PeckShield

Web3 行业安全报告

2022年度报告

PeckShield「派盾」

2023.01

目录

一、研究背景综述

2022年，美联储持续加息，全球流动性紧缩，加密行业跌入第三次「寒冬」。今年，加密资产总市值缩水超过 2.2 万亿美元，中心化金融类机构（下称“CeFi”）业务规模下降约 71.4 %。受到 Terra 崩盘、三箭资本（下称“3AC”）和 Celsius 等黑天鹅事件以及跨链桥攻击的影响，去中心化金融（下称“DeFi”）总锁仓值（下称“TVL”）腰斩，DeFi 进入去杠杆阶段。2022年年末 FTX 等 CeFi 巨头的崩塌，倒推市场提高对中心化交易所（下称“CEX”）透明度的要求，DeFi 领域落地应用的真实价值显现。

虽然行业因一连贯的黑天鹅事件受到重创，但行业基础设施的建设和扩张并未停止。以太坊开启 PoS 新时代，Layer2 快速发展，Move 系公链乘风而起，Web2 抢滩布局 NFT，M2E 探索 GameFi 新模式，SocialFi 被视为资本看好的新蓝海，继续扩展社交边界。

2022年「浮华」退却，行业发展逐步回归理性，泡沫逐渐出清，CeFi 领域监管趋严，DeFi 领域监管开展，合规需求激增。

相较于上一轮泡沫破裂（2018年），市场上已经落地以 Uniswap 和 Compound 为代表，拥有内在价值并经受住了市场长期检验的 DeFi 产品。8月，Tornado.Cash 遭制裁，折射出各主要经济体对 DeFi 领域监管逐渐展开的趋势，Web3 行业进入有序发展阶段。熊市期间，行业参与者投身新一轮的基础设施建设，为下一个叙事周期寻找新的增长点。

接下来，本报告将以时间为序，从市场、技术、政策、安全等四方面梳理 Web3 行业一年来发生的重大事件。

1月，以 StepN 为代表的 M2E 引领 GameFi 热潮。同时，Crypto.com 在本月遭黑客入侵，损失超 3,000 万美元。

2月，俄乌冲突将众筹 DAO 和加密资产跨境支付推向台前[1]。

3月，拜登签署加密资产行政命令[2]，将研发潜在的美国央行数字货币（下称“CBDC”）选项置于最紧迫位置。各主要经济体也稳步推进其 CBDC 的研发与落地。

4月，一众传统金融巨头涉足数字商品业务抢滩布局[3]，积极试水 NFT、元宇宙和 Web3，明星与品牌方紧随其后。在明星与品牌效应加持之下，以 NFT 为主的 Web3 加速破圈。以 Lens Protocol、Galxe 为代表的 SocialFi 社群初现规模。

5月，算法稳定币（下称“算稳”）UST 脱锚，Terra 崩盘，DeFi TVL 腰斩，NFT 市场日销售量锐减，DeFi 进入去杠杆化阶段。以波场（下称“Tron”）为代表的公链推出基于自己公

链的算稳 USDD，在第二季度逆势上扬。

6月，受 Terra 的影响[4]，头部 CeFi 接连陷入大规模清算危机[5]，CEX 被爆跑路或停止兑付。Celsius 破产重组、3AC 破产清算、贝宝金融停止提现、Voyager Digital 申请破产保护、虎符交易所暂停交易、AEX 暂停平台相关服务……多家加密资产机构 Coinbase、Opensea 传出缩减规模计划。同时，Move 系新公链崭露头角，公链赛道进入新一轮角逐。

7月，美联储副主席布雷纳德呼吁美国决策者对加密资产行业进行更严格的监管。以财长耶伦为首的政府官员提出推动对稳定币更严格的监督[6]。同时，老牌 DeFi 借贷协议 Aave 和 Curve 宣布发行稳定币，为陷入沉寂的稳定币赛道注入新的活力。

8月，美国财政部外国资产控制办公室（下称“OFAC”）以涉嫌帮助受制裁的黑客组织 Lazarus Group 洗钱和参与其他洗钱活动为由[7]，将 Tornado.Cash 以及其相关的地址添加到「特别指定国民名单」（下称“SDN 名单”）中。全球最大的资产管理公司贝莱德为美国的机构客户推出首个直接投资于比特币的产品。美国联邦调查局就 DeFi 存在的风险发出警告。

9月，以太坊合并[8]，共识机制从工作量证明（下称“PoW”）过渡到权益证明（下称“PoS”），以太坊生态完成近年来最大升级，为加密行业史新增一笔重要注脚。

10月，DeFi 领域安全事件频发，掠走价值 7.6 亿美元加密资产（部分被盗资金返还，损失计为 6.58 亿美元）。香港百域资本旗下的并购基金以 30 亿美元的估值正式收购 Huobi Global（下称“火币”）[9]。NEAR 公链上的算稳 USN 因资不抵债而宣布停止运营；基于 Waves 公链的稳定币 USDN 的流通量在反复脱锚后锐减近 90%；USDD 出现下探 0.93 美元的情况；稳定币市场迎来新的监管拐点。

11月，香港考虑放开加密资产散户交易，以期将香港发展成为加密资产中心。全球最大的中心化加密资产交易所之一 FTX 陷入财务危机，在短短十天内流动性枯竭后申请破产，泡沫加速破裂。BlockFi 破产重组，DCG 陷入流动性危机。曾被认为大而不倒的加密资产行业中心化领军者们的信誉备受质疑。

12月，市场恐慌情绪飙升，币安遭遇大量资金外流。FTX 前首席执行官 Sam Bankman-Fried（下称“SBF”）[10]应美国当局的要求被巴哈马皇家警察逮捕。Mango 攻击者 Avraham Eisenberg[11] 在波多黎各被捕。

回顾2022年，行业格局发生巨变，交易所进入新一轮的洗牌期，「透明」、「合规」、「安全」成为 Web3 行业的年度关键词。

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、BNB Chain 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加密资产汇总和溯源分析；

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 多种主流加密资产；

5）PeckShield 态势感知服务：

PeckShield 态势感知服务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）穿透 DeFi 的可视化追踪

PeckShield 提供一整套穿透 DeFi 的可视化追踪服务，自动追踪敏感资金动向，各类 DeFi 领域犯罪、受制裁资金的分析统计，实时预警犯罪资金的异动，以及提示受制裁地址的风险。

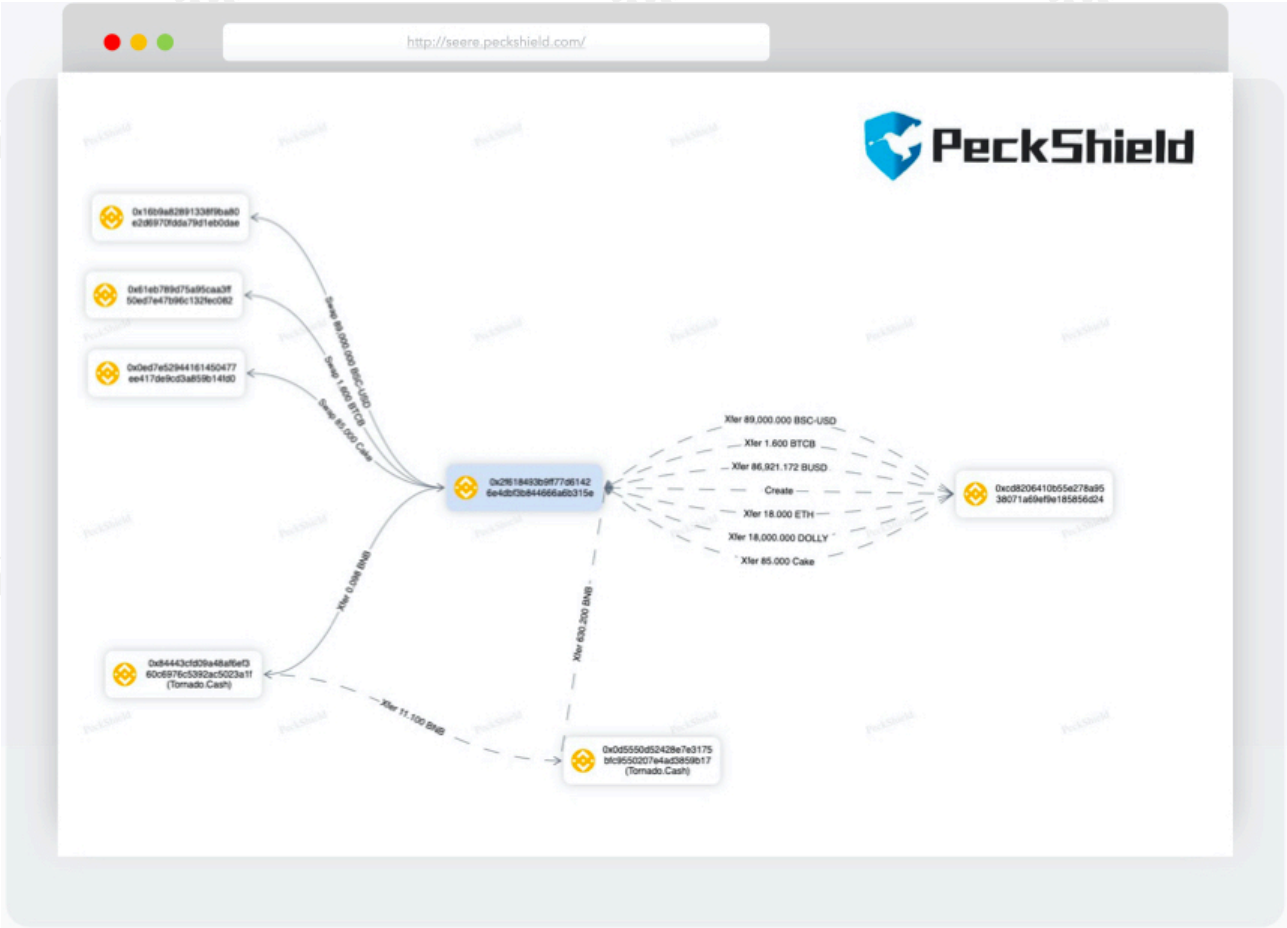


图2 穿透 DeFi 的可视化追踪系统截图

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3 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、全球加密资产流向现状

3.1 中心化和去中心化交易所交易量

PeckShield「派盾」结合已有的 1 亿地址标签，对 CEX 地址和 DEX 地址的以太坊（下称“ETH”）交易量进行监控、分析发现，2022年 CEX 的交易量有所下降。受黑天鹅事件的影响，头部 DEX 的交易量小幅增长。

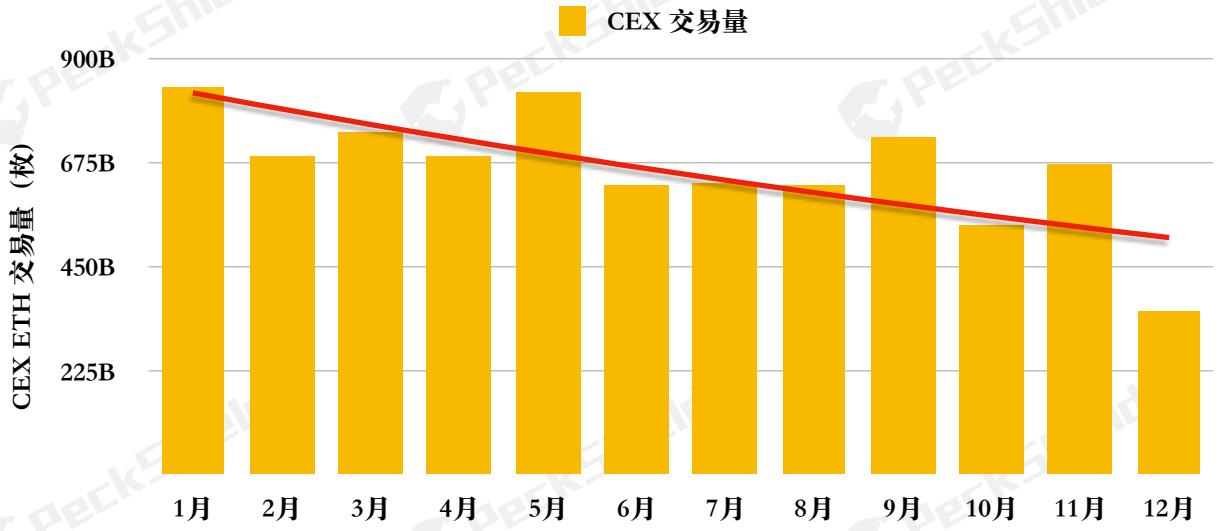


图4 2022年每月 CEX 的 ETH 交易量（CryptoCompare）

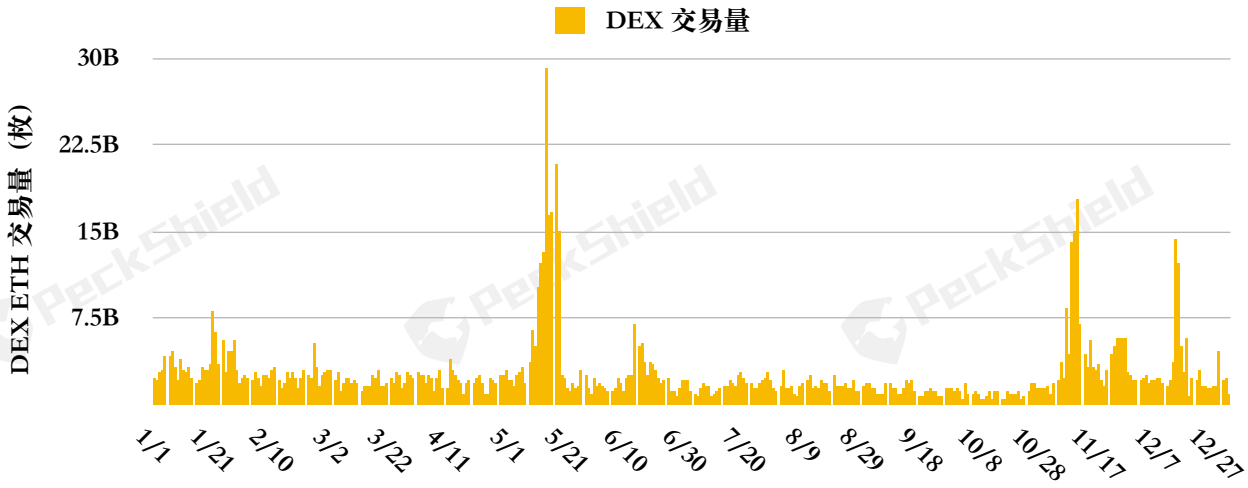


图5 2022年每日头部 DEX 的 ETH 交易量

据 CryptoCompare 数据显示，CEX 的交易量在 2022 年期间下降了 46%。尤其是在 FTX 破产后，头部 CEX 的交易量大幅下降，从日均 300 多亿美元的交易量下降到日均 100 亿美元的交易量。值得注意的是，在诸如 FTX 挤兑、币安「FUD」的极端市场行情出现的情况

下，用户不再受到 CEX 暂停提款等掣肘，有转向使用能够管控自己资产的 DEX 的苗头。

CEX 的交易流程类似银行，用户把自己资产转入到交易所，在交易所的背书下完成交易，最后再把加密资产提取到自己的钱包，在这个交易过程中 CEX 收取一定的手续费。其交易本质是卖家把加密资产转到 CEX 的账户托管，买家所交易的加密资产也是转入在 CEX 里的子账户，只有把加密资产提到钱包才真正属于用户。所以如果 CEX 作恶或发生流动性危机时，都会增加用户的资产风险系数。得益于 CEX 的易操作性，现阶段 CEX 交易量仍普遍高于 DEX。

DEX 提供 CEX 的核心交易功能，略去「转入」和「提出」的步骤，用户使用自己的地址与 DEX 的智能合约地址交易。DEX 的优点在于用户资产完全掌握在自己手中，用户不会受到 CEX 掣肘。但受限于区块链网络吞吐量的问题，DEX 的交易速度低和交易成本高。再者，DEX 需要用户有一定的智能合约交互基础，目前行业开始探索跨链 DEX 的模式，安全性是该赛道目前面临的挑战之一。

3.2 全球主要中心化交易所储备金现状

受到 FTX 交易所破产事件的影响，多家 CEX 迅速作出反应，提供交易所用户资产的默克尔树储备证明（下称“Merkle Tree Proof of Reserves”），以表明自己储备金足够且未动用用户的资金。

