PeckShield

数字货币
反洗钱研究报告

2020年度报告

PeckShield（派盾）

2021年1月

目录

一、研究背景综述

2020年数字货币市场迎来迸发式增长，在新冠疫情的蔓延、美国大选以及原油价格暴跌等多重因素的影响下，数字货币的投资价值开始凸显。特别是下半年星展银行、Visa、PayPal 等传统金融巨头的加持，DeFi 等金融创新产品引领的市场狂热，再次激发起参与者的热情。

纵观全球，各主要国家都在加速布局区块链技术和央行数字货币，与此同时，监管也在不断地强化和推进。国内一批与虚拟货币相关的诈骗、勒索案件告破，政府严打电信诈骗和赌博，导致加密资产行业迎来“冻卡潮”[1]。此外，OKEx、火币两大交易所接连配合调查。另一方面，矿业在四川有合规化趋势，交易所合规化监管要求不断落地，行业格局开始出现变化。

回顾2020年，「监管」、「合规」成为数字货币行业绕不开的话题，而反洗钱则是当前监管最核心的目标之一。

1.1 传统金融巨头开始拥抱数字货币

2020年3月，币安交易所（Binance）宣布推出「币安卡」，支持 Visa 支付渠道，使用该卡的用户可以在全球 200 多个地区的超过 4600 万户 Visa 商家（线上和线下）使用数字货币进行支付。

9月，美国支付巨头 PayPal 宣布推出比特币买卖功能。PayPal 宣布正式支持四种加密货币服务未满 1 个月，其交易额已超过币安美国的 65%。与此同时，美国的其他主流金融科技公司，例如移动支付提供商 Square 公司和股票交易应用程序公司 Robinhood，也都允许用户购买和出售数字货币。

10月，新加坡最大的商业银行——星展银行（DBS）宣布启动数字交易平台 DBS Digital Exchange。平台支持 BTC、BCH、ETH 和 XRP 这四个代币的法币（SGD，HKD，JPY，USD）交易。同时，相关合规企业还可通过该平台进行融资，允许企业将其证券或资产转变为数字货币。DBS 数字交易平台不持有任何数字货币，所有数字货币都存放在星展银行（DBSBank）。

2020年，传统金融巨头开始拥抱数字货币，一方面使得数字货币引起社会更广泛地关注，另一方面传统金融巨头因其更合规和安全的管理和运营，增强了主流数字货币的普世性

和可信度。而反过来，数字货币交易所面临监管和传统巨头的双重压力，行业格局开始发生变化。

1.2 数字人民币领跑全球 中国加强虚拟货币监管

国内方面，2020年4月区块链被正式纳入我国「新基建」范围，位列新型基础设施中的信息基础设施。与此同时，我国央行数字货币（DC/EP）试点加速推进。10月在深圳试点「数字人民币钱包」，随后在苏州开展大规模的 DC/EP 支付系统试点。12月29日，北京首个央行数字货币应用场景落地丰台丽泽，获得授权的消费者可以使用数字人民币钱包支付购买各类商品。

国际方面，2020年1月，日本央行与英国央行、瑞士央行、瑞典央行、加拿大央行以及欧洲中央银行和国际清算银行（BIS）于成立工作组，进行央行数字货币联合研究。2月，美联储委员会理事莱尔·布雷纳德（Lael Brainard）表示，美联储正在研究围绕数字支付和数字货币的相关问题，包括可能发行数字货币的政策、设计和法律等事项。

无论是技术层面还是金融应用领域，我国都展现出在央行数字货币研发、应用、普及上全面领跑世界的壮志雄心。其他主流国家虽然发出对央行数字货币的积极态度，但仍处于探索阶段。

随着区块链核心技术被上升到国家战略高度，公众对区块链领域也愈发关注，各式骗局亦应运而生，而其中以「区块链」概念包装的「资金盘」、「杀猪盘」层出不穷。针对挂靠「区块链」概念的骗局，国内相关执法部门收紧对虚拟货币活动的监管，展开排查、追溯、冻卡等行动，并已初现成果。

9月，在第九届中国支付清算论坛上公安部国际合作局局长廖进荣指出，每年自中国境内流出涉赌资金超出一万亿元，特别点名虚拟货币被用于转移赌资。在近期的案件当中，执法部门发现部分涉赌团伙利用虚拟货币收集转移赌资，甚至在缅甸部分地区以虚拟货币投资为由，行网络赌博之实。这类新型虚拟货币流转通道通常不可冻结，匿名难以溯源，给打击治理工作带来了很大的挑战。

10月，在全国范围内开展「断卡」行动，严厉打击整治非法开办贩卖电话卡、银行卡违法犯罪。随着「断卡行动」和「反洗钱法」的生效，传统洗钱渠道遭遇沉重打击，虚拟货币越来越受到犯罪分子的喜爱，越来越多的非法资金开始通过虚拟货币洗钱。据中国检察网数据显示，2020年来已经有 85 例与 USDT 关联的犯罪案件，而在2020年之前只有 5 例。数字货币洗钱案件呈高发趋势。

随着虚拟货币洗钱案件愈来愈多，监管压力开始落实到交易所主体。10月，OKEx 交易所创始人接受警方调查，导致OKEx 无法提币长达一个月。11月，火币Huobi 交易所高管也开始接受警方调查。

1.3 全球主要国家逐步推进数字货币合规化运营

2020年1月10日，欧盟第五项反洗钱指令（5AMLD）正式生效，5AMLD 旨在阻止不法分子通过「信用卡匿名支付」或「虚拟货币交易所平台」进行洗钱或为恐怖主义融资，值得注意的是，该指令首次将监管范围扩大到包含虚拟货币交易所和托管钱包供应商在内的加密服务供应商，以反洗钱和反恐怖主义融资的名义获取加密交易的参与者的信息。

1月10日，英国金融行为管理局（FCA）宣布，将根据修订后的《反洗钱、反恐怖主义融资和资金转移条例》对所有从事虚拟货币经营活动的英国企业展开监管。

1月28日，新加坡《支付服务法》（PSA）正式生效，将虚拟货币纳入 MAS 的监管范围下，并规定数字支付令牌（DPT）服务提供商（涉及新加坡绝大多数数字货币相关企业）需遵守严格的反洗钱和恐怖主义融资新规。新规引入反洗钱要求清单，同时还针对国际组织「反洗钱金融行动特别工作组」（FATF）的《转移规则 Travel Rule》向本地 DPT 做出特别要求，包括 KYC 流程（包含受益所有权在内）、账户审查措施以及对可疑交易的监控和报告。

由社交媒体巨头 Facebook 牵头的虚拟货币项目 Libra（天秤币）在美国监管压力下，于12月2日更名为 Diem，计划将于2021年1月发行。Diem 更改为锚定美元的稳定币方案。

2020年，全球主要国家开始落地对虚拟货币的监管，但由于主流的虚拟货币如 BTC、ETH、USDT 等具有天然的无国界性，使得虚拟货币未纳入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，该虚拟货币在其他国家依然能有流通空间，这提高了监管介入的门槛。

二、研究方法和工具

2.1 研究方法论

PeckShield（派盾）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。

过去三年，PeckShield（派盾）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。

工具库分为如下六个主要部分：

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，生成了总数超过一亿的地址标签库，基于此展开后续一系列的虚拟货币汇总和溯源分析；

3）风险量化体系：

我们独有的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，通过模型进行风险评估。通过这套引擎，我们曾成功的发现一系列高风险交易，以及和不明实体的关联地址。并能在高风险交易发生时，第一时间感知，通知交易所及合作伙伴；

图1 风险量化评估流程示意图

4）Cerberus智能追踪工具：

Cerberus 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。Cerberus 工具可以追踪 BTC、ETH、USDT、USDC 等 20 多种主流虚拟货币；

5）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。该系统支持网站登录和使用，同时开放API给合作伙伴；

6）虚拟货币反洗钱态势感知：

CoinHolmes 提供一整套完整态势感知服务，协助警方掌握已知实体间的敏感转账信息，自动追踪敏感资金动向，各类犯罪资金的分析统计，以及实时区块链安全事件预警。

图2 虚拟货币反洗钱态势感知系统截图

2.2 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（派盾）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（派盾）并非投资顾问、经纪人或交易员，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。

三、未受监管的虚拟货币跨境流出现状

自2009年比特币诞生以来，尤其「丝绸之路」[2]利用比特币在其线上集市交易非法商品及服务，虚拟货币成为暗网经济的首选资产。由于虚拟货币具备不可撤回、不可审查的特性，容易被用于非法买卖外汇、洗钱、勒索等，因此各国正逐步加强对于比特币等虚拟货币的监管。

人民网[3]文章指出以支付人民币的方式在境内买入虚拟货币，再通过任何形式卖出提现为外币，或者持有人以支付外币的方式在境外买入虚拟货币，再通过任何形式卖出提现为人民币，无论买入与卖出之间经过多少次币币交易转换，其本质上违反了中国外汇管制相关规定并涉嫌洗钱犯罪。

金融行动特别工作组（FATF）执行秘书兼 G20 代表 David Lewis 曾公开表示，G20 一致认为，支付系统必须更新，虚拟货币可以在其中发挥作用，所发布「旅行规则」（Travel Rule）在内指南只是监管迈出的第一步，FATF 不会容忍一些国家在立法中留下漏洞，允许虚拟货币公司绕过旅行规则和其他反洗钱协议。

据 PeckShield（派盾）研究发现，取证难、追踪难仍是司法机关攻克涉及比特币等虚拟货币的洗钱案件难点，由于比特币具有匿名性，它仍是目前暗网选择最多的虚拟货币，其次是门罗币和莱特币。

3.1 未受监管的国家间资金流动情况

CoinHolmes 结合已有的 1 亿地址标签，对包括资金盘地址、暗网地址、赌博地址等多种高风险地址进行追踪、监控时发现，这些黑产地址和交易所地址存在频繁的交互行为。CoinHolmes 将此类高风险地址资产，流入流出交易所行为定义为「可疑资产」流入流出。

我们基于 CoinHolmes 的数分析了各主要交易所每天的资产余额以及交易所之间的资产流动情况。由于注册在世界各地的交易所拥有不同的用户群体，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，基本等于虚拟货币在不同国家之间的流动。

