PeckShield

数字资产交易所合规性研究报告

2020上半年度

杭州派盾信安科技有限公司

2020.07

目录

0. 研究背景综述

2020年以来，在全球新冠肺炎疫情的影响下，全球经济开启了数字化转型的步伐。互联网科技巨头 Facebook 牵头发起的 Libra 项目试图做新一代的全球数字货币，而全球各国央行则纷纷推出国家层面的数字货币项目，包括，中国人民银行发起的 DCEP、欧盟发起的 CBDC，以及美国即将发行的数字美元等等，都在用主权货币的数字化为即将到来的数字经济社会筑底。我国更是提出了以 5G、大数据、云计算、互联网、人工智能、区块链等为代表的数字新基建，以构筑结构性力量，助力数字经济发展。

然而，在数字经济如火如荼的今天，原本因经济全球化而猖獗的跨国犯罪和贪污腐败问题，随着比特币等数字加密货币的普及而更加猖獗，严重危害了全球经济和金融秩序。洗钱这一黑色产业也已经成为世界经济血脉上的毒瘤，严重危害了世界经济秩序的健康发展。

虽然，各国相继出台政策和法律严控洗钱犯罪行为，但更多停留在传统金融领域，由于暗网和大部分数字资产交易所目前尚处于监管盲区，不少不法分子于是通过匿名性更好的暗网和数字资产交易所实施洗钱和犯罪行为，如同找到了庇护所，更加的猖獗和为非作歹。

过去半年，我们统计发现，全球不同国家的警方都有参与处理涉及到数字货币洗钱相关的刑侦案件。

据 Cointelegraph 消息，英国莱斯特郡警官 Phil Ariss 表示，04月18日，当局逮捕暗网贩毒男子 Paul Johnson，并查获了约37.5万美元加密资产。随着越来越多的罪犯转向使用比特币和其他金融隐私手段，执法部门必须了解比特币。而在过去两年中，英国全国范围内共发生了562起与比特币相关的诈骗事件。

据 itnews 消息，05月14日，悉尼一女子因涉嫌经营非法数字货币交易而被指控。该女子被新南威尔士州网络犯罪调查局逮捕，同时被没收60,000澳元的现金和价值超过73,000澳元的比特币。警方将在法庭上指控该女子经营着一个非法的在线洗钱集团将现金兑换成加密货币。网络犯罪调查局侦探总监称，这是首次逮捕该州不合规的数字货币提供商，并且可能是澳大利亚首创。

据新快报消息，近日，广州白云警方在强化打击电信网络诈骗犯罪过程中打掉了首个利用数字货币为电信网络诈骗“洗钱”的团伙，嫌疑人落网后，向警方交代了他们“洗钱”的过程：在账户收到诈骗犯罪分子转入的钱款后，他们会在网上以私下交易的方式，买卖数字货币，并从中抽取一定比例的佣金。大约半年前，嫌疑人开始通过数字货币为诈骗团伙“洗钱”，至今已获利 30 余万元。

据每日经济新闻消息，05月13日，济南市公安局章丘分局反诈咨询热线接到冀先生报警电话，称自己在网上购买比特币的时候被骗18.99万元，民警开展相关资金流向调查，在受害人及时提供准确信息和金融方的密切配合下，3 小 时后，民警成功将冀先生的被骗款进行了止付。 这是一起境外犯罪分子利用市民的银行卡洗钱的典型案例，犯罪分子通过网站链接出售比特币，随后让受害人将钱打到市民银行卡中，再通过非法手段撤回比特币，以此来诈骗钱财。

在此背景下，全球范围内的政府和金融监管机构开始加大力度对流入暗网的资产进行技术侦查和监控，而对数字资产交易所也展开了有序合规化监管，以此来制约违法分子进行洗钱操作。

2019年6月，FATF (Financial Action Task Force) 发布了 INR15 (Interpretive Note to Recommendation 15)，进一步明确了对数字资产的监管细节，并给出了具体实施时间表。根据 INR15 的规定，各国和 VASP 必须在一年以内即2020年6月以前，开始执行 FATF 的监管要求。

- 要求 VASP（虚拟资产服务提供商）注册，进行评估并采取有效行动，以减轻其洗钱和恐怖主义融资风险；
- 要求 VASP 提供 KYC（发起人、受益人的账号、地址、身份ID）信息
- 要求 VASP 向监管报备 1,000 美元以上的交易；
- 各国应确保能管理或降低使用交易混合服务提供商（mixers）、滚动交易提供商（tumbler）或是类似工具的来转移风险；
- FATF 建议，各国应考虑使用开源信息和网络抓取工具来识别未经注册或未经许可的加密货币交易业务。

INR15 最核心的一项要求就是 “Travel Rule”, 它要求所有超过 1,000 美元/欧元的交易，必须把交易的发起人信息，受益人信息，和交易金额报备给 FATF。

这就意味着，原先并不透明对外的数字资产交易所要把交易信息向 FATF 报备，对于当中混入的非法或被污染交易，FATF 有可能会随时介入监管，这样一来势必会打破现在区块链世界不受监管的局面，对整个区块链生态的进一步发展产生关键性影响。

PeckShield 安全团队分析认为，这项规定对分布于全球的数字资产交易所而言是一项巨大的挑战。一方面意味着，数字资产交易所要在今年 6 月以前建立起完整的 KYC 和大额交易监控和汇报机制和 KYT 交易信息的赃款排查机制，以及相关地址的溯源等技术难题。

PeckShield 经过持续一年以上的链上和链下数据搜集、核对、验证，分析，截至目前共计掌握了近1亿个链上地址和标签，其中仅交易所相关的地址标签就超过了5,000万，包括 BTC、ETH 网络以及上面运行的 USDT 等主要数字资产。

经 PeckShield 安全团队深入挖掘、洞察这些地址标签数据发现：

- 据 PeckShield 数据显示，截至2020年06月30日，全球数字资产交易所资产余额排行榜（以 BTC+ETH+USDT 资产折算为美元计）为：Coinbase 交易所的资产总量为111亿美元，排行第一位，Huobi 交易所资产总量为57.9亿美元，排行第二位，Binance 交易所资产总量34.5亿美元，排行第三位，Bitfinex 资产总量 29.9 亿美元，排行第四位，而 OKEx 资产总量为 25.2 亿美元排行第五位, BitMEX, kraken, Germini, mtGox, bittrex 等分别排行第六到第十位。

- 据 PeckShield 旗下数字资产追踪平台 CoinHolmes 数据显示，包括黑客攻击、资金盘、暗网、赌博等在内的我们已标记为高风险的地址，在过去6个月共计流入数字资产交易所13,927笔高风险资产，合计14.7万个 BTC，时价折合超过14亿美元，已经是一笔非常惊人的资产。我们把流入赃款最多的交易所做了排名发现，排名前十位的交易所分别为：Huobi、Binance、OKEx、ZB、Gate.io、BitMEX、Luno、HaoBTC、Bithumb、和Coinbase。

- 据 PeckShield 数据显示，截至2020年06月30日，我们已监控高危风险地址中，流入黑名单地址的资金有16.2亿美元，流入混币服务商的资金有15.9亿美元，特别要强调的是，经混币服务的资金如同石沉大海，大部分很可能已经被成功洗钱，很难有再被技术性追踪的可能性。常见的混币服务商有：Bitlaunder, HelixMixer, Samourai, Wasabi, BitcoinFog 等；中心化倒卖机构有：ChangeNow、CoinSwitch 等。

除了以上三个数据维度，接下来的报告内容中，我们将围绕交易所地址标签对目前交易所的合规性情况做一个数据画像，包括：交易所过去半年的进账出账情况、交易所之间资金互相转移情况、未受监管的交易所资产情况等等。透过数据分析我们看出目前数字资产交易所面临的合规性挑战。

此外，针对数字资产交易所存在的合规性压力，PeckShield 安全团队研发出了一套服务工具，其不仅可以帮助数字资产交易所对黑名单地址进行有效监控，对目标地址进行风险评分，还能对每笔交易所进出账做 KYT 实时监控追踪，弥补 KYC 信息的不足。最终，帮助交易所拥抱监管避开赃款陷阱，联同网警及生态合作伙伴多方力量，帮助受害者封堵、阻截、寻回被盗或诈骗资产。

注：本报告所指的交易所合规性主要聚焦于AML反洗钱领域，其他合规性问题诸如：合规牌照、注册地法规等问题尚不在本报告讨论范围之内。且以下报告涉及到的数据和排名，均基于 PeckShield 现有地址标签库的资金流向所统计，若有疑问可联系我们。

1. 研究方法和工具

1.1 研究方法论

PeckShield 研究团队通过采集区块链网络链上和链下的公开原始数据，并基于此展开了专业、系统、深入的研究和分析。过去一年多时间内，PeckShield 积累了大量头部公链的交易和日志等链上数据信息，生成了海量的地址标签，构建了丰富全面的数据库，并开发了专业的数据分析工具。

我们的工具库可以分为如下七个主要部分：

1）各大公链的交易级数据库。通过搭建全节点和对公链原生数据存储文件的解析，我们生成了各大公链的交易级数据库，包括比特币，以太坊，EOS，和波场等公链，并实时进行同步更新；

2）海量的地址标签。由于区块链网络本身的匿名特性，绝大部分的链上地址背后所对应的用户身份信息是未知的。我们通过收集链下信息，并分析其链上交易的关联性，再融合机器学习算法，生成了总数近1亿个地址标签库，基于此展开后续一系列的数字资产汇总和溯源分析；

3）数据分析和可视化软件。我们自主开发了数据分析和可视化工具，能把复杂的区块链资金流向可视化，从成千上万的交易和地址中制作出清晰的可视化图表，每当输入一笔交易，系统便可自动进行追踪，并自动展示出层级结构和主体信息。例如各大数字资产交易所的资产余额及相互间转账交易频次和总额；欺诈安全事件中赃款的转移路径及最终流向等。

4）交易所地址结构分析。交易所的地址主要分三类：冷钱包、热钱包和用户充提地址。冷钱包是交易所用来固定储存资产的地方，额度大，输入输出频次低且单次额度比较大；热钱包是交易所用来满足用户提币所需的动态资金，热钱包是用户充提地址和冷钱包地址的中转站，热钱包地址不多，但其输入输出的资金额度小但频次较高；充提地址是直接连接用户的地址，一个用户会有多个不同资产对应的充币地址，充提地址占交易所地址的大多数，额度不大但交易频次比较高。

