**Developing Emerging Internet Applications**

**以太坊智能合约编程**

1. 逻辑描述及源码截图

（1）创建结构体 **crowdfunding** 包含众筹合约的基本信息。

并创建一个数组 **allcrowdfunding** 存储所有已经创建的众筹合约

**Id ->** 合约id,同时也是合约在数组中的位置

NeedMoney -> 众筹合约需要的钱的总数

ReceivedMoney -> 已经筹集到的金钱总数

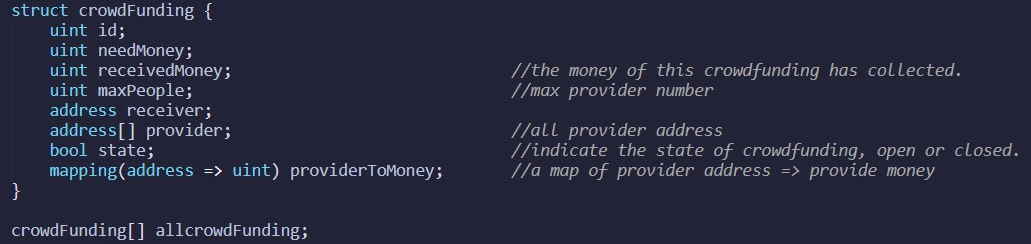
Maxpeopple -> 最多的捐赠人数

Receiver -> 发布众筹合约的人的地址

Provider[] -> 所有捐赠人的地址，方便众筹失败时的退回

State -> 众筹合约的状态，分为open状态和close状态（close 又分为完成或失败终止）

providerToMoney -> 捐赠者地址和捐赠额的对应，方便退回



1. 创建一些event

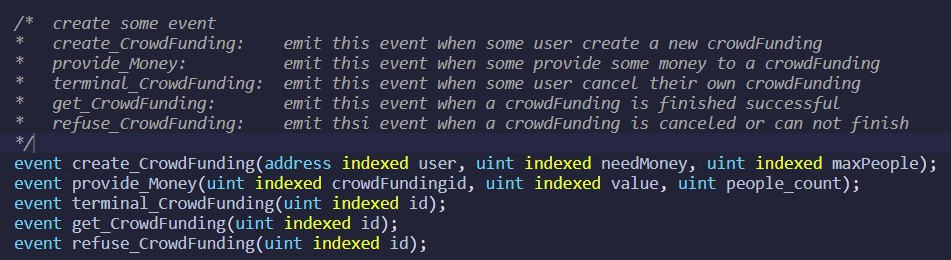
Create\_CrowdFunding -> 当一个新的合约被创建时调用

Provide\_Money -> 当有人成功捐赠时调用

Terminal\_CrowdFunding -> 当一个合约完成或终止时调用

Get\_CrowdFunding -> 当合约成功，并把筹集资金转给接受者时调用

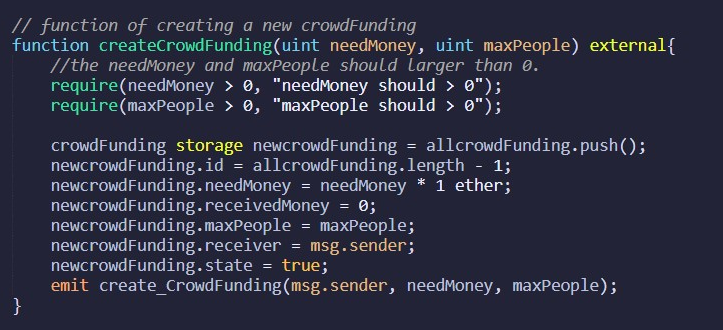
Refuse\_CrowdFunding -> 当合约失败或终止，资金原路退回时调用



