e8dcd9a461ebba937e1944f66f21bedb37bf39617a4df36a5c
input	0x62b499ca0000000000000000000000000000000000000000000000000000000000000005
decoded input	{ "uint256 value": "5" }

transact to Parent.parentFunc3 pending ...

[vm] from:0xca3...a733c, to:Parent.parentFunc3(uint256) 0x692...77b3a, value:0 wei, data:0x510...00005, 0 logs, hash:0x397...9af86 Details Debug

status	0x1 Transaction mined and execution succeed
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	Parent.parentFunc3(uint256) 0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
gas	3000000 gas
transaction cost	26933 gas
execution cost	5469 gas
hash	0x397caa20cb877112c77fde7ec360778a93412f534907e2dcbc588a945239af86
input	0x510dbafb0000000000000000000000000000000000000000000000000000000000000005
decoded input	{ "uint256 value": "5" }
decoded output	{ "0": "uint256: 5"

```
contract test {
   uint8 public a = 0;

   function set() {
      a -= 100;
   }
}
```

```
transact to test.set pending ...

[vm] from:0xca3...a733c, to:test.set() 0x5e7...26e9
f, value:0 wei, data:0xb8e...010de, 0 logs, hash:0x
03a...cc964

call to test.a

[call] from:0xca35b7d915458ef540ade6068dfe2f44e8fa7
33c, to:test.a(), data:0dbe6...e671f, return:
{
        "0": "uint8: 156"
}
```

Details Debug Details Debug

a = 101 时正常

```
transact to test.set pending ...

[vm] from:0xca3...a733c, to:test.set() 0xef5...46e4
1, value:0 wei, data:0xb8e...010de, 0 logs, hash:0x
8fe...c6e81

call to test.a

[call] from:0xca35b7d915458ef540ade6068dfe2f44e8fa7
33c, to:test.a(), data:0dbe6...e671f, return:
{
        "0": "uint8: 1"
}
```

Details Debug Details Debug

```
contract test {
   uint8 public a = 1;

   function set() {
      uint8 c = a - 100;
      assert(c < a);
      a = c;
   }
}
```

此时抛出异常

```
[vm] from:0xca3...a733c, to:test.set() 0x9dd...d44d
d, value:0 wei, data:0xb8e...010de, 0 logs, hash:0x
952...9f798

transact to test.set errored: VM error: invalid opcode.
invalid opcode
        The execution might have thrown.
        Debug the transaction to get more information.
```

Details Debug

```
pragma solidity ^0.4.14;

import "./SafeMath.sol";
contract test {
   uint8 public a = 1;

   function set() {
      a = SafeMath.sub(a,100);
   }
}
```

```
import "./SafeMath.sol";
contract test {
   using SafeMath for uint8;
   uint8 public a = 1;

   function set() {
      a = a.sub(100);
   }

}
```

```
transact to test.set pending ...

[vm] from:0xca3...a733c, to:test.set() 0x038...072b
a, value:0 wei, data:0xb8e...010de, 0 logs, hash:0x
10e...5d588

transact to test.set errored: VM error: invalid opcode.
invalid opcode
        The execution might have thrown.
        Debug the transaction to get more information.
```

Details Debug

调用 owner

```
call to Payroll.owner

[call] from:0xca35b7d915458ef540ade6068dfe2f44e8fa733c, to:Payroll.owner(), da
ta:8da5c...5cb5b, return:
{
        "0": "address: 0xca35b7d915458ef540ade6068dfe2f44e8fa733c"
}
```

Details Debug

调用 addfund

```
transact to Payroll.addFund pending ...

[vm] from:0xca3...a733c, to:Payroll.addFund() 0x692...77b3a, value:10000000000
0000000000 wei, data:0xa2f...09dfa, 0 logs, hash:0x19c...15697
```

Details Debug

status	0x1 Transaction mined and execution succeed
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	Payroll.addFund() 0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
gas	3000000 gas
transaction cost	21962 gas
execution cost	690 gas
hash	0x19c3ff90432916a43bc3a7d69d8097032a0e0757a683e226deb1a662a7615697
input	0xa2f09dfa
decoded input	{}
decoded output	{ "0": "uint256: 10000000000000000000" }
logs	[]
value	10000000000000000000 wei

调用 addEmployee(“0x14723a09acff6d2a60dcdf7aa4aff308fddc160c”, 1)

```
transact to Payroll.addEmployee pending ...

[vm] from:0xca3...a733c, to:Payroll.addEmployee(address,uint256) 0x692...77b3
a, value:0 wei, data:0xe7f...00001, 0 logs, hash:0xa7b...0d868
```