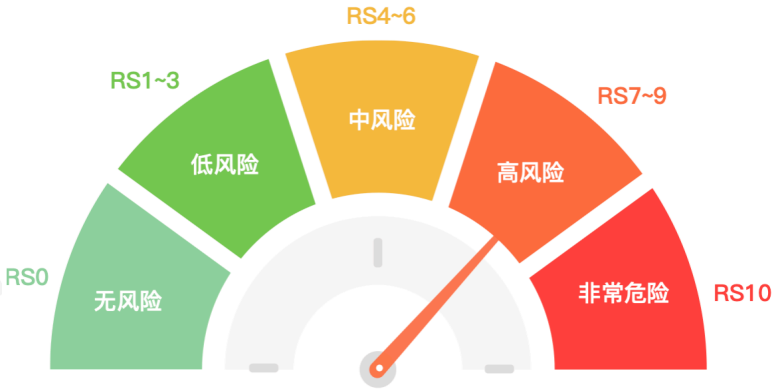
5）Common Spending：我们通过分析发现，如果一笔 (BTC) 交易同时有多个输入地址，那么就可以认定这些输入地址是由同一个实体控制。我们可以通过已有标签的地址不断辐射，挖掘更多的关联新地址，这会带来指数级的数据增长。

6）Cerberus 工具：为了提高挖掘地址标签的效率，我们专门开发了 Cerberus 工具，利用该工具可以从大数据库中批量提取关联的交易信息，然后结合内部收集的其他标签数据做内部过滤统计，再结合图数据库分析并结果并可视化展示资金流向。特别说明的是，利用该工具向前向后可秒级触达最高 100 层的全链路交易信息，能快速锁定和目标地址存在弱关联的交易并提取出来，比如黑客洗钱地址、交易所特征地址等。

7）CoinHolmes 系列服务：CoinHolmes 基于已有的标签数据库一整套包括黑名单地址监控、地址风险分评估，关联交易可视化路径分析等等。该系统会开放 API 给第三方平台，并且可在日常运营过程中直接输入查询地址，查询地址风险分并结合第三方平台已有的风控平台实施封堵，熔断等应急响应举措。

如上图，我们研发了一套反洗钱风险评估体系，通过分析地址的风险和交易的特征以及相关地址的风险信息，对交易和地址进行风险评估。

风险评估引擎实时动态评估，给出每笔交易和每个地址的风险评级。我们建立一套「五档十级」的风险评估体系，帮助 VASP 区分不同的交易风险，进而制定出合理安全的风控体系。



1.2 免责声明

本报告内容基于我们对区块链行业的理解以及多项研究实践，但由于区块链的匿名特性，我们在此并不能保证所有数据的绝对准确性，PeckShield 也不能对其中的错误、疏漏、或使用本报告引起的损失承担责任。

同时，PeckShield 并非投资顾问、经纪人、或交易员，我们也不拥有该研究领域的非公开信息。所以，本报告不作为投资建议或其他分析的根据。

2. 交易所地址标签概览

2.1 已统计交易所地址概述

截至2020年06月30日，PeckShield 安全团队共计搜集、梳理了覆盖 BTC、ETH、EOS 三条主链总计近1亿个地址标签，主要包含**交易所和暗网、资金盘、混币服务商地址、跨链中心化倒卖机构以及涉及非法攻击的黑客地址等一系列高风险地址。**

- **1）交易所地址：**由于大部分数字资产交易所目前尚是中心化管理模式，交易所相关的充币地址、冷钱包地址、热钱包地址等，由于交易所只公开了一小部分地址，大部分地址是未公开的，因此我们需要根据链上数据特征，基于少量冲提地址进行扩充抽调，挖掘出藏在背后的交易所地址。

- **2）暗网地址：**在暗网市场，很多不法分子都以比特币、门罗币等数字资产作为结算，因此分布着大量的暗网收款地址，其地址所有人多为黑客或一些参与非法犯罪交易的主体所为。

- **3）混币服务商地址：**严格来讲比特币的链上地址不管拆分多少层，都能追溯到最终的源头及流向路径情况，因此混币服务商就成了洗钱的必经路径。混币服务商利用比特币 多个输入输出 UTXO 的特性，同时输入很多洗钱地址，然后在找零环节混入其他正常交易进而将资金流向秩序打乱。比如：BitLaunder, HelixMixer, sideshift.ai 等服务商。

- **4）跨链中心化倒卖机构地址：**由于大部分中心化交易所存在严格的 KYC 审查机制，一些黑客地址被盯上后想很快把资金清洗干净面临着很大被交易所封堵的风险。于是一部分黑客会选择一些免 KYC 的中心化倒卖机构进行洗钱操作。比如：Changenow、CoinSwitch 等平台。

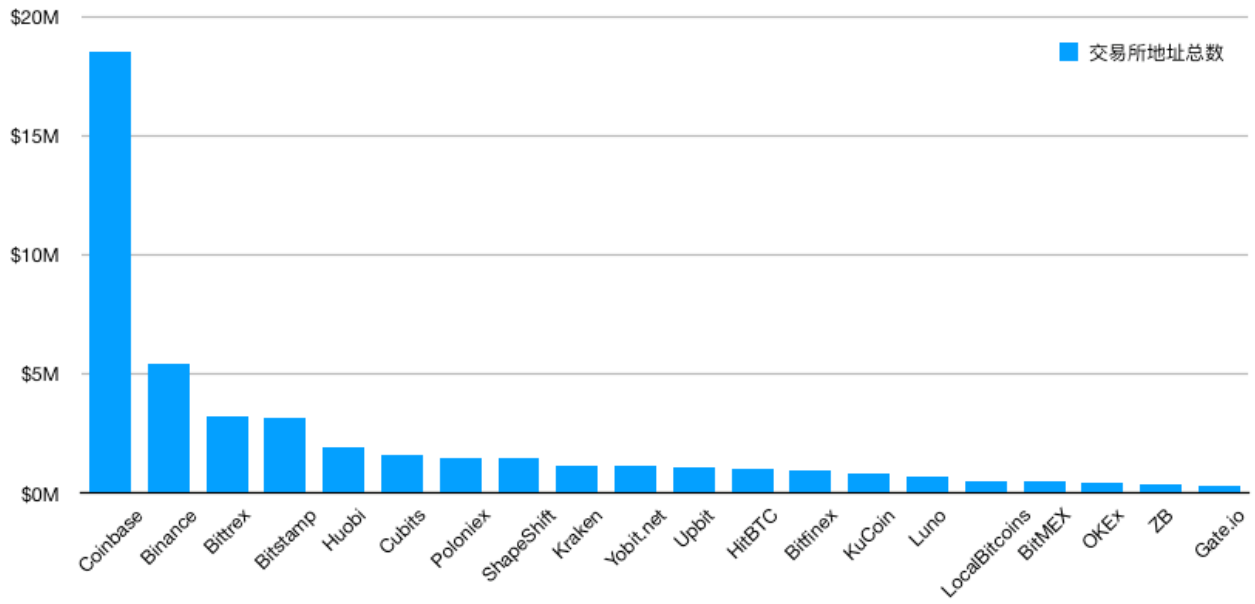
- **5）高风险黑客地址：**我们统计了包含利用技术漏洞攻击、利用理财陷阱诈骗、利用要害信息勒索以及大量博彩赌博相关的地址标签，这些我们统一概括为高风险地址。以利用技术漏洞攻击的黑客地址为例，黑客攻击成

功后会进行周密的分散洗钱操作，过程中会产生大量的关联地址。这些地址的每一次链上异动背后都存在黑客用来洗钱的可能。

- 6）**资金盘地址：**过去一年内，我们已经监控包括 TokenStore、PlusToken 等在内的数十个资金盘相关地址，这些地址为了掩人耳目往往进行了密集的多账号转移和复杂的洗钱操作。

- 7）**赌博平台地址：**我们监控到存在一些专门从事非法赌博的平台，当中存在一些洗钱行为。

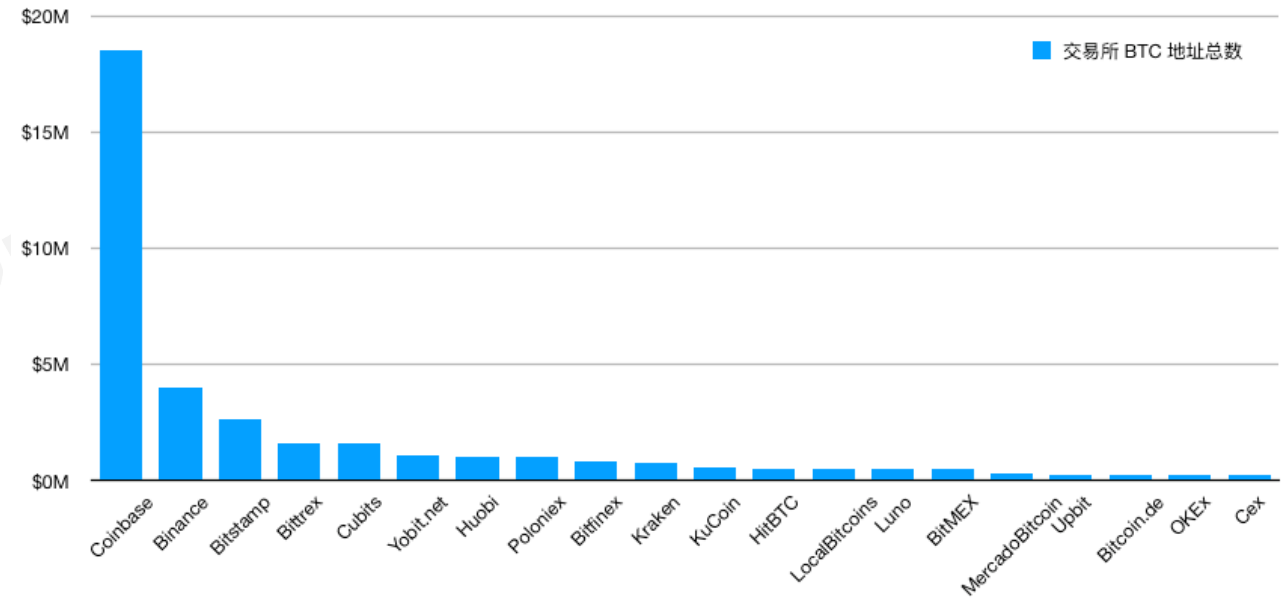
这近1亿个地址标签中，包含 BTC 地址超6,000万+，ETH 地址3,000万+，其中交易所地址标签将近5,300万个，占比75%以上，共计覆盖包括：Huobi、Binance、OKEx、Coinbase、ZB、Bitfinex、Bitstamp、Poloniex、Bithumb、Gate.io、Upbit、KuCoin 等头部交易所在内的数百个交易所。