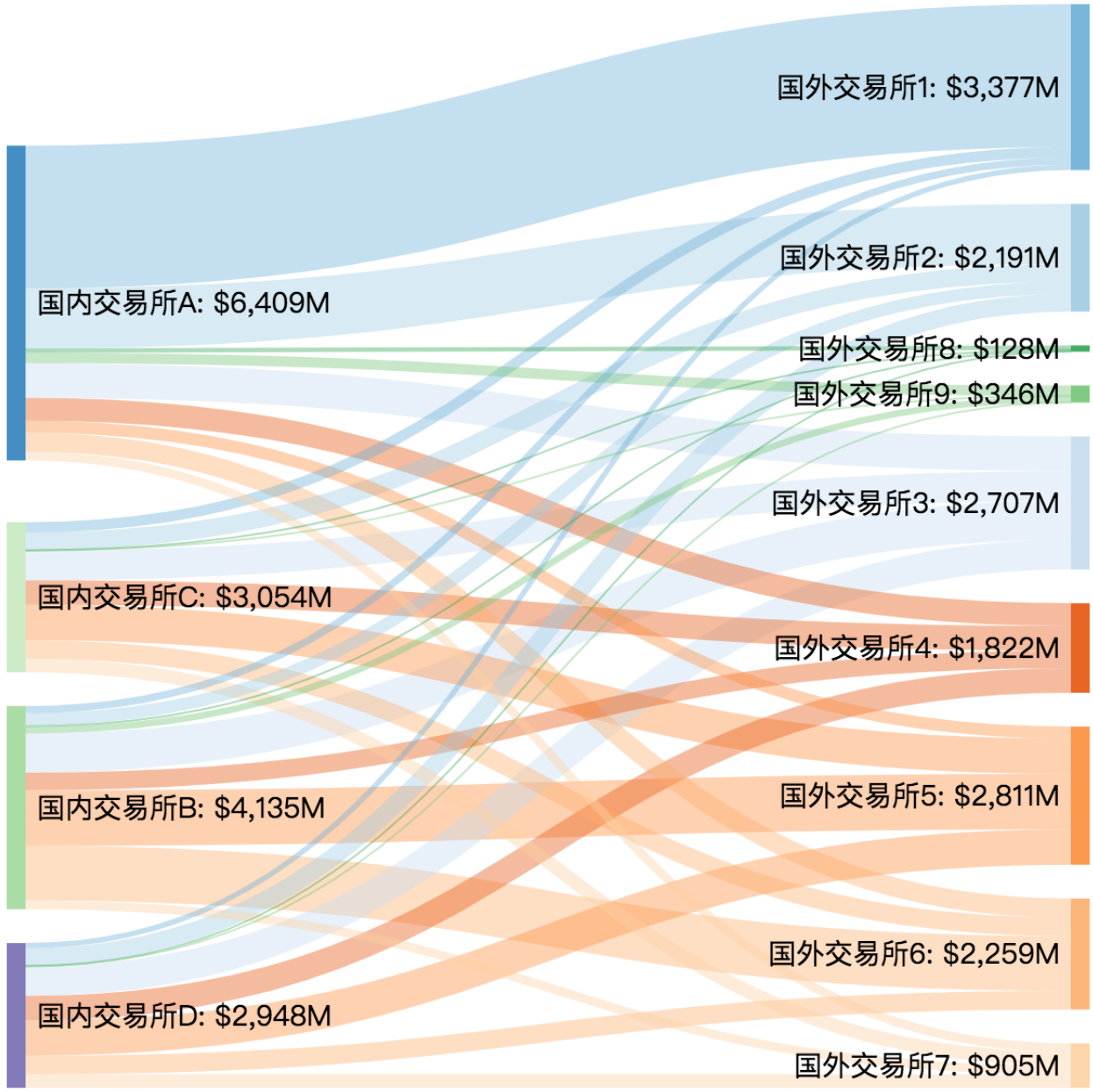

图3 2020年从国内交易所流出到国外交易所的资金总量

如图3所示，在世界主要交易所中，我们用主要用户群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，计算出目前未受监管的资金从国内流向国外的流通量。

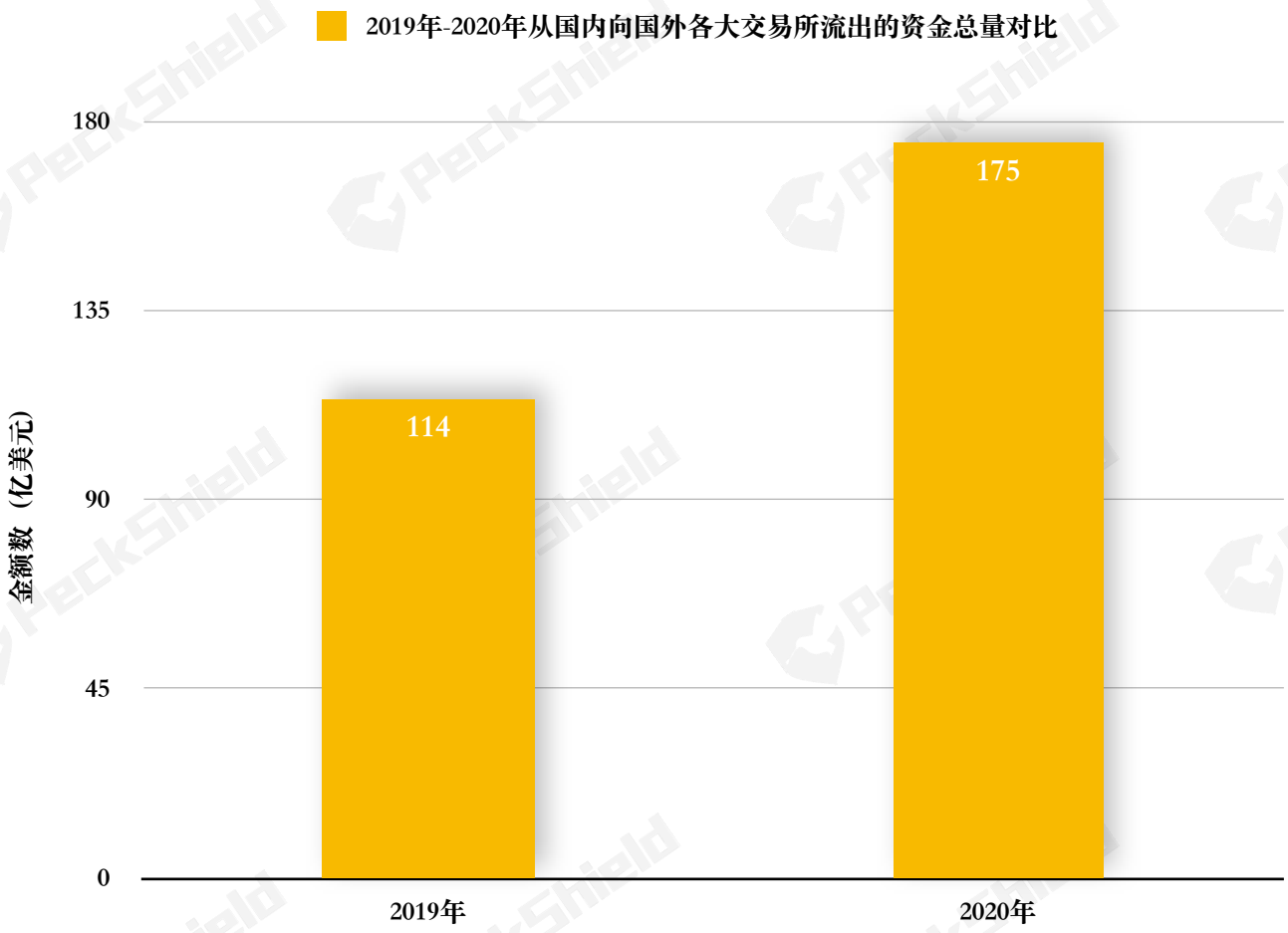

图4 2019-2020年从国内向国外各大交易所流出的资金总量对比

2020年从中国交易所流出到国外交易所的资金总量达到 175 亿美元。以 BTC 为例，按交易时价计算，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1.5%[4]。

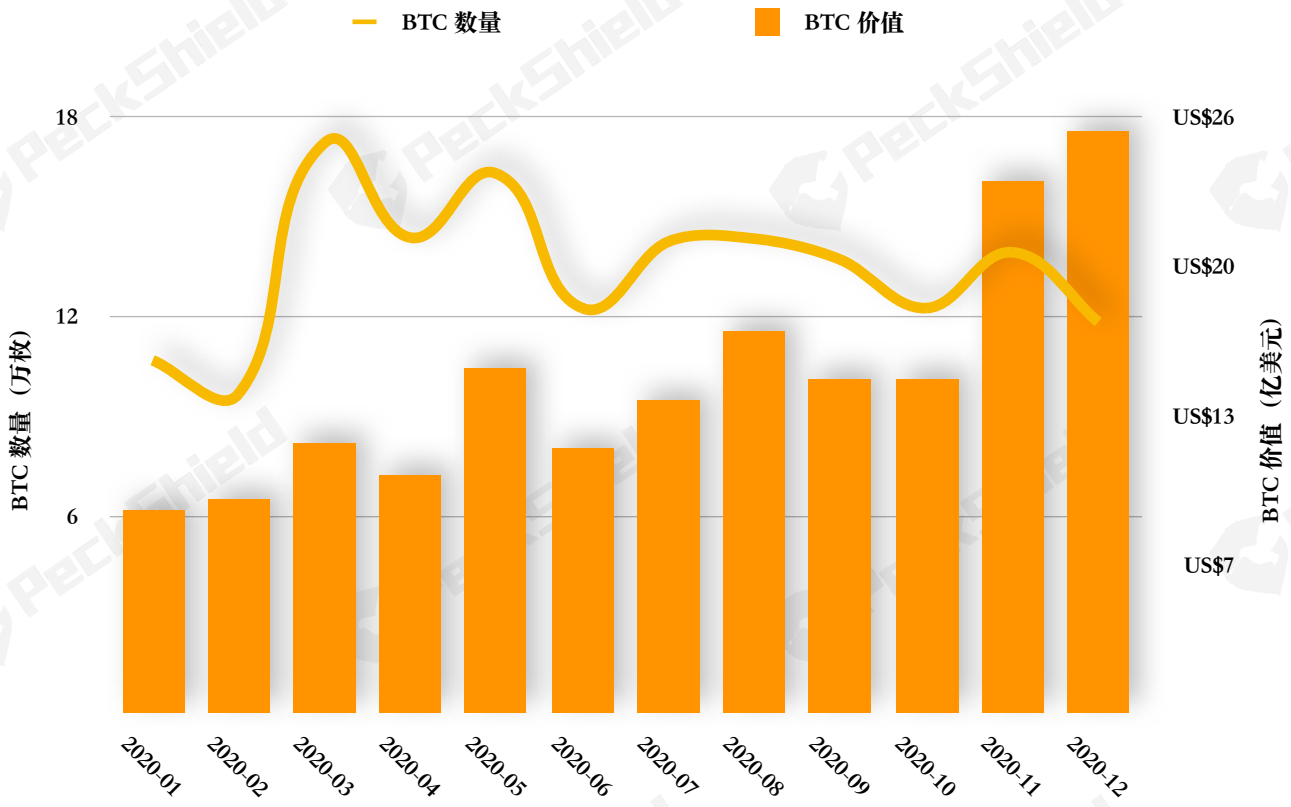

图5 2020年从国内向国外各大交易所流出的资金总量

如图5所示，今年3月从国内流到国外的比特币数量最多，达到 172,115.39 枚；今年12月从国内流到国外的比特币价值达到全年最高，逾 25 亿美元，这是由于自11月24日起，比特币单价屡破新高，先是站上 20,000 美元，随后突破 30,000 美元关口。

值得注意的是，我们以几个大的交易所为研究样本来分析全球交易所「可疑资产」流向的趋势，所以所得统计数据为保守估计值，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。

我们的这项研究的研究样本，包括以下主要头部交易所的数据：火币、OKEx、Bitfinex、Gate.io、ZB、 Kucoin、Bibox、币安Binance、Bitstamp、Bittrex、Kraken、Coincheck、Coinbase、Poloniex、Bitflyer 和 Upbit 等主流虚拟货币交易所。

3.2 暗网流入各大交易所的资金量

在暗网进行的非法交易中，比特币至今仍是最主要的支付虚拟货币。这些比特币中的一部分会被转移到交易所洗白，或转换成法币及其它虚拟货币。经 PeckShield（派盾）研究发现，2020年从暗网直接流入各大交易所的比特币总数为 213,431.6 枚，按交易时价计算总值为 2881.6 万美元（如图6所示）。