但 CEX 面临的资产证明问题依然复杂[12]，首先是树根的更新频率问题，更新频率是保障这套系统有效性的一个关键参数；其次是前端欺诈问题难以验证，需要一些第三方的开源软件解决这个信任问题；最后是第三方审计的信用问题。

交易所	总储备金（$）	净储备金（$）	交易所代币储备金（$）	储备金干净度（%）
Binance	$62.1B	$54.3B	$7.8B	87.32%
OKX	$7.2B	$7.2B	0	100%
Bitfinex	$7.6B	$5.3B	$2.2B	70.1%
Crypto.com	$3.7	$3.6B	$162.4B	95.7%
Kucoin	$2.8B	$2.3B	$549.9M	80.71
Bybit	$2.4B	$2.2B	$234.9M	90.52%
Huobi	$2.9B	$1.7B	$1.1B	59.72%
Deribit	$1.5B	$1.5B	0	100%

图6 2023年1月16日八大 CEX 储备金现状（CryptoQuant）

除了上述问题，由于 FTX 使用其平台币 FTT 来抵押贷款扩大其本身的风险值，因此，在评估 CEX 储备金时，交易所平台币（例如，Binance 发行的平台币 BNB，Huobi 发行的平台币 HT，OKX 发行的的平台币 OKB）的储备金占比成为考量 CEX 整体健康度的重要参考维度之一。交易所平台币储备金的占比越高，CEX 储备设置的潜在风险就越高。如图6，截至2023年1月16日 CryptoQuant 所列出的八大 CEX 的储备金现状所示，除去交易所平台币的储备金占比，Binance 净储备约占 87.32%，Bitfinex 净储备约占 70.1%，Huobi 净储备约占 59.72%。

FTX 的破产促使用户对 CEX 的信任产生质疑，CEX 出现资金外流的现象。如图7，2022年11月至12月 CEX 的 ETH 流入流出量以及 ETH 余额所示，从2022年11月初起，ETH 开始有流出 CEX 的趋势。CEX 地址中的 ETH 数量从11月初近 2,600 万枚到11月21日降至 2,353 万枚，流失占比达到 9.5%。但得益于其较强的易用性，CEX 仍占据整个交易所格局的主导地位。

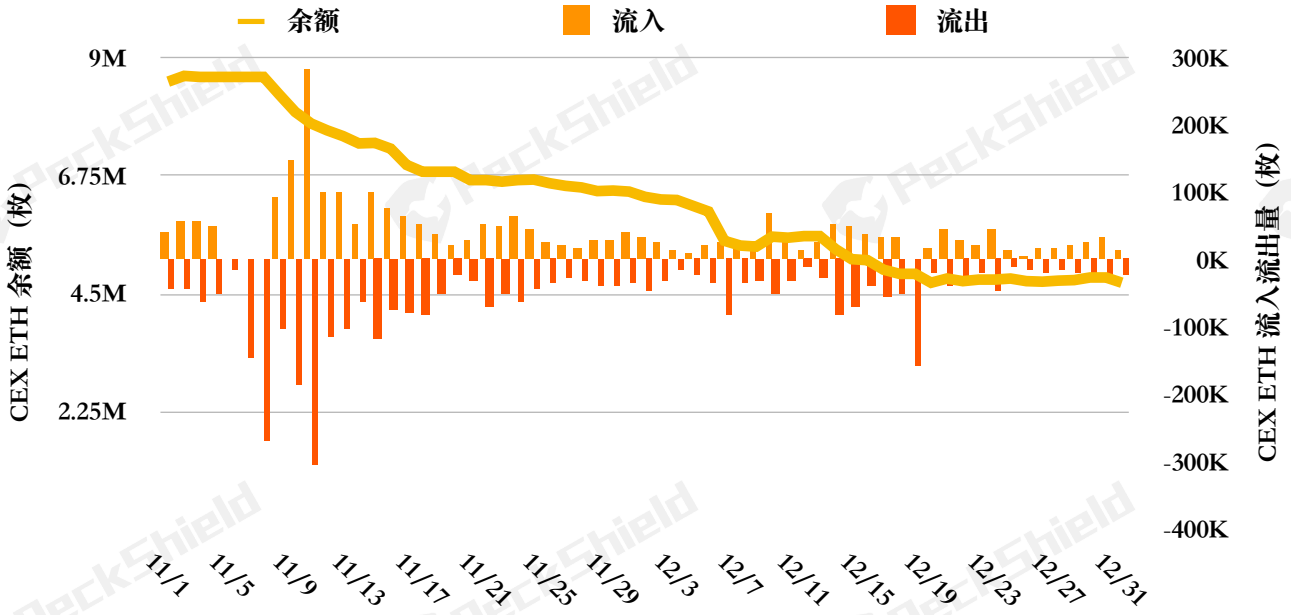


图7 2022年11月至12月 CEX 的 ETH 余额及 ETH 流入流出量

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：币安（又称“Binance”）、Bitfinex、Bithumb、BitMEX、Bitstamp、Bittrex、Coinbase、Coincheck、FTX、Gate.io、Gemini、HitBTC、火币（又称“Huobi”）、Kraken、KuCoin、Luno、OKX、Poloniex 等主流中心化交易所，以及 Uniswap、Curve、0x、Sushiswap、Balancer 等去中心化交易所。

3.3 Tornado.Cash 加密资产流入流出现状

Tornado.Cash 是以太坊上的隐私解决方案之一，它使用简洁非交互式零知识证明（又称为“zk-SNARK”）来实现属于同一用户地址之间的不可链接性，并以无需信任的方式保护用户隐私。虽然 Tornado.Cash 的初衷是为了保护用户的隐私权，但由于其隐私性强的特性，在无形之中被广泛应用于黑灰产业的「洗钱」环节。

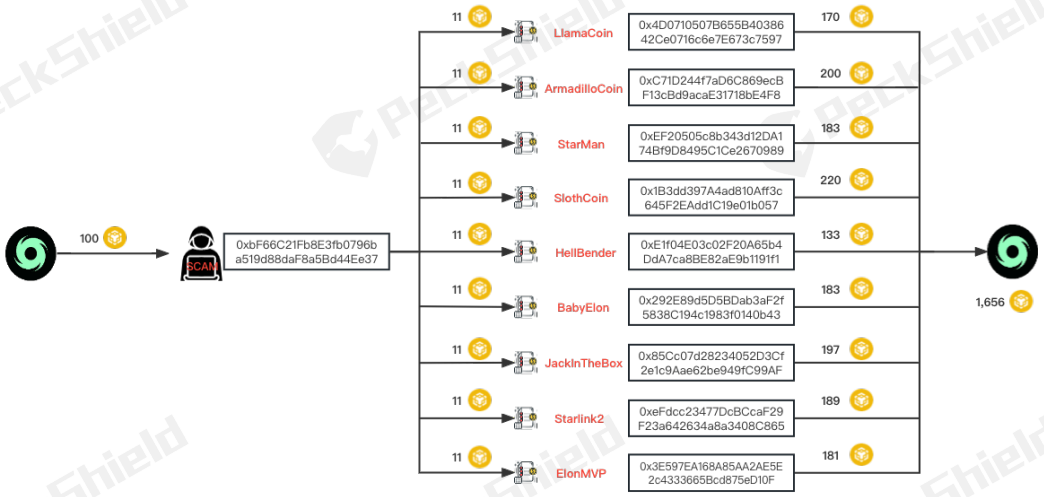


图8 Tornado.Cash 被用于黑灰产业的资金流转过程示例图

在很多黑客攻击事件或欺诈事件中，攻击者或诈骗者会选择通过 Tornado.Cash 获得启动资金，然后在实施攻击之后使用 Tornado.Cash 掩盖获利的去向。Tornado.Cash 打破了资金来源地址和资金到达地址之间的链上关联，加大了溯源和追踪的难度，使得其对反洗钱工作的开展带来很大的挑战。

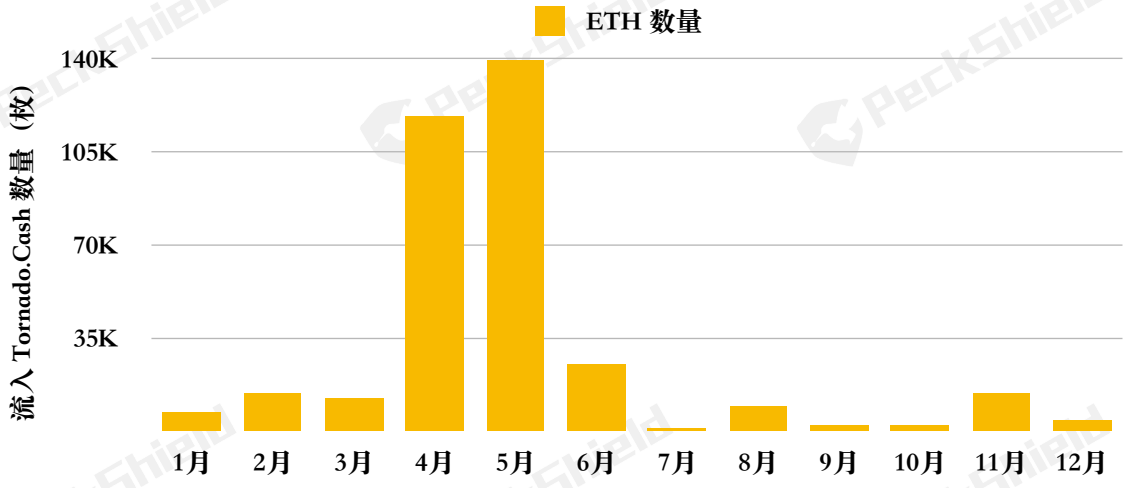
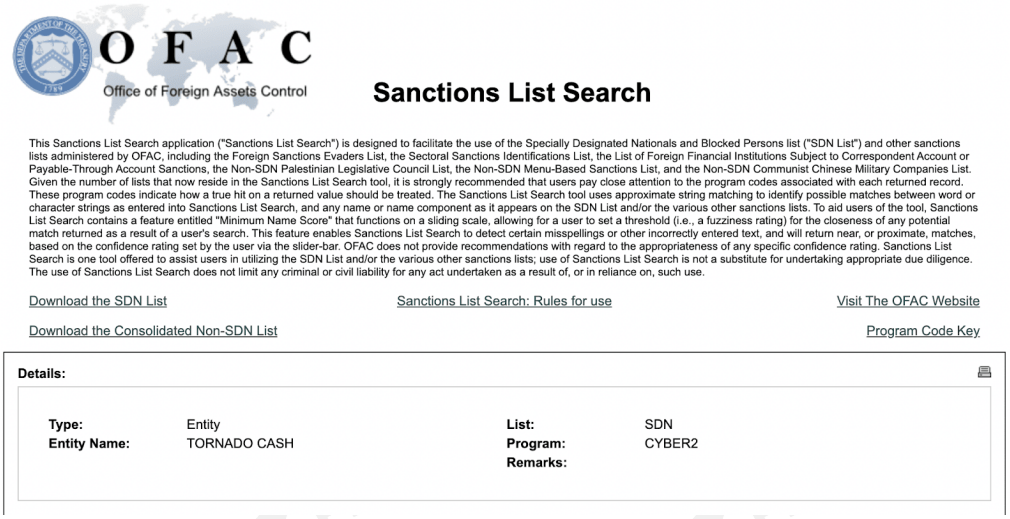


图9 DeFi 黑客事件被盗 ETH 转入 Tornado.Cash 的数量

经 PeckShield「派盾」研究发现，黑客攻击事件发生后，攻击者将所盗 ETH 转入 Tornado.Cash 的总量达到 35 万枚（按当前价格 1,325 美元/枚），约合 4.6 亿美元（由于加密资产价格波动大，实际转入 Tornado.Cash 的加密资产规模可能会更大）。

由于 Tornado.Cash 在诸多安全事件中扮演了「洗钱通道」的角色，引起了监管与执法部门的关注。2022年8月8日，OFAC 以涉嫌帮助受制裁的黑客组织 Lazarus Group 洗钱和参与其他洗钱活动为由，将 Tornado.Cash 以及其相关的地址添加到 SDN 名单中。


OFAC
Office of Foreign Assets Control

Sanctions List Search

This Sanctions List Search application ("Sanctions List Search") is designed to facilitate the use of the Specially Designated Nationals and Blocked Persons list ("SDN List") and other sanctions lists administered by OFAC, including the Foreign Sanctions Evaders List, the Sectoral Sanctions Identifications List, the List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions, the Non-SDN Palestinian Legislative Council List, the Non-SDN Menu-Based Sanctions List, and the Non-SDN Communist Chinese Military Companies List. Given the number of lists that now reside in the Sanctions List Search tool, it is strongly recommended that users pay close attention to the program codes associated with each returned record. These program codes indicate how a true hit on a returned value should be treated. The Sanctions List Search tool uses approximate string matching to identify possible matches between word or character strings as entered into Sanctions List Search, and any name or name component as it appears on the SDN List and/or the various other sanctions lists. To aid users of the tool, Sanctions List Search contains a feature entitled "Minimum Name Score" that functions on a sliding scale, allowing for a user to set a threshold (i.e., a fuzziness rating) for the closeness of any potential match returned as a result of a user's search. This feature enables Sanctions List Search to detect certain misspellings or other incorrectly entered text, and will return near, or proximate, matches, based on the confidence rating set by the user via the slider-bar. OFAC does not provide recommendations with regard to the appropriateness of any specific confidence rating. Sanctions List Search is one tool offered to assist users in utilizing the SDN List and/or the various other sanctions lists; use of Sanctions List Search is not a substitute for undertaking appropriate due diligence. The use of Sanctions List Search does not limit any criminal or civil liability for any act undertaken as a result of, or in reliance on, such use.

Download the SDN List | Sanctions List Search: Rules for use | Visit The OFAC Website

Download the Consolidated Non-SDN List | Program Code Key

Details:

Type: Entity
Entity Name: TORNADO CASH

List: SDN
Program: CYBER2
Remarks:

图10 OFAC 将 Tornado.Cash 以及其相关的地址添加到 SDN 名单的公告

这并不是第一次 OFAC 新增受制裁的链上地址。据 PeckShield「派盾」统计，近三年来，遭到 OFAC 制裁过的新增链上地址数量逐年递增，2022年较2021年新增遭到过 OFAC 制裁的链上地址增长 76%。值得注意的是，Tornado.Cash 遭制裁是美国政府首次对智能合约应用进行制裁。

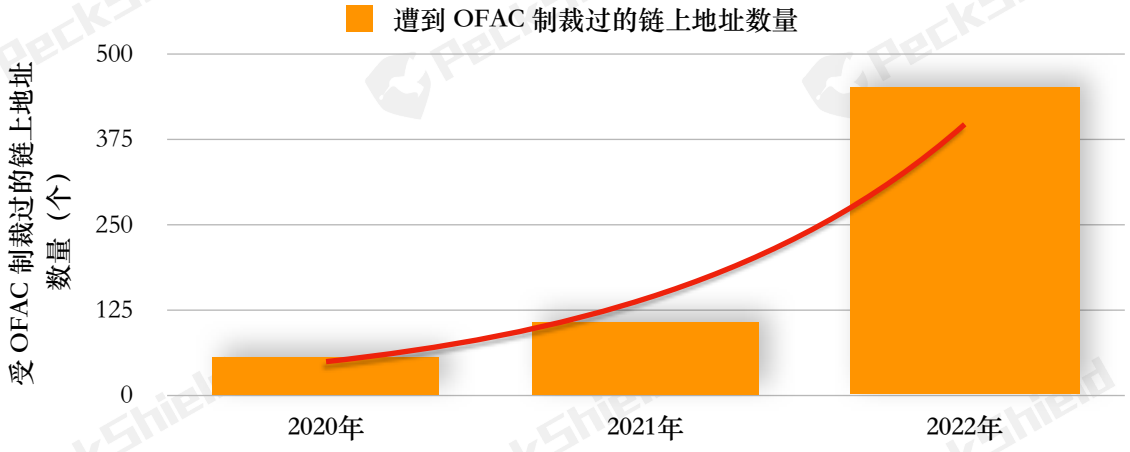


图11 近三年新增受 OFAC 制裁过的链上地址数量

在 OFAC 官方禁令发布后不久，Tornado.Cash 官网无法访问，更多相关项目方推出了各自的制裁措施，包括 Gitcoin 提出暂停 Tornado.Cash 赠款（Tornado.Cash 曾是 Gitcoin 的早期受赠者）、稳定币 USDC 发行方 Circle 宣布冻结 SDN 地址中的 USDC 资产、Web3 开发平台 Infura 和 Alchemy 宣布阻止 Tornado.Cash 的 RPC 请求（依托 Infura 和 Alchemy 服务的相关节点将无法为 Tornado.Cash 提供服务）。

