数字货币反洗钱暨DeFi行业安全报告

2021上半年报告

PeckShield（派盾）

2021.07

目录

一、研究背景综述

2021上半年前期，数字货币市场增长势头强劲，特别是在全球第一家数字货币交易所 Coinbase 在纳斯达克上市、支付巨头 PayPal 向美国用户开放虚拟服务等多重因素的影响下，主流数字货币的价值屡破新高。随着多链部署构建的 DeFi 生态蓬勃发展，各个公链逐步完善基础设施，NFT（非同质化代币）频繁出圈，DeFi 版块延续2020年的火热，迎来新一轮显著的增长。

2021上半年后期，为保证国家金融稳定，各主要国家在加速布局区块链技术的同时，开始对虚拟货币行业实施严厉打击。其中，以主要欧美国家和中国为代表的市场监管机构加强对该领域的监管力度。中国香港特别行政区政府也发布《有关香港加强打击洗钱及恐怖分子资金筹集规管的立法建议》，明确对虚拟资产服务提供者提出了打击洗钱与恐怖融资的监管要求。

为有序地完成「碳中和」的远景目标，我国多个政府机构陆续对虚拟货币「挖矿」企业进行清理整顿，在国内政策不断趋严的情况下，包括「挖矿」、「交易所」等将迎来新一轮行业格局的洗牌。

回顾2021上半年，「监管」、「合规」、「创新」成为数字货币行业发展的核心，而以虚拟货币追踪为切入点，将反洗钱、反勒索、反恐怖融资提升至国家安全高度，成为当前监管肃清整顿的战略目标。

1.1 涉虚拟货币犯罪形势严峻 监管力度进一步升级

国内方面，从「9·4 禁令」到「6·21 约谈」，我国在积极推进区块链技术发展的同时，政府部门对虚拟货币的炒作始终秉承零容忍的态度。即便是在如此高压的态势下，虚拟货币在洗钱、勒索领域的运用仍日益增长。

据中国检察网数据显示，2020 年来已经处理 249 例与虚拟货币泰达币「 USDT」 关联的犯罪案件，仅 2021 年上半年就有 147 例，而在 2020 年之前只有 5 例。涉及虚拟货币的洗钱、转移赃款等案件呈现出持续高发的趋势。

随着涉及虚拟货币的洗钱、勒索、欺诈的案件愈来愈多，监管范围开始扩展至虚拟货币交易所、虚拟货币交易信息中介、挖矿等主体。

今年以来，我国金融监管部门对虚拟货币的监管力度进一步升级。

5月18日，中国互联网金融协会、中国银行业协会、中国支付清算协会联合发布《关于防范虚拟货币交易炒作风险的公告》，重申开展法定货币与虚拟货币兑换及虚拟货币之间的兑换业务、为虚拟货币交易提供信息中介和定价服务等活动，违反有关法律法规，并涉嫌非法集资、非法发行证券、非法发售代币票券等犯罪活动。

5月21日，国务院金融稳定发展委员会召开五十一次会议。会议强调，强化平台企业金融活动监管，打击比特币挖矿和交易行为，坚决防范个体风险向社会领域传递。与此同时，内蒙古、新疆、云南和四川等国内主要虚拟货币「挖矿」地区，陆续发布对虚拟货币「挖矿」企业进行清理整顿的通知，严禁各地区立项、批复各类虚拟货币「挖矿」项目，对现有的各类虚拟货币「挖矿」项目全面关停；坚决查处纠正以大数据、超算中心等名义立项但从事虚拟货币「挖矿」的项目主体，禁止向虚拟货币「挖矿」行为提供场所、电力支持。

6月7日，在2021年国家打击治理跨境赌博网络工作组专题会议上，国家网信办提出「加大对虚拟货币平台及衍生平台应用的监测力度」。

6月9日，中国支付清算协会强调「利用虚拟币、区块链技术逃避资金溯源，使用虚拟币作为赌博跑分媒介或以虚拟币进行充值交易」的风险。

6月17日，最高人民法院、最高人民检察院、公安部联合发布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》（以下简称“《意见》”），《意见》明确指出，电商平台预付卡、虚拟货币、手机充值卡、等经销商，在公安机关调查案件过程中，被明确告知其交易对象涉嫌电信网络诈骗犯罪，仍与其继续交易，符合刑法第二百八十七条之二规定的，以帮助信息网络犯罪活动罪追究刑事责任。同时，明知是电信网络诈骗犯罪所得及其产生的收益，以明显异于市场的价格，通过电商平台预付卡、虚拟货币、手机充值卡、等转换财物、套现的，以转账、套现、取现，以掩饰、隐瞒犯罪所得、犯罪所得收益罪追究刑事责任。

6月21日央行官网发文称，人民银行有关部门就银行和支付机构为虚拟货币交易炒作提供服务问题，约谈了包括工商银行、农业银行在内的部分银行和支付机构。随后，工商银行、建设银行、邮政储蓄银行、兴业银行以及支付宝纷纷发表公告禁止开展比特币等虚拟货币交易。

此外，监管部门接连下发通知，持续整治虚拟货币乱象，微博和百度等社交和搜索平台也对虚拟币交易所、「火币」、「币安」、「OKEx」等关键词进行了封禁。

我国香港特区也在不断加码对虚拟货币的监管。2020年11月，香港特区政府财经事务及库务局对加强打击洗钱及恐怖分子资金筹集规管的立法建议进行公众咨询，建议建立虚拟资

产服务提供商发牌制度。业界预计将成为香港证监会目前颁发 10 种金融牌照以外的第 11 号牌。根据咨询文件，规管涵盖的活动包括虚拟资产交易、转移、托管及管理，以及为发行虚拟资产提供金融服务等。

一方面，强监管信号表明当前打击虚拟货币交易的工作效果还没有达到中国监管的要求；另一方面，反映出中国监管坚决推进这项工作的决心。从政策和监管要求来看，监管要求各机构加强对虚拟货币交易所及场外交易商资金账户的全面排查识别，及时切断交易资金支付链路，加大技术投入，完善异常交易监控模型，切实提高监测识别能力；完善内部工作机制，明确分工，压实责任，保障有关监测处置措施落实到位。

但由于虚拟货币交易平台「马甲」账户频繁更换，导致相关部门在阻断过程中，存在追踪路径难分辨、涉币人群难定位、跑分平台交易难识别等难题，银行和支付机构仅靠内部交易系统监控可疑资金、账户，无法解决跨行、跨平台甚至跨国的交易跟踪问题，亟需建立虚拟货币反洗钱态势感知系统，对目前的虚拟货币交易场景、涉币人群进行动态的开源情报大数据分析，对整个虚拟货币交易网络进行整体的监测与关注。

1.2 全球主要国家加速落地数字货币合规化运营

国际方面，在稳扎稳打地与美国监管当局合作多年后，全球第一家数字货币交易所 Coinbase 在纳斯达克上市；获得纽约金融服务部批准的 BitLicense 牌照的 PayPal 向美国用户开放虚拟服务。美国监管积极鼓励「创新」的同时延续铁腕政策，加速惩治不合规的虚拟货币企业，开启「罚款」模式。

据 PeckShield「派盾」统计，2021上半年，美国监管部门对涉及虚拟货币交易的公司和个人处以罚款约 6.28 亿美元，包括美国商品期货交易委员会「CFTC」以欺诈、洗钱、操纵市场等违规行为提起诉讼罚款 6.19 亿美元，以及美国证券交易委员会「SEC」以欺诈、未经注册发行证券等违规行为提起诉讼罚款 9,000 多万美元。

从美国监管部门频频出手打击涉及虚拟货币货币的非法活动来看，美国方面一再树立虚拟货币行业并非金融业以外的「狂野西部」的思路，利用现有法律制止和惩罚打击虚拟货币进行的非法活动，包括庞氏骗局、洗钱、勒索、非法集资，并追究企业未遵守合规的责任。

2021 年 3 月，韩国出台的《特定金融信息法》正式施行，规定虚拟货币交易所必须取得银行实名账户，履行反洗钱义务。据悉，韩国有超过 200 个虚拟货币交易所。然而，绝大多数现有交易所尚满足不了韩国政府在监管批准方面设定的条件。由于政策的不确定性，许多

韩国银行限制与虚拟货币交易所开展合作。满足条件的虚拟货币交易所屈指可数。届时，随着韩国交易所的大洗牌，韩国虚拟货币行业会逐步走向合规化。

欧美国家加速打击涉及虚拟货币的犯罪。2021年6月25日，英国伦敦警察厅「Metropolitan Police」查获史上最大涉及加密货币洗钱案件之一，涉案规模达到 1.14 亿英镑（约合 10 亿元）。其副助理局长 Graham McNulty 表示，随着科技和线上平台的发展，一些犯罪分子正在转向使用更复杂、技术门槛更高的洗钱方法，为有效打击结合虚拟货币的犯罪，他们与本土区块链业界安全相关力量建立合作机制，获得技术支持服务，从犯罪财富调查角度撬动对灰黑产业链条的打击。

新加坡金管局将虚拟货币交易所列为数字支付代币服务供应商，适用法例为新加坡《支付服务法》。《支付服务法》要求所有加密货币行业参与者必须登记并申请相关牌照，并对涉及虚拟货币的洗钱和恐怖主义融资提出防控风险。

2021上半年，全球主要国家开始加速落实对虚拟货币的监管，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，这仍是当前相关执法部门面临的最迫切的挑战。

1.3 多链迸发 DeFi 推向新高潮 安全成为生态维稳的基石

得益于以太坊拥堵带来的窗口期，DeFi 领域于2021年第一季度（Q1）拉开多链时代的大幕，交易所公链 BSC、Layer2 赛道内的 Polygon、新生代高性能公链 Solana、Fantom 都迅速在短期内积累了一定的生态规模。

数据显示，自2020年10月起，智能合约中的总锁仓值「TVL」呈指数增长。在多个扩展解决方案和 Layer-1 中，流向不同智能合约平台的资产从 172.3 亿美元增加到最高点 1292.9 亿美元，增长率达到 650%。从几乎全部虚拟资产锁定在以太坊中，转变为锁定在多条链上。

2020下半年在 Compound 催生的流动性挖矿热潮下，以以太坊为代表的 DeFi 生态迅速崛起，它在巅峰时期掌控着 75% 以上的 TVL，成为第一轮 DeFi 热潮的佼佼者。然而，受以太坊交易费用上涨的影响，2021年第一季度（Q1）开发人员和用户开始从具有潜力的公链中寻找交易手续费低、产品体验良好的替代品，此时，以太坊的主导地位开始下降。它迎来的第一个强有力的挑战者是币安智能链「BSC」。

在 1 亿美元的种子基金扶持和全球最大交易所为后备的支持下，BSC 开始迅速扩张其 DeFi 生态系统，并以低门槛、易操作两大催化剂结合可观的代币激励，吸引了大量新用户涌入，到2021年5月初，BSC 成功斩获 150 亿美元的 TVL，约占以太坊 TVL 的 13%。

凭借平台币 BNB 及其衍生产品（如 CAKE 和 XVS）在价格上的卓越表现，BSC 的 TVL 在2021年第二季度（Q2）前期翻了一番，达到 350 亿美元，但受到「5 · 19」大盘暴跌和持续高频的黑客攻击的影响，BSC 上的 TVL 出现回调。

值得注意的是，Polygon 的 TVL 在2021Q2从不到 5,000 万美元跃升至 50 亿美元，并且其整体增长趋势没有被「5 · 19」这一轮市场下行打乱，于6月15日突破 80 亿美元历史最高点。

Polygon 的强劲涨势得益于 DeFi 头部协议 Aave、SushiSwap 和 Curve 的多链部署，这些协议在2021年第二季度（Q2）初开始探索 Polygon 的可扩展性能力，试图解决在以太坊上交易堵塞的问题。基于这些头部协议强大的社区支持，用户迁移为 Polygon 带来爆炸性的增长。再者，Polygon 宣布推出 DeFiforAll 基金，较高的收益率在前期能够为其有效地吸引了那些希望快速获利的用户的雇佣资本，但这种激励机制的长远效果还有待时间的验证。

DeFi 生态的愈发多样化、丰富化，扩大了存放在各种协议中的有价资产规模，却也加速了黑客和作恶者的「收割」。

据 PeckShield「派盾」统计，截至2021年6月30日， DeFi 安全事件达到 86 起，损失逾 7.69 亿美元，同比增长 2100%，是2020全年 DeFi 安全事件损失的 3 倍。

频发的 DeFi 安全事件倒逼行业参与者反思现存的安全漏洞问题，促使他们提高对生态安全性的重视程度，生态安全不仅紧系用户的信心，而且在市场行情大幅震荡时，尤其是从增量市场变为存量市场以后，各个公链生态需要寻求新的突破点，公链作为维系整个生态发展的基石，只有加强生态安全才能确保整个生态可持续、稳定的发展。

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2020年10月全国范围内积极开展「断卡」行动，严厉打击整治非法开办贩卖电话卡、银行卡以来，传统洗钱渠道遭遇沉重打击，作为非法赌博、勒索、欺诈、恐怖融资等上游犯罪的「链条下游」，具有匿名性、复杂性和跨国性的虚拟货币越来越受到犯罪分子的青睐，虚拟货币跨境洗钱的形势愈发严峻。

据中国裁判文书网显示，近年来，以虚拟货币为案由的案件持续增长。数据显示，2016年与虚拟货币相关的案件文件仅有 390 篇，2020年已增长至 1761 篇。

PeckShield「派盾」研究发现，由于比特币等虚拟货币具有匿名性、跨国性和抗审查性，勒索软件、恐怖组织利用虚拟货币进行勒索、融资的行为激增，涉及虚拟货币的安全事件已经上升至国家安全层面。对于洗钱团伙及其上游犯罪的全链条打击，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。

再者，随着 DeFi 生态的蓬勃发展，更复杂的用虚拟货币洗钱的模式已经出现。除了常用的中心化混币服务、跨链交易用于模糊资金源头，「洗白」虚拟货币，利用协议实现自动化混币的去中心化的混币服务器的出现，为黑客、欺诈者打破了去中心化与中心化机构之间的壁垒，为犯罪分子持有的虚拟货币多加了一层，甚至几层保护膜，给相关司法部门在追踪、取证上带来更大的挑战。

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。

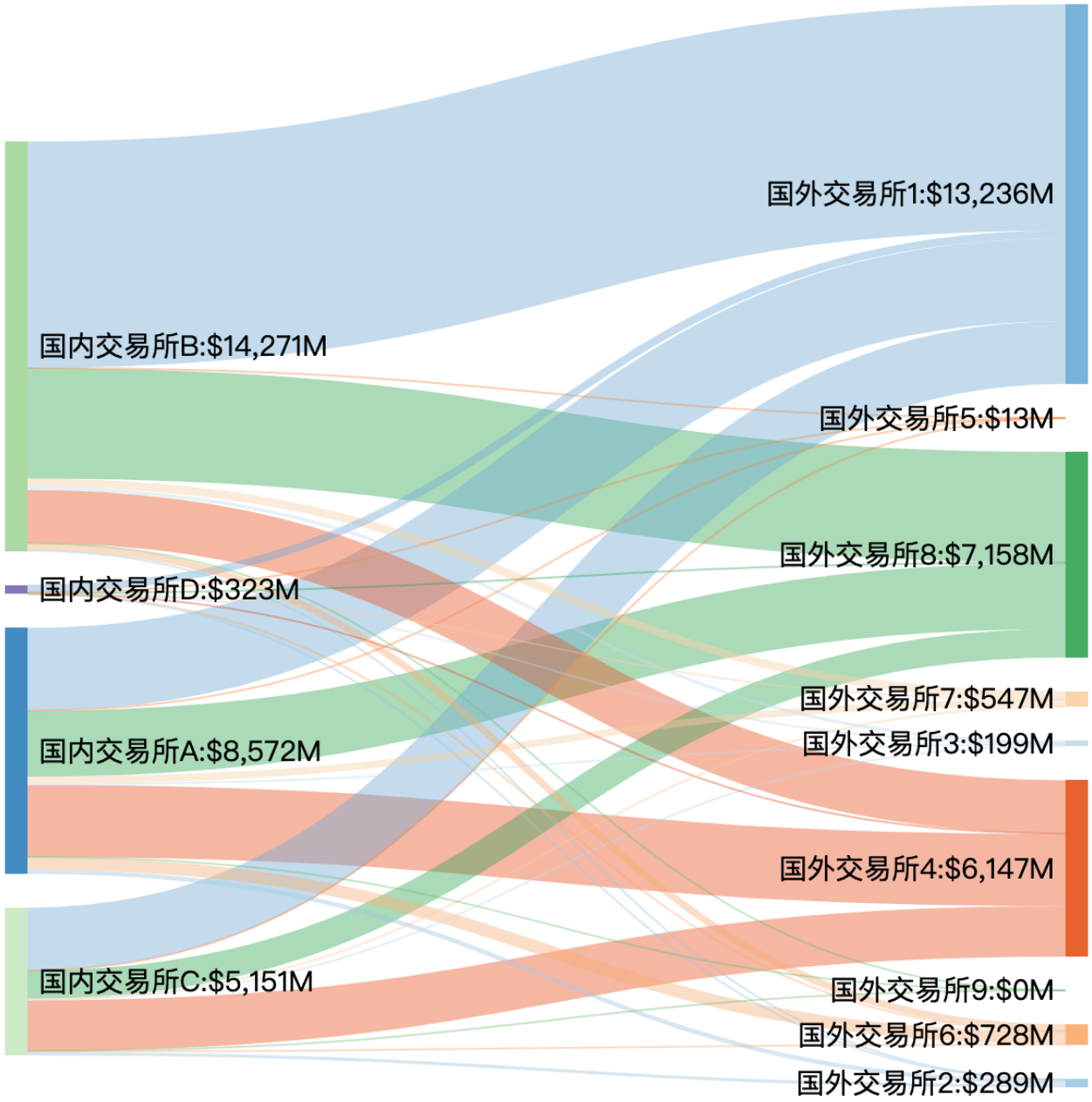

图3 2021上半年从国内向国外各大交易所流出的资金总量

如图3所示，在世界主要交易所中，我们用主要用户分布于中国内地和香港的四家交易所来代表国内，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。