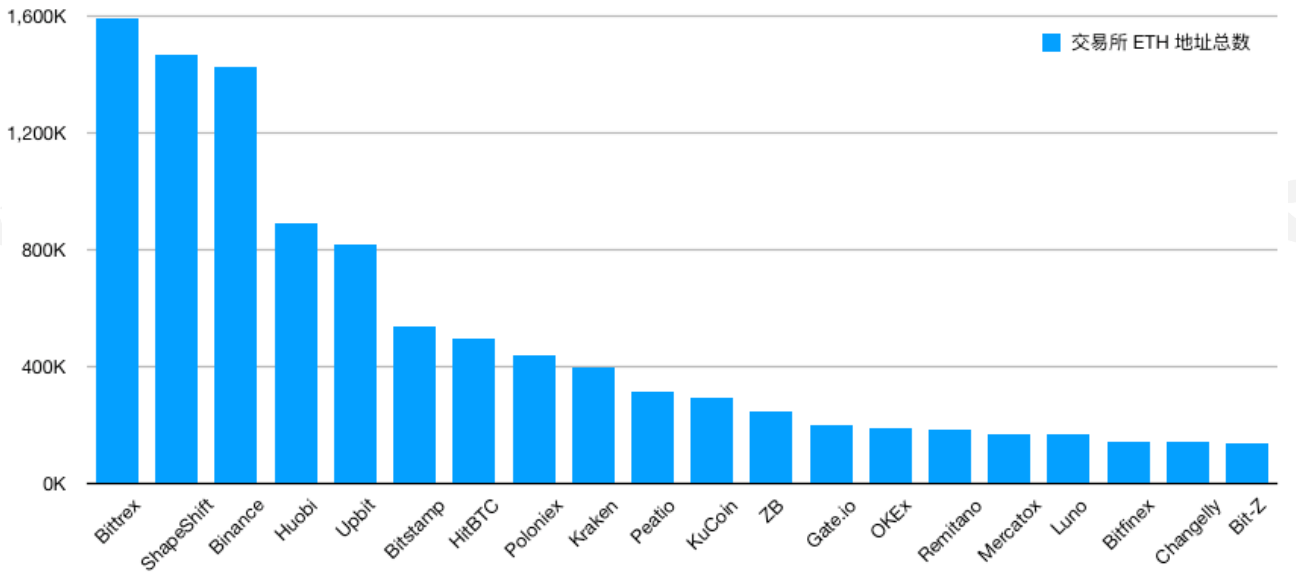
（图一：交易所地址总数排行榜）

如图一所示，我们对已知的全部地址标签进行了归类分析发现（该统计主要以 BTC 和 ETH 为主），我们目前已知地址最多的数字资产交易所排行前五位分别为：**Coinbase 排行第一位，共有 1,852 万个地址、Binance 排行第二位，共有 542 万个地址、Bittrex 排行第三位 共有 323 万个地址、Bitstamp 排行第四位，共计 319 万个地址、Huobi 排行第五位，共计 193 万个地址。**需要说明的是，我们已掌握的链上地址，只是我们利用技术手段挖掘出的的地址情

况，这些地址量级不完全等同于交易所的实际掌握地址，只是在交易所地址尚未透明的背景下，给出的一个参考性的展示。



（图二：交易所 BTC 地址排行榜）



（图三：交易所 ETH 地址排行榜）

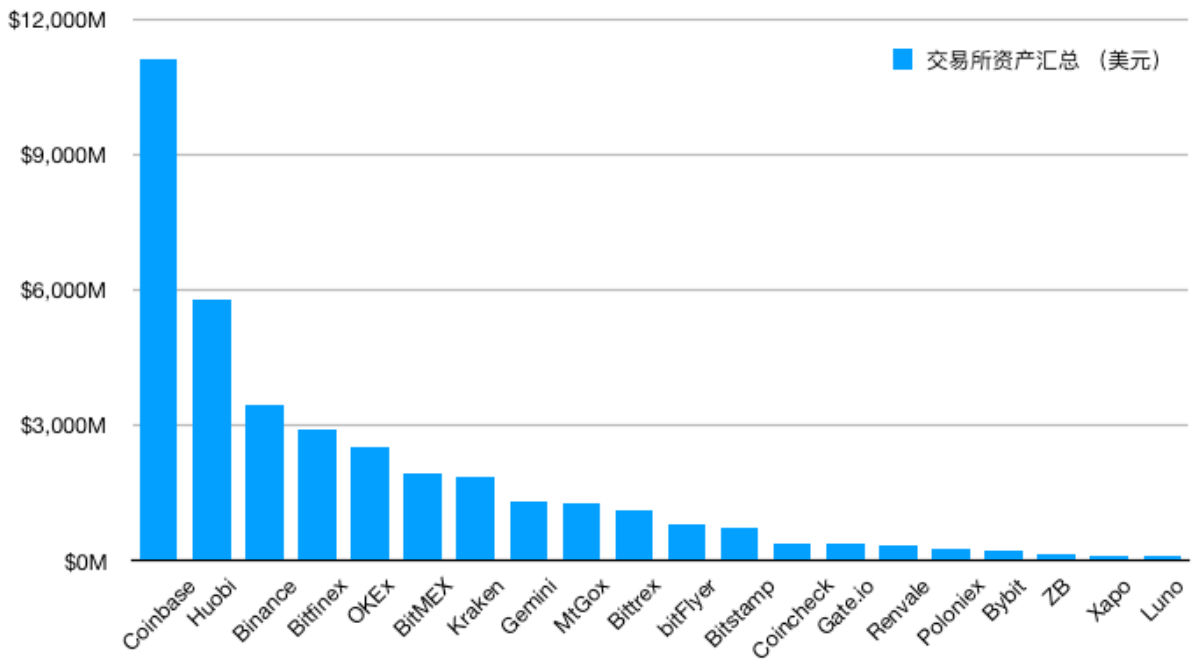
如图二、图三所示，我们对各个交易所拥有的 BTC 和 ETH 地址标签进行了排行。

BTC 方面：其中 Coinbase 交易所拥有个 1,851 万地址，排名第一位，Binance 交易所拥有地址 400 万个，排名第二位；排名第三位的是 Bitstamp 交易所，拥有地址 265 万个；

ETH 方面：Bittrex 地址 拥有 158 万个，排行第一位，ShapeShift 拥有地址 146 万个，排行第二位，Binance 拥有地址 142 万个，排行第三位。

需要说明的是，查找交易所地址过程具有一定的复杂性，**我们先要搜集一部分充提地址作为种子地址，然后再链上利用 Cerberus 工具，进行大批量关联性的地址抓取、入库，与此同时，我们同时会对所挖掘的地址进行必要的链下验证确认，以确保地址的准确性。**

2.2 交易所地址余额情况



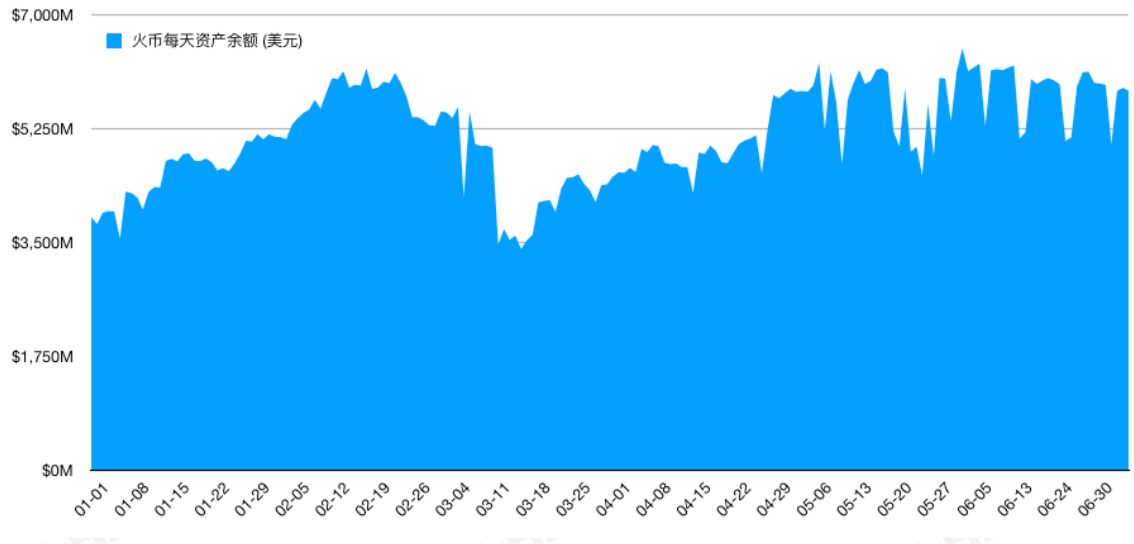
（图四：已统计交易所地址余额排行榜）

我们对已监控的不同交易所所属不同资产（主要为 BTC，ETH，和 USDT）进行汇总以美元统计发现：Coinbase 交易所的资产总量为111亿美元，排行第一位，Huobi 交易所资产总量为 57.9 亿美元，排行第二位，Binance 交易所资产总量 34.5亿美元，排行第三位，Bitfinex 资产总量29.9亿美元，排行第四位，而 OKEx 资产总量为25.2亿美元排行第五位。

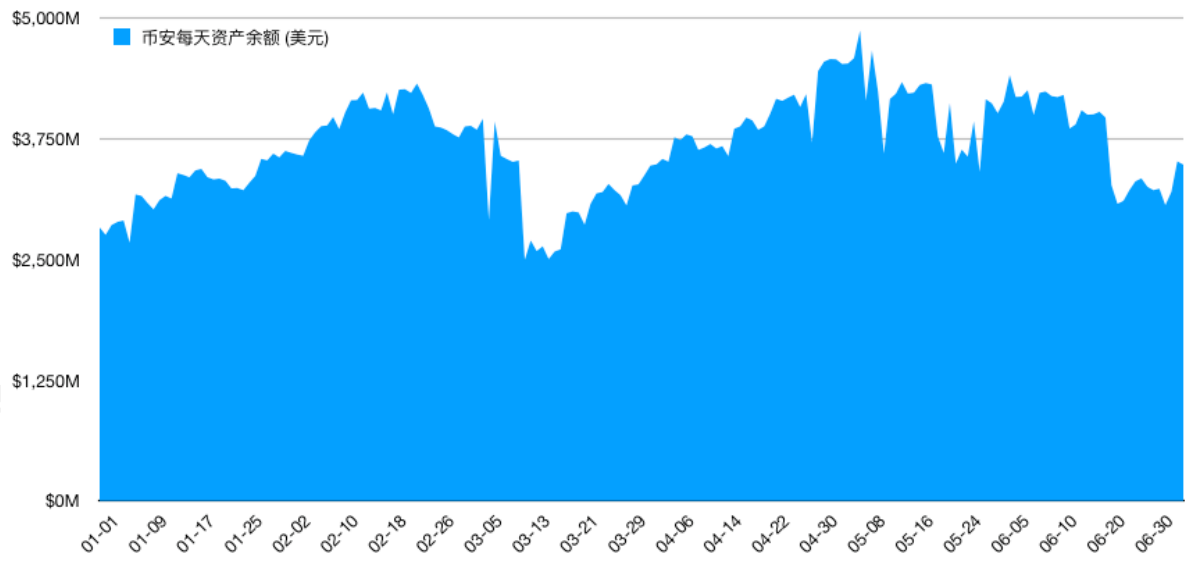
name	total_balance
Coinbase	11,111,526,779.57
Huobi	5,793,681,007.38
Binance	3,458,458,160.16
Bitfinex	2,909,315,774.75
OKEx	2,527,488,840.79
BitMEX	1,933,295,126.63
Kraken	1,848,664,431.63
Gemini	1,321,485,864.12
MtGox	1,268,596,924
Bittrex	1,142,921,425.15

