PeckShield

# 数字货币反洗钱暨DeFi行业安全报告

## 2021年度报告

PeckShield（派盾）

2022.01

# 目录

# 一、研究背景综述

2021年上半年，全球第一家数字货币交易所 Coinbase 宣布在纳斯达克上市、特斯拉 15 亿美元购入比特币，在多重因素的影响下，主流数字货币的价值持续走高。5月起，各国政府不断收紧监管政策，多国执法部门向币安（Binance）交易所发出警告。9月24日我国监管祭出堪称史上最严禁令，全球虚拟货币交易所迎来了一场大洗牌，“伪出海”的中心化虚拟货币交易所在这次风暴中受挫，主动发声清退。另一方面，《每一天：前5000天》NFT 以 6,934.6 万美元在佳士得成交，这使得 NFT 在市场上备受瞩目，随后 CryptoPunks 掀起全民头像热潮。多链迸发，跨链并进带动资产涌入「去中心化」协议，DeFi 领域再度跃升。2021年下半年，在千亿美元 DeFi 锁仓的强力刺激，以及首支比特币期货 ETF 上市等利好因素的加持下，数字货币市场呈现 V 型复苏态势。

2021年 DeFi 锁仓连破 100 亿、1,000 亿、2,000 亿美元三道大关，一度创下 2,700 亿美元的历史高点。数字货币市场虽迭遭各国监管打压，锁在 DeFi 中的资产仍大幅增长，热力一直未减，在此过程中不乏出现蹭 DeFi 热点进行「收割」与「欺诈」的乱象，同时，凸显出「监测」与「风控」的空缺。如雨后春笋般涌现的 Layer1 和 Layer2 技术方案经过一年的迅速扩张，依然在摸着石头过河，寻求打破依赖「羊毛党」吸引流动性的桎梏，打开可持续发展的道路。

华尔街大资本的入场，以及去中心化的深耕成为行业的新变量。回顾2021年，「行业重塑」、「出海」、「去中心化」成为数字货币行业的年度关键词。

## 1.1 「交易」与「挖矿」肃清双管齐下 国内迎来最严监管

国内方面，监管建立健全对「交易」和「挖矿」治理的防范政整治机制，为建立常态化工作机制奠定基础。

9月24日，中国人民银行联合网信办、公检法等十部委联合发布《关于进一步防范和处置虚拟货币交易炒作风险的通知》（下称央行《通知》），该《通知》被外界称为「史上最严」的监控政策，除了再次强调虚拟货币相关业务活动属于非法金融活动之外，首次明确了境外虚拟货币交易所通过互联网向中国境内居民提供服务同样属于非法金融活动。

《通知》甫一落地，十余家虚拟货币交易平台随即宣布停止在中国大陆涉及虚拟货币的业务。其中 Huobi Global（下称“火币”）率先表示，在2021年12月完成对中国内地存量用户的清退。币核、BiONE 等平台则直接宣布停止运营。

事实上，自今年5月以来，我国秉承对虚拟货币明确的、一贯的监管政策，在整治政策的部署上持续升级。

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》，直接否定虚拟货币的货币属性，指出有关机构不得开展与虚拟货币相关的业务。

5月21日，中共中央政治局委员、国务院副总理、金融委主任刘鹤在国务院金融稳定发展委员会召开五十一次会议上明确指出，坚决防控金融风险，打击比特币“挖矿”和交易行为。国务院金融稳定发展委员会召开五十一次会议。

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21日，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，约谈的部分银行和支付机构，要求其不得为相关活动提供账户开立、登记、交易、清算、结算等产品或服务。

7月，北京市地方金融监督管理局、央行营业管理部发布《关于防范虚拟货币交易活动的风险提示》（下称《风险提示》），警告辖内相关机构不得为虚拟货币相关业务活动提供经营场所、商业展示、营销宣传、付费导流等服务。同时，辖内金融机构、支付机构不得直接或间接为客户提供虚拟货币相关服务。

新政策的不断向市场释放出两个前所未有的重要信号。一是我国监管部门将建立多维度、多层次的风险防范和处置体系，针对虚拟货币交易炒作活动的监管，不再是单一部门的单一职责，而将是联合金融管理部门、网信部门、电信主管部门、公安部门、市场监管部门等多个部门；同时将从切断支付渠道、依法处置相关网站和移动应用程序、加强相关市场主体登记和广告管理等方面系统施策，来全方位防范和处置虚拟货币交易炒作风险。二是明确定性虚拟货币和相关业务活动，包括开展虚拟货币兑换、做市、中介等相关业务活动都被定性为非法金融活动；境外交易所向我国境内居民提供服务被定性为非法金融活动；普通人参与虚拟货币投资交易活动也存在法律风险。这象征着我国已经步入虚拟货币常态化监管的新阶段。

## 1.2 全球主要国家监管机构相继出手

国际方面，在中国祭出打击虚拟货币的重拳之后，越来越多的国家也加速落地收紧对虚拟货币的监管。

今年10月，全球首支比特币期货 ETF 正式在纽交所开启交易，被誉为区块链领域的一座里程碑。尽管美国通过了第一支比特币期货 ETF，但并不代表美国监管层面的整治力度有所放缓，相反地，监管机构将监管重心集中到包含传统金融市场系统性风险的地方，例如稳定币、DeFi 借贷等。美国的监管态度愈发明确：鼓励「创新」但必须细化监管。

针对从推出就备受各监管部门密切关注的虚拟货币交易所和托管钱包，美国监管再度出台了更为严格的监管政策。

9月，美国财政部公开声明重点关注「嵌套交易所」、「混合交易所」和「P2P」等虚拟货币平台。

美国金融市场工作组（PWG）呼吁国会通过新的紧急立法以"填补稳定币监管的空白"。

11月起，美国联邦机构对加密产业的监管态势更是来势汹汹。11月初，美国 SEC 专员 Caroline Crenshaw 在国际期刊上发表了署名文章《关于 DeFi 的风险、监管和机会的声明》，要求 DeFi 社区必须在遵守美国 SEC 规则的同时，解决透明度和假名问题，并呼吁 DeFi 项目与 SEC 合作探索合规路径。很快 SEC 将对加密企业实施管制。

11月13日，SEC 向 Terra 的开发公司 Terraform Labs 及其 CEO 发传票，调查其是否违反了联邦证券法；11月16日，SEC 再次对 Marathon Digital 公司发起调查，要求后者提供比特币挖矿数据中心的文件和通讯；同时起诉 Ripple 违反证券法。

11月15日，美国总统拜登正式签署了「基建法案」，该法案明确要求虚拟货币的「经纪人」，即任何代表其他人促成数字资产交易的人，向税务机构报告交易的相关信息。法案规定作为「经纪人」，必须将超过 10,000 美元的交易的详细信息上报给美国国家税务局（IRS）；作为收款方，当接受超过价值 1,000 美金的虚拟货币时，必须要核验发送人的信息，记录对方的社会保障号（SSN），以及交易的其他相关信息，并于15天之内上报给 IRS。

欧洲也加速采取行动，欧盟委员会针对投资者和开发者起草一份名为《加密资产市场监管规则》（MiCA）的新规则手册，该规则将虚拟货币交易所纳入监管，包括制定监督欺诈行为方面的标准，确保透明度以及建立治理标准。新规还拟禁止某些种类的稳定币的存放支付利息，并要求现有的稳定币寻求授权才能在欧盟内进行交易。

自新加坡金管局宣布，将与虚拟货币交易相关的服务纳入新加坡《支付服务法》监管范围以来，严格要求所有虚拟货币行业参与者登记并申请相关牌照，未申请到资格的虚拟货币服务商或被全面取缔。

## 1.3 TVL 爆炸性增长 新安全问题涌现

2021年 DeFi 的市场规模呈现抛物线式增长，智能合约中的总锁仓值「TVL」突破 2,000 亿美元，较年初的 200 亿美元，增长率达到 1,100%。

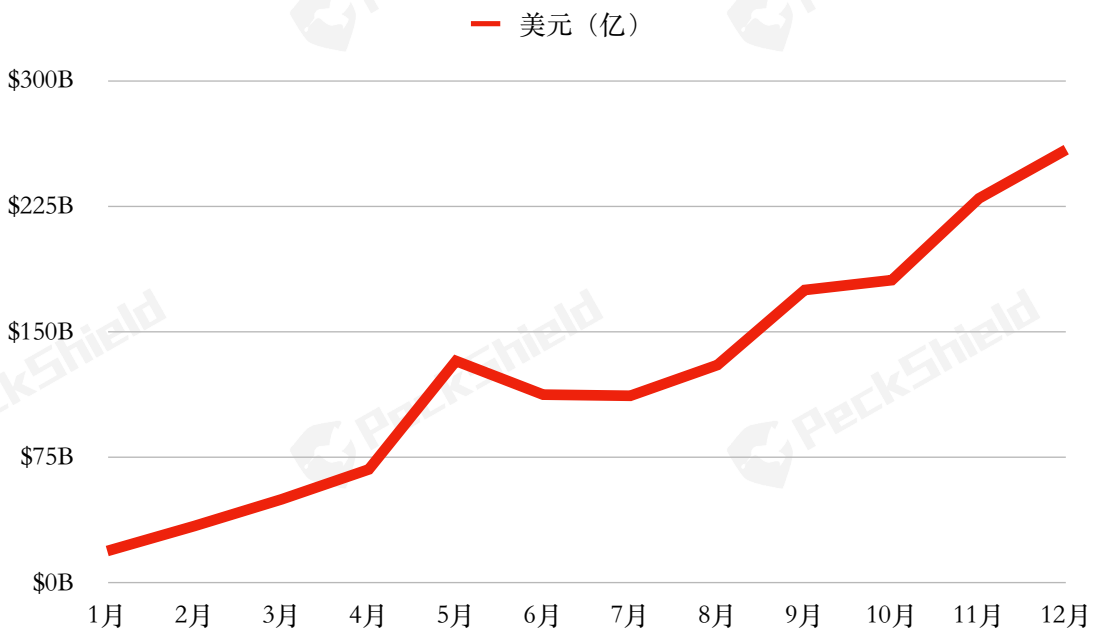



图1 2021年 DeFi 市场整体发展趋势

随着2021年上半年向多链拓展的落地，DeFi 展现出以以太坊为主导的「百链齐放」的态势，并呈现出多链并行的常态化趋势。

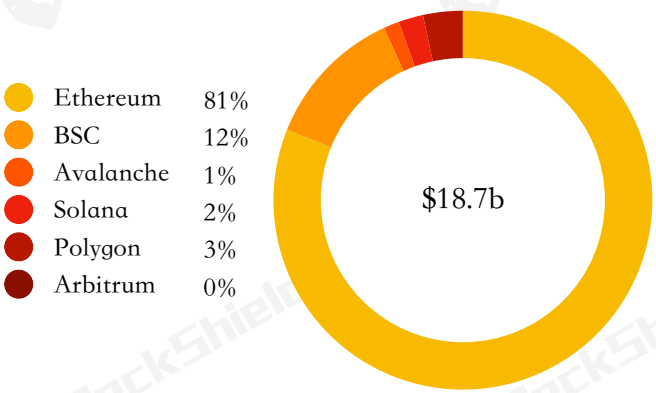



图2 2020年 DeFi 市场占比

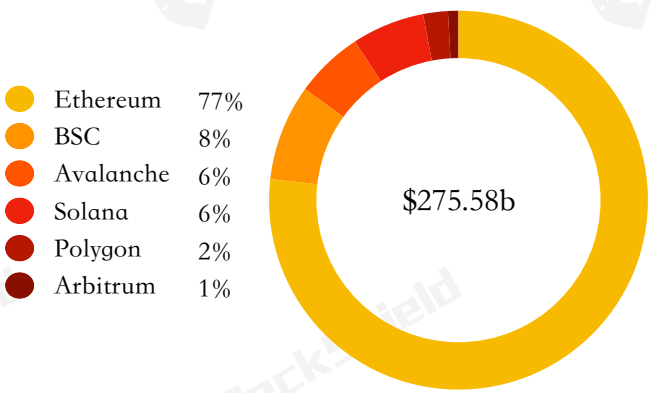



图3 2021年 DeFi 市场占比

从各公链的市场份额来看，以太坊以绝对优势独占鳌头，呈现出稳步增长之势，币安智能链（BSC）在受到5月行情影响回调后增长放缓。自9月起，在加码激励机制、引入头部协议等因素的影响下，Avalanche、Solana、Arbitrum 等新兴公链增长势头强劲。

随着 DeFi 领域的扩展，各协议间的边界逐渐模糊，协议间的竞争日趋白热化。以以太坊为基础的 DeFi 生态系统中占据领先地位的协议（按流通市值、锁仓价值、月度独立用户等指标来看）已凸显优势，而这些协议开始朝着具有健全功能的金融集团发展壮大。虽然大多数协议在推出时针对协议进行特定金融细分市场的功能集定位，但随着协议提高委托资本的流动性效率，并在吸引到关注度时进一步变现，协议之间的边界变得模糊，各个协议之间犬牙交错，在成本、防篡改与灵活性的权衡、激励结构、社区和网络效应、多链拓展等方面的竞争愈演愈烈。

跨链桥生态在这一年蒸蒸日上，成为链接协议在 Layer1 和 Layer2 拓展和沟通的刚需，巨大营运资金需求和服务的涌现，使得跨链桥快速扩张，帮助嫁接代币的快速流转。

在规模急速扩大的同时，DeFi 隐藏的安全问题也逐渐暴露出来，随着准入门槛的提高，大机构的入场，「安全」、「合规」的要求愈加严苛，再加上监管部门的关注，DeFi 行业缺乏风险管理和链上监测工具的短板亟待解决。

# 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。

PeckShield「派盾」通过积累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、BSC、HECO 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，我们曾成功地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，并及时通知交易所及合作伙伴；


图4 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通过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 基于拥有的一整套标签数据库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，以及实时预警安全事件。


图5 虚拟货币反洗钱态势感知系统截图

### 7）DeFi 生态威胁情报：

PeckShield Alert 是 PeckShield 旗下的威胁情报 SaaS 平台，它支持快速搜索 DeFi 生态最新安全威胁，汇总可操作情报、安全专家定位分析多方位并行。PeckShield Alert 结合专业人员和机器生成的情报支持，通过自适应风险评分将信号与噪声分离开，利用安全工具集成和

情报订阅源的生态系统自动从内部和外部数据源中获取威胁情报，从而协助去中心化生态更快、更准地检测和定位风险点。

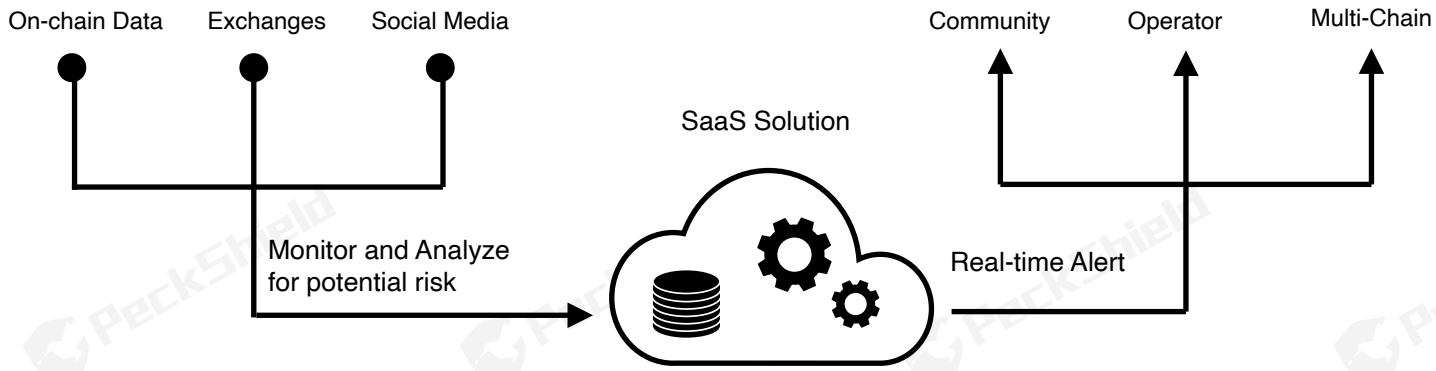



图6 PeckShield Alert 威胁情报系统

## 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2021年5月起，不断收紧的监管政策给为虚拟货币提供服务的公司带来巨大挑战。国内政策的调整，使得全球交易所排位战再次发生变化。9月24日，中国人民银行联合网信办、公检法等十部委联合发布《关于进一步防范和处置虚拟货币交易炒作风险的通知》，在中国境内叫停包括通过互联网向中国境内居民提供服务的境外虚拟货币交易所。

一方面，切断虚拟货币交易所在国内的流通通道有效地控制了利用虚拟货币实施的洗钱、赌博等犯罪活动和以虚拟货币为噱头的非法集资、传销等犯罪活动；另一方面，监管政策也倒逼黑灰产业转向更加隐蔽、不做 KYC 认证的 C2C 洗钱通道，以及滋生出快速扩张的「嵌套交易所」、「混合交易所」等灰色地带。

虚拟货币蔓延至各类网络犯罪活动中，越来越多的犯罪活动不再通过传统的金融系统支付，而是利用虚拟货币的匿名性、跨国性和抗审查性，通过虚拟货币收取勒索赎金等形式逃避监管和执法机关的追踪。

由于涉及虚拟货币洗钱的手段愈发复杂、多样、隐蔽，要实现有效遏制，除了在监管措施上，采取监管科技理念，引入虚拟货币合规化及反洗钱（AML）服务等技术，落实风控措施，虚拟货币交易平台也应当加强自身的风险防控意识，针对寄生在平台中的各项风险点，利用技术手段采取风险控制措施。

## 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。

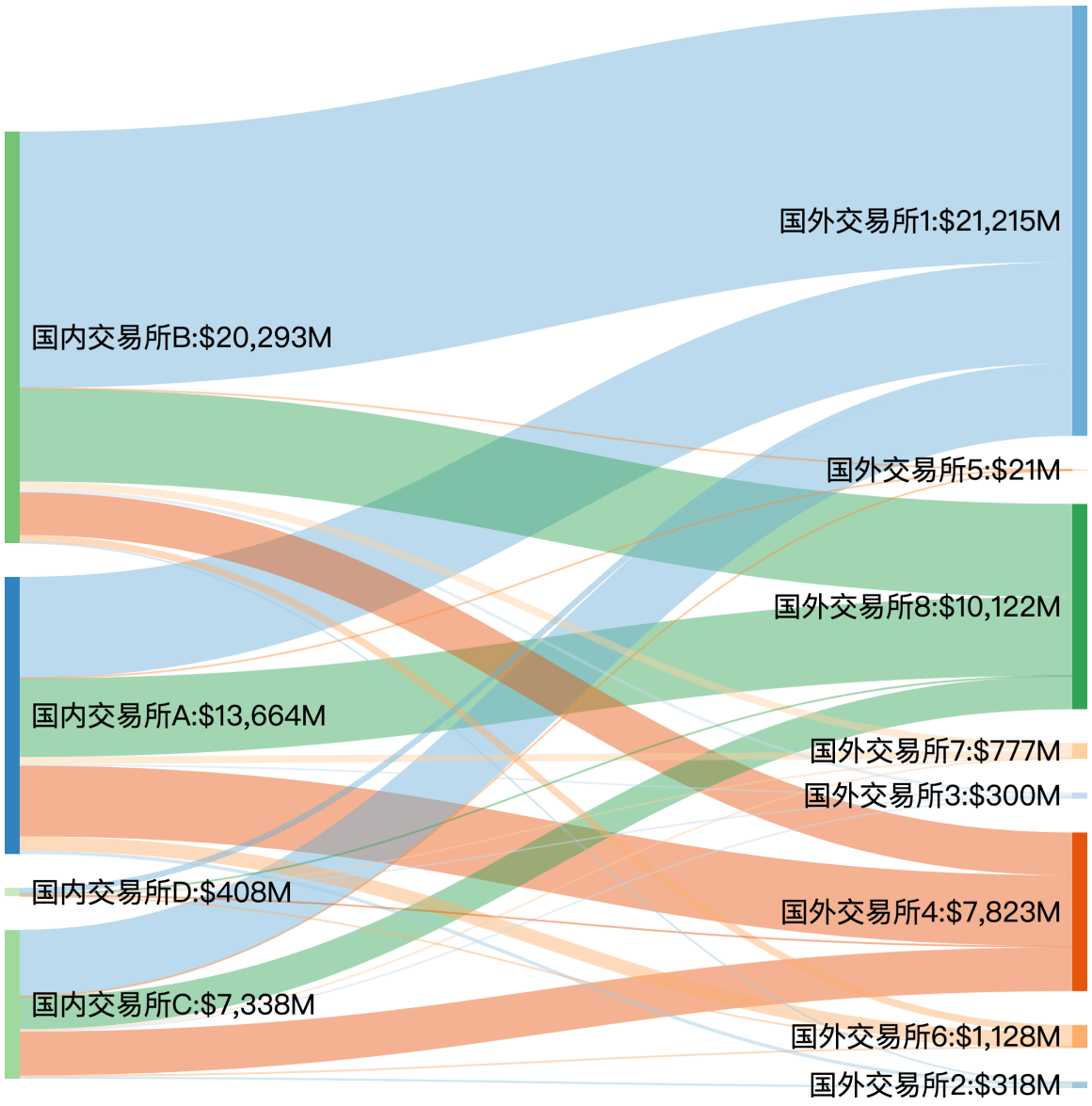



图7 2021年从国内向国外各大交易所流出的资金总量

如图7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年从国内交易所流出到国外交易所的资金总量达到 417 亿美元，同比增长了 138%。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年的 BTC 流出资金总量是2020年流出的资金量的 2.4 倍。这主要是受到国内发布一系列的监管政策以及比特币的价值在2021年持续走高等因素的影响，国内中心化交易所内的比特币呈现出明显的流出状态。值得注意的是，在政策的监管下，以往在海外注册壳公司、服务器放在国外、技术和运营放在国内的方式无法持续，随着多家交易所或相关服务陆续在2021年年底完成对中国大陆用户的彻底清退，预测2022年跨境流出的虚拟货币资金将会骤减。