2021上半年从国内交易所流出到国外交易所的资金总量达到 283 亿美元，较2020全年增长了 62%。以 BTC 为例，按交易时价计算，2019全年为 114 亿美元，2020全年为 175 亿美元，2021年仅上半年的 BTC 流出资金总量是2020全年流出的资金量的 1.6 倍，这主要是源于 BTC 价格在上半年前期持续攀升。

图4 2021上半年从国内交易所流出到国外交易所的 BTC 数量和资金总量

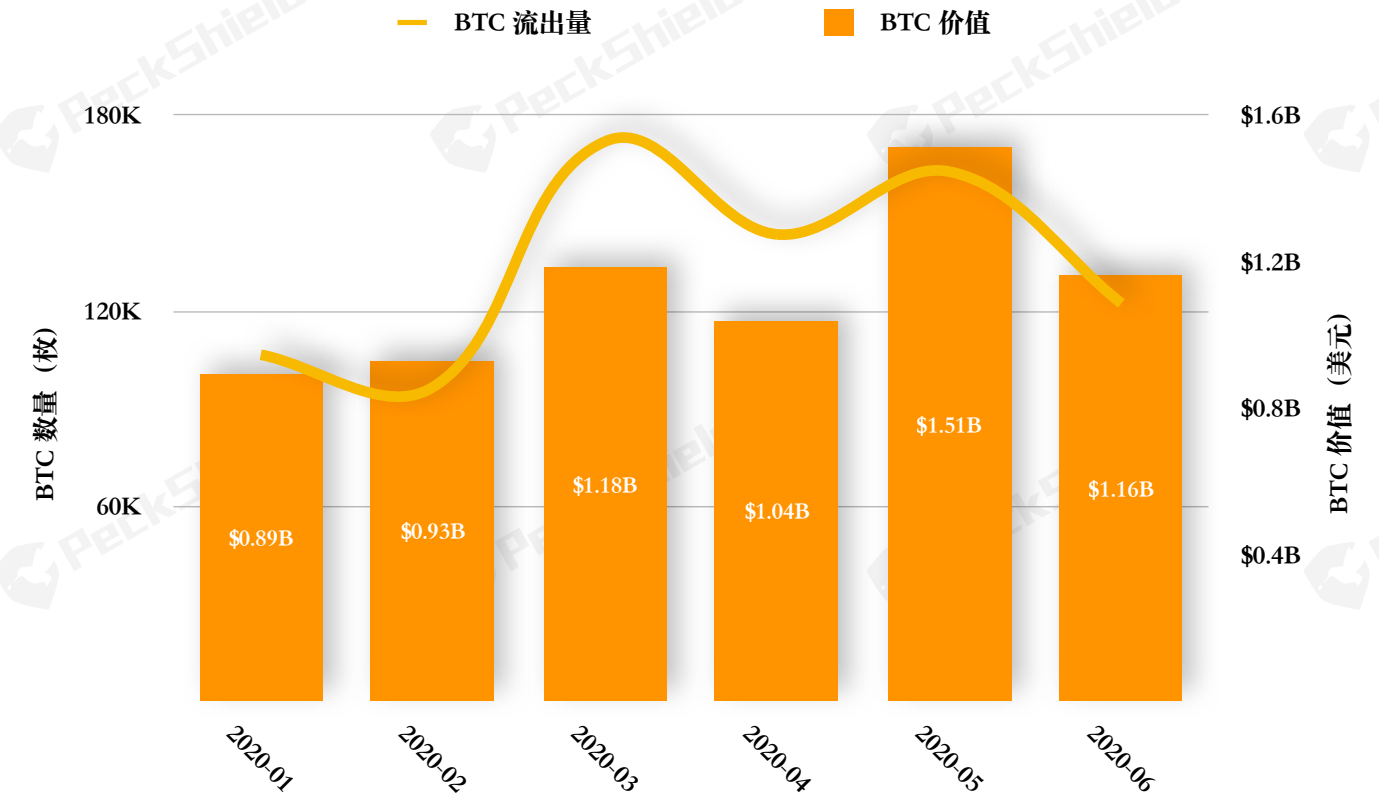

图5 2020上半年从国内交易所流出到国外交易所的 BTC 数量和资金总量

从图4和图5中可以看出，从1月到4月，BTC 价格不断攀升，从国内交易所流出到国外交易所的 BTC 资金总量也呈上升趋势；而5月至6月，由于国内政策在挖矿、交易上加强监管

力度，流出量呈现出下降的趋势。

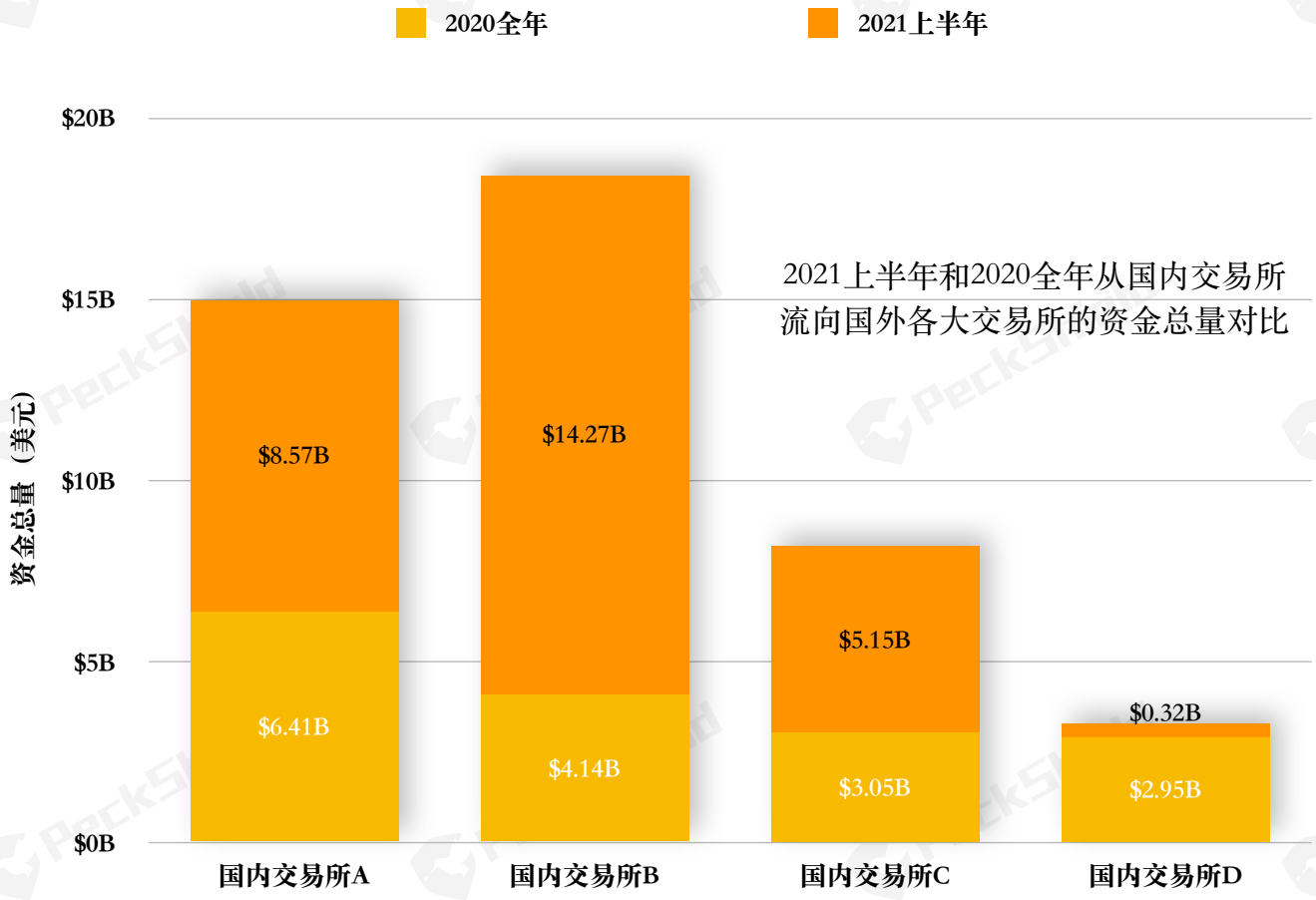

图6 2021上半年和2020全年从国内交易所流向国外各大交易所的资金总量对比

如图6所示，国内交易所 A、B、C 在2021上半年流出的资金总量分别为 85.7 亿美元、142.7 亿美元和 51.5 亿美元，较2020年全年流出的资金总量增长了 33.7%、244.7%、68.8%；国内交易所 D 在2021上半年流出的资金总量为 3.2 亿美元，较2020年全年流出的资金总量大幅下降，下降了 821.9%。

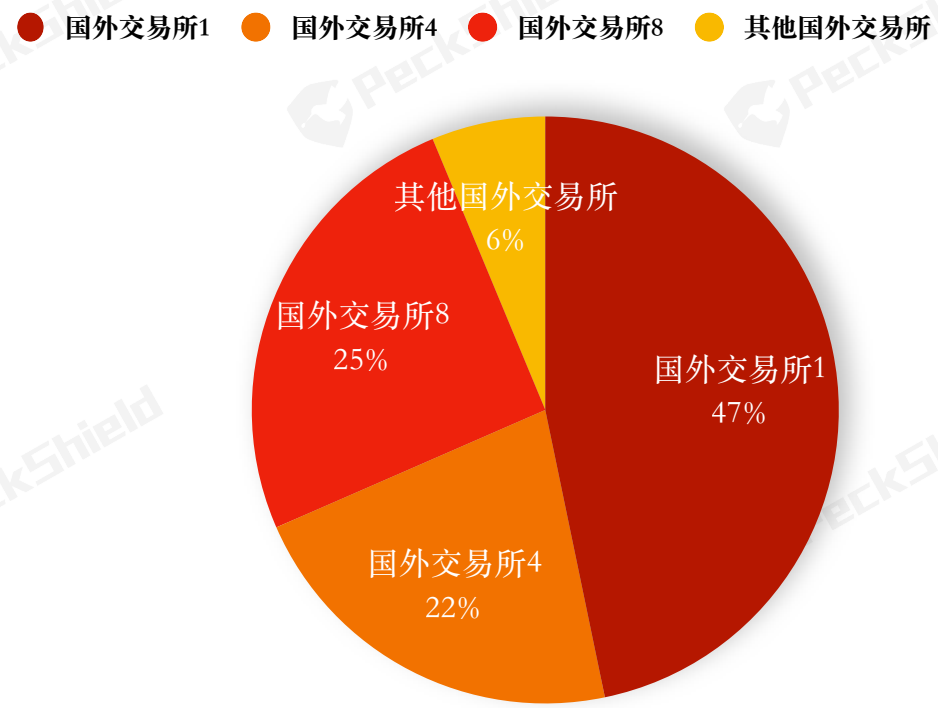

图7 2021上半年流向国外各大交易所的资金总量占比

如图7所示，在2021上半年国内交易所向国外交易所流出的资金总量中，流向国外交易所1、4、8 的资金量较2020年同期都有所增长，分别同比增长 292%、70%、55%；流向国外交易所 2、3、5、6、7、9 的资金量较2020全年都有大幅下降，下降比例分别为 86.8%、92.6%、99.5%、67.8%、39.6%、100%。从国内交易所流向国外交易所的增减比例可以看出，各国监管政策的不同，使得交易所的行业格局悄然变化。

从 BTC 流出量看，2021上半年 BTC 流出量较2020年同期有所减少。2021上半年 BTC 流出量为 620,322 枚，2020年同期 BTC 流出量为 804,175.49，2021上半年较2020上半年减少了22.9%。2021年1月从国内流到国外的比特币数量最多，达到 115,991.75 枚，较去年上半年最高点 172,115.39 枚下降了 48%。而今年3月从国内流到国外的比特币价值达到全年最高，逾 56 亿美元，较去年最高点翻了一番，这是由于自2月17日以来，比特币单价屡破新高，先是站上 50,000 美元，随后于4月15日站上迄今为止的最高点 63,109.7 美元。

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。

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：OKEx、火币、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。

四、DeFi 行业安全现状

4.1 DeFi 安全事件概览

2021上半年，DeFi 总锁仓量持续增长，于 5 月超过 1000 亿美元的规模，有价资产规模的跃升，也使其成为攻击的「重灾区」。

截至2021年6月30日， DeFi 安全事件达到 86 起，损失逾 7.69 亿美元，同比增长 2100%，是2020全年 DeFi 安全事件损失的 3 倍。

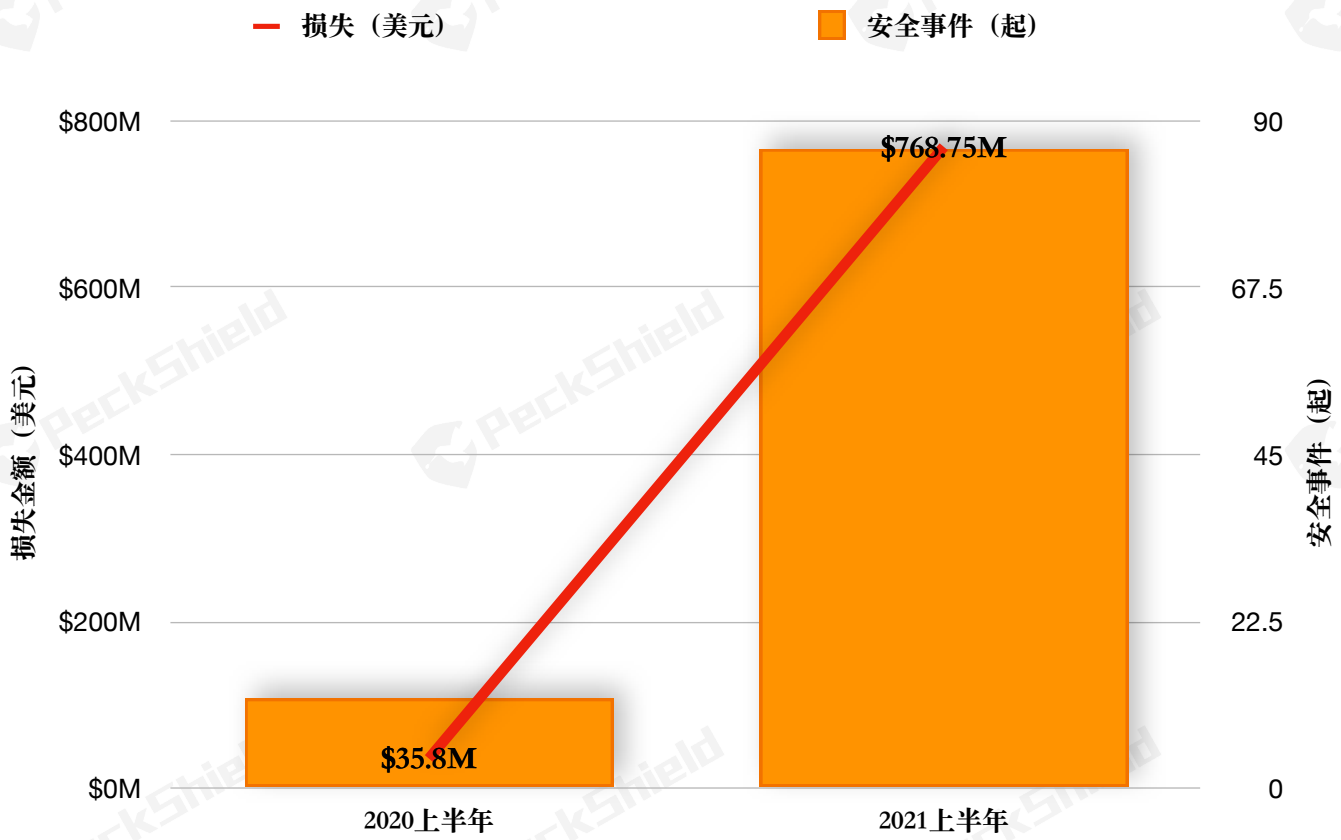

图8 2021上半年与2020上半年 DeFi 安全事件数量和损失对比

如图8所示，2021上半年 DeFi 安全事件统计，较2020上半年骤增，2020年上半年 DeFi 安全事件仅 12 起，2021上半年则达到 86 起，同比翻了近 7 番。2021上半年 DeFi 安全事件造成损失 7.69 亿美元，2020年上半年损失为 3,580 万美元，同比增长近 2,100%。