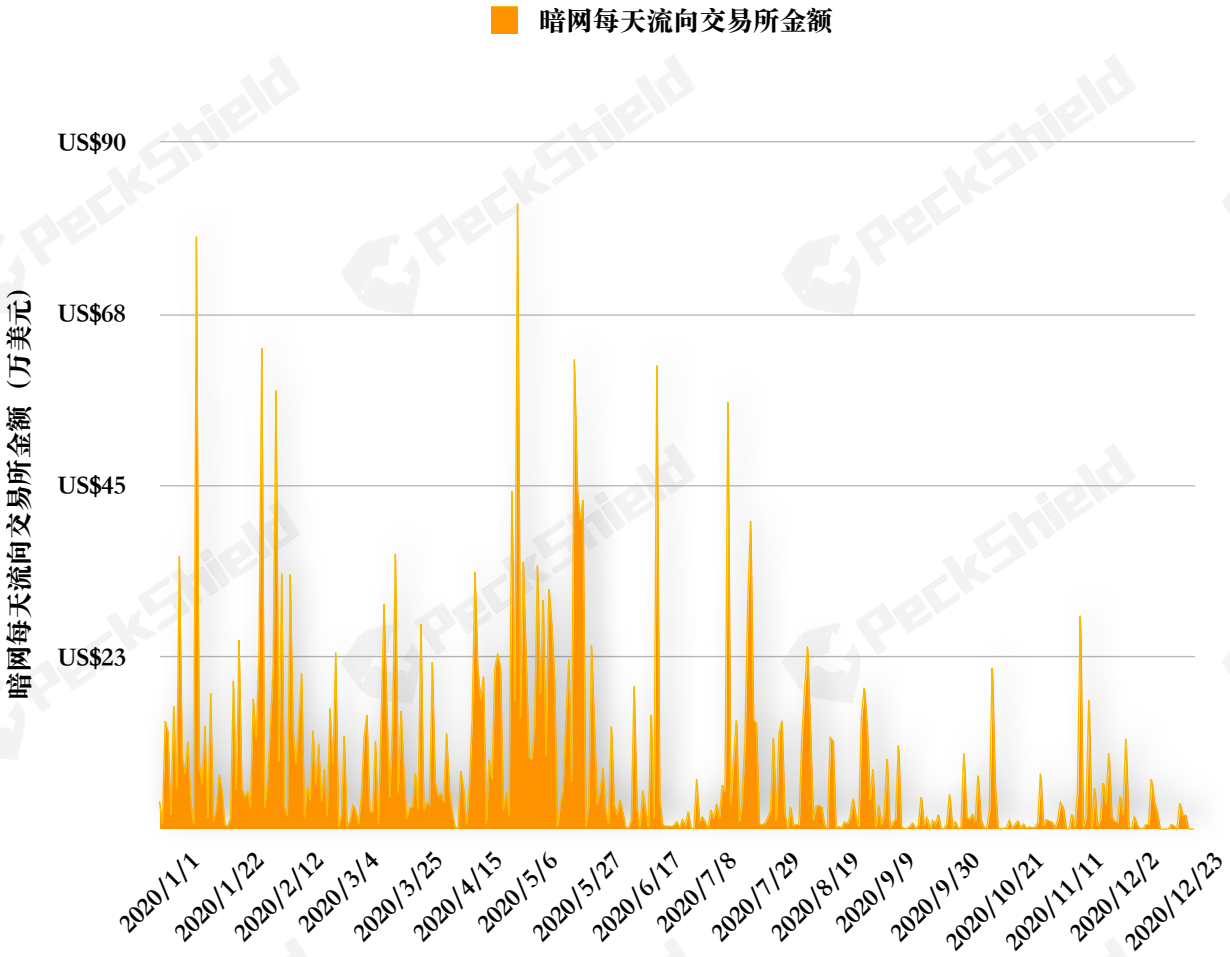

图6 2020年每日从暗网流入交易所的资金量

值得注意的是，暗网中的比特币只有一小部分会直接流向交易所，但通过中间地址转入交易所的这部分未被统计在内。需要指出的是，目前统计的直接转入金额近 3 千万的总资金量，也表明虚拟货币反洗钱态势依旧严峻，监管亟待加强。

四、虚拟货币重大安全事件概览

4.1 虚拟货币安全事件总体统计

2020年虚拟货币行业共发生重大安全事件 461 起，共计损失近 55 亿美元，其中黑客攻击逾 170 起，诈骗事件 151 起，勒索攻击近 140 起。

如图7所示，2018年至2020年虚拟货币安全事件统计，2020年较前两年勒索事件骤增，2018年欺诈事件仅 4 件，2020年则逾 150 件，较2019年增长了 7 倍，黑客攻击事件较2019年增长了 4 倍。虽然各国政府正在加强与虚拟货币相关的反洗钱、反欺诈政策，但新型欺诈、攻击事件仍层出不穷。

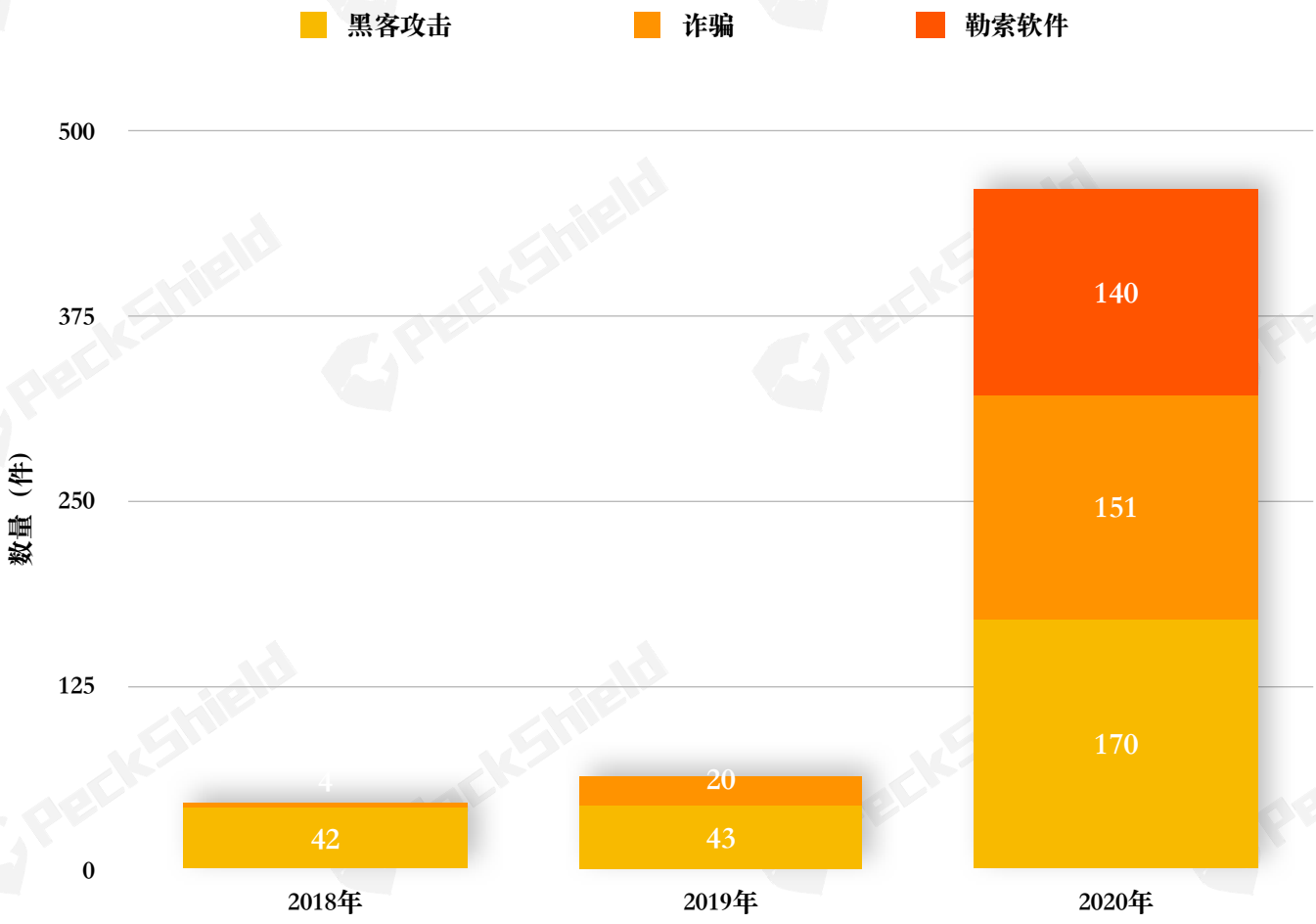

图7 近三年虚拟货币安全事件统计

2018年虚拟货币安全事件造成的损失高达 47.58 亿美元，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，勒索攻击损失 524 万美元。

2019年虚拟货币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，诈骗事件造成 73.73 亿美元损失，勒索攻击 55 万美元。

2020年虚拟货币安全事件造成经济损失逾 55 亿美元，较2019年下降 39.6%，黑客攻击造成 21.3 亿美元的损失，其中 DeFi 安全事件造成 2.55 亿美元的损失，诈骗事件造成 31.3 亿美元的损失，勒索攻击造成 一千万美元的损失。

4.2 2020年虚拟货币安全事件统计分析

2020年造成主要危害的是诈骗和洗钱事件，如图8所示，在与虚拟货币相关的安全事件中，诈骗事件逐年增长，2020年达到 151 件，较2018年增长了 37 倍，较2019年增长了 4 倍。在诈骗事件中除了挂靠「区块链」的资金盘，「杀猪盘」也蔓延至虚拟货币领域。值得注意的是，黑客攻击兴起的 DeFi 攻击事件和企业勒索在今年呈现爆发的趋势。

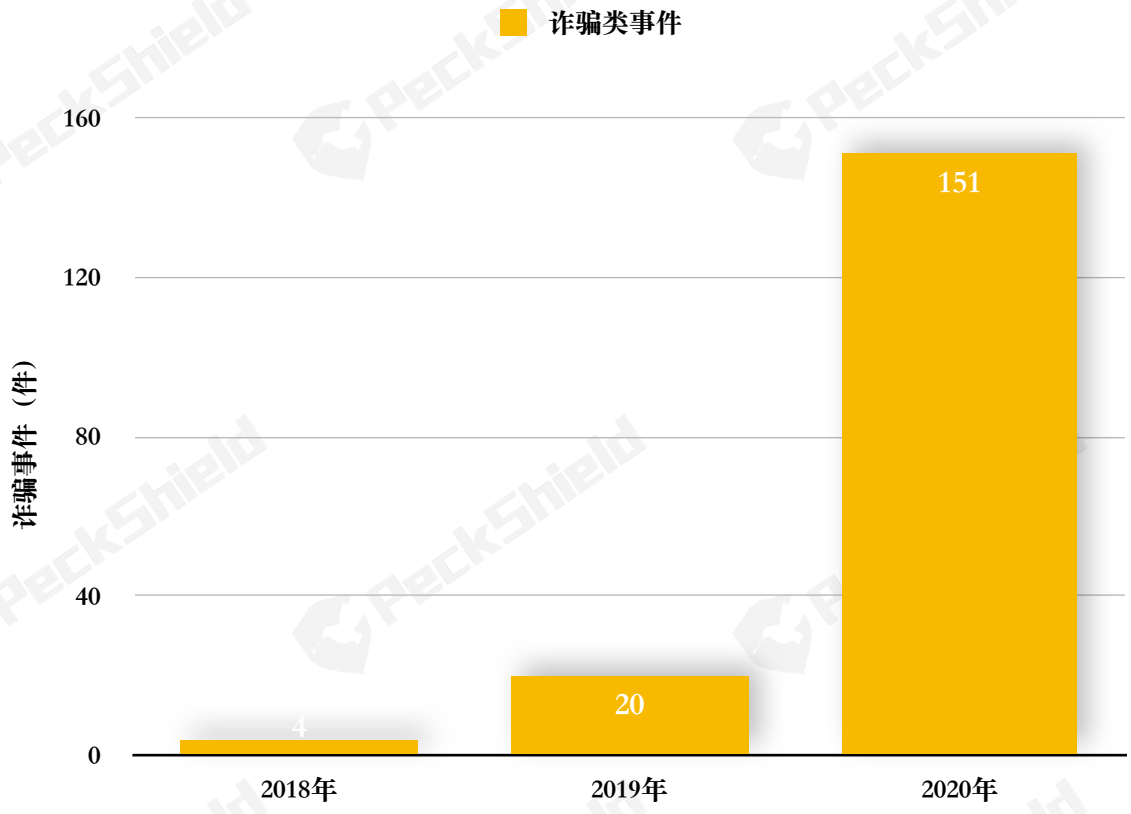

图8 诈骗类安全事件统计

如图9所示，2019年与虚拟货币相关的诈骗事件损失金额达到近三年最高，为 73.7 亿美元。主要由于2019年第一季度与虚拟货币相关的庞氏骗局 PlusToken 造成损失约 42 亿美元，占据总损失额的 50% 以上。

