Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact

一、本文简介

本文是对以太坊中的旁氏骗局进行的一个探索性工作，其核心的内容在于构造了一个旁氏智能合约的数据集，以及对典型的旁氏智能合约模式进行了分析介绍，对合约交易等内容进行了描述性分析。这篇文章使我们之前分享文章的基础，更加详细的阐述了基于以太坊的智能合约和交易进行常规性数据分析的方法

二、重点内容总结

1. 数据集构造方法

数据分析的首要任务是构造出一个用于实践的数据集。本文中，作者详细阐述了数据集的构造方式：

（1） 从公开途径（etherscan.io 等）找到可以获取源码的所有智能合约，通过人工的方式去阅读源码、注释和相关网页，判断该合约是否是“旁氏骗局”

（2） 以字节码的编辑距离为指标，计算已经被认定是诈骗的智能合约和其他智能合约的相似度，找出潜在的旁氏骗局合约

（3） 通过网络搜索、论坛社区等地方，进行相应关键字查询，判断是否是骗局合约。

以上途径，作者最终收集到 137 个骗局合约和 54 个“可能”的旁氏合约。

2. 诈骗合约模式

旁氏骗局的典型特征在于“借新还旧”，也就是通过不断加入的后续投资者来偿还先前投资者的本金利息。在作者分析的智能合约中，模式相对简单，都是以简单的“游戏”为包装，只是在具体的偿还模式有一些区别：

（1） 阵列金字塔模式：使用数组记录投资人序列，按先后顺序进行资金返还。

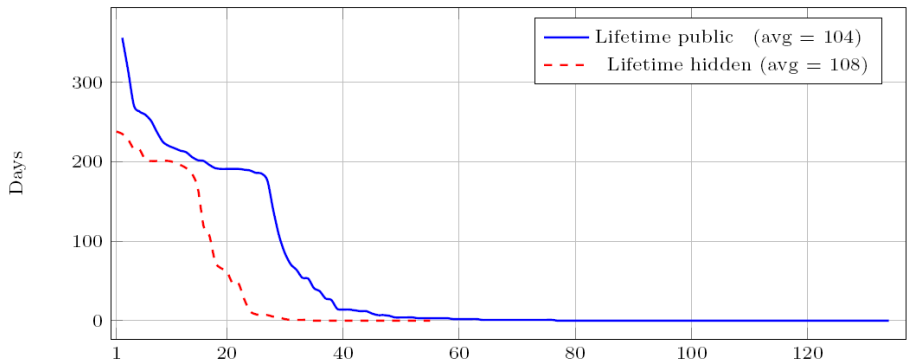
（2） 树形的金字塔模式：类似于传销模式，投资人需要指定自己的父节点，在父节点获得足够投资回报以后才轮到自己。

（3） 移接模式：新加入投资者必须支付金额和利息给之前的一个投资者，类似于“击鼓传花”的游戏。

（4） 瀑布模式：每次新入的资金，按照一定的比例规则分配给之前所有的投资者。

文中明确说道，绝大多数的庞氏骗局是第一种形式。

3. 诈骗合约与交易特征描述



我们重点看一下旁氏智能合约存在的生命周期（第一笔交易到最后一笔交易），75%旁氏骗局的生命周期都只有 0 天，很多庞氏骗局并没有多少人参与。

三、重点内容分析

从本文中，我们可以解释在之前的学习中，所存在的我们之前无法理解的一些问题。

1. 交易特征无法有效区分“旁氏合约”

如上图所示，75%以上的旁氏合约生命周期只有 0，意味着绝大多数的合约可能缺乏足够的交易用于分类。大多数的旁氏骗局太过于明显，其交易量并不大，让人难以获得足够的特征将其区分出来。

2. 字节码特征具备很强的分类能力

在作者对旁氏合约模式的分析说明中，谈到绝大多数的旁氏合约类似于阵列型的金字塔模式。并且大多数的智能合约集中出现在某个时期，他们的代码高度相似，因此字节码有着较强的分类能力。

3. 未来研究方向

文中作者统计出的智能合约都是一目了然的简单模式，但是现实世界中，绝大多数的旁氏骗局有隐藏在一个“包装之下”，比如博彩，游戏等。现阶段的任务中，缺少一种有效的手段，通过公开可见的数据就能够区分出表明正常而实际是骗局的智能合约的模型。