1. 创建众筹合约方法

创建条件为 **需要资金 > 0 && 最大捐赠人数 > 0**

根据方法传递的参数创建合约实例，添加到包含所有合约的数组中，emit对应的event。



1. 创建捐赠方法

捐赠条件： 合约存在并且合约的状态是开启的

如果捐赠者第一次捐款，则把捐赠者的地址添加到合约的provider数组中

修改这个捐赠者对应的捐款额（providerToMoney），修改合约接收到的总的捐款额（receivedMoney）

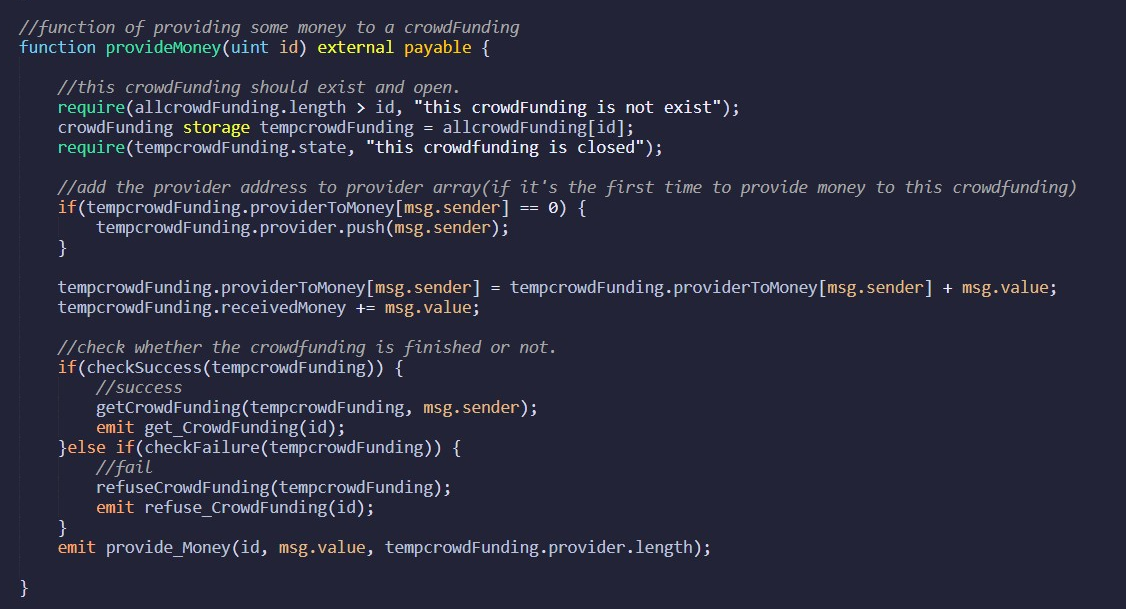
完成捐赠操作后判断：

若合约成功（checkSuccess方法）

申请人获得众筹资金（getCrowdFunding方法），并emit对应event

若合约失败（checkFailure方法）

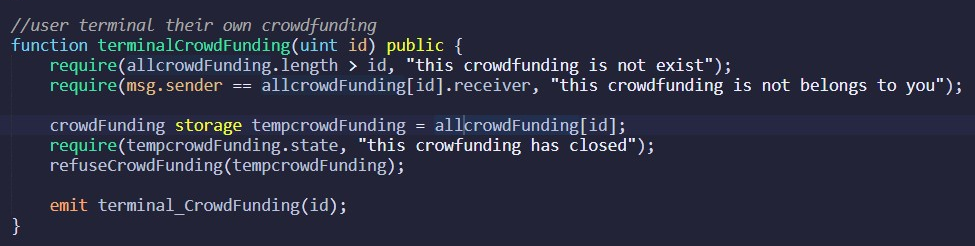
原路退回资金（refuse\_CrowdFunding方法），并emit对应event