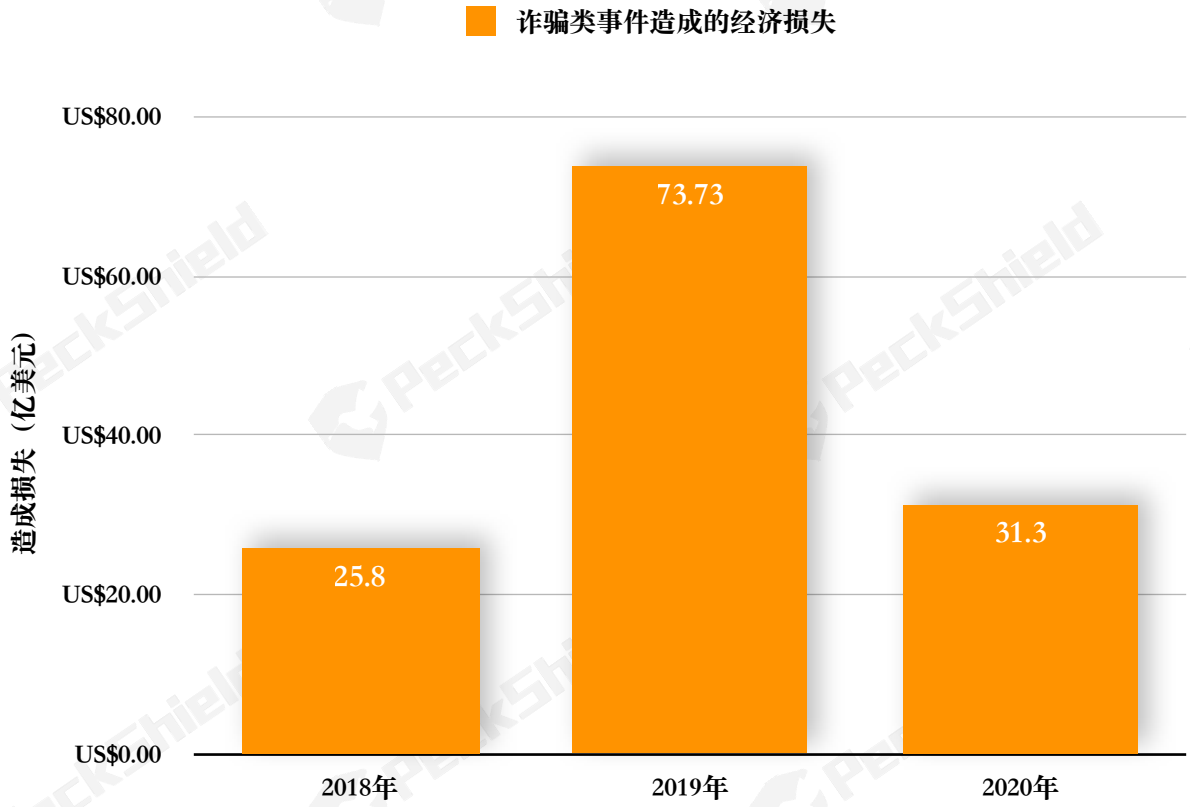

图9 诈骗类安全事件造成的经济损失统计

相较2019年，2020年虚拟货币诈骗事件造成损失有所下降，但出现了新型诈骗手段，例如针对社交网站的「杀猪盘」案件骤增[5]，主要是由于对普通用户而言，虚拟货币领域技术和参与门槛相对较高，一些投机份子利用大众的知识盲区炮制各种骗局。

除此之外，网络罪犯利用虚拟货币洗钱呈现增长趋势，单笔洗钱数额均逾 1 亿美元，他们利用虚拟货币将黑客攻击、勒索软件、盗窃、欺诈和毒品犯罪的收益洗白。据悉，今年6月，新西兰警方冻结了Canton 商业公司和 BTC-e 交易所创始人 Alexander Vinnik 的 1.4 亿美元，是目前为止历史上最大的资金限制。

2020年，虚拟货币勒索病毒呈现爆发趋势，勒索目标从个人转为企业、金融机构，甚至政府网站，勒索者索要比特币、门罗币作为赎金。随着虚拟世界和物理世界的打通，网络攻击能够造成大面积、全局性的破坏后果，它的威力超越传统的单点式安全威胁。小毛贼、小黑产不再是主要威胁，国家级对手发动的高级持续威胁、网络犯罪组织、网络恐怖主义或成为最大的安全威胁。

黑客攻击事件在2020年也呈爆发的趋势，如图10所示，2020年黑客攻击事件达到 170 件，较2018年和2019年增长了 300%。如图11所示，2020年黑客攻击事件所造成的经济损失达到 23.3 亿美元，较2019年增长了 660%，较2018年增长了 7.2%。

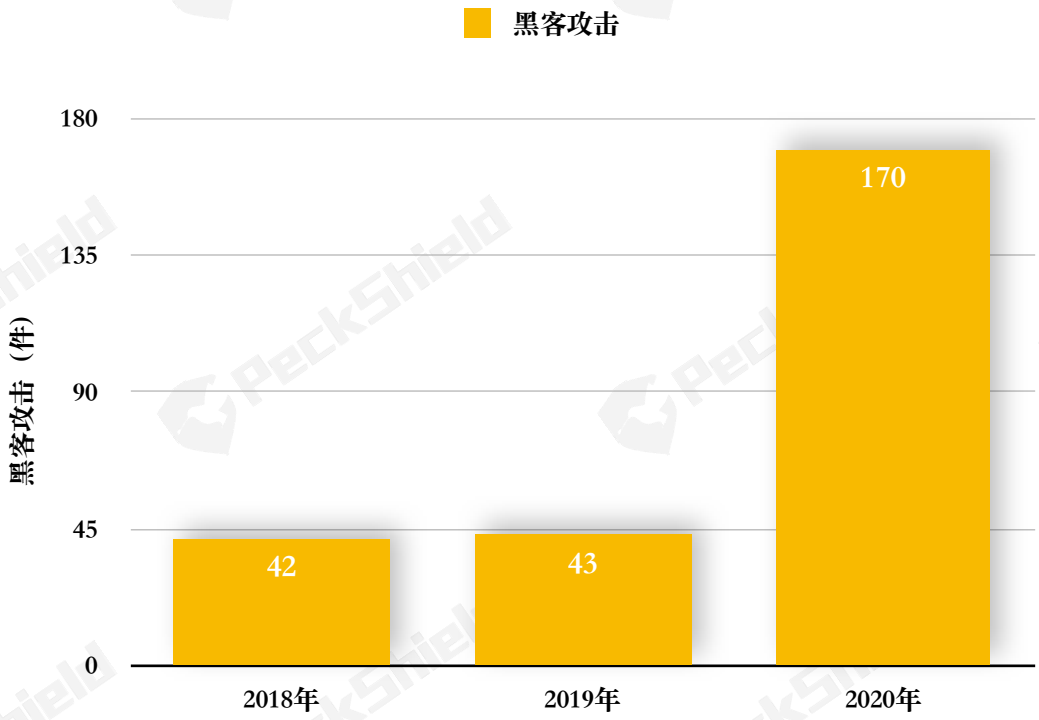

图10 黑客攻击类安全事件统计

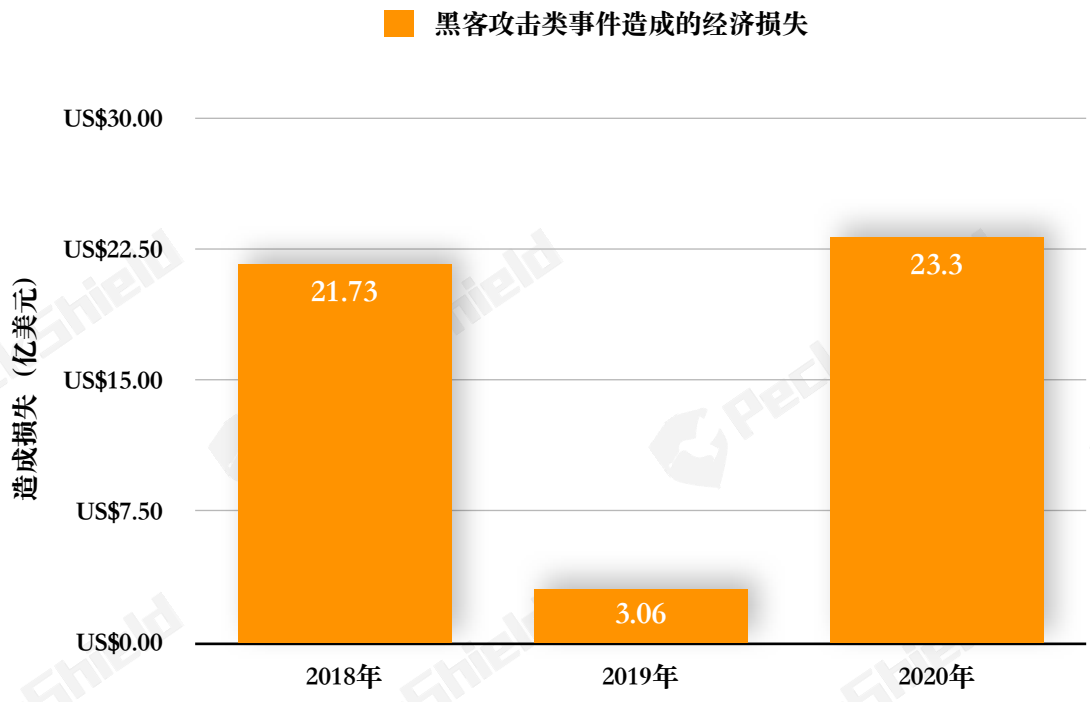

图11 黑客攻击类安全事件造成的经济损失统计

自2017年起，黑客攻击的对象主要集中在公链、虚拟货币交易所、数字钱包、矿场、矿池、矿机厂商等区块链基础设施。

从细分赛道来看，如图12所示，在2020年黑客攻击事件中，黑客攻击仍主要集中在离交易最近的地方，包括交易所、智能合约 & DApp、DeFi、理财钱包等多个领域。虽然过去一年开发者安全意识和举措整体有所提高，DApp、智能合约等原先存在的溢出、重放、随机数等基础型攻击方式整体减少，但这也倒逼了黑客手段的升级，使他们的攻击方式趋于多样化。

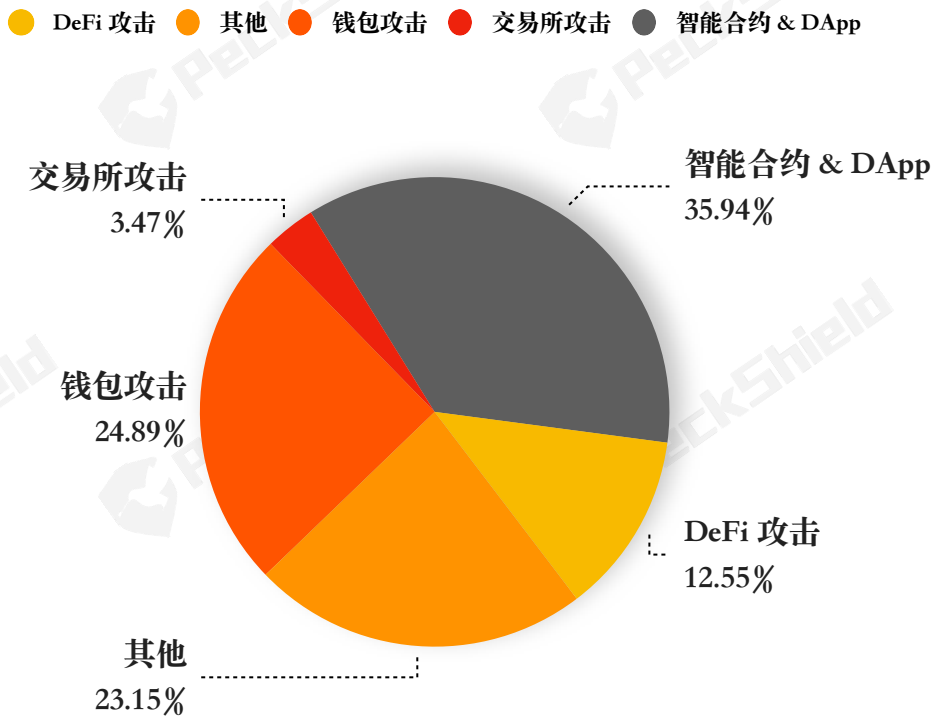

图12 黑客攻击类安全事件分类所占百分比

同时，安全危机事发背后的原因也愈发丰富，出现了私钥丢失、代码预留后门、冷钱包被攻击等花式漏洞。

2020年新秀 DeFi 被黑客盯上。由于 DeFi 产品大都基于智能合约和交互协议搭建，代码普遍开源，资产完全在链上，技术发展处于萌芽期，开发者整体安全意识较为薄弱，行业规模增长潜力大，因而成为今年黑客重点攻击的对象。