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年，DeFi 领域实现了飞跃式发展，截止2021年12月31日 DeFi 总锁仓量（TVL）超过2,000 亿美元的规模。锁在各链上的有价资产规模再度跃升，使得逐利者趋利而来。

值得注意的是，纵览整个 DeFi 版块在这一年中快速扩张的整体趋势，以及整个生态对安全基建的布局，2021年 DeFi 领域发生的安全事件实际上较2020年有所改善。2021年 DeFi 造成的损失占整个 DeFi TVL 的比例为 0.93%，2020年 DeFi 造成的损失占整个 DeFi TVL 的比例为 1.43%。

截至2021年12月31日，DeFi 安全事件达到 205 起，损失超 17.87 亿美元，单从数量上来看，同比增长 242%，损失金额同比增长 600%。

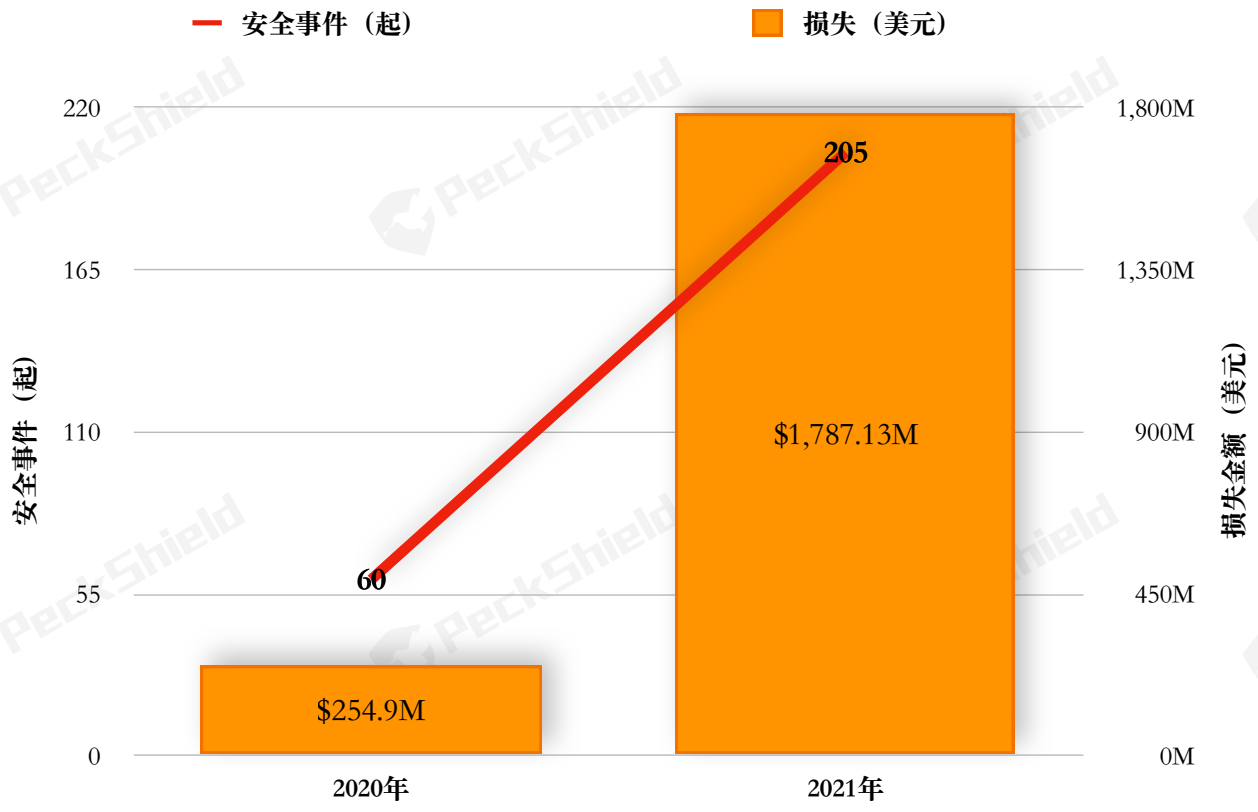



图8 2021年与2020年 DeFi 安全事件数量和损失对比

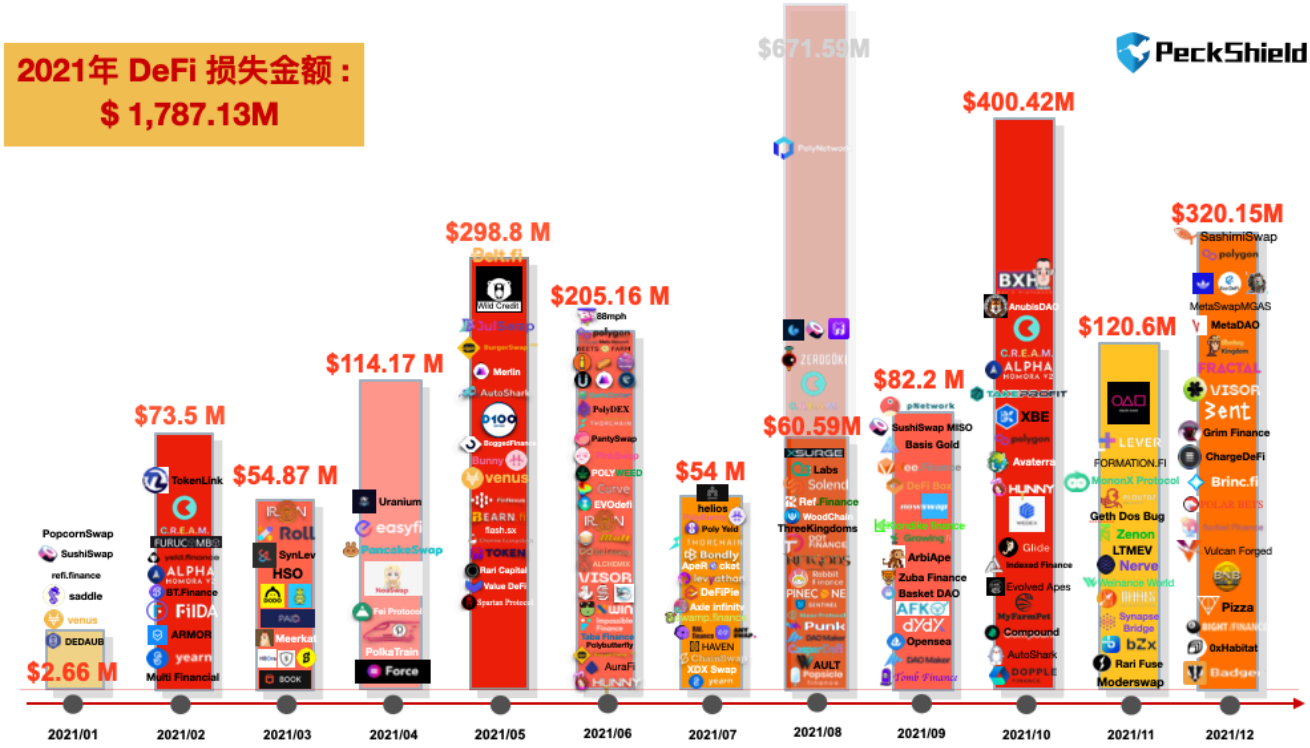



图9 2020全年 DeFi 安全事件数量和损失概览

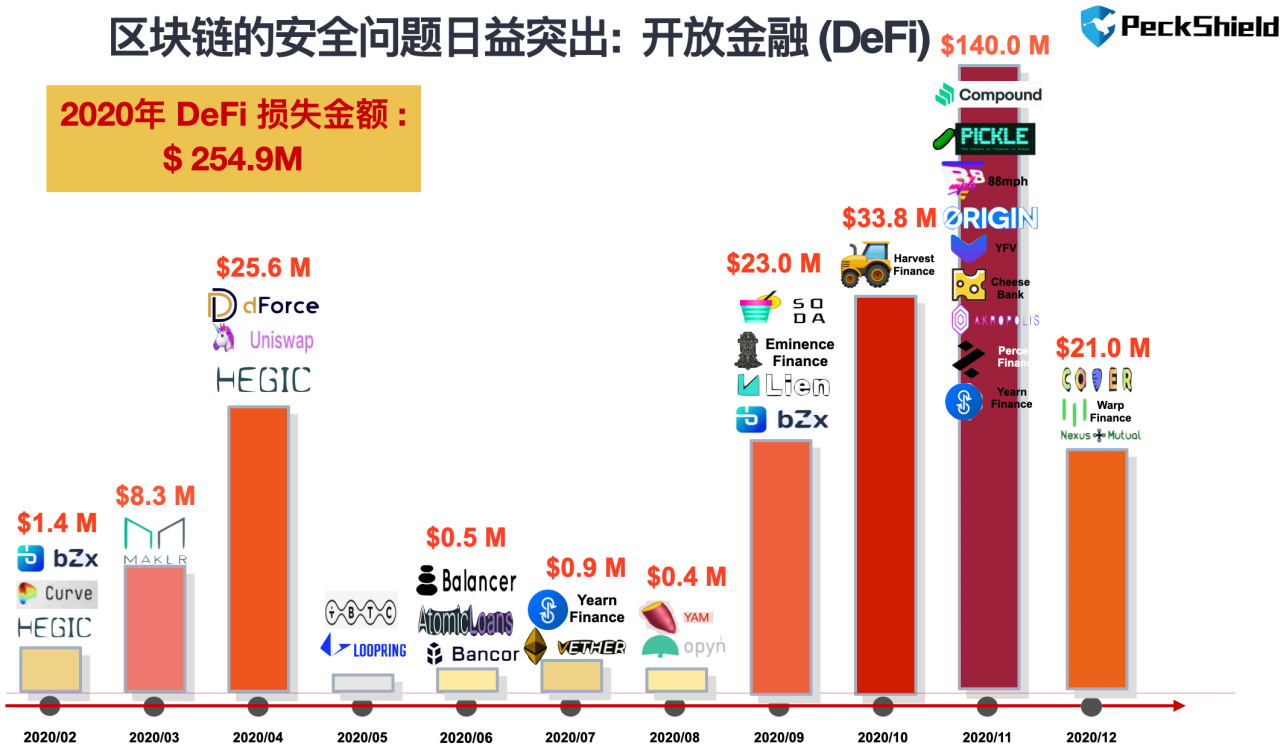



图10 2021全年 DeFi 安全事件数量和损失概览

## 4.2 2021年 DeFi 安全事件统计分析

在经过这一年的高速发展，DeFi 在产品、资金和用户规模上再次有了质的飞跃。虽然受到5月整体行情的影响出现小幅回落，但在各新兴公链相继推出激励策略的驱动下，锁定在各公链上的 DeFi 协议中的价值快速回升，并进一步突破新高，以 BSC 为首的新晋者开始重塑市场格局。

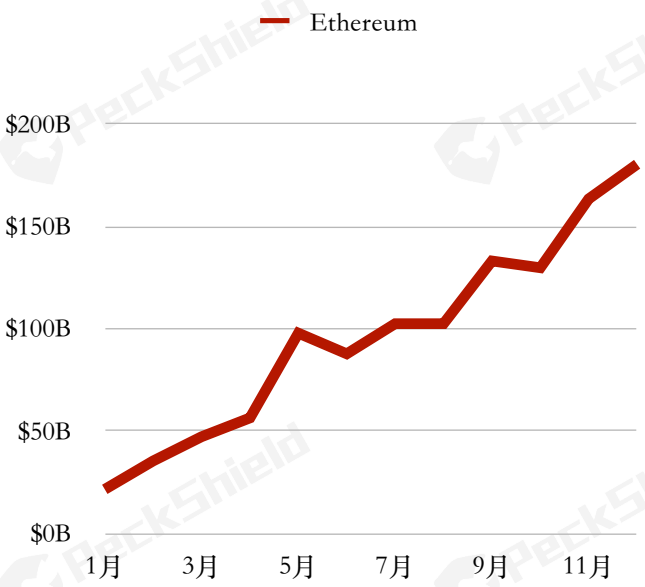



图11 以太坊 TVL 全年趋势

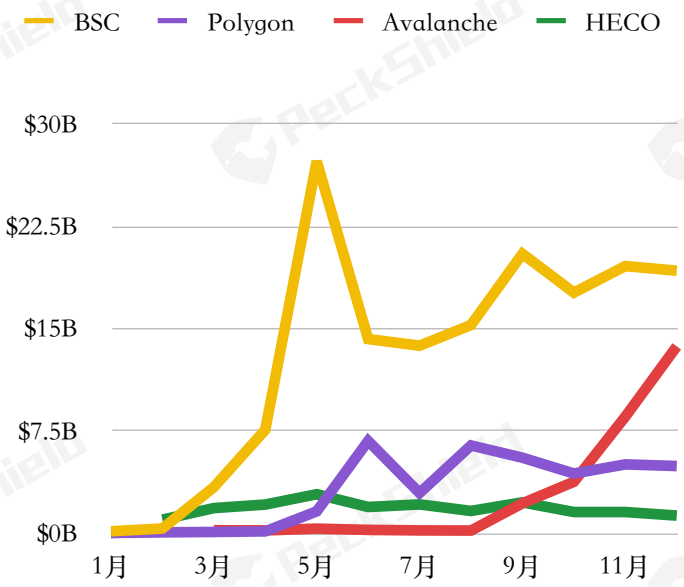



图12 主要公链 TVL 全年走势

虽然新兴公链表现亮眼，但以太坊仍是 DeFi 的焦点，它以超过 1,800 亿的锁仓量攥着 DeFi 市场 75% 以上的份额，增速放缓但仍在稳步增长（如图11和图12所示）。

BSC 以约 200 亿美元的锁仓量紧随其后，占整体 TVL 的 8%，较年初的 12% 出现资金外流的情况，但 BSC 不论是锁仓量还是在市场份额上的扩张速度都不容小觑（如图12所示）。

2021年，DeFi 的链上资产量迎来井喷式增长，但尚处于发展初期，在发展壮大的过程中不得不经历欺诈、主观作恶、技术漏洞、风控风险等阵痛。

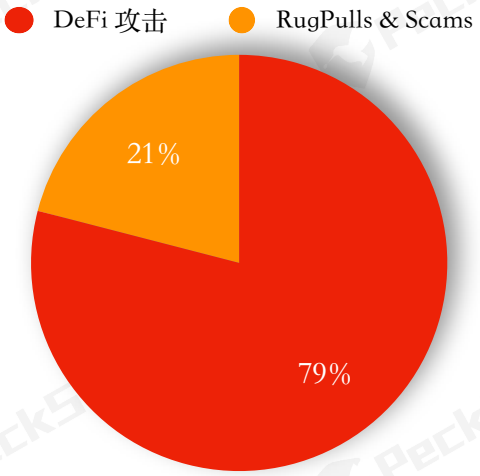



图13 2021年 DeFi 安全事件攻击和 RugPulls & Scams 数量对比

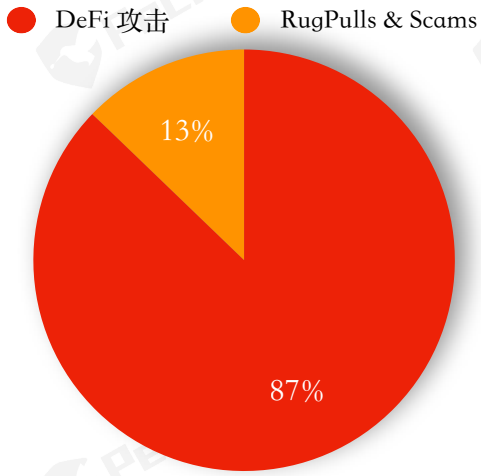



图14 2021年 DeFi 安全事件攻击和 RugPulls & Scams 损失对比

如图13和图14显示，2021年发生的 DeFi 安全事件中，79% 源于攻击者利用 DeFi 协议自身（外部或内部）存在的漏洞套利，损失金额约 15.6 亿美元，占 DeFi 安全事件总损失的 87%；21% 则源于 RugPulls & Scams，造成损失约 2.29 亿美元，占 DeFi 安全事件总损失的 13%。

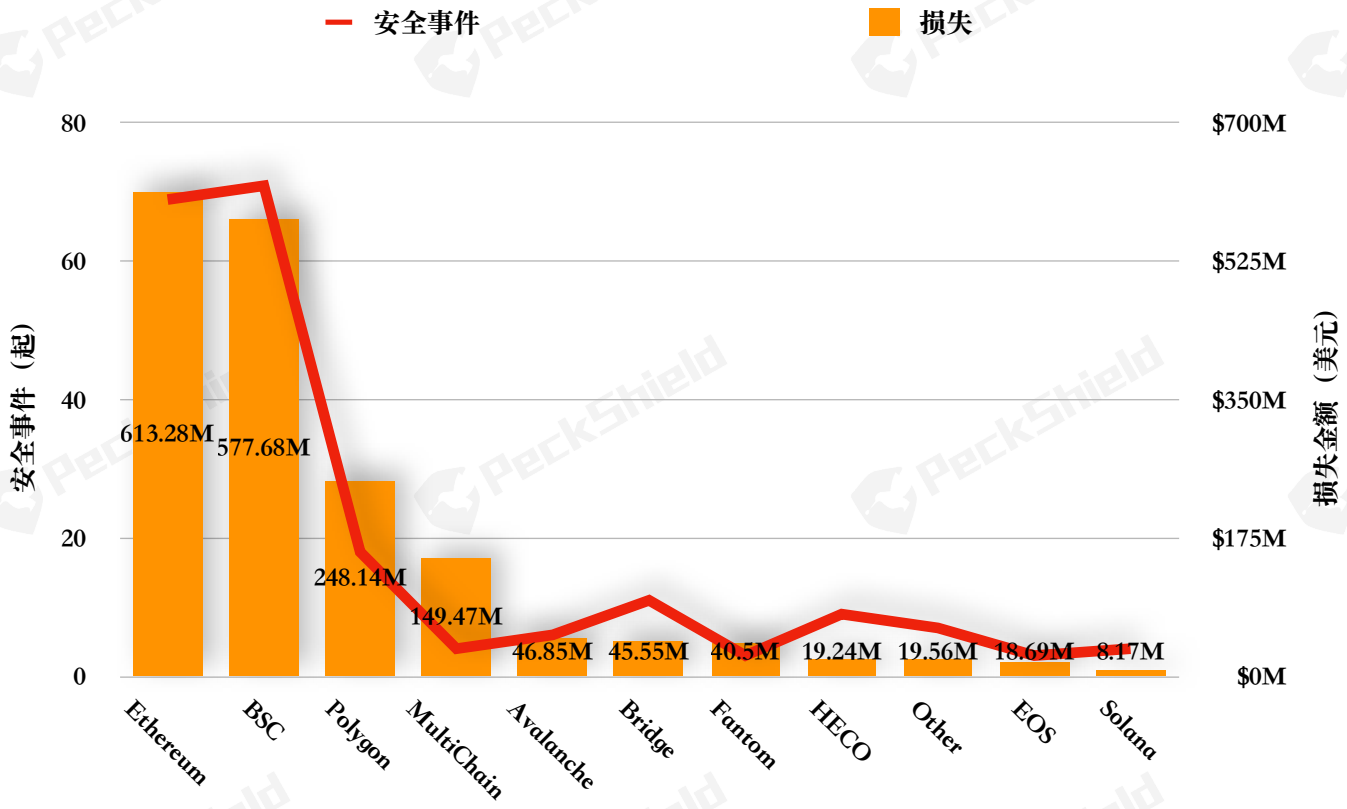



图15 2021年安全事件在各生态上的数量和损失统计

图15展示了在以太坊、币安智能链（BSC）、Polygon、Avalanche、跨链桥、HECO、EOS、Solana、Fantom 上发生的 DeFi 安全事件概况，在这几个生态发生安全事件数量分别为 69 起、71 起、18 起、6 起、11 起、9 起、3 起、4 起、3 起；所造成损失分别为 6.1 亿美元、5.78 亿美元、2.48 亿美元、4,685 万美元、4,555 万美元、1,924 万美元、1,869 万美元、817 万美元和 4,050 万美元，占比依次为 34%、32%、14%、3%、3%、1%、1%、不到 1%、2%（如图16和图17所示），反映出在各公链生态上锁仓的资金量越大，链上日活度越高，生态的增长速度就越快，相应地，也越容易遭到欺诈者、攻击者的觊觎。

