在区块链行业，地址追溯是一个相对敏感的话题。虽然在反洗钱，丢币事件以及追踪黑客时，我们可以通过追溯地址和链上转账行为获取更多信息，但由于区块链本身具有的匿名/加密属性，再加上各种反追踪和匿名技术的发展，地址追溯似乎成了一件“苦差事。”这次我们就以追踪近期Upbit交易所被盗的以太坊资金为例，也谈谈以太坊上的地址追溯方法和工具。

大体来说，我们可以将地址追溯拆分为以下四个步骤：

1. 大额转账指路

2. 关注小额资金流动

3. 分析交易所出入金地址

4. 对地址进行持续性的监控

一、大额转账

我们在收到某交易所/地址资金被盗后，通常会先拿到一个可疑地址，也就是黑客将盗来的资金转出的地址。这时我们可以先关注该地址的大额转账动向，从而确定黑客盗取资金后的第一步动作。

具体方法是通过区块链浏览器输入可疑地址，查询该地址的交易，从交易结果列表中寻找出大额的资金流向，按照新的流向打开每层地址，逐层深入查询，即可得出大额资金的流向图。

此处以Upbit交易所被盗的以太坊资金流动为例：

被盗以太坊从交易所流出的地址是0x5e032243d507c743b061ef021e2ec7fcc6d3ab89，而流入的黑客地址是0xa09871aeadf4994ca12f5c0b6056bbd1d343c029。依据下图步骤即可获取黑客的第一步行动：

1. 打开Tokenview区块浏览器，输入黑客地址0xa09871aeadf4994ca12f5c0b6056bbd1d343c029，点击“搜索”

截止本篇文章截稿，可以看到该地址已进行114笔交易，我们可以先查看该地址的前2笔交易。

第一笔交易是来自上面提到的0x5e03开头的Upbit交易所地址，说明该黑客地址是新的链上生成地址，转出金额为342000枚ETH。

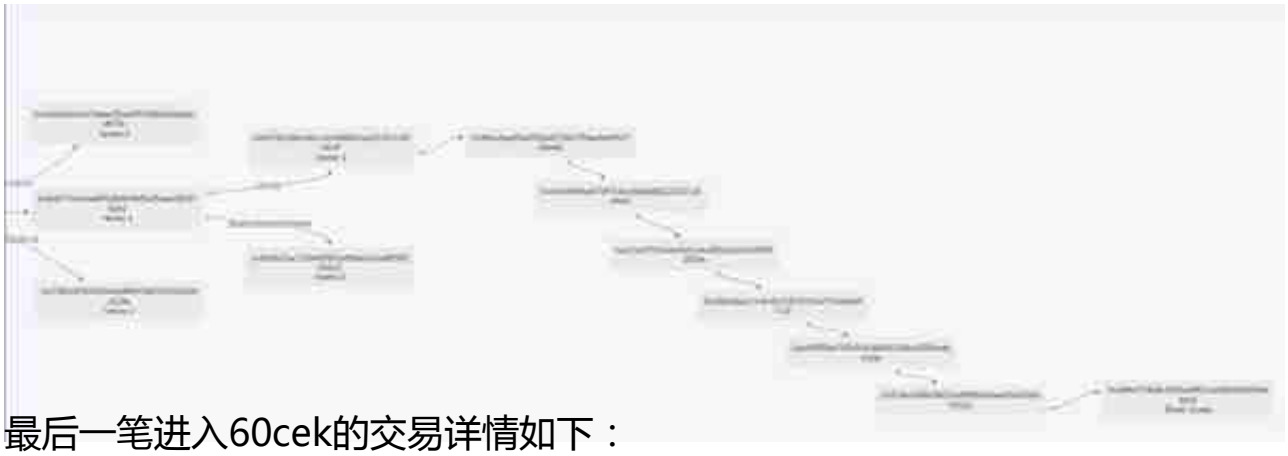
接下来观察后续交易中的转出交易，从第一笔转出交易开始的后续转出交易，他的转出地址即会是第一层的分散地址。

依次观察到从0xa098转出111000枚ETH给地址0x9a207194cbed9f229694fdf5a28caab59157920d，

转出111010枚ETH给地址0x3408edca2d47ddaa783a3563d991b8ddebcd973b，

转出120280.16枚ETH给地址0xc7d64e6509333a3b68f6fc09d7d19404bfdd229a；

至此该地址中绝大部分以太坊已被转出，我们就可以重点监控以上三个地址，并分析随后的资金流动，从而得出更进一步的资金流向：



最后一笔进入60cek的交易详情如下：

如果Binance拥有相关的KYC记录，我们即可确定一个详细的用户信息。当然，这种想法往往过于直接，黑客既然选择转入交易所账户，必然会考虑到自身信息的匿名性，其KYC信息大概率也就不会是真实的了。

四、地址持续监控

一般来说，黑客不会在短期内将盗来的资金转到交易所。从盗得资金到完全出手，整个过程可能会持续半年甚至更长的时间。这也给我们的监测带来很多困难。这时候如果可以订阅某个地址的余额变动情况，在第一时间获取相关信息，那么监测就会变得容易很多。这里我们主要介绍Tokenview开发的【地址监控】功能。

打开微信搜索并关注“Tokenvew区块链浏览器“，在菜单栏点击”数据监控“，随后点击”地址监控“，把需要监控的地址输入随后的页面，选择阈值即可。监控成功后，一旦该地址的余额变动符合监控的范围，公众号就会发送余额变动通知。