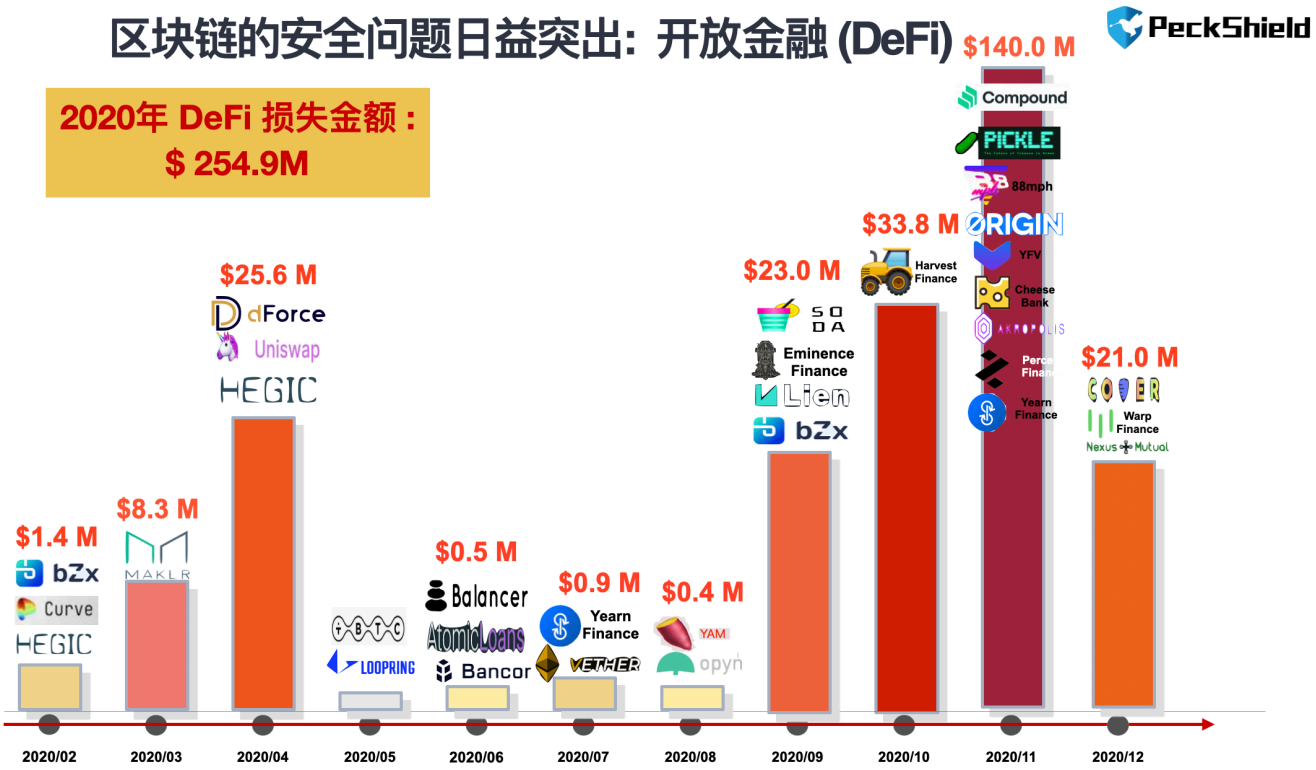

图9 2020全年 DeFi 安全事件数量和损失统计

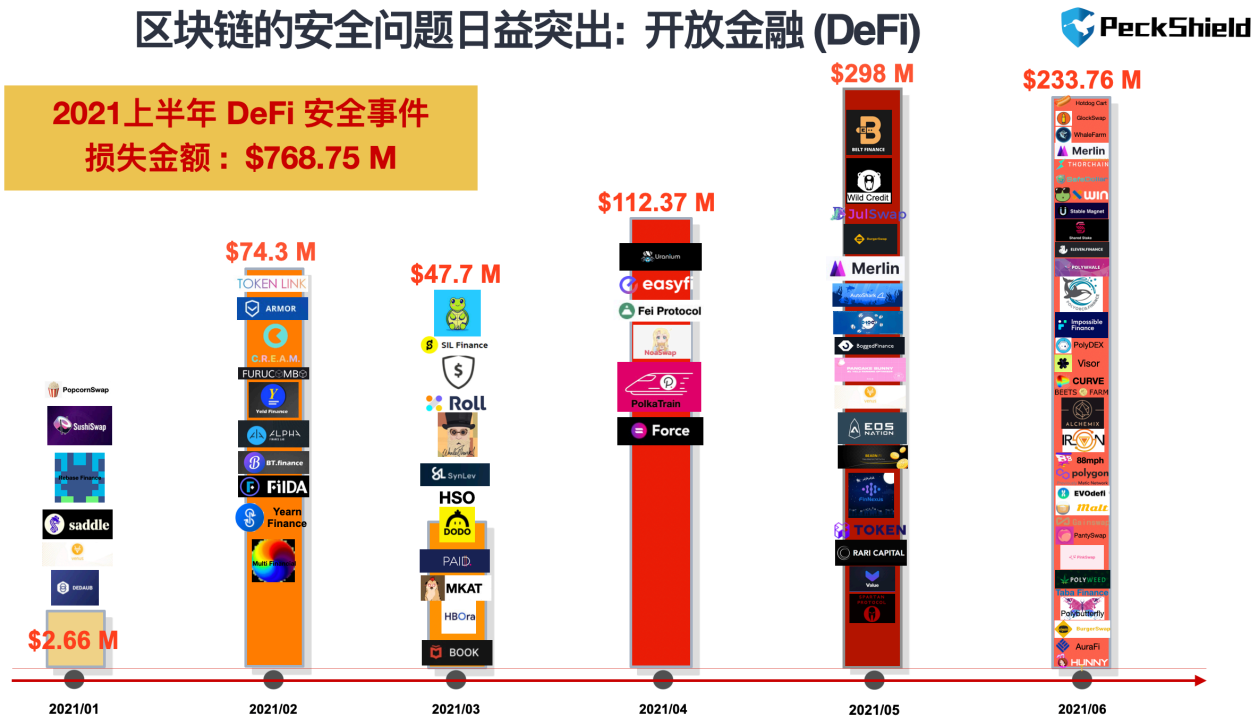

图10 2021上半年 DeFi 安全事件数量和损失统计

此外，从图9和图10来看，2021上半年发生的 DeFi 安全事件无论是从数量上，还是损失金额上都远远超过2020全年 DeFi 领域发生的安全事件。

2020全年共计发生 60 起 DeFi 安全事件，损失约 2.5 亿美元。值得注意的是，2020年 DeFi 安全事件几乎全部发生在以太坊上，且在2020年11月攻击频率最高。

2021上半年 DeFi 安全事件呈现出多链爆发的趋势，特别是前 5 个月迅速崛起的 BSC，它在2021年5月遭到高频攻击，损失金额占当月总损失额的 85%。由于 BSC 生态系统以成功复刻基于以太坊的应用为特色，一方面，有利于 BSC 快速蚕食以太坊生态的市场份额；另一方面，同质化协议的占比过大，也让攻击者更容易通过同源漏洞获利。

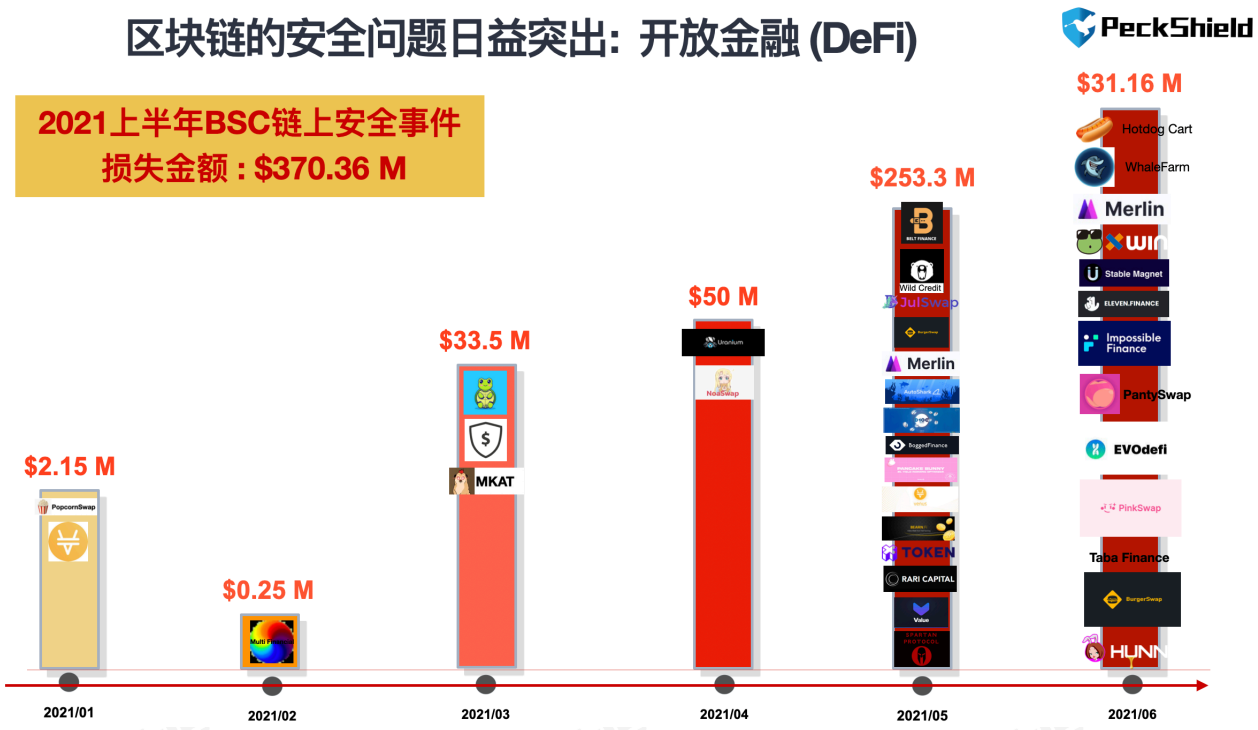

图11 2021上半年 BSC 链上安全事件数量和损失统计

4.2 2021上半年 DeFi 安全事件统计分析

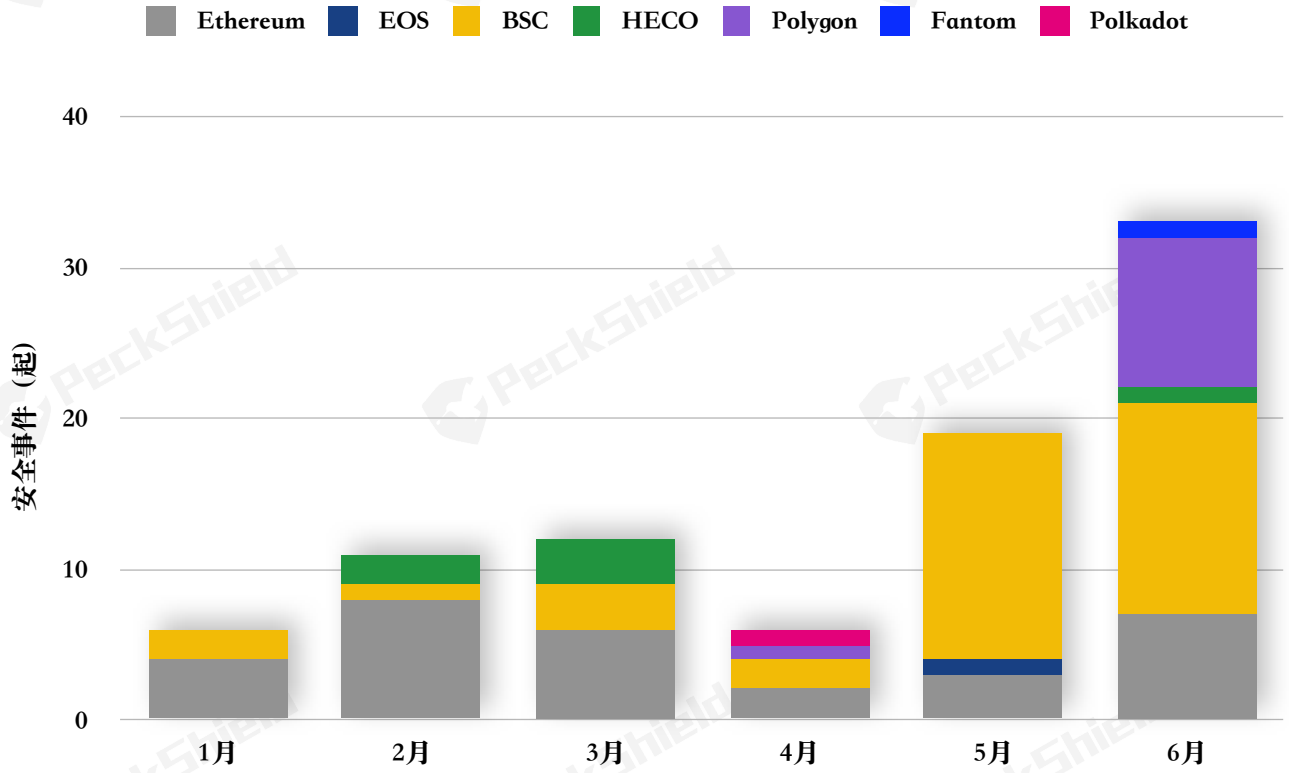

图12 主要公链1月至6月安全事件分布统计

如图12所示，2021上半年 DeFi 安全事件主要分布在以太坊、BSC、HECO、Polygon、Fantom 和 Polkadot 等公链上。

2021年2月以太坊上的 DeFi 安全事件达到小高点，随后呈现出趋于稳定波动的状态。BSC 上的 DeFi 安全事件在今年 5 月到达峰值，Polygon 上的安全事件则在 6 月呈现出增长的趋势。

相较于2020全年 DeFi 安全事件主要集中在以太坊上，2021上半年 DeFi 安全事件出现多链迸发的趋势。这主要是源于自2021年初以来，以太坊公链上的 DeFi 生态发展趋势放缓。2020年3月 DeFi 的爆炸式增长带来以太坊链上交易的需求激增，同时也再次暴露出以太坊手续费高、可扩展性差的沉疴。

虽然以太坊 2.0 试图解决这些问题，但改进并非一朝一夕的过程，在此期间，其他交易手续费低、出块速度快的解决方案逐步搭建起自己的 DeFi 生态，并借机从以太坊引流。

为分流以太坊上的用户，各公链生态中的 DeFi 协议使出浑身解数，以丰厚的流动性挖矿收益、社区激励和显著的赚钱效应吸引用户参与，那些在以太坊上没有吃到红利的用户，

在 FOMO（Fear of Missing Out）情绪的冲击下，争相成为第一个吃螃蟹的人。

用户极高的参与度，推动了生怕错过各类飞速发展的 DeFi 协议迭代，一些未经审计的合约，或者尚未审计完成的合约争先恐后地上线，由于 DeFi 协议内存放着各类有价虚拟资产，这使得它们成为被攻击的重灾区。