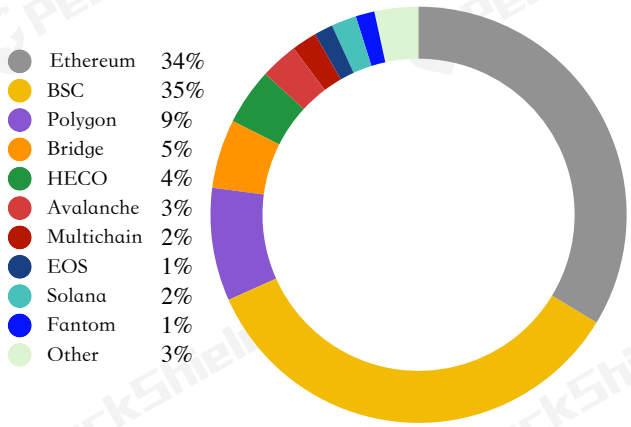



图16 各生态 DeFi 安全事件数量分布

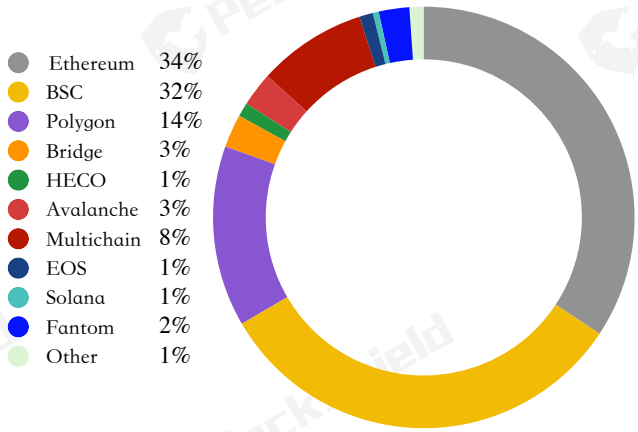



图17 各生态 DeFi 安全事件损失分布

2021年 DeFi 安全事件主要集中在以太坊和 BSC 上，数量和损失的总占比都达到整个生态安全事件分布的 68%。随着多链并行的局势稳步发展，DeFi 安全事件开始出现跨链、多链并发的趋势。

各 Layer1 和 Layer2 相继推出激励机制吸引雇佣资本，前期依托于资本的快速注入增长势头强劲，刺激 TVL 短时飙升，也吸引了攻击者、欺诈者在热钱堆里辗转。

Polygon 的 TVL 在6月达到全年峰值时，在其上发生的安全事件也达到峰值。同样地，9月 Avalanche 生态呈指数增长后，在其上发生的安全事件呈现出从无到有的趋势（如图18所示）。

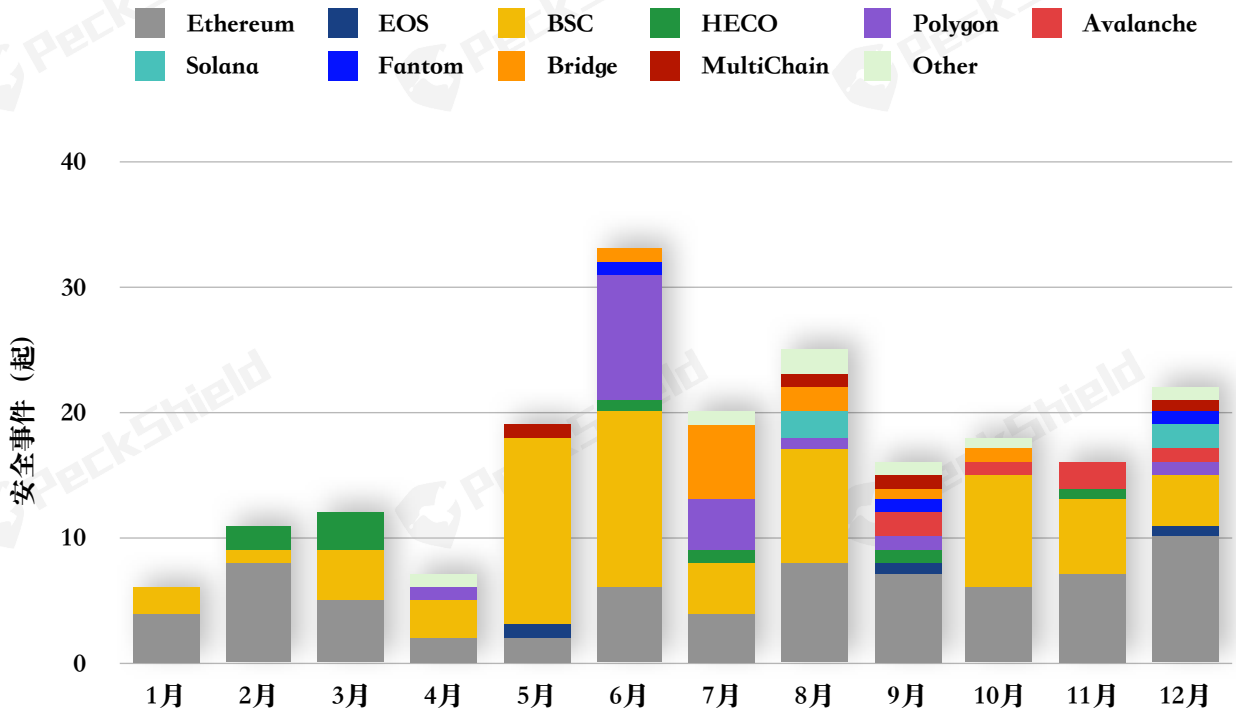



图18 2021年1月至12月安全事件分布统计

## 4.3 DeFi 攻击种类概览

从攻击类别来看，攻击者的手法可谓是五花八门，从逻辑缺陷，到利用闪电贷为资本的攻击、重入攻击、私钥破解、前端漏洞，甚至是通过社交手段对关键信息进行一一攻破。

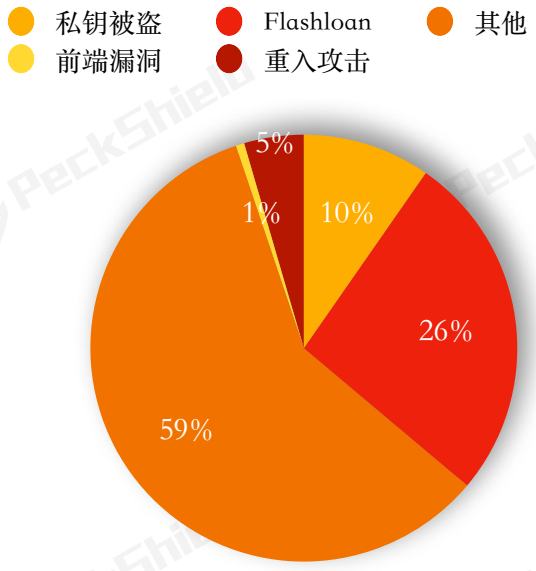



图19 主要攻击手段数量占比

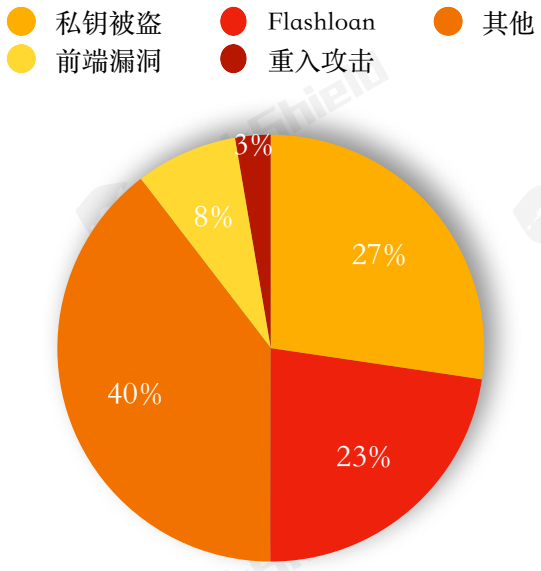



图20 主要攻击手段损失占比

据 PeckShield「派盾」统计，这 197 起 DeFi 安全事件中（除却统计中的 8 起白帽攻击），主要的攻击手法集中在利用 FlashLoan（闪电贷）作为资本发起的攻击、RugPulls & Scams、前端漏洞以及私钥被盗引入的运营风险、重入攻击，这几种主要攻击手段占比达到 DeFi 安全事件总数量的 41%，在总损失中的占比达到 60%。

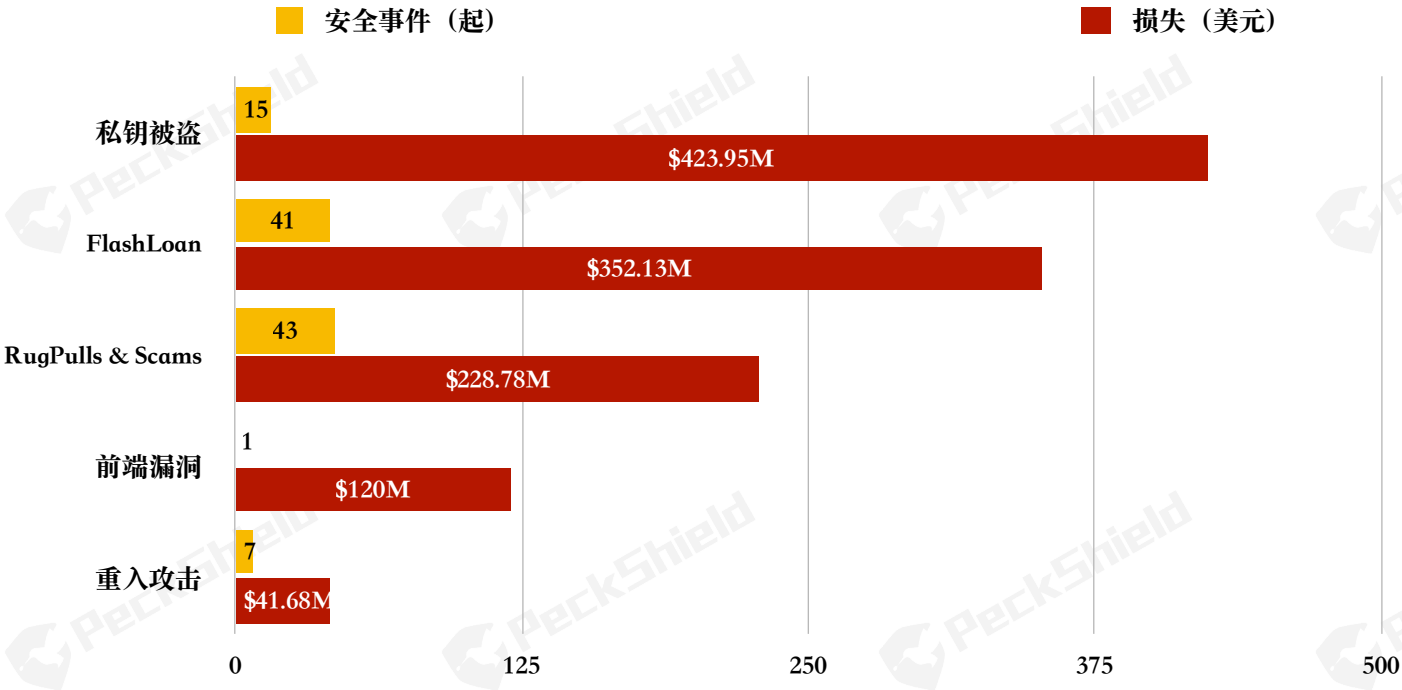



图21 DeFi 安全事件主要攻击手段数量和损失统计

2021年，发生 41 起利用 FlashLoan（闪电贷）作为资本发起的攻击，造成损失 3.52 亿美元，作为 DeFi 领域衍生出来的全新的借贷模式，FlashLoan 从诞生到兴起就备受争议，一方面，FlashLoan 为普通用户带来以小博大的资本，如套利、抵押物互换、清算等；另一方面，FlashLoan 无需抵押的借贷特性使得攻击者能以很小的代价获得大量的可用资产，从而实现价格操纵攻击，或者放大攻击产生的收益。

RugPulls & Scams 达到 43 起，损失金额 2.29 亿美元，RugPull 可视为「软跑路」，即 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。由于去中心化交易所的发币门槛低，不需要上币费，甚至可能没有认证和审核，这不仅大大降低了欺诈者行骗的成本，而且为他们打着「去中心化」、「社区自治」的幌子，不披露创建团队的信息，甚至在事情败露之后，换「马甲」提供了便利。

私钥被盗引入的运营风险虽然仅发生 15 起，但造成的损失大、影响范围广。因私钥被盗造成损失金额达到 4.24 亿美元，发生率仅为 9%，损失占比达到 27%。如果把智能合约视为一个提供服务的「机器人」，很多时候运营方需要留有人工的权限去控制这个「机器人」，例如关停「机器人」，再例如冻结、转移、没收智能合约中某个账户的资产等，如果存在这样的私钥管理人工权限，就会引入额外的风险。

这种类型的安全事件在技术上并不需要攻击者攻克复杂的智能合约，只需要获取或盗取私钥就可以转走锁在整个协议的虚拟资产，甚至摧毁整个协议。它在 2021年第四季度成为作恶者或攻击者使用频率最高的攻击手段。这种攻击手段在2018年至2019年期间主要运用于盗取中心化交易所中热钱包的资产，2021年无论是中心化交易所还是去中心化协议都或多或少受到私钥被盗导致的重创。

近几起私钥被盗安全事件显示出目前去中心化协议仍处于处于「半中心化」治理的过渡过程，而这样的「半中心化」就会随之引入「中心化」运营风险。这也给 DeFi 的生态敲响警钟，给社区留下思考：去中心化的社区是否需要引入密钥管理；运营团队是否需要主动披露密钥权限的存在；是否对密钥权限设置了延时生效机制；是否引入了密钥的风控管理。

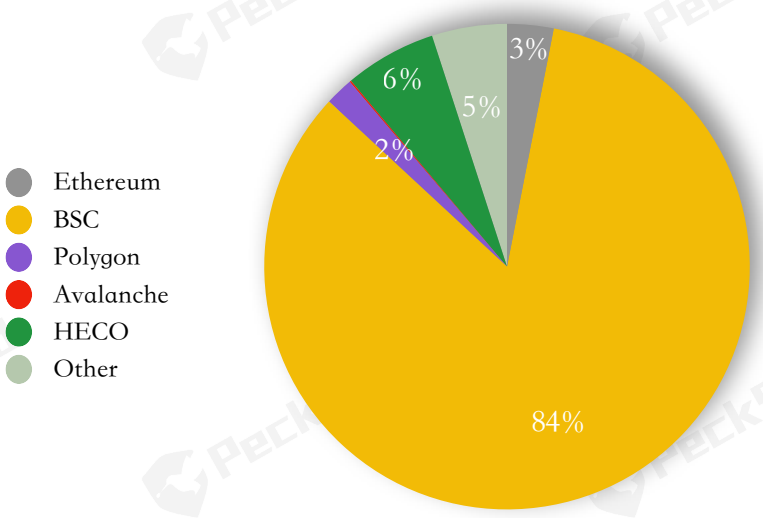



图22 各主要公链 RugPulls & Scams 比例分布

从上图可知，在交易所公链上发生的 RugPulls & Scams 造成的损失达到整个 DeFi RugPulls & Scams 造成总损失的 90% 以上。

从推出到声势壮大，与中心化交易所紧密相关的公链受困于横亘在投资者与交易所之间对「中心化」的认知鸿沟。一方面，得益于交易所本身的庞大社区基数，交易所公链快速崛起，甚至达到繁荣；另一方面，质量参差不齐的协议涌入生态，其中掺杂着嵌入「去中心

化」概念、被用户斥为割一波就走的「土狗」项目。一时间卷池跑路、币跌矿塌，团队信息造假，项目方砸盘等乱象充斥着整个生态，使交易所公链陷入信任危机。

事实上，这样的「土狗」项目在2020年下半年因流动性挖矿模式在以太坊上掀起 DeFi 热潮时，也曾大规模席卷以太坊，使其信誉受损。

频发的 RugPulls & Scams 推动整个生态的参与者摸索防范和整治的方法，例如，引入疑似 RugPulls & Scams 高危预警，联动监管机构、中心化机构、去中心化机构围堵拦截被骗资产，减小用户的损失，以及探索设立社区治理方案、保险方案来完善社区建设。

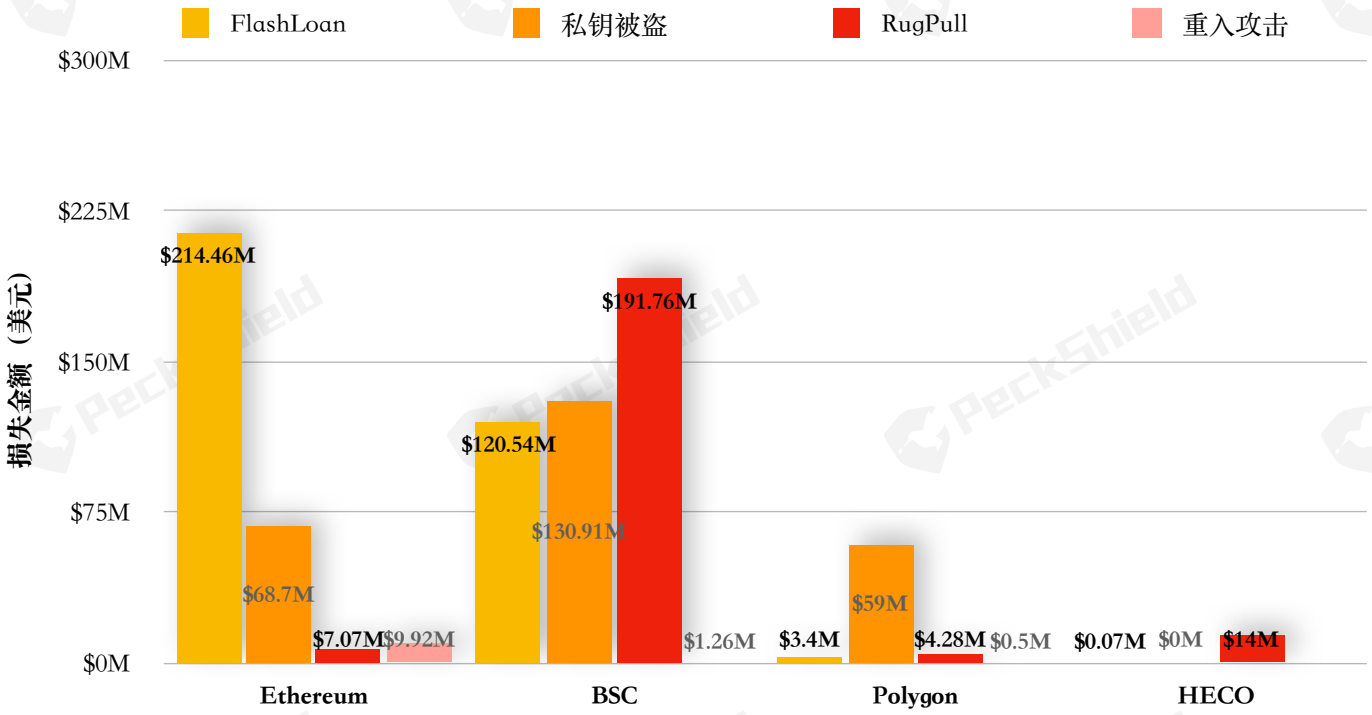



图23 各主要生态上 DeFi 安全事件主要攻击手段数量分布统计

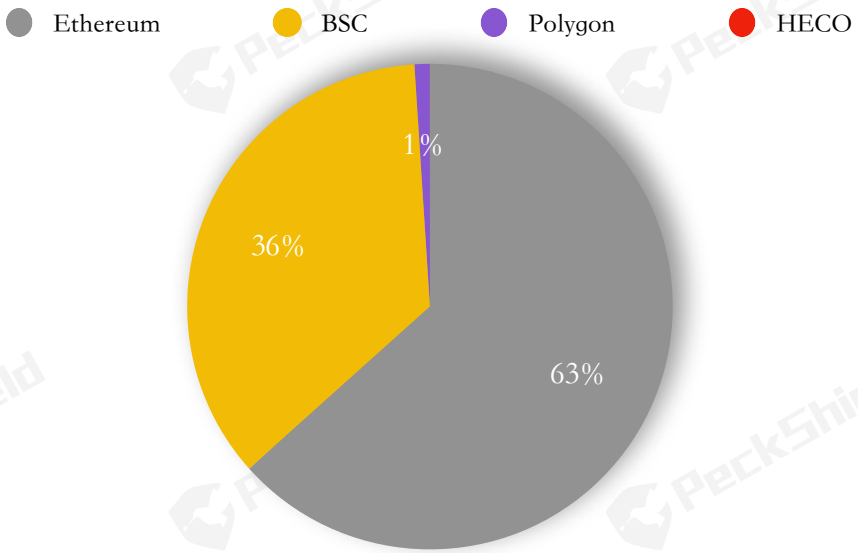



图24 各主要公链利用 FlashLoan 为资本进行攻击比例分布

利用 FlashLoan 作为资本进行攻击造成的损失，60% 以上发生在以太坊上。FlashLoan 自2020年兴起后，就成为攻击者最常用的试错手段之一。幸运的话，攻击者在借出闪电贷后，可以借助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，只要在一个区块交易中偿还 FlashLoan 就可以获得可观的收益。