（图五：交易所地址余额列表－前十位）

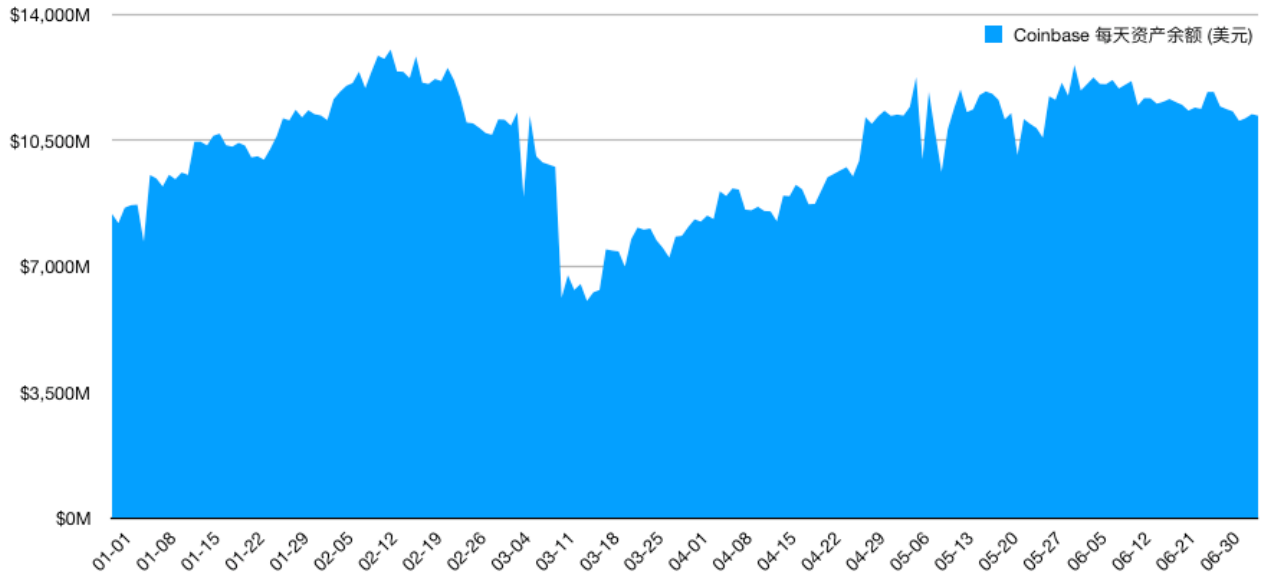
为了更直观地看到交易所的资产余额变动情况，我们单又独例举了火币、币安和 Coinbase 三家头部交易所的资产余额情况，发现这三家交易所的资产余额走势保持相对平稳，偶尔出现较大的波动基本和行业波动有直接关系，如图六、图七、图八所示。



（图六：2020上半年火币交易所资产余额情况）



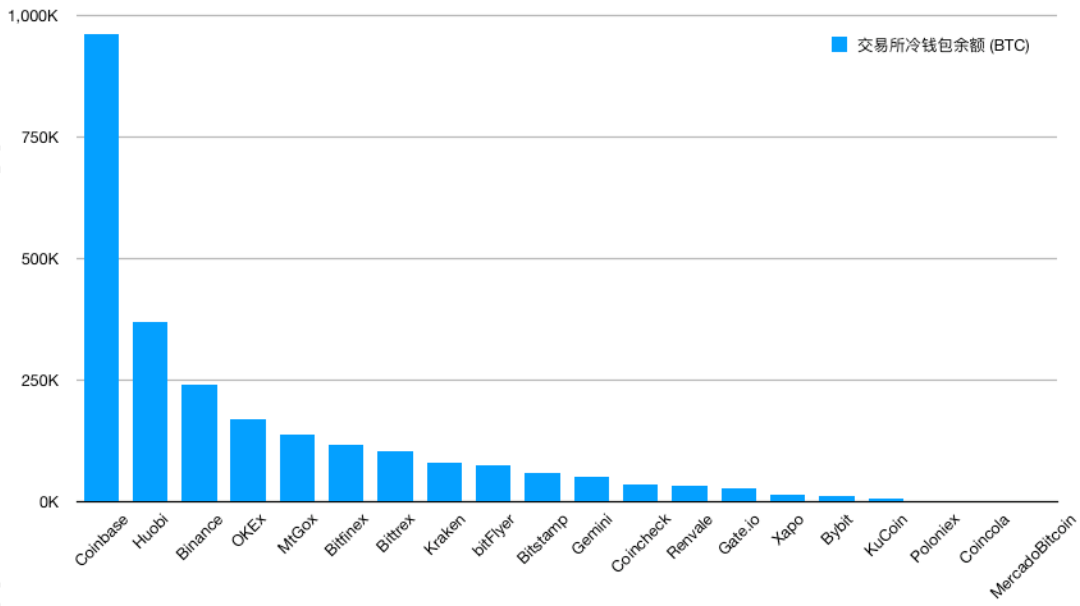
(图七：2020上半年币安交易所资产余额情况)



（图八：2020上半年 Coinbase 交易所资产余额情况）

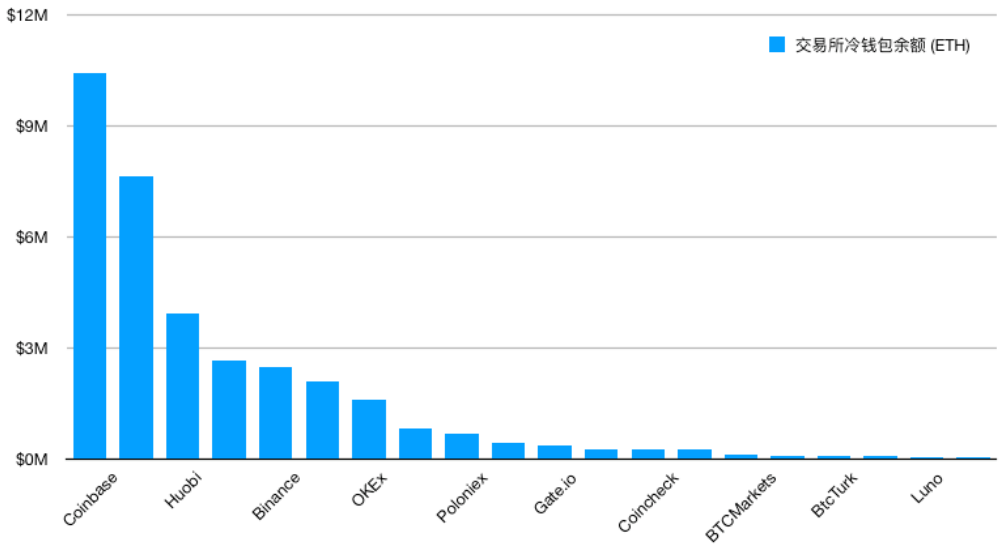
2.2.1 交易所地址冷热钱包分布情况

正如前文中所说，我们从各个主链挖掘出大量的交易所地址，再根据这些地址的交易频次和交易数额等交易特性分别梳理出各个交易所对应的冷钱包、热钱包、充币地址等。



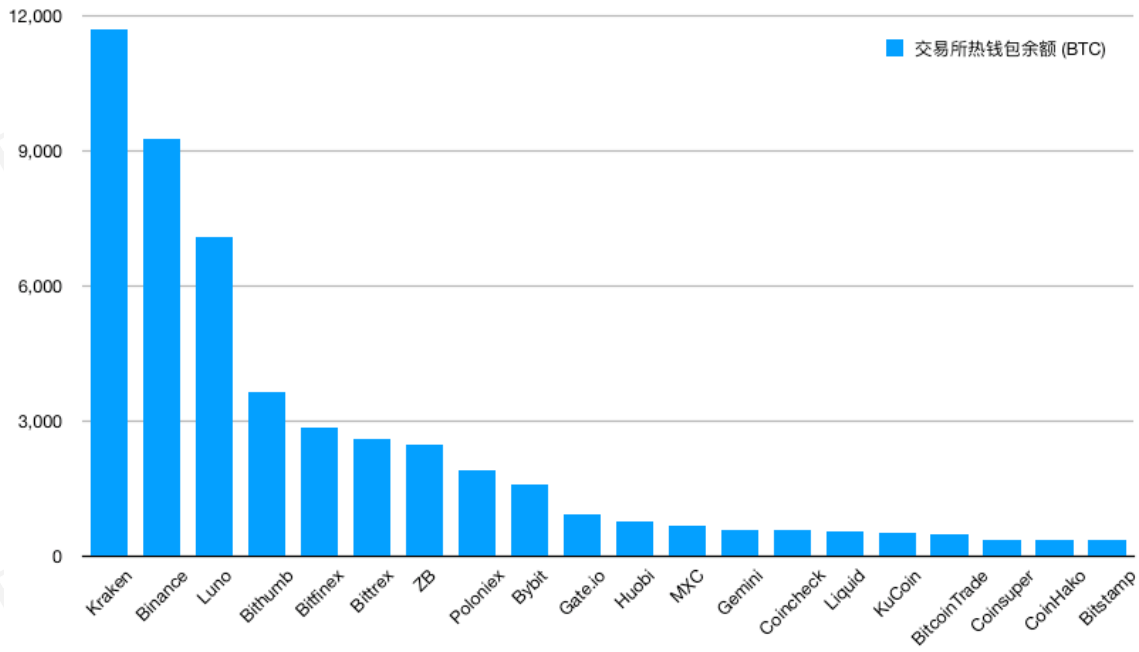
（图九：交易所冷钱包情况——BTC资产）

图九为交易所的 BTC 冷钱包分布情况，地址余额最大的为 Coinbase 拥有 96.2 万个 BTC，火币次之拥有 36.9 万个 BTC，而币安紧随火币之后拥有 23.8 万个 BTC。



