PeckShield

数字资产反洗钱(AML)

研究报告

2019年度

杭州派盾信安科技有限公司

2020.01

目录

0. 概要

比特币等数字资产早期主要被用于从暗网购买毒品，假钞等违禁物品。现在，随着区块链技术的逐渐成熟，比特币作为主流数字资产，成为许多人追捧的价值标的，也延伸出了更多的使用场景，非法交易已不再是其主流用途。但是，PeckShield 通过对大量地址和交易深入剖析发现，违法交易还普遍存在于数字资产交易中，且绝对规模仍在不断扩大中。

PeckShield 安全团队全面梳理了近几年使用数字资产进行的“非法或未受监管”的交易现状，并深入分析了以下三方面的数据：

重大安全事件和损失情况：PeckShield 统计发现：2017年共发生重大安全事件11起，共计损失2.94亿美元； 2018年共发生重大安全事件46起，共计损失47.58亿美元。2019年共发生重大安全事件63起，总共损失达到了76.79亿美元。

暗网市场交易规模：截至目前，运行 TOR 协议的暗网网站已有6万个左右，其中大约一半从事非法交易。暗网市场中的交易需求非常大，不断有大型黑市被关闭，但很快又会有新的黑市涌现出来，其总交易额还在不断增长。2018年流入暗网的比特币总数为33万枚，2019年为54万枚，按交易时价计算，总金额分别是21亿美元和39亿美元。

国际间未受监管资金流动情况：以数字资产作为载体的资金在国际间的流动已经非常巨大，但不同国家对比特币等数字资产的法律界定还很模糊，意味着这些流动资金并未受到合理、合规的监管。

PeckShield 安全团队深入研究发现，2017年通过数字资产从中国流到国外的资金总量为101亿美元，2018年为179亿美元，2019年为114亿美元，三年总额超出中国3万亿美元外汇储备的1%。

今年以来，各国政府及国际机构开始研究如何监管这些数字资产，比如，2019年6月，FATF 作出规定，要求从2020年6月开始，数字资产服务商必须对金额超过1,000美元/欧元的交易报备。

1. 背景介绍和研究方法

2008年11月，一位化名中本聪 (Satoshi Nakamoto) 的神秘人物在网上发表了一篇论文，“Bitcoin: A Peer-to-peer Electronic Cash System” (比特币：一个点对点的电子现金系统)，宣告了加密资产比特币的诞生，同时也开启了区块链技术跌宕起伏的十年发展征程。

比特币的设计初衷是做一个去中心化，不需要第三方中介平台验证，任何人都可以使用的全球电子支付系统。由于其匿名性和全球化的特性，比特币一问世就吸引了各种非法交易者，包括暗网商贩，以及诈骗、勒索犯罪份子的注意。

比特币早期主要充当了暗网市场中的流通介质，包括购买毒品，假钞等货物。丝绸之路 (Silk Road) 就是第一个著名的暗网黑市，在那里可以买到几乎所有的违禁物品，它后来于2013年被美国 FBI 查封 [1]。

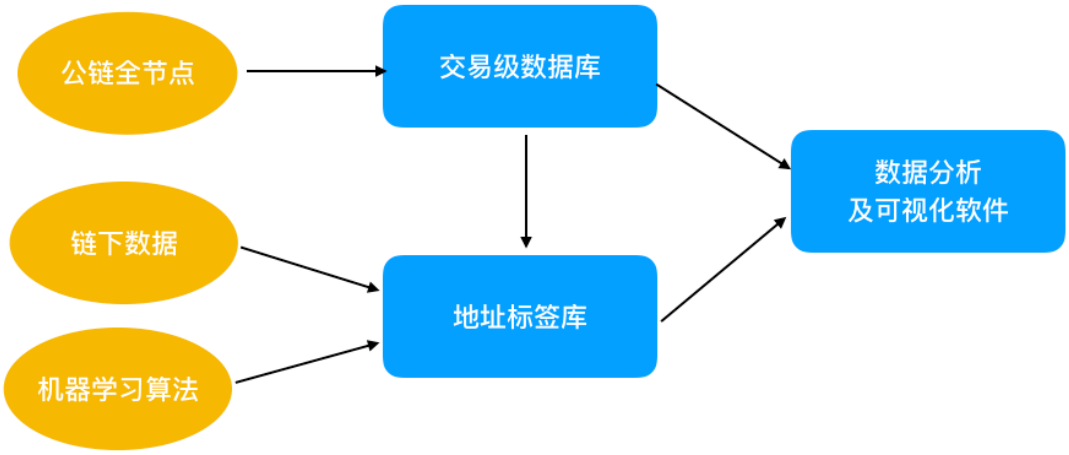
随着区块链技术的不断成熟和应用场景的拓展，目前用于非法用途的比特币交易量仅占其总交易的2%左右 [2] ，更多的交易量还是主流合法用途，不过，一个引人担忧的事实是，比特币的非法用途近些年仍呈现不断上涨的趋势。

PeckShield 数据表明，2019年流入暗网的比特币价值超过39亿美元，而流出直接到交易所的比特币规模也超过2亿美元。这其中，有一部分资产可能是由于数字资产交易所被黑客攻击之后赃款的流入，还有诈骗、勒索事件中，罪犯要求受害者用比特币等数字资产进行的付款。

在这个报告中， 我们全面梳理了过去一年，未受监管的数字资产交易数据 (包括使用数字资产进行非法用途的交易等) ，并进行了深入、详细的统计和分析。具体包括以下三个方面的数据：1）近年来主要安全事件和损失情况；2）暗网市场交易规模；3）国际间未受监管的资金流动情况。

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。



图一 分析工具架构图

如图一所示，我们的工具库可以分为三个主要部分：

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，生成了总数超过6,000万的地址标签库，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，用于对 1) 和 2) 的数据分析，以便能从海量庞杂的不相关数据中，挖掘出具有相关性的可视化数据路径和图表，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。在报告的下文中，我们罗列的几个重要案例正是基于这些分析工具所呈现的结果。

在本报告的第三章中，我们对暗网数字资产交易展开了系统的分析。我们制作了一个用 Python 语言编写的，可并行、高速运行的 TOR 网页收集和分析工具，先从暗网服务器中找出大量网页内容，然后分析网页结构、内容、关键字等信息，用它来爬取暗网中存在大量的数字资产地址。

1.2 免责声明

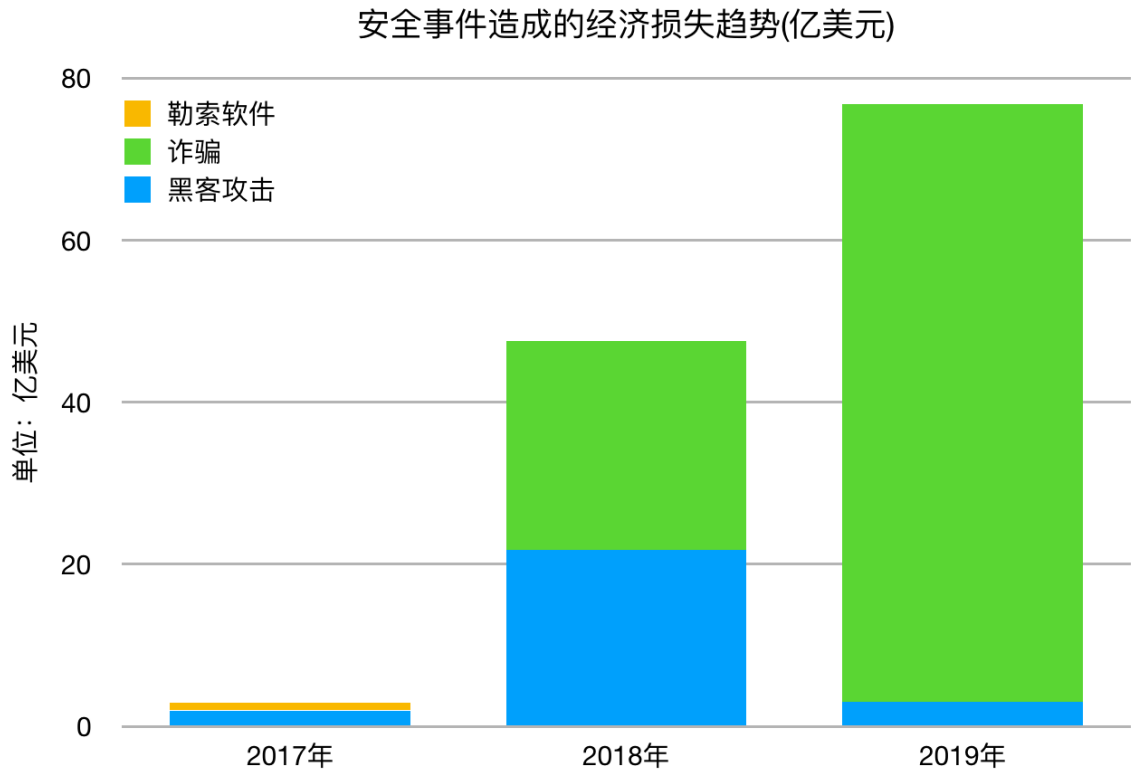
本报告内容基于我们对区块链行业的理解以及多项研究实践，但由于区块链的匿名特性，我们在此并不能保证所有数据的绝对准确性，PeckShield 也不能对其中的错误、疏漏、或使用本报告引起的损失承担责任。