从2021年起，以太坊上的 DeFi 应用接踵而至，DeFi 协议之间的可组合性，使得 DeFi 协议的复杂性指数性增长，除了「乐高性」，协议之间的相互影响也引入了兼容性的风险，而往往这些安全性最差的一环容易被攻击者盯上。此外，过于依赖复刻以太坊上 DeFi 协议的协议也会因此受到连带影响。这就使得在成本极低的状况下，攻击者们开启了在多条链上找相似漏洞的帷幕。

## 4.4 跨链桥安全事件统计

2021年市面上涌现出上百条公链，且它们的资金量颇具规模，随着涌入的公链越来越多，促使不同网络之间需要互操作性的刚需。过去一年中，跨链桥已经呈现了爆炸式增长。据 Dune 数据平台数据显示，截至2021年12月27日，跨链桥 TVL 突破 400 亿美元，较4月增长 700%。

| 日期 | 跨链协议 | 攻击原理 | 损失金额 |
|---|---|---|---|
| 2021-06-29 | THORChain | Logic error on ETH Bifrost when handling symbols same as ETH | $140k |
| 2021-07-02 | ChainSwap | Funds are drained by sendfrom | $800k |
| 2021-07-10 | Anyswap | Deduced the private key | $7.9M |
| 2021-07-11 | ChainSwap | White list to call receive | $8M |
| 2021-07-14 | RAI Finance | RAI access and payment authority addresses | $410k |
| 2021-07-16 | THORChain | Logic error on ETH Bifrost | $8M |
| 2021-07-23 | THORChain | Logic error on ETH Router | $8M |
| 2021-08-10 | O3 Swap | Poly Network was hacked | $200k |
| 2021-08-10 | Poly Network | BookKeeper manipulation bug | $611M (Retured) |
| 2021-09-20 | pNetwork | Event logs bug | $12M |
| 2021-10-21 | Plasma bridge | Double spending by bypass branch mask verification | $2M |

图25 跨链桥安全事件数量与损失统计

自7月初到8月末，跨链协议屡遭攻击者“光顾”，究其缘由，主要是因为跨链协议往往涉及到与多条链和多个合约交互，流程上相对复杂，风险点也较多，就更容易面临安全挑战。

尤其是今年8月跨链项目 Poly Network 突遭黑客攻击，由于其损失金额高达 6.1 亿美元（已返还），不仅被载入 DeFi 史上涉案金额最大的黑客事件，更是成为整个虚拟货币历史上涉案金额最大的黑客事件，超过了 Mt.Gox 事件（744,408 枚 BTC，当时总价值约 4 亿美元），以及 2018 年的 Coincheck 大案（5.23 亿枚 XEM，当时总价值约 5.34 亿美元）。 Poly Network 被盗推动整个行业在各个维度加强对安全问题的反思。

虽然跨链桥为区块链生态系统释放了创新，但随着该赛道的蓬勃发展，其承载的资金量也在快速膨胀，这就不免让伺机而待的攻击者寻找其薄弱的地方进行试探。

从赛道演变趋势来看，跨链桥的生态将会进一步扩张，跨链桥的边界将会向外扩大，例如，嵌接其他金融服务，提供跨链+交易、跨链+挖矿、跨链+借贷等方案，跨链桥间的竞争不论从功能上还是社区上都会愈发激烈，这也进一步抬高了对跨链桥的安全要求。

## 4.5 DeFi 的安全风险与解决思路

DeFi 领域的风险点主要集中在智能合约执行风险、操作安全性以及对其他协议和外部数据的依赖性风险。

智能合约执行风险：如果攻击者利用代码本身存在的漏洞，就有机会耗尽智能合约的资金、造成混乱，甚至摧毁协议。合约执行中也存在类似的风险，例如，一些 DApps 会向用户确认授权，授权转移用户钱包中无限数量的代币，以此来减少操作次数，提高效率，但这种授权会使用户的资金处于风险当中。

操作安全：许多 DeFi 协议和应用引入了密钥管理的方案，允许预定义的个人（通常为协议方的核心团队）有权限升级合约并执行紧急停机机制。虽然这种预防措施能够规避一些安全风险并保持一定的灵活性，但同时也为协议本身埋下风险点，如果密钥持有者管理或存储密钥不当，使得作恶的第三方有机可乘获得密钥，就会威胁到协议的安全。另外，核心团队成员本身也可能作恶。

一些协议试图通过多重签名或时间锁（Timelock）来降低这种风险，多重签名需要 M-of-N 个密钥来执行智能合约的任何管理功能，时间锁（Timelock）则是指定可确认交易的最早时间。另一些项目则依赖于治理机制来解决问题，但仍存在话语权掌握在少数人手里、高度集权化的风险。

依赖关系风险：DeFi 的创新点在于其开放性和可组合性。可组合性允许各种智能合约和 DApps 相互交互，并基于现有合约的组合衍生出更多玩法，但这些交互会引入协议之间严重的依赖性，如果一个智能合约存在漏洞，则可能对整个 DeFi 生态系统中的多个应用产生连锁反应。

外部数据风险：在 DeFi 应用中，不论自身配置还是依赖第三方供应，都需要通过预言机来与外界行情保持实时联动，这种依赖也引入了潜在的外部数据风险。

PeckShield「派盾」建议新合约在上线之引入第三方专业机构对智能合约进行全面而专业

的检查，除了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。

如果出现资产被盗的情况，及时暂停智能合约中的交易服务，或者在专业机构的指导下采取相关紧急措施，避免再度遭到攻击的风险；寻求专业机构定位漏洞根源，引入一定的风控熔断机制，引入第三方态势感知服务等，做到第一时间响应安全风险，及时排查封堵安全攻击，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。

# 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

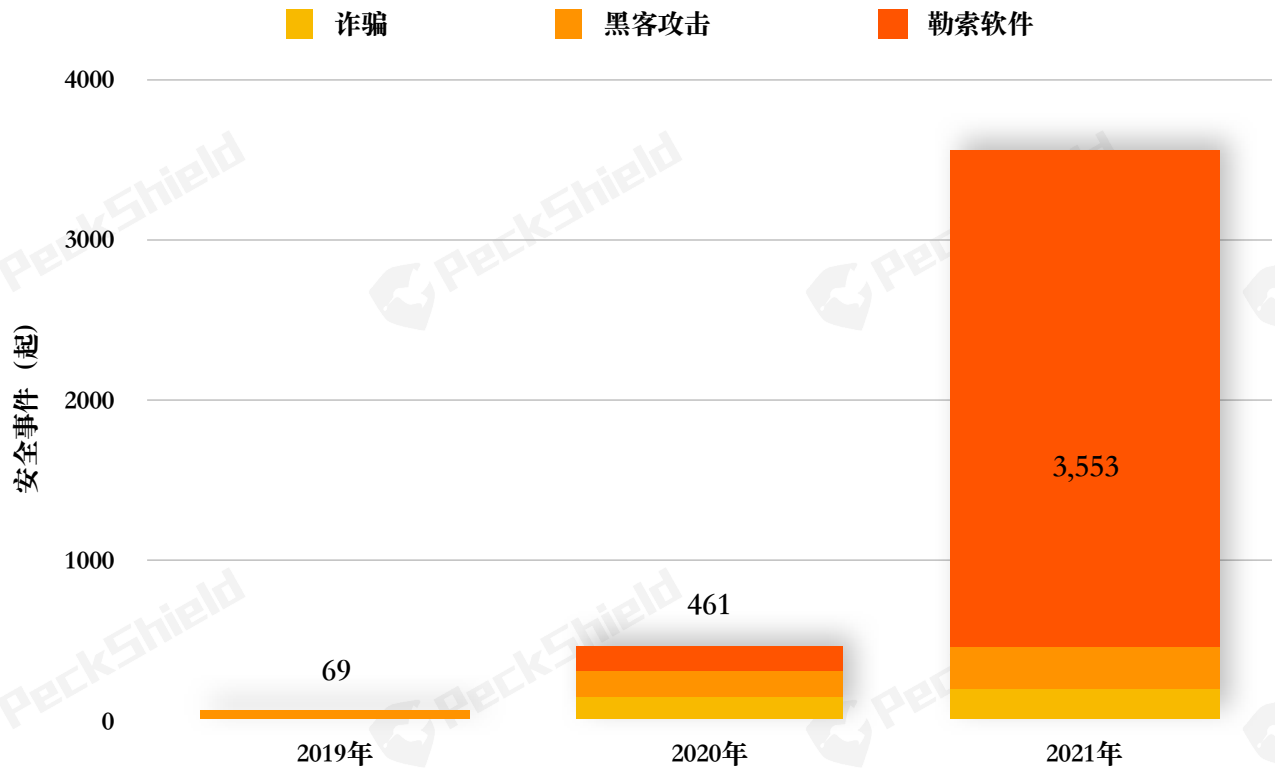



图26 近三年年虚拟货币安全事件统计

截至2021年12月31日，虚拟货币行业共发生重大安全事件 3,553 起，共计损失逾 148.2 亿美元，其中黑客攻击约 261 起，诈骗事件 201 起，勒索攻击约 3,091 起。

如图26所示，2021年涉及虚拟货币的勒索事件的数量较前两年呈抛物线式飙升，2019年年勒索事件仅 6 起，2020年年增长了 22 倍，达到 140 起，2021年超过 3,000 余起，同比增长 2,107%。

黑客攻击从中心化交易所、钱包等基础设施拓展至去中心化领域，2019年黑客攻击达到 43 起，2020 年同比增长 263%，达到 170 起，2021年激增至 261 起。在2021年发生的 261 起黑客攻击中，有 60% 以上源于 DeFi 攻击事件。

随着各主要监管机构普及虚拟货币交易特征分析工具的应用，2021年监测到的涉及虚拟货币的欺诈事件的曝光度有所增长，同时，欺诈蔓延至 DeFi 领域，衍生出「貔貅盘」、「RugPull」等新型欺诈模式。2021年欺诈数量同比增长 33%。2019年欺诈事件为 20 起，2020年达到 151 起，2021年达到 201 起。

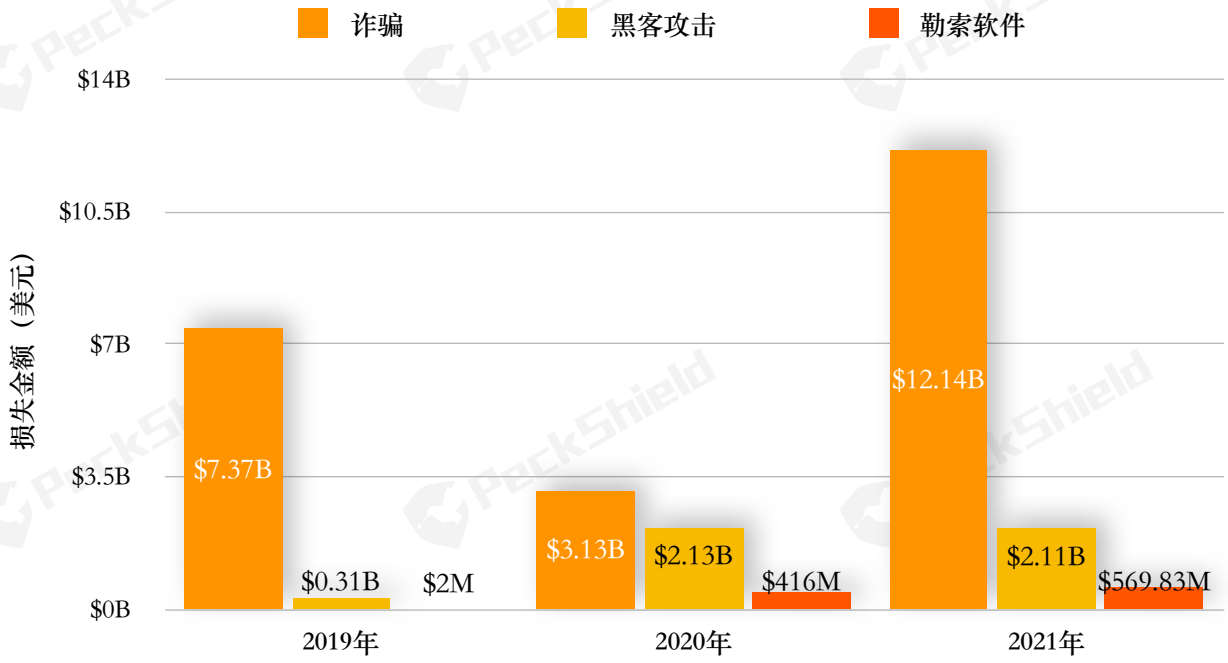



图27 近三年虚拟货币安全事件造成损失统计

如图27所示，2019年虚拟货币安全事件造成的经济损失高达 76.79 亿美元，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，其中黑客攻击造成 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 1,000 万美元的损失。

2021年虚拟货币安全事件造成经济损失 148.2 亿美元，其中黑客攻击造成损失 21.1 亿美元，欺诈事件造成损失 121.4 亿美元，勒索事件造成损失至少 5.7 亿美元。从损失数额来看，诈骗事件仍是整个涉虚拟货币行业的主要威胁，2021年诈骗事件造成损失同比增长388%。

## 5.2 2021年虚拟货币安全事件统计分析

2021年，随着各主要国家加大投入引进针对虚拟货币的监管、追踪工具和技术，例如，英美日韩等国各监管部门与区块链业界安全相关力量建立合作机制，获得技术支撑服务，涉及虚拟货币的欺诈案件的曝光量大幅增长，包括南非虚拟货币平台 Africrypt 创始人被曝携价值 36 亿美元 BTC 潜逃，韩国 V Global 虚拟货币交易所骗取受害者 34 亿美元，土耳其虚拟货币交易所 Thodex 创始人携价值大约 20 亿美元的用户虚拟货币跑路，虚拟货币「庞氏骗

局」Finiko 被曝筹集价值超 15 亿美元的比特币。

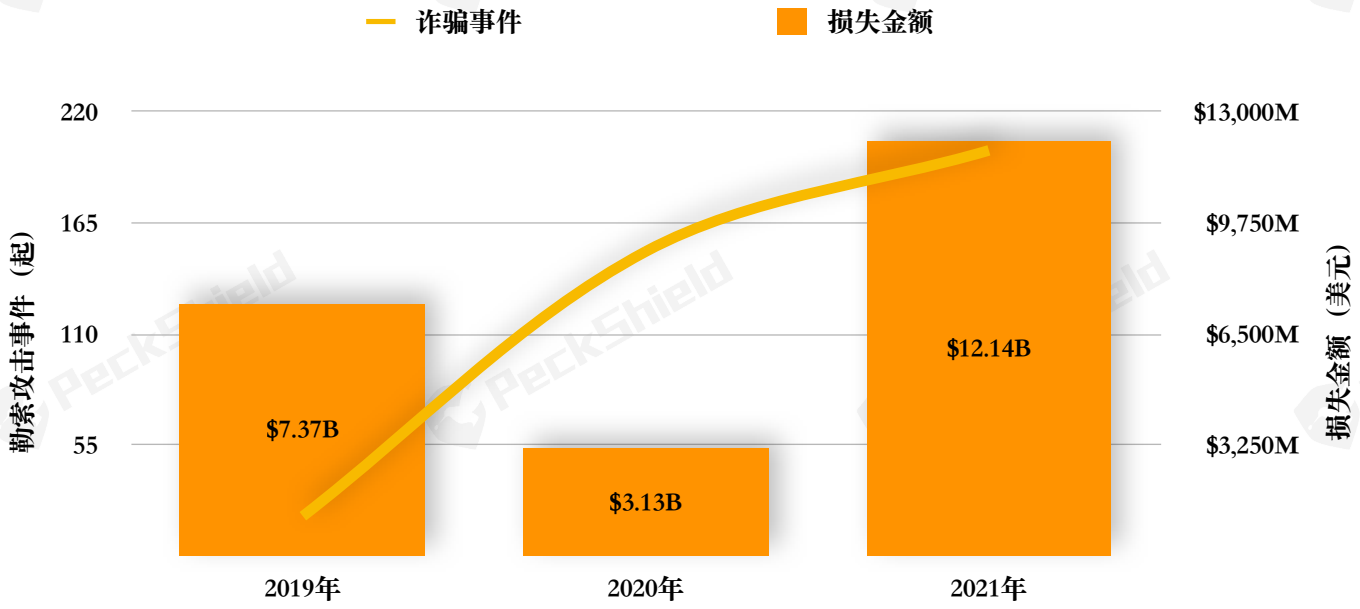



图28 近三年虚拟货币诈骗类事件统计

此外，我国监管机构联合银行和第三方支付机构，从交易场景识别——切断交易资金支付链路——分析虚拟货币交易特征的全链路监控模型入手，加大技术投入，打通虚拟货币的上下游监控，使得涉及虚拟货币的欺诈、洗钱案件曝光量大幅增长。例如，遵义警方打掉利用虚拟货币涉案金额 8 亿元（约合 1.33 亿美元）的“洗钱”团伙，徐州警方破获 BBGO 虚拟货币传销案，并扣押价值约 4.5 亿元（约合 7,500 万美元）的虚拟货币。

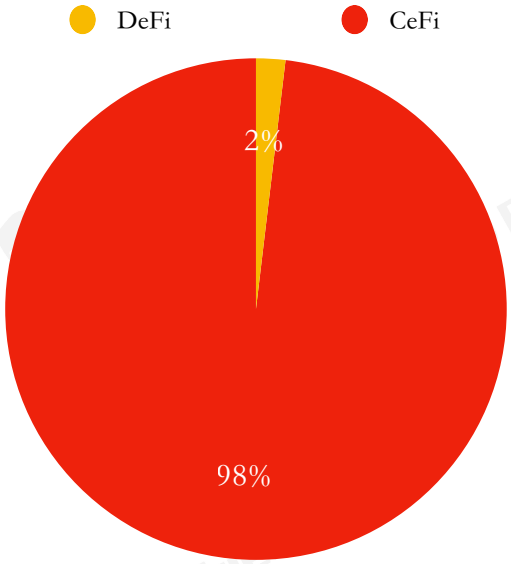



图29 DeFi vs. CeFi RugPulls & Scams 占比

除了延续以往利用虚拟货币「暴富神话」炮制的骗局，2021年下半年还出现了结合当下的时髦热门元素，例如「热门IP」、「Meme」，以及新兴概念，例如「NFT」、「GameFi」、「DeFi」和虚拟货币进行炒作，在短时间内通过操纵市场的"割韭菜"行为。

