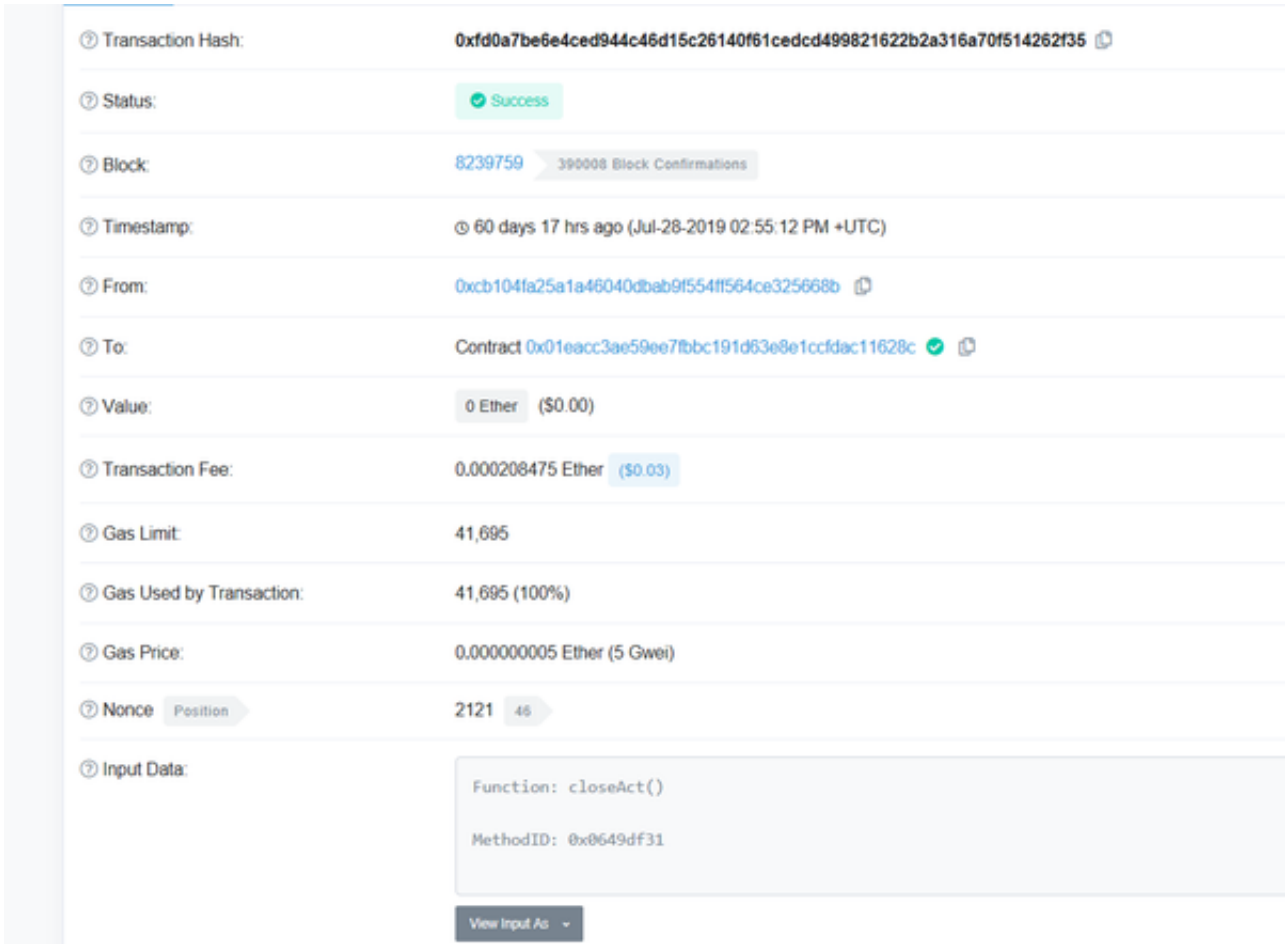
近日，FAIRWIN 智能合约存在漏洞这一问题引起各方关注，FAIRWIN 作为近日以太坊链上交易量最高的资金盘模式应用，在以太坊链上还存在大量类似的克隆盘，如果存在隐藏漏洞会给公链带来较大风向，因此成都链安安全人员对FAIRWIN智能合约展开了深度分析，分析结果如下：