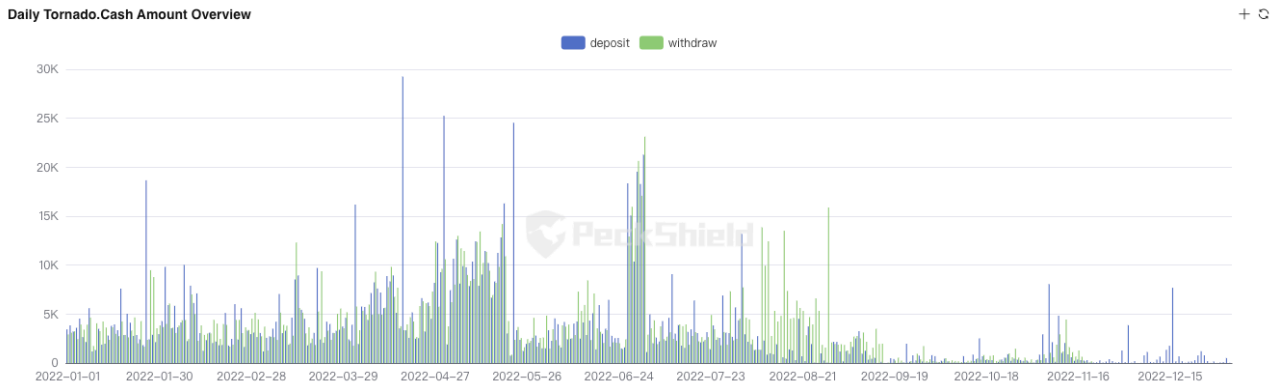


图12 Tornado.Cash 的 ETH 池流入流出量

如图12，Tornado.Cash 的 ETH 池流入流出量所示，受到制裁后，Tornado.Cash 的 ETH 池虽然仍有新的 ETH 流入，但流入量较被制裁前大幅下降。

同样地，转入 Tornado.Cash 的黑钱在数量上也有所减少。这些禁令提高了使用 Tornado.Cash 的门槛，在一定程度上阻拦了部分不法分子将黑钱转入 Tornado.Cash。但市面上也出现了其他一些新的之前不太常用的加密资产洗钱路径，例如，利用跨链等工具将黑钱跨到 BTC 链上再转入 ChipMixer 等混币器。

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。Tornado.Cash 等 DeFi 协议遭制裁凸显出监管展开对 DeFi 领域的监管趋势增加，合规需求提升。

四、Web3 行业安全现状

4.1 Web3 行业安全现状概览

截至2022年12月31日，2022年 Web3 行业共发生重大安全事件 1,637 起，共计损失逾 121.6 亿美元，其中黑客攻击（包含 CeFi 和 DeFi 领域） 260 起，诈骗事件 1,377 起。2022年 Web3 行业安全事件的数量较前两年呈抛物线式飙升。

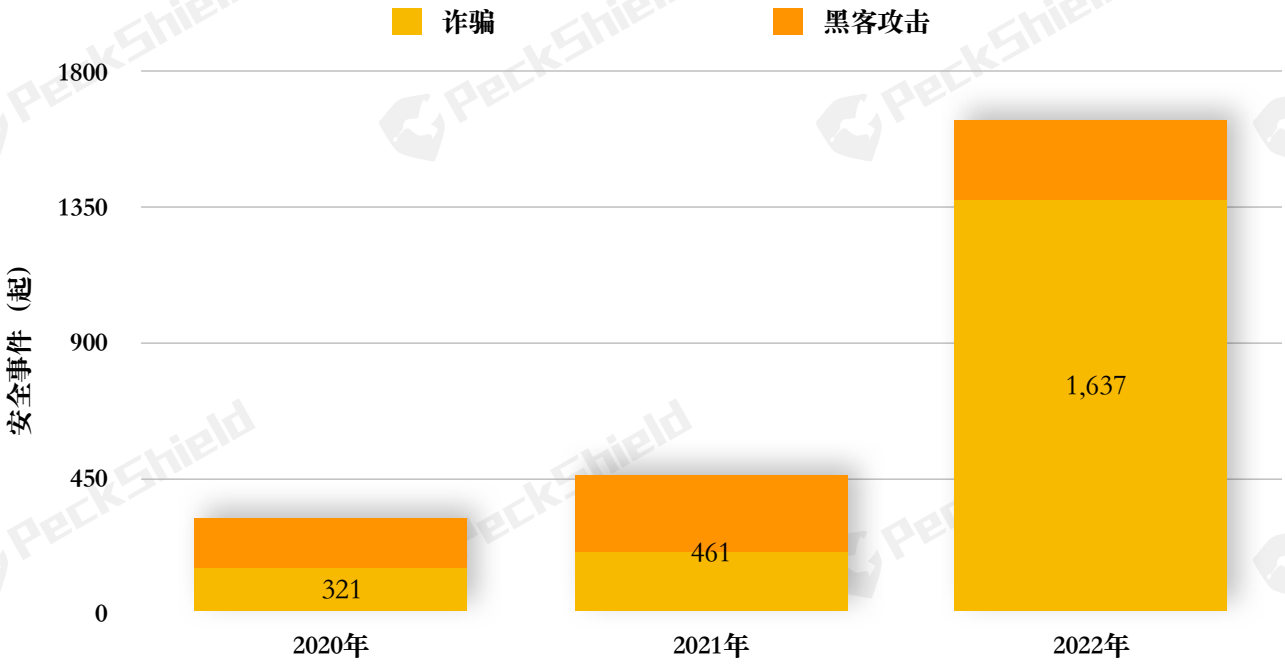


图13 近三年 Web3 行业安全事件统计

2020年加密资产行业共发生重大安全事件 321 起，其中黑客攻击约 170 起，诈骗事件 151 起；共计损失逾 55 亿美元，黑客攻击造成 21.3 亿美元的损失，诈骗事件造成 31.3 亿美元的损失。

2021年加密资产行业共发生重大安全事件 461 起，其中黑客攻击约 261 起，诈骗事件 201 起；共计损失逾 142.5 亿美元，黑客攻击造成损失 21.1 亿美元，诈骗事件造成损失 121.4 亿美元。

2022年共计 260 起黑客攻击，从数量上看与2021年（261起）相差不大，从损失来看，同比增长 39%，其中去中心化领域成为黑客攻击主要目标，占总损失的 86%。

2022年 Web3 行业的诈骗事件在数量上激增，以高收益、高回报吸收资金的 CeFi「传统骗局」占比居高不下，包括 JuicyFields.io 大麻投资庞氏骗局（损失 2.73 亿美元）、omegapro.world 骗局（损失 1.06 亿美元）、Unique-exchange.co 和 PARAIBA.world 钱包基础

设施的互连服务骗局（损失 2.68 亿美元）。因受黑天鹅事件的影响，具有一定规模的 CeFi 机构（以 CEX 为主）跑路频发。此外，欺诈蔓延至 NFT、GameFi 等细分领域，且诈骗手段愈发多样化，除却「貔貅盘」、「RugPull」等链上诈骗模式，还引入了在 Web2 行业盛行多时的社会工程学骗局，与 NFT 相关的 Web2 社交平台遭钓鱼攻击呈高发态势。

相较2021年，受熊市的影响，2022年 Web3 领域诈骗事件造成损失整体呈小幅下降趋势，但在 DeFi 领域涉及 RugPull 的损失较2021年所造成的损失翻了近一番。

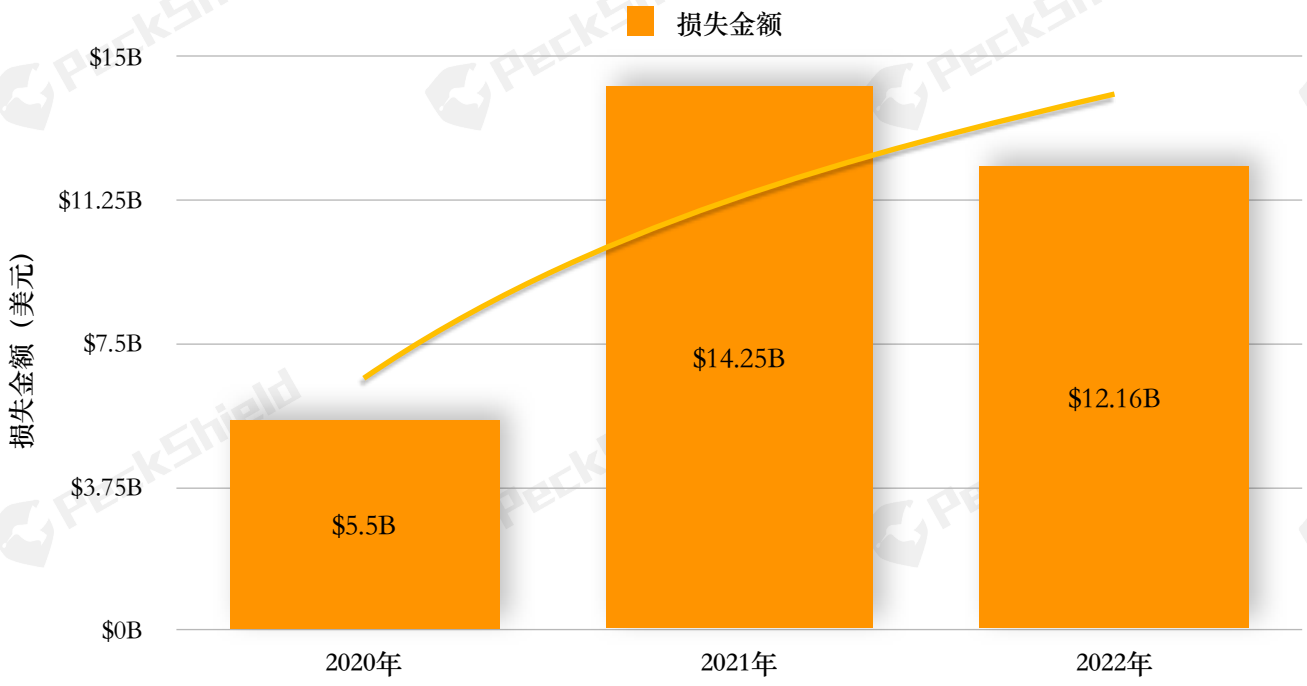


图14 近三年 Web3 行业安全事件损失统计

NFT、GameFi 等垂直行业的兴起使得低成本、技术含量较低的钓鱼事件在今年呈现爆发的趋势。这给市场敲响警钟，即发展新兴技术的同时，需要同步构建相应的安全基础设施来确保 Web3 行业的健康发展。此外，还要加强公众的安全意识，时时提示公众经受住诱惑，保护好钱包，不参与任何带有炒作色彩的活动。

4.2 DeFi 安全事件统计分析

随着 Web3 行业跌入「寒冬」，DeFi 领域也进入急剧收缩期。据 DefiLlama 数据显示，截至2022年12月31日，2022年全年 DeFi 生态所有协议内的 TVL 为 447.6 亿美元，较全年顶峰的 2,057 亿美元已缩水逾四分之三。

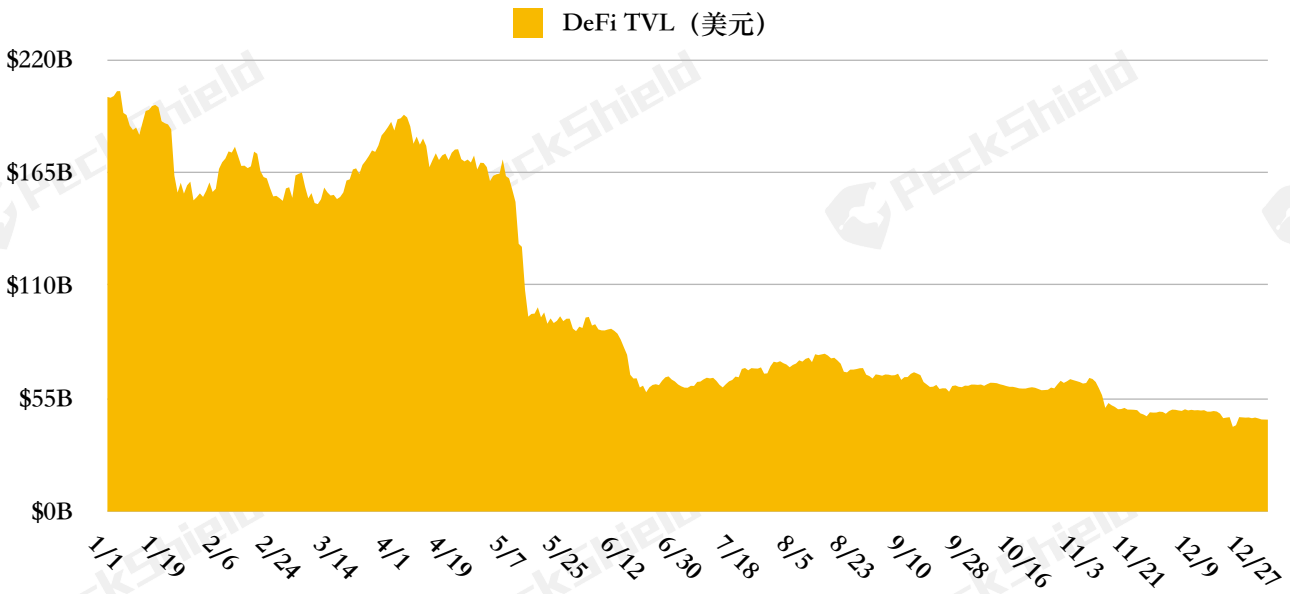


图15 DeFi 生态 TVL 全年变化趋势（DefiLlama）

虽然 DeFi 生态的 TVL 有所下降，但从整体来看，在整个 Web3 行业格局的发展与巨变中，DeFi 生态已经建成，且占有愈发重要的一席之地。

今年5月 Terra 算稳生态的崩塌，对整个 Web3 行业无论是 CeFi 还是 DeFi 都带来巨大的冲击。年末位列全球第二的中心化交易所 FTX 的破产，引发整个 Web3 行业尤其是中心化交易所格局的再一次洗牌。DeFi 领域尤其是 DEX 赛道，在 CeFi 信誉遭到质疑的情况下，作为近两年崛起的行业颠覆性创新模式的新变量，成为整个 Web3 行业发展中不可或缺的重要板块。

2021年延续「DeFi 元年」（2020年6月至2020年末）的热潮，DeFi 生态迅速成长壮大，涌现出一批在各赛道激烈拼杀中脱颖而出的头部项目。2022年熊市降临，资本热情消退，劣币逐步清除，整个行业的竞争愈发激烈甚至惨烈，头部效应逐步凸显。基于公链构建的 DeFi 垂直生态在牛市通过投资、激励机制刺激 TVL 飙升，在吸引流动性上起到立竿见影的效果。但资本遇冷后，对于以公链为基础建设的 DeFi 生态除了需在技术创新上有所突破，对其安全性也提出更高要求。