（图十：交易所冷钱包情况——ETH资产）

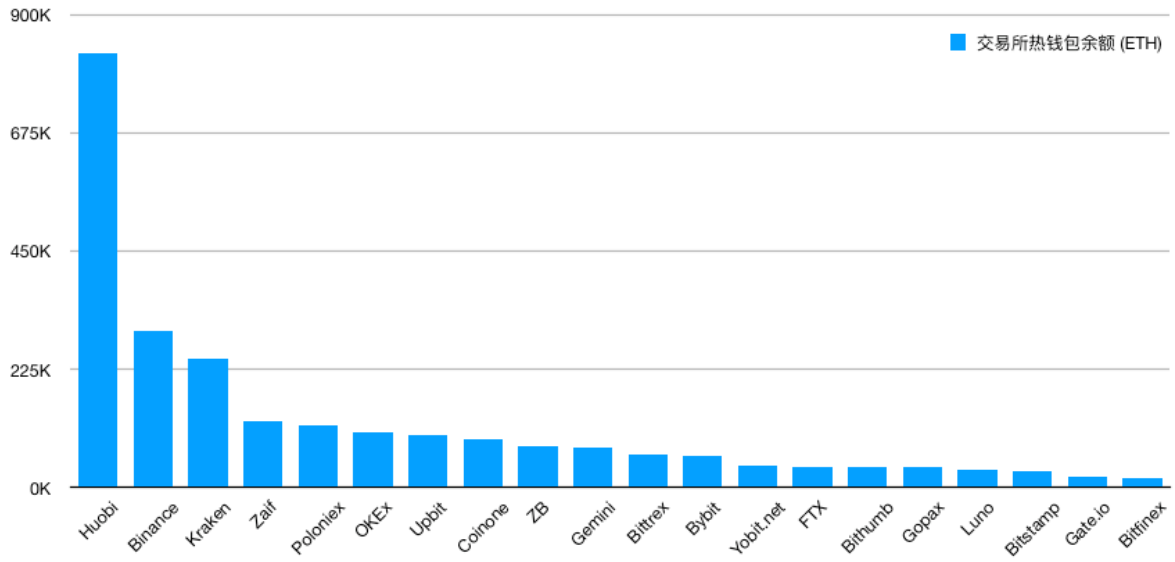
如图十所示，交易所的冷钱包 ETH 资产排行情况，Coinbase 拥有1,044万个 ETH 排行第一位，Bitfinex 拥有764万个 ETH 排行第二位，排名第三位的是火币，拥有394万个 ETH。



（图十一: 交易所热钱包资产情况——BTC资产）

如图十一所示，交易所的热钱包 BTC 资产排行情况，Kraken 拥有11,708个 BTC 排行第一位，币安拥有9,255个 BTC 排行第二位，排名第三位的是 Luno，拥有7,072个 BTC。

如图十二所示，交易所热钱包 ETH 资产排行榜中，Huobi 拥有82.6万个 ETH 排行第一位，币安拥有29.8万个 ETH 排行第二位，排行个第三位的是 Kraken 拥有24.6万个 ETH。

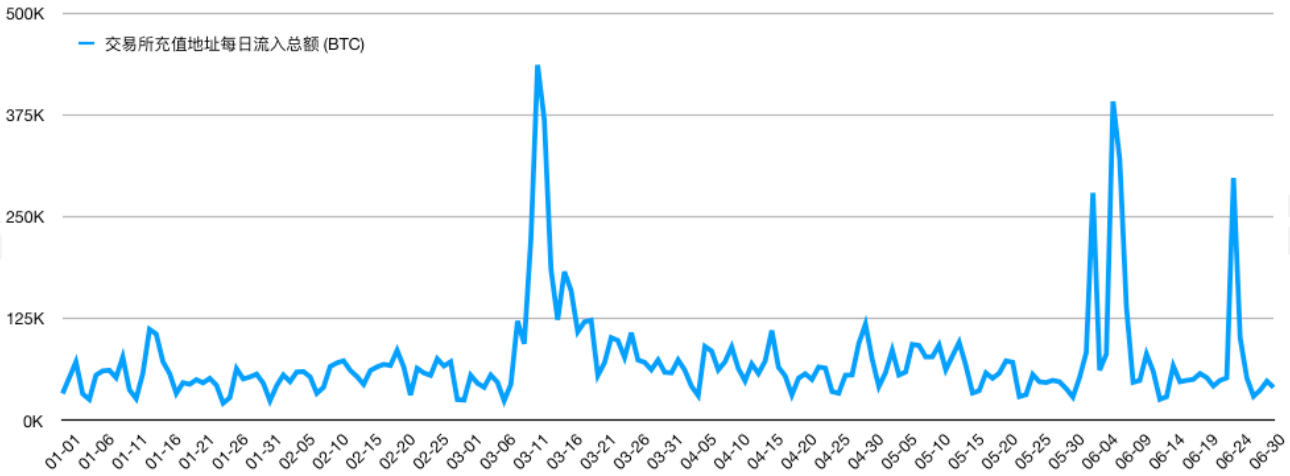


（图十二: 交易所热钱包资产情况——ETH资产）

3. 交易所地址流向全画像

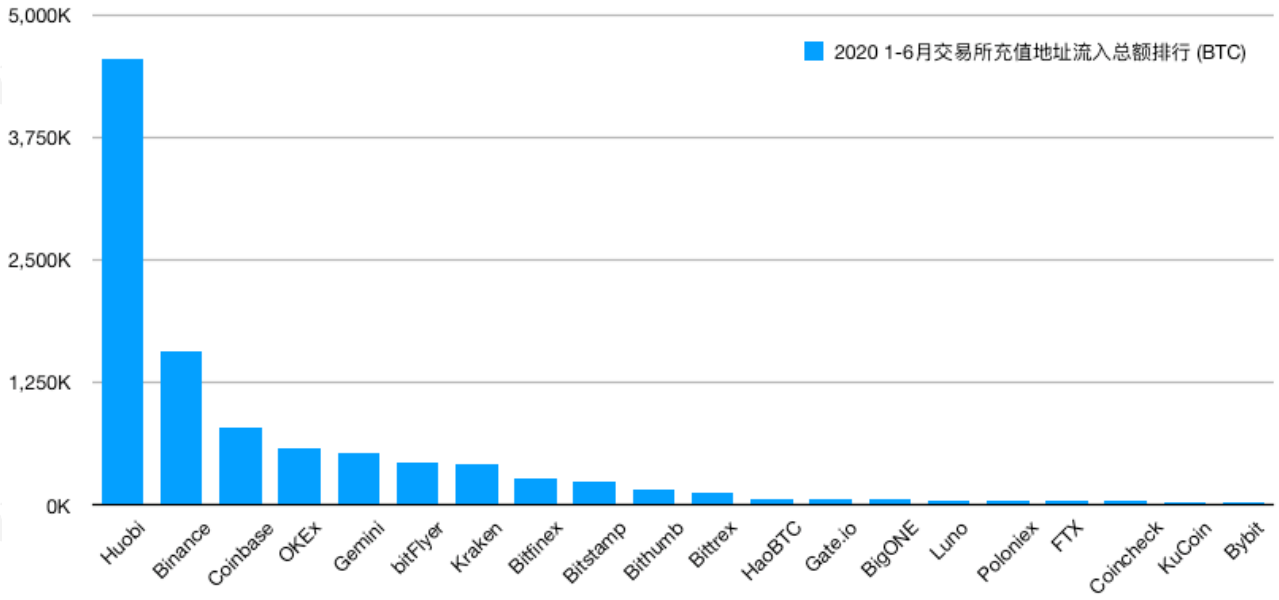
3.1 已统计交易所地址冷热钱包交互情况

我们在对大量的交易所地址进行纵向和深入分析之后，发现不同交易所冷热钱包之间交互频次大相径庭。对用户而言，如果一个交易所的冷钱包资产相对稳定，进账远远大于出账的时候说明该交易所的资产和负债相对稳定，反之则代表该交易所的资产相对不稳定。而如果一个交易所热钱包地址比较活跃的话则说明该平台的用户充提行为比较活跃，侧面则反映出该交易所有相对较好的市场活跃度。



（图十三: 2020上半年交易所充币地址充值情况）

如图十三反映了今年年初以来，已统计全部交易所的 BTC 资产充值情况。数据显示，自03月09日起，BTC 充值额度就有明显的爬升，并于03月12日达到峰值，当天 BTC 充值额度达到了43.66万枚。众所周知，今年03月12日加密市场遭遇了一次行情血崩，当天 BTC 行情振幅最高最高达到了40%，大家等待中的减半行情没有到来，价格先遭遇了减半。从链上数据来看，充值地址的异常活跃背后可能潜伏着一次较大的行情波动可能。



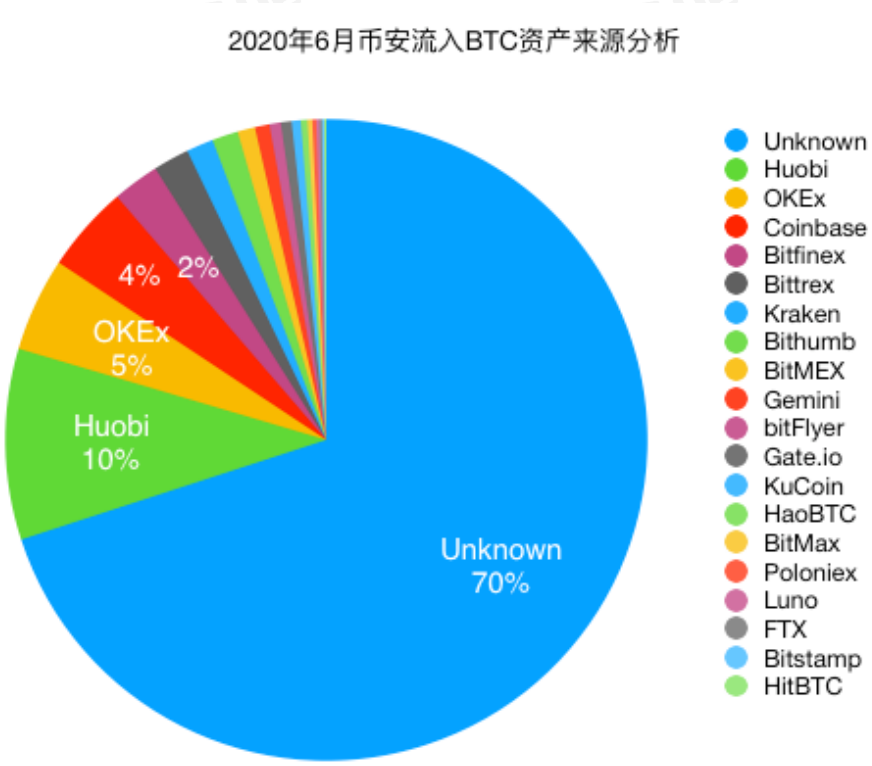
（图十四：2020上半年交易所充币地址流入数额排行榜）

如图十四所示，我们对2020上半年流入交易所的资金进行了详细划分发现，**自年初以来流入资金最多的交易所为火币交易所，共计流入454万个 BTC，排名第二位的是币安交易所，共计流入157万个 BTC，排名第三位的是 Coinbase 交易所，共计流入了79万个 BTC。**