以高收益、高回报吸收资金的 CeFi「传统骗局」占比居高不下，造成损失占比达到98%，涉及 DeFi 的欺诈事件所造成的损失占比仅为 2%。仅土耳其虚拟货币交易所 Thodex，单笔就卷走了价值 20 亿美元的虚拟货币。

虽然 DeFi 领域涉及 RugPulls & Scams 占比小，但这也给市场敲响警钟，即在技术发展的过程中，需要引进创新的监控和风控等安全措施来确保 DeFi 生态安全稳定运行，同时，公众需要提高安全意识，经受住诱惑，保护好钱包，不参与任何形式的炒作活动。

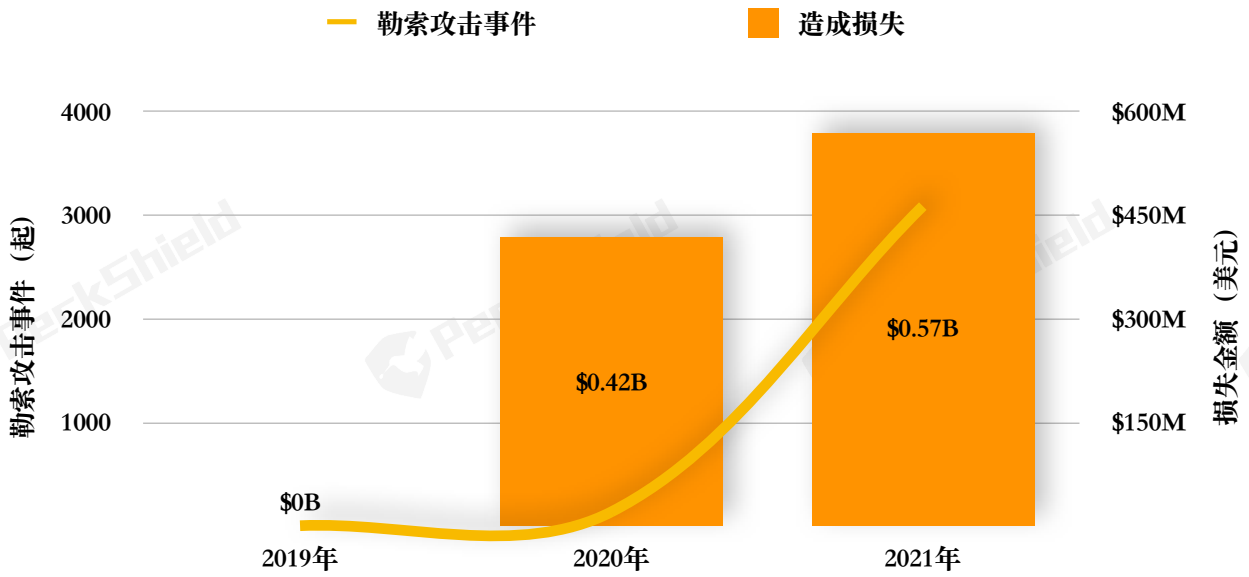



图30 近三年年虚拟货币勒索类安全事件统计

如图30所示，2021年虚拟货币勒索病毒的规模和攻击频率进一步扩大。值得注意的是，由于绝大多数遭遇勒索的企业担心损害企业的形象和名誉，在遭到大面积勒索攻击后，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能够被及时曝光，其他遭到勒索软件攻击的企业都未纳入统计，勒索集团真实所得远超统计的数据。此外，勒索软件对国家基础设施的攻击，造成例如政府、医院、学校等瘫痪的损失无法用经济损失来估算。

勒索软件团伙呈现出集团模式，形成完整的「勒索即服务」（RaaS）产业链，开发者向下家提供作案工具和方法，然后抽成获利。勒索集团利用虚拟货币的匿名性和跨国性，以小击大，通过相互合作、更换「马甲」来混淆视听，并且有组织、有预谋地针对国家重要枢

纽、重要基础设施进行定向攻击。例如，今年美国最大的燃油管道 Colonial Pipeline 遭到勒索软件攻击导致输油管线关闭、肉类加工商 JBS 遭勒索软件攻击导致肉制品生产线关停。

利用区块链的公开可查性，我们发现，勒索集团在得手后，主要将所获虚拟货币转移到主流虚拟货币交易所、KYC 宽松甚至没有 KYC 的虚拟货币交易所或混币器进行洗钱和套现，且在洗钱的过程中，由主要成员掌管所获虚拟资产，待到套现后再按比例进行进一步分赃。

此外，自2020年起，双重或多重勒索成为勒索软件攻击的一种趋势，勒索者通过威胁目标机构或企业泄露其网络中窃取的数据，向目标机构或企业施压迫使他们支付赎金。如果目标机构或企业没有在规定时间内缴纳赎金，他们将把所盗数据上传到暗网上，当中包括一些敏感信息，例如目标机构或企业的重要客户数据等，且赎金会定时增加。迫于这种压力，近年来，愈来愈多机构或企业选择缴纳高额赎金。

监管的收紧促使网络罪犯利用虚拟货币衍生出新的洗钱形态，它们被称为「嵌套交易所」，而且这种寄生于主流交易所的「嵌套交易所」在短时内扩张，愈来愈受到全球洗钱者的青睐。

据美国财政部外国资产控制办公室 （OFAC） 披露，自2018年以来，受其制裁的「嵌套交易所」Suex 协助勒索软件参与者、诈骗者和暗网市场运营商转移了数以亿计的虚拟货币。在其大型交易所托管的存款地址中，近 1,300 万美元来自 Ryuk、Conti、Maze 等勒索软件运营商，超过 2,400 万美元来自虚拟货币庞氏骗局运营商 Finiko，超过 2,000 万美元来自暗网 Hydra 市场。

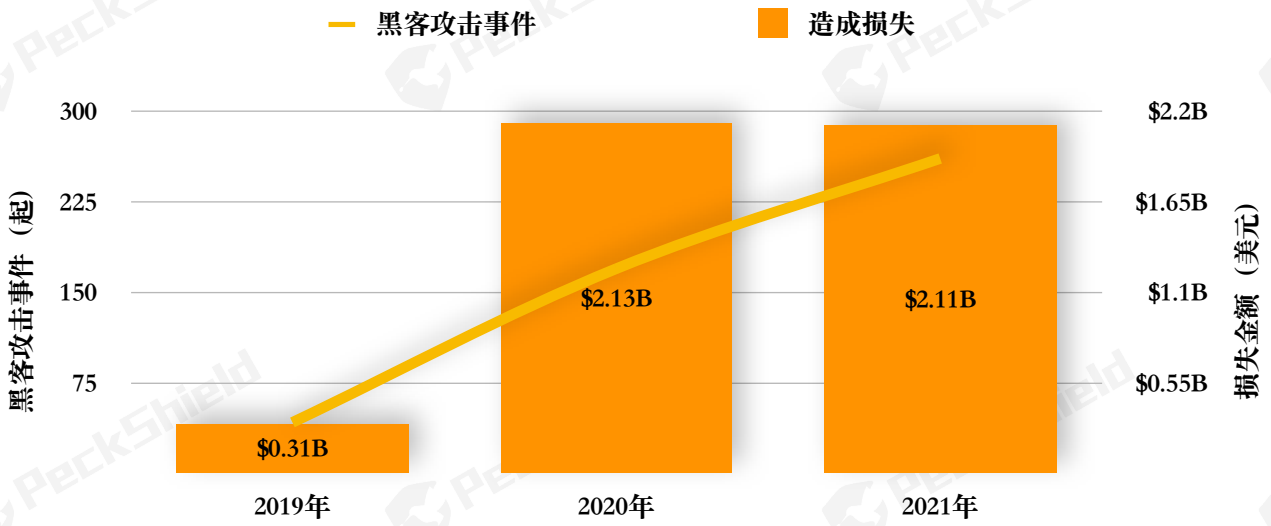



图31 近三年年黑客攻击类安全事件统计

如图31所示，2021年黑客攻击事件达到 261 起，同比增长 53%，是2019年的 6 倍，损失金额达到 21.1 亿美元。

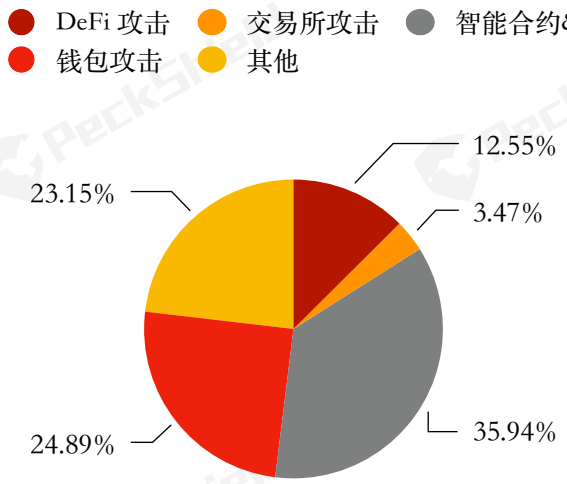



图32 2020年黑客攻击事件分类百分比

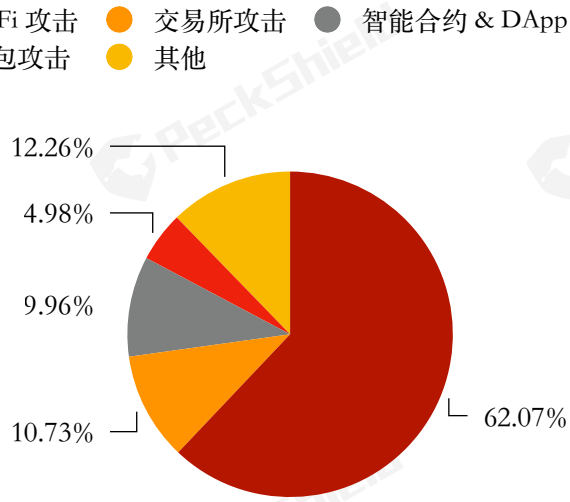



图33 2021年黑客攻击事件分类百分比

如图32和图33所示，从细分赛道来看，在2021年黑客攻击事件中，DeFi 安全事件占所有黑客攻击事件中损失的 60% 以上，达到 162 起，较2020年增长近 400%。涉及虚拟货币交易所的安全事件达到 28 起，较2020年增长了 280%，涉及智能合约的安全事件达到 26 起，数字钱包的安全事件达到 13 起，其他安全事件约 32 起。

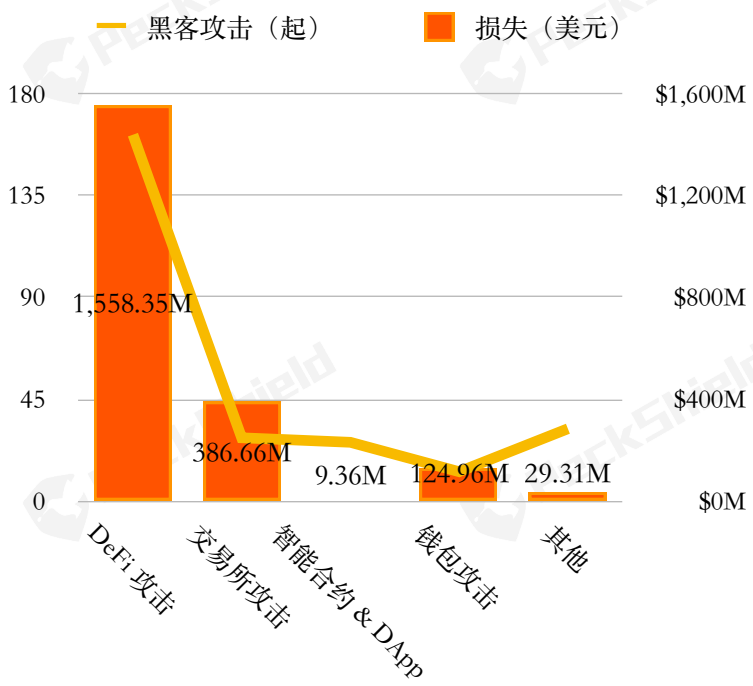



图34 2021年黑客攻击损失统计

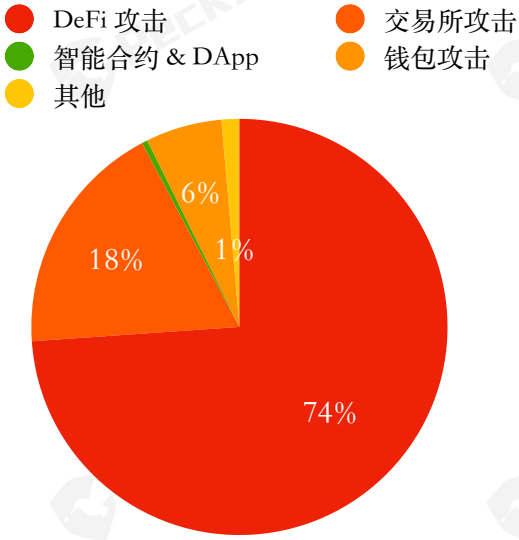



图35 2021年黑客攻击损失占比统计

如图34和图35所示，在2021年黑客攻击事件中，从损失数额上看，仍是 DeFi 安全事件位居榜首，损失达到 15.6 亿美元，占总损失近 74%，其次是交易所攻击，损失达到 3.86 亿美元。

2021年，DeFi 延续2020年的繁荣，在 BSC、Solona、Terra、Avalanche 和 Fantom 等诸多公链「烧钱营销」模式的推动下，锁在 DeFi 上的资金量愈来愈大，DeFi 迎来全面爆发，并向 DeFi 2.0 迈进。

此外，多链格局下各链的 DeFi 生态仍然相对独立，这就催生了打破链与链之间信息孤岛壁垒的跨链桥的兴起，随着跨链桥中储存的虚拟资产越来越多，继而越来越受各界的关注，包括攻击者、欺诈者，反映出 DeFi 市场在快速扩张的过程中安全环境仍十分脆弱。

频发的 DeFi 安全事件让开发者和社区开始关注 DeFi 安全。由于频繁遭遇攻击，一些社区从生态着手，注重生态安全的基础建设，引入 PeckShield「派盾」等可信赖的第三方机构的安全方案，对链上动态保持持续监控，筹划社区白帽赏金计划、建立 SAFU 基金或保险协议等等，但仍缺乏一定的风控熔断机制，特别是之前几起跨链协议安全事件，披露出跨链协议在对合约的查缺补漏和私钥管理及授权等方面的短板。

目前虚拟货币市场仍以中心化交易所（CEX）为主，经过近几年的发展，市场上涌现出愈来愈多的去中心化交易所（DEX），一些中心化交易所也在走向去中心化。

经过一年多的蓬勃发展，DEX 构建生态雏形，出现了以 Uniswap 为代表的现象级项目。相较于 CEX，DEX 拥有用户自主、数据透明、隐私保障、实时结算等优势，这也对 DEX 本身的技术安全提出更高的要求。

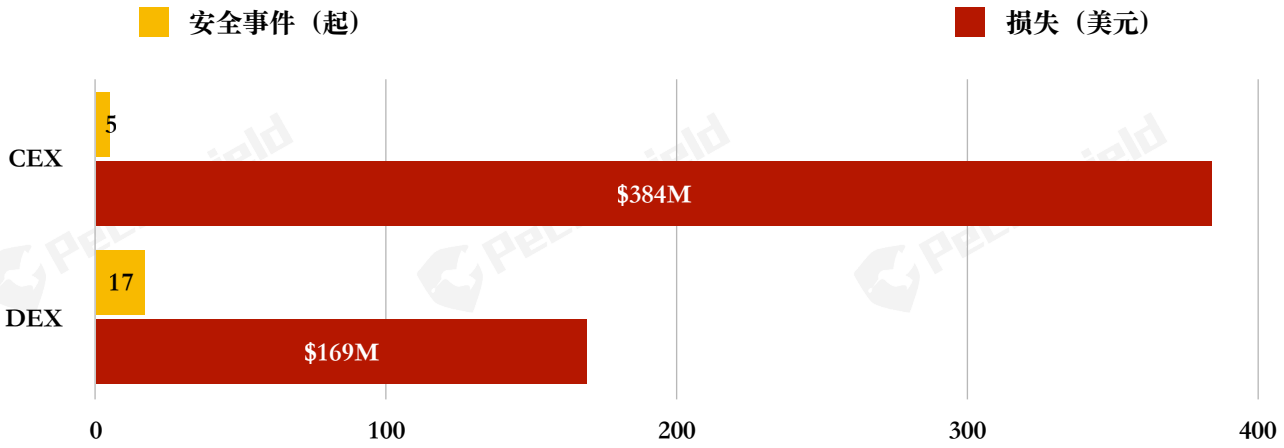



图36 DEX 和 CEX 安全事件数量和损失对比

据 PeckShield「派盾」统计，2021年共计发生 17 起针对 DEX 的重大安全事件，造成损失达到近 1.7 亿美元；针对 CEX 的重大攻击事件 5 起，造成损失达到 3.84 亿美元，是 DEX 损失的一倍。CEX 的安全隐患不容忽视，除却容易遭到黑客入侵，还存在信息、资金和私钥的存储和托管存在风险等问题。

8月19日，日本交易所 Liquid 热钱包中价值 9,000 多万美元虚拟资产被盗；8月29日，香港虚拟货币交易所 Bilaxy 热钱包被盗价值 2,100 多万美元的虚拟资产；12月5日，注册地在开曼群岛的虚拟货币交易所 BitMart 在以太坊和 BSC 上的热钱包私钥被盗，损失 1.96 亿美元；一周后（12月12日），AscendEX 热钱包中的 ERC-20、BSC 和 Polygon 代币在未经授权的情况下被转移，损失 7,700 万美元。

除了私钥管理薄弱，PeckShield「派盾」在分析、追踪近几起中心化交易所热钱包被盗的过程中发现，交易所的应急响应过于迟钝。一般来说，在热钱包出现多笔大额异动的间隙，如果交易所联动中心化或去中心化机构采取相关措施，就能在一定程度上减小损失，或者给追踪被盗资产留下足够的响应时间。如若待到攻击者掏空热钱包，将所盗资产转入 Tornado.Cash 等隐私服务或跨链到以太坊、去中心化协议中，再去应急响应的话就会处于被动，这也凸显出中心化交易所亟需引入私钥异动监控、潜在风险动态探测等机制。

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在数量和损失上逐年增长，但呈现出增速放缓的趋势。2021年，黑客对虚拟货币的攻击已造成 21.4 亿美元的损失。其中 DeFi 领域的安全事件占比达到 60% 以上，除了对各公链生态的攻击，还涌现了对跨链桥的攻击，以及用最原始的方式盗取去中心化协议中的资金的案例。

### 6.1.1 Log4j2 漏洞爆发 被勒索、挖矿、僵尸网络广泛利用

Apache Log4j2 是一个 Java 的日志库，可用于控制日志信息的级别和日志生成过程。12月10日，Apache Log4j2 被曝出 JNDI 注入漏洞（CVE-2021-44228），攻击者可通过向目标服务器发送特定 JNDI 链接，来触发漏洞并在目标机器上执行任意代码，影响面和破坏力极大。

12月10日凌晨0点左右，攻击者利用 Log4j2 漏洞，对荷兰、中国、德国、美国、奥地利等国家发起猛烈攻击。对此，新西兰计算机紧急响应中心（CERT）、美国国家安全局、德国电信 CERT、中国国家互联网应急中心（CERT/CC）等多国机构相继发出警告。

12月11日10点25分， Mirai 家族利用 Apache Log4j2 漏洞进行样本传播。随后10点58分，Muhstik 家族也开始利用此漏洞进行传播。同时，Minerd、LifeCalendarWorm、HSMiner、BigWolf、SnakeMiner、HideShadowMiner、BlueHero 等数十个挖矿病毒家族也开始利用该漏洞攻击数字货币挖矿活动。

12月12日下午5点到12月12日下午7点期间，勒索家族 Tellyouthepass 使用 log4j2 漏洞对某 OA 系统和某开源项目发起上千次起攻击，并开价 0.05 比特币（约合 2,579 美元）。

### 6.1.1 DeFi 史诗级安全事件

8月10日，异构跨链协议 Poly Network 遭到攻击，损失达到 6.1 亿美元，包含 2,857 ETH、9,630万 USDC、26,000 WETH、1,000 WBTC、3,340万 USDT、2,590亿 SHIB、14 renBTC、673,000 DAI和 43,000 UNI 转至以太坊，6,600 BNB、8,760万 USDC、26,600 ETH、1,000BTCb、3,210万 BUSD 转至BSC，8,500万 USDC 转至 Polygon。