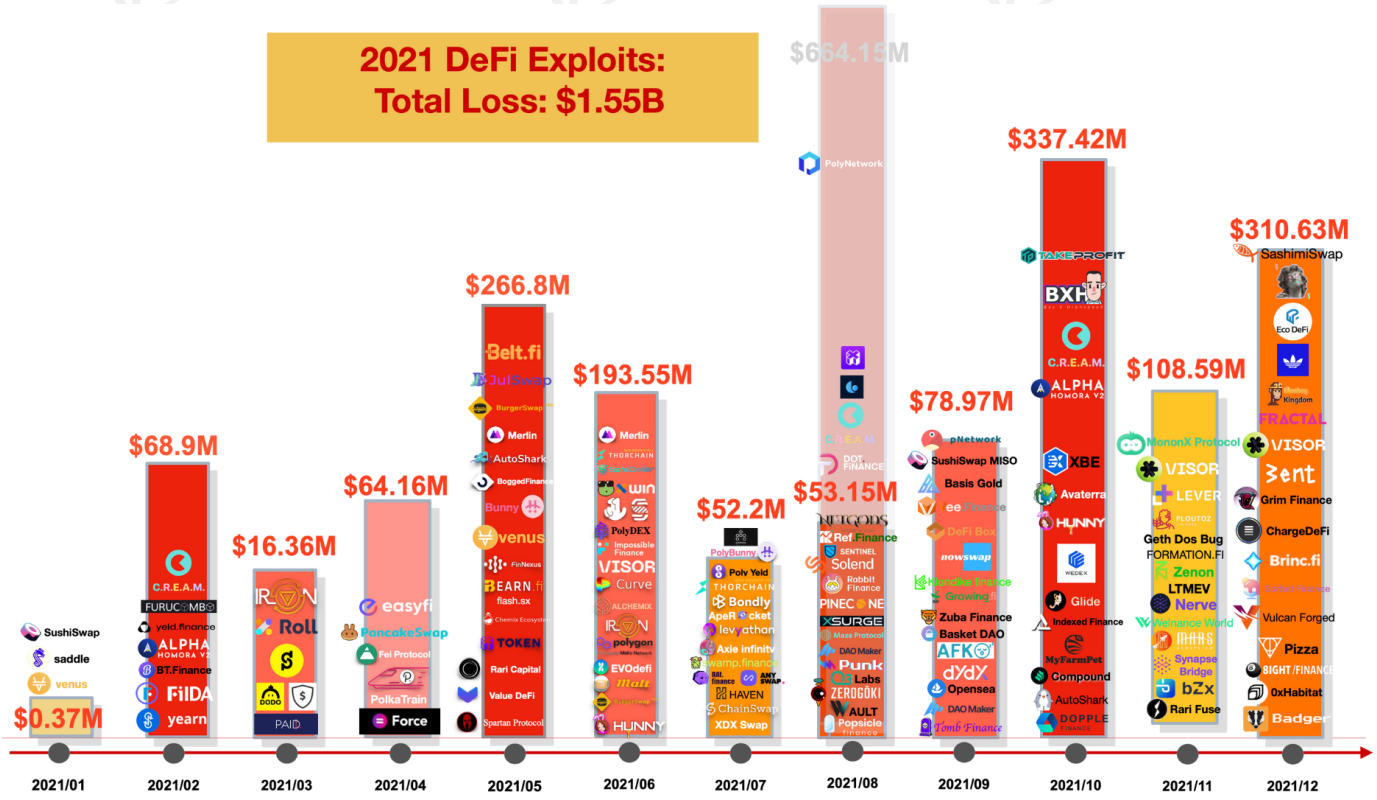


图16 2021年 DeFi 安全事件全览图

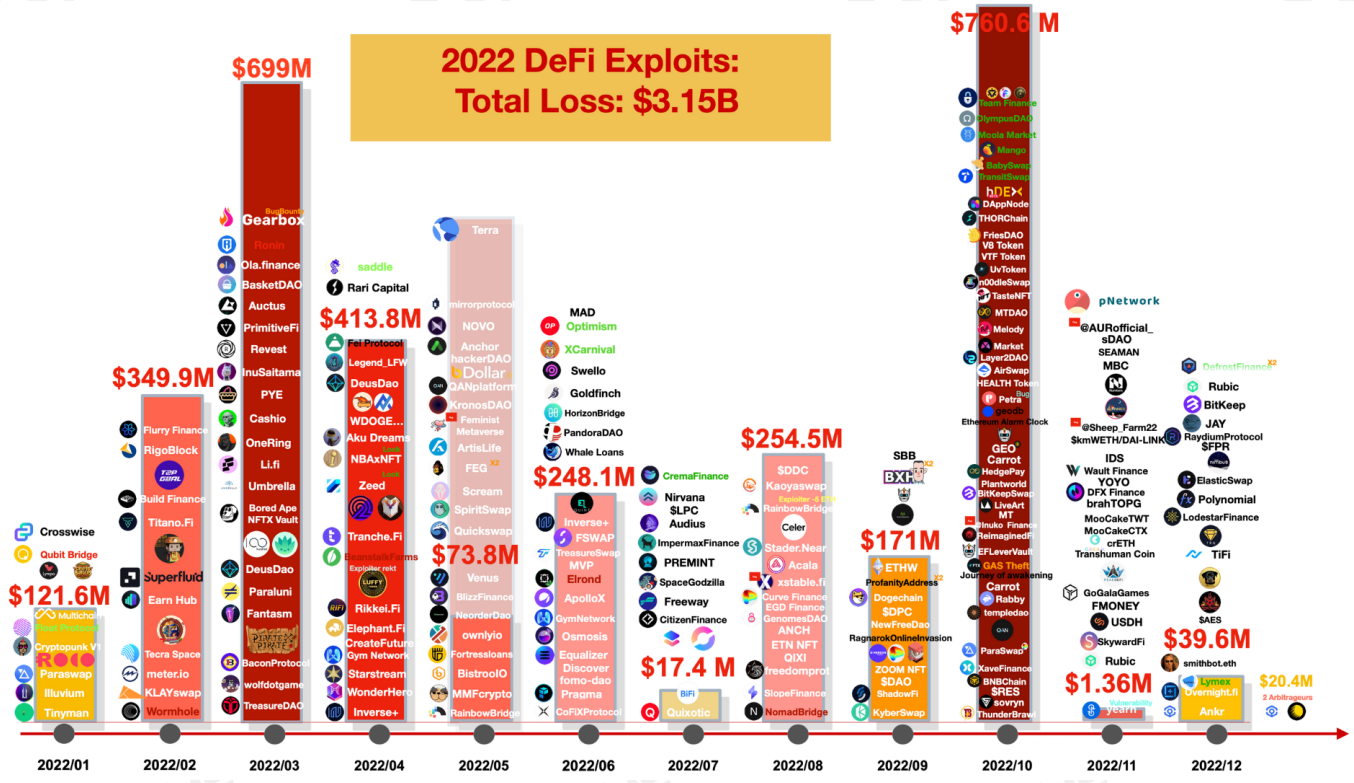


图17 2022年 DeFi 安全事件全览图

截至2022年12月31日，2022年 DeFi 安全事件达到 671 起（未计入 Terra）（注：DeFi 安全事件包含 DeFi 黑客攻击和 RugPull），损失超 36 亿美元。其中有 13 起安全事件中的白帽攻击者归还部分或全部被盗资金，不计入白帽攻击的 DeFi 安全事件被盗资金损失为 34.6 亿美元。从数量上来看，较2021年同比增长了 2 倍，损失金额翻了一番。

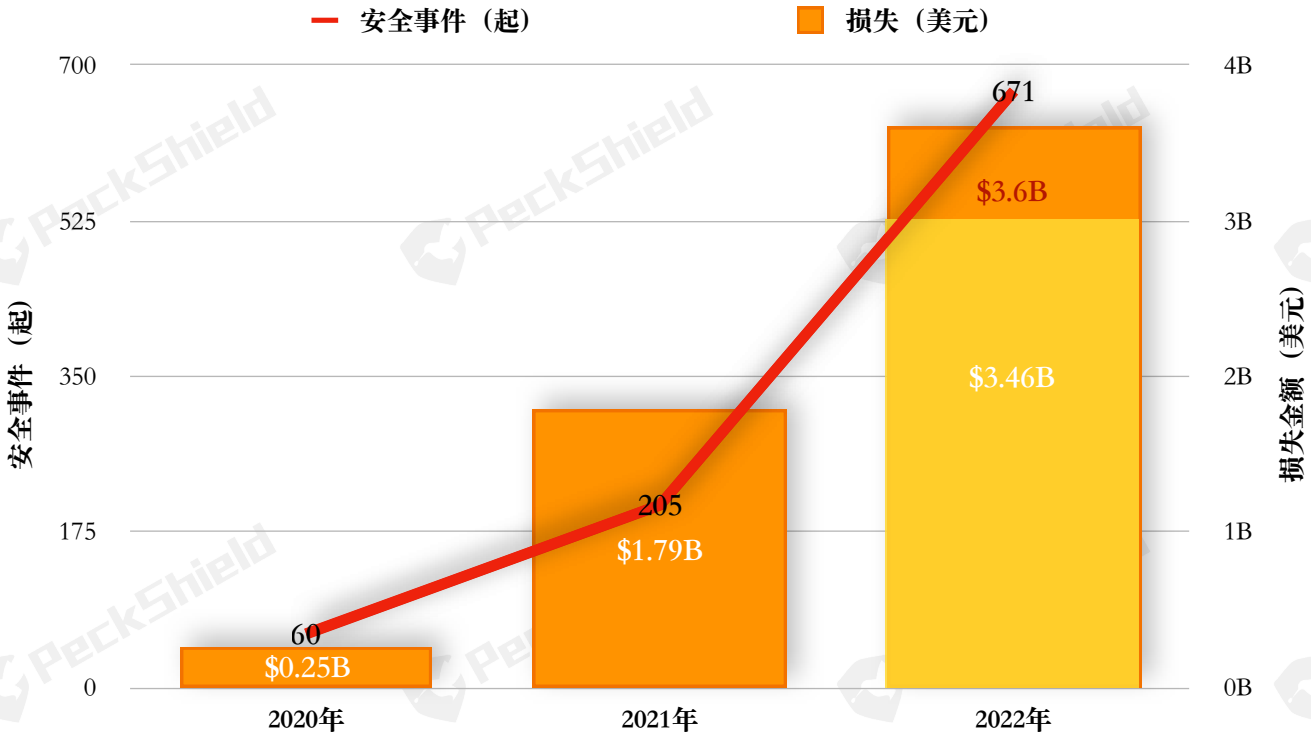


图18 近三年 DeFi 安全事件数量和损失对比

2022年发生的 DeFi 安全事件中，37%（251起）源于攻击者利用 DeFi 协议自身（外部或内部）存在的漏洞套利或攻击，损失金额约 30 亿美元，占 DeFi 安全事件总损失的 87%；63%（420起）则源于 RugPull，造成损失约 4.57 亿美元，占 DeFi 安全事件总损失的 13%。

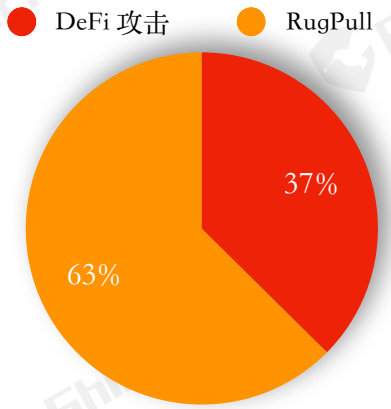


图19 DeFi 黑客攻击和 RugPull 数量对比

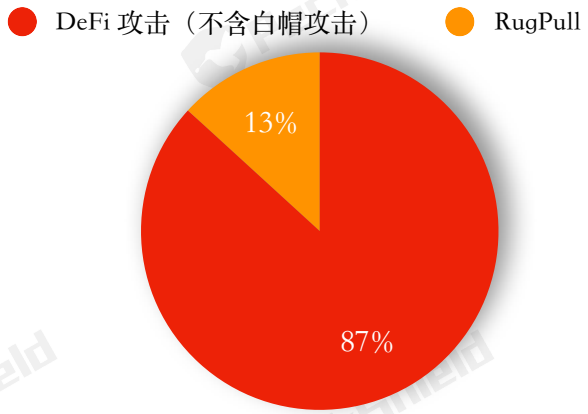


图20 DeFi 黑客攻击和 RugPull 损失对比

2022年 DeFi 领域发生的 RugPull 共计 420 起，损失金额 4.57 亿美元，占 DeFi 安全事件总损失的 13%，较2021年 DeFi 领域 RugPull 损失翻了一番。2022年 RugPull 事件不仅在 DeFi 协议细分领域频发，NFT 领域也出现 RugPull 的迹象。

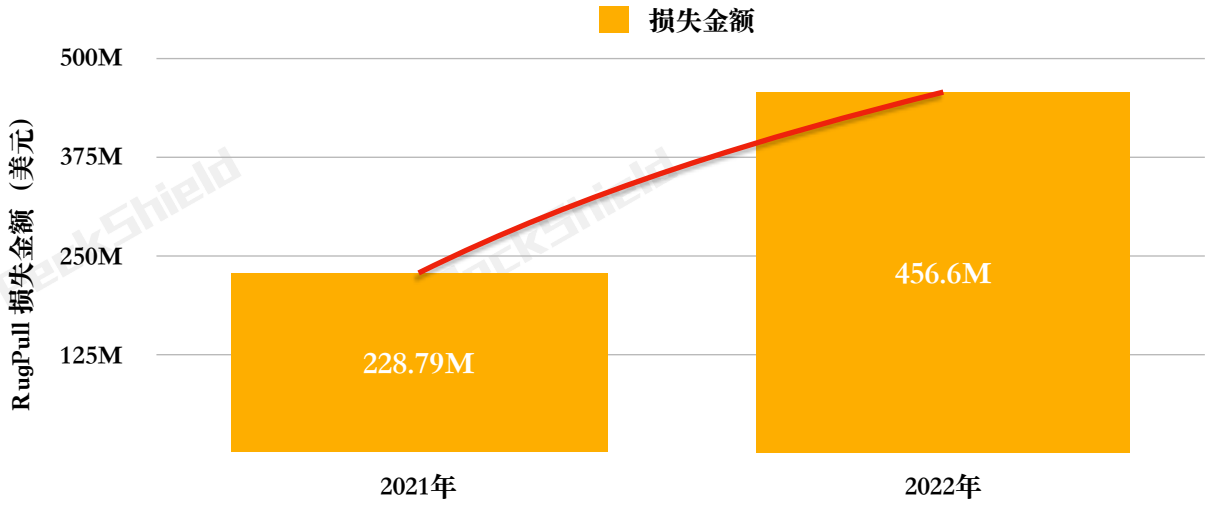


图21 近两年 DeFi 领域 RugPull 损失金额统计

从数量上看，RugPull 这种「软跑路」的方式在熊市发生的频率仍高企，特别是在市场挤泡沫的过程中，资本处于观望状态，在资金链紧张甚至断裂的情况下，这种低成本的主观作恶情况发生频率呈高发态势。

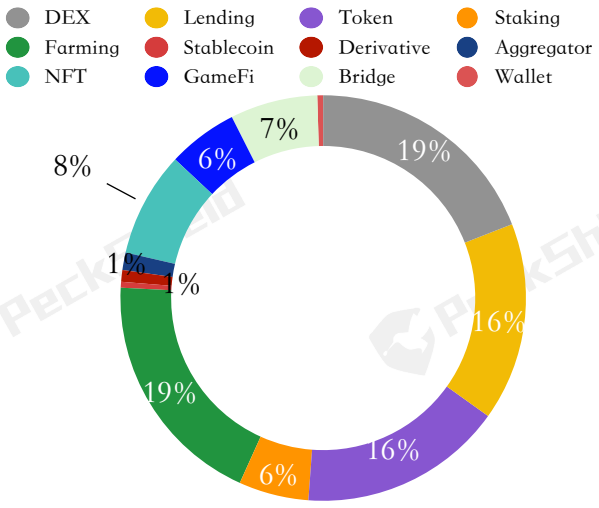


图22 各类别 DeFi 安全事件数量分布

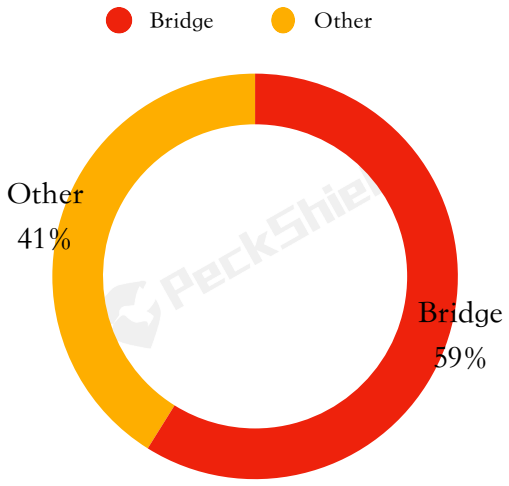


图23 各类别 DeFi 安全事件损失分布

如图22和图23，DeFi 各细分领域安全事件的数量和损失所示，15 起跨链桥安全事件造成损失 19.2 亿美元，占比达 59%。虽然跨链桥遭到攻击的频率较其他领域，例如 DEX、挖矿