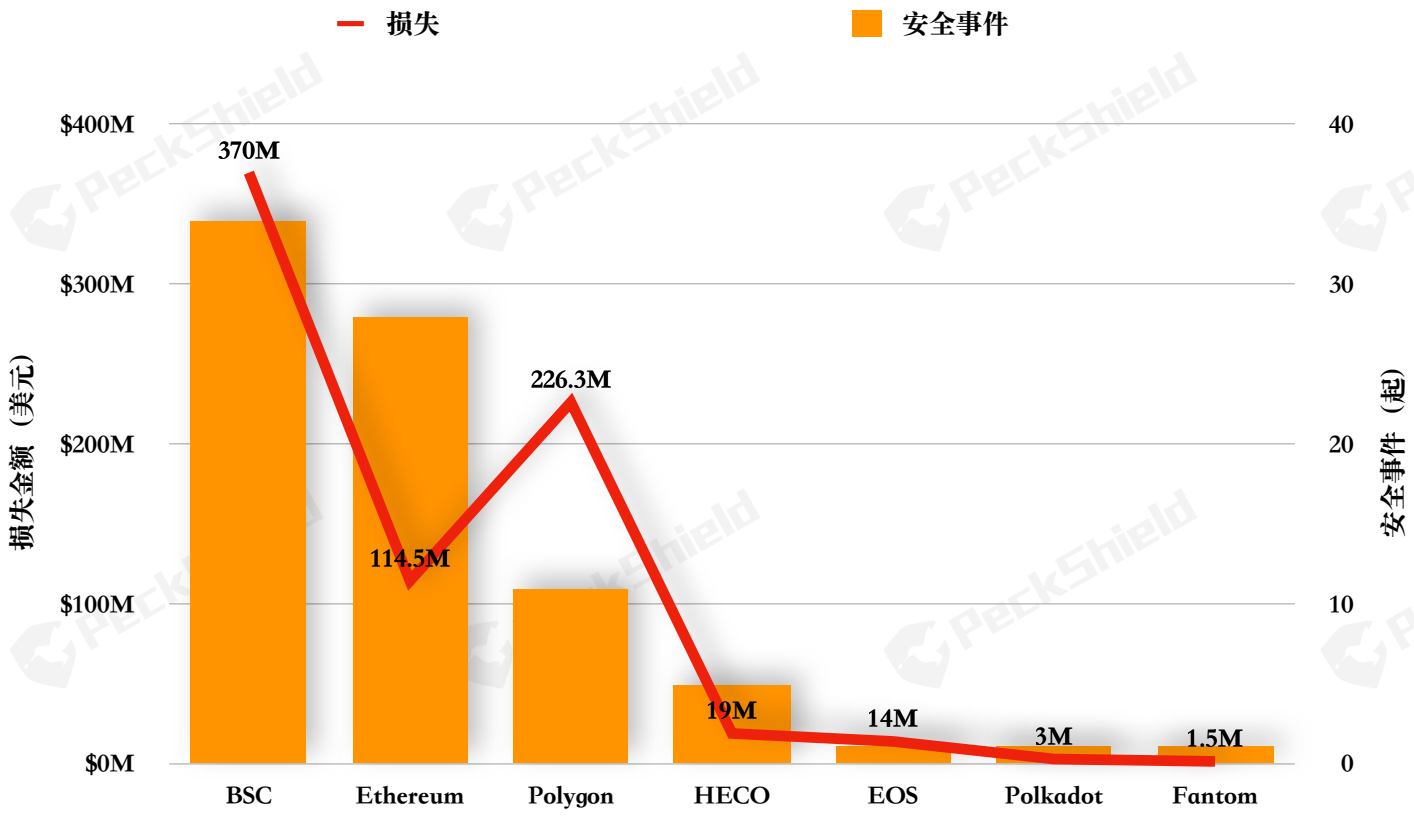

图13 主要公链1月至6月链上安全事件数量和损失统计

从图13可看出，攻击者跟着热钱跑。2020年第三、四季度刚上线的币安智能链（BSC）和火币生态链（Heco）在2021年第一季度的热度不断攀升，这也让攻击者们蠢蠢欲动。而2021第二季度除了以太坊，安全事件多集中在 DeFi 生态趋于成熟的 BSC，和崭露头角的以太坊侧链 Polygon 上显现。

从各链上发生的安全事件造成的损失来看，在这半年内，BSC 上的安全事件造成的损失位居榜首，达到近 3.7 亿美元，其次是 Polygon，达到 2.27 亿美元，以太坊位列第三，造成损失近 1.14 亿美元。

BSC 和 Polygon 上的安全事件造成的损失数额较大，一是 BSC 和 Polygon 的平均锁仓量、平均交易量和平均地址数综合表现在2021上半年明显好于其他链；二是这两条链出现了现象级的项目，例如，BSC 上的 PancakeSwap 和 Venus、Polygon 上的 QuickSwap，这些项

目不论是在锁仓量、交易量还是在地址数上都显著高于同链其他应用。尤其是 BSC 上的 PancakeSwap，其锁仓量曾一度超过以太坊上的明星项目 Uniswap；三是锁仓量不断攀升和高流动性吸引了一批已经有用户基础的 DeFi 协议也部署在这些链上。然而，锁仓量和交易量骤增不但会吸引用户参与，还会吸引伺机待发的攻击者和作恶者。

4.3 DeFi 攻击种类概览

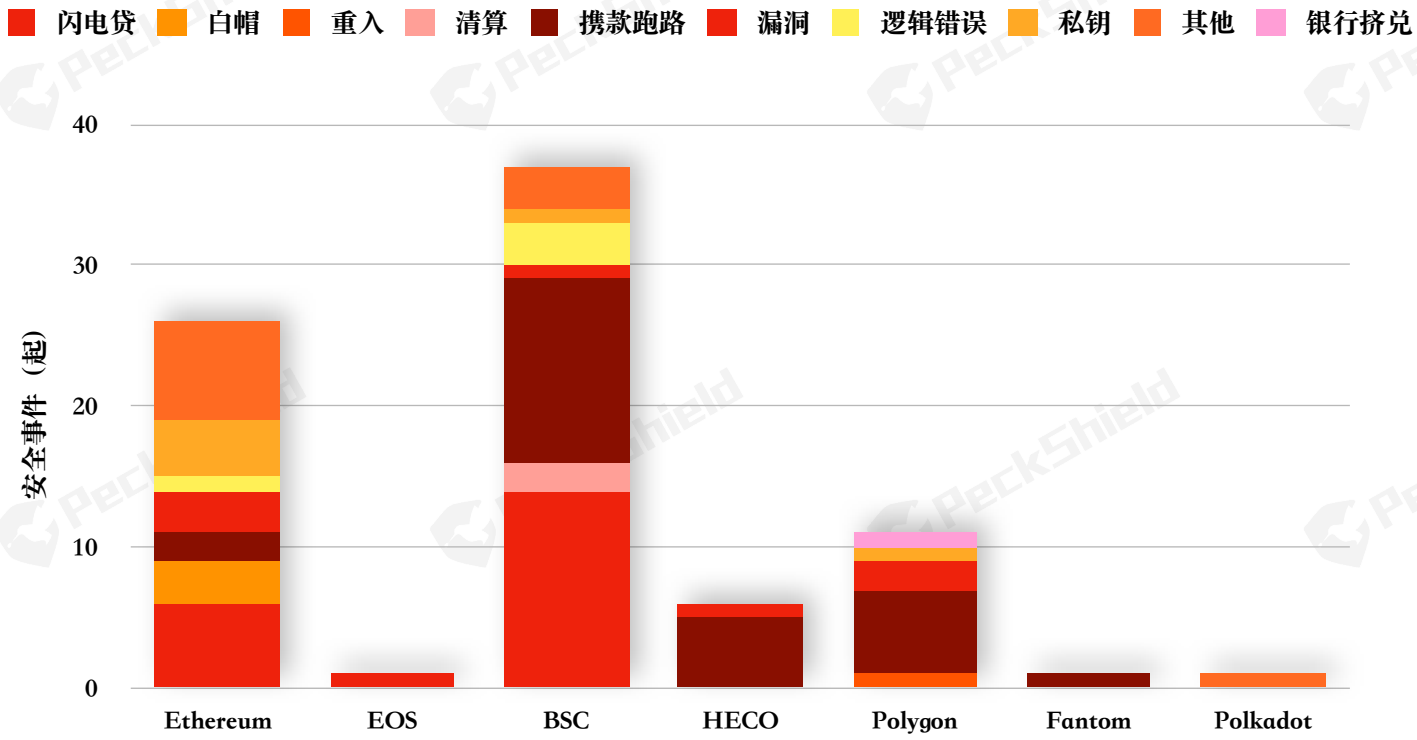

图14 各主要公链上 DeFi 安全事件主要攻击手段数量分布统计

据 PeckShield「派盾」统计，这 86 起 DeFi 安全事件中，至少有 15 种攻击手段，包括在 DeFi 协议中常见的闪电贷攻击、重入攻击、携款跑路、套利、代码漏洞、私钥泄漏/窃取、代币增发以及清算攻击，2021上半年还出现了银行挤兑的新型安全事件类型。

从数量上看，携款跑路位居榜首，达到 28 起。携款跑路是虚拟货币领域中的一种恶意操纵，它包含一些比较常见的攻击手段，例如，DeFi 协议的开发团队突然从流动性池子中撤走大部分流动性，流动性的突然移除可能会造成代币的死亡螺旋，因为代币持有者会试图尽快抛售手中的代币，来减小自己的损失，从而使得该项目的代币进一步在市场上抛售，最终代币趋于归零，项目崩盘。

由于这种类型的安全事件在技术上实施起来非常简单，通常情况下，作恶的项目参与方

只需投入较低的成本即可获得可观的利益，因此，它也成为作恶者首选的攻击手法。

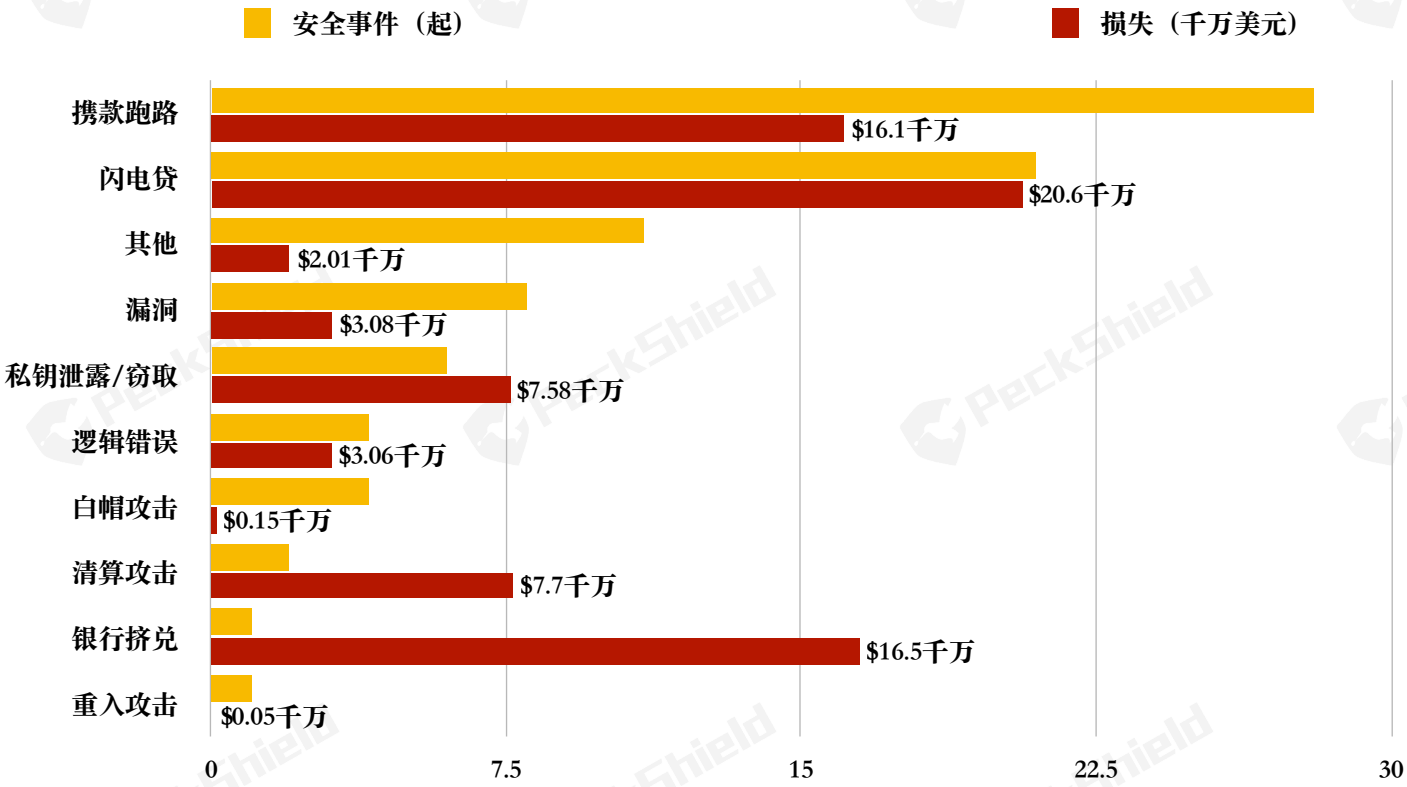

图15 DeFi 安全事件主要攻击手段数量和损失统计

据 PeckShield「派盾」统计发现，在公链的 DeFi 生态构建初期，攻击者倾向于利用这种简单粗暴的携款跑路圈钱。在2021年第一季度中，携款跑路占 BSC 链上安全事件的 66%；2021年第二季度，在刚刚积累起一定规模的 Polygon 上发生的 11 起安全事件中，携款跑路占 50% 以上。

其次，运用较多的攻击手段就是利用闪电贷的攻击，这也是自2020年 DeFi 兴起后攻击者最常用的攻击手段之一。攻击者借出闪电贷，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，并在一个区块交易中偿还闪电贷，完成攻击。

值得注意的是，2020年利用闪电贷的攻击集中发生在以太坊上，2021上半年利用闪电贷的攻击主要发生在 BSC 链上，达到 14 起，在以太坊上发生利用闪电贷的攻击达到 6 起，EOS 上发生 1 起。

从损失金额上来看，攻击者获利最多的仍是利用闪电贷的安全事件，损失超过 2 亿美元；其次是银行挤兑，损失达到 1.65 亿美元，位列第三的是携款跑路，损失达到 1.62 亿美元。

4.4 跨链资金流转统计与分析

2021上半年市面上涌现出了多条公链，且它们的资金量颇具规模，但不同的链间如同孤岛，不同链上的资产无法自由交换，此外，很多新兴公链仍缺失基础设施，因此，需要将其它链上的资产通过跨链的方式引入自身的公链，在当前常用的跨链方式中，除了中心化机构如交易所钱包中跨链提币服务之外，最常见的就是各种去中心化跨链资产桥。

跨链桥的出现不仅有效地打破了链与链之间的信息孤岛，还将各个公链的生态打通。但随着跨链桥生态愈发多样化、丰富化，PeckShield「派盾」发现攻击者将其视为资产出逃的重要环节，在帮助被盗或遭到攻击的项目追踪资产流转的过程中，我们发现攻击者成功得手后，55% 以上的交易通过跨链桥将资产快速转移，再结合混币服务将资产洗白，这种新兴的洗钱方式，给反洗钱工作提出新的挑战。

Date (UTC+8)	Protocol	Type	Cross-Chain Bridge
2021/7/1	yieldparrot.finance	Scam	
2021/6/29	Merlin Labs	Exploited	AnySwap
2021/6/25	xWin	Exploited	-
2021/6/24	StableMagnet	Exploited	AnySwap、Binance Bridge
2021/6/22	ElevenFinance	Exploited	AnySwap
2021/6/22	ElevenFinance	Exploited	-
2021/6/21	Impossible Finance	Exploited	AnySwap
2021/6/10	EvoDefi	Exploited	-
2021/6/5	BurgerSwap	Exploited	-
2021/6/3	PancakeHunny	Exploited	-
2021/5/29	Belt Finance	Exploited	-
2021/5/28	JulSwap	Exploited	AnySwap
2021/5/28	BurgerSwap	Exploited	AnySwap
2021/5/26	Merlin	Exploited	-
2021/5/24	Autoshark	Exploited	-
2021/5/22	Bogged Finance	Exploited	AnySwap
2021/5/20	PancakeBunny	Exploited	
2021/5/19	Venus	Exploited	
2021/5/18	BinanceGoat	Scam	
2021/5/17	bEarn	Risk	-
2021/5/16	bEarn	Exploited	RenBridge、AnySwap
2021/5/14	Chemix	Exploited	RenBridge
2021/5/9	PumaSwap	Rug Pull	AnySwap
2021/5/9	HyperGalaxy	Rug Pull	-
2021/5/8	ValueDeFi	Exploited	Binance Bridge、AnySwap
2021/5/6	ValueDeFi	Exploited	AnySwap
2021/5/2	Spartan	Exploited	AnySwap
2021/4/28	Uranium	Exploited	Binance Bridge、AnySwap、POA Network
2021/4/29	DogFather	Risk	-
2021/4/21	Safemoon	Risk	-
2021/4/11	NoaSwap	Scam	

图16 利用跨链桥转移攻击获利虚拟货币

4.5 DeFi 安全事件典型案例

4.5.1 闪电贷攻击

今年5月起，继 PancakeBunny 遭到闪电贷攻击之后，复刻 Bunny 的同源攻击呈现出多米诺效应，包括 AutoShark、Merlin、PancakeHunny 等 DeFi 协议接连遭到攻击。

从2020年11月在以太坊上激增的闪电贷攻击，再到今年5月 BSC 爆发的闪电贷攻击，闪电贷攻击是 DeFi 的潘多拉魔盒吗?