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. 安全事件统计及典型案例

经过十年多的快速发展，区块链技术已经延伸出了一个包含公链、联盟链、数字资产交易所、数字钱包、矿场、矿池、矿机厂商等一个完整的产业生态系统。今年10月24日，国家更是把区块链技术列为核心技术突破口，为区块链产业的后继发展奠定了信心和基础。

然而，早期区块链生态并不成熟，在各个环节各种安全问题也屡见不鲜。PeckShield 安全团队整理了自2017年至2019年发生的重大区块链安全事件，我们的数据显示：



图二 近三年安全事件损失统计

2017年共发生重大安全事件11起，共计损失2.94亿美元，其中黑客攻击事件8起，诈骗类事件3起，损失最大的一笔来自12月07日发生的挖矿平台 NiceHash 遭黑客攻击事件，共计超过4,700个比特币被盗，损失约 8,000万美元；此外，还有多起钱包被盗事件，共计价值损失超过了6,550万美元。

2018年共发生重大安全事件46起，共计损失47.58亿美元，其中黑客攻击事件42起，诈骗事件4起。损失最大的一笔来自4月22日的黑客攻击事件，黑客利用以太坊 ERC20 智能合约存在的 BatchOverFlow 漏洞攻击美链 BEC 智能合约，导致 BEC 数字资产价值几近归零，市值蒸发9亿美元。值得一提的是，在这46起重大安全事件中，交易所被盗事件包含17起，共计损失8.7亿美元。

2019年共发生重大安全事件63起，共计损失76.79亿美元，其中黑客攻击43起，诈骗事件20起。相较2018年，今年交易所安全事件下降了20%，其中影响较大的两起安全事件分别为：币安被盗7,074个 BTC，韩国交易所 Upbit 34.2万枚 ETH 被盗，整体而言，交易所爆发安全事件的概率显著降低。然而，这一年诈骗类安全事件却增长了4倍，成了区块链世界最大的安全威胁，尤其是 PlusToken、TokenStore、OneCoin 等资金盘项目，均造成了数亿美元不等的巨额损失。

2.1 2017 - 2019安全事件演变态势

图二是近三年区块链安全事件的损失数据统计。下面我们将从不同维度数据来对这些安全事件进行进一步剖析和解读。

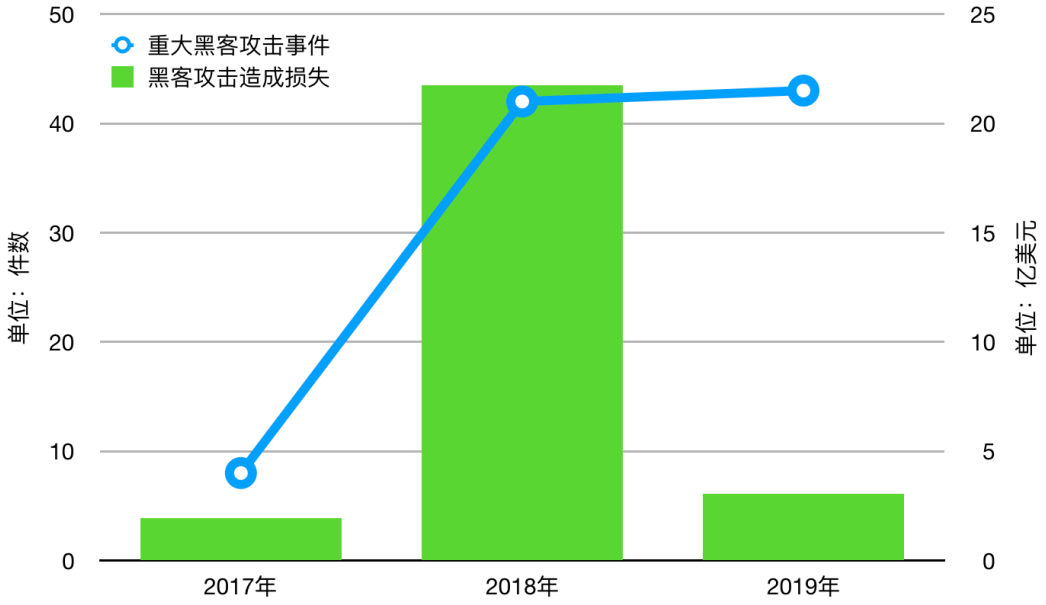
我们按事件类型和损失数额把已经发生的安全事件进行了归纳梳理发现：

1）2017年区块链安全事件造成的2.94亿美元的损失中，黑客攻击造成1.92亿美元损失，诈骗事件造成460万美元损失，通过勒索软件收取的比特币价值9,700万美元；

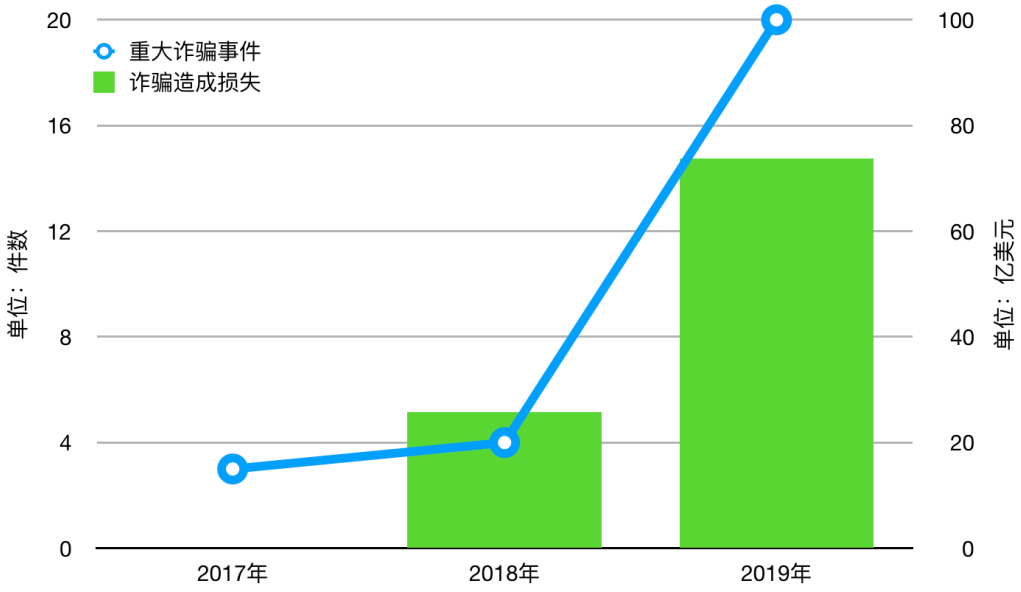
2）2018年区块链安全事件造成的损失高达47.58亿美元，较2017年大增1,523%，其中黑客攻击造成21.73亿美元损失，诈骗事件造成25.8亿美元损失，勒索软件损失524万美元；