（下称“Farming”）、借贷（下称“Lending”）等协议低，但是一旦跨链桥遭到攻击，对整个 DeFi 生态都会造成极大的冲击。

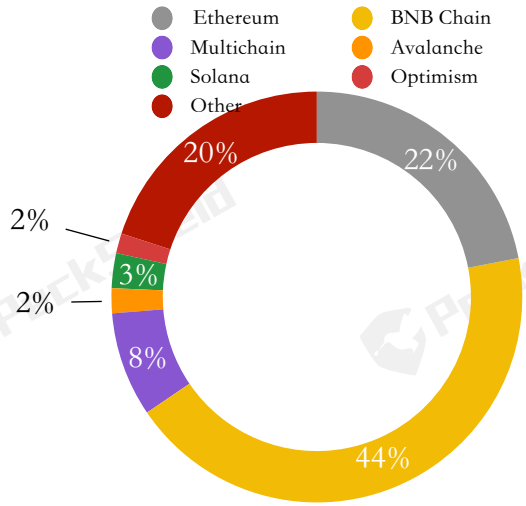


图24 各链上安全事件数量分布

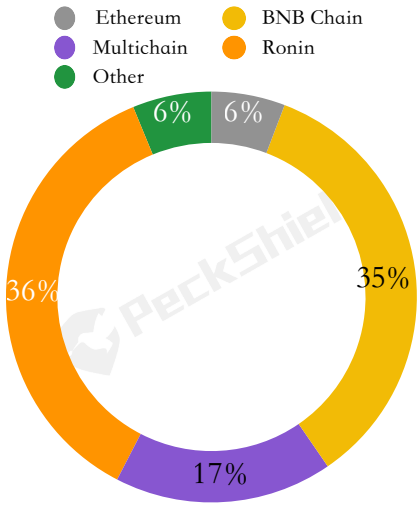


图25 各链上安全事件损失分布

如图24，各链生态上所发生的安全事件所示，2022年 DeFi 安全事件发生在以太坊和 BNB Chain 上的频率较高，两条链上所发生的黑客攻击占比达到 66%。

如图25，各链生态安全事件造成的损失来看，由于 Ronin Network 遭攻击，黑客劫走 6.24 亿美元，使得 Ronin 链的损失占比达到 36%，位列第一；其次是 BNB Chain，由于 BSC Token Hub 跨链桥被盗 5.86 亿美元，使其整条链上的损失金额占比较大。跨链桥生态为用户提供多条链上桥接资产的服务，因而在其遭到攻击时多链生态就会受到影响，占比达 17%。

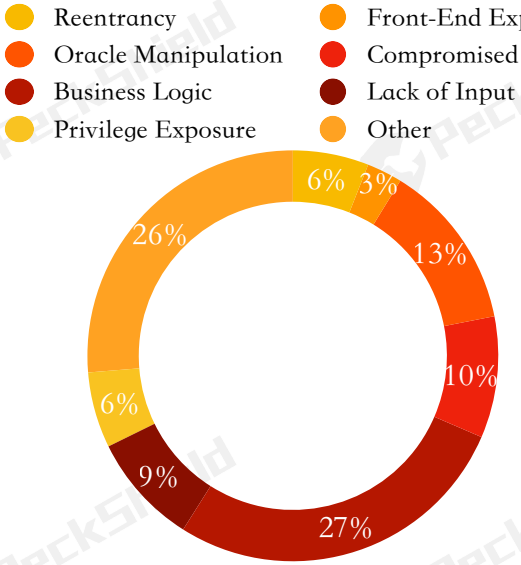


图26 主要攻击手段数量统计

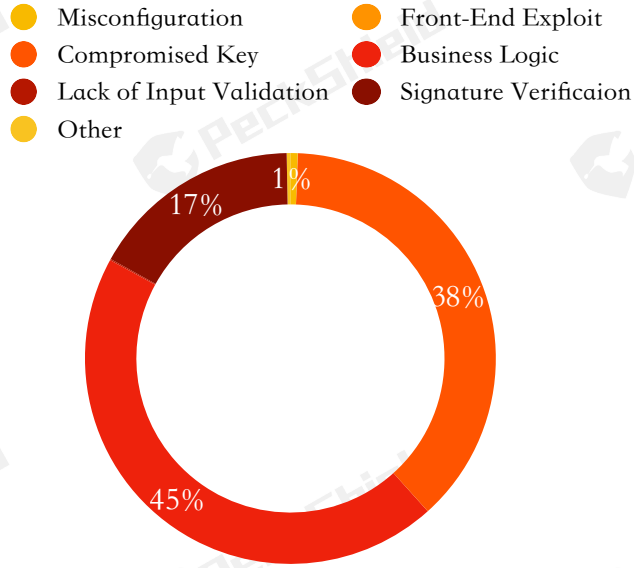


图27 主要攻击手段损失统计

如图26和图27所列出的 DeFi 领域主要攻击手段来看，这 251 起 DeFi 黑客攻击中，主要的攻击手法包括前端漏洞、私钥被盗、重入攻击、预言机操纵、业务逻辑漏洞等。这几种主要攻击手段占比达到 DeFi 黑客攻击总数量的 74%，在总损失中的占比达到 71%。其中 33% 的黑客攻击中利用 FlashLoan（又称“闪电贷”）作为发起攻击的资本。另外，当项目方自身反应不及时且攻击手段较易复制时，容易形成群体性攻击现象。

私钥被盗引入的运营风险发生率为 10%，共计 24 起。因私钥被盗造成的损失大、影响范围广，损失占比达到 38%。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。被劫 6.24 亿美元的 Ronin Network 跨链桥攻击，其攻击者就是使用「被盗的私钥」来签署交易，从而得以伪造交易来盗取资金。

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，技术处于发展阶段。DeFi 协议之间的可组合性，使得 DeFi 协议的复杂性呈指数性增长，除了「乐高性」，协议之间的相互影响也引入了兼容性的风险，而往往安全性差、承载资金量大的一环容易被攻击者盯上。

通过整理、统计和分析2022年 DeFi 安全事件，PeckShield「派盾」发现 DeFi 领域的风险点主要集中在智能合约执行、操作安全以及对其他协议和外部数据的依赖性这四个方面。

智能合约执行风险指的是攻击者利用代码本身存在的漏洞，伺机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。

操作安全风险指的是许多 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（又称“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。

依赖关系风险指的各种智能合约和 DApps 之间互相交互，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。

外部数据风险指的是在 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。

对于 DeFi 领域所存在的安全风险，PeckShield「派盾」建议新 DeFi 合约在上线之前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，需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。在发现异常后，第一时间寻求专业机构定位漏洞根源。此外，项目方引入一定的风控熔断机制，引入第三方态势感知等服务，做到第一时间响应安全风险，及时排查封堵安全攻击，搭建一套完善的加密资产追踪机制。事后需做到查缺补漏、举一反三，完善防御系统。

4.3 NFT 安全事件统计分析

2022年年初爆火的 NFT 市场，受到 DeFi 黑天鹅事件的影响，在总交易量、交易额、市值等数据侧显现出热潮褪却的趋势。但从用户数量、NFT 持有者等数据维度来看，NFT 市场仍处于高活跃度和持续扩张的态势。据 NFTGo 数据显示，自5月起，NFT 总市值持续走低的情况下，仍维持在 200 亿美元的量级。

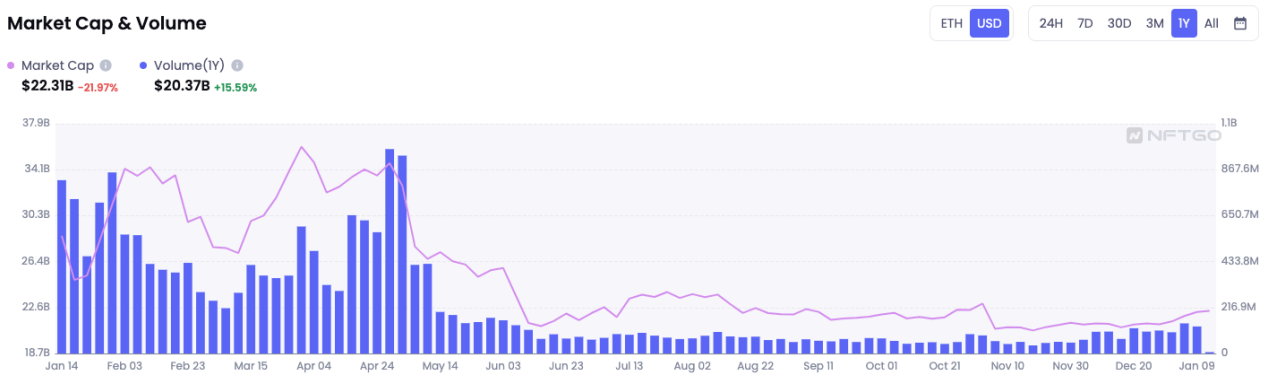


图28 2022年每月 NFT 市场市值与交易量变化（NFTGo）

此外，NFT 版块在近两年迅猛发展。在明星效应、Web2 跨界布局和使用案例多样化方面的推动下，NFT 的价值和流行度持续扩展。2022年 NFT 在元宇宙、票据、游戏等领域的

应用中取得了不俗的效果，涌现出一批以无聊猿（下称“BAYC”）为代表的明星 NFT 项目，它们已经构建具有规模的社群基础、独特的实用程序和具有价值的收藏性，而动辄数十万美元的单价估值，也让它们成为攻击者或作恶者觊觎的目标。

2022年 NFT 安全事件造成经济损失约 4,164 万美元，其中因 NFT 合约漏洞遭到黑客攻击的事件 19 起，造成损失 1,164 万美元 （由于 NFT 市场波动大，本报告中计入的损失金额为在可统计范围内的数额，实际损失可能更大）。

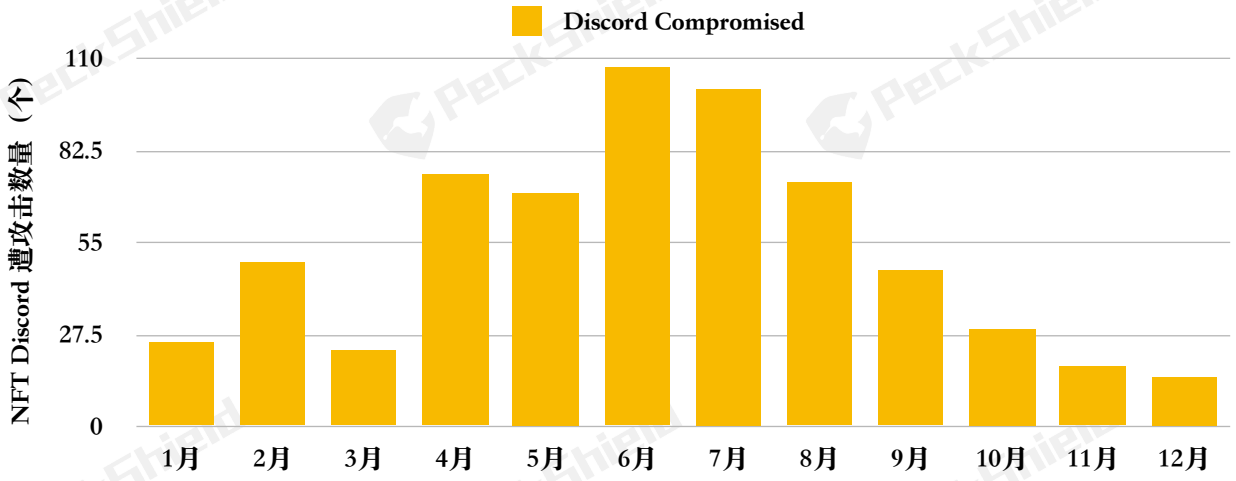


图29 2022年每月 NFT 项目的 Discord 平台遭攻击数量（@NFTherder）

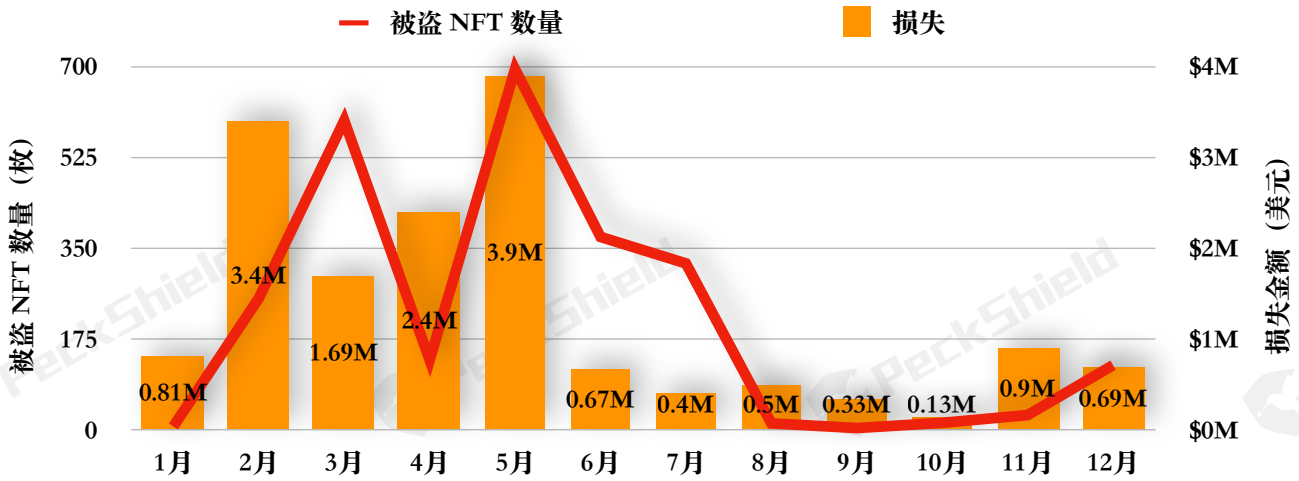


图30 2022年每月 NFT 被盗数量及损失

据不完全统计，2022年至少 617 个 NFT 项目的 Discord 平台遭到不同程度的劫持，造成损失至少 3,000 万美元。其中价值至少 1,582 万美元的 NFT 被盗，NFT 领域的欺诈事件所造成的损失占 NFT 安全事件总损失的 72%。从损失数额和攻击手段来看，诈骗成为 NFT 领域的主要威胁。