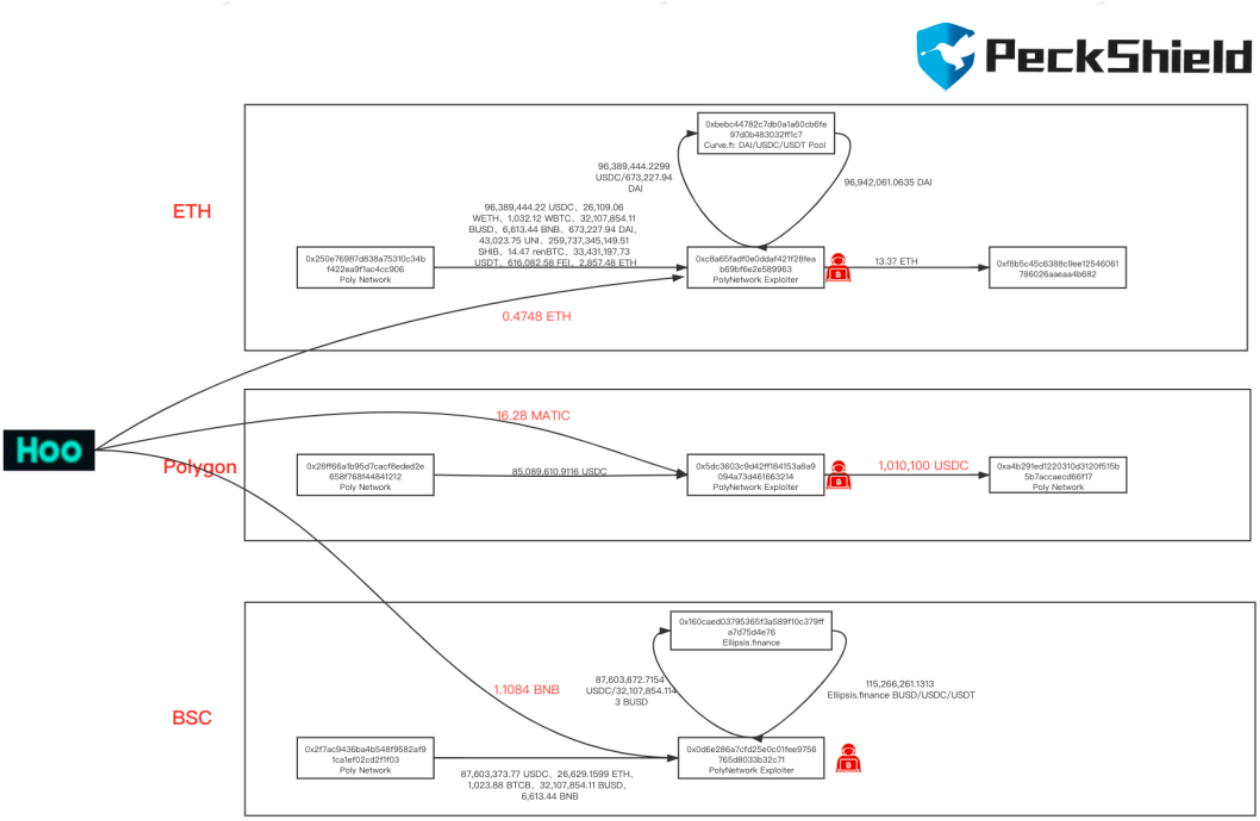



图37 Poly Network 安全事件资金流转

PeckShield「派盾」分析显示，Poly Network 中有一特权合约 EthCrossChainManager，此合约主要用于触发来自其他链的信息。

在跨链交易中，任何人都可调用 verifyHeaderAndExecuteTx 来执行跨链交易，这个函数主要有三个作用：一是通过检验签名来验证区块头是否正确，二是利用默克尔树来验证交易是否包含在该区块中，三是调用目标合约。

此次攻击事件源于 Poly Network 允许调用目标合约，但在此过程中没有限制用户调用 EthCrossChainData 合约，该合约可追踪来自其他链上数据的公钥列表，即便在没有盗取公钥的情况下，如果你已经获取了修改公钥列表的权限，那么只需要设置公钥来匹配自己的私钥，基本上就可以利用漏洞了。

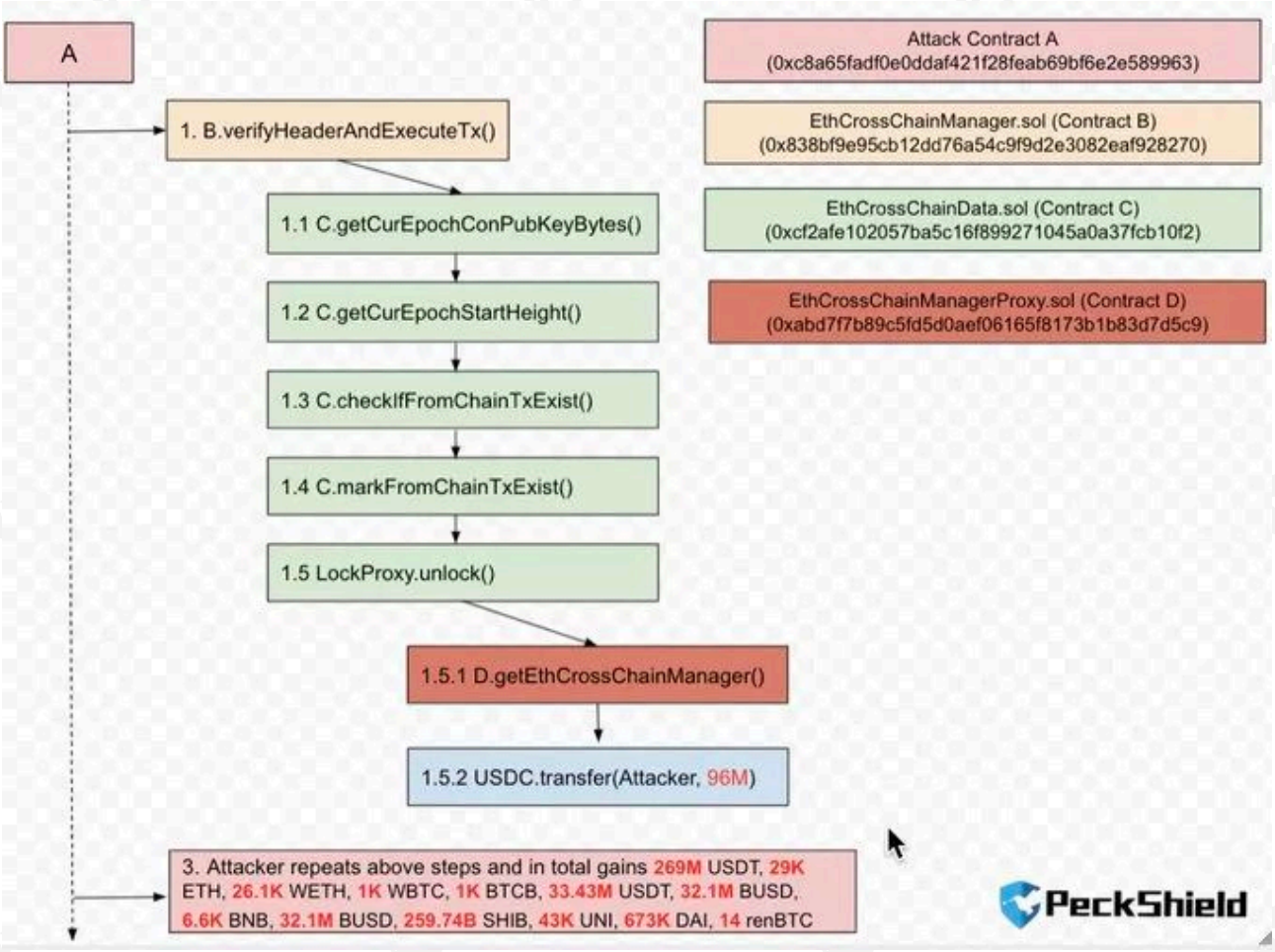


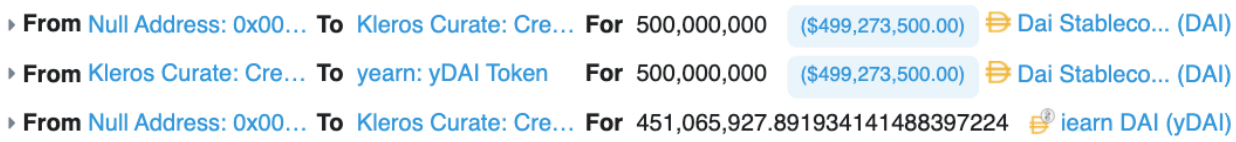

图38 Poly Network 安全事件攻击流程

由于用户可通过发送跨链请求欺骗 EthCrossChainManager 合约调用 EthCrossChainData 合约，来蒙混 onlyOwner 的检验，此时，用户只需要杜撰一个正确的数据就能触发修改公钥的函数。

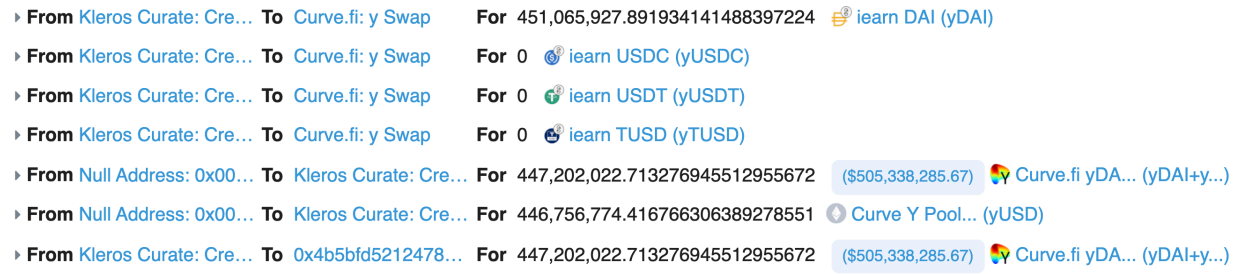
结合以上分析，攻击者只需在其他链正常发起跨链操作的交易，发起此笔交易的目的是为了调用 EthCrossChainData 合约中的 putCurEpochConPubKeyBytes 函数来修改 Keeper 角色。随后通过正常的跨链流程，Keeper 会解析用户请求的目标合约以及调用参数，构造出一个新的交易提交到以太坊上。这表面上看起来也只是一笔正常的跨链操作，因此可以直接通过 Keeper 检查与默克尔根检查。最后成功执行修改 Keeper 的操作，达到入侵的目的。

### 6.1.2 Cream Finance 被黑 1.3 亿美元安全事件

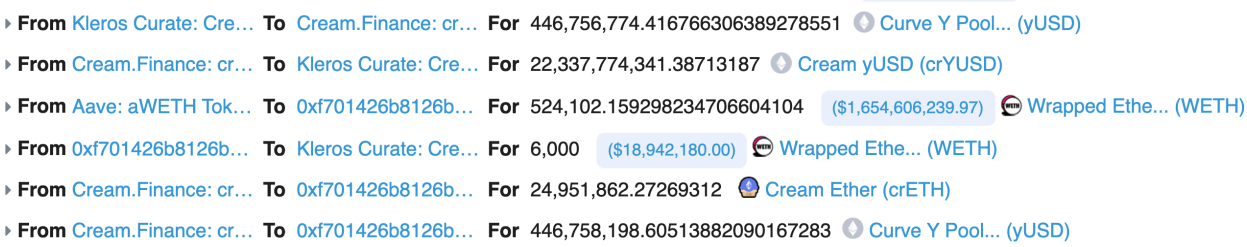
2021年10月，Cream Finance 协议遭到黑客入侵，损失大约有 1.3 亿美元。



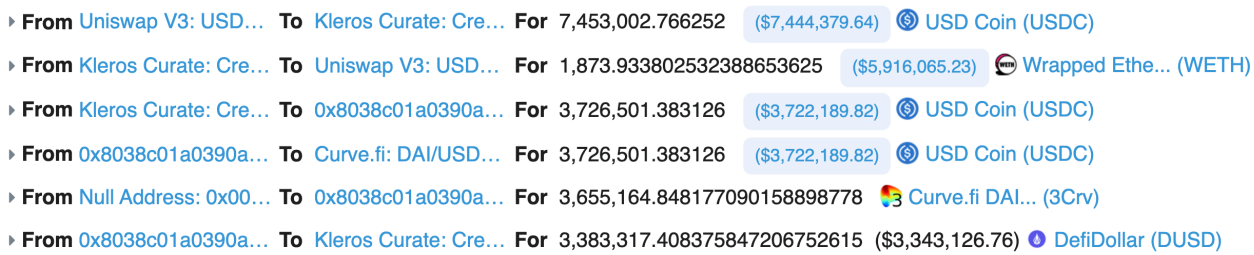

攻击者从 MakerDAO 通过闪电贷借出价值 5 亿美元的稳定币 DAI，将其抵押至 Yearn 的 yDAI 池中，获得 4.5 亿枚 yDAI 凭证。




随后攻击者将获得的 yDAI 代币存入 Curve 的 yDAI/yUSDC/yUSDT/yTUSD 池子中添加流动性，以获得相应的流动性凭证。紧接着攻击者将获得的凭证抵押到 yUSD 池子中以获得 yUSD 凭证，为后续在 Cream crYUSD 借贷池中进行抵押做准备。




攻击者开始向 Cream 的 crYUSD 借贷池中抵押其获得 yUSD 凭证，为了扩大其抵押规模，攻击者又从 Aave 通过闪电贷借出约 52.4 万枚 WETH，并将这些 WETH 抵押到 Cream 的 crETH 池子中。



攻击者在 Uniswap V3 中将约 1,873 枚 ETH 兑换成约 745 万枚 USDC，并通过 Curve 3Pool 将其兑换成约 338 万枚 DUSD 代币。

From Kleros Curate: Cre... To Null Address: 0x00... For 3,383,317.408375847206752615 ($3,343,126.76) DefiDollar (DUSD)
From 0xa89bd606d5dad... To Kleros Curate: Cre... For 3,022,172.845916671953865487 Curve Y Pool... (yUSD)
From 0xd802a8351a76e... To Null Address: 0x00... For 3,026,610.42212333714053228 Curve.fi yDA... (cvxyDA...)
From Curve.fi: yCrv Gauge To Convex Finance: V... For 3,026,610.42212333714053228 ($3,420,069.78) Curve.fi yDA... (yDAI+y...)
From Convex Finance: V... To Convex Finance: ... For 3,026,610.42212333714053228 ($3,420,069.78) Curve.fi yDA... (yDAI+y...)
From Convex Finance: ... To 0xa5189cb014976... For 3,026,610.42212333714053228 ($3,420,069.78) Curve.fi yDA... (yDAI+y...)
From 0xa5189cb014976... To 0x4b5bfd5212478... For 3,026,610.42212333714053228 ($3,420,069.78) Curve.fi yDA... (yDAI+y...)
From Kleros Curate: Cre... To Null Address: 0x00... For 449,780,371.451055492855538317 Curve Y Pool... (yUSD)
From 0x4b5bfd5212478... To Kleros Curate: Cre... For 450,228,633.135400282653487952 ($508,758,355.44) Curve.fi yDA... (yDAI+y...)

接下来攻击者通过获得的 DUSD 代币从 YVaultPeak 中赎回 yDAI/yUSDC/yUSDT/yTUSD 4Pool 凭证，并利用此凭证从 yUSD 池子中取回 yDAI/yUSDC/yUSDT/yTUSD 代币。

From 0x4b5bfd5212478... To Kleros Curate: Cre... For 450,228,633.135400282653487952 ($508,758,355.44) Curve.fi yDA... (yDAI+y...)
From Kleros Curate: Cre... To 0x4b5bfd5212478... For 8,431,514.81679698041016119 ($9,527,611.74) Curve.fi yDA... (yDAI+y...)

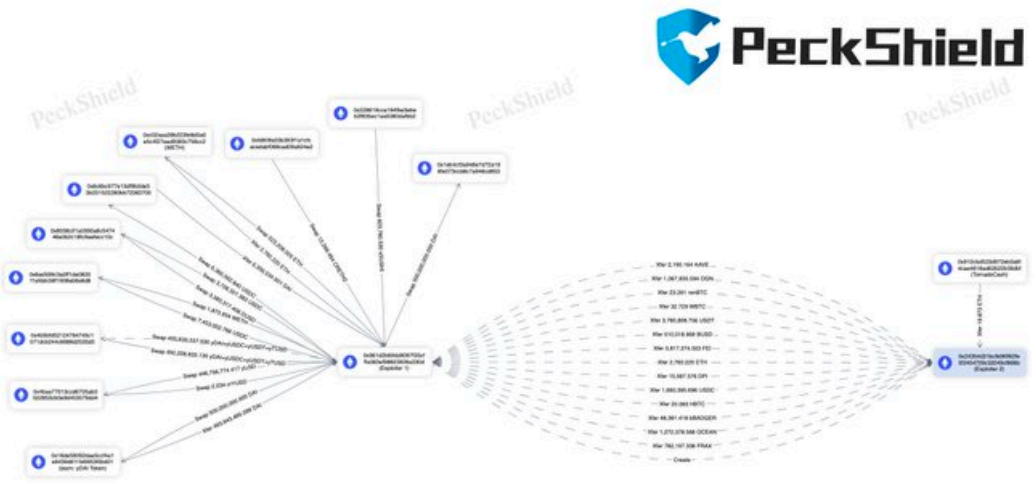
随后攻击者开始将约 843 万枚 yDAI/yUSDC/yUSDT/yTUSD 代币直接转到 yUSD 池子中，由于这些代币不是通过正常抵押操作进行抵押的，所以这 843 万枚 yDAI/yUSDC/yUSDT/yTUSD 代币并没有被单独记账，而是直接分配给了 yDAI/yUSDC/yUSDT/yTUSD 凭证的持有者，这相当于拉高了价格。

From Cream.Finance: cr... To Kleros Curate: Cre... For 12,266.463816009145730493 Cream ETH 2 (CRETH2)
From Cream.Finance: cr... To Kleros Curate: Cre... For 623,760.529988486822779519 ($4,909,170.79) SushiBar (xSUSHI)
From Cream.Finance: cr... To Kleros Curate: Cre... For 135,402.94454130151708413 ($7,123,077.66) Wrapped NXM (wNXM)
From Cream.Finance: cr... To Kleros Curate: Cre... For 447,222.593590652214743874 ($3,672,274.24) Perpetual (PERP)
From Cream.Finance: cr... To Kleros Curate: Cre... For 418,917.294792442850457949 ($2,438,001.55) THORChain ET... (RUNE)
From Cream.Finance: cr... To Kleros Curate: Cre... For 15,567.575750097560251951 ($3,791,974.43) DefiPulse In... (DPI)
From Cream.Finance: cr... To Kleros Curate: Cre... For 156,629.158238930877722356 ($2,657,996.82) Uniswap (UNI)
From Cream.Finance: cr... To Kleros Curate: Cre... For 4,324,457.1528 ($4,319,453.76) USD Coin (USDC)
From Cream.Finance: cr... To Kleros Curate: Cre... For 3,817,374.503105485458327683 ($3,808,911.38) Fei USD (FEI)
From Cream.Finance: cr... To Kleros Curate: Cre... For 3,780,808.755759 ($3,769,757.45) Tether USD (USDT)

在 crToken 中由于其抵押物价格被恶意拉高了，因此攻击者抵押的大量 yUSD 可以使其借出更多的资金，最后攻击者将 Cream 的其他 15 个池子全部借空。

From Kleros Curate: Cre... To 0x1eb4cf3a948e7... For 500,000,000 ($499,273,500.00) Dai Stableco... (DAI)
From 0x1eb4cf3a948e7... To Null Address: 0x00... For 500,000,000 ($499,273,500.00) Dai Stableco... (DAI)

最后攻击者在借空其他池子后归还了闪电贷。



完成攻击后，攻击者将资金转入 Tornado Cash。此后，攻击者使用了 renBridge 将 BTC 资金发送到了比特币网络，并向 Uniswap 的 ETH-CRETH2 池子添加了超过 4000 万美元的 CRETH2 流动性。