3）2019年区块链安全事件造成的经济损失高达76.79亿美元，较2018年增长60%，其中黑客攻击造成3.06亿美元损失，诈骗造成73.73亿美元损失，勒索事件则是55万美元。很显然，这一年造成主要危害的是理财钱包诈骗事件，其中排名前两位的分别是 OneCoin 和 PlusToken，分别造成近40亿和30亿美元损失，同时产生了巨大的社会影响。

综上不难看出，2017、2018年相对处于区块链技术早期，区块链行业开发者整体安全意识较为薄弱，因项目本身漏洞诱发的黑客攻击事件占绝大多数。



图三 黑客攻击事件损失统计



图四 诈骗事件损失统计

2019年以来，整个区块链生态经过一两年的黑客攻击市场教育，开发者整体安全防御举措有所提高，整体上，因漏洞产生的安全事件减少了。然而却集中爆发了一批，包括 OneCoin、PlusToken、TokenStore、波场超级社区等在内的

资金盘项目。数据显示，2019年因诈骗造成的损失金额达到了惊人的73.74亿美元，相较2018年，增长了近48亿美元。这是由于数字资产市场有强大的财富效应，对普通用户而言，技术和参与门槛相对较高，这给了一些投机份子炮制各种骗局的可能性。

OneCoin 创建于2014年，该骗局从受害者手中非法赚取了40亿美元，其首脑于2019年3月在美国被捕；2019年6月 PlusToken 项目跑路，涉及多种数字资产，造成至少30亿美元的损失；而 TokenStore、波场超级社区则分别造成数千万美元的损失。

图三和图四分别是黑客攻击事件和诈骗事件的损失统计数据。在以下章节中，我们将筛选三个社会影响巨大，用户损失惨重的典型诈骗案例，对其事件过程和资金转移途径进行详细剖析。

2.2 PlusToken 事件

PlusToken 号称是一家在韩国注册的“加密币钱包和交易所”，但它的真面目是一个用高回报吸引投资者的庞氏骗局。PlusToken 许诺给投资者10%-30%的月息，并以此高回报吸引大量投资者相继投入超过20万枚BTC，78万枚ETH，和2,600万EOS等价值不菲的数字资产 [3] [4] [5]，涉及资金达到30多亿美元，用户超300余万人，故而影响范围非常广且危害巨大。

2019年6月29日，PlusToken 用户反馈无法提币，项目方也被媒体曝光跑路，随后又传出六名主要负责人被中国警方逮捕。然而，其涉及的巨额赃款至今仍没有追回并返还受害者。

PeckShield 第一时间就介入了对 PlusToken 资金的追踪调查，并对其钱包涉及的若干关键地址进行锁定监控追踪。图五是利用 PeckShield 研发的数字资产追踪工具 CoinHolmes，对 PlusToken 事件进行复盘和资金流向追踪图。

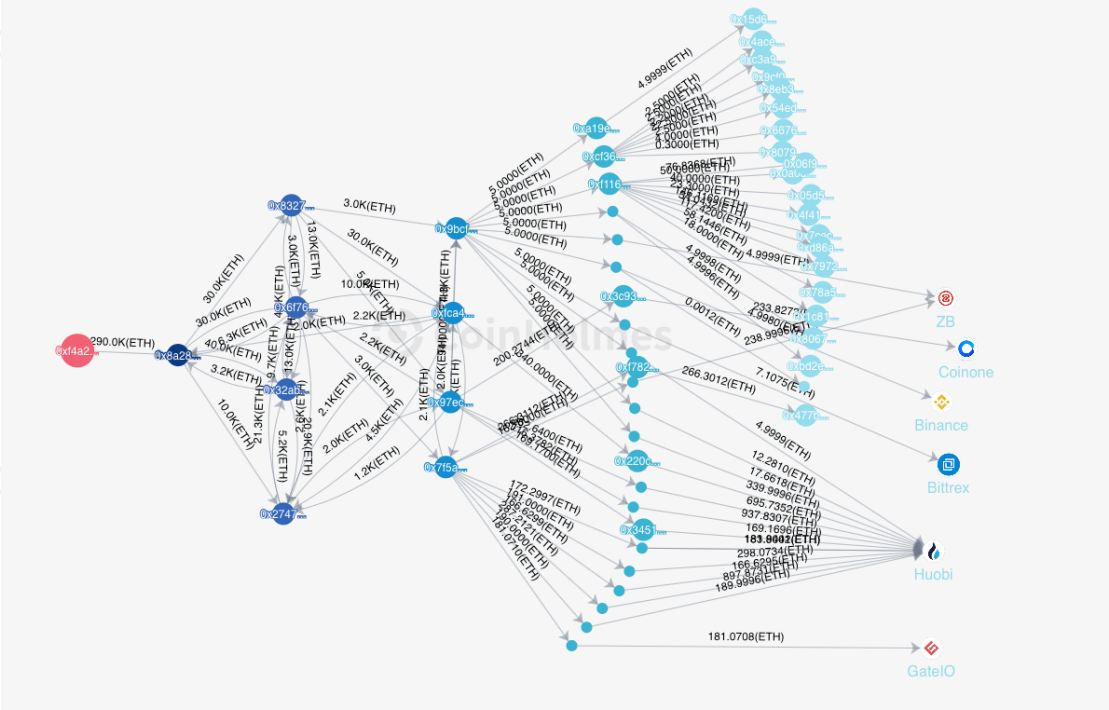
可以看出，PeckShield 锁定监控的目标地址进行了多次周密的分散转移乃至混淆洗钱等操作，最终部分资金流入了交易所。

第一阶段主要是资金转移，自03月14日起，我们观察到14BWH6G开头的地址开始活跃起来，分批次向其他账号转移资金，总计有95,228个 BTC 被全部转移清空。

第二个阶段出现了洗钱行为，从08月20日开始，CoinHolmes 系统监测到众多跑路地址上的资金发生汇聚，91,779个原属于多签地址的 BTC 被集中汇聚到5

个单签地址中，再由单签地址进行转移。部分资金并没有直接流入交易所，而是通过类似 ChipMixer 的工具进行混淆，再通过场外 OTC 的渠道卖出。

截至目前， PlusToken 事件的影响并没有结束，仍有大量的数字资产并未进行转移，成了数字资产市场一个很大的不稳定性因素，以至于一旦出现不明缘由的行情下跌，大家就会把原因归结为“PlusToken砸盘”。PeckShield 正在对其相关地址进行持续监控，并联合区块链生态各方力量进行追踪标记，同时协助警方追踪在逃数字资产，尽可能帮助受害投资者减少损失。