事实上，闪电贷本身并不是一种作恶工具，而是一项非常有意义的金融创新，它利用区块链技术，将传统借贷市场无法实现的事情带来一种新的可能。理论上，闪电贷借贷允许用户通过无抵押的方式借出流动性池内的所有通证，并要求用户在进行一系列互换抵押清算操作之后、交易结束之前归还所借通证以及固定的借贷成本。

DeFi 协议的同源闪电贷安全事件频发，主要源于这些项目存在同质化的问题，开发者单纯地复刻「Fork」明星项目的源代码，但忽略了理解这些代码背后逻辑的重要性。这体现在运维、管理、与其他协议互动，以及在参数设置、风险控制点，甚至包括在一些预言机（Oracle）价格的使用方案上，他们可能不如原创团队考虑得周全，这也就为之后的安全事件埋下了隐患。

事实上，闪电贷攻击并非无解，在这场长达一年的闪电贷攻击「攻防战」中，PeckShield「派盾」联合多方行业参与者，竭力追回攻击造成的损失，以及帮助遭攻击协议开发者避免更大的损失。

6月23日，PeckShield「派盾」预警定位到曾攻击过 Impossible Finance 协议的攻击者利用 ElevenFinance 协议的漏洞进行闪电贷攻击，攻击者先后共计获利 100 万美元。

PeckShield「派盾」第一时间定位并分析漏洞根源，积极与协议开发团队沟通，并提出有效的安全方案。同时，启动 PeckShield「派盾」旗下反洗钱态势感知系统，实时追踪攻击者的资金流转。

在 PeckShield「派盾」的协助下，社区定位到潜在的攻击者，并积极与其交涉。最终，Impossible Finance 攻击者先后于6月25日和6月30日，分三次将全部攻击所得归还给 Impossible Finance，将部分攻击所得归还给 Eleven Finance。

4.5.2 银行挤兑

在传统金融领域，如果银行券持有人或存款人对发行银行的信用产生动摇，或银行券贬值，银行券持有人急于银行券抛出，来防止经济上蒙受重大损失，在这两种情况下，银行券持有人或存款人会涌入银行提款，当此时银行准备金不足，银行券兑现发生困难，就会发生挤兑。

在 DeFi 领域也出现了银行挤兑的情况，且造成 1.65 亿的损失。2021年6月18日，Polygon 链上的部分算法稳定币 IRON Bank 在一夜之间从锁仓 24 亿美元，稳定币发行量超过 7 亿走向治理代币归零，主要源于发生「银行挤兑」。

IRON Finance 是采用稳定币 IRON + 治理代币 TITAN 双币机制的部分算法稳定币。一旦有大户开始抛售，治理代币价格下跌，赎回稳定币 IRON 时由于会产生与下跌前同等价值的 TITAN 代币，使得流通中的 TITAN 代币数量大幅增加。增发的代币再次流向市场，导致价格继续下跌，流动性挖矿产出的价值减少，使用 IRON/USDC 交易对进行挖矿的用户开始退出并赎回 USDC 和 TITAN，稳定币铸币用户需要收回成本，赎回的 TITAN 部分被兑换为稳定币等价值稳定的资产。

最终，用户持有资产中的所有 TITAN 流向二级市场，提供流动性的用户成为接盘侠。值得注意的是，随着 TITAN 价格的下跌，赎回同等价值的资产，会导致 TITAN 流通量的骤增。从官网文档中可以看到，TITAN 的总发行量为 10 亿枚，但在一夜之间却额外增发了上万倍，其原因很可能是由于协议进入死亡螺旋的过程中，需要增发更多的代币用于铸币者赎回资产。

由于 IRON 中的大部分稳定币 USDC 会被存到 Aave 中产生收益，当用户涌入赎回 USDC 时，协议中没有预留足够多的 USDC，协议就会暂停所有用户的赎回行为，等待从 Aave 中提取资金。可以预料，如果项目方不采取其它措施，赎回之后的TITAN部分会继续流向市场。

TITAN 在第一次从 65 美元跌至 30 美元后，又升至 52 美元，IRON 恢复锚定。北京时间6月17日凌晨，大户再次开始抛售，卖出 TITAN 兑换 IRON。由于预言机价格每 10 分钟根据 TWAP 更新一次价格，由于现货的价格跌幅更大，用户恐慌抛售，价格下跌，进一步铸造更多的 TITAN，并形成负反馈循环，导致挤兑，造成损失 1.65 亿美元。

4.5.3 清算攻击

5月18日，BSC 上的借贷协议 VENUS 突发大额清算，产生 7,700 万美元的坏账。几个手攥 300 多万 XVS 的大户，花费几千万美金，在短短两个多小时里，把 XVS 的价格从 70 多美元直线拉升至 140 多美元。待 XVS 的价格稳定在 140 多美元后，这几个大户马上将手中的 XVS 进行抵押。质押了 200 万枚 XVS，贷出 4100 枚 BTC 和 9600 枚 ETH。与此同时，还有另外一个账户通过抵押 XVS 借出了 12,986 枚 ETH。等大户们把 BTC 和 ETH 借出来之后，XVS 的价格就开始迅速下跌，他们抵押的 XVS 也开始被平台陆续清算。最后，经过 XVS 的一路下跌，这场有预谋的操作给 VENUS 平台造成了接近 1 亿美元的坏账。

这并非 VENUS 平台遭到的第一次清算攻击，早在今年年初 VENUS 就因价值 1.57 亿美元的 CAN 借空其平台逾 2,000 枚比特币和 7,000 枚 ETH 而备受诟病。

4.5.4 解决思路

蓬勃发展的 DeFi 协议俨然成为黑客的「羊毛地」。由于缺乏法律监管使得黑客肆意攻击，联合虚拟货币的匿名的特性所带来的低风险、高回报，使得黑客攻击愈加猖獗，再加上，资金体量不断飙升的新兴协议大多依赖于复刻以太坊上的明星协议，这大大降低了黑客的时间成本和技术门槛。

PeckShield「派盾」建议新合约在上线之前除了要进行全面而专业的智能合约安全审计，排查已知的各类漏洞外，还要注意排查与其他 DeFi 产品进行组合时的业务逻辑漏洞，避免出现跨合约等逻辑兼容性漏洞。另外，更重要的是要引入一定的风控熔断机制，引入第三方安全公司的态势感知服务等，做到第一时间响应安全风险，及时排查封堵安全攻击。在攻击事件发生时，应联动行业各方力量，搭建一套完善的资产追踪机制，事后需做到查缺补漏，完善防御系统。所有的 DeFi 协议都存在着变数，即使一个小的更新，都有可能将 DeFi 协议置于风险之中。

五、虚拟货币重大安全事件概览

5.1 虚拟货币安全事件总体统计

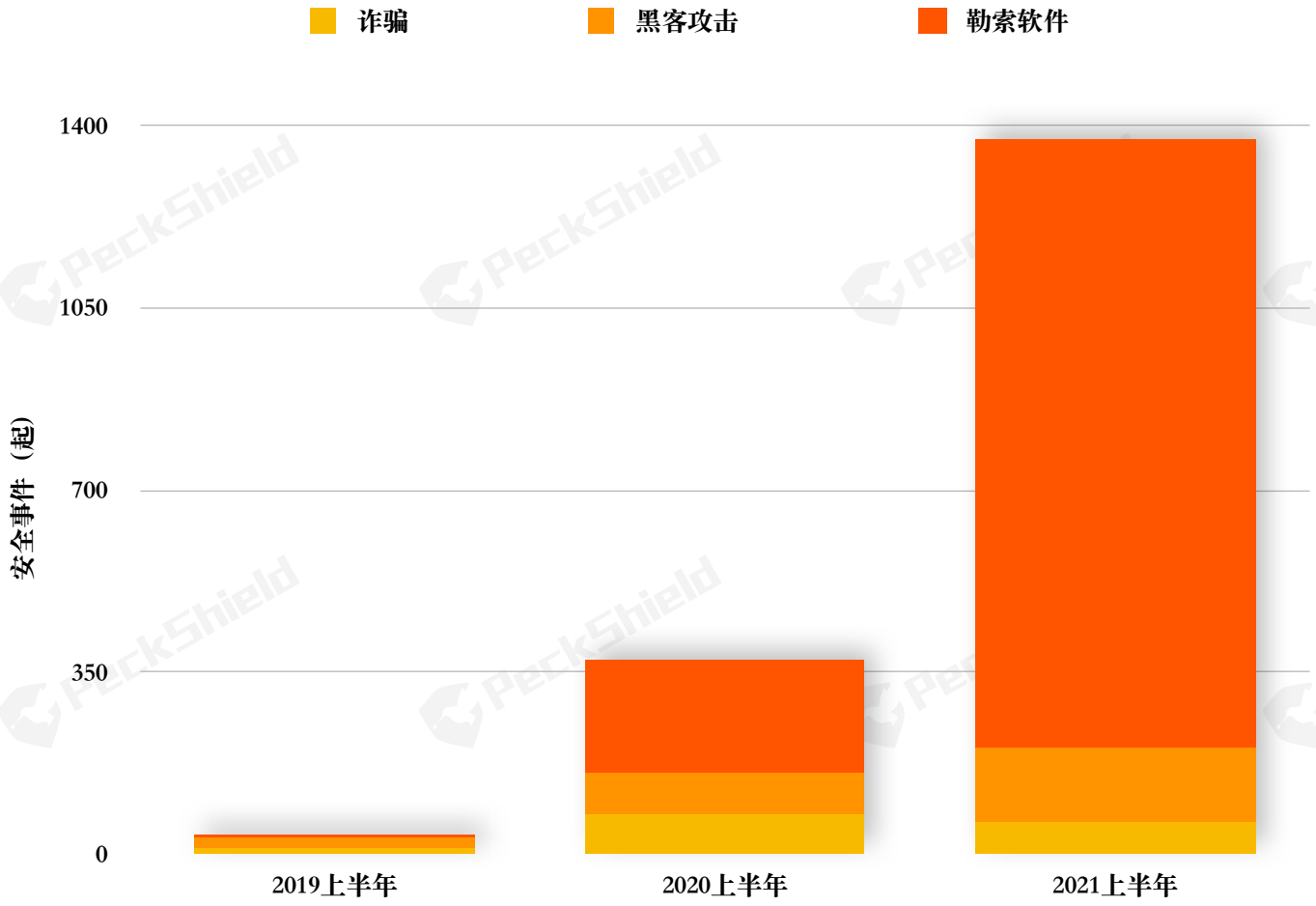

图17 近三年上半年虚拟货币安全事件统计

截至2021年6月30日，虚拟货币行业共发生重大安全事件 1,375 起，共计损失逾 142.4 亿美元，其中黑客攻击约 143 起，诈骗事件 60 起，勒索攻击约 1,172 起。

如图18所示，近三年上半年虚拟货币安全事件统计，2021上半年涉及虚拟货币的勒索事件较前两年成倍增长，2019年上半年勒索事件仅 6 起，2020年上半年增长了 36 倍，达到 218 起，2021上半年则快速增长至 1,172 起，同比增长 438%。

此外，黑客攻击也呈现出快速增长的趋势，2019年上半年黑客攻击达到 22 起，2020 年同比增长 263%，达到 80 起，2021上半年激增至 143 起。在2021上半年发生的 143 起黑客攻击中，有 60% 以上源于 DeFi 安全事件。

在各国政府加强出台与打击与虚拟货币相关的反洗钱、反欺诈政策和犯罪下，2021上半

年涉及虚拟货币的欺诈事件的数量呈现出小幅下降的趋势，2019上半年欺诈事件为 10 起，2020上半年达到 76 起，2021上半年下降至 60 起。

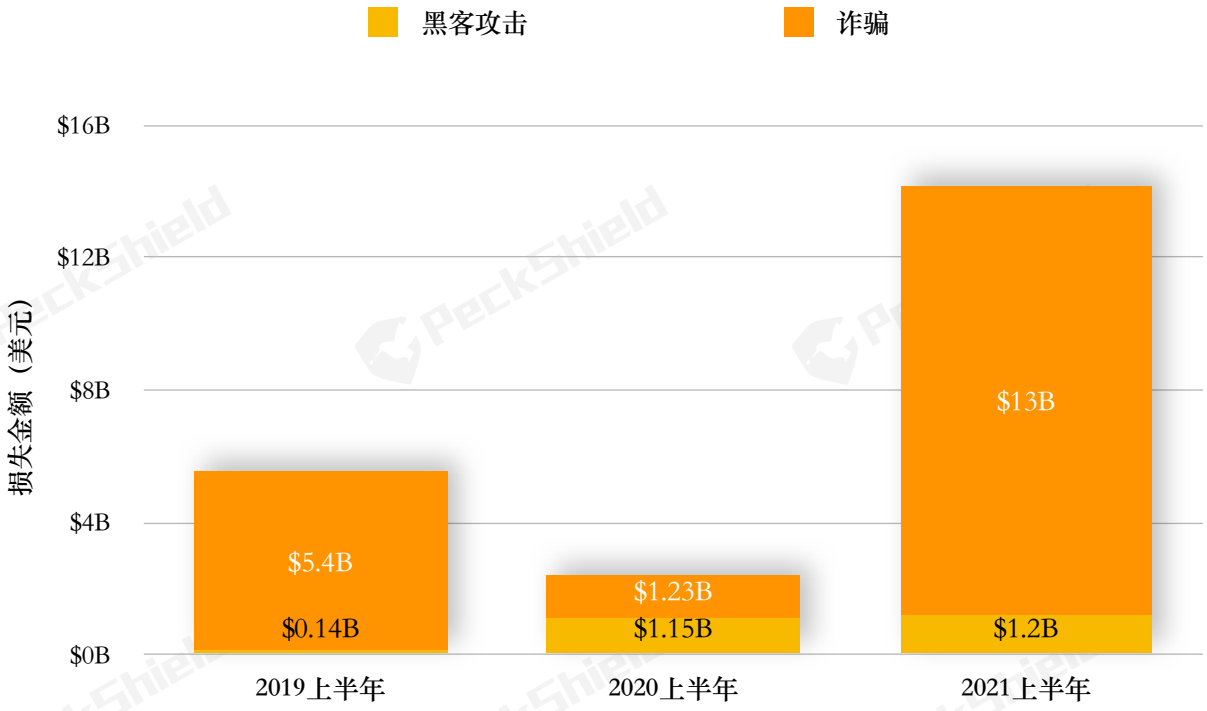

图18 近三年上半年虚拟货币安全事件造成损失统计

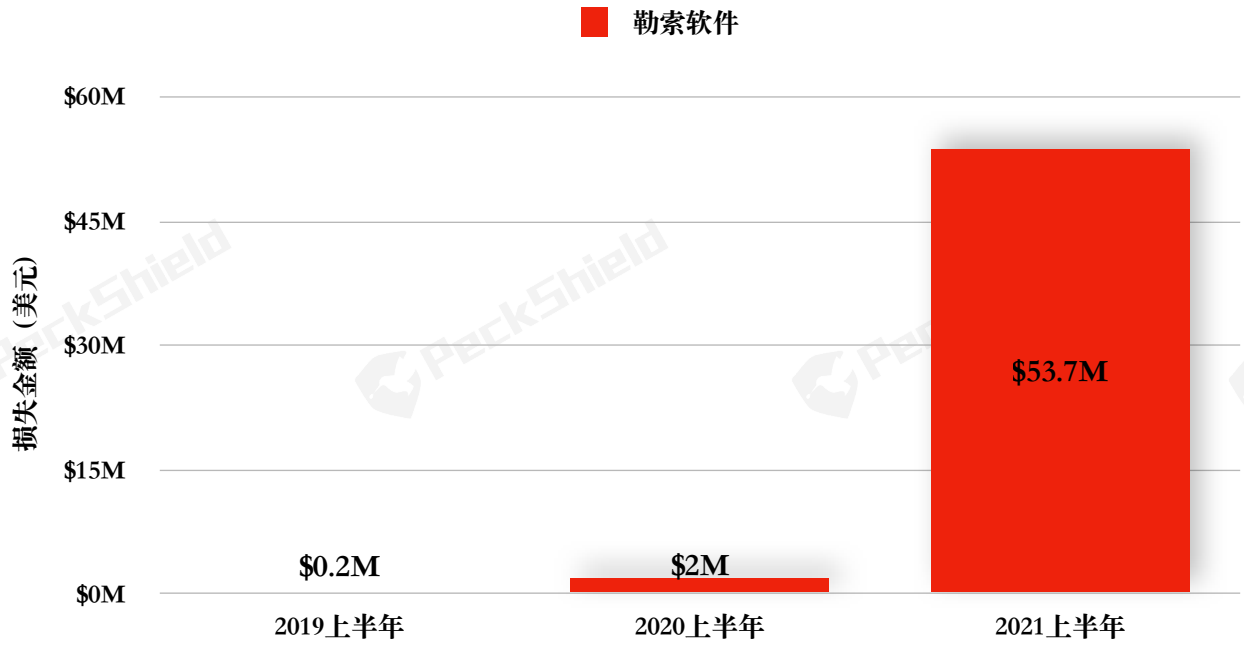

图19 近三年上半年虚拟货币安全事件造成损失统计

如图18和19所示，2019年上半年虚拟货币安全事件造成的经济损失高达 55.36 亿美元，其

中黑客攻击造成 1.36 亿美元损失，诈骗事件造成 54 亿美元损失，勒索攻击 20 万美元。

2020上半年虚拟货币安全事件造成经济损失近 24 亿美元，较2019上半年下降 56.6%，黑客攻击造成 11.5 亿美元的损失，其中 DeFi 安全事件造成 3,580 万美元的损失，诈骗事件造成 12.3 亿美元的损失，勒索攻击造成 200 万美元的损失。