Details Debug

status	0x1 Transaction mined and execution succeed
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	Payroll.addEmployee(address,uint256) 0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
gas	3000000 gas
transaction cost	105223 gas
execution cost	82351 gas
hash	0xa7b6854e5c21f37fc769671602bfe3eb3dbd2ee5e5eb4e988ce2ffc398e0d868
input	0xe7fd9a1300000000000000000000000014723a09acff6d2a60dcdf7aa4aff308fddc160c0000000000000000000000000000000000000000000000000000000000000001
decoded input	{ "address employeeId": "0x14723a09acff6d2a60dcdf7aa4aff308fddc160c", "uint256 salary": "1" }
decoded output	{}
logs	[]
value	0 wei

调用 addEmployee("0x4b0897b0513fdc7c541b6d9d7e929c4e5364d2db", 1)

```
transact to Payroll.addEmployee pending ...

[vm] from:0xca3...a733c, to:Payroll.addEmployee(address,uint256) 0x692...77b3
a, value:0 wei, data:0xe7f...00001, 0 logs, hash:0x470...50b9b
```

Details Debug

status	0x1 Transaction mined and execution succeed
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	Payroll.addEmployee(address,uint256) 0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
gas	3000000 gas
transaction cost	90223 gas
execution cost	67351 gas
hash	0x470db724a64b0222fb48390512810c4184ce614fca646b3329f9459d55b50b9b
input	0xe7fd9a1300000000000000000000000004b0897b0513fdc7c541b6d9d7e929c4e5364d2db000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001
decoded input	{ "address employeeId": "0x4b0897b0513fdc7c541b6d9d7e929c4e5364d2db", "uint256 salary": "1" }

调用 employees("0x4b0897b0513fdc7c541b6d9d7e929c4e5364d2db")

```
call to Payroll.employees

[call] from:0xca35b7d915458ef540ade6068dfe2f44e8fa733c, to:Payroll.employees(a
ddress), data:d0678...4d2db, return:
{
        "0": "address: id 0x4b0897b0513fdc7c541b6d9d7e929c4e5364d2db",
        "1": "uint256: salary 1000000000000000000",
        "2": "uint256: lastPayday 1521603022"
}
```

Details Debug

调用 calculaterunway

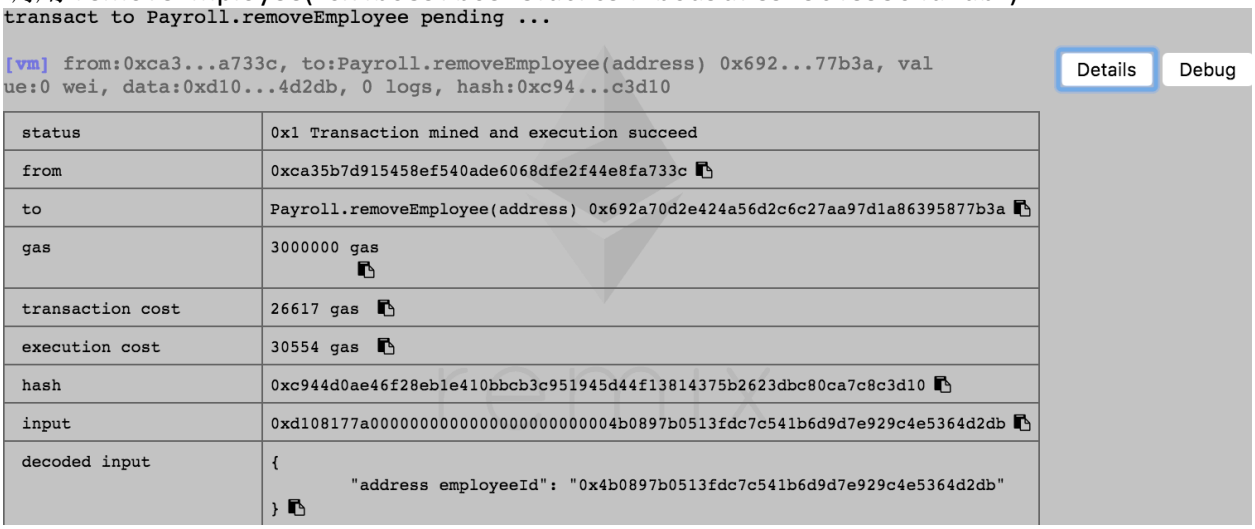
```
transact to Payroll.calculateRunway pending ...

[vm] from:0xca3...a733c, to:Payroll.calculateRunway() 0x692...77b3a, value:0 w
ei, data:0x4ec...19512, 0 logs, hash:0x6e0...2c873
```