### 6.1.3 中心化和去中心化生态因私钥被盗损失至少 8 亿美元

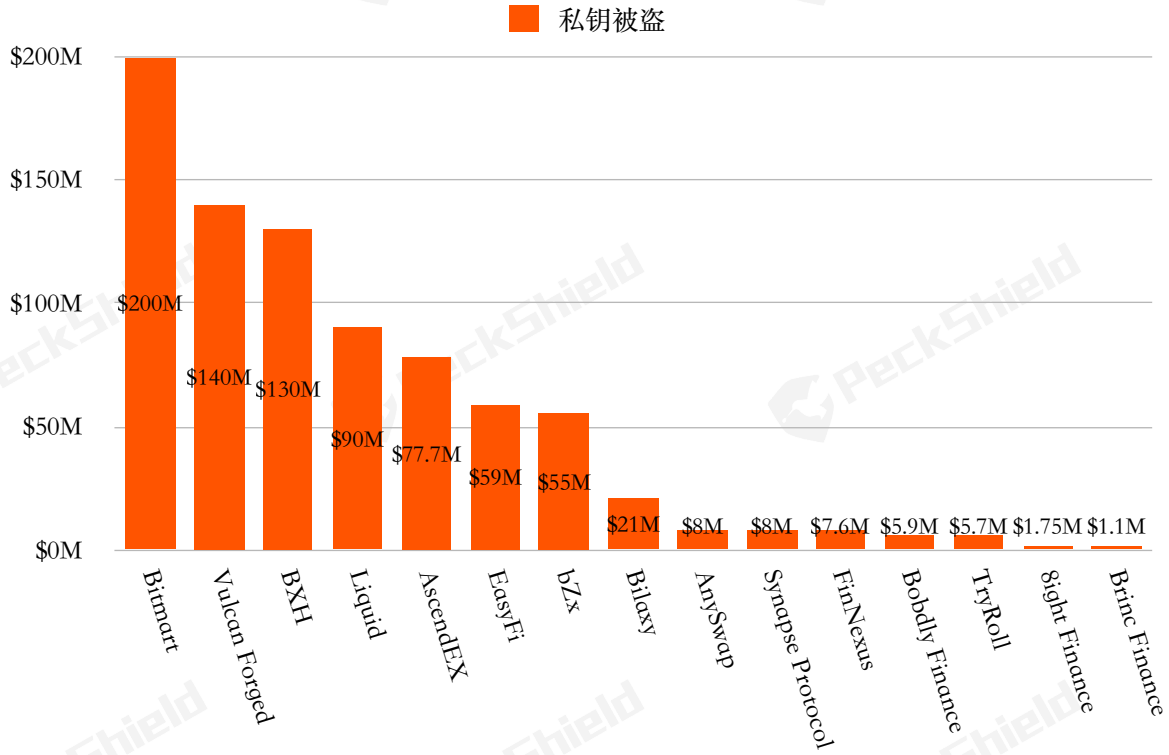



图39 CeFi vs. DeFi 因私钥被盗造成损失的安全事件统计

PeckShield「派盾」数据显示，2021年在中心化和去中心化生态因私钥被盗造成损失 100 万美元及以上的安全事件共计 15 起，损失总计逾 8 亿美元，其中单笔造成损失 1 亿美元的安全事件 3 起，单笔造成损失 5,000 万元的安全事件 7 起。

从占比来看，中心化交易所因私钥被盗发生的安全事件仅 4 起，但造成损失占比达到 80%，去中心化机构因私钥被盗发生的安全事件频率较中心化机构要高。

密钥管理引入的运营风险仍集中在中心化机构上，这就要求中心化机构切勿放松对密钥的权限管理以及加强对风控的管理，也凸显出目前仍处于半中心化治理的 DeFi 领域在风控管理方面出现亟待解决的空白。

12月5日，PeckShield「派盾」首个发现，注册地在开曼群岛的虚拟货币交易所 BitMart 热钱包发生异动，疑似在以太坊和 BSC 上的热钱包私钥被盗，损失近 2 亿美元。

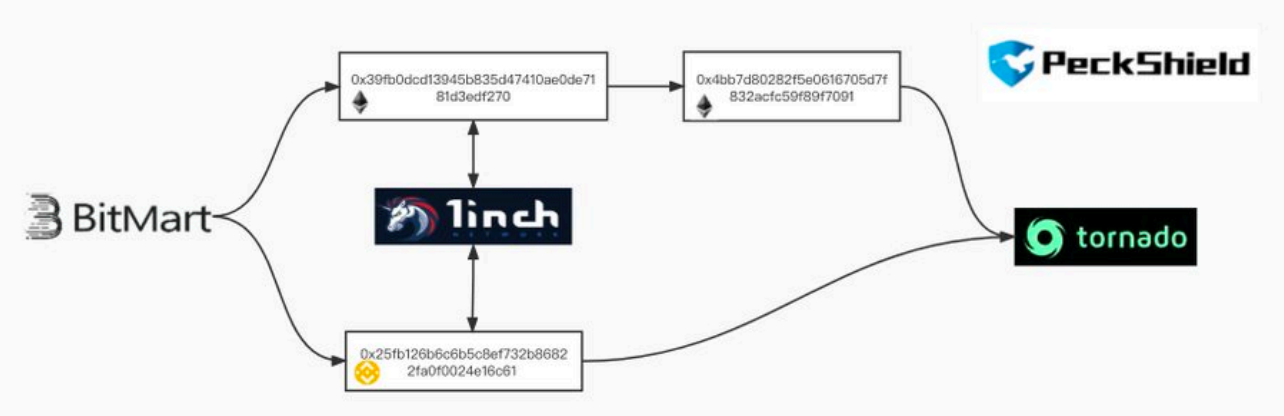



图40 BitMart 安全事件资金流转

得手后，攻击者通过 DEX 1inch 将币卖成 ETH，并发送至 TornadoCash 进行混币。

### 6.1.4 Badger DAO 前端遭攻击，损失达 1.2 亿美元

12月2日，Badger DAO 协议因前端漏洞被盗走价值 1.2 亿美元的虚拟资产，巨额损失使其成为2021年造成损失第五大的安全事件（包含 Poly Network 在内）。

据 PeckShield「派盾」统计，其中损失最大的一笔资金包含 900 枚 BTC（比特币），价值逾 5,000 万美元。

利用前端的漏洞，攻击者植入劫持病毒，当用户无限授权后，攻击者就可以通过调用函数 increaseAllowance() 转走用户钱包中的虚拟资产。

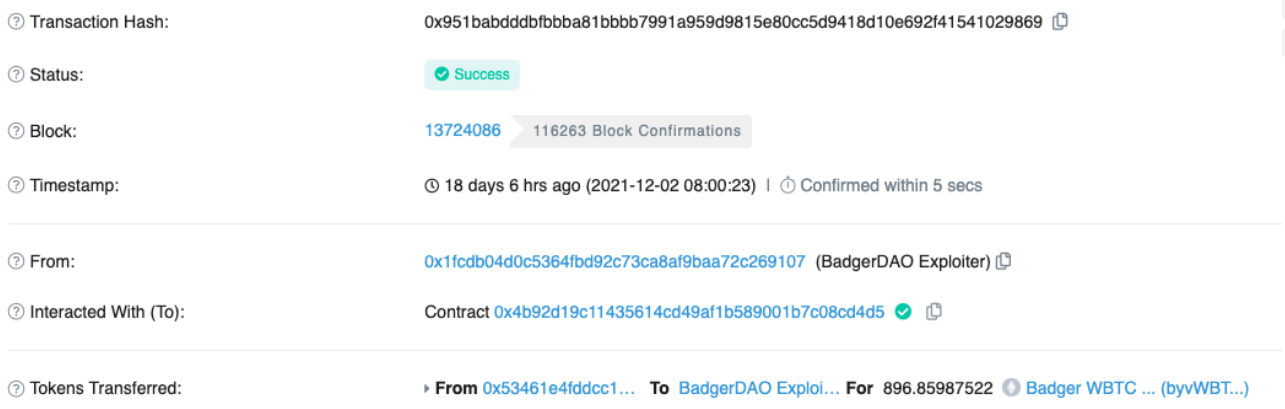



图41 Badger DAO 安全事件中单笔转账超过 900 BTC 转账记录

PeckShield「派盾」在追踪 RugPulls & Scams 中也发现，多起用户被盗安全事件主要源于用户对协议的无限授权。

PeckShield「派盾」提示用户参与 DeFi 时，最好只授权可信任的合约，如果仅是体验新的 DeFi 协议或对 DeFi 协议存疑，需要把风险控制在自己能够承担的范围之内；还需要定期撤回、整理授权。

## 6.2 诈骗类犯罪案例

### 6.2.1 借《鱿鱼游戏》IP 炒 虚拟货币 暴涨数万倍后瞬间归零

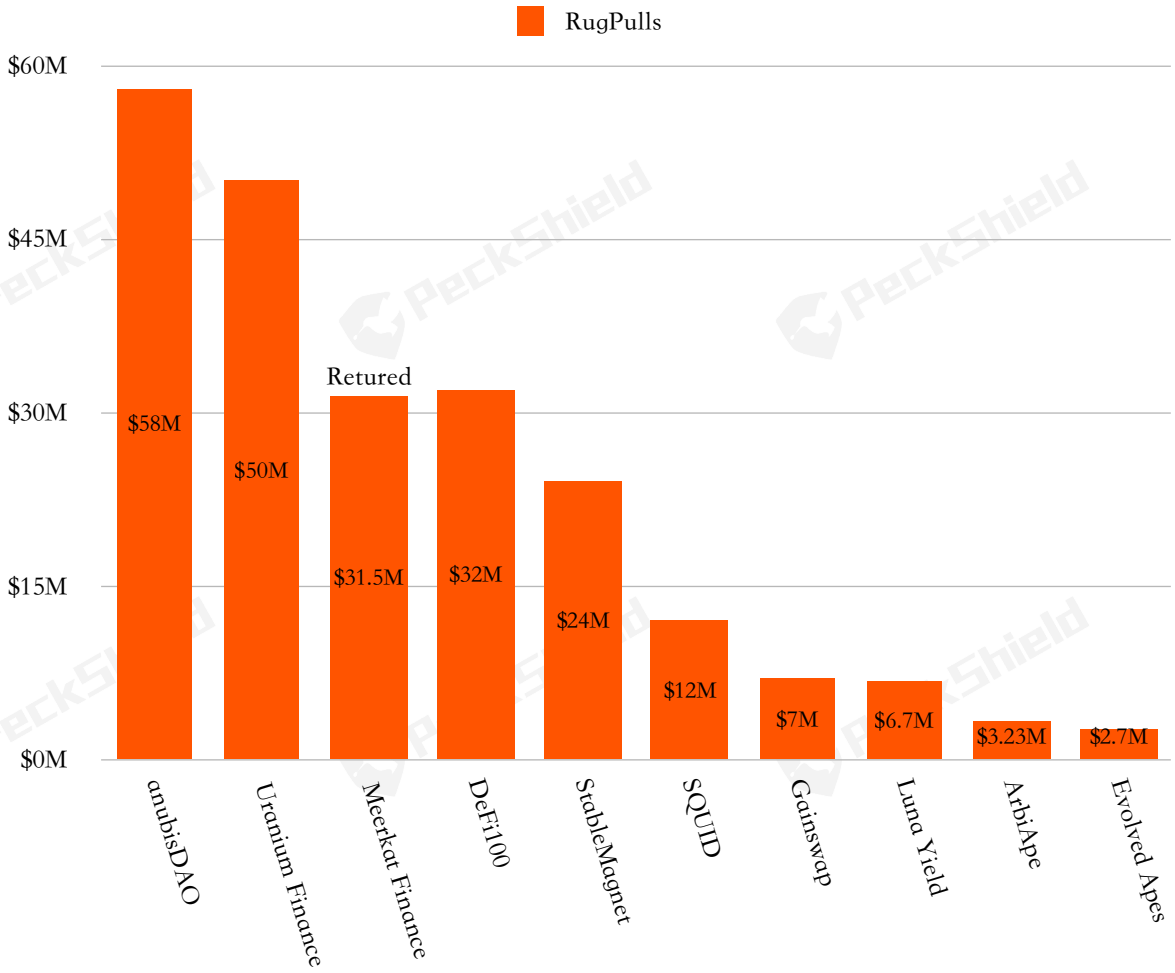



图42 2021年 DeFi 领域 Top10 RugPulls & Scams 统计

PeckShield「派盾」数据显示，2021年 DeFi 领域发生 RugPulls & Scams 造成损失 100 万美元 及以上的安全事件共计 18 起，损失总计逾 2.4 亿美元（包含 StableMagnet 已退还的 2,400 万美元）。

RugPull 分为 Hard RugPull 和 Soft RugPull，Hard RugPull 一般指我们在上文所述的 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，由于 Token 极速下跌，用户手中的 Token 的价值趋于归零；Soft RugPull 较 Hard RugPull 更加难以辨别，前期 DeFi 协议的开发团队花费大量时间建立口碑、信任，例如，在流动性池子上时间锁，或将开发团队的 LP Tokens 发送至销毁地址。一般情况下，开发团队会创建多个钱包地址，当 Token 的价格上涨后就会偷偷地抛售储存在未公开的钱包地址中的 Token，以此牟利。


图43“鱿鱼币”（SQUID）短时归零

11月备受瞩目的「鱿鱼币」崩盘就是一起典型的 Hard RugPull 事件。美东时间11月1日9时35分，鱿鱼币从 0.15 美元短线暴涨突破 2,850 美元后，在短短几分钟内突然暴跌至近乎归零，跌幅超过 99%。奈飞（Netflix）出品的韩国网剧《鱿鱼游戏》风靡全球，催生出以该 IP 命名的 Meme 币 —“鱿鱼币”（SQUID）。有投资者表示：「买进就开始跌，来不及反应，直接跌到几分钱。」

自2021年起，以「动物币」为首的 Meme 币成为虚拟货币市场的一个热门类别，这些 Token 基于网络社交环境下的段子、讽刺、热门，甚至名人效应而创建。由于价格低，涨幅大，Meme 币在短时间内吸引了资金体量较小的用户入局，其中不乏掺杂抓住投资者以小博大的心态的欺诈者。鱿鱼币就是典型的 Meme 币之一。

鱿鱼币项目的白皮书显示，该项目是BSC公链上的一个虚拟货币游戏赚取平台，灵感来源于奈飞同名韩国热播剧。该币种于10月20日开始预售，1 秒内全部售罄。

鱿鱼币创始人曾在媒体报道中表示，该项目是奈飞的官方代币合作伙伴。并与虚拟货币平台 CoinGecko 建立了战略合作关系，但遭到 CoinGecko 联合创始人 Bobby Ong 否认。

据报道，在「鱿鱼游戏」崩盘的前几天，曾有投资者抱怨，他们无法在唯一可交易 Token 的去中心化交易所（DEX）Pancakeswap 上出售持有的鱿鱼币。随后，鱿鱼币创始人解释称，因为该项目部署了一种创新的「反倾销技术」，即限制人们在需求下降时出售代币。

随着「去中心化」在短期内的爆发，去中心化平台免除了繁杂的上币手续和昂贵的上币费，甚至免除了认证和审核的通道，这极大地降低了欺诈者的成本和发币门槛，致使 DeFi 领域涌现出新型的欺诈模式，欺诈者利用。

随着狗狗币、屎币此类依赖名人喊单在获得惊人暴涨的「叙事」虚拟货币成为币圈「暴富」传说后，此类利用「叙事」取得成功的虚拟货币越来越多，鱿鱼币就是其中一种利用《鱿鱼游戏》影视剧在全球的热度和虚拟货币市场的炒作，取得了「叙事」上的成功，在传播上获得了深远的影响力，相较于其他诈骗项目吸引了更多的投资者入场，最后导致被收割。

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，骗局横生的虚拟货币领域，需要做的就是时刻提高警惕。

### 6.2.2 一键授权 钱包被无形中掏空

9月10日，多名用户发现其钱包账户意外收获数十万枚名为 Zepe 的代币。获得意外之财的用户打开代币的关联网站并授权自己的钱包，不料储存在钱包中的虚拟资产全部被转走。 Zepe 对应合约未做代码验证，且所有授权与转账事务都执行失败，而所有执行失败的备注中都要求用户到对应网站进行提取，一旦用户登陆网站进行钱包授权，代币就会被盗。

这种空投骗局在2021年下半年频繁出现。诈骗者会先创建代币并完成空投，并添加代币到 DEX 中增加流动性，使代币具有价值。一些用户看到账户中出现了「有价值」的空投币后，就想去 DEX 进行兑换，而这一步的授权交易通常都会失败，但失败后会有 Error 提示用户去它的官网兑换，陷阱就在此时出现，当用户在指定页面授权交易后，其账户中的价值币就会被转走。

而设局者在得手后，往往会选择在去中心化交易所混币，并转移到其他地址进行套现。

PeckShield「派盾」在追踪中发现，类似的空投骗局有一个主要的共同特征，即代币名字大多是网站地址，如 ShibaDrop.io、AirStack.net、BNBw.me 等，当用户接收到类似的代币，就需要加以防范。

PeckShield「派盾」提示，用户在进行链上协议交互时不要过度授权，比如授权代币交易时可以设置指定数量而不要设置最大数量。同时，用户应定期对不常用的 Dapp 取消授权，并注意防范欺诈者「换马甲」。

### 6.2.3 CeFi RugPull 单笔卷走 20 亿美元

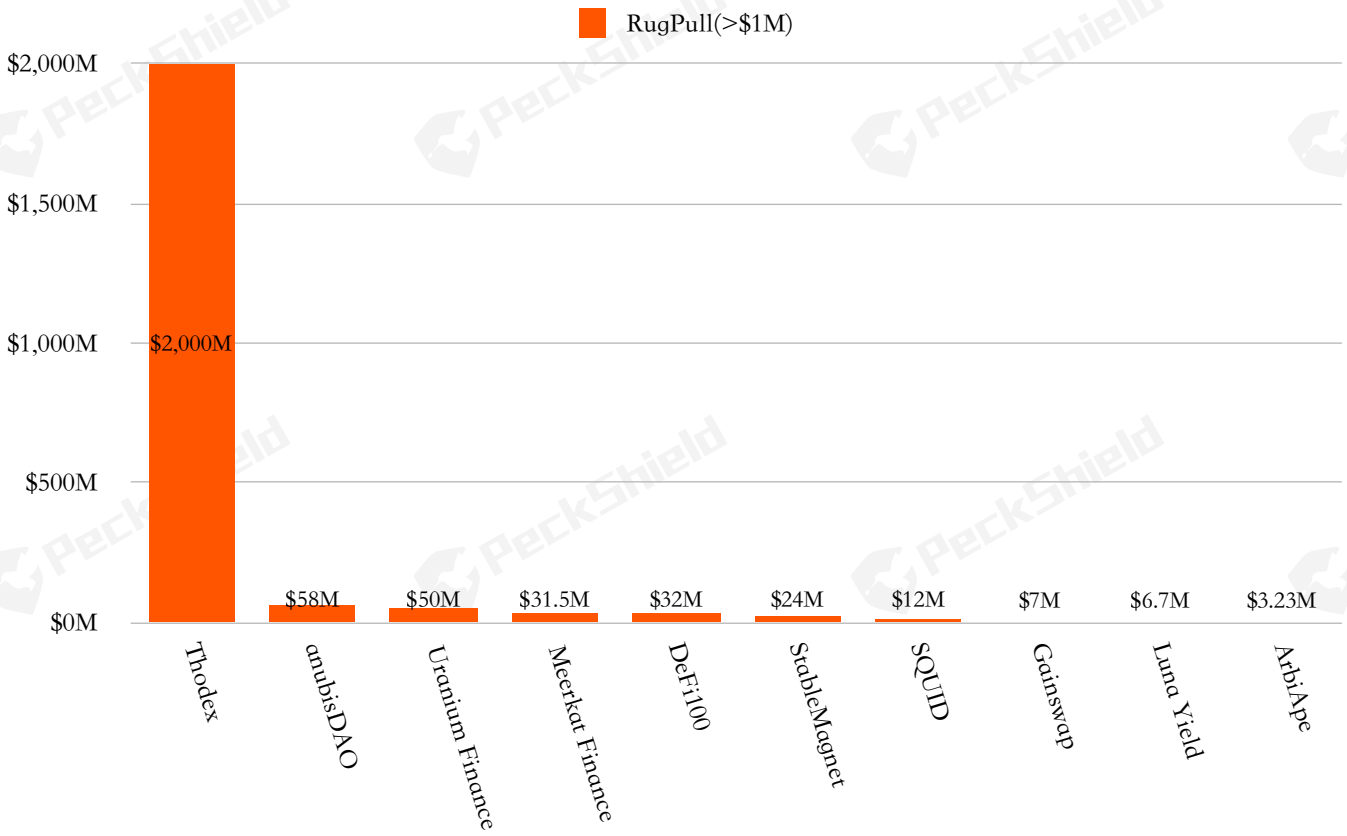



图44 2021年 RugPulls & Scams 造成损失 Top10 安全事件统计

4月25日，据土耳其多家媒体报道，名为 Thodex 的土耳其虚拟货币交易平台下线，其首席执行官（CEO）Faruk Fatih Ozer 卷走价值 20 亿美元的虚拟货币，目前仍在逃。