2021上半年虚拟货币安全事件造成经济损失逾 142.4 亿美元，其中黑客攻击造成损失 12.09 亿美元，欺诈事件造成损失 130 亿美元，勒索事件造成损失至少 5,370 万美元。

5.2 2021上半年虚拟货币安全事件统计分析

2021上半年造成主要危害的仍是诈骗和洗钱事件，高额诈骗金背后有组织严密的团伙。值得注意的是，2021上半年在多链迸发和流动性挖矿的激励下，DeFi 领域在资金、用户和产品等方面的规模都再次有了质的跨越，但同时，也成为了攻击者重点「光顾」的领域，DeFi 安全事件在数量上和损失金额上呈现大幅增长，在今年上半年勒索攻击愈发猖獗。

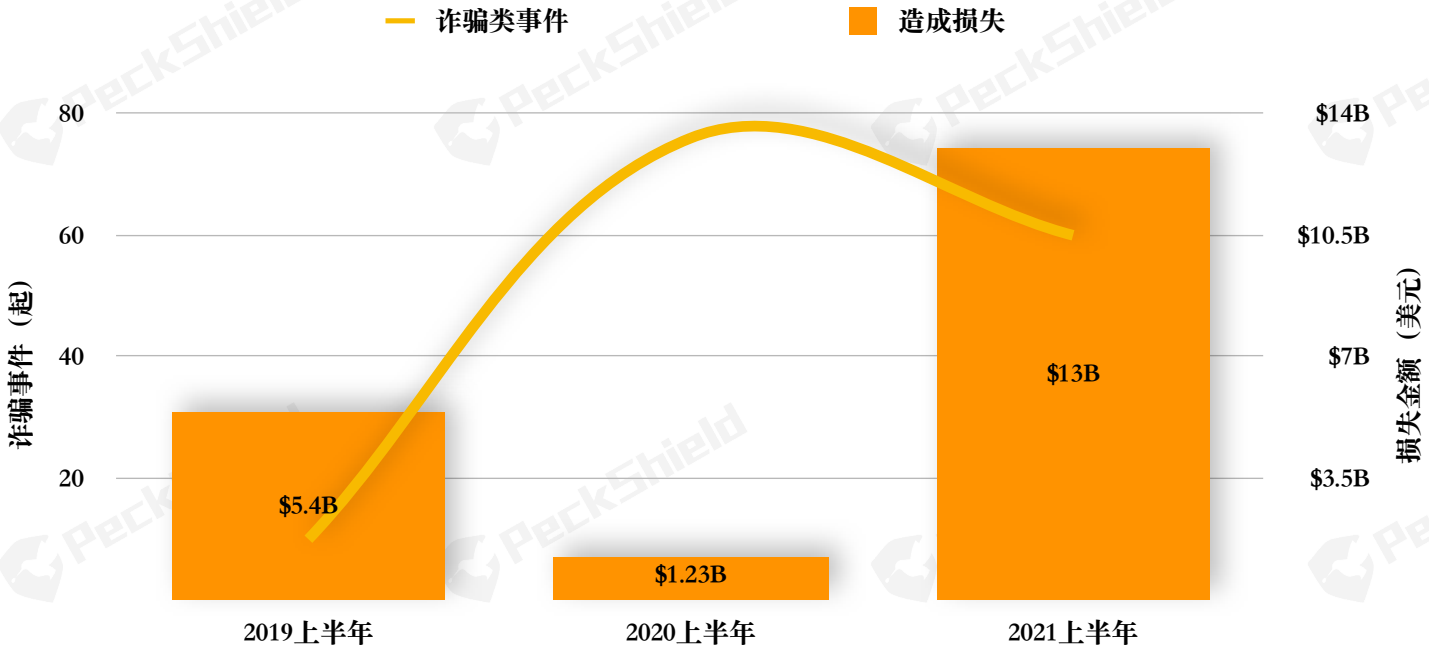

图20 近三年上半年虚拟货币诈骗类安全事件统计

如图20所示，2021上半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 130 亿美元，主要与参与庞氏骗局的韩国 V Global 虚拟货币交易所有关，该骗局在波及人数和损失金额上可与2019年我国破获的 PlusToken 媲美，V Global 受害者数量或达 6.9万人，经济损失达 34 亿美元。

相较2020上半年，2021上半年虚拟货币诈骗事件在数量上有所下降，但损失金额大幅上升，同比增长近 1000%。2021年年初在特拉斯购入比特币的示范效应下，比特币的价格屡破新高，越来越多的机构资金也涌入虚拟货币市场，同时比特币概念股、矿机、芯片在全球股市受到资本的热捧，全球比特币牛市行情让中国的虚拟货币交易重新活跃起来，但对于普通用户而言，虚拟货币领域技术和参与门槛仍相对较高，一些投机份子利用大众的知识盲区炮制各种骗局，据悉，仅利用特斯拉创始人马斯克喊单的骗局收益就达到 600 万美元。

除此之外，网络罪犯利用虚拟货币洗钱显现出新形态。在2021年3月19日，最高人民检察院、中国人民银行联合发布的惩治虚拟货币洗钱犯罪典型案例中，PeckShield「派盾」通过反欺诈态势感知系统 CoinHolmes 观察发现，犯罪嫌疑人通过购买比特币「矿工」密钥进行洗钱，并将洗白的赃款转出境外兑换使用。整个洗钱链路的走向十分隐蔽。在传统的洗钱案例侦查中，相关执法部门通常要跟着资金的流向走。但在该案中，明面上的资金流向是中断的，犯罪嫌疑人将钱从银行账户打给「矿工」，「矿工」将密钥发送给犯罪嫌疑人，两者之间银行账户并无来往，无法构成完整的洗钱链条，这不仅使侦查陷入困境，而且还绕过了外汇管制。

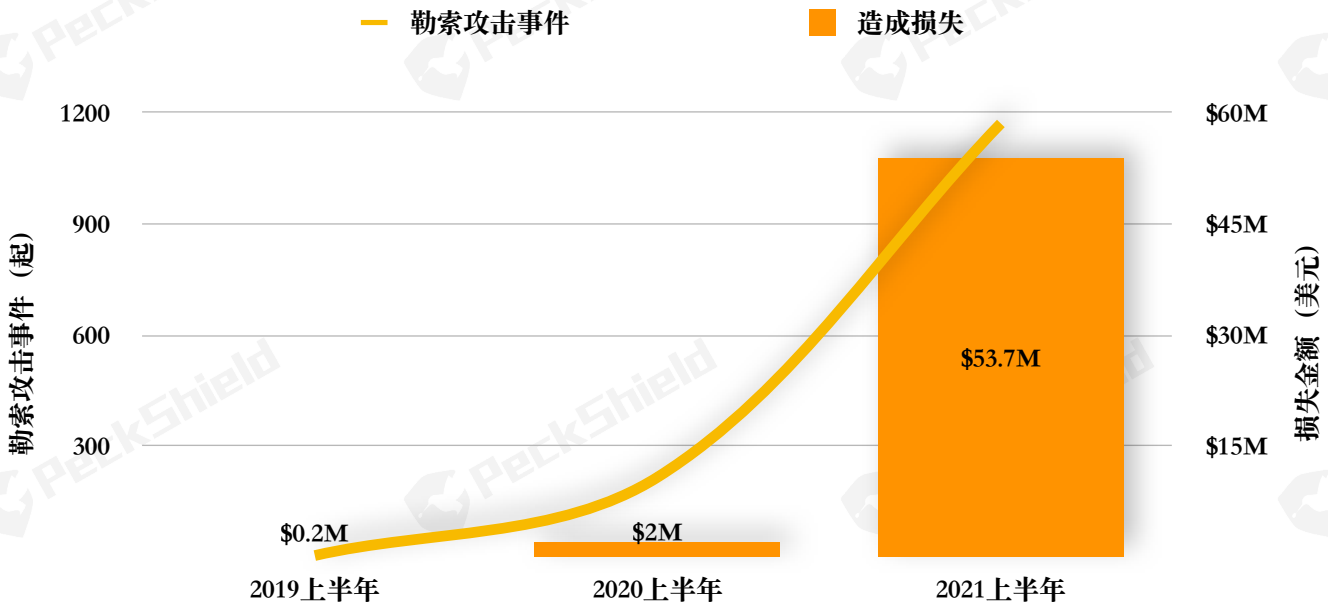

图21 近三年上半年虚拟货币勒索类安全事件统计

如图21所示，2021上半年，虚拟货币勒索攻击愈发猖獗，在过去的半年里，每天平均发生近 7 起勒索事件。勒索软件团伙呈现出更强的组织性、联盟性，不同犯罪组织相互配合，形成更广泛、完整的犯罪生态，此外，勒索攻击不再拘泥于广撒网的模式，而是呈现出定向攻击的新形态，针对高价值目标的定向攻击越来越多。

勒索攻击开始走向产业化，攻击手段愈加专业化、系统化、分工更加细化；勒索者将虚拟货币和勒索产业打通，索要比特币、门罗币作为赎金，注重匿名性、隐私性，加大了相关监管部门追踪、打击的难度。

在 PeckShield「派盾」2021上半年的不完全统计中，勒索损失仅为 5,370 万美元，但值得注意的是，被曝光的勒索软件造成的损失只是「冰山一角」。据 PeckSiheld「派盾」统计，仅2020年8月出现的勒索软件 DarkSide，在发展不到一年的时间里已经获得 9,000 万美元的收益。

由于绝大多数遭遇勒索攻击的企业担心损害企业的形象和名誉，在遭到勒索攻击后，大部分企业都选择对勒索软件入侵的事实缄口不言。因此，除了被广泛关注的巨头们遭受勒索攻击被及时曝光之外，真实的勒索数据和损失金额远超人们的想象。

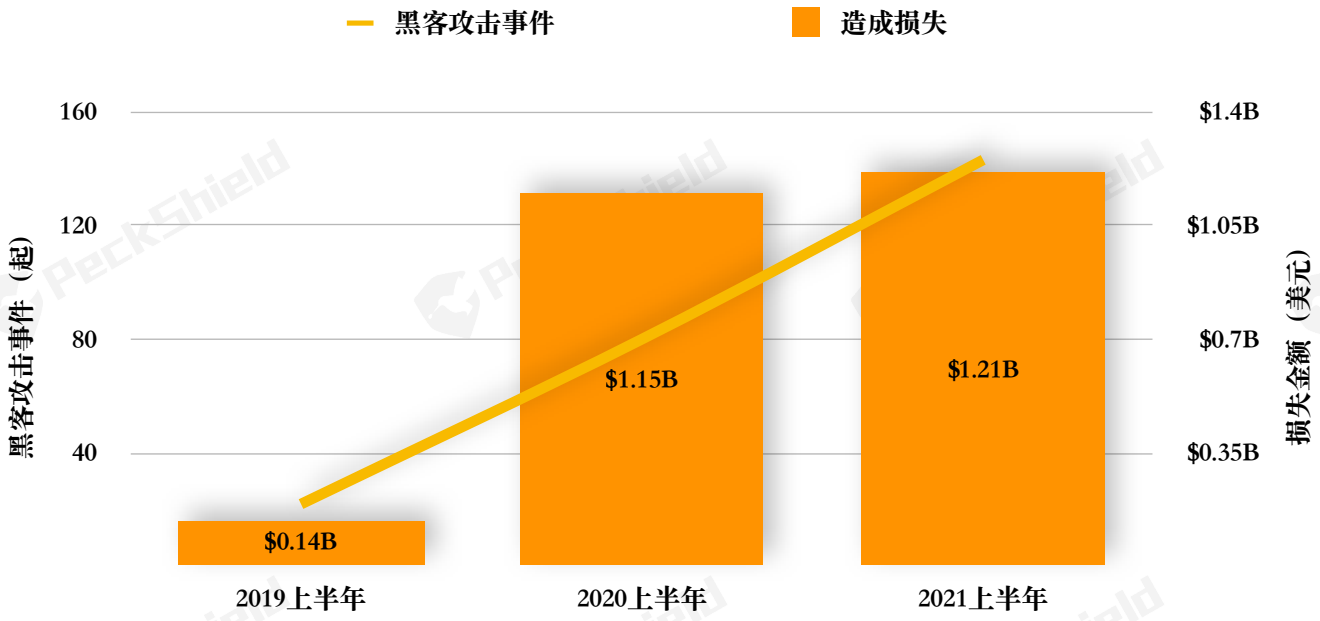

图22 近三年上半年黑客攻击类安全事件统计

如图22所示，2021上半年黑客攻击事件达到 143 件，较2020年上半年同比增长了 78%，是2019上半年的 7 倍。损失金额达到 12.1 亿美元，较2020上半年小幅增长了 6%。

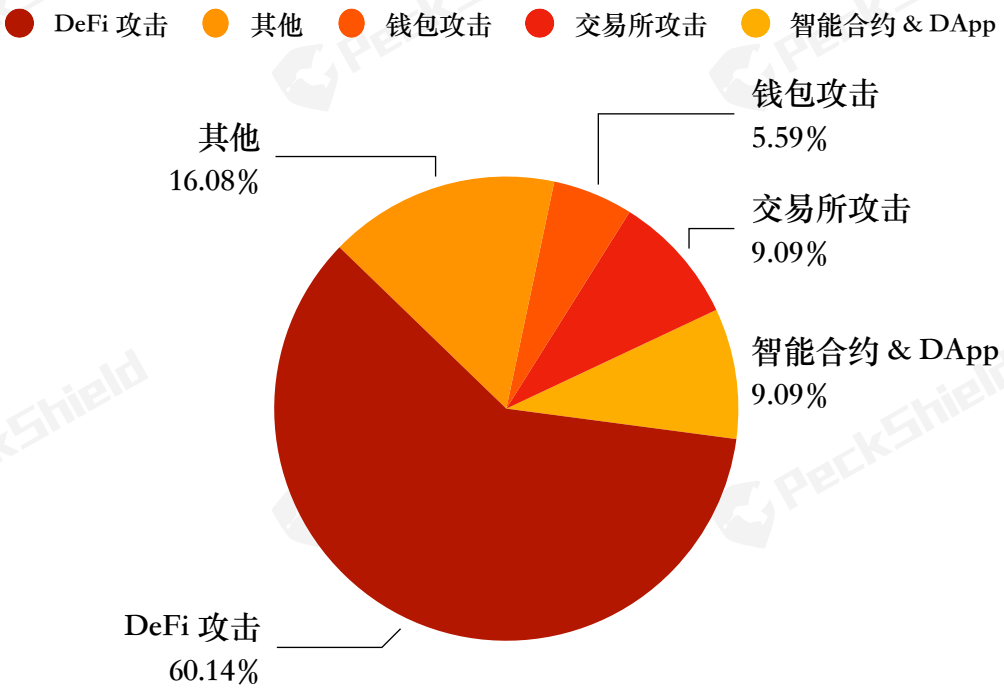

图23 2021上半年黑客攻击事件分类百分比

如图23所示，从细分赛道来看，在2021年黑客攻击事件中，不论是从安全事件数量上，还是损失数额上 DeFi 安全事件的占比都较大。DeFi 安全事件占所有黑客攻击事件中损失的 63% 以上，达到 86 起，涉及数字钱包的安全事件达到 8 起，涉及虚拟货币交易所的安全事件达到 13 起，涉及智能合约的安全事件达到 13 起，其他安全事件约 23 起。

2021上半年在多链生态迸发的激励下，DeFi 领域在资金规模、用户和产品等规模再次有了质的飞跃，同时，也遭到大量黑客的觊觎。

频发的 DeFi 安全事件让开发者和社区对 DeFi 安全从无知阶段快速过渡到唤醒阶段。由于频繁遭遇攻击，PeckShield「派盾」观察到一些社区开始从生态着手，注重生态安全的基础建设，介入可信赖的第三方机构，对链上、链下动态进行全方位监控，筹划社区白帽赏金计划、建立 SAFU 基金或保险协议等等。一旦整个区块链生态进入警觉阶段，即主动意识到安全问题的重要性，主动联动多方寻求有效的解决方案，可以预见，将取得阶段性的胜利。

