25 美链 Beauty Chain

背景介绍

- 美链(Beauty Chain)是一个部署在以太坊上的智能合约，有自己的代币BEC。
  - 没有自己的区块链，代币的发行、转账都是通过调用智能合约中的函数来完成的
  - 可以自己定义发行规则，每个账户有多少代币也是保存在智能合约的状态变量里
  - ERC 20是以太坊上发行代币的一个标准，规范了所有发行代币的合约应该实现的功能和遵循的接口
  - 美链中有一个叫batchTransfer的函数，它的功能是向多个接收者发送代币，然后把这些代币从调用者的帐户上扣除

ERC Ethereum request for comments

```
function batchTransfer(address[] _receivers, uint256 _value) public whenNotPaused returns (bool) {
  uint cnt = _receivers.length;
  uint256 amount = uint256(cnt) * _value;
  require(cnt > 0 && cnt <= 20);
  require(_value > 0 && balances[msg.sender] >= amount);

  balances[msg.sender] = balances[msg.sender].sub(amount);
  for (uint i = 0; i < cnt; i++) {
      balances[_receivers[i]] = balances[_receivers[i]].add(_value);
      Transfer(msg.sender, _receivers[i], _value);
  }
  return true;
 }
}
```

问题出现在uint256 amount = unit256(cnt) * _value这个乘法是有可能溢出的，导致amount是一个非常小的数字，导致扣了非常小的一个数字的代币，但是给每个账户转了非常多的代币。最终的处理方式就是回滚了。

预防措施

- SafeMath库
  - 只要通过SafeMath提供的乘法计算amount，就可以很容易地检测到溢出

```
library SafeMath {

  /**
  * @dev Multiplies two numbers, throws on overflow.
  */
  function mul(uint256 a, uint256 b) internal pure returns (uint256 c) {
    if (a == 0) {
      return 0;
    }
    c = a * b;
    assert(c / a == b);
    return c;
  }
```

上面的代码里就是*一不小心写成了普通的，而加法减法都是使用了safeMath库。