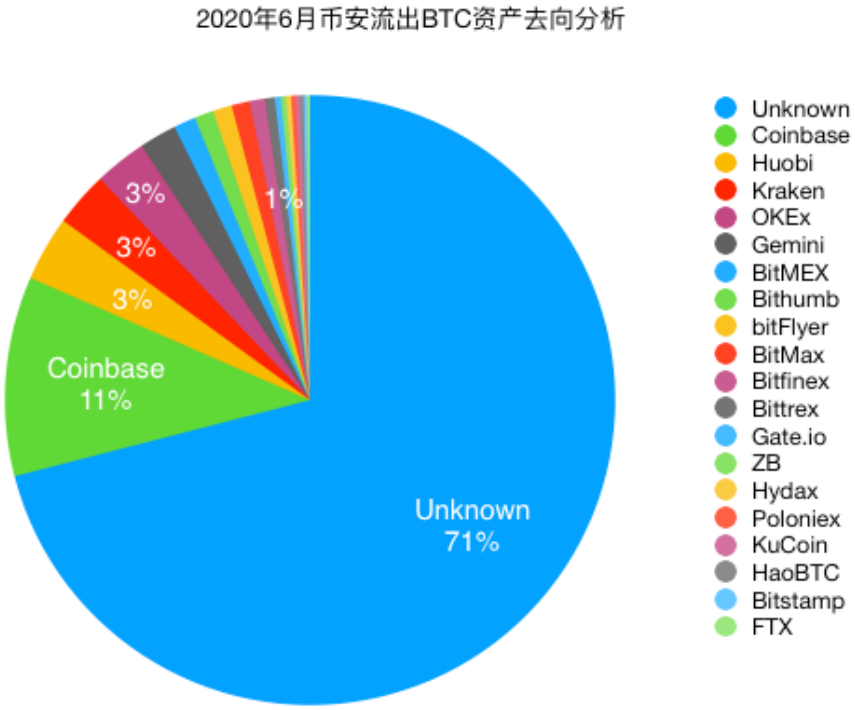
我们进一步观察发现，交易所之间彼此存在的资金流动比较频繁。接下来，我们将以币安交易所为例，并选取过去一个月的资金流动情况为参考，可以进一步管窥交易所之间的资金转移情况。

如下图十五、图十六所示，我们分别统计了今年六月币安交易所资产流进流出资金情况发现：过去一月，未知地址流入币安交易所的资产共计 39.88 万个 BTC，占比70%，而从火币流入币安的 BTC 有5.12万个，占比9%，OKEx 流入币安的 BTC 有2.81万个，占比5%。而过去一月，币安交易所流入未知地址的资产共计43.24万个，占比70%，流向 Coinbase 交易所的 BTC 有7.06万个，占比11%，而流向 OKEx 交易所的 BTC 有1.92万个，占比3%。

不难发现现在数字资产的流动主要集中在几个头部交易所之间，他们控制着大部分流通性。



（图十五：六月份币安交易所流入BTC 资产情况）



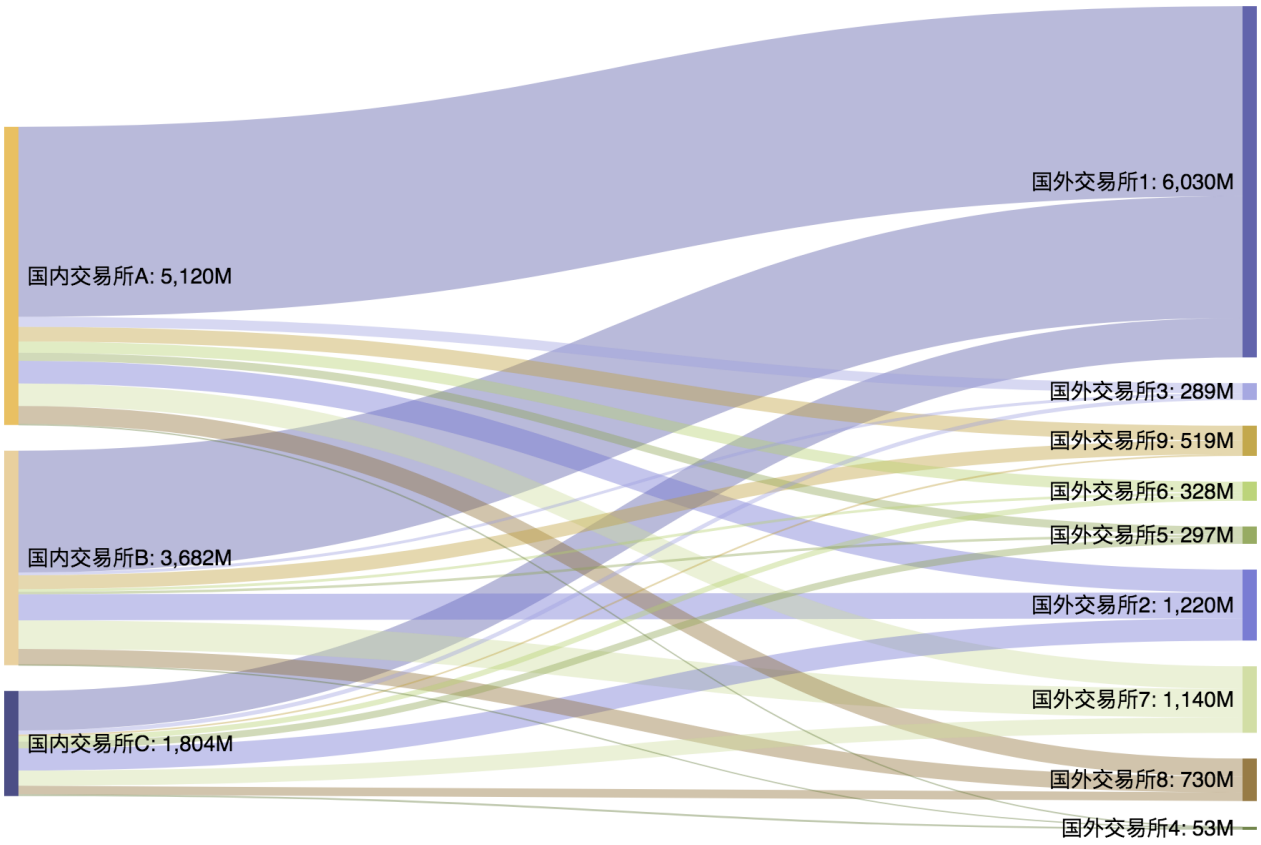
（图十六：六月份币安交易所流出 BTC 资产情况）

整体而言，我们可以初略估算出，过去30天，流入币安交易所的 BTC 数额为56.69万枚，而流出币安交易所的 BTC 数额为61.7万枚，币安现在资产属于净流出状态。

相比之下，国内另一大知名数字资产交易所火币网，过去30天，流入BTC资产19.88万枚，而流出BTC资产则为19.89万枚，基本持平。

3.2 已统计交易所跨国界资产流动情况

由于现在交易所注册在世界各地，有着不同的用户群体，我们分析各主要交易所的每天的资产余额以及交易所之间的资产流动情况，某种程度上，交易所可以和国家产生一些对应关系，分析一些交易所之间的资金流动，基本等于数字资产在不同国家之间的流动。



（图十七： 2019年从中国向国外各大交易所流出的资金总量）

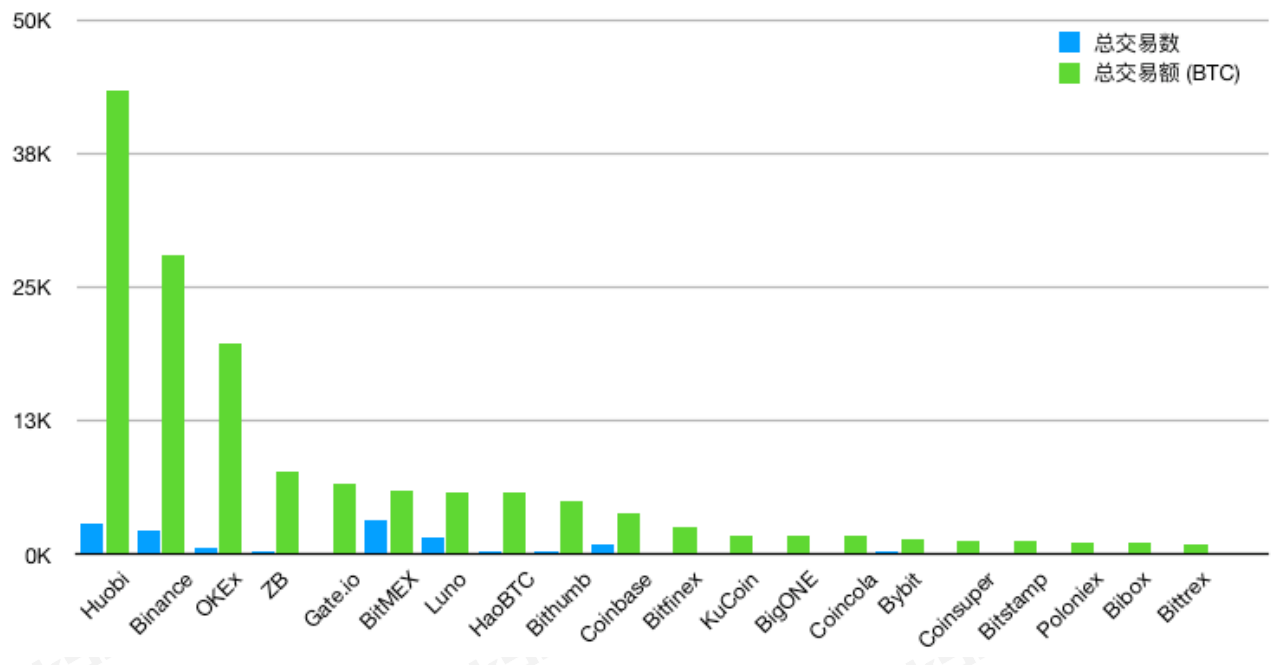
我们在此前的*2019*年度数字资产反洗钱（*AML*）报告中，部分阐述了关于数字资产跨国界流动的内容。

据 PeckShield 研究数据发现，以 BTC 为例，按交易时价计算，2017 年通过数字资产交易所从中国流向国外的资金量为101亿美元，2018 年为179亿美元，2019 年为114亿美元。近三年的流出资金总额超出中国三万亿美元外汇储备的1%。