通过对FAIRWIN合约代码进行审计，我们发现其合约存在一个remedy()接口，如果合约owner没有通过close()关闭接口时，该接口可以被任意用户调用，并且可以通过这个接口伪造投注数据，实现“无中生有”，在不使用任何资金的情况下伪造了充值记录，之后攻击者便可以享受分红，或者通过userWithDraw()将余额全部提出。

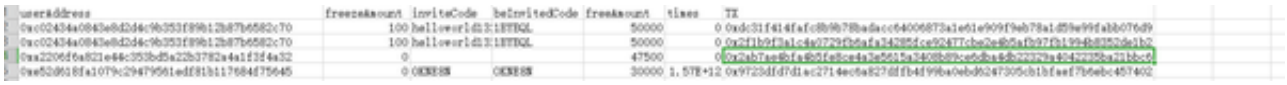


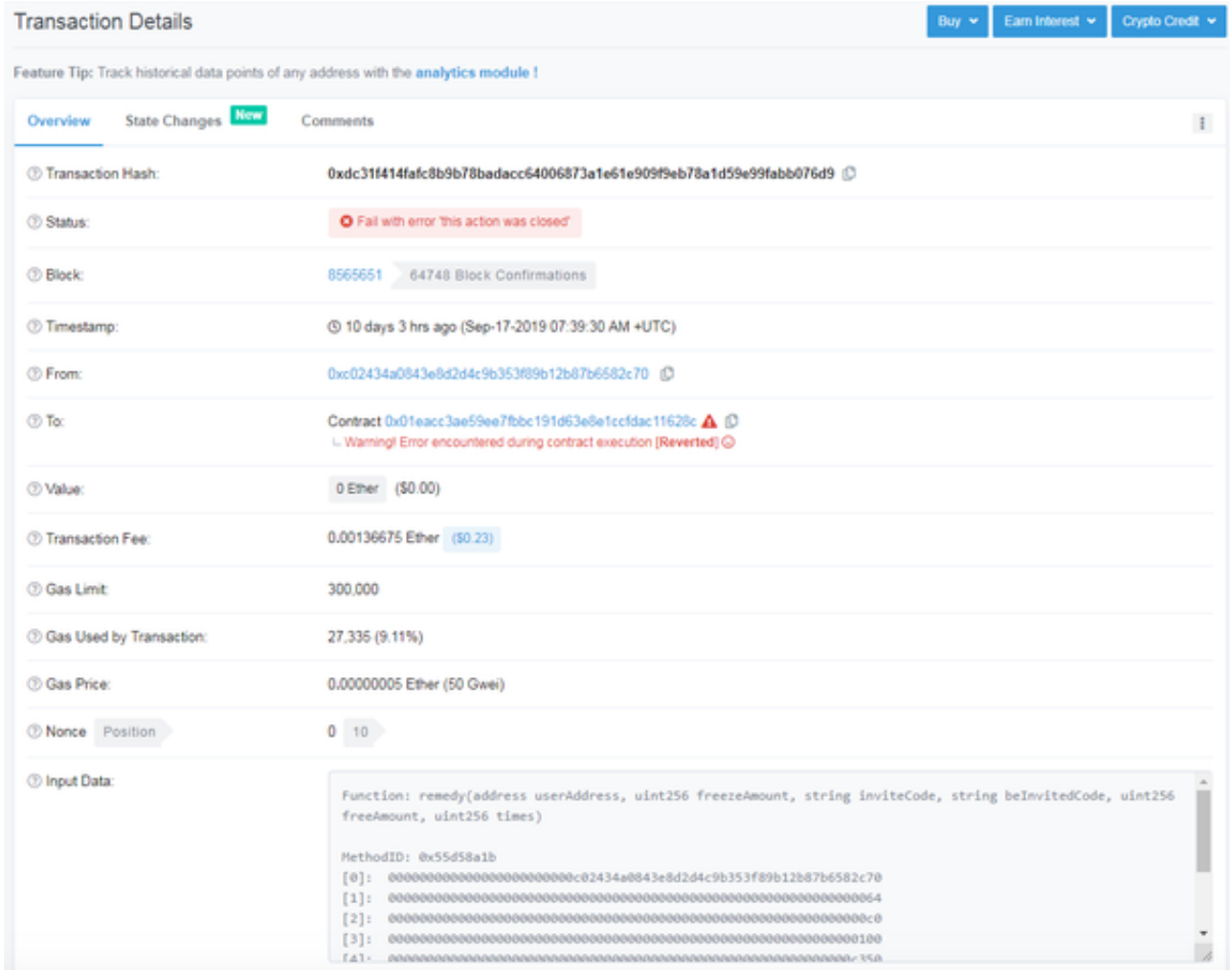

```
function remedy(address userAddress ,uint freezeAmount,string  inviteCode,string  beInvitedCode ,uint freeAmount,uint times) public {
  require(actStu == 0,"this action was closed");
  freezeAmount = freezeAmount * ethWei;
  freeAmount = freeAmount * ethWei;
  uint level =util.getlevel(freezeAmount);
  uint lineLevel = util.getLineLevel(freezeAmount + freeAmount);
  if(beginTime==1 && freezeAmount > 0){
      Invest memory invest = Invest(userAddress,freezeAmount,now, inviteCode, beInvitedCode ,1,1,times);
      invests.push(invest);
  }
```