NFT 领域的主要诈骗手段包括：钓鱼攻击（又称“Phishing”）、高仿域名和内容的 NFT 钓鱼、NFT 社交媒体攻击 、赠品/空投诈骗、钓鱼邮件。

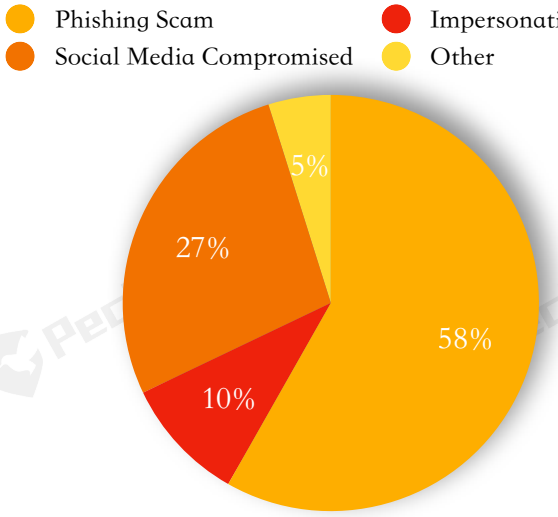


图31 主要欺诈手段数量占比

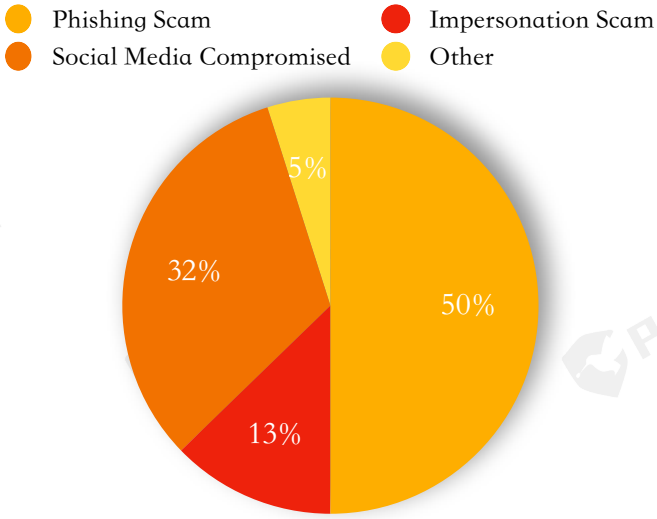


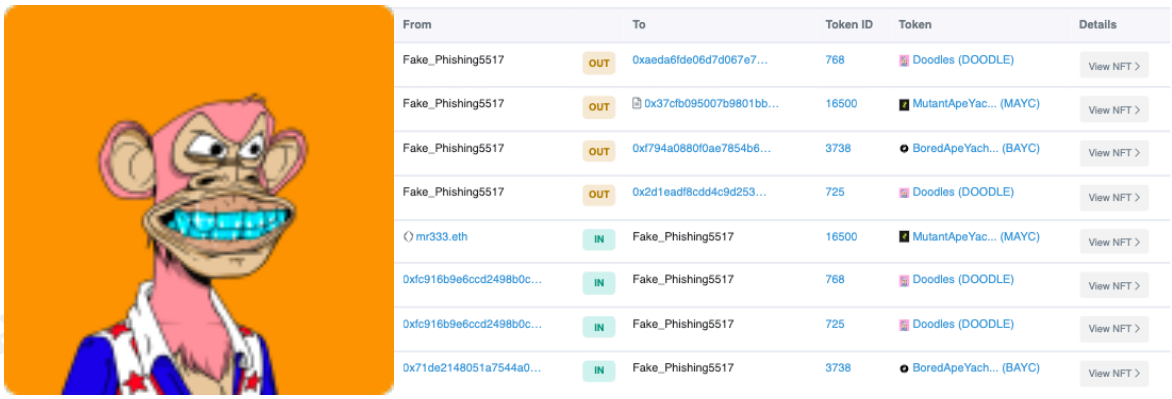
图32 主要欺诈手段损失占比

从数量和损失来看，网络钓鱼占比达 50% 以上。由于钓鱼攻击技术含量和成本低，成为当前骗取用户加密资产的较盛行的方法之一。

2022年2月21日，全球最大的加密资产数字藏品平台 Opensea 遭遇钓鱼攻击。攻击者伪造钓鱼邮件在 Opensea 升级前发送给用户。由于 Opensea 支持盲签，所以用户在不了解自己签署的交易具体内容情况下签名。当用户访问钓鱼邮件中的链接时，钓鱼邮件引导用户对其在 Opensea 上的卖单进行签名，以 0 元的价格将 NFT 发送给攻击者。在此次事件中，至少 32 名用户签署了来自攻击者的恶意交易，导致用户部分 NFT 被盗。攻击者得手后，将攻击所得部分 NFT 出售获利，将至少 1,100 ETH 转入 Tornado.cash。

图33 Opensea 平台遭钓鱼攻击 用户 NFT 被转走示例图

4月1日，华语歌手周杰伦在社交媒体平台上发文称[13]，自己此前获赠的 BAYC #3738 因钓鱼被盗。



From		To	Token ID	Token	Details
Fake_Phishing5517	OUT	0xaeda6fde06d7d067e7...	768	Doodles (DOODLE)	View NFT >
Fake_Phishing5517	OUT	0x37cfb095007b9801bb...	16500	MutantApeYac... (MAYC)	View NFT >
Fake_Phishing5517	OUT	0xf794a0880f0ae7854b6...	3738	BoredApeYach... (BAYC)	View NFT >
Fake_Phishing5517	OUT	0x2d1eadf8cdd4c9d253...	725	Doodles (DOODLE)	View NFT >
mr333.eth	IN	Fake_Phishing5517	16500	MutantApeYac... (MAYC)	View NFT >
0xfc916b9e6ccd2498b0c...	IN	Fake_Phishing5517	768	Doodles (DOODLE)	View NFT >
0xfc916b9e6ccd2498b0c...	IN	Fake_Phishing5517	725	Doodles (DOODLE)	View NFT >
0x71de2148051a7544a0...	IN	Fake_Phishing5517	3738	BoredApeYach... (BAYC)	View NFT >

图34 周杰伦被盗 BAYC NFT 链上流转图

对社交媒体的攻击是 NFT 领域常见的钓鱼手段之一。通过劫持项目方 Discord、Instagram、Twitter 等社交平台服务器，控制创始团队成员账号作伪装，利用机器人发布虚假链接，窃取用户的加密资产或 NFT。这种攻击在受追捧的 NFT 项目 Free Mint 期间发生频率较高。

4月25日，BAYC 官方 Instagram 社交账号被黑[14]。据 BAYC 称，攻击者通过虚假空投发布了一个指向仿冒 BAYC 网站的欺诈链接，并诱导用户签署「safeTransferFrom」交易，将用户链上资产转移到诈骗者的钱包中。

攻击者盗取了 765.3 ETH，涉及 BAYC、MAYC、BAKC、CloneX 等 91 枚 NFT。攻击者已出售 23 枚 NFT，并获利 240 万美元。此外，他们向乌克兰 Crypto Donation 捐赠了价值约 1.6 枚 ETH，并将被盗的 ETH 转移到 CEX。

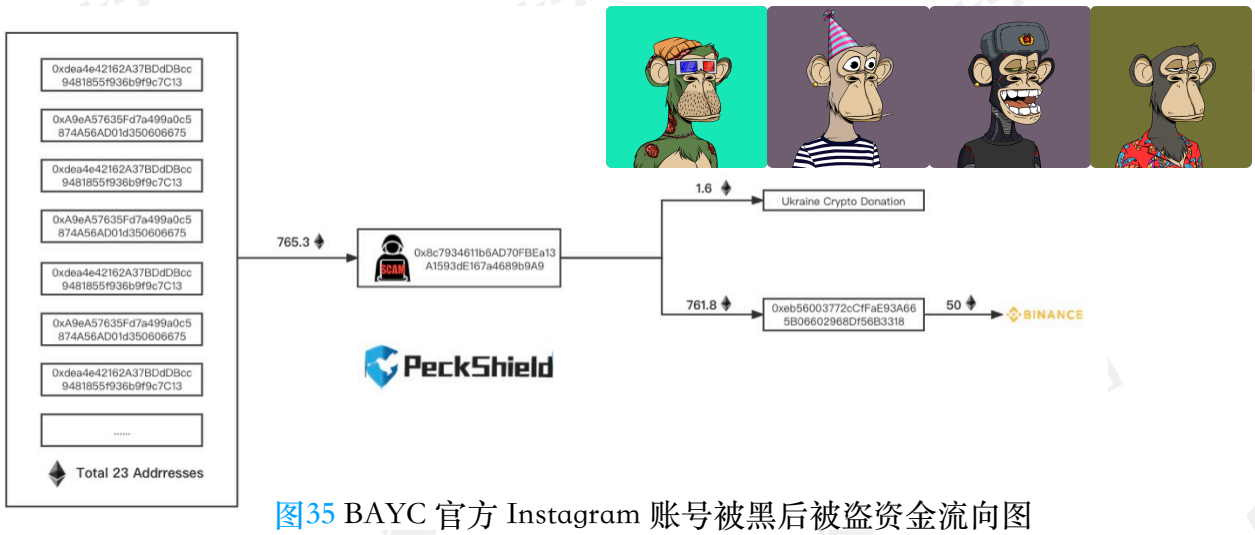


图35 BAYC 官方 Instagram 账号被黑后被盗资金流向图

高仿域名和内容的 NFT 钓鱼，即伪造 NFT 项目官网 UI 界面，诱骗用户连接钱包之后，点击「Mint」按钮进行铸币，用户点击之后会向虚假的项目方地址转账，但是并不会收到对应的 NFT，此类骗局利用投机者 FOMO 的心态骗取加密资产和 NFT。

另外，攻击者将恶意软件转换成恶意空投，利用链上收件人无法拒绝空投的属性，诱导用户访问钓鱼网站，同时对钓鱼网站的黑地址进行授权，继而窃取用户钱包中的加密资产。

针对频遭钓鱼攻击的 NFT 安全问题，PeckShield「派盾」提出以下几点建议：第一，用户的私钥或助记词要用物理方式备份，永不触网。第二，仔细甄别邮件及网站的网址，尽量从官网或项目官方推特或 Discord 等社交平台进入项目官网，同时谨慎对待授权，不要在一些小项目或者所谓的「免费」领取 NFT 的网站上对自己的钱包进行授权。第三，定期清理授权项目。在对存放 NFT 的数字钱包进行授权的时候，一定要确定授权的种类和限额，避免被无良项目卷走资产。同时，要定期清理授权的项目，在进行授权之前再三核对合约地址，对来源可疑智能合约绝不授权。第四，应用市面上的防钓鱼工具。

4.4 跨链桥安全事件统计分析

2022年受到熊市的影响，公链的格局开始出现动荡，但跨链桥仍是多链并存市场格局下不可或缺的「通信」刚需。虽然跨链桥 TVL 呈现下降趋势，但其数量和应用场景的需求仍在持续增长，并且扩张至 NFT 等多领域。

虽然跨链桥为 Web3 生态系统释放了创新性与多样性，随着该赛道的蓬勃发展，其承载的资金量也在增长，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，目前跨链桥面临的最大挑战仍是安全问题。

2022年发生的跨链桥安全事件约为 15 起，损失约 19.2 亿美元。从数量上来看，同比增长 33%，损失金额增长 3,740%（不计入白帽攻击），占2022年 DeFi 生态被盗金额的 59%。

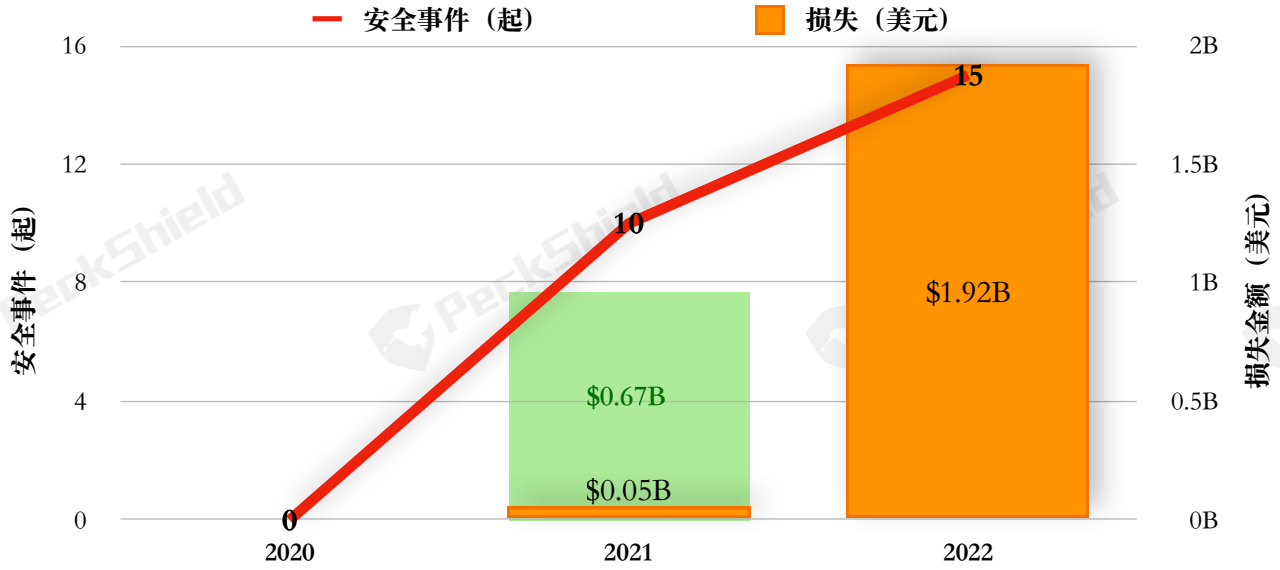


图36 近三年跨链桥安全事件数量和损失对比

2022年发生在跨链桥上的安全事件频率较2021年增幅不大，但纵观2022年跨链桥安全事件不仅单笔损失巨大，被盗资金动辄达到数亿美元，而且波及影响甚广。

跨链协议屡遭攻击者光顾，究其缘由，除了跨链桥生态发展时间尚短（2021年初跨链桥生态初现雏形），再者就是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。

这些跨链桥安全事件再一次为该生态敲响了警钟，解决多链流通安全性将成为立足该赛道的核心竞争力。

日期	跨链协议	攻击原理	损失金额
2022-01-18	Multichain（Anyswap）	Lack of Input Validation	$1.8M
2022-01-28	Qubit Bridge	Business Logic	$80M
2022-02-02	Wormhole Bridge	SignatureValidation	$320M
2022-02-05	Meter Bridge	Lack of Input Validation	$4.3M
2022-03-30	Ronin Network	Compromised Key	$624M
2022-05-01	Rainbow Bridge	N/A	Exploiter lost 5 ETH
2022-05-19	QANplatform	Business Logic	$355K
2022-06-23	Horizon Bridge	Compromised Key	$100M
2022-08-02	Nomad Bridge	Business Logic	$190M
2022-08-18	Celer Bridge	Front-end Exploit	$235K
2022-09-18	ETHW Bridge	Signature Replay	200 ETHW
2022-10-06	BSC Token Hub	Business Logic	$586M
2022-10-11	QANplatform	Compromised Key	$1.16M
2022-10-18	THORChain	Network Halts	-
2022-11-04	pGALA (BNB Chain)	Misconfiguration	$10.8M