3.3 已统计交易所地址赃款流进流出情况

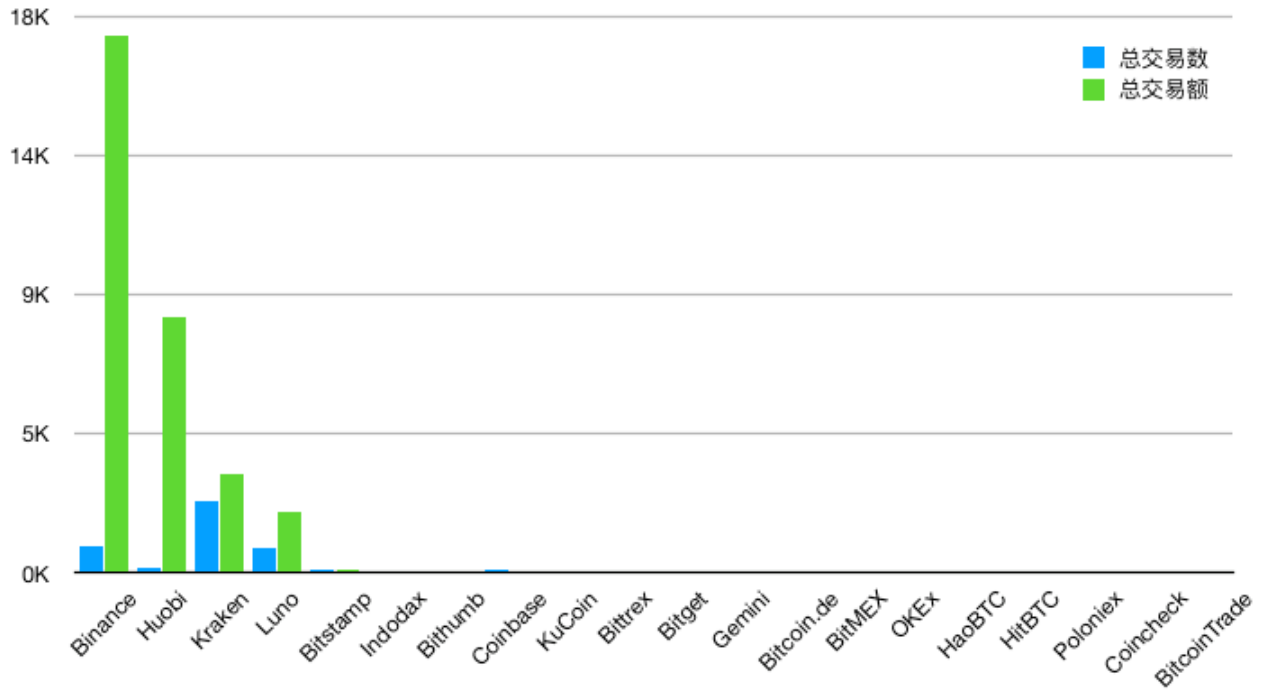
根据 PeckShield 旗下数字资产追踪平台 CoinHolmes 数据显示，截至06月30日，我们统计了 101 起黑客攻击事件，共计赃款 25.91 亿美元，其中至少 1,482 万美元已经流入交易所，此外还有 32 个包括 TokenStore、PlusToken 等在内的理财钱包或资金盘诈骗案件，受影响人群超百万，共涉及资产 75.18 亿美元，且目前已经有至少 2.1 亿美元流入交易所。

当然，黑客攻击和资金盘只是我们所统计高风险地址中的一部分，整体而言，我们对标记为高风险的地址进行了针对性监控发现，过去6个月共计流入数字资产交易所 13,927 笔高风险资产，合计 14.7 万个BTC，时价折合超过 14 亿美元，已经是一笔非常惊人的资产。

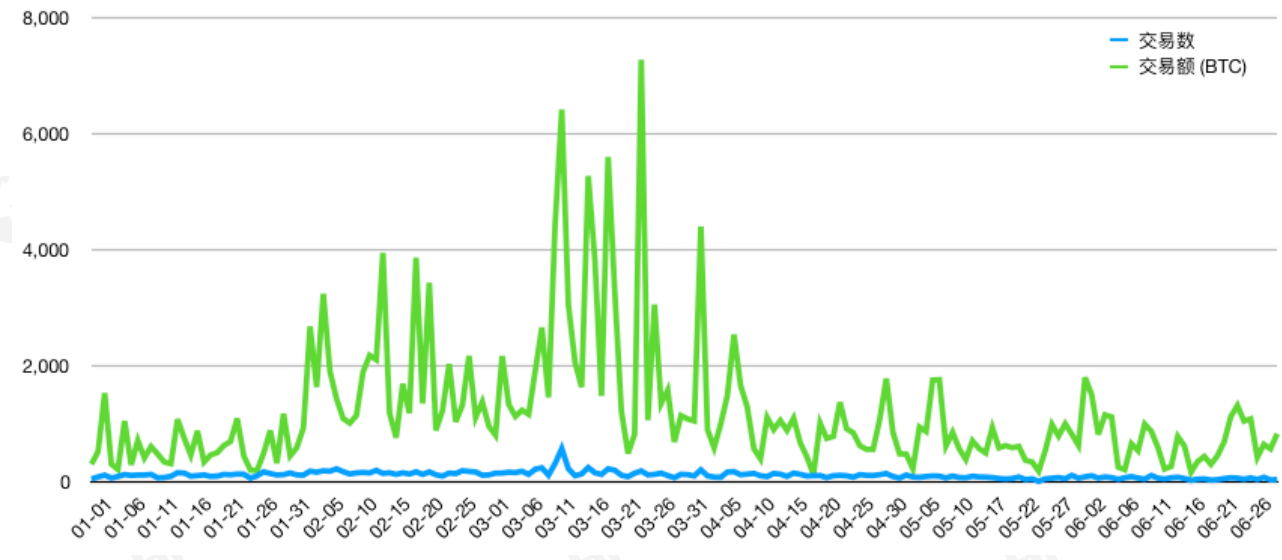


（图十八：2020上半年，赃款流入交易所排行情况）

如图十八所示，**我们把涉及赃款最多的交易所做了个排名发现，排名前十位的交易所分别为：Huobi、Binance、OKEx、ZB、Gate.io、BitMEX、Luno、HaoBTC、Bithumb、和Coinbase。**



（图十九：2020上半年，交易所每天涉及赃款交易频次和数额）



（图二十：2020上半年，交易所流出赃款频次和数额排行）

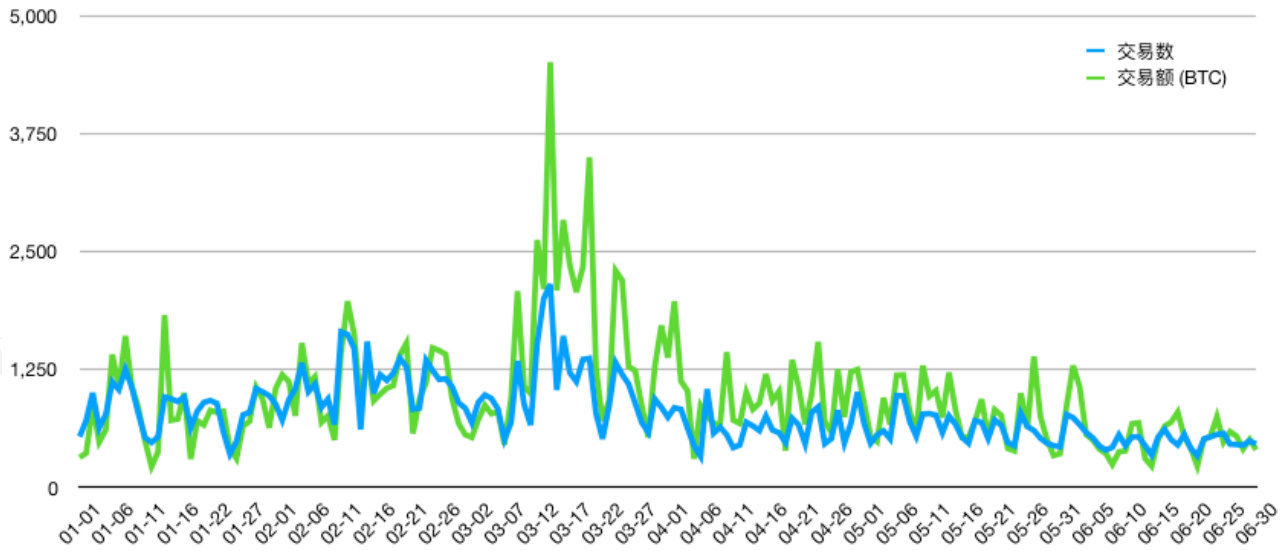
如图十八所示，我们对标记为高风险的地址做了详细分析发现，过去的6月份共计有377笔赃款交易流入火币网，交易总额达7,787个 BTC，而共计有 534 笔赃款交易流入币安网，交易总额达5,732个 BTC，而流入 OKEx 交易所共计94笔赃款，交易总额为3,491个 BTC。

如图二十所示，也存在大量从交易所流出赃款的情况，过去一个月共计145笔赃款从 Binance 交易所流出，共计总额3,887个BTC，而共计35笔赃款从火币交易所流出共计总额达1,430个 BTC，而共计463笔赃款从 Kraken 交易所流出，共计总额为434个BTC。

3.3.1 已统计赃款洗钱情况说明

我们在分析研究过程中发现，整个区块链生态面临的合规挑战非常艰巨，除了已知数字资产交易所本身的合规性问题之外，还存在一些完全不受监管的中间环节，比如：混币服务商和中心化倒卖机构。

这些中间环节犹如黑洞一般，吸走了大量的资产，使得整个资金流向环境变得错综复杂且难以追踪。一方面，我们在对地址做研究分析的时候发现，部分赃款会流入一些混币服务工具进行洗钱，截至目前我们已监控至少有 15.9 亿美元资产和混币服务商有关联；