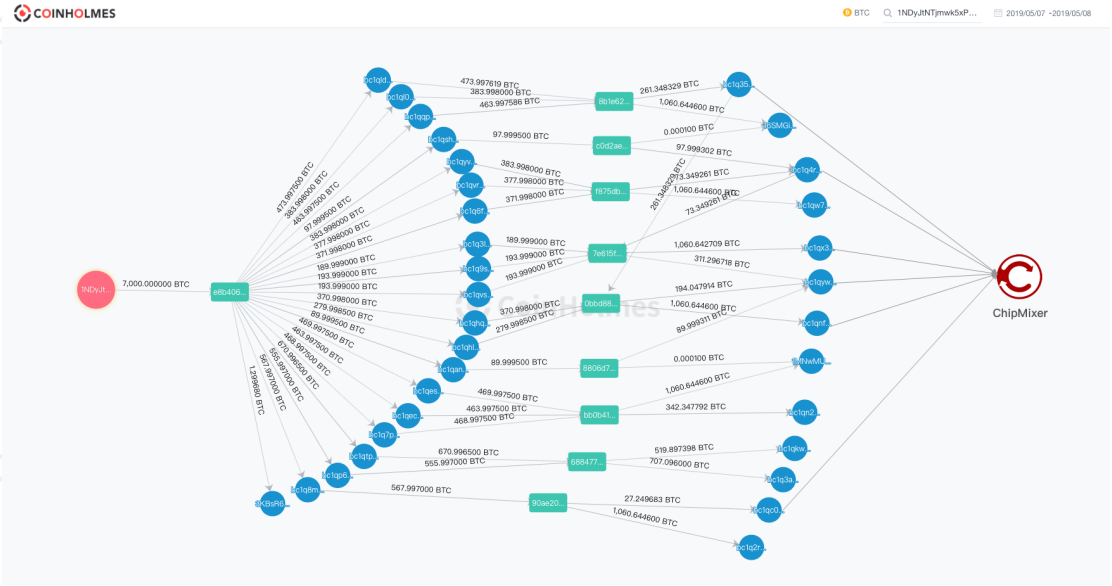


图五 PlusToken 资产转移过程图

2.3 币安7,000枚 BTC 被盗事件

全球知名的数字资产交易所币安于05月08日上午发布公告称，当天凌晨1时15分，币安遭到了黑客大规模的系统性攻击，黑客获取了大量 API 密钥，谷歌验证 2FA 码等信息，一次性提走了7,000枚BTC [6]。

据我们数据显示，本次黑客攻击事件中，币安共计损失了7,074枚 BTC (按当天价格计，价值约4,200万美元) 。PeckShield 安全人员深入剖析了黑客实施攻击的全过程，并对被盗链上资产进行全路径还原 (见图六) 后发现：



图六 币安资产转移图

第一步：20个主要分散存储地址

本次黑客攻击得手之后，首先对资金进行了分散转移存储，总计将7,074枚 BTC 以每个地址100枚-600枚不等的额度分散于20个主要 (大于1枚 BTC) 新地址。

第二步：开始汇聚地址，实施资产转移

在将所盗取7,074枚 BTC 分散存储开后，7个小时后，黑客再一次开始整理资金，先清空了20个地址中的2个地址，并将2个分别存储有566枚和671枚的 BTC 汇聚成1,226枚 BTC 转入 bc1qkwu、bc1q3a5 开头的两个新地址。最终又将该笔资金中的其中519.9枚 BTC 汇入另一个地址，剩余的707.1枚 BTC 停留在原地址。

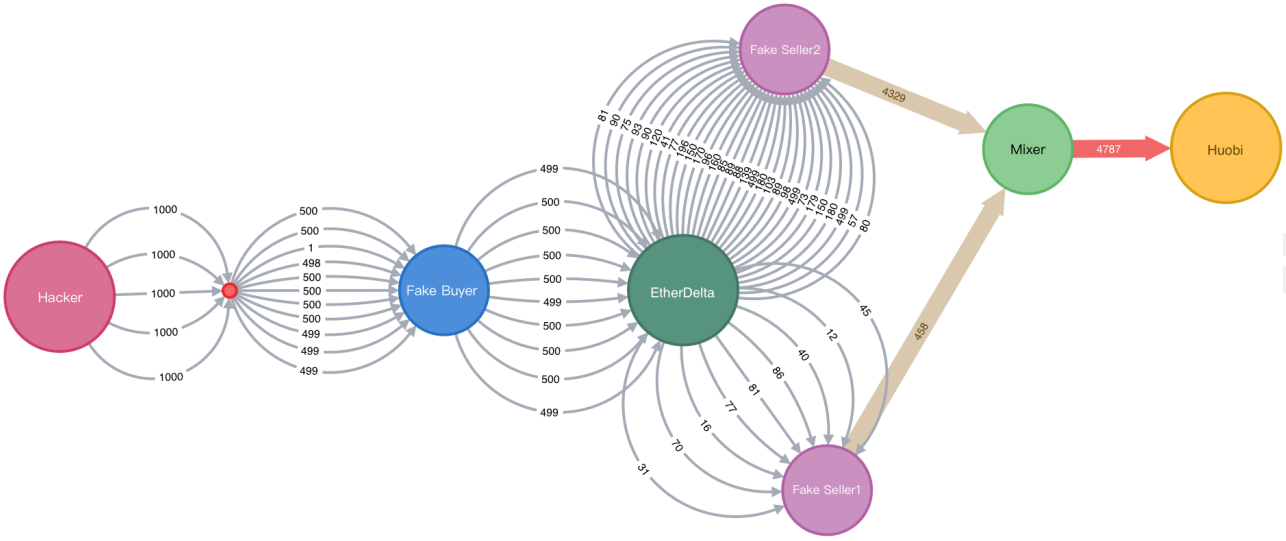
最终，将资金转移至 bc1q2rd、16SMGih、1MNwMUR、bc1qw7g、bc1qnf2、bc1qx36、bc1q3a5 开头的7地址中。

第三步：通过 ChipMixer 实施洗钱。

在此后的一段时间内，黑客开始分批次进行洗钱操作，将资金分拆成小额，再通过类似 ChipMixer 的工具进行混淆，最后再经过场外 OTC 渠道卖出。

2.4 新西兰交易所 Cryptopia 被黑事件

2019年1月，黑客攻击了新西兰的虚拟资产交易所 Cryptopia，盗取了以 ETH 为主的数字资产 (当时价值1,600万美元左右) 之后销声匿迹 [7]。在间隔几个月后，黑客开始利用不同方式进行洗钱。



图七 Cryptopia 被盗资产转移图

如图七所示，据 CoinHolmes 数据显示，2019年5月黑客先是将5,000枚 ETH，分批汇聚进入去中心化交易所 EtherDelta，伪装成买家卖家倒手买卖，最终汇聚进入火币交易所。

时隔4个月黑客再次发生动作，09月22日，Cryptopia 被盗资产关键地址中，0x845f93 开头的地址向 0xd759ea 开头的地址转移了5,010个 ETH，开始分散转移洗钱操作。黑客首先转出120个 ETH 至 Yobit，发现未被冻结后再陆续转出大额 ETH，总计有1,410个 ETH 流入 Yobit 交易所。

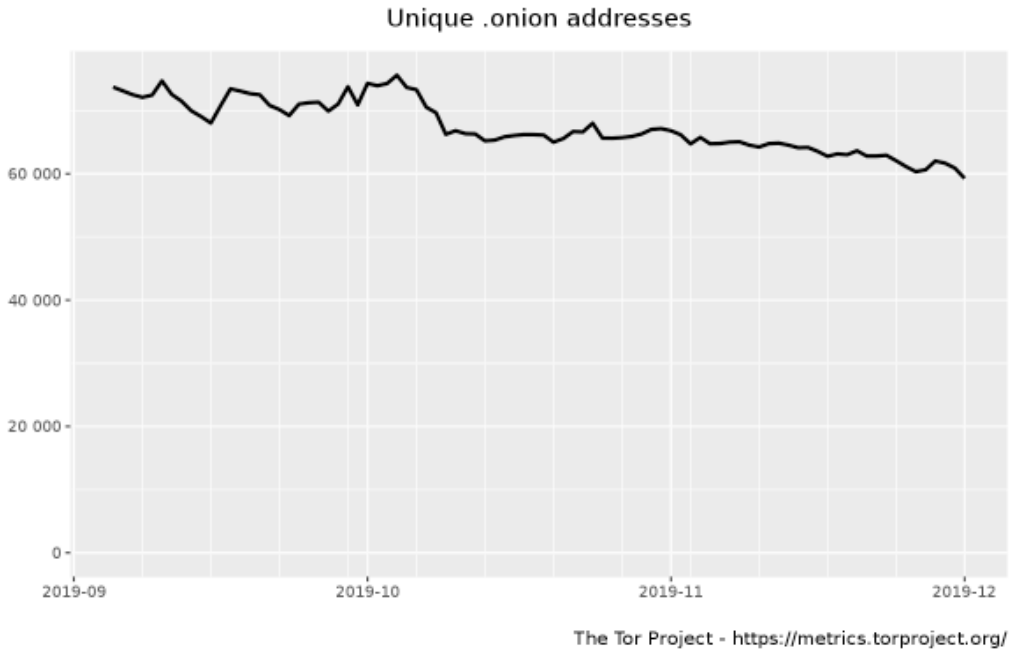
10月11日至17日间，黑客又采取了全新的洗钱方式进行资金转移。Cryptopia 被盗资产关键地址中，0x9481bd 开头的地址向多个地址分散转移了657个 ETH，其中有部分通过 Uniswap 去中心化交易所兑换成 DAI，最终流入知名 DeFi 借贷平台 Compound，还有少部分流入一个称作 DeFi 2.0 的项目。