据称，就在 Faruk Fatih Ozer 携款跑路的前几天， Thodex 官方网站以投资估价为由宣布临时关闭 4 至 5 天。在此期间，用户反映无法提款，或登入账户，疑似交易所跑路。

对于外界质疑，Thodex 官网称将会披露投资机构和合作方，但直到整个流程结束，将暂停交易。

据 CoinmarketCap 数据显示，彼时， Thodex 最后一个交易日 24 小时交易量为 5.38 亿美元。

一名起诉 Faruk Fatih Ozer 的律师表示，Thodex 有 40 万名用户，其中 39 万为活跃用户。对此，Faruk Fatih Ozer 反驳称，仅 3 万用户受影响，卷走 20 亿美元的报道是失实报道。

土耳其政府已经下达拘捕令，逮捕 Faruk Fatih Ozer，警方已经在伊斯坦布尔等多座城市逮捕拘留与 Thodex 交易所相关的 60 余人。

据悉，由于土耳其通货膨胀率快速抬升和货币里拉贬值，大多数土耳其居民将购买虚拟货币视为资产保值的途径之一，致使大量资金涌入虚拟货币交易所。土耳其中央银行不久前宣布禁止使用虚拟货币购买货品和服务。土耳其总统雷杰普·塔伊普·埃尔多安曾呼吁对虚拟货币实施监管，警示虚拟货币市场可能出现「金字塔骗局」。

## 6.3 恐怖融资和政治渗透类犯罪案例

据外交部消息，10月7日，国务委员兼外长王毅在全球反恐论坛第十一次部长级会议上发言表示，在各国共同努力下，国际反恐合作取得显著成效，但恐怖势力剿而不灭，恐怖网络仍在蔓延。恐怖组织利用社交网络、加密通信、虚拟货币、人工智能等新兴技术从事恐怖活动，增加了防范和打击难度。

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」认为面对恐怖主义威胁，各相关监管部门要着力应对恐怖分子滥用网络和新兴技术、利用新兴技术打击恐怖融资多元化等新威胁新挑战，加强对反恐的重视程度，深化多国协调合作。

## 6.4 勒索攻击与洗钱犯罪案例

### 6.4.1 「嵌套交易所」协助黑灰产业洗白数亿美元虚拟资产

9月21日，美国财政部外国资产控制办公室（OFAC）宣布，根据 13694 号行政命令指定虚拟货币场外交易（OTC）经纪商 Suex。

Suex 是一家在捷克共和国合法注册的加密货币场外交易经纪商。然而，它在那里没有已

知的实体存在，而是在莫斯科和圣彼得堡以及俄罗斯及其周边地区和中东的其他地区开展业务。自2018年，Suex 已经协助黑灰产业转移价值数亿美元的虚拟货币，包括比特币、以太币和锚定美元的稳定币—泰达币（USDT）。单从比特币流水来看，Suex 在主流交易所，特别是需要 KYC 验证的交易所，托管的充值地址收到超过 1.6 亿美元的资金来自于勒索软件组织、诈骗者和暗网市场运营商。

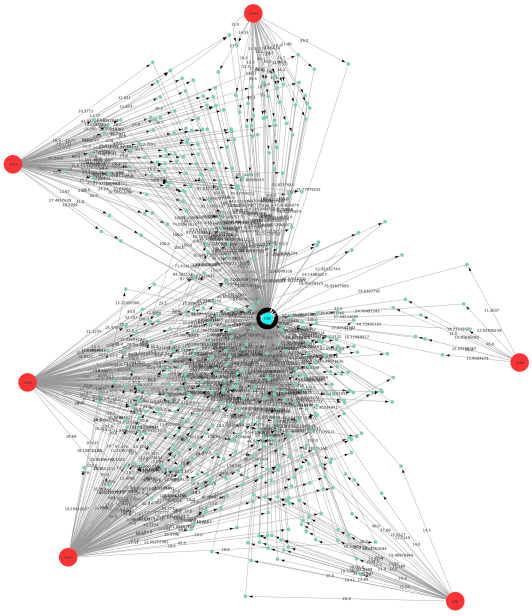


图45 Suex 交易轨迹

如同 Suex 这样的不需要 KYC 验证，注册地与实际运营地址不在同一个地方、寄生于主流交易所的虚拟货币场外交易 (OTC) 经纪商，又被称为嵌套交易所。

嵌套交易所，是类似于 Apple Pay/GooglePay 的平台。此类 OTC 经纪商的运营寄生于主流中心化交易所——类似于银行在 ApplePay 方面所扮演的角色。

首先，他们会在主流中心化交易所上开设账户，如果客户想将一种加密货币转换成另一种加密货币，或者兑现，那么他们就先通过 OTC 服务汇集虚拟货币，然后将所获虚拟货币在主流中心化交易所进行交易，几经流转后从主流交易所流出或兑现。整个过程嵌套交易所利用主流中心化交易所提供的流动性和低廉的交易费用。

在多级托管模式下，账户体系层层嵌套，托管链条越长、参与者越多，资金链源头就越模糊，在多级托管体制下，监管机构难以有效获取实际虚拟货币源交易信息，难以实现穿透监管。多级托管形成若干混同账户，监管部门会受制于不同司法辖区的法律、市场规则和中

介机构的配合程度，只能获取经层层汇总后的信息，难以及时准确掌握实际虚拟货币流转的情况，增加了对虚拟货币穿透式监管、实时监测的难度。

### 6.4.2 详解利用去中心化工具洗白 Liquid 被盗 9,000 多万美元

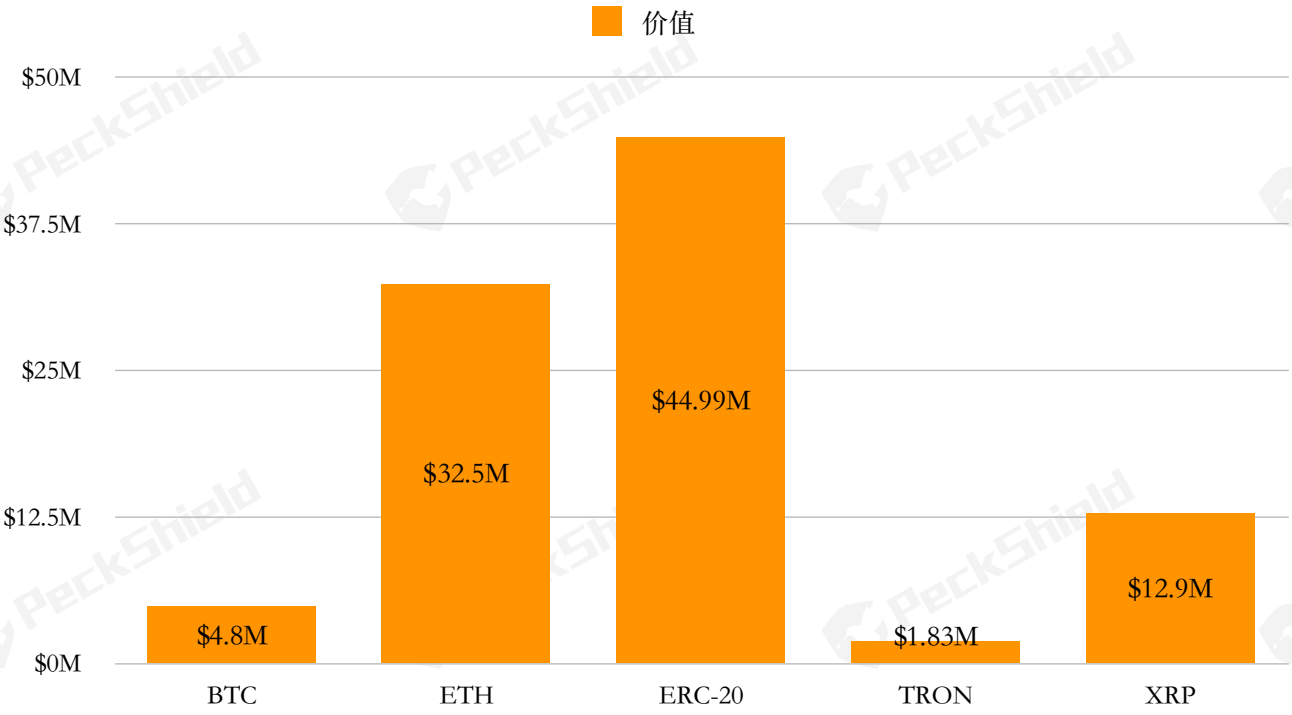



图46 日本交易所 Liquid 被盗价值 9,000 多万美元虚拟货币统计

2021年8月19日，日本交易所 Liquid 热钱包中价值 9,000 多万美元（按当时币价计算）虚拟资产被盗，包含约 480 万美元的 BTC（107.43 枚）、3,250 万美元的 ETH、4,490 万美元的 ERC-20 代币（近百种代币：AAVE、UNI、LINK、SNX、USDC）、183 万美元的 TRON（含 USDT-TRON 和 2,393,334.86 枚 TRON）、1,290 万美元的 XRP（11,467,479 枚）。

据 PeckShield「派盾」旗下反洗钱态势感知系统 CoinHolmes 显示，攻击者在得手后，大致将洗钱的流程分为三步：

1. 批量转移：将所盗 ERC-20 资产转入 DEXs，避免被冻结、回滚，同时将所盗资产进行整合，为下一步实施清洗做准备工作；

2. 批量兑换：通过 DEXs 或跨链桥将 ERC-20 代币兑换为 ETH 或 BTC，通过跨链桥将加密资产归置，为批量转移到隐私协议做准备；

3. 隐蔽阶段：将归置后的 ETH 或 BTC 转移到 Tornado Cash、Typhoon、Wasabi Wallet 等混币工具中，混淆资产来源和最终收益者，抹除非法资产的痕迹，混淆资产源头逃离追踪。

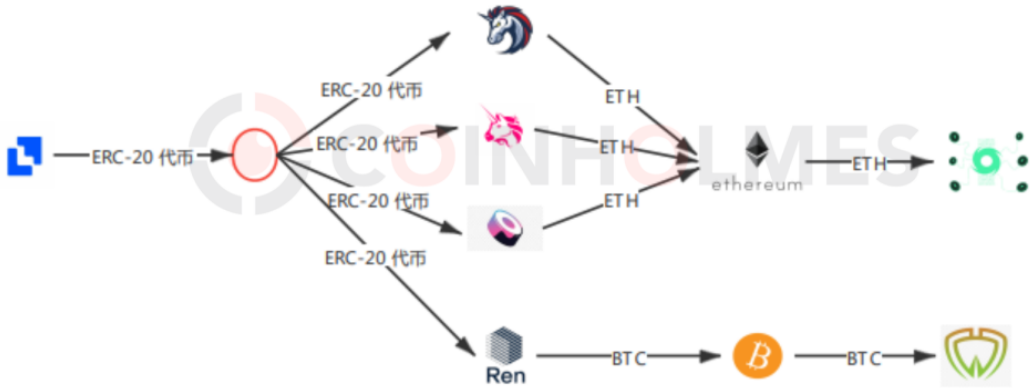



图47 Liquid 攻击者洗钱流程

再将逾千万枚 XRP 分四次转入其地址后，分三批分别转入 Binance、Huobi、Poloniex 等交易所。

Liquid 在获悉此信息后，紧急联系这几家中心化机构将攻击者地址设置黑名单，旨在紧急冻结被盗的 XRP 资产。

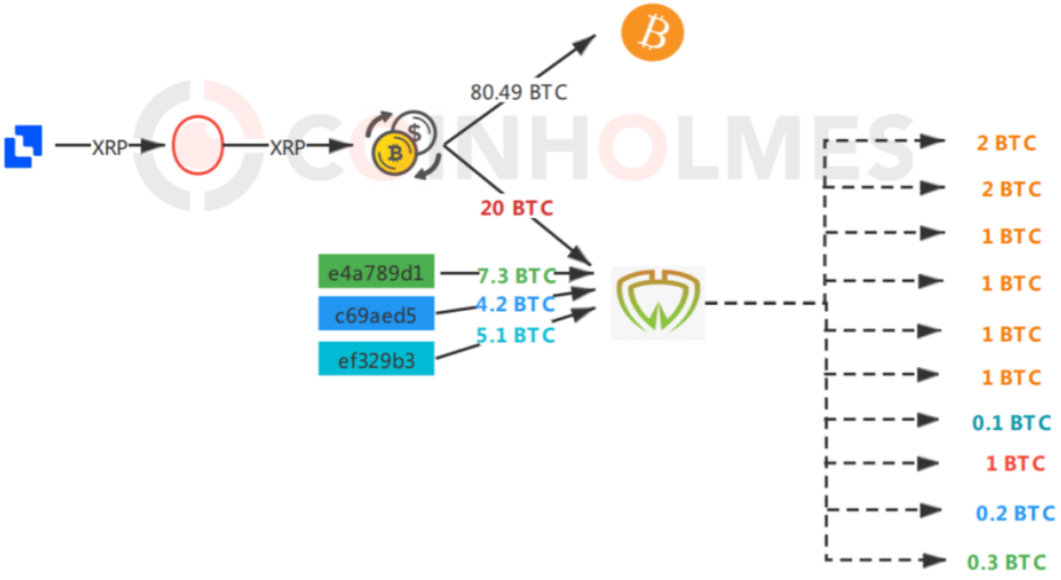



图48 Liquid 攻击者利用混币器 Wasabi 钱包清洗 XRP 过程

但在此之前攻击者已经通过交易所将部分 XRP 转换为 BTC，据 CoinHolmes 反洗钱态势系统显示，这些 XRP 已经被转换为 192 枚 BTC，并经通过去中心化的混币器 Wasabi 钱包流出。

随着监管部门对中心化机构洗钱情况的严厉监管，中心化机构不断提高 KYC 需求，使得中心化洗钱渠道遭到沉重打击，去中心化工具越来越受到犯罪分子的青睐，越来越多的非法资金开始转向去中心化渠道洗钱。

据 PeckShield「派盾」统计，目前中心化机构被盗后，通过去中心化服务进行洗钱的案例屈指可数，但已经出现利用 DeFi 协议洗钱的苗头。

# 七、结论

综上所述，PeckShield（派盾）安全团队通过分析2021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，得出如下三个重要结论：

## 7.1 2021年虚拟货币跨境流动规模达 417 亿美元 交易所和相关服务对大陆用户有序清退

2021年未受监管的出境资金规模高达 417 亿美元，是2020年流出的资金量的 2.4 倍。9月24日，十部委联合发布《关于进一步防范和处置虚拟货币交易炒作风险的通知》，首次明确境外虚拟货币交易所通过互联网向中国境内居民提供服务同样属于非法金融活动，国内中心化交易所内的留存比特币呈现出明显的流出状态，同时多家国内交易所陆续发布清退声明。

随着多家交易所或相关服务在2021年年底有序地完成对中国大陆用户的清退工作，在政策有效监管虚拟货币出入金通道的影响下，预测2022年跨境的虚拟货币流出数量和价值会大幅下降。

## 7.2 2021年DeFi 锁仓突破 2,000 亿美元　生态呈现持续高速发展趋势

2021年锁在 DeFi 中的虚拟资产再度大幅跃升，突破 2,000 亿美元关口。随着 DeFi 领域的扩展，公链发展呈现出百花齐放的总体态势，多链格局的日益稳固，催生出打破信息孤岛的刚需 — 跨链技术。

2021年跨链桥生态蒸蒸日上，巨大营运资金需求和服务的涌现，使得跨链桥在数量和功能上快速扩张。从赛道演变趋势来看，跨链桥的生态将会进一步扩张，跨链桥的边界将会向外扩大，跨链桥间的竞争将进入白热化，不论从功能上还是社区上都会愈发激烈，这也进一步抬高了跨链桥对自身安全的要求。

## 7.3 2021年DeFi 安全事件同比增长 242%　链上监控和风控措施亟待完善

PeckShield「派盾」统计显示，2021年 DeFi 安全事件达到 162 起，较2020年增长近400%，骤增的安全事件凸显出亟待完善 DeFi 领域「链上监控」与「风险控制」的基础设施

建设，引入第三方安全机构风控方案，主动监控链上数据、发现潜在风险点，结合第三方安全机构对链上数据的积累，以及敏锐洞察业务逻辑变更对 DeFi 协议的影响，深耕业务积累与技术支持在多方面的双重配合，利用态势感知工具对 DeFi 协议予以实时监控，当监控维度发生变化时做到及时预警，安全人员利用经验识别影响并及时采取行动，进一步加强和维护 DeFi 生态的稳定和健康。

# 参考文献

[1] 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

[2] 外交部，《王毅国务委员兼外长在全球反恐论坛第十一次部长级会议上的书面发言》，外交部，2021-10-08：https://www.fmprc.gov.cn/web/wjbzhd/202110/t20211008_9584107.shtml

[3] 央视网，《央行：我国对虚拟货币的监管政策是明确的、一贯的》，央视网，2021-09-24：https://jingji.cctv.com/2021/09/24/ARTIDni3LeGGTj9n2YGGjdIz210924.shtml

[4] 卜晓明，《土耳其一虚拟币交易平台老板被曝携款跑路》，新华网，2021-04-25：http://www.xinhuanet.com/world/2021-04/25/c_1211126442.htm

[5] 侯嘉成、荣迅，《虚拟货币整治升级：清退挖矿与禁止相关业务双管齐下》，澎湃新闻，2021-09-26：http://news.jcrb.com/jsxw/2021/202109/t20210926_2322856.html

[6] 中国证券报，《疯狂！狂飙 2300 倍后血崩归零，创办人跑路，投资者：“这是场鱿鱼游戏”》，中国证券报，2021-11-04：https://cj.sina.com.cn/articles/view/1656058115/62b5710301900zess?sudaref=www.google.com.hk&display=0&retcode=0

[7] 吴斌，《监管风暴席卷而来 加密货币出路何在？》，21世纪经济报道，2021-02-04：http://www.21jingji.com/2021/9-21/4MMDE1MTFfMTYyNzM4MQ.html

[8] The Treasury Department，《FINANCIAL TREND ANALYSIS：Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021》，FinCEN，2021-10：https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

[9] Maple Leaf Capital，《2020年 DeFi 复盘与展望：新兴价值网络崛起和华尔街接口之潜力》，网易，2020-12-29：https://www.163.com/dy/article/FV12EP3C0519SM7A.html

[10] 蜂巢Tech，《交易所公链如何冲破「土狗」困局？》，蜂巢Tech，2020-03-13：https://www.tuoniaox.com/news/p-491309.html

[11] 深潮TechFlow，《交易所公链的"中心化"困局：土狗坠落，交易所背锅？》，深潮TechFlow，2021-03-08：https://www.odaily.news/post/5165196

[12] Blocklike，《开局一张图：DeFi、Uniswap 和土狗们》，2021-08-14：https://www.odaily.news/post/5154571

[13] MacKenzie Sigalos，《BitMart says it will compensate victims of $196 million hack and restore trading by Tuesday》，CNBC，2021-12-05：https://www.cnbc.com/2021/12/05/hackers-take-196-million-from-crypto-exchange-bitmart-in-large-breach.html

[14] 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

[15] 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

[16] PeckShield「派盾」，《美国联邦调查局 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

[17] 360 Netlab，《从蜜罐视角看 Apache Log4j2 漏洞攻击趋势》，2021-12-21：https://blog.netlab.360.com/apache-log4j2-vulnerability-attack-trend-from-the-perspective-of-honeypot/

[18] Fabian Schär，《Decentralized Finance: On Blockchain and Smart Contract-Based Financial Markets》，2021-11-02：https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets

[19] PeckShield「派盾」，《详解利用去中心化工具洗白 Liquid 被盗 9,000 多万美元》，2021-09-07：https://mp.weixin.qq.com/s/wCXS337HpsfFd4S1K_NX0g

[20] PeckShield「派盾」，《黑客在 Poly Network 狂揽6.1亿美元利用 DeFi 出金》，2021-08-11：https://www.panewslab.com/zh/articledetails/D05230551.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 3 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