

PAX兑换PAXO流程

1. 背景

PAX是在以太坊上发行的、ERC-20规范的稳定币，现将PAX引入到Ontology平台。

Ontology 在以太坊链上发行PAX销毁合约，PAX(ERC-20)持有人将Token转入到合约，Ontology 会部署监控程序监控销毁合约，监控程序会将任意一笔PAX兑换PAXO交易，在Ontology 链上给用户的ONT钱包地址转入相同数量的PAXO，1: 1锚定

2. PAX->PAXO步骤

以下步骤通过Remix演示，实际场景下需要使用SDK调用合约

2.1. PAX ERC-20 Token合约编译

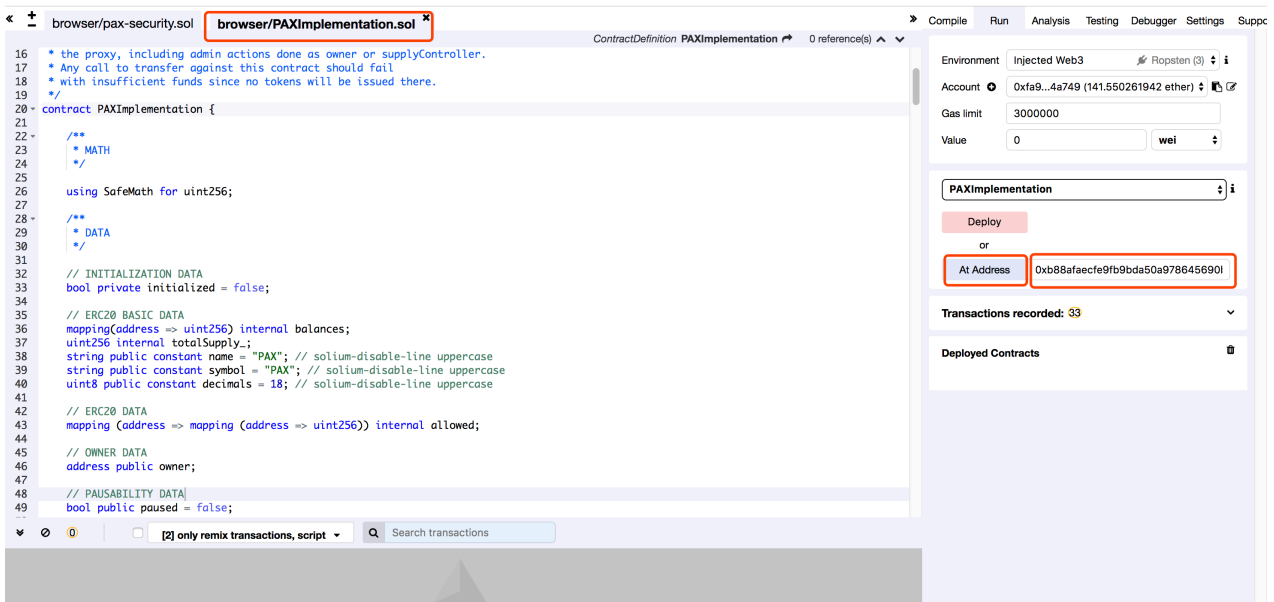
PAX Token合约地址：[Pax Contract](#)

需要把contracts目录下的主合约PAXImplementation在REMIX下编译，solidity编译器版本0.4.24

编译成功后，在右上角Run选项页面，选择PAXImplementation合约

在At Address输入框输入PAX Token的合约Hash地

址: 0x8e870d67f660d95d5be530380d0ec0bd388289e1



PAX合约加载成功后，如下图

Environment

Injected Web3

Ropsten (3)

Account

0xfa9...4a749 (141.550261942 ether)

Gas limit

3000000

Value

0

wei

PAXImplementation

Deploy

or

At Address

0xb88afaecfe9fb9bda50a978645690I

Transactions recorded: 33

Deployed Contracts

PAXImplementation at 0xb88...d0490 (blockchain)

2.2. Approve PAX给销毁合约




PAX合约地址 0x8e870d67f660d95d5be530380d0ec0bd388289e1

调用接口 approve

参数

- : **spender**, `address` 类型, 销毁合约地址: `0x0628ba39a124b772fae5edd52d2aa330e0f1078a`
- : **value**, `bigint` 类型, PAX的精度是18, Approve 1个PAX, Value应输入: `1000000000000000000`

Compile Run Analysis Testing Debugger Settings Supp

Account  `0xfa9...4a749 (141.550261942 ether)`  

Gas limit `3000000`

Value `0` `wei` 

PaxLock  


Deploy

or

At Address

`0xcc744467981fab32e5c37afd28a593`

Transactions recorded: **33** 

Deployed Contracts 

 **PAXImplementation at 0xb88...d0490**
(blockchain)  

approve 

`_spender:` `0xcc744467981fab32e5c37afd28a593t`

`_value:` `1000000000000000000`



transact

decreaseSupply	uint256 _value	✓
freeze	address _addr	✓
increaseSupply	uint256 _value	✓
initialize		
pause		
setLawEnforcementRole	address _newLawEnforcementRole	✓
setSupplyController	address _newSupplyController	✓
transfer	address _to, uint256 _value	✓

2.3. PAX入金

销毁合约地址：0x0628ba39a124b772fae5edd52d2aa330e0f1078a

调用接口：PAXTOOEP4

参数

- **_ont_base58_address**: `string` 类型,PAX持有人的ONT钱包地址
- **_value**: `bigint` 类型, 转换PAXO的数量, 要求和2.2接口的参数value相同, 且数量不能超过2.2接口Approve的Token数量

PaxLock

Deploy

address[] _owners, uint256 _required

or

At Address

0x250545a9b5806e38a94866d0453f

Transactions recorded: 41

All transactions (deployed contracts and function executions) in this environment can be saved and replayed in another environment. e.g Transactions created in Javascript VM can be replayed in the Injected Web3.

Deployed Contracts

PAXImplementation at 0xb88...d0490 (blockchain)

PaxLock at 0x250...51b5f (blockchain)

ChangeOwner

string _txId, uint8[] _v, bytes32[] _r, byte

OEP4TOPAX

string _txId, address _to, uint256 _value

PAXTOOEP4

_from:

0xfA98bb293724fA6b012DA0F39D4e1f

ont_bas58

Ad4pjz2bqep4RhQrUAzMuzJkBC3qJ1tZ

_address:

_value:

10000000000000000000

transact

owners

调用成功后，用户的PAX会成功减少，用户的PAXO余额会增加。

PAXO的合约hash为 6bbc07bae862db0d7867e4e5b1a13c663e2b4bc8

可以使用[ONT浏览器](#)查看余额