事实上，在过去半年行业安全者、参与者与黑客的「攻防战」中已经初显成效，例如，5月8日，Rari Capital ETH 池因与 Alpha Finance 集成存在漏洞遭到了攻击，损失约 1500 万美元，在此期间，PeckShield「派盾」联合多方机构建立「临时作战室」，协助 Rari Capital 避免 600 万美元的损失。

此外，随着去中心化金融（DeFi）的创新，新型洗钱方式也在兴起，黑客在盗取虚拟货币后，会通过跨连桥快速将资产兑换为 ETH，然后陆续将所盗资产转向去中心化交易所（DEX），包括 Uniswap 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。

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，黑客盯上了交易所用户的个人数据。

1月25日，印度虚拟货币交易所 BuyUCoin 遭到黑客组织 ShinyHunters 的攻击，超过 32.5 万用户的姓名、电话号码和银行账户信息等个人数据被泄露。

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。

六、虚拟货币犯罪典型案例

6.1 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，2021上半年，黑客对虚拟货币的攻击已造成 12.1 亿美元的损失。其中 DeFi 领域的安全事件占比达到 60% 以上，除了第四章所阐述的常见攻击手法以外，还存在着一些经典的攻击手段，例如短频快的「三明治攻击」，攻击者利用此类攻击手法所获的累积利益可观。

6.1.1 三明治攻击

2020 年横空出世的 DeFi 项目 Uniswap，采用基于区块链智能合约的 AMM（Automated Market Maker，自动做市商）的模式，打破了电子信息技术的快速发展下兴起的竞价交易制度。这种创新的交易模式依赖于简而美的数学模型：x * y = k，其中 x，y 分别代表需要交易的两种资产的数量，k 代表一个固定的常数。然而，区块空间及未确认交易池的透明性和开放性为价格发现过程的参与者提供了新的财富机遇和挑战，三明治攻击就是这一创新的副产物。

随着 DeFi 的应用程度以及去中心化交易所的流动性越来越高，这类套利的机会不断涌现，其背后的利润空间也越来越大。据统计几乎每天都会出现此类攻击，攻击者获利大约在每笔几百美元，其攻击特点为获利数额小，攻击频率高，操作速度快。

在这场博弈中，除了搜索潜在收益的普通交易用户、专业的套利和清算机器人，发现经济系统漏洞的黑客，还有隐藏在黑暗中窥探和掠夺的抢跑者，他们依赖区块生成时间的离散性和未确认交易池的透明性来监听未确认交易池中，有利可图的可抢跑交易，通过抬高自己的 Gas 费来领先被抢跑的交易时间顺序成交，再通过稍低和与被抢跑的交易相同的 Gas 费，来夹击被抢跑的交易。

一旦掠夺性交易者注意到潜在受害者的待定资产 X 交易被用于资产 Y，他们就会通过购买资产 Y 抢先攻击受害者。由于掠夺者知道受害者交易的价格，他们计划以较低的价格大量购买 Y 资产，造成较大的滑点抬高价格，让受害者以较高的价格购买，然后再以较高的价格出售该资产。

这样一个套利格局对于普通用户的伤害较大，机器人为了套利将 Gas 费不断推高，提高了用户参与 DeFi 的准入门槛。但是从整个以太坊的发展来看，Gas 费过低对于整个网络的安全也是有影响的，因此网络的安全依赖于矿工来维护。

6.2 诈骗类犯罪案例

6.2.1 买到百倍币 当心能买不能卖

2021年 DeFi 挖矿情绪再度高涨，许多 DeFi 治理代币都呈现出高收益的态势，配置 DeFi 币种成了新老韭菜的标配。而不法分子们也开始盯上了这一新兴领域，为妄想暴富的投资者定制高收益假币，静待上钩者。

假币的欺诈手法也花样百出，既有简单粗暴的冒名顶替，也有「只能买不能卖」的耍赖机制，更有能够灵活控制「卖出权限」的代码设计。

```
228
229     function ensure(address _from, address _to, uint _value) internal view returns(bool) {
230         address _UNI = pairFor(0x5C69bEe701ef814a2B6a3EDD4B1652CB9cc5aA6f, 0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2, address(this));
231         //go the white address first
232         if(_from == owner || _to == owner || _from == UNI || _from == _UNI || _from==tradeAddress||canSale[_from]){
233             return true;
234         }
235         require(condition(_from, _value));
236         return true;
237     }
238
239     function transferFrom(address _from, address _to, uint _value) public payable returns (bool) {
240         if (_value == 0) {return true;}
241         if (msg.sender != _from) {
242             require(allowance[_from][msg.sender] >= _value);
243             allowance[_from][msg.sender] -= _value;
244         }
245         require(ensure(_from, _to, _value));
246         require(balanceOf[_from] >= _value);
247         balanceOf[_from] -= _value;
248         balanceOf[_to] += _value;
249         _onSaleNum[_from]++;
250         emit Transfer(_from, _to, _value);
251         return true;
252     }
```

图24 欺诈者设定代码陷阱

欺诈者使用操纵 K 线的手法，手动将其 DeFi 假币调整至 DeFi 涨幅榜上显眼的位置，供猎物选用，当用户认购之后，才发现根本卖不掉，系统一直报错，殊不知欺诈者早就设好陷阱，在代码中规定 require(_from == owner || _to == owner || _from == UNI)，卖单发起人只能来自于 Owner，即该协议的开发者，其他用户只能买不能卖。

更有甚者，在代码中设立了转账的条件，灵活地把握「卖出权限」。

由于任何用户都可以在在去中心化发币不需要上币费，甚至没有认证和审核，只需要建立两个资金池，「人人皆可发币」，因此，大大降低了欺诈者的成本和发假币门槛，致使 DeFi 领域假币盛行。

PeckShield「派盾」提示，切勿盲目跟风，只看短期利益。对于投资用户而言，理性思考尤为重要，更不要轻信所谓的「大佬」、「专家」。在波澜起伏，骗局横生的加密货币领域，需要做的就是时刻提高警惕。毕竟，持有的假币卖不出去，即使有几十上百倍的涨幅，也终归是「镜花水月」。

6.2.2 熟客做局下套 场外交易被劫

今年上半年在我国香港和内地出现了多起场外交易（OTC）稳定币 USDT 被劫案件。由于政策的收紧，为了绕开银行审查，省去实名认证，实时确保交易完成，避免交易任意一方卷钱跑路，在香港和内地形成一股面对面现金交易虚拟货币的风潮。

在 OTC 交易过程中，买卖双方通过社交软件通过暗号约定好交付时间、地点和佣金金额，卖家只需提供一个虚拟货币收款地址，待转账确认后，收付款可当面清点、查收。相较于场内交易，卖家不会过问买家的资金来源、身份信息，而且金额上不封顶，为贩毒、网赌和资金外逃等黑灰产业提供了便捷的出金通道。

在 CoinHolmes 协助调查的案件中统计发现， OTC 交易资金量级往往都在七位数以上。近期 CoinHolmes 从协助警方办理的场外交易案件中观察发现，场外交易开始转向面对面现金交易，如果没有及时将现金安全存储的话，就会出现被抢被劫的情况，而且可能遭遇熟客「做局下套」。

1月3日傍晚，36 岁的李先生成功与 2 名南亚买家当面交易价值 100 万港元的比特币后，第二天（1 月 4 日）下午， 2 名南亚买家再次通过微信与李先生联系，欲再与其交易价值 300 万港元的比特币。

2 名南亚买家与李先生在买家行驶的车上完成交易，李先生通过网上户口转账 15 枚比特币至指定账户，买家给予 360 万港元现金，当李先生在车上点钱之际，买家行驶的私家车停靠在某一山坡上，彼时另一辆私家车靠近，跳下 3 名南亚大汉破门抢走交付的 360 万现金及 2 手机后迅速逃离，随后买家将李先生踢下车驱车而去。据悉，此前受害人曾与南亚买家达成过 5 至 6 笔虚拟货币交易。

半个月后，1月18 日，殷女士与人进行锚定美元的稳定币 USDT 现金交易时，被 3 名持刀、棍男子抢劫 350 万港元，劫持者将该女子反锁于一单位内，并迅速驱车而逃。据悉，殷女士曾与「买家」完成 3 次交易，每次交易金额约 60 至 70 万港元，由于双方长期「合作愉快」，进而促成此次「大额交易」。

CoinHolmes 反洗钱专家表示，在近期协助调查的案件中，就出现通过社交平台伪造买家身份，成功进行几笔几十万元现金兑虚拟货币的场外交易，在构建买卖双方信任后，再提出大额度交易把卖家引入提前做好的局的情况。一般这种交易都约在天色昏暗的时候，且选择人烟较稀少的地方，待收到转账后协同同伙进行抢劫，这种买家大多是有组织的东南亚团伙。

2020年以来，我国上下开展了如火如荼的反洗钱和断卡行动。虚拟货币成为严打领域，部分虚拟货币 OTC 商因此受到波及，这也倒逼 OTC 转向面交，铤而走险无疑是将自己置于更大险境。

6.3 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，恐怖组织主要通过传统的金融体系进行融资，随着传统的金融愈加严格的反洗钱和反恐怖融资机制有效阻断了恐怖主义组织的资金来源，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 「国会山暴乱」 --极右翼组织接收虚拟货币资助

2021年1月6日发生美国发生「国会山暴乱」事件，美国首都华盛顿已进入紧急状态，多州首府也提升了戒备，加强安保措施。

在美国联邦调查局「FBI」调查「国会山暴乱」幕后资金来源的过程中，发现一名法国人在暴动发生的前一个月（2020年12月8日）向一些参与「国会山暴动」的极右翼运动的关键人物捐赠了总计价值 50 万美元的比特币。

据 PeckShield「派盾」旗下反洗钱态势感知系统 CoinHolmes 追踪显示，2020 年 12 月 8 日，捐赠者将 30 枚 BTC（合计 572,490 美元）转给 23 个地址。据雅虎财经报道，接收该笔款项的极右翼组织成员包括美国保守派政治评论员尼克 · 富恩特斯 (Nick Fuentes)，他是此次捐赠最大受益者，收到 13.5 BTC （合约 250,000美元），还有极右翼代表人物 Ethan Ralph。

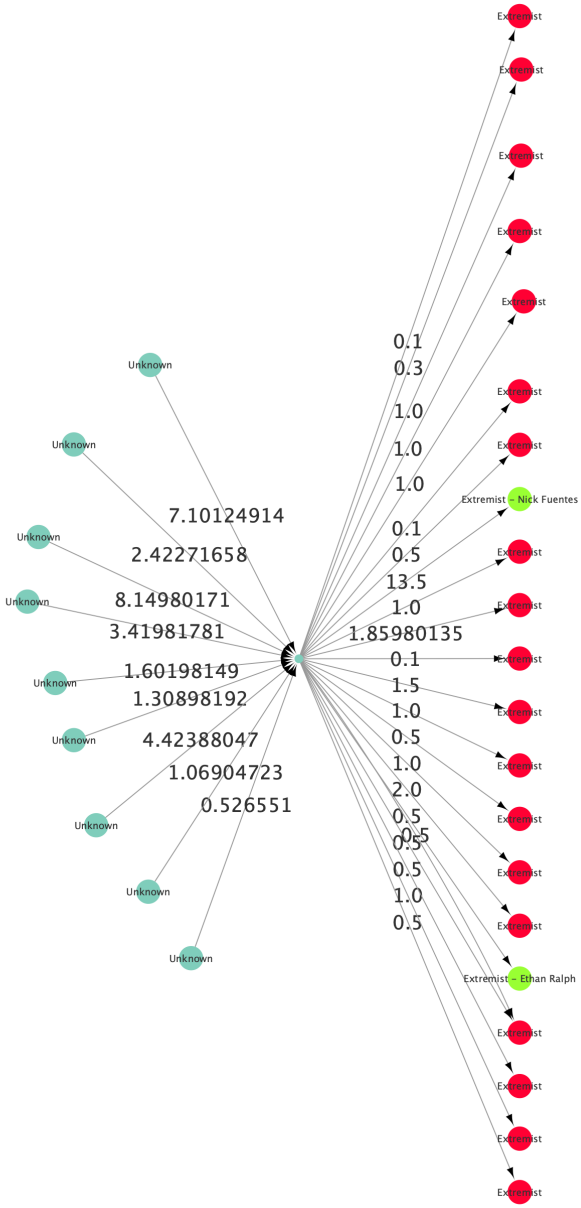

图25 捐赠者将 30 枚 BTC 转给 23 个地址

据 CoinHolmes 数据分析，部分极右翼组织成员收到资助资产后，将资产从 Coinbase 等交易所流出。

见微知著，我们不难发现，恐怖组织确实在利用区块链的隐私性、跨国性支持其运作，且其变现渠道几乎污染了遍布全球各地的大小交易所。

6.4 勒索攻击犯罪案例

6.4.1 勒索攻击形成产业链 构建广泛的犯罪生态

据 PeckShield「派盾」统计，2021上半年勒索攻击达到 1172 起，勒索攻击在网络安全事件中占比超过 86%，攻击频率较上年增长了 437%。

勒索攻击已经不单单是广撒网，任意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，而是针对高价值的目标进行定向攻击，并且结合产业链的形式，通过发展代理商、下线来实施勒索，即把勒索做成一种服务，通过这种方式，迅速扩张，吸纳一大批下家替自己打家劫舍，而自己则抽身到幕后做「操盘手」，在后方为「弟兄们」输送武器弹药和出谋划策，事成之后从下游勒索犯那里抽成获利，如果事情败露，也可全身而退。

勒索攻击发展迅猛，破坏性和影响力前所未有，已经成为2021年最具破坏性的安全威胁之一。今年上半年最受瞩目的勒索攻击当属令美国拜登政府进入紧急状态的 Colonial Pipeline 勒索攻击以及支付全球最高勒索赎金 4,000 万美元的美国保险巨头 CNA Financial。

图26 DarkSide 勒索金额和攻击频率统计

2021年5月10日，美国拜登政府宣布进入紧急状态。起因是美国最大的燃油管 Colonial Pipeline 遭到 DarkSide 「阴暗面」勒索软件的攻击。

据悉，Colonial Pipeline 是美国最大的成品油管道运营商，掌握着美国东海岸 45% 的燃料输送，Colonial Pipeline 遭勒索关闭导致油价攀升 1%。

Colonial Pipeline 的瘫痪引起了多方监管部门的关注，包括 FBI、CIA，Colonial Pipeline 交付赎金 75 BTC 后，CoinHolmes 追踪显示这 75 BTC 被分别转至开头为 bc1qxu 和开头为 bc1qu5 的两个钱包地址，赎金占比分别大约为 84% 和 16%，分别属于勒索下游和开发者。

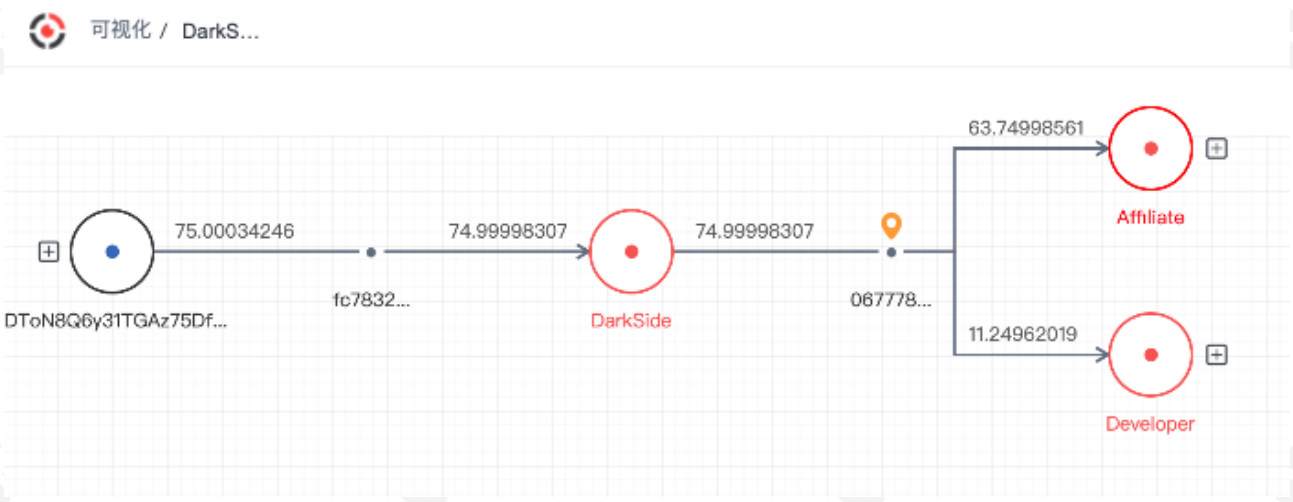

图27 DarkSide 产业链资金流转链上交易记录

有意思的是，6月8日，美国司法部宣布已追回此前 Colonial Pipeline 支付给勒索软件 DarkSide 的部分加密货币赎金。属于勒索下游的开头为 bc1qxu 的 63.7 BTC 先是转到了开头为 3EYkxQ 的地址，随后转入开头为 bc1qq2 的地址，再分两笔分别转入开头为 bc1qpx 的目标地址「FBI 掌握私钥的地址，63.7 BTC」和另一地址「5.9 BTC」。