通过链上记录，我们发现项目方已于2019年7月28日(合约上线第二天)通过closeAct()关闭了该接口。通过成都链安Beosin-AML系统分析项目方所有的交易记录，我

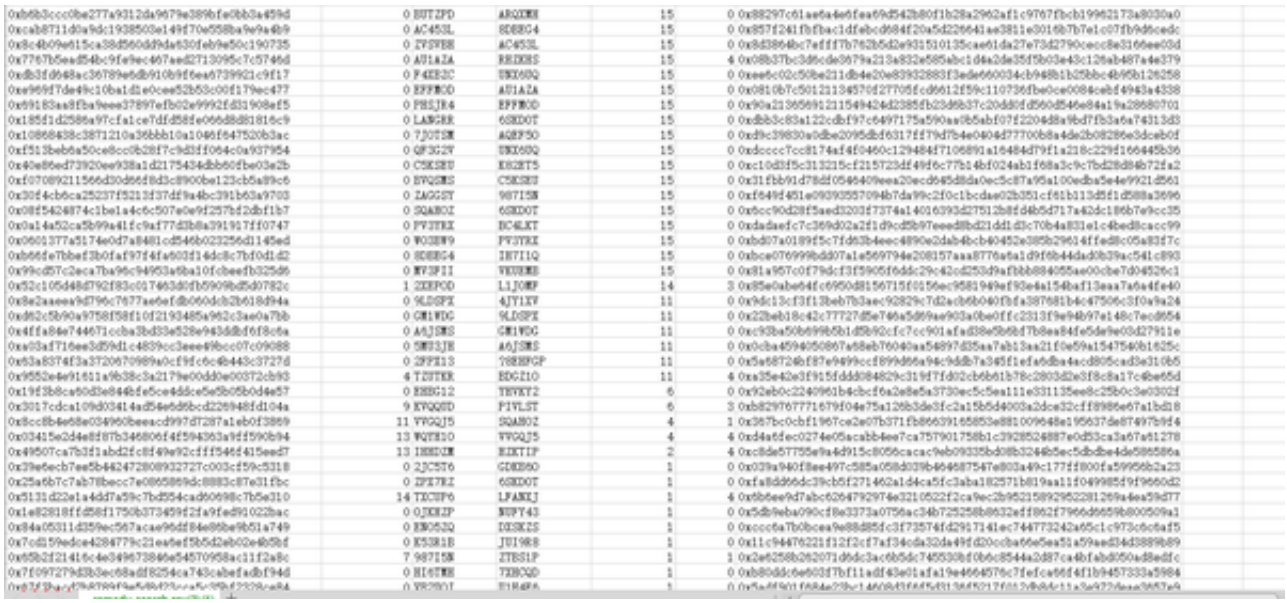
们进一步分析是否已经存在攻击者插入投注数据成功的情况。通过分析发现，该漏洞已被严重滥用。从十天前到现在为止，陆续有账户尝试调用remedy()接口来插入投注数据，不过由于该操作已被关闭，导致插入数据失败，可以看到插入金额都是几万ETH。