Details Debug

status	0x1 Transaction mined and execution succeed
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	Payroll.calculateRunway() 0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
gas	3000000 gas
transaction cost	22200 gas
execution cost	928 gas
hash	0x6e09a07d6d697987411f7c64378dd68a57318c405a70d87a09baea9da102c873
input	0x4ec19512
decoded input	{}
decoded output	{ "0": "uint256: 50" }

调用 hasenoughfund

调用 removeEmployee(“0x4b0897b0513fdc7c541b6d9d7e929c4e5364d2db”)



调用 updateEmployee("0x14723a09acff6d2a60dcdf7aa4aff308fddc160c", 2)

```
transact to Payroll.updateEmployee pending ...

[vm] from:0xca3...a733c, to:Payroll.updateEmployee(address,uint256) 0x692...77
b3a, value:0 wei, data:0x5e9...00002, 0 logs, hash:0x7e7...423a8
```

Details Debug

status	0x1 Transaction mined and execution succeed
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	Payroll.updateEmployee(address,uint256) 0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
gas	3000000 gas
transaction cost	53956 gas
execution cost	46084 gas
hash	0x7e73a1c8ba82c9712f362e66e1a1c6b040562ceebc68645db4d45ac7cd2423a8
input	0x5e91d8ec00000000000000000000000014723a09acff6d2a60dcdf7aa4aff308fddc160c000000000000000000 000000000000000000000000000000000000000000002
decoded input	{ "address employeeId": "0x14723a09acff6d2a60dcdf7aa4aff308fddc160c", "uint256 salary": "2" }

调用 getPaid

```
transact to Payroll.getPaid pending ...

[vm] from:0x147...c160c, to:Payroll.getPaid() 0x692...77b3a, value:0 wei, dat
a:0xcf4...1d6f8, 0 logs, hash:0x607...bed5d
```

Details Debug

status	0x1 Transaction mined and execution succeed
from	0x14723a09acff6d2a60dcdf7aa4aff308fddc160c
to	Payroll.getPaid() 0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
gas	3000000 gas
transaction cost	35196 gas
execution cost	13924 gas
hash	0x607244ff362123a5e1d807fd5bd214892eef788b32cd194785b2a80f6ecbed5d
input	0xcf41d6f8
decoded input	{}
decoded output	{}
logs	[]
value	0 wei

调用 changePaymentAddress(“0x583031d1113ad414f02576bd6afabfb302140225”)

```
transact to Payroll.changePaymentAddress pending ...
```

```
[vm] from:0x147...c160c, to:Payroll.changePaymentAddress(address) 0x692...77b3
a, value:0 wei, data:0x712...40225, 0 logs, hash:0xaa9...d869a
```

Details Debug

status	0x1 Transaction mined and execution succeed
from	0x14723a09acff6d2a60dcdf7aa4aff308fddc160c
to	Payroll.changePaymentAddress(address) 0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
gas	3000000 gas
transaction cost	54355 gas
execution cost	76675 gas
hash	0xaa9a51d808b36681992e85d6de39d18dbcf6721faf8fddd507ff32c2e6bd869a
input	0x7124d61300000000000000000000000000583031d1113ad414f02576bd6afabfb302140225
decoded input	{ "address newaddress": "0x583031d1113ad414f02576bd6afabfb302140225" }

调用 transferOwnership("0x583031d1113ad414f02576bd6afabfb302140225")

```
[vm] from:0xca3...a733c, to:Payroll.transferOwnership(address) 0x692...77b3a,
value:0 wei, data:0xf2f...40225, 1 logs, hash:0xcce...25827
```

Details Debug

status	0x1 Transaction mined and execution succeed
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	Payroll.transferOwnership(address) 0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
gas	3000000 gas
transaction cost	30438 gas
execution cost	7758 gas
hash	0xcce6e81225844097fdd15975799e9926f158615afa693dc9bb606e2f4d825827
input	0xf2fde38b00000000000000000000000000583031d1113ad414f02576bd6afabfb302140225
decoded input	{ "address newOwner": "0x583031d1113ad414f02576bd6afabfb302140225" }
decoded output	{}
logs	[{ "topic": "8be0079c531659141344cd1fd0a4f28419497f9722a3daafe3b4186f6b6457e0", "event": "OwnershipTransferred", "args": ["ca35b7d915458ef540ade6068dfe2f44e8fa733c", "583031d1113ad414f02576bd6afabfb302140225"] }]