我们不难看出，Cryptopia 交易所被盗后黑客通过各种方式进行洗钱，方式不仅包含传统的利用中心化交易所，还有通过去中心化交易所，以及 DeFi 项目 Compound 等。由于中心化交易所存在被冻结、追溯的可能，流通性较大的去中心化交易所和 DeFi 借贷平台也慢慢成为黑客洗钱的新选择。

3.暗网市场数字资产流向

1990年代中期，美国海军实验室研发了一种匿名、机密的通讯机制，原本要用于美国政府部门间的保密信息通讯。然而，这个项目研究成果最终没有得到政府的采用，不过，在2004年其代码被美国军方开源。运行这些代码的服务器在互联网上形成了一个独立的网络，他们的网页对谷歌，百度等搜索引擎是不可见的，主流浏览器也无法访问这些网页，所以这个网络也被称为暗网 [8]。

暗网，也叫 Darknet, Dark Web，或者 TOR network。TOR 是 The Onion Router (洋葱路由器) 的缩写。 TOR 协议把一个数据包像洋葱一样层层加密，然后通过一系列随机挑选的路由器转发。由于每个路由器只能解密下一层，且只知道下一个站点的地址，所以在这一链路的任一点监测都无法知道这一通信的源头和目的地。这样不仅可以保护浏览者的身份和地点，同时也可以对抗网络封锁。

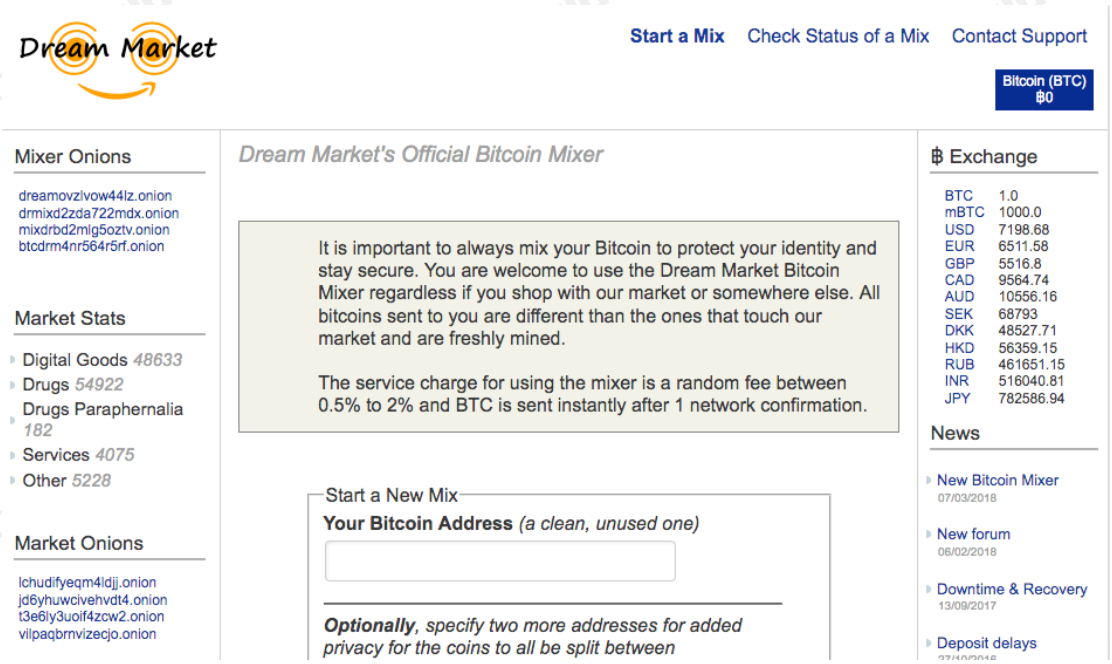


图八 暗网网站数量

暗网的规模远小于互联网，目前网站总数仅6万个左右，如图八所示。暗网中的网站也并非都从事非法活动，也有一些是为了提倡言论自由，保护用户个人隐私而开设。世界主要报纸和新闻机构在暗网中都设有网站，还包括 Facebook, CIA等。据 Terbium Labs 研究发现，大约有一半的暗网网站从事非法活动，主要包括毒品交易，武器走私，色情，极端恐怖主义活动等。

比特币的出现对暗网的非法交易起到了很大的推动作用，也在2011年直接催生了暗网第一个著名黑市，Silk Road (丝绸之路)。丝绸之路每年的交易额保守估计在4,000万美元左右。但好景不长，美国 FBI 于2013年查封了丝绸之路，逮捕了其创始人 Ross Ulbricht，并没收了14.4万枚比特币（当时价值2,800万美元）。

不过，很快 Silk Road 2.0 版就又出来了，它在被关闭之前的总交易量甚至达到了惊人的12亿美元。此后又有 AlphaBay 和 Hansa 等黑市相继问世。



图九 Dream Market比特币混币服务页面

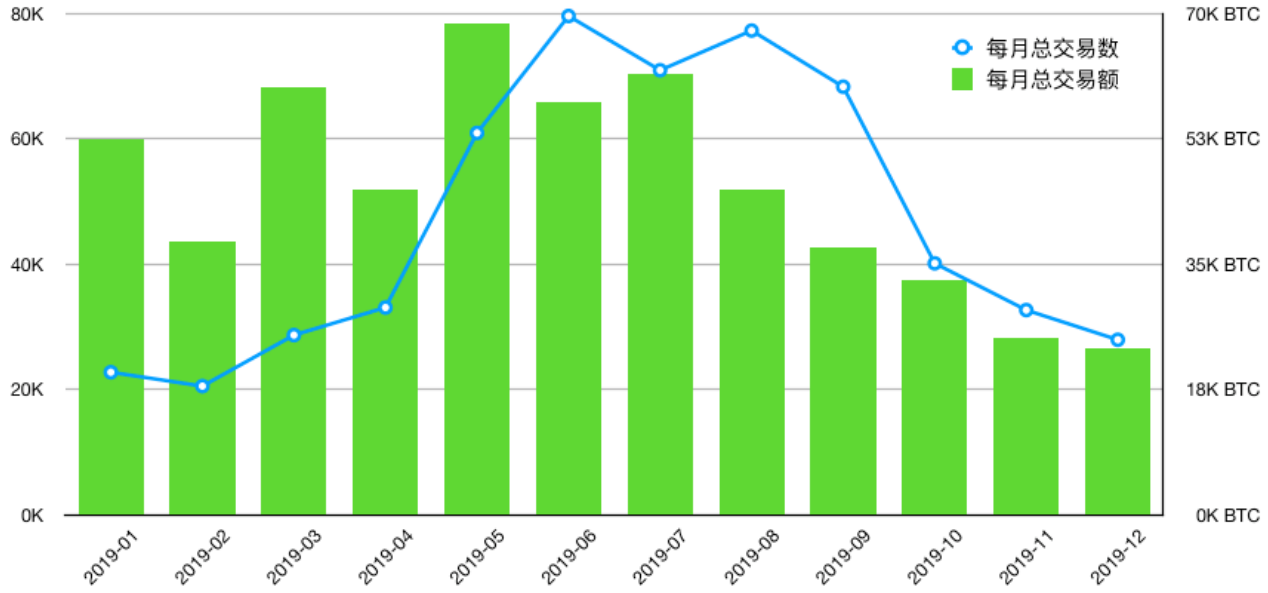
野火烧不尽，春风吹又生。旧的黑市不断被关闭，新的黑市又不断涌现出来，由于非法交易的需求持续存在，暗网市场很难被彻底封杀，反倒其交易规模还在不断扩大。图九是目前还在经营的一个大型黑市，Dream Market，页面展示的是它提供的一个比特币混币服务。