据 PeckShield（派盾）统计，2020年 DeFi 攻击事件达到 60 起，损失逾 2.5 亿美元。

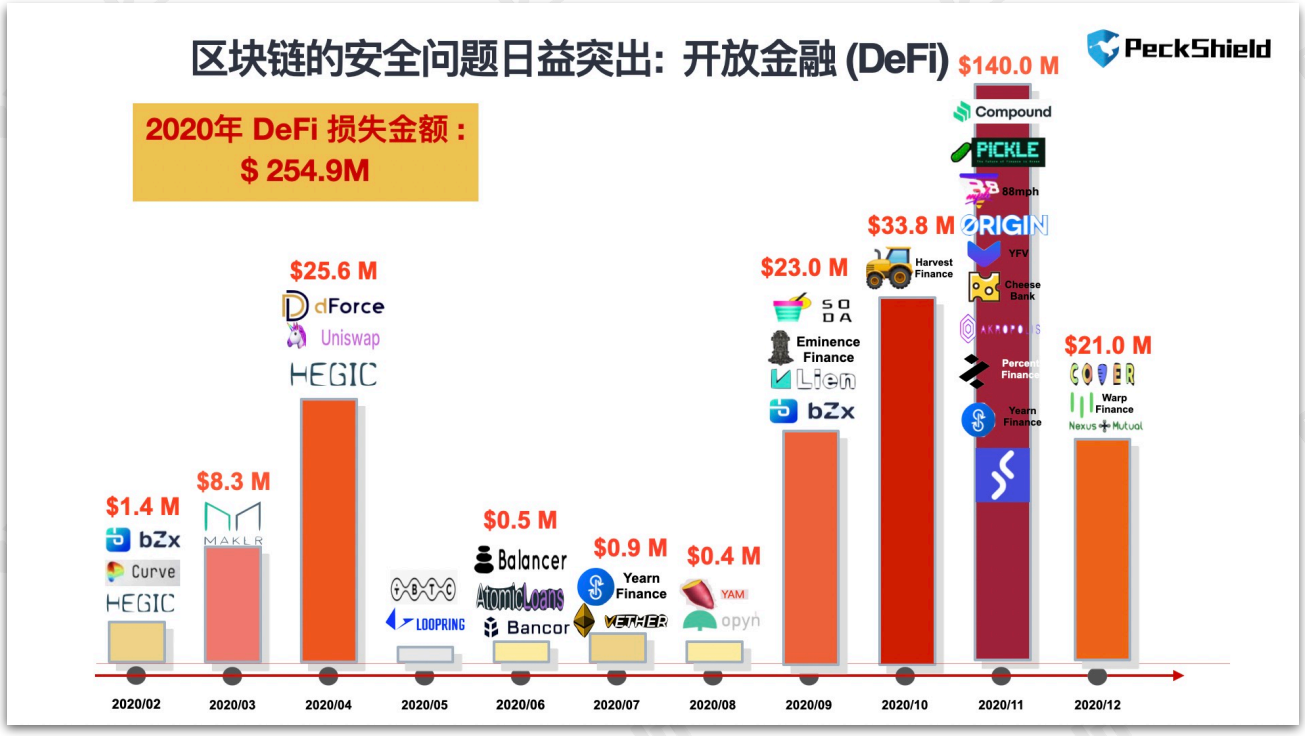

图13 DeFi 安全事件

频发的 DeFi 攻击事件引发从业者对资产安全性的高度重视，严审代码成为保障 DeFi 可持续发展的基石。据 PeckShield（派盾）统计，这 60 起 DeFi 攻击事件中，有至少 10 起为闪电贷攻击，即黑客利用闪电贷，以极低的成本撬动巨量资金，在多个协议间进行价格操纵或套利；有至少 5 起重入攻击，重入攻击是以太坊智能合约上最经典的攻击手段之一，著名的 The DAO 被盗事件就是攻击者运用重入攻击导致以太坊硬分叉，损失价值 5000 万美元以太币。

虽然今年造成经济损失的交易所安全事件发生率有所下降，但中心化交易所安全仍不可忽视，PeckShield（派盾）发现，黑客在攻击交易所后开始尝试新型洗钱方式。

2020年的交易所安全事件共计 39 起，包括币安（Binance）、OKEx、BitMEX 等多家交易所遭到多次 DDoS 攻击，导致交易所在短时内宕机。虽然较2019年与交易所相关的安全事件数量有所下降，但其所存在的问题仍未得到改善，例如易被黑客入侵。

2020年交易所影响较大的安全事件分别为：2月10日，意大利交易所 Altsbit 遭到黑客攻击，被盗 6,929 BTC、 23,210 ETH、3,924,082 ARRR、414,154 VRSC、1,066 KMD（合计 7250 万美元），因没有足够资金补偿用户，该交易所在退还部分客户资金后宣布关闭。

9月26日，交易所 KuCoin 被盗价值逾 2 亿美元的虚拟货币。事件发生后，KuCoin 与多家中心化虚拟货币交易所（CeFi）、项目方、安全机构以及警方联系，并采取部分有效措施，竭力追捕被盗资产。截至目前，据 KuCoin 官网显示已追回 85% 被盗资产。

在安全事件发生后，一些交易所联合 CeFi（中心化金融）及时止损，虽然有效地冻结和追回了部分损失的资产，但随着去中心化金融（DeFi）的创新，新型洗钱方式也在兴起，例如，在KuCoin 安全事件中，遭到 CeFi 联冻后，黑客陆续将所盗资产转向去中心化交易所（DEX），包括 Uniswap、Kyber 等进行扫荡式逐一清空，亦为虚拟货币交易所反洗钱带来新的挑战。

在下一章节中，我们将筛选各个类别中社会影响巨大，用户损失惨重的典型案例，对其事件过程和资金转移途径进行详细剖析。

五、虚拟货币犯罪典型案例

5.1 黑客攻击类犯罪案例

与虚拟货币有关的黑客攻击事件逐年增长，2020年，黑客对虚拟货币的攻击已造成21.3 亿美元的损失。其中，黑马 DeFi 项目让黑客玩出了新花样。由于缺乏法律监管使得黑客肆意攻击，再加上虚拟货币的匿名性所带来的低风险、高回报，使得黑客攻击愈加猖獗。PeckShield（派盾）建议 DeFi 项目发起方应务必对智能合约做好第三方安全审计。

据 PeckShield（派盾）统计，2020年全年至少有 10 起利用闪电贷攻击的 DeFi 安全事件，包括bZx、Balancer[6]、Harvest、Akropolis、Cheese Bank[7]、Value DeFi[8] 和 Origin Protocol[9] 等多个 DeFi 项目遭到攻击。

5.1.1 利用闪电贷攻击 DeFi 项目

今年11月起，闪电贷攻击频发，一周曾接连发生过 4 起闪电贷攻击。闪电贷本是一种创新金融工具，用于高效提供大额资金，促进价值循环。但却被攻击者频频利用，成为黑客借来生「金蛋」的鸡。

区块链上的闪电贷是一种不需要抵押就可以借贷的贷款方式，但贷方必须在同一区块内还贷，否则这个交易就会失败。所以闪电贷对借款平台来说基本是零成本、零风险。而黑客就可以利用这样的贷款方式，以很小的成本借出大笔资金，然后用这笔资金去造成一些虚拟货币的价格波动，再从中渔利。

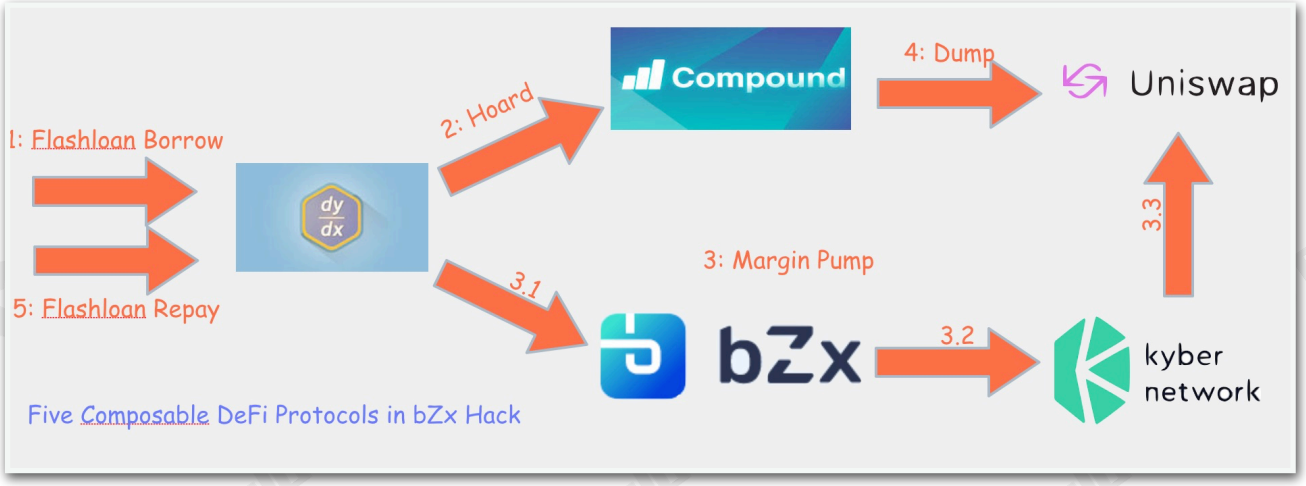

图14 bZx 闪电贷攻击事件

以 bZx 为例，攻击者通过 dYdX 闪贷贷借出 10,000 ETH；随后，攻击者将其中的 5,500 ETH 存入 Compound 作为抵押品，贷出 112 WBTC，所贷 WBTC 在第四步中抛售；随后攻击者利用 bZx 的杠杆交易功能，做空 ETH 购入大量 WBTC，从而抬高 Uniswap 中 WBTC 价格；待 Uniswap 中的 WBTC 价格飙升后（价格为61.4 WETH / WBTC），攻击者将第二步中通过 Compound 借来的 112 WBTC 全部在 Uniswap 中卖出，并返还相应的 WETH。最终攻击者还款闪电贷，获利 6,871.41 ETH。

闪电贷本是一项非常有意义的金融创新，但由于闪电贷攻击频发也备受诟病。PeckShield（派盾）建议："根据闪电贷的特性，借贷和取款都要在一个区块内完成，所以对 DeFi 协议开发方来说，更稳妥的设计是不允许在同一个区块内存款和取款，这样试图利用闪电贷的黑客便无计可施。"

5.1.2 勒索攻击已经成为2020年度最普遍的安全威胁

据 PeckShield（派盾）统计，2020年勒索攻击超 140 起，勒索攻击在网络安全事件中占比达到 41%，攻击频率较上年增长了 260%。

勒索攻击是指黑客通过钓鱼攻击、病毒软件、网络渗透或漏洞攻击后，锁定受害者的网络设备或加密重要的文件，以此向用户勒索钱财。勒索攻击并非新生事物，从第一个已知的勒索软件出现至今，已有近30年的历史，但近几年勒索攻击和虚拟货币结合，利用虚拟货币收款后攻击收益率大幅提升。