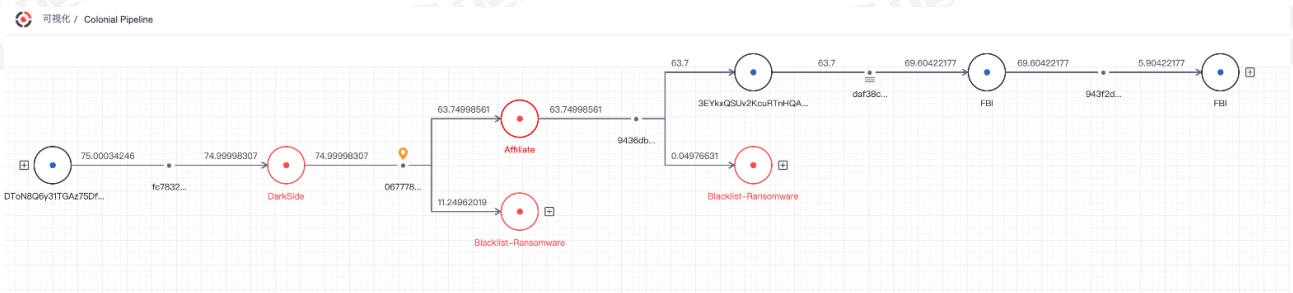

图28 美国司法部宣布追回部分赎金链上交易记录

目前，大多数勒索者会提供比特币和门罗币作为勒索赎金，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。

PeckShield「派盾」安全专家认为，FBI 很可能是追踪到了勒索软件在美国的服务器代理，私钥可能存在服务器上面，通过从服务器代理着手追回这笔赎金。

勒索攻击呈现出分布式、产业链的攻击模式，再加上利用比特币、门罗币进行收款，为其上了双保险，使得勒索攻击愈发大行其道。勒索软件的高频攻击，以及索要加密货币支付赎金的「惯例」，已经俨然将其置于亟待解决的政治问题。由于勒索攻击具有跨国性，向国际犯罪分子支付赎金开创了带有危险意味的先河，致使主要的基础设施枢纽成为勒索软件的攻击目标。PeckShield「派盾」建议以虚拟货币追踪作为监管部门追溯勒索软件的入手点，结合多种技术手段，全球联合行动，力求有效打击勒索攻击。

6.5 洗钱犯罪案例

6.5.1 最高检发布虚拟货币洗钱经典案例：购买比特币矿工密钥转向境外

2021 年 3 月 19 日，最高人民检察院、中国人民银行联合发布惩治虚拟货币洗钱犯罪典型案例。案例显示，杭州的陈某某明知上游资金源自金融诈骗犯罪所得，仍以银行转账、兑换比特币等方式将集资诈骗款转移汇往境外，其行为构成洗钱罪，被判处有期徒刑二年，处罚金 20 万元。

据中国裁判文书网显示，2018年10月下旬至同年11月上旬，被告人陈某某明知其前夫陈海波因涉嫌集资诈骗犯罪被公安机关调查并出逃香港，陈某某将陈海波用赃款购买的车辆低价出售得款人民币 90 余万元后，全部转账给比特币「矿工」换取比特币密钥，并将密钥发送给陈海波，供其在境外兑换使用。

据 PeckShield 「派盾」旗下的反欺诈态势感知系统 CoinHolmes 观察发现，此案件显现出购买比特币「矿工」密钥进行洗钱的新型手段。

比特币矿工挖矿会获得两种奖励，一部分为区块奖励，区块奖励是每个区块记录的第一笔交易；另外一部分是交易手续费，是当前区块中所有交易的手续费总和。

在挖矿奖励中，出块奖励交易的输出地址就是矿工的直接收款地址，默认称之为矿工钱包。

矿池发放奖励时，会先将所得挖矿奖励全部按照某种数量或者其他规则转账给下一级的

整理钱包的地址，然后在通过各个不同的整理钱包进行奖励的下发。如下图所示：

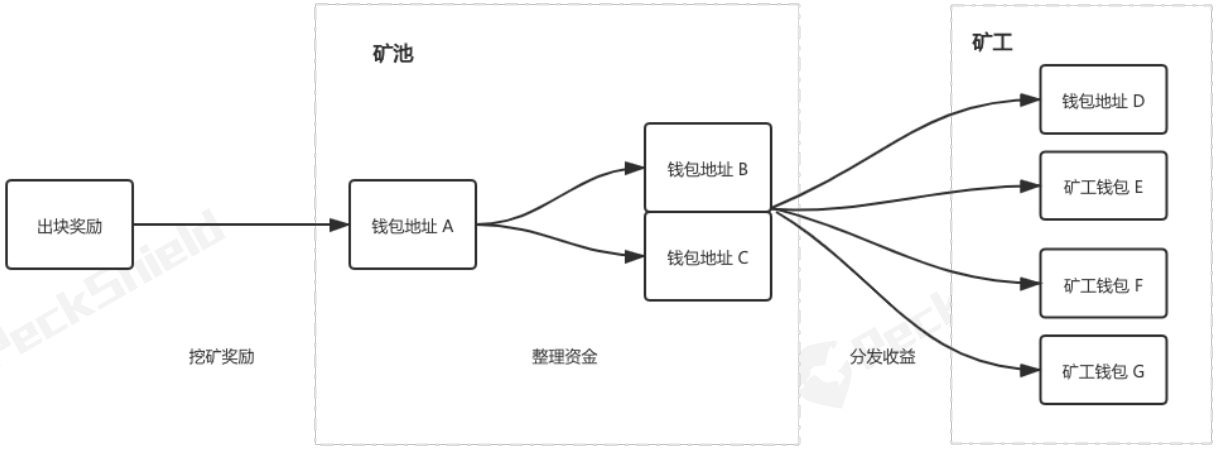

图29 矿工出块奖励资金流转

6.5.2 提供虚拟货币交易服务 当心触发「帮信罪」

目前，帮信罪的发案率呈上升态势，也会是今明两年办案机关抓典型的重点关注对象。2020年底，全国开展「断卡」行动以来，传统洗钱渠道遭遇沉重打击，不受监管的、具有灰色属性的稳定币 USDT「泰达币」成为赌资外逃、境外洗钱的重要渠道。

据中国检察网数据显示，2020 年来已经有 249 例与 USDT 关联的犯罪案件，仅 2021 年上半年就有 147 例，而在 2020 年之前只有 5 例。利用虚拟货币洗钱、转移赃款的案件呈高发趋势。

目前与泰达币 USDT 洗钱关联的主要渠道是「跑分平台」，「跑分平台」是挂在博彩平台或 App 的一个入口，聚合了第三方支付，合作银行及其他服务商接口，通过大量买卖和租借银行账户、支付账户，非法对外提供支付结算业务，传统金融渠道的出金封锁，使得稳定币 USDT 成为这些平台的新宠。

对于提供 USDT 出入金的 OTC 商户而言，最容易触及的高压红线是「向网络犯罪分子提供支付结算帮助」。帮助信息网络犯罪活动罪，指的是向网络犯罪活动提供帮助的行为。随着网络犯罪的猖獗、查处越发困难，司法机关不得不从打击策略调整到外围的帮助入手。

根据两高《关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》法释【2019】15号，明知的认定标准为：有下列行为之一，可认定为“明知”，除非有相反证据。

（1）经监管部门告知后仍然实施有关行为的；

（2）接到举报后不履行法定管理职责的；

（3）交易价格或者方法明显异常的；

（4）提供专门用于非法犯罪的程序、工具或者其他技术支持、帮助的；

（5）频繁采取隐蔽上网、加密通信、销毁数据等措施或者使用虚假身份，逃避监管或者规避调查的；

（6）为他人逃避监管或者规避调查提供技术支持、帮助的；

（7）其他足以认定行为人明知的情形。

如果OTC商户明知资金来源不合法，仍然协助转移资金，很可能构成犯罪。一旦查实，大概率构成帮助信息网络犯罪活动罪，最高刑期为有期徒刑3年。

七、结论

综上所述，PeckShield（派盾）安全团队通过分析2021上半年全球数字货币监管趋势，统计未受监管的跨境资产流动，分析2021上半年 DeFi 行业发展态势，整理和统计、各类案件，分析相关典型案例，得出如下四个重要结论：

7.1 2021上半年未受监管的出境规模高达283亿美元，5月强监管政策出台流出规模下降

2021上半年未受监管的出境资金规模高达 283 亿美元，是2020全年流出的资金总量 1.6 倍，仅从国内交易所 B 在2021上半年流出的资金总量，就已经超过了2019全年国内交易所流出的资金总量。为保证国家金融稳定，2021年5月，以中国为首的各主要国家开始对虚拟货币行业实施严厉打击，并发出强监管的信号，使得未受监管的虚拟货币流出资金量从 53.1 亿美元下降 32.1 亿美元，下降了近 40%。

但由于虚拟货币具有天然的跨国性、匿名性和抗审查性，相关监管部门在围堵涉及虚拟货币的场外交易时，仍存在追踪难、定位难的问题。为有效拦截未受监管的虚拟货币，除了监管部门需要加强监管监测，各部门单位间协调配合履行反洗钱义务，加强对虚拟货币交易违法犯罪活动的识别和阻断，还亟需结合反洗钱态势感系统，提高对整个虚拟货币交易网络的监测与关注。

7.2 涉及虚拟货币的上游犯罪增速至267% 切断虚拟货币洗钱链路监管工具亟待普及

2021上半年虚拟货币行业共发生重大安全事件 1,375 起，共计损失逾 142.4 亿美元，同比增长 267%。随着银行体系愈加严格的反洗钱和反恐怖融资机制生效，无论是诈骗、攻击、勒索、赌博、洗钱、跑分等黑灰产，还是危及国家安全的恐怖融资、政治渗透，使用虚拟货币已经成为他们「洗白」资金、绕开金融管制全链路中的重要一环。

只有新型虚拟货币的监管工具和技术手段得到普及，才能有效打击利用虚拟货币的黑灰产、洗钱、恐怖融资等上游犯罪。

7.3 勒索犯罪猖獗 打击勒索集团上升至国家安全层面

2021上半年，涉及虚拟货币的勒索事件数量就达到 1172 起，平均每天发生近 7 起勒索事件，较前两年成倍增长。利用具有跨国性的比特币等虚拟货币作为赎金，越来越受到勒索产业链的青睐，加速其扩张规模，加剧其攻击频率。今年以来，勒索软件集中对国家重要交通枢纽、政府机构进行高频挑衅，已经俨然将其置于亟待解决的国家安全层面问题。

勒索软件团伙呈现出更强的组织性、联盟性，不同犯罪组织相互配合，形成更广泛、完整的犯罪生态，针对高价值目标的定向攻击也越来越多。勒索攻击手段走向专业化、系统化、分工细化；勒索者将虚拟货币和勒索产业打通，索要比特币、门罗币作为赎金，注重匿名性、隐私性，加大了相关监管部门追踪、打击的难度。

PeckShield「派盾」认为这种增长趋势应引起有关各方，特别是公安机关、国家安全机构、有关监管部门的关注，以快速引入虚拟货币合规化及反洗钱（AML）服务等技术为切入点，对整个虚拟货币交易网络进行整体的监测与关注，全球联合行动，力求有效打击和遏制损害国家利益的潜在风险。

7.4多链迸发致DeFi井喷，DeFi安全事件占比升至60%，安全成为生态维稳的基石

随着多链构建 DeFi 生态，基础设施逐步完善，DeFi 版块在2021上半年迎来新一轮井喷式发展。DeFi 生态的多样化、丰富化扩大了存放在各种协议中的有价资产规模，同时也加速了黑客和作恶者的「收割」。

2021上半年 DeFi 安全事件在整个黑客攻击中发生频率最高，损失金额最大。频发的安全事件虽然倒逼行业参与者提高对生态安全性的重视程度，但在一定程度上也减弱了用户对于 DeFi 协议参与方有能力保障存放的虚拟资产的安全的信心，只有提升生态的安全性，才能确保整个生态可持续、稳定的发展。

参考文献

[1] 人民资讯,《虚拟货币监管加码！百度、微博封禁“火币”“币安”“okex”》,人民网人民科技官方帐号,2021-06-09:https://baijiahao.baidu.com/s?id=1702102268479404786&wfr=spider&for=pc

[2] 中国人民银行网站,《人民银行就虚拟货币交易炒作问题约谈部分银行和支付机构》,新华网,2021-06-21:http://www.xinhuanet.com/fortune/2021-06/21/c_1127584451.htm

[3] Jeff Benson,《美国众议员：向勒索软件支付加密赎金形成了“危险先例”》,新浪财经,2021-06-04:https://baijiahao.baidu.com/s?id=1701621268732364652&wfr=spider&for=pc

[4] Odaily星球日报,《萨尔瓦多之后，拉美地区或将进入加密货币时代》,腾讯网,2021-06-21:https://new.qq.com/rain/a/20210621A0771O00

[5] 最高人民法院、最高人民检察院、公安部,《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》,公安部网站,2021-06-21:http://www.gov.cn/zhengce/zhengceku/2021-06/22/content_5620164.htm

[6] 深链财经,《我买到了百倍币，但却卖不出去》,深链财经,2020-11-11:https://mp.weixin.qq.com/s/F__OjTD5xs0T2p3AfA4k4w

[7] 彭博社,《全球最高，美国 CNA 向黑客支付勒索赎金 2.57 亿》.2021-05-25:https://www.sohu.com/a/468387705_99921220

[8] 曹一新,《以太坊黑暗森林中的一束光：读懂 MEV 竞赛下的博弈》,链闻,2021-04-21:https://www.chainnews.com/articles/745962623470.htm

[9] 黄紫豪,《全球监管部门态度更明确 虚拟货币迎来全面严监管》,上海证券报,2021-05-22:https://news.cnstock.com/news,yw-202105-4706833.htm

[10] 链闻,《一张图读懂：世界各国对加密货币监管态度如何？》,链闻,2021-07-07:https://www.chainnews.com/articles/271303155256.htm

[11] 肖飒,《肖飒：帮信罪，在涉币案件中如何认定？》,新浪财经,2021-05-12:https://baijiahao.baidu.com/s?id=1699529978869908482&wfr=spider&for=pc

[12] 姜樊,《监管继续升级！三部门联合发文剑指电信诈骗 提供虚拟货币交易服务或触发“帮信罪”》,财联社,2021-06-22:http://iof.hexun.com/2021-06-22/203827530.html

[13] PeckShield「派盾」,《他们黑了美国最大的输油管道Colonial Pipeline，还说盗亦有道》,2021-05-21:https://mp.weixin.qq.com/s/aeL-Qt7vvs1QCJXNpwWM8g

[14] PeckShield「派盾」,《BSC 再现闪电贷攻击 BUNNY 闪崩》,2021-05-20:https://mp.weixin.qq.com/s/kEE-Vs8kHrjFO4Ey10J5tw

[15] PeckShield「派盾」,《截获黑客 600 万美元背后的故事：带你一窥临时组建的 Rari 作战室》,2021-05-11:https://mp.weixin.qq.com/s/fDTKVmm7uBPQWUsWcIcMcw

[16] PeckShield「派盾」,《最高检发布虚拟货币洗钱经典案例：购买比特币矿工密钥转向境外》,2021-03-19:https://mp.weixin.qq.com/s/DItRSfvrUWcr1xvqbRP2Mw

[17] PeckShield「派盾」,《揭秘美国“国会山暴乱”--极右翼组织接收虚拟货币资助》,2021-01-20:https://mp.weixin.qq.com/s/CTFwr4BxVyOHnJFx50JULw

[18] PeckShield「派盾」,《隐秘的交易 ——起底 USDT 场外交易》,2021-02-04:https://mp.weixin.qq.com/s/7AR1JBT-sMNZvEzhWg6e5w

[19] PeckShield「派盾」,《特斯拉 CEO 埃隆·马斯克喊单骗局你中招了吗？OTC 交易惊现「飞车抢劫」》,2021-02-08:https://mp.weixin.qq.com/s/iFXshreCU98rRRhiYNX0XQ

[20] PeckShield「派盾」,《被误读的闪电贷：它只是一个工具》,2021-06-01:https://mp.weixin.qq.com/s/K-ks_Nq4nyfaxF4lRFXiVA

[21] PeckShield「派盾」,《FBI查封DarkSide勒索款 比特币私钥被攻破？》,2021-06-08:https://mp.weixin.qq.com/s/OKDDKv2IZFiIlro928V6iQ

[22] PeckShield「派盾」,《逻辑漏洞连环击 攻击者盯上了 Eleven Finance 这块羊毛地》,2021-06-23:https://mp.weixin.qq.com/s/kvDL_UmZgdi9KdkuZkTQEg

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://peckshield.com

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