1. 用户主动取消众筹合约方法

条件：合约存在并是开启状态，调用者是合约的拥有者

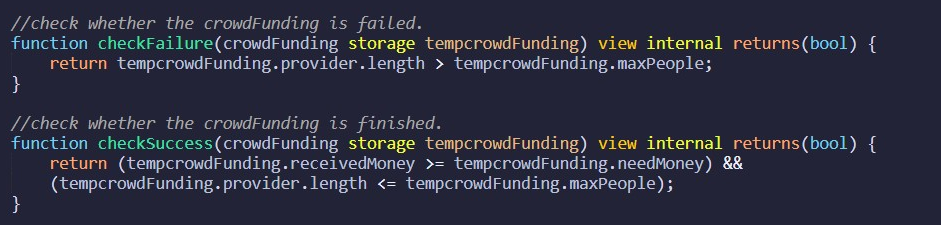
原路退回所有资金（refuseCrowdFunding方法）



1. 检测合约是否成功方法

检测失败（checkFailure）：当捐赠人数大于合约限制的最多人数

检测成功（checkSuccess）： 当获得的捐赠额大于需求数，并且捐赠人数不大于合约的限制人数



1. 申请人获得资金和资金原路退回方法

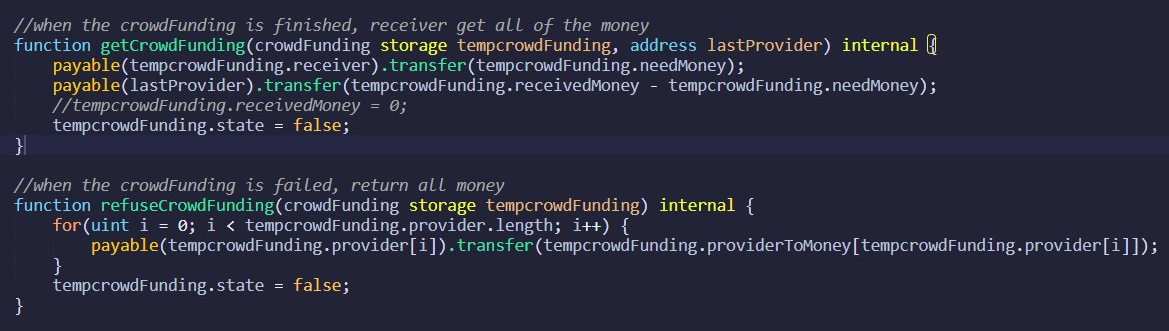
获得资金（getCrowdFunding）：

申请人获得他所需要的金钱数额，超过部分原路退回给最后一个捐赠者

原路退回资金（refuseCrowdFunding）：

根据所以的捐赠者地址（provider[]）和每个捐赠者对应的捐赠额（providerToMoney）原路退回

由于这两个方法都对应合约的关闭，所以在最后设置合约状态为False

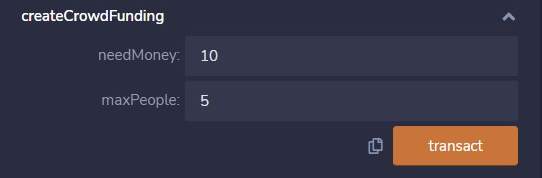
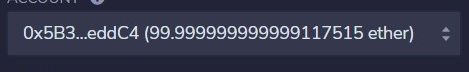


·

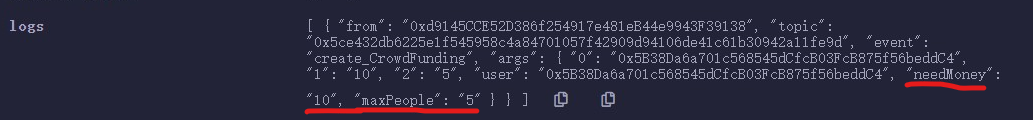
1. 部署截图

众筹成功演示

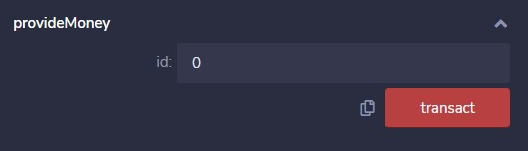
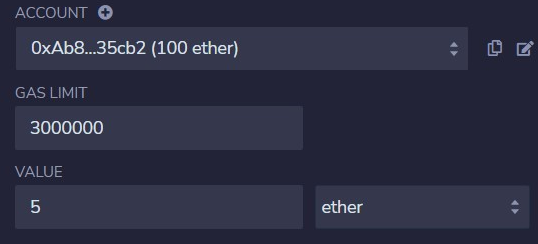
（1）账号..C4（余额为100ether）创建一个合约（需要金钱额：10 ether，捐赠人数： 10）



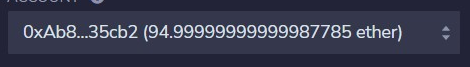
一下截图为创建的log截图，表明创建成功



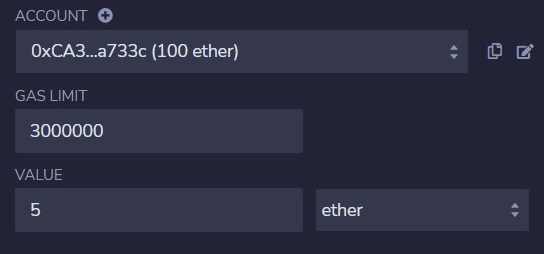
（2）另一个账户...cb2(余额100ether)为这个合约捐赠5 ether，由于我们只创建一个合约，所以这个合约id= 0