图37 2022年跨链桥安全事件汇总

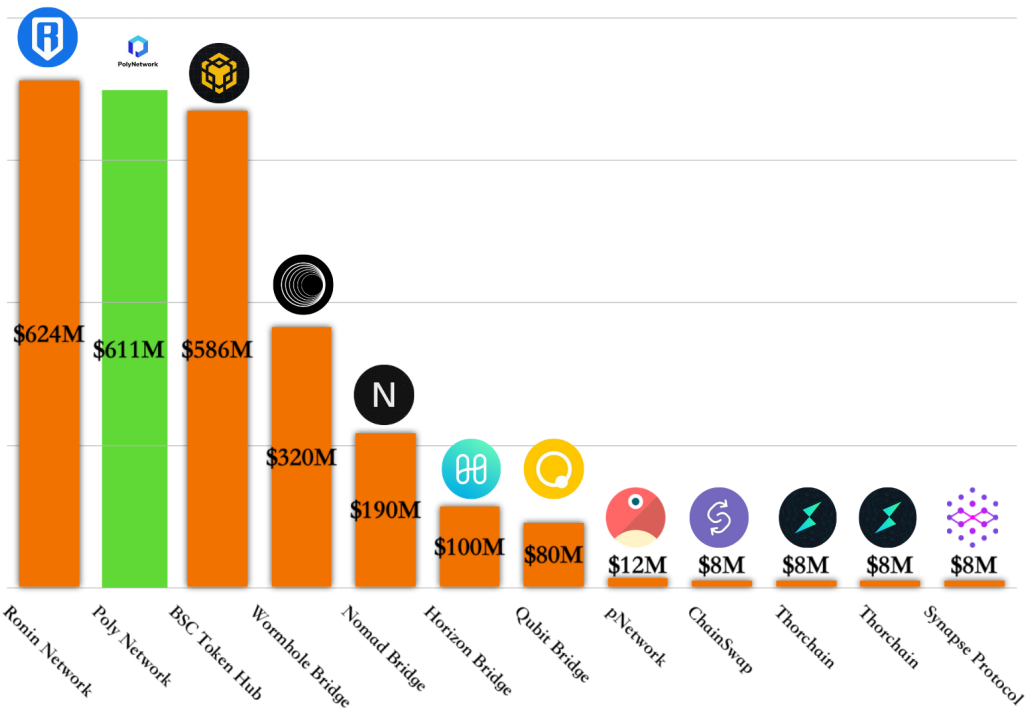


图38 近三年跨链桥重大安全事件概览

五、Web3 行业典型事件回顾

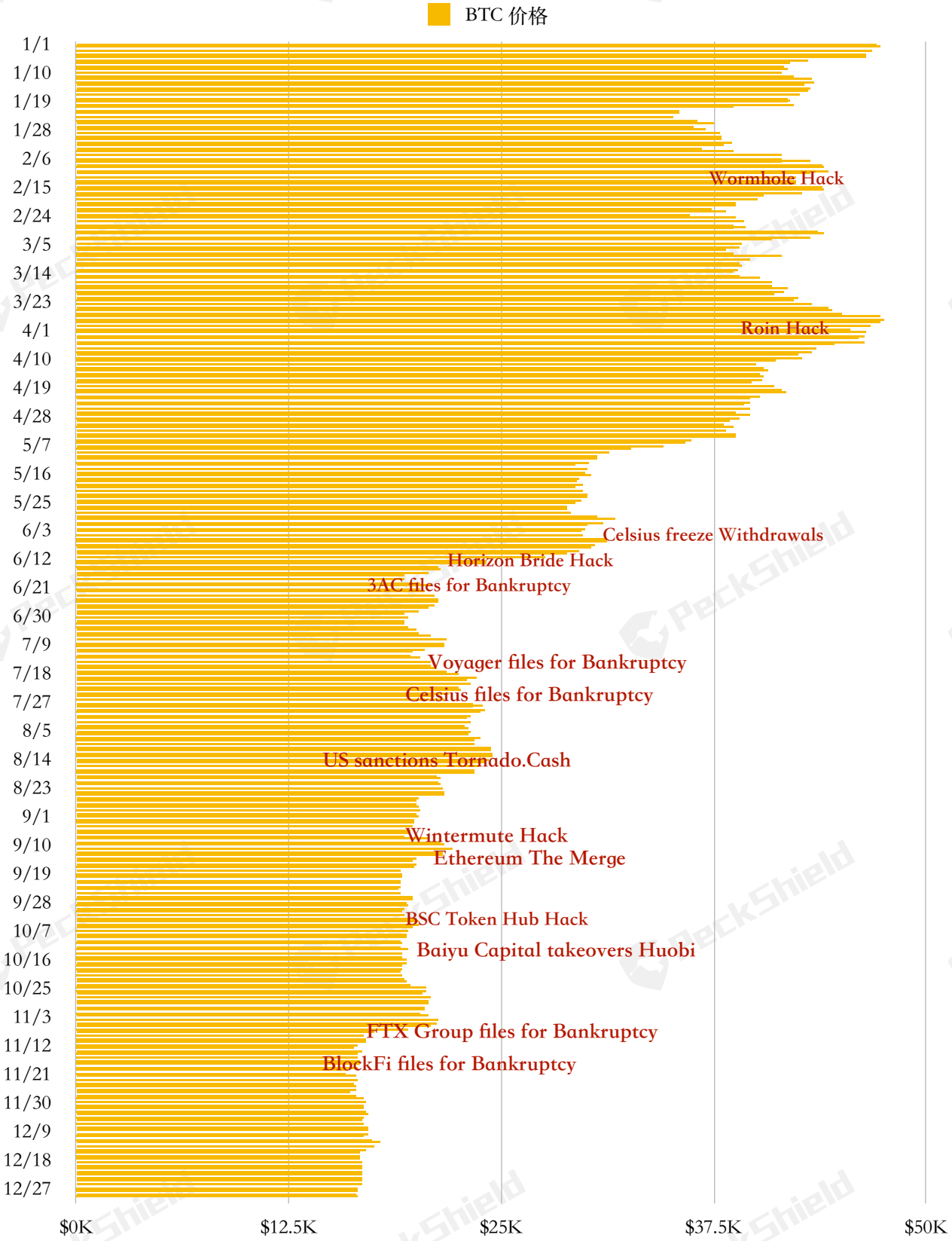


图39 2022年 BTC 价格走势与相关大事记一览图

5.1 市值 400 亿 Terra 算稳王国崩塌

在全球经济动荡的环境背景下，攀升的市场恐慌情绪蔓延至 Web3 行业，主流加密资产的价值一路下跌，以算稳创新者问世的 Terra 生态的崩塌成为加速 Web3 行业跌入寒冬的导火索之一。

图40 Terra 算稳王国崩塌事件始末

图41 稳定币 UST 脱锚（CoinMarketCap）

图42 Anchor 协议 TVL 走势图（DefiLlama）

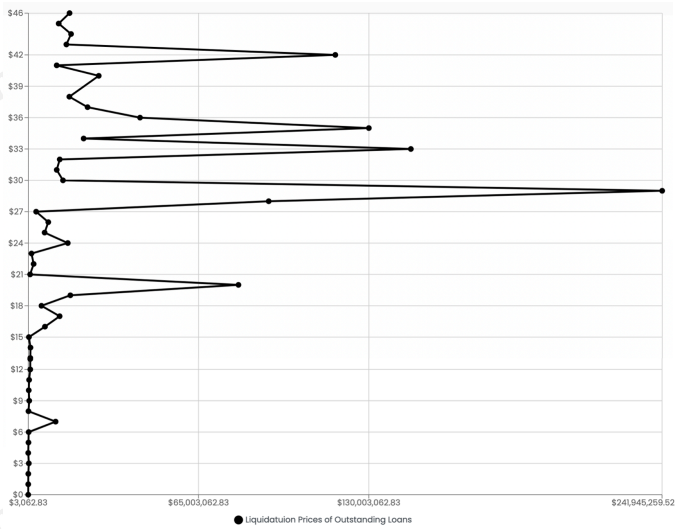


图43 LUNA 清算价格图（DeFi Alpha）

5月10日，Terra 生态的原生算稳 UST 因资本围剿和债务危机，出现严重脱锚事件，最低跌至 0.6 美元，随后倾泻至趋于归零，Terra 链 TVL 急剧萎缩。

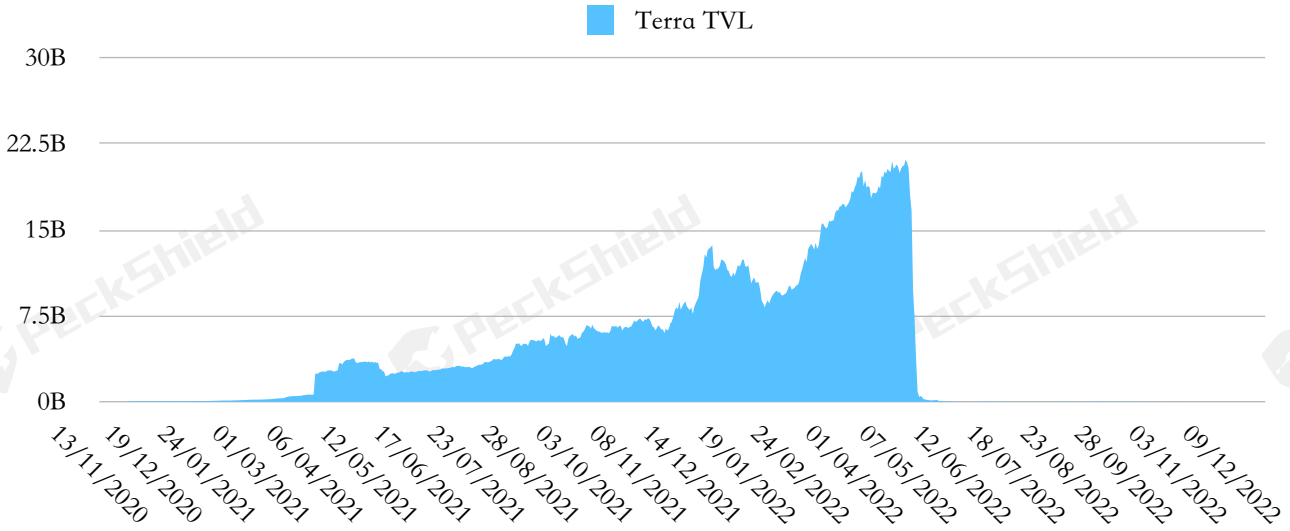


图44 2020年至2022年 Terra 链 TVL 走势图（DefiLlama）

市值近 400 亿美元的 Terra 生态在短短两天内蒸发。Terra 的历史性崩盘，对整个 Web3 生态产生了巨大的涟漪效应。除了多个新兴稳定币出现了不同程度的脱锚，随着恐慌情绪的不断攀升，甚至连稳定币龙头 USDT 也出现了短时小幅脱锚的状况。在2021年急速扩张的态势下，Terra 曾跃升至第二大公链生态，其算稳 UST 更是作为跨链资产在多链布局，它的崩盘触发了对其他各个生态不同程度的清算和连带影响。

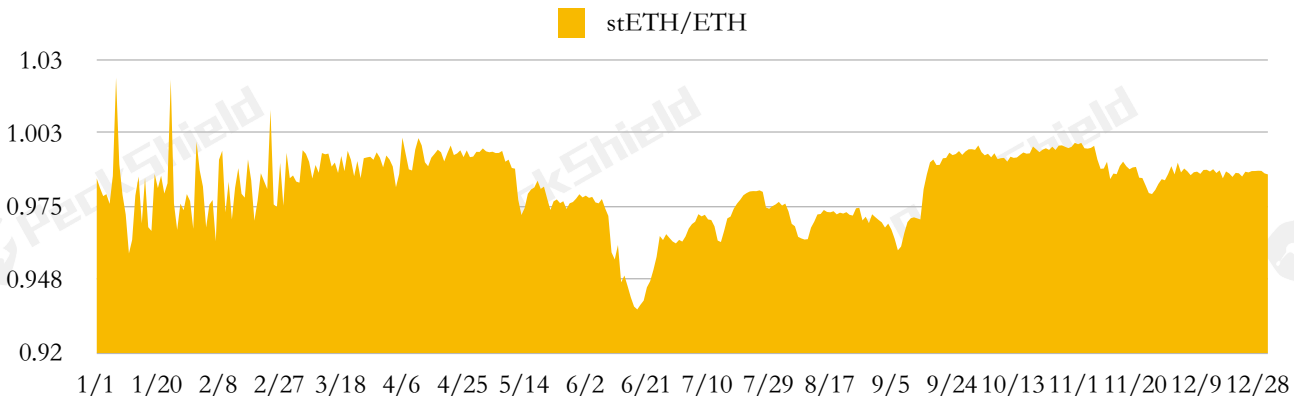


图45 2022年每日 stETH/ETH 转换率波动图

链上数据显示，在此期间在去中心化交易所 Curve 上，累计超过 16.9 万枚 stETH 被卖出，Curve 池短时流动性衰竭导致 stETH 出现折价[15]。

5.2 循环加杠杆，市场下挫触发 Celsius 和 3AC 遭清算

根据 Celsius 咨询合作伙伴 Kirkland & Ellis 提交给纽约南区美国破产法院的文件，Celsius 持有 43 亿美元的资产和 55 亿美元的负债，即存在 12 亿美元的缺口。其中非用戶资产仅为 7.8 亿美元。

Celsius 将其大量客户资金（7.5 亿美元的信贷额度）投资于自身的采矿业务。截至2022年5月底，有 5.76 亿美元未偿还。在市场下行的情况下，其所拥有的矿机的价格出现大幅折价。

2021年，以太坊 2.0 的质押服务提供商 StakeHound 丢失私钥导致 Celsius 损失了超过 38,000 枚 ETH[16]，价值超 7,000 万美元。此外，Celsius 还在 BadgerDAO 被盗事件中损失了约 2,100 枚 BTC 和 151 枚 ETH，价值超 5,000 万美元。

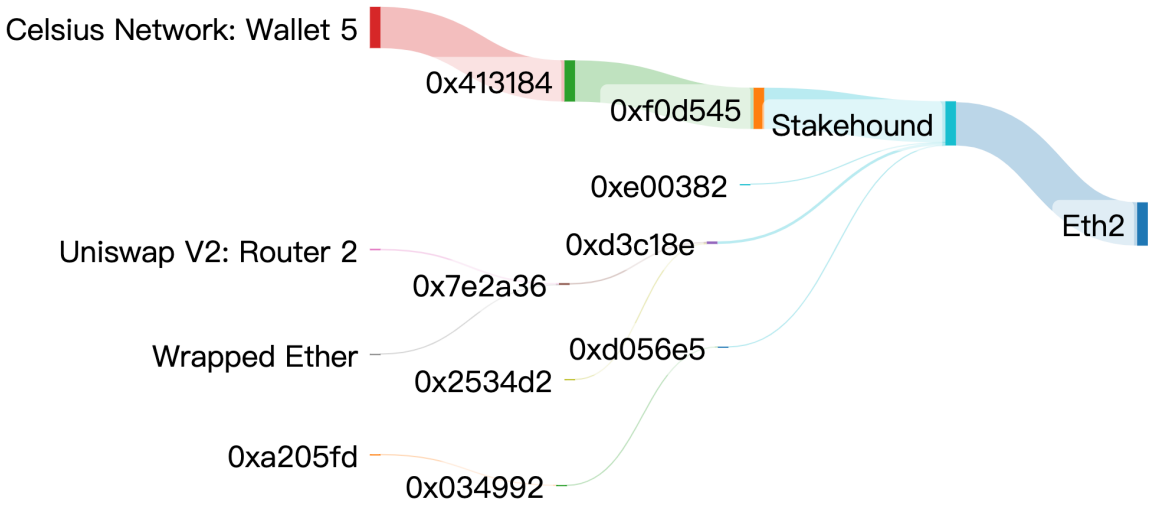


图46 Celsius 将 ETH 转入 StakeHound 资金流转图

Celsius 还持有 UST，虽然在 Terra 崩盘事件中撤回大部分 UST，仍损失 1,580 万美元。受到 Terra 崩盘的市场压力，用户在 5 天内提现超过 10 亿美元造成 Celsius 挤兑。

2022 年 6 月 13 日，Celsius 宣布暂停所有提款、交易和转账。

3AC 也受到 Terra 的影响。据 Terra 研究论坛成员 FatMan 表示，3AC 曾以 5.596 亿美元的价格购买了 1,090 万枚 LUNA（Terra 的平台币）。LUNA 价格倾泻后，3AC 所持 LUNA 价值仅 670.45 美元。

此外，3AC 在2022年年初大规模建仓 ETH，并在 Lido 专为 stETH 质押。在 Celsius 的清

算压力下，3AC 将多枚 stETH 折价换为 WETH，然后全部抛售换做 DAI 以偿还债务。

除了 stETH 外，3AC 还将大量贷款用于购买灰度比特币信托基金（又称“GBTC”）的仓位。自2021年以来，GBTC 的价差便持续恶化，负溢价一度扩大至 -50% 以上，这也使得 3AC 这部分资产严重缩水，面临清算风险。

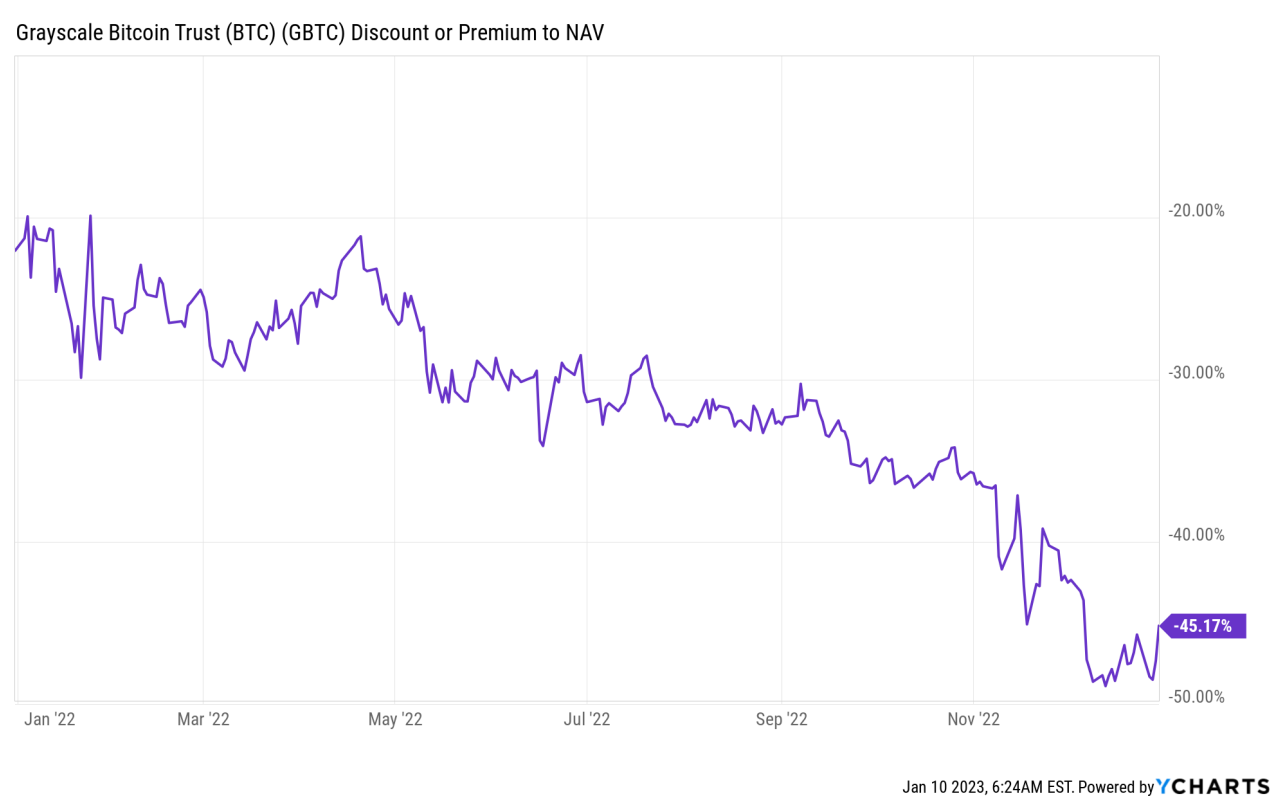


图47 GBTC 负溢价走势图（YCHARTS）

主流加密资产的下跌也带来了杠杆头寸的连环清算。许多 CeFi 借贷公司作为 3AC 撬动杠杆的资金来源，也都受到巨大的影响，或等待救助或面临破产，例如 Voyager、BlockFi。