勒索攻击发展迅猛，破坏性和影响力前所未有，已经成为2020年最普遍、最具破坏性的安全威胁之一，其中 DoppelPaymer 是最具攻击性的勒索软件之一。

DoppelPaymer 勒索软件始于2019年6月，主要通过远程桌面登录协议（RDP）暴力破解和垃圾邮件进行传播，邮件附件中带有一个自解压文件，运行后释放勒索软件程序并执行。由于它与 BitPaymer 勒索件在部分代码段、勒索信内容和支付赎金网页较为相似，因此疑似为 BitPaymer 的变种。

2020年9月，德国杜塞尔多夫的一家大型医院杜塞尔多夫大学诊所遭到 DoppelPaymer 的网络攻击，此次攻击活动导致 30 多台内部服务器被感染。期间，医院因未能收治一位需要接受紧急治疗的女性患者，造成患者未及时接受治疗不幸去世，该案例是史上首次勒索软件攻击间接造成人员伤亡的案例。

2020年11月29日，苹果最大的产品制造商富士康位于墨西哥华雷斯城的工厂于遭到DoppelPaymer 勒索软件的攻击。受到攻击后，该工厂的网站已关闭，访问页面显示为错误。攻击者索要 1804.10 枚比特币的赎金，合计约逾 3400 万美元（折合人民币 2.27 亿元）。

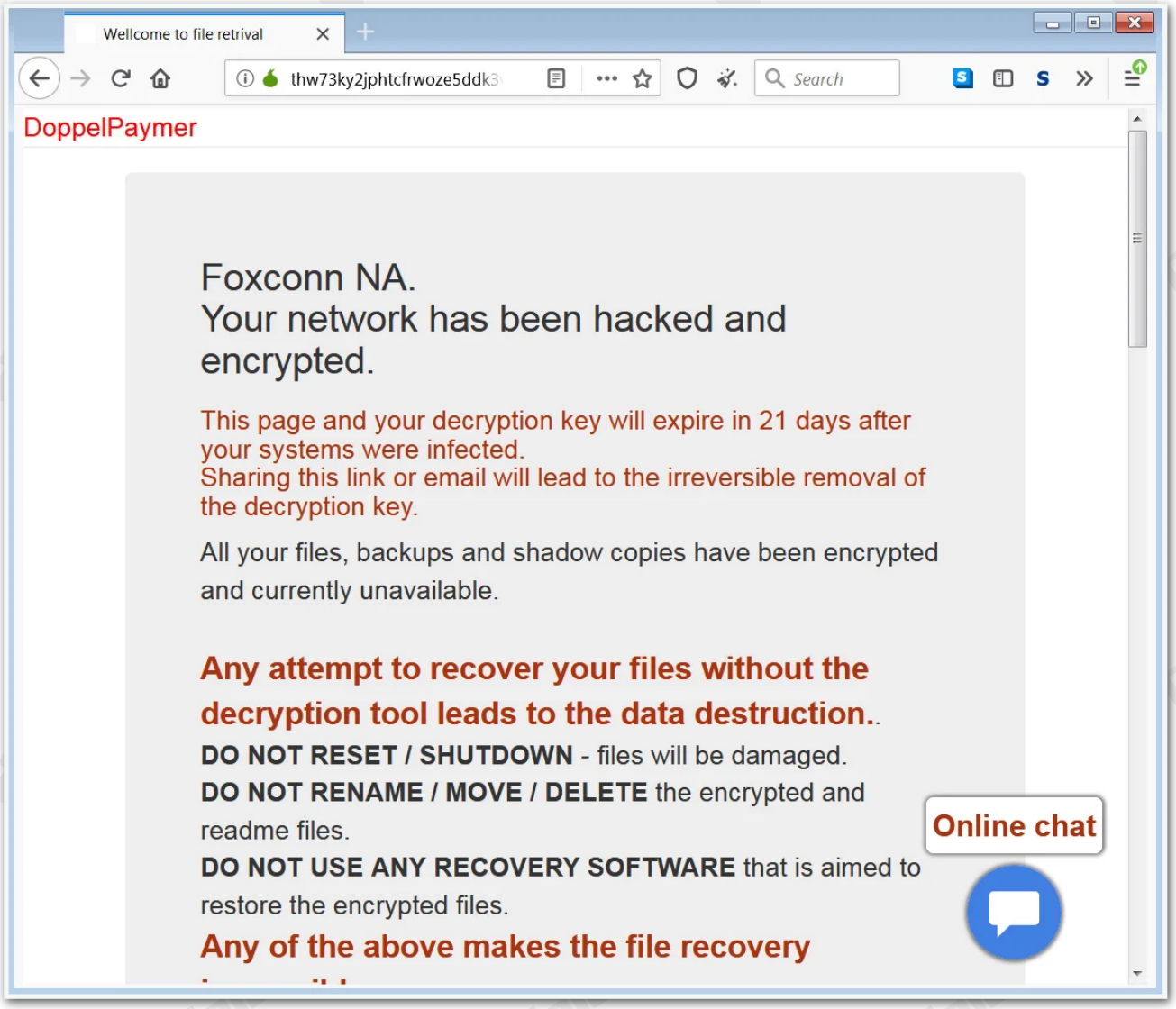

图15 富士康被勒索软件攻击事件

此前，DoppelPaymer 曾攻击过台湾笔记本制造商 CompalElectronics（仁宝电脑）、PEMEX（PetróleosMexicanos）、加利福尼亚州托伦斯市、纽卡斯尔大学、乔治亚州霍尔县、BanijayGroupSAS 与 BretagneTélécom。

据悉，门罗币作为勒索赎金已成为新趋势，由于门罗币等隐秘币更难被追踪，大部分加密勒索团伙已经开始转向使用门罗币。2020年7月，一家澳大利亚饮料制造商和阿根廷电信公司（TelecomArgentinaS.A）均遭到勒索软件攻击，被要求用门罗币（XMR）支付赎金。

PeckShield（派盾）安全专家认为，从过去的经验看，勒索软件多是黑客进行的跨国攻击，利用比特币进行收款。虚拟货币追踪是很好的途径来追回被勒索资金，但打击勒索软件需要多种技术手段结合，需要全球联合行动。

5.2 诈骗类犯罪案例

随着区块链技术的发展和国家对区块链的重视，央行数字货币的试点，不法分子们开始利用虚拟货币、区块链的名头，以高收益诱导受害人投资诈骗。

欺诈手段换汤不换药，仍以钓鱼网站、承诺高收益等方式为主，但值得注意的是，针对单身男女的「杀猪盘」也蔓延至虚拟货币领域。

5.2.1 政要商界领袖 Twitter 被盗发送比特币钓鱼信息

2020年7月16日，多位政商界名人账户，包括美国前总统奥巴马和当选总统拜登、比尔·盖茨，亚马逊创始人贝索斯特斯拉 CEO 马斯克等名人 Twitter 账号被盗并发布比特币的钓鱼信息。黑客宣称称任何人只要往某个比特币账户发送比特币，就会得到双倍回报，且活动只限 30 分钟内参与。

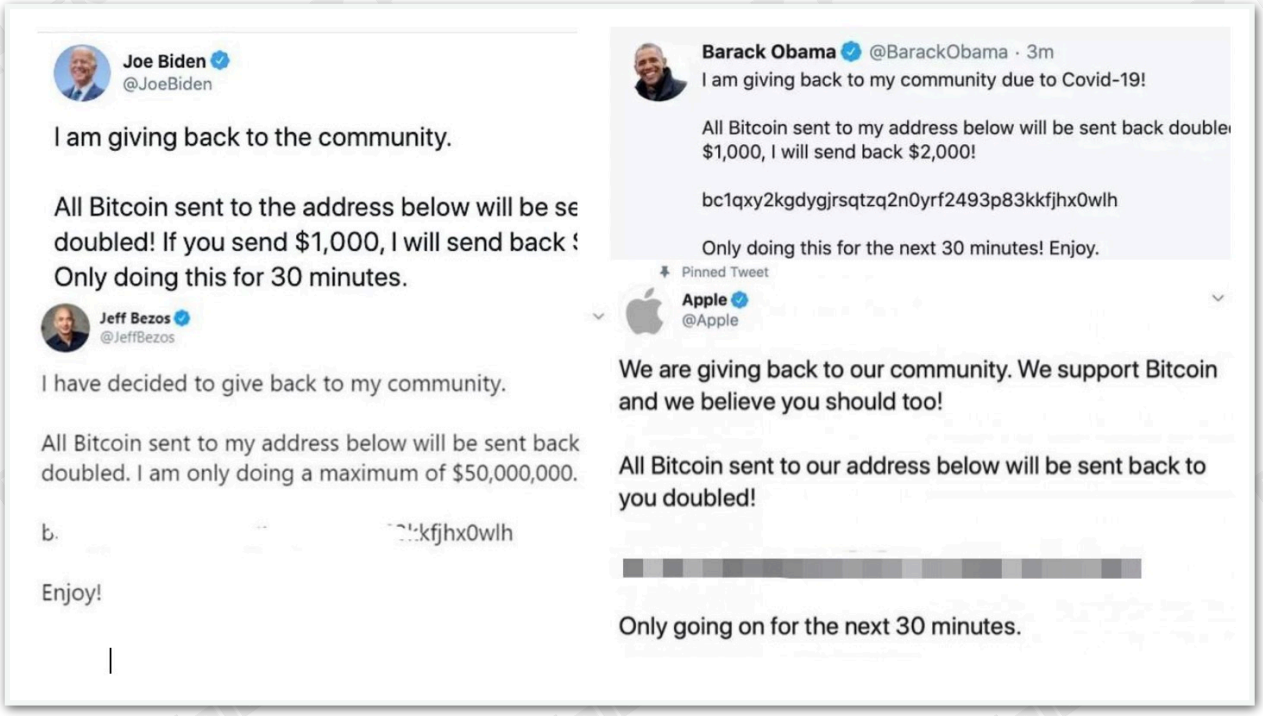

图16 Twitter 账户发布的虚假消息截图

根据 PeckShield（派盾）反洗钱态势感知平台数据显示，涉案的两个诈骗钱包地址一共收到 13 枚 BTC，黑客动用了超过 100 个中转地址进行洗钱。其中有部分 BTC 流入了 Coinbase 交易所。而根据媒体披露的消息，FBI 正是根据 Coinbase 提供的 KYC 信息最终锁定了嫌疑犯。

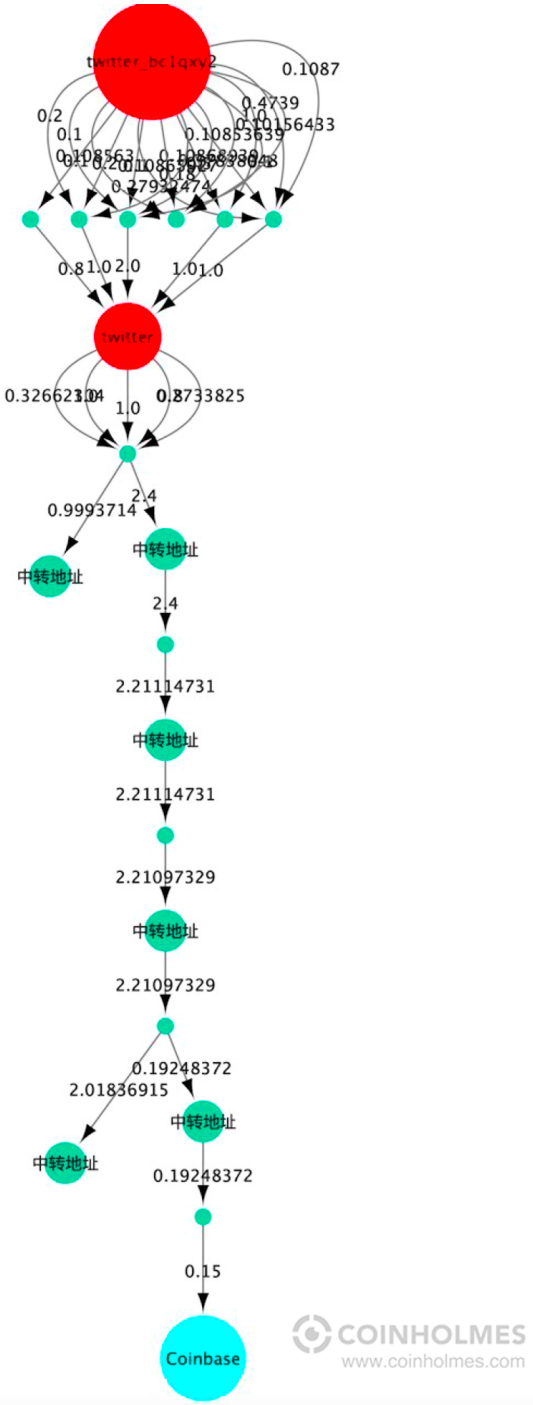

图17 Twitter 诈骗资金流入 Coinbase 路径图

5.2.2 虚拟货币「杀猪盘」上热搜 女性受伤更深

2020年11月「杀猪盘」这个话题登上了微博热搜，话题阅读量高达 3.3 亿。最开始是一位网友发微博称自己前段时间遭遇了「杀猪盘」被骗了 40 万元，而后这条微博引发了很多网友的心声，他们纷纷在微博底下评论、转发，大都是在倾诉发生在自己身上的「杀猪盘」经历。

