EIP 20: ERC-20 代币标准（Token Standard）

作者	状态	类型	分类	创建时间
Fabian Vogelsteller, Vitalik Buterin	Final	Standards Track	ERC	2015-11-19

简要说明

代币（Token）的标准接口。

> Token 亦有人翻译为通证，指在以太坊上通过智能合约发行的资产（或权益）。

摘要

本标准说明了在智能合约中实现代币的标准API。

该标准提供了代币的基本功能：如转移代币，授权代币给其他人（如链上第三方应用）使用。

动机

标准接口允许以太坊上的任何代币被其他应用程序重用，如钱包、去中心化交易所等。

API 规范

函数

注意:

- API 规范使用 Solidity 0.4.17（或以上版本）的语法
- 调用者必须处理 `returns (bool success)` 返回 `false` ，不能假定 `false` 不会返回。

可选函数: name

函数返回代币的名称 - 如 `"MyToken"` 或 `"我的代币"`

此函数是可选函数，但是这个函数可以提高代币可用性，不过调用者不能假定这个函数存在。

```js
function name() public view returns (string)
```

可选函数: symbol

函数返回代币的代号(通常为字母缩写)，如 "HIX"，"UPT"。

此函数是可选函数，但是这个函数可以提高代币可用性，不过调用者不能假定这个函数存在。

可选函数: decimals

返回令牌使用的小数位数 - 例如"8"，意味着将令牌量除以"100000000"以获取其用户表示形式。

此函数是可选函数，但是这个函数可以提高代币可用性，不过调用者不能假定这个函数存在。

```js
function decimals() public view returns (uint8)
```

函数: totalSupply

返回总令牌供应量。

```js
function totalSupply() public view returns (uint256)
```

函数: balanceOf

返回帐户（通过参数"_owner"）的余额。

```js
function balanceOf(address _owner) public view returns (uint256 balance)
```

函数: transfer

向 `_to` 地址转移 `_value` 数量的代币，函数必须触发事件 `Transfer` 。

如果调用方的帐户余额没有足够的令牌，则该函数需要抛出异常。

注意 转移0个代币也是正常转移动作，同样需要触发 `Transfer` 事件。

```js
function transfer(address _to, uint256 _value) public returns (bool success)
```

函数: transferFrom

从 `_from` 向 `_to` 地址转移 `_value` 数量的代币，函数必须触发事件 `Transfer` 。

`transferFrom` 函数，可以允许第三方代表我们转移代币。

如果 `_from` 账号没有授权调用帐户转移代币，则该函数需要抛出异常。

注意 转移0个代币也是正常转移动作，同样需要触发 `Transfer` 事件。

```js
function transferFrom(address _from, address _to, uint256 _value) public returns (
```

函数: approve

这个函数可以再次调用，以覆盖授权额度 `_value` 。

注意: 为了阻止向量攻击(这里有**描述**和**讨论**)，调用者可以在调整授权额度时，先设置为0，然后在设置为一个其他额度。

> 简单描述下：向量攻击， 假如 Alice 开始时给Bob授权了 N, 现在 Alice 想调整为 M ，于是发起了一笔调整授权的交易，这时Bob观察到了这笔交易， 迅速通过 transferFrom 交易（用更高的手续费，矿工优先打包）把 N 个币转移走，待 Alice 调整授权的交易打包后，Bob 又获得了 M 个授权。 这就相当于 Bob 获得了 N + M个授权， 而不是 Alice 想要的 M个授权。

```js
function approve(address _spender, uint256 _value) public returns (bool success)
```

函数: allowance

查询 `_owner` 授权给 `_spender` 的额度。

```js
function allowance(address _owner, address _spender) public view returns (uint256
```

事件Events

事件：Transfer

当有代币转移时（包括转移0），必须触发 Transfer 事件。

如果是新产生代币，触发 Transfer 事件的 `_from` 应该设置为 `0x0` 。

```js
event Transfer(address indexed _from, address indexed _to, uint256 _value)
```

事件：Approval

`approve(address _spender, uint256 _value)` 函数成功执行时，必须触发 Approval 事件。

```js
event Approval(address indexed _owner, address indexed _spender, uint256 _value)
```

实现

在以太坊网络上已经有大量符合 ERC20 的代币。 各个团队有不同的实现， 有些注重安全性，有些关注使用更少的gas。

实现示例

- OpenZeppelin
- ConsenSys 实现

讨论历史

相关讨论的历史链接:

- Original proposal from Vitalik Buterin: https://github.com/ethereum/wiki/wiki/Standardized_Contract_APIs/499c882f3ec123537fc2fccd57eaa29e603
- Reddit discussion: https://www.reddit.com/r/ethereum/comments/3n8fkn/lets_talk_about_the_coin_standard/
- Original Issue #20: https://github.com/ethereum/EIPs/issues/20

版权

原文采用CC0， 本翻译采用BY-NC-ND许可协议，译者：深入浅出区块链 Tiny熊。

帮助完善文档

Last Updated: 9/4/2019, 11:28:22 PM

← 所有标准提案（ERC） EIP 55: 混合大小写校验和地址编码 →