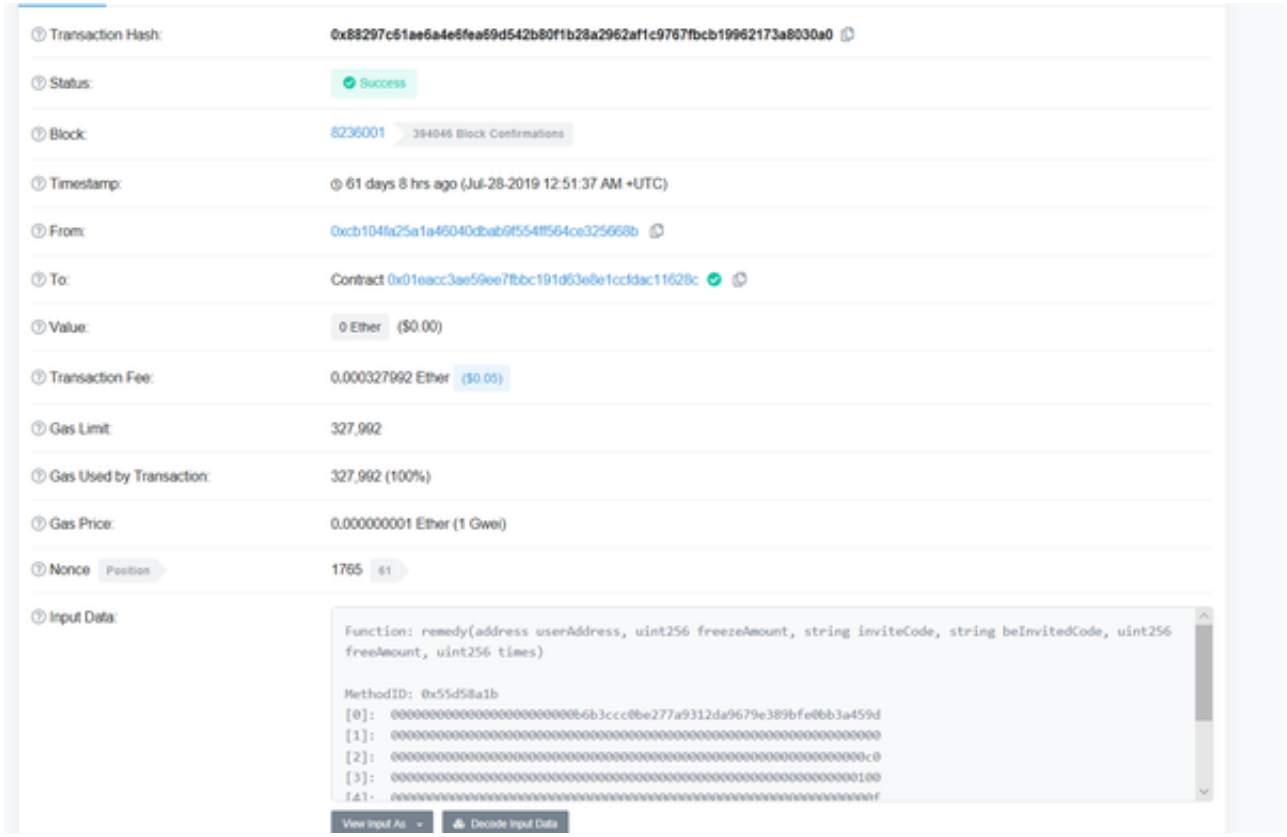
插入失败记录：



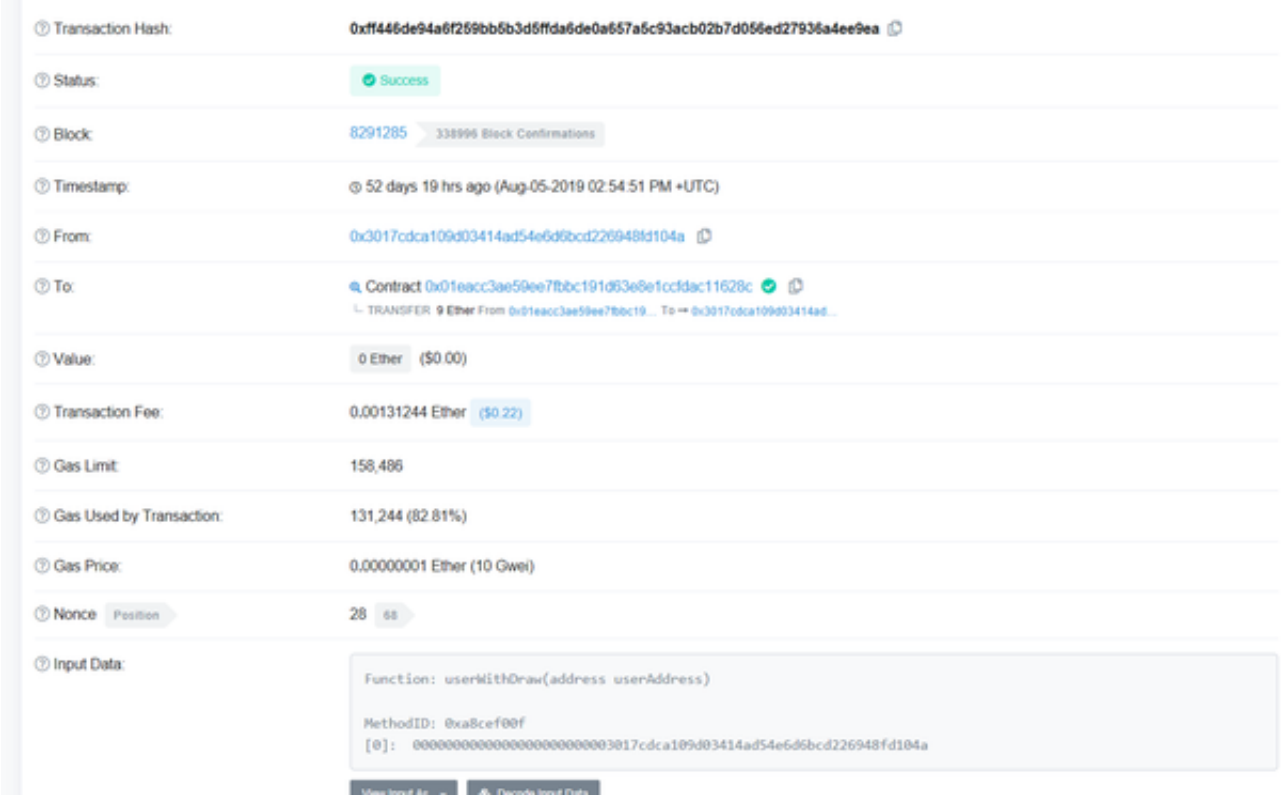


通过完整追溯，我们总共发现503条插入成功的交易记录(500个地址)，且插入日期都在项目方关闭接口之前。经统计，这503条交易全部由地址0xcb104fA25a1a46040DBaB9F554FF564CE325668b发起。





通过统计得出总共插入了5093个ETH，其中包括4711个冻结ETH，382个未冻结ETH。并且攻击者通过插入投注记录设置的500多个小号已经进行过提现操作。



通过进一步分析其合约部署情况发现，在项目方关闭actStu的前一天，也就是2019年7月27日，项目方刚刚部署FAIRWIN合约，在短短一天时间不到之内，项目合约之内便无中生有了5000多个ETH。
7月29日，以太坊浏览器显示合约进行了开源。