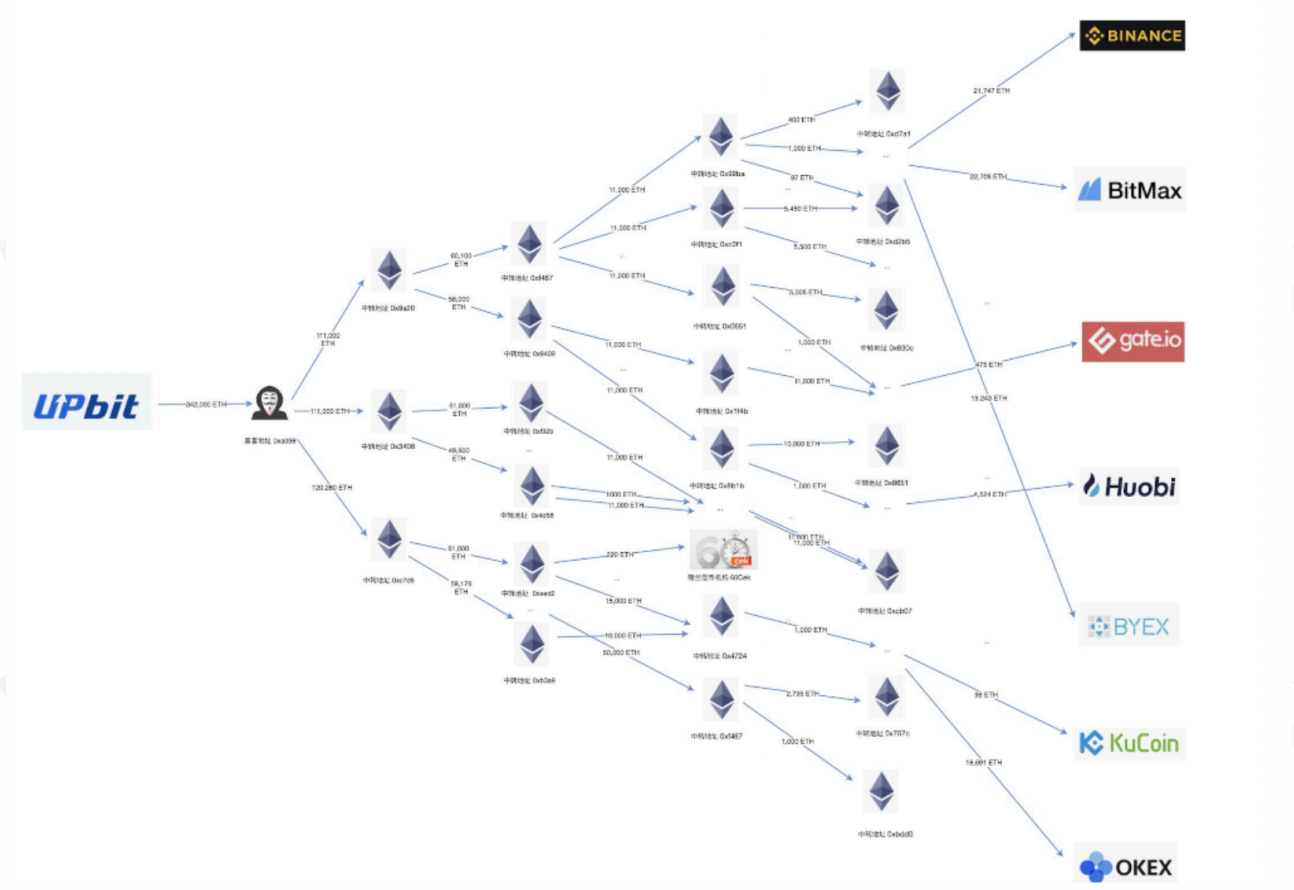


（图二十一：已统计混币服务商的资金吸纳情况）

另一方面，我们同时也发现，有一部分被盗资产会流向类似 ChangeNow、CoinSwitch 之类的中心化倒卖机构，这些机构不需要 KYC 环节，可以帮助用户人工倒卖各类数字资产，也成为一种比较主流的洗钱通道。

透过看混币服务商和跨链中心化倒卖机构，我们不难理解现在区块链生态面临的洗钱生态的复杂性。

2019年年底， Upbit 交易所遭受黑客攻击损失了3.4万个 ETH，过去半年时间，黑客一直在持续进行资产转移、切割、分散转移、混币、洗钱等操作，且于近日全部资金已清洗完成。如图二十二所示，黑客在攻击 Upbit 交易所得手后分了四层转移，最终资金分别流入了币安、BitMax、Gate.io、Huobi、KuCoin、OKEx、BYEX 等交易所。



（图二十二：Upbit 项目赃款流入交易所情况分析）

4. 交易所合规性挑战

值得一提的是，最初世界各个国家队数字资产交易所的监管态度都是模糊的，因此出台的策略也是简单粗暴一刀切。世界其他国家中，对数字资产比较友好的国家分别有瑞士、韩国、英国等；保持中立态度的国家有印度、印尼等；态度较强硬，明确限制的国家有俄国等。

以我们国家为例，早在*2013-2017*年因监管条例缺失，央行发布了两份报告，第一次否定了比特币的合法性，第二次则禁止了 *ICO* 和数字货币交易等行为。但*2019*年*10*月*24*日，国家将区块链技术升级为核心技术突破口，等同于明确了对于区块链行业的监管态度，因此行业合规性问题也就变得尤为重要。

对于区块链行业而言，短期看是一把双刃剑，监管会促使政策加大对行业违法乱纪行为的一棍子棒打行为，一方面这会让很多徘徊在政策和法规模糊边缘的项目被一网打尽加快行业格局的重新洗牌；另一方面这会让一些优质的项目能够突出重围得到更主流的资本、人才等青睐进而得到长期稳固的发展。

然而，监管之路并非一帆风顺，现在政府要全面介入区块链生态的监管面临如下挑战：

1) **现在主流的数字资产比如，*BTC*、*ETH*、*EOS* 等基本都是跨国界的，并无明确的政府监管范围。而且即使是某一个国家的政府强行干涉，该数字资产在其他国家依然能有流通空间，这使得监管介入的门槛比较高；**

2) **现在主流的数字资产交易所比如币安等，基本注册地都在海外，但其大部分用户却在国内，这就导致国内的法律或政策很难对交易所主体实施监管；**

3) **现在区块链生态环境比较复杂，有中心化交易所、去中心化交易所、混币服务商、免 *KYC* 交易所、暗网等等种种不受监管的渠道，而且比特币有 *UTXO* 找零等复杂的机制，一笔赃款在链上经过层层转移之后，尤其是经过一些混币渠道就几乎没法追踪到了。**

4) **现在各国 政府监管区块链的态度都不明确，地方司法或公安系统虽然接到了大量关于区块链诈骗相关的案宗，但目前没有明确的法律政策供参考执行，因**

此这类案件立案程序比较复杂，会存在一定时间窗口；另外大部分交易所都不愿意在警方没有立案的情况下私自对用户的资产进行处理，也会给黑客洗钱留下很多时间空间。整体而言，现在追查赃款存在的时间窗口太大，让很多违法分子洗钱操作容易得逞。

此外，交易所面临的合规性挑战还体现在其内部构建环境的复杂性上：

1) **数字资产交易所要对目前上架的全部数字资产做统一的合规性检查，而不同币种的合规性情况，在不同国家均有较大差异，这会给交易所自身业务带来巨大挑战；**

2) **数字资产交易所服务的用户目前更更多是一些崇尚去中心化和自由的技术极客，交易所面临拥抱监管还是选择用户的二选一难题。**

3) **数字资产交易所的内部账本目前都是不透明的，但其合约市场一直存在后台控盘，拔网线等争议性，这些道不清说不明的问题，目前很难有一套公允的说法。**

5. 结论

综上所述，PeckShield 安全团队向大家展示了 FATF 政策落地前夕，数字资产交易所整体面临的合规性问题，包括，交易所之间的资金往来合规性问题，流入交易所的赃款情况等等，整体而言：

1）据 PeckShield 数据显示，截至2020年06月30日，全球数字资产交易所资产余额排行榜（以 BTC+ETH+USDT 资产折算为美元计）为：Coinbase 交易所的资产总量为111亿美元，排行第一位，Huobi 交易所资产总量为57.9亿美元，排行第二位，Binance 交易所资产总量34.5亿美元，排行第三位，Bitfinex 资产总量 29.9 亿美元，排行第四位，而 OKEx 资产总量为 25.2 亿美元排行第五位, BitMEX, kraken, Germini, mtGox, bittrex 等分别排行第六到第十位。

2）据 PeckShield 旗下数字资产追踪平台 CoinHolmes 数据显示，包括黑客攻击、资金盘、暗网、赌博等在内的我们已标记为高风险的地址，在过去6个月共计流入数字资产交易所13,927笔高风险资产，合计14.7万个BTC，时价折合超过14亿美元，已经是一笔非常惊人的资产。我们把流入赃款最多的交易所做了排名发现，排名前十位的交易所分别为：Huobi、Binance、OKEx、ZB、Gate.io、BitMEX、Luno、HaoBTC、Bithumb、和Coinbase。

3）据 PeckShield 数据显示，截至2020年06月30日，我们已监控高危风险地址中，流入黑名单地址的资金有16.2亿美元，流入混币服务商的资金有15.9亿美元，经混币服务的资金如同石沉大海，很难有再被技术性追踪的可能。常见的混币服务商有：Bitlaunder, HelixMixer, Samourai, Wasabi, BitcoinFog 等；中心化倒卖机构有：ChangeNow、CoinSwitch 等。

参考文献

[1] FATF INR15 监管条例

[2] PeckShield 数字资产反洗钱报告

[3] CoinHolmes 数字资产可视化追踪平台

关于我们

PeckShield「派盾」成立于2018年，是全球顶尖的区块链安全公司，核心团队曾服务于360、Intel、Juniper、Alibaba 等全球知名厂商，团队成员多次原创发现底层核心安全漏洞获得各大厂商官方致谢。

PeckShield 作为早期专注于区块链生态的头部安全公司，基于安全团队二十年来在代码分析、操作系统、大数据等安全业务领域的积累，提出了一整套渗透测试、代码审计、应急响应、链上数据监测，AML 反洗钱等安全与数据综合解决方案，业务覆盖区块链生态安全的各个环节。包括公链提供商 (EOS、Nervos、TRON、IOST、Harmony)，头部钱包和矿池 (imToken、SparkPool、比特派、Cobo 钱包)，以及头部交易所(Huobi、KuCoin)等。PeckShield 团队因多个关键安全漏洞发现而广受业内关注，被 Etherscan.io 纳入智能合约安全审计推荐名单，同时跻身「以太坊赏金猎人」全球排名 Top 3。

目前，PeckShield安全业务已覆盖全球范围，主要客户包括有：公链提供商 (EOS、Nervos、Harmony、AVA、HBTC、NEO 、IOST、Bytom、TRON、OKChain），头部钱包和矿池 (imToken、SparkPool、比特派、Cobo 金库，VoiceWallet)，以及头部交易所(Huobi、KuCoin、Bithumb、Upbit、OKex)、DeFi 应用及智能合约（MakerDAO、StarkWare、Tokenlon、InstaDApp、Set Protocol、Ren Project、Hydro Protocol、dForce、Newdex、HoneyLemon）等。

PeckShield 旗下成立了 DAppTotal、DAppShield、CoinHolmes 等多个独立的数据与安全服务品牌，致力于提升区块链生态整体的安全性、隐私性以及可用性，并为生态用户提供切实有效的数据与安全解决方案和服务。

关于CoinHolmes

CoinHolmes 是 PeckShield 推出的独立品牌，专门为数字资产服务商（交易所、钱包、托管服务等）、监管组织和犯罪调查机构提供 AML 合规的解决方案、调查和追踪工具。

CoinHolmes 专注于区块链地址的身份识别、追踪不良资产和情报挖掘。目前已成功识别 近1亿地址的实体，并且推出了BTC、USDT和ETH的资产追踪工具和反洗钱 API。

交易所和钱包、矿池可以通过 CoinHolmes，实时监控和识别从暗网市场、制裁地址、诈骗地址发起的异常交易， 防止黑产的流入和保障客户的取款安全。

犯罪调查机构、监管机构可以通过 CoinHolmes，了解每笔交易背后的现实世界实体，绘制直观的资金流向到可视化视图中， 使打击洗钱、诈骗、暗网交易等数字资产犯罪变得更为轻松 。

我们为各种类型的客户提供完整的反洗钱解决方案，和灵活的访问途径。

网站：https://www.coinholmes.com

联系：contact@coinholmes.com