3.1 暗网比特币交易规模

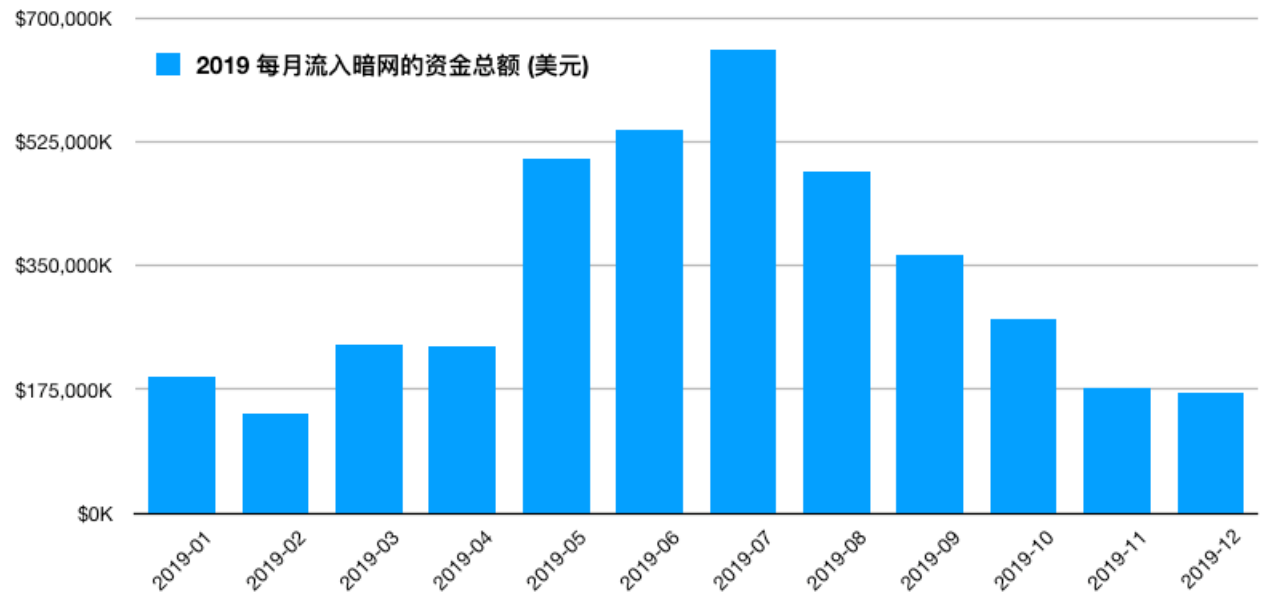
为了统计暗网中比特币的交易规模，我们部署了多个暗网数据爬虫工具，在数百万网页中寻找比特币地址，并分门别类存入数据库，形成了暗网比特币地址库。再和我们已有的海量比特币地址标签进行比，最终得到几千个在暗网从事交易的比特币地址。然后结合我们的公链交易数据库，可以得出比特币在暗网的交易规模数据。

我们的研究结果显示，在2018年共有334,329个比特币流入这些地址；2019年

增加到了546,825个，按交易时价计算，总额分别为21亿美元和39亿美元。图十是2019年每个月这些暗网地址的交易数和流入的比特币总数，图十一是按交易时价计算，2019年每月流入这些地址的美元总额。



图十 2019年每月流入暗网的交易数和交易额



图十一 2019年每月流入暗网的资金总额

从这些数据可以看出，比特币在暗网中的交易规模相当巨大，虽然这不是比特币的主要用途，但它也是比特币交易的一个重要部分，而且其规模还是不断扩大中。还有一个维度的数据，从暗网向各大数字资产交易所直接流入的资金规模，我们将在下一章给出。

4. 未受监管的全球数字资产流向

区块链技术自比特币2009年诞生以来，至今已有十年的发展历程。各国政府和各个国际金融监管机构也从最初的模糊处理过渡至较清晰的尝试监管阶段。

整体而言，所有国家和监管机构都认为区块链是一门新兴技术，并表示接受和支持。然而，对以比特币为代表的数字资产应用，各国态度不一，支持、中立、反对的国家都有。比如，日本承认比特币为合法货币；美国认为比特币是一种商品，并非证券，不能按证券标准纳入监管；中国则禁止比特币等数字资产在交易所的公开买卖行为。

本章我们将概述各个国家和机构对数字资产的监管和合规要求，提供未受监管的资金在国家间的流动情况，以及暗网资金流入各大交易所的数据情况。

4.1 国际机构和各国政府对数字资产的监管和合规要求

世界上最重要的国际金融监管机构是 FATF (Financial Action Task Force)，它是一家总部位于巴黎，专门做反洗钱和打击金融恐怖主义的机构，有39个成员国。2018年10月，FATF 声明它的监管规则同样适用于虚拟资产 (VA, Virtual Asset) 和虚拟资产服务提供商 (VASP, Virtual Asset Service Provider)，包括数字资产交易所和数字钱包等。

2019年6月，FATF 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，并给出了实施时间表。INR15 规定各国和 VASP 必须在一年以内，也就是2020年6月以前，开始执行 FATF 的监管要求。二十国集团 (G20) 已表示支持这一决定。

INR15 最核心的一项要求就是 “Travel Rule”, 它要求所有超过1000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。

这项规定对 VASP 是一项巨大挑战，意味着数字资产交易所等机构要在不到一年的时间内建立起完整的 KYC 和大额交易监控和汇报机制，与此同时，还要克服对没有 KYC 的地址进行溯源等技术难题。

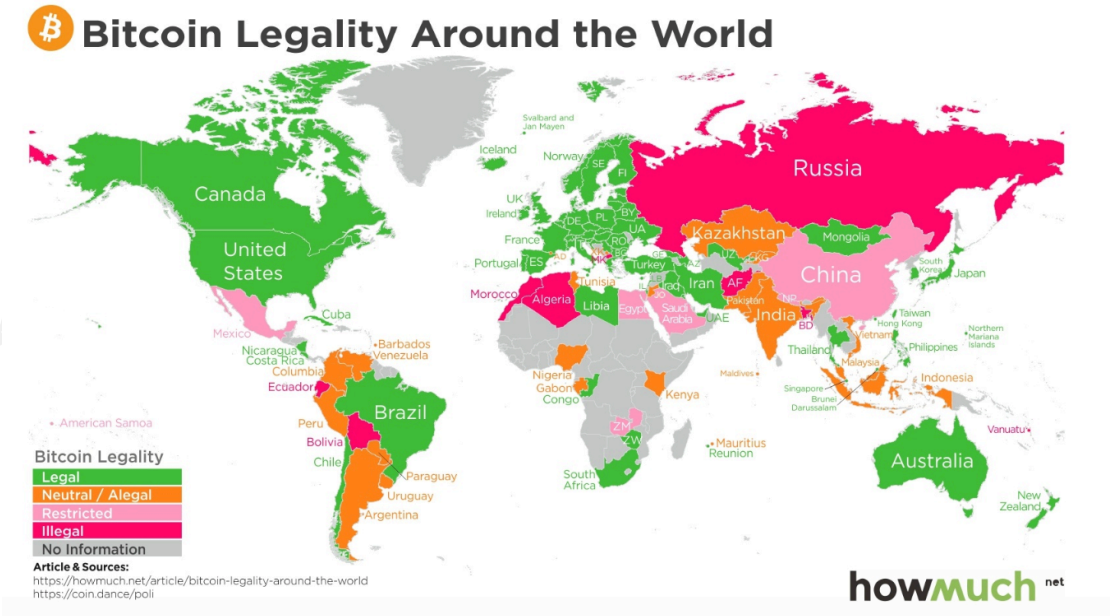
各个国家对区块链和数字资产的态度也不尽相同。美国是区块链技术的主要研发中心，世界上大约1/4的区块链公司都位于美国，美国政府也积极鼓励和推