「杀猪盘」骗局是一种新型的网络诈骗手法，诈骗分子通过网络交友的形式诱导受害人参与各类理财、博彩游戏和外汇交易等类型虚假投资的诈骗方式。诈骗者把被骗的受害人叫做「猪」，按照一些既定的剧本去包装自己，装扮成高富帅，谈感情获取信任阶段称之为「养猪」，待聊到有一定情感基础后就开始引诱对方投资，最后的诈骗行为叫做「杀猪」。

与传统「杀猪盘」不同的是，虚拟货币「杀猪盘」利用受害人对区块链技术的盲目推崇和对虚拟货币的不了解，以投资名义让受害人先到正规交易平台用现金购买虚拟货币，再诱骗对方将已经购买的虚拟货币转移到诈骗分子指定的虚假平台或者地址。一旦受害人将购买的虚拟货币转移到骗子指定的虚假平台，资金会迅速通过境内的洗钱团伙处理或直接流入境外交易所，为追回资金造成极大的难度。

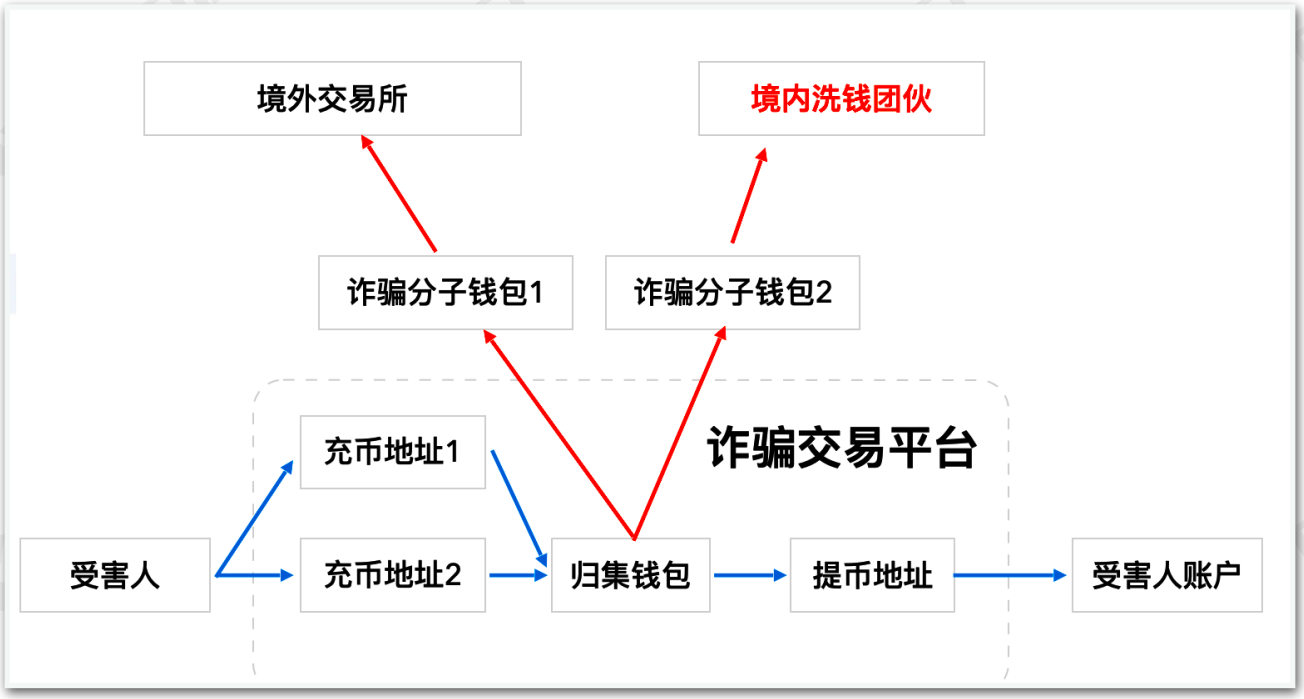

图18 典型虚拟货币诈骗交易平台结构图

5.3 恐怖融资和政治渗透类犯罪案例

鉴于资金在支持恐怖主义组织运作的关键作用，打击恐怖组织的融资渠道十分重要。过去，恐怖组织主要通过银行体系进行融资，随着银行体系原来越严格的反洗钱和反恐怖融资机制取得成效，PeckShield（派盾）发现恐怖组织开始转向虚拟货币领域融资以支持其活动。

PeckShield（派盾）认为这个趋势应该引起有关各方的高度重视，包括与反恐相关的国家安全机构、有关金融监管部门，以及从事加密交易的交易所和场外交易商。

5.3.1 ISIS 利用虚拟货币洗钱和融资

2020年8月，由基地组织、卡萨姆旅组织和伊斯兰国（ISIS）等恐怖组织拥有和使用的虚拟货币账户被美国政府查封并公布。在本次行动中，查获价值超 200万 美元的虚拟货币。

PeckShield（派盾）对 al-Qassam-Brigades（卡萨姆旅组织）17QAWGVpF 开头的地址进行路径全方位分析发现：涉恐地址上的资产在经过层层分散转移后疑似进入某个混币服务系统和聚合器，最终有部分资产流入 Bitstamp、Coincola、Gate.io 等交易所。

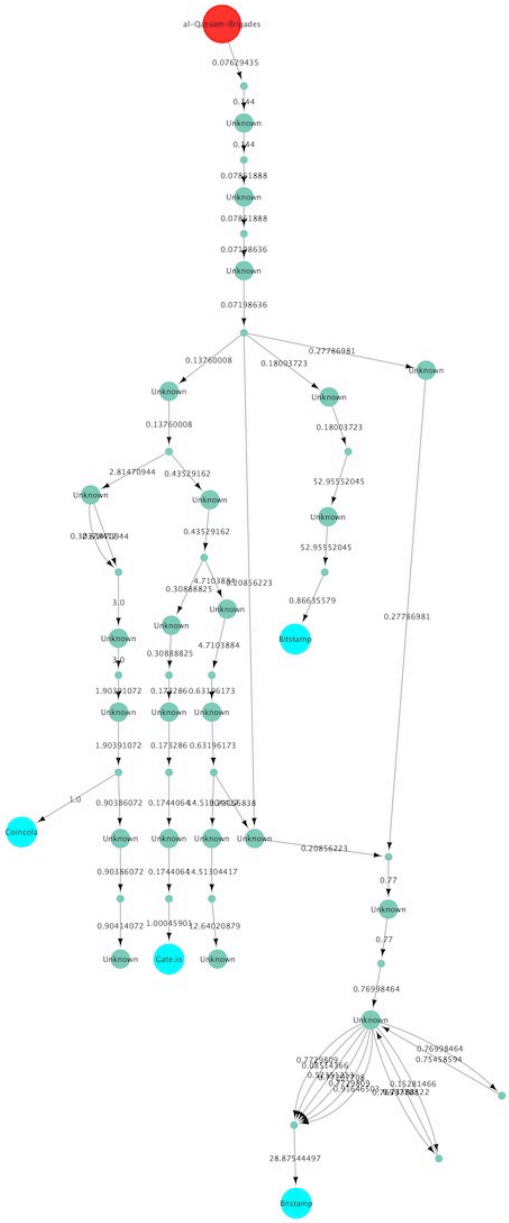

图19 卡萨姆旅资金变现路径图

以上的分析只是其中一个涉恐地址的资产流向情况。涉恐地址 al-Qassam-Brigades（卡萨姆旅组织）的资产链上经过层层转移后，和包括 Binance、Coinbase、BitMEX、Bitfinex、Bitstamp、Bittrex、Huobi、OKEx、KuCoin、Upbit、Poloniex、HaoBTC、HitBTC 等数十个主流的虚拟货币交易所有发生交互。

见微知著，我们不难发现，恐怖分子确实在利用区块链的隐私特性进行恐怖主义融资，且其变现渠道几乎污染了遍布全球各地的大小交易所。

5.3.2 朝鲜黑客攻击虚拟货币交易所洗钱案

两名中国公民因涉嫌帮助朝鲜黑客组织清洗了 1 亿美元被盗的虚拟货币，而被美国司法部指控犯有洗钱阴谋罪和经营无证汇款业务罪[10] 。美国政府正试图扣押 113 个不同地址的虚拟货币，并称这两名被告清洗了「大部分被盗的 BTC」。根据文件显示，总共有 2.34 亿美元的虚拟货币被盗，包括 BTC、ETH、ZEC、DOGE、XRP、LTC 和 ETC 等。大多被盗虚拟货币通过「逐步脱链（PeelChain）」进行洗钱。

据 PeckShield（派盾）数据分析，朝鲜黑客组织 LazarusGroup 先通过钓鱼获取交易所私钥等手段，攻击了四个虚拟货币交易所；之后黑客用 PeelChain 等手法把所窃的资产转入到 HitBTC、KuCoin、Bittrex、Yobit 4 个交易所；再然后黑客又使用 PeelChain 把资产转移到负责洗钱的两位责任人的交易所 Huobi 和 Coincola 的账户中，最后换成法币完成整个过程。美国司法部这次起诉的就是最后一环负责洗钱的田寅寅和李家东。

1）处置阶段：放置资产至清洗系统

在 Bter、Bithumb、Upbit、Youbit 交易所被盗事件发生后的数月内，朝鲜黑客组织开始通过各种手段处置他们的非法获利。将获利资产流到自己可以控制的账号之中，为下一步的清洗做准备。

2）离析阶段：分层、混淆资产逃离追踪

离析过程中，朝鲜黑客组织试图利用 PeelChain 的技术手段将手里的资产不断拆分成小笔资产，并将这些小笔资产存入交易所。下图中我们挑选了一笔比较典型的拆分过程，对于第一笔 2,000 BTC 的流程细述如下（其它交易流程上相似，不再赘述）。

3）归并阶段：整合资产伺机套现

朝鲜黑客组织在完成上一步的洗钱操作之后，开始尝试进行将非法所得进行 OTC 抛售套现。攻击者总共把 3,951 个 BTC 分一百多次存入田寅寅的 Huobi 和 Coincola 三个 OTC 帐号中变现。