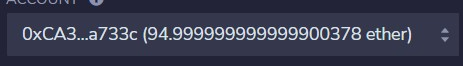
一下为捐赠之后这个账户的余额（100 -> 95）



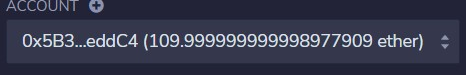
1. 同样，选择另一个账户..733c（余额为100 ether）再转5 ether



捐赠之后余额变为95 ether

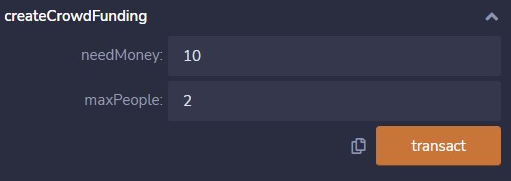
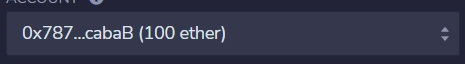


1. 观察结果，合约的提出者的余额由100增加到110 ether



失败演示：

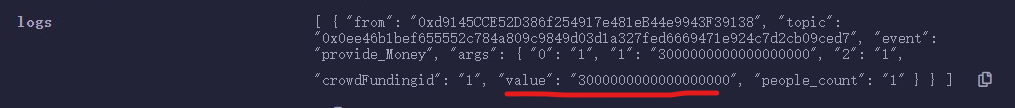
1. 账号baB(余额100)创建一个合约，需要金钱：10， 最大人数：2



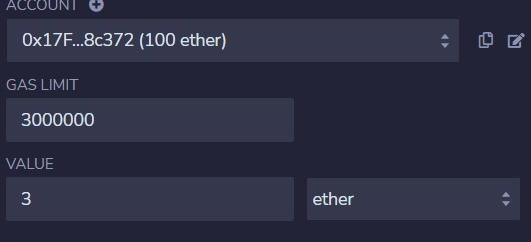
1. 另一个账号转3 ether给这个合约（余额从100变为97）



捐赠后输出的log



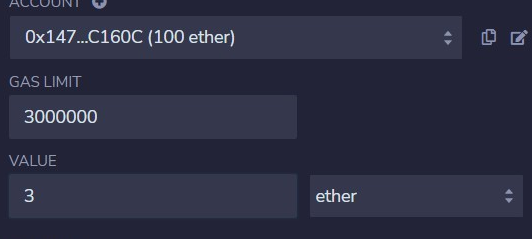
1. 另一个账户...372转3 ether（余额从100变为97）



转账之后截图

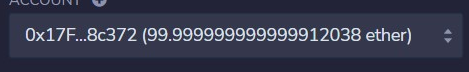


1. 另一个账户再转账3ether



由于人数超过合约限制，所以会调用资金退回方法，一下是结果截图，捐赠人的金额从97变为100

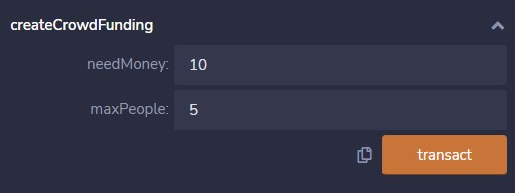
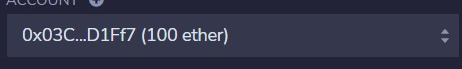






终止演示：

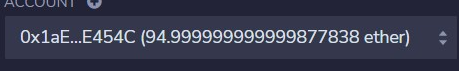
（1）账号Ff7创建合约，需要金额：10，最大人数：5



1. 账号454C捐赠5ether



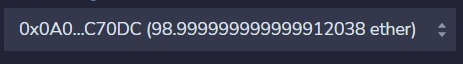
结果显示，捐赠者余额从100变为95



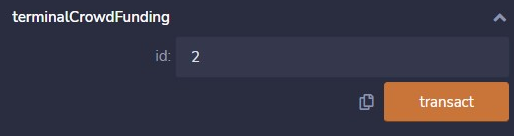
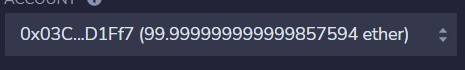
1. 账号0DC捐赠1ether



结果显示，余额从100变为99



1. 账户拥有者调用终止方法



结果截图，两个账户的金额都退回，余额都变为100