动区块链技术的创新和发展。但是，美国对数字资产态度相对保守，对 ICO 等融资项目监管非常严格。美国证券委员会 (SEC) 认为比特币、以太币等主流数字资产不是证券，仅可以作为商品流通和交易。如果一种数字资产被 SEC 认定是证券，那它现阶段基本不可能在美国流通。所以，很多交易所，发币机构和 ICO 项目都不对美国公民开放，以避免来自美国政府的监管。

日本政府对区块链和数字资产则非常支持。早在2017年4月，日本就通过“Payment Service Act”，确立了比特币作为一种货币和支付手段的合法地位。长期以来，日元对比特币的交易量经常超过比特币交易量的一半，日本金融和技术公司在区块链业界也非常活跃。然而，日本并没有对 ICO 等融资项目明确立法，目前这些项目在日本尚属于未被监管的灰色地带。

中国政府支持区块链技术的发展，但禁止数字资产在交易所公开买卖。中国香港对区块链技术也持有支持态度，其证券委员会曾发布了 “沙盒规则” (Regulatory Sandbox)，允许一些公司在数字资产领域作一些尝试。

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。图十二来自 howmuch.net, 它列出了世界各国对比特币不同的接受程度。



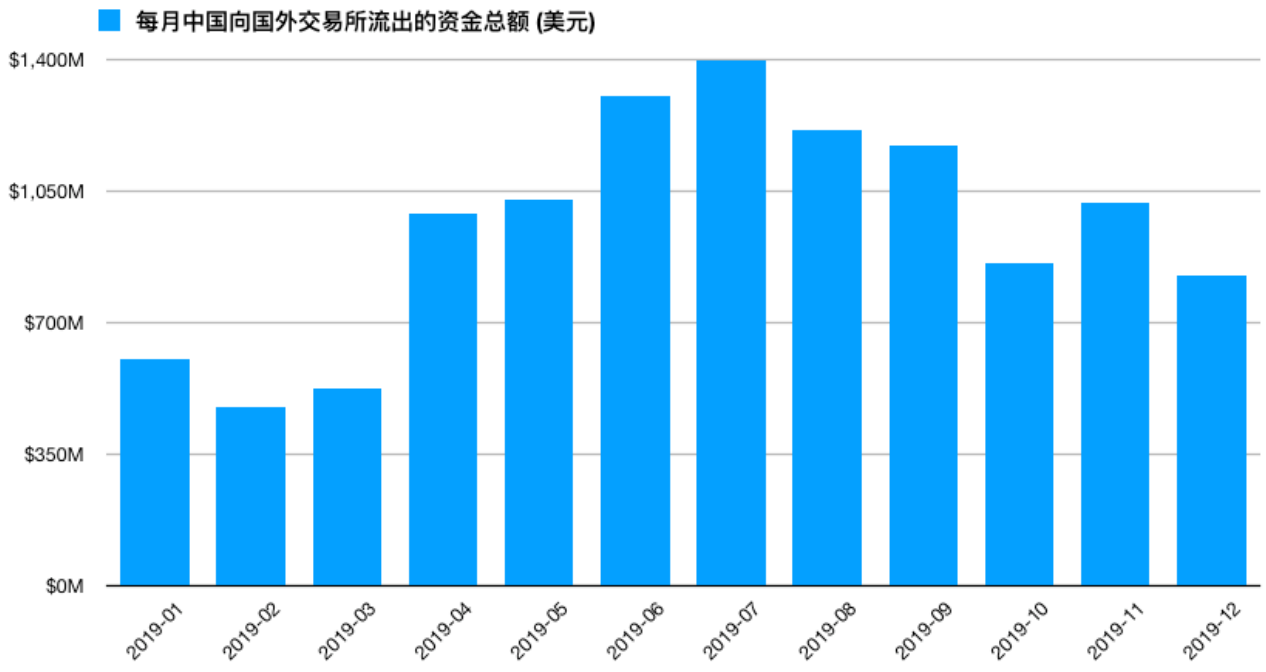
图十二 比特币在各国的合法性

长远来看，数字资产一定会被纳入各个国家和金融机构的监管范围之内。那么，现阶段有没有监管的必要呢？这就需要定量分析一下目前未受监管的数字资产在国家间的流动量，以及它被用作非法交易支付工具的规模。在以下两节，我们将展示一下比特币在不同国家间的流动和用于非法交易的情况。

4.2 未受监管的国家间资金流动情况

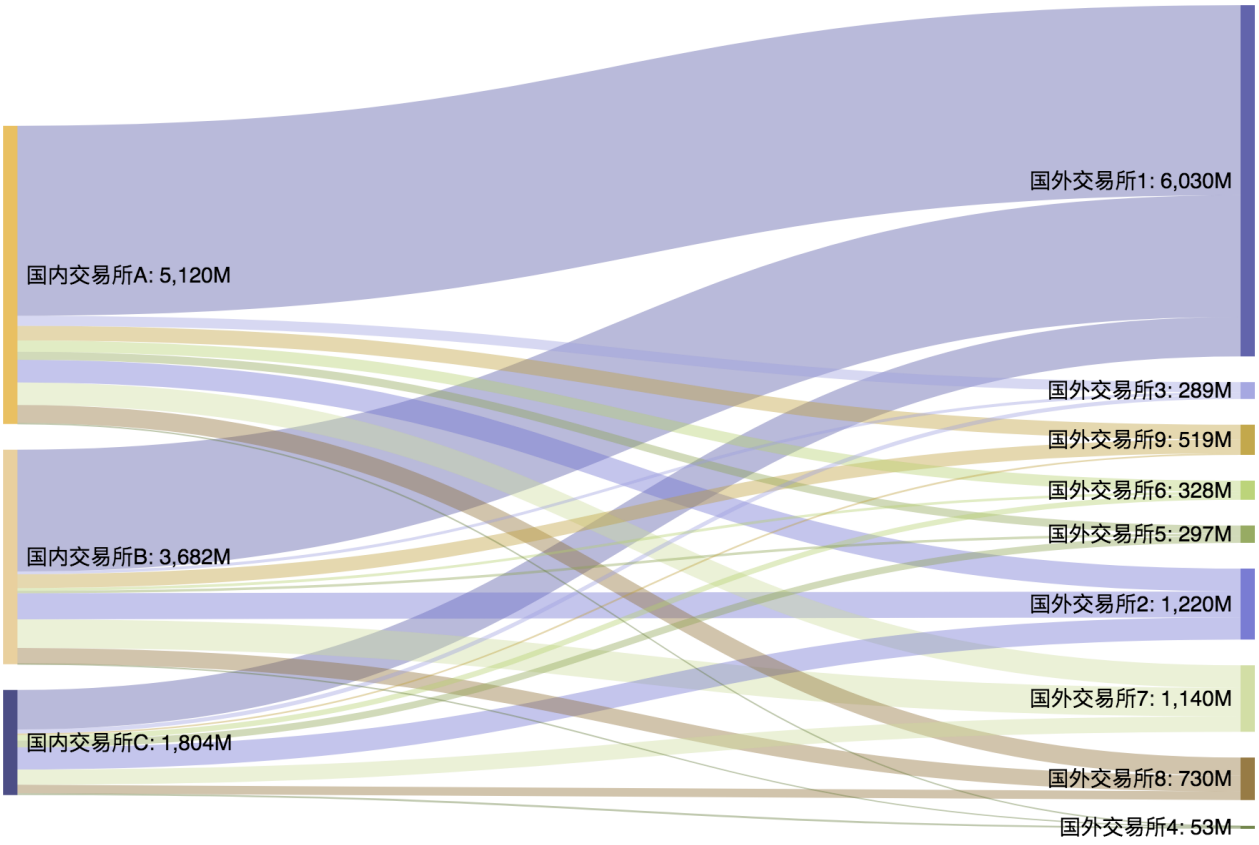
我们积累了海量的交易所地址标签和各大公链的交易数据。在此基础上，我们可以分析各主要交易所的每天的资产余额以及交易所之间的资产流动情况。而注册在世界各地的交易所有着不同的用户群体，某种程度上，交易所可以和国家产生一些对应关系，分析一些交易所之间的资金流动，基本等于数字资产在不同国家之间的流动。