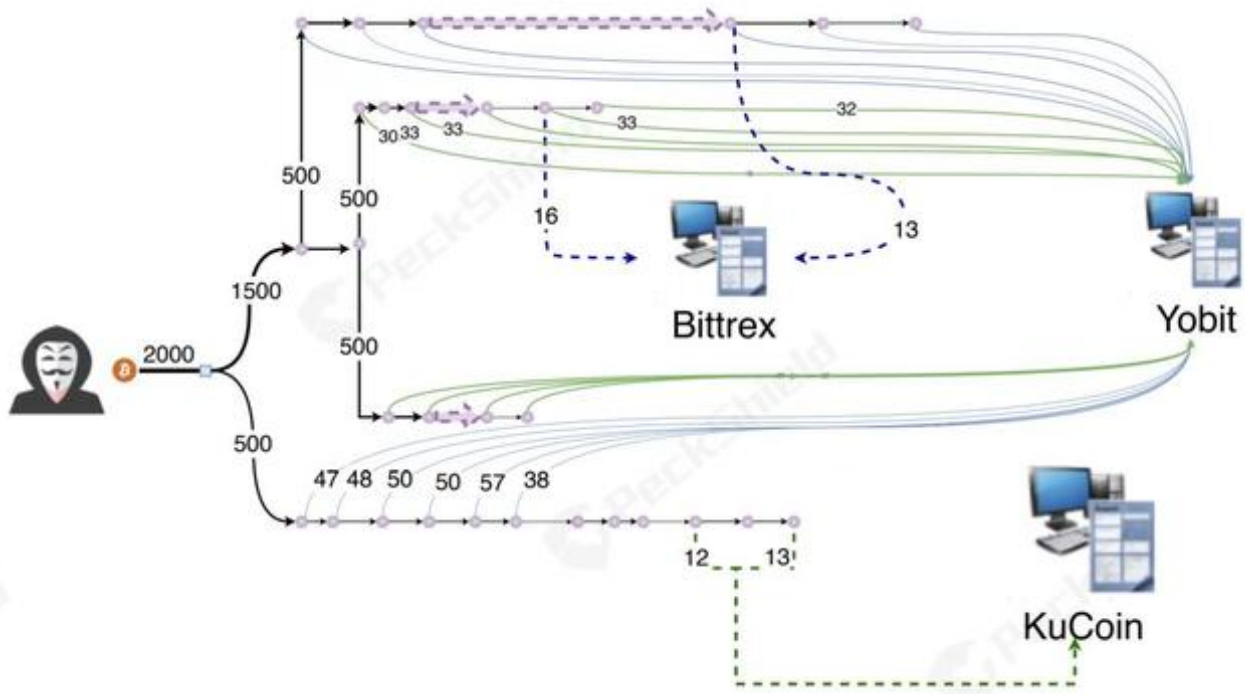

图20 朝鲜黑客盗取资金后拆分过程

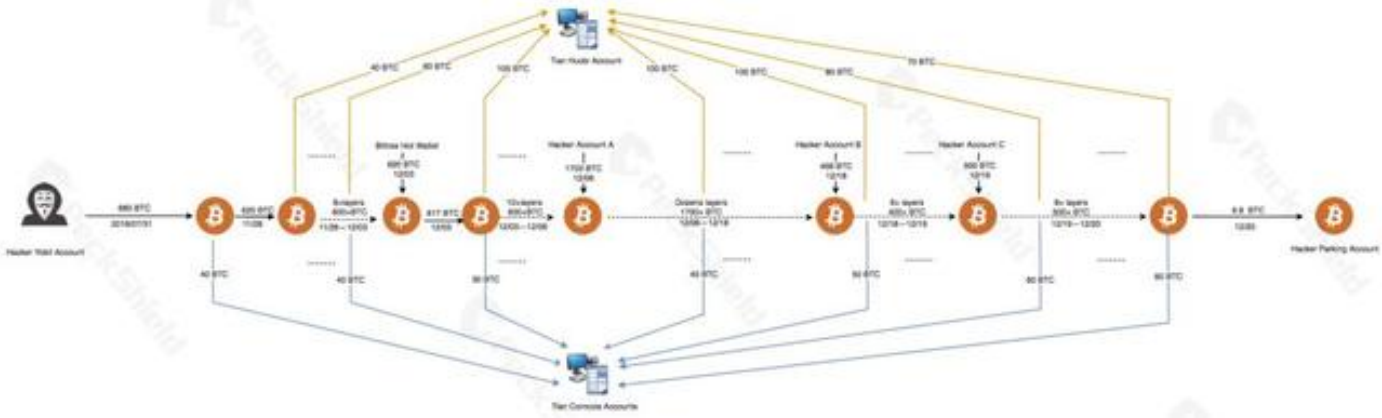

图21 朝鲜黑客非法所得 BTC 再次转移过程

5.3.3 美国使用 USDC 支持委内瑞拉反对派

2020年11月，稳定币 USDC 发行方 Circle 披露其首次与美国政府合作[11]，使用锚定美元的稳定币 USDC 绕过委内瑞拉现任总统马杜罗，直接支持反对派瓜伊多，并向委内瑞拉医务人员和其他当地居民发放救援资金。2020年初新冠肺炎疫情在全球蔓延，马杜罗政府曾向国际货币基金组织（IMF）提出 50 亿美元抗疫援助贷款的申请，旨在实施预防性措施，但 IMF 以委内瑞拉政府不受国际社会普遍承认拒绝其请求。

虽然 USDT 仍手攥稳定币最大市场份额，但它并不受美国金融部门的监管，自去年5月起，它遭到美国纽约州总检察长办公室的打压。而 USDC 的发行方 Circle，所有的发币行为都受到美国政府的监管，这是美国金融部门最喜闻乐见的方式。

速度、无国界、币值稳定、市场份额大这四点正是 USDC 具有的优势，这对高通胀国家的国民来说很有吸引力，而对于美国来说，USDC 已经形成与数字美元的联盟关系，它与传统美元不同，其实质是数学，其他国家可以通过疆域治理传统美元，通过金融管制来阻止美元进入，但数字美元打破了疆域的壁垒，使其更加方便地渗入任何国家。

一方面，使用 USDC 有助于美国相关部门监控和掌握资金的流转情况，加强对反对派瓜伊多的实际控制；另一方面，更是为了绕过拉政府的外汇政策管制，削弱主权国家经济调控的能力。

USDC 虽然只是一个稳定币，但它正在影响世界的政治体系，包括对委内瑞拉、伊朗的影响；这次，USDC 带头打入委内瑞拉市场，正在经济领域扮演着类似的角色。这或许就是美国的驱动力所在——通过数字美元霸权世界。

PeckShield（派盾）相关负责人表示：“此类国家组织利用加密货币的匿名性、无国界性等特性绕开外汇管制的行为，会对他国的经济和社会造成恶劣影响，其意在使用经济手段颠覆该国现政府。对此，PeckShield（派盾）已输出 CoinHolmes 安全方案，为助力监管部门有效打击此类事件提供技术支持，将追踪、溯源加密货币流转透明化、可视化。”

六、结论

综上所述，PeckShield（派盾）安全团队通过分析2020年全球数字货币反洗钱相关的政策，统计未受监管的跨境资产流动，整理和统计2020年各类案件，分析相关典型案例，得出如下三个重要结论：

6.1 2020年未受监管的出境规模高达 175 亿美元，国际监管合规逐步落地

2020年未受监管的出境规模高达 175 亿美元，较2019年增长 51%，且仍在快速增长。各主要国家逐步落地对虚拟货币的监管，推出了一系列针对虚拟货币的监管法规，对于虚拟货币特别是交易所的监管合规开始落地。但由于主流虚拟货币如 BTC、ETH、USDT 等具有天然的无国界性和匿名性，极大的提高了各国政府监管介入的门槛。

6.2 涉及虚拟货币的诈骗案件持续高发，勒索案件快速增长，虚拟货币反洗钱形势严峻

2020年虚拟货币诈骗案件达到 151 起，较2019年增长 655%。勒索类案件更是达到了 140 起。随着中国国内断卡行动的深入以及反洗钱法的生效，传统的洗钱途径遭遇沉重打击。犯罪分子转移至虚拟货币领域，而2020年下半年，火币和 OKEx 两大交易所接连接受警方调查，这两起事件也已明显传达了监管层的坚定态度。PeckShield（派盾）建议虚拟货币交易所、场外交易商、钱包软件等服务商应尽快引入反洗钱工具，主动规避风险资金。

6.3 监管需求快速提升，监管工具亟待创新和普及

由于数字货币和传统金融的金融领域完全不同，具备天然的匿名性、复杂性和跨国性三大特点，使得监管机构在调查和打击虚拟货币相关犯罪时，面临重重困难。除了需要完善相关的法律法规，也急需引入新的监管工具和技术。

PeckShield（派盾）发现2020年下半年开始无论是诈骗、攻击、勒索、赌博这类黑产，还是洗钱、跑分等灰色产业，使用虚拟货币已经成为趋势，特别是恐怖组织开始转向虚拟货币领域融资以支持其活动，我们认为这个趋势应该引起有关各方的高度重视，特别是公安机关，国家安全机构、有关金融监管部门。

只有新型虚拟货币的监管工具和技术手段得到普及，利用虚拟货币的黑灰产、洗钱、恐怖融资才能遭到打击和遏制。

参考文献

[1] PeckShield（派盾），《冻卡潮再起波澜背后：加密世界OTC出金通道监管之殇》,搜狐新闻,2020-10-19：https://m.k.sohu.com/d/490112671

[2] 人民资讯，《正本清源之三：在中国持有和交易“数字货币”的法律分析》，人民网,2020-11-03：https://baijiahao.baidu.com/s?id=1682298823973729845&wfr=spider&for=pc

[3] 新华社，《11月末我国外汇储备规模增505亿美元至31785亿美元》，新华社,2020-12-07：http://www.gov.cn/xinwen/2020-12/07/content_5567783.htm

[4] VanityFair，《互联网阴暗前传：暗网“丝绸之路”覆灭始末》，虎嗅网,2017-05-17：https://www.huxiu.com/article/195204.html

[5] PeckShield（派盾），《杀猪盘案件频发，数字货币领域也成了“养猪根据地”？》，搜狐新闻,2020-09-25：https://www.sohu.com/na/420852936_100217347

[6] PeckShield（派盾），《DeFi 平台 Balancer 遭黑客攻击全过程技术拆解》，腾讯新闻,2020-06-30：https://new.qq.com/omn/20200630/20200630A0BYWF00.html

[7] PeckShield（派盾），《“科学家”的盛宴 Cheese Bank 被带走的 330 万美元》，区块律动 BlockBeats,2020-11-17：https://www.theblockbeats.com/news/20787

[8] PeckShield（派盾），《Value DeFi 遭黑客攻击始末：一次基于 AMM 价格预言机的“神级”操作？》，百家号，2020-11-15：https://baijiahao.baidu.com/s?id=1683419524442840382&wfr=spider&for=pc

[9] PeckShield（派盾），《OUSD 遭“经典重入攻击”损失 770 万美元 DeFi 安全亟待解决》，搜狐新闻,2020-11-23：https://www.sohu.com/a/433675388_100217347

[10] PeckShield（派盾），《硬核：解密美国司法部起诉中国 OTC 承兑商洗钱案件》，陀螺财经,2020-03-12：https://www.tuoluocaijing.cn/article/detail-9992814.html

[11] PeckShield（派盾），《数字美元欲颠覆委内瑞拉 加密资产反渗透如何破局？》，腾讯新闻,2020-11-24：https://new.qq.com/omn/20201124/20201124A0DYX500.html

关于我们

PeckShield（派盾）成立于2018年，由前 360 首席科学家蒋旭宪教授创办，高榕资本三千万人民币的天使投资，研究团队分布于杭州、北京、旧金山，核心成员来自于 360、英特尔、Juniper、阿里巴巴 等全球知名企业，是全球领先的区块链数据与安全服务提供商，致力于区块链数据和安全技术的研发和商用。业务覆盖区块链生态安全的各个环节，包括渗透测试、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。

PeckShield（派盾）凭借过硬的代码漏洞发掘能力和权威的链上数据及业务逻辑整合实力，被 etherscan.io（以太坊官方）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 Top3。

过去 2 年，PeckShield（派盾）利用自主研发的 CoinHolmes 虚拟货币反洗钱系统，协助北京、上海、湖南、四川，广州、杭州、温州、漯河、上饶、泉州等 10 多个省级和市级网安、经侦、刑侦、国安等安全机关打击了一系列虚拟货币相关的犯罪案件，受到了各级安全机构的高度认可。

关于我们：https://www.peckshield.cn/zh

联系我们：contact@peckshield.com

公司总部：杭州市滨江区物联网街道 369 号大华江虹国际创新园 A 座 606

北京分部：北京市海淀区知春路量子芯座大厦 1708

更多资讯：请关注 PeckShield「派盾」微信公众号