例如，在世界主要交易所的行列中，我们可以用主要用户分布于中国内地和香港的三大交易所来代表中国，用其他各大交易所代表国外，通过分析这些交易所之间的资金流动情况，我们计算出了目前未受监管的资金从国内流向国外的流通量。



图十三 2019年每月从中国向国外流出的资金量

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[9] 的1%。



图十四 2019年从中国向国外各大交易所流出的资金总量

图十三是按月计算，2019年从中国流出到国外的资金量；图十四是按交易所统计，2019年从中国交易所流出到国外交易所的资金总量。

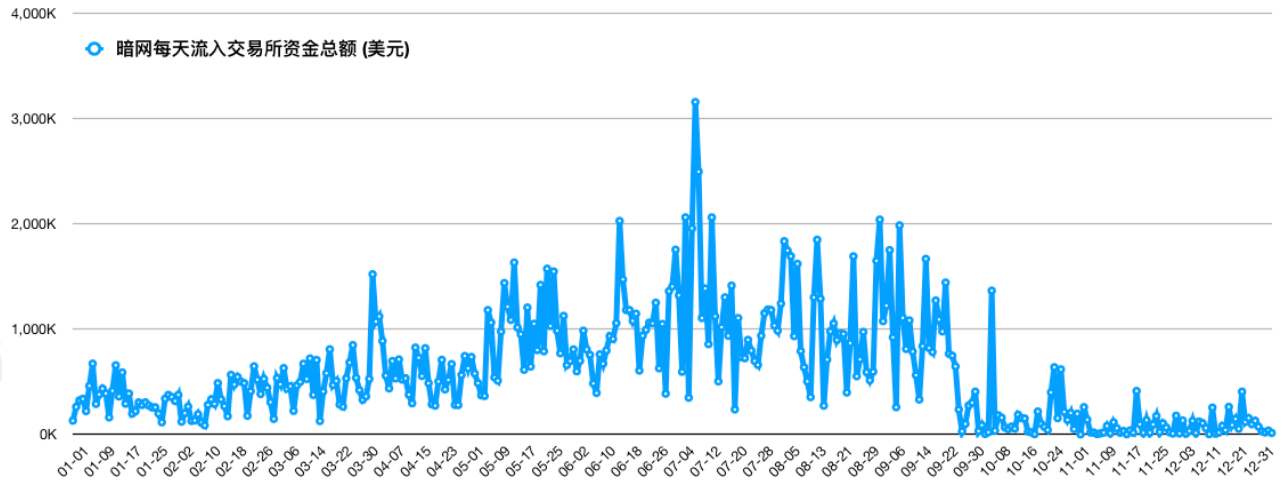
需要注意的是，我们只是以几个大的交易所来代表整个国家，所以统计数据只是一个保守的估计，实际的资金流动量会大于我们所统计的数据。即便这样，我们发现每年通过交易所流出的资金也相当巨大，超过了百亿美元。作为参照物，2018年中国对外直接投资的总额为1,430亿美元 [10]。

我们的这项研究，包括了以下主要头部交易所的数据：火币，OKEx，Bitfinex，Binance, Bitflyer, Bitmex, Bitstamp, Bittrex, Coinbase, Coincheck, Gate.io, Kraken, Poloniex, 和 Upbit 等主流数字资产交易所。

4.3 暗网流入各大交易所的资金量

在暗网进行的非法交易中，比特币至今仍最主要的支付工具。这些比特币中的一部分会被转移到交易所洗白，或换成法币及其它数字资产。经 PeckShield 研究发现，2019年从暗网直接流入各大交易所的比特币总数为29,471.64个，按交易时价计算总值为2.16亿美元。

图十五所示为2019年每天从暗网流入交易所的资金量。需要注意的是，暗网中的比特币只有一小部分会直接流向交易所，但2019年超过2亿美元的总资金量也足以表明反洗钱监管的必要性。



图十五 2019年每天从暗网流入交易所的资金量

5. 结论

本报告基于 PeckShield (派盾) 的研究成果，全面梳理了区块链上非法和未受监管的交易现状。PeckShield 通过对各大公链链上数据，地址标签的长期积累，并借助 CoinHolmes 可视化资产路径工具对这一领域进行了系统的研究。从报告中的数据规模来看，非法交易还普遍存在于区块链交易中，未受监管的数字资产交易总量也已经不容忽视。

本报告深入分析了以下三个方面的数据：

重大安全事件和损失情况：2017年共发生重大安全事件11起，共计损失2.94亿美元； 2018年共发生重大安全事件46起，共计损失47.58亿美元。2019年共发生重大安全事件63起，总共损失达到了76.79亿美元。

整体而言，过去三年以来，区块链生态安全事件所引起的损失额呈逐年攀升态势。但安全事件的重灾区在不断交替，从最初交易所和智能合约的问题，再到 DApp、DeFi 等离钱近的领域，今年以来各类理财钱包诈骗又成了行业新的隐患。总结下来，黑客会始终朝着安全薄弱的领域发起攻击，开发者务必在各个环节加强安全防御。

暗网市场交易规模：2018年流入暗网的比特币总数为33万枚，2019年为54万枚，按交易时价计算，总金额分别是21亿美元和39亿美元。

整体而言，暗网比特币流通一直处于相对稳定的量，这是由于其市场需求决定的。随着数字资产市场监管的迫近，交易所该如何规避暗网市场的资金污染，成了行业亟需处理的难题。

国际间未受监管资金流动情况：2017年通过数字资产从中国流到国外的资金总量为101亿美元，2018年为179亿美元，2019年为114亿美元，三年总额超出中国3万亿美元外汇储备的1%。

整体而言，从数据可以看出目前未受监管的资产流动已经占据相当大的市场份量，到了监管机构亮明态度进行监管的时候了。对数字资产交易所而言，加速合规化也成了迫在眉睫的事情。

参考文献

[1] Wikipedia：Silk Road, https://en.wikipedia.org/wiki/Silk_Road_(marketplace)

[2] ambcrypto.com：Bitcoin use for illicit activities, https://eng.ambcrypto.com/bitcoin-use-for-illicit-activities-is-only-2-while-21-transactions-are-lawful-and-77-are-unclassified/

[3] PeckShield：图文追踪PlusToken资产转移行踪 (一) https://www.8btc.com/media/440193

[4] PeckShield：图文追踪PlusToken资产转移行踪 (二) https://www.8btc.com/media/465386

[5] PeckShield：图文追踪PlusToken资产转移行踪 (三) https://www.8btc.com/media/473062

[6] PeckShield：图文还原币安被盗7,074枚BTC转移全过程 https://www.8btc.com/media/407207

[7] PeckShield：图文剖析Cryptopia交易所黑客洗钱行踪 https://www.8btc.com/media/415453

[8] Wikipedia： TOR network, https://en.wikipedia.org/wiki/Tor_(anonymity_network)

[9] 中国政府网：中国外汇储备规模，http://www.gov.cn/shuju/2019-12/09/content_5459549.htm

[10] 新华网：我国已成为第二大对外投资国，http://www.xinhuanet.com/money/2019-09/16/c_1124999299.htm

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。

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。