5.3 FTX 崩塌，上演加密雷曼时刻

2022年11月，全球第二大交易所 FTX 宣告破产，交易所格局再次洗牌。

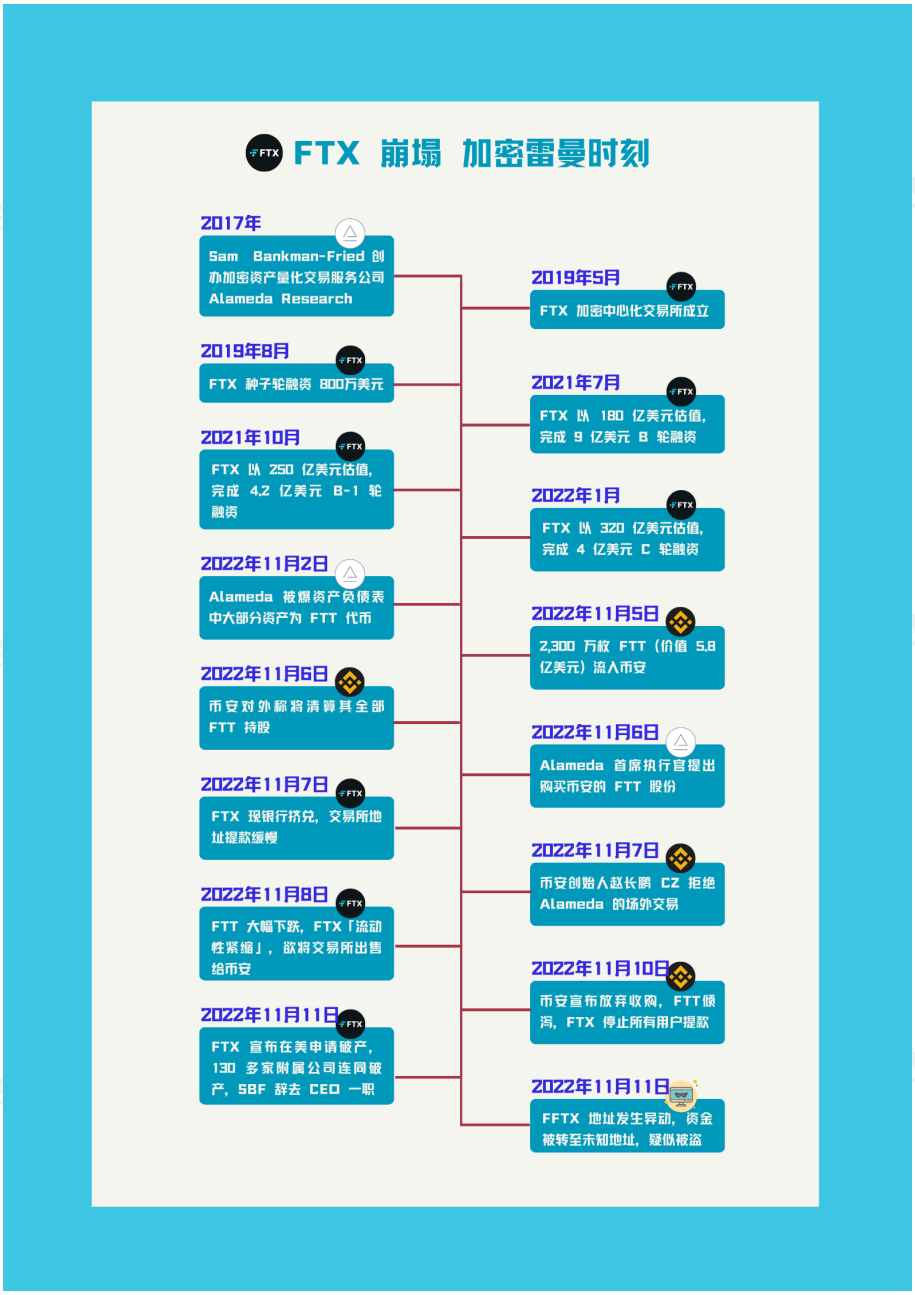


图48 FTX 事件始末

11月2日，加密资产量化交易服务公司 Alameda Research 被爆资产负债表中大部分资产为 FTX 平台币 FTT 引发市场对 FTT 的流动性质疑，市面上出现巨鲸用户开始出售 FTT。

11月6日，FTX 的提款需求激增至平日的 25 倍，短短几天内 FTX 的资金净流出量达到了 50 亿美元，其中包括至少 20,000 枚 BTC 以及大量稳定币。

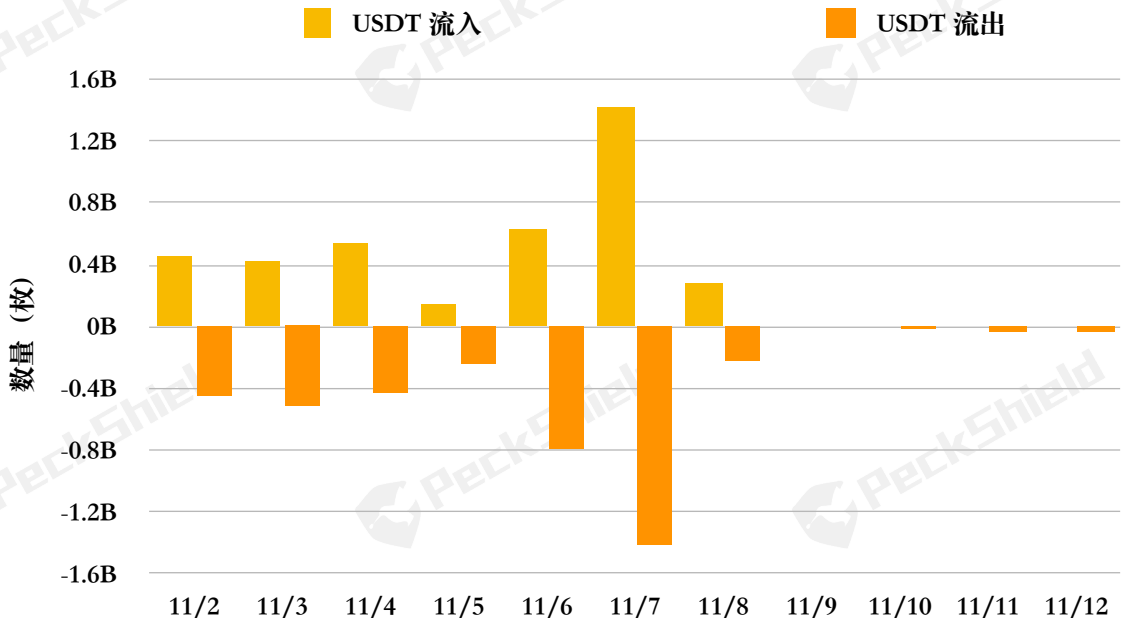


图49 2022年11月 FTX 上 USDT 的流入流出量

伴随流动性蒸发的还有 FTX 相关加密资产价格的暴跌。FTX 持有的流动性低的加密资产，包括 FTT 的总市值大幅缩水约 2/3，由 150 亿美元跌至 50 亿美元。在遭遇挤兑和资产减值后，FTX 陷入流动性危机，FTX 交易所宣布停止用户提款。

图50 FTT 价格走势图（CoinMarketCap）

值得注意的是，在出金需求增长激增期间，有用户发现巴哈马用户仍能从 FTX 巴哈马用户侧提款，成为彼时用户出金的突破口。巴哈马用户在 FTX 的 NFT 市场上架一些 NFT，其

他要出金的用户事先私下与该用户协商，再用自己被困的资产从 NFT 市场买下指定的 NFT，巴哈马用户收到款项后代为提款。在此期间，FTX 的 NFT 市场交易记录出现多笔巨额成交，以及溢价过高的 NFT 挂单。

图51 FTX NFT 市场中价格异常的 NFT 交易订单

11月11日，FTX 宣布在美申请破产，130 多家附属公司连同破产，SBF 辞去 CEO 一职。同一天，FTX 地址发生异动，链上资产被转至未知地址，疑似被盗。

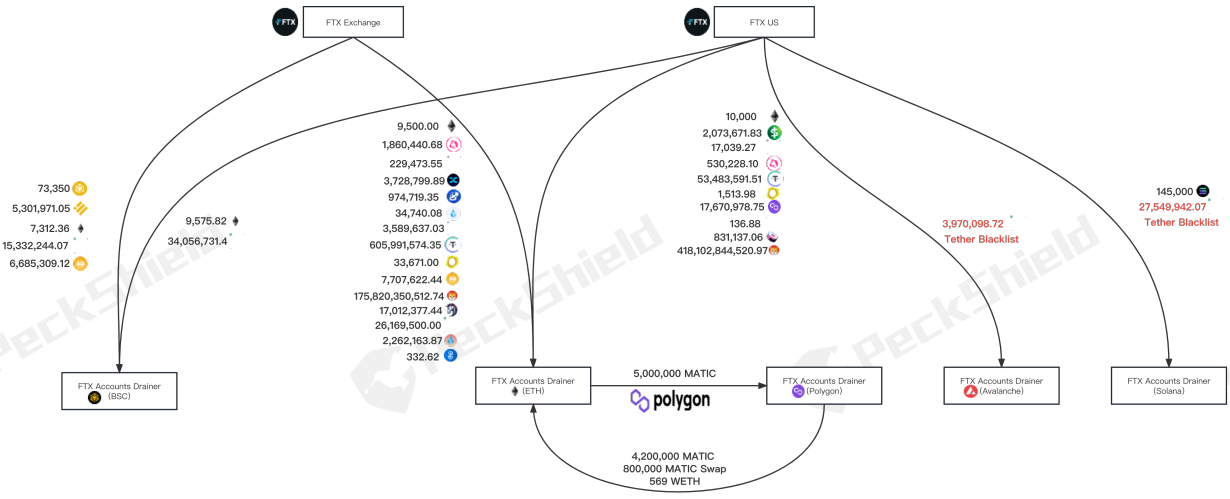


图52 FTX 被盗加密资产链上流转图

伴随 FTX 危机而来的是其他相关企业的相关风险，关联企业业务受到冲击。Genesis 公司在11月11日宣布，该公司在 FTX 上的交易账户中有 1.75 亿美元的锁定资金。区块链金融服务公司 Galaxy Digital 披露了其对 FTX 的 7,680 万美元敞口。对冲基金 Galois Capital 承认

其部分资金滞留在 FTX 上，估计约为 1 亿美元。加密资产借贷公司 BlockFi 也承认对 FTX 和相关公司实体有重大风险敞口，11月11日该公司限制了其平台上的活动并停止了客户提款，并建议客户不要向其 BlockFi 钱包或利息账户存款。风险投资公司 Multicoin Capital 在 FTX 上冻结了约 8.63 亿美元的加密资产。

5.4 OFAC 制裁 Tornado.Cash，释放 DeFi 监管强信号

2022年8月8日，OFAC 将加密资产混币平台 Tornado.Cash 及其关联的加密资产钱包地址添加到 SDN 名单中。禁止美国公民与该协议或与之相关的任何以太坊地址进行交互，如果与 SDN 名单中的地址进行交互，相关人和实体都或将面临高额罚款和监禁。

这是美国政府首次对智能合约应用进行制裁。这次制裁导致访问 Tornado.Cash 被限制，用户不能访问网站的前端页面。并且像 Infura 和 Alchemy 这样的第三方节点运营商，也宣布停止支持 Tornado.Cash 的相关服务。此外，对 Tornado.Cash 的制裁，还扩展至 Tornado.Cash 的开发者和代码贡献者。

Tornado.Cash 遭制裁，反映出相关监管机构对 DeFi 协议的监管提上日程。随着各国加密资产监管框架的出台和监管政策的落地，可能出台专门针对 DeFi 协议的相关立法，比如欧盟正在试验的 DeFi「嵌入式监管」方案；DeFi 协议反洗钱措施需求增多。

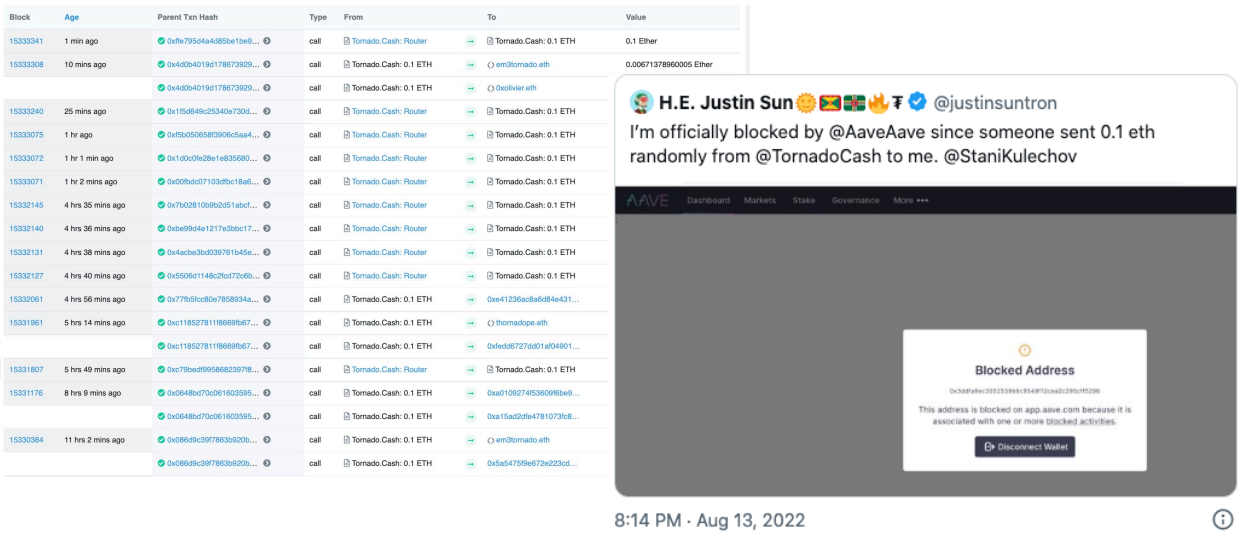


图53 孙宇晨在社交媒体控诉受「投毒」事件影响被 AAVE 协议封禁

值得注意的是，在 OFAC 对 Tornado.Cash 进行制裁后，上演了大规模「投毒」事件。「投毒」指的是通过将经过 Tornado.Cash 混币的小额加密资产发送到用户钱包，大规模「污染」钱包，此举被视为是行业对 Tornado.Cash 制裁的某种反击。

5.5 以太坊里程碑：The Merge

2022年9月15日，以太坊协议从工作量证明过渡到权益证明。合并后，以太坊完成从工作量证明到权益证明的转型，这不仅是一个技术上的更新，更是共识意识形态的转变。The Merge 也被视为以太坊向打造安全、可扩展、去中心化、可持续发展网络迈进的重要里程碑。

从宏观来看，The Merge 使以太坊网络变成强有力的处理层和数据可用性层，作为基础设施为 rollup 提供服务，以及分片奠定基础。从技术上来看，The Merge 意味着于 2020 年上线的 PoS 平行运行信标链将取代 PoW 作为共识层。保持不变的是执行层将继续托管以太坊虚拟机，并验证和广播交易。此外，节点运营商必须同时运行执行层和共识层客户端才能保持在线。The Merge 之后以太坊还将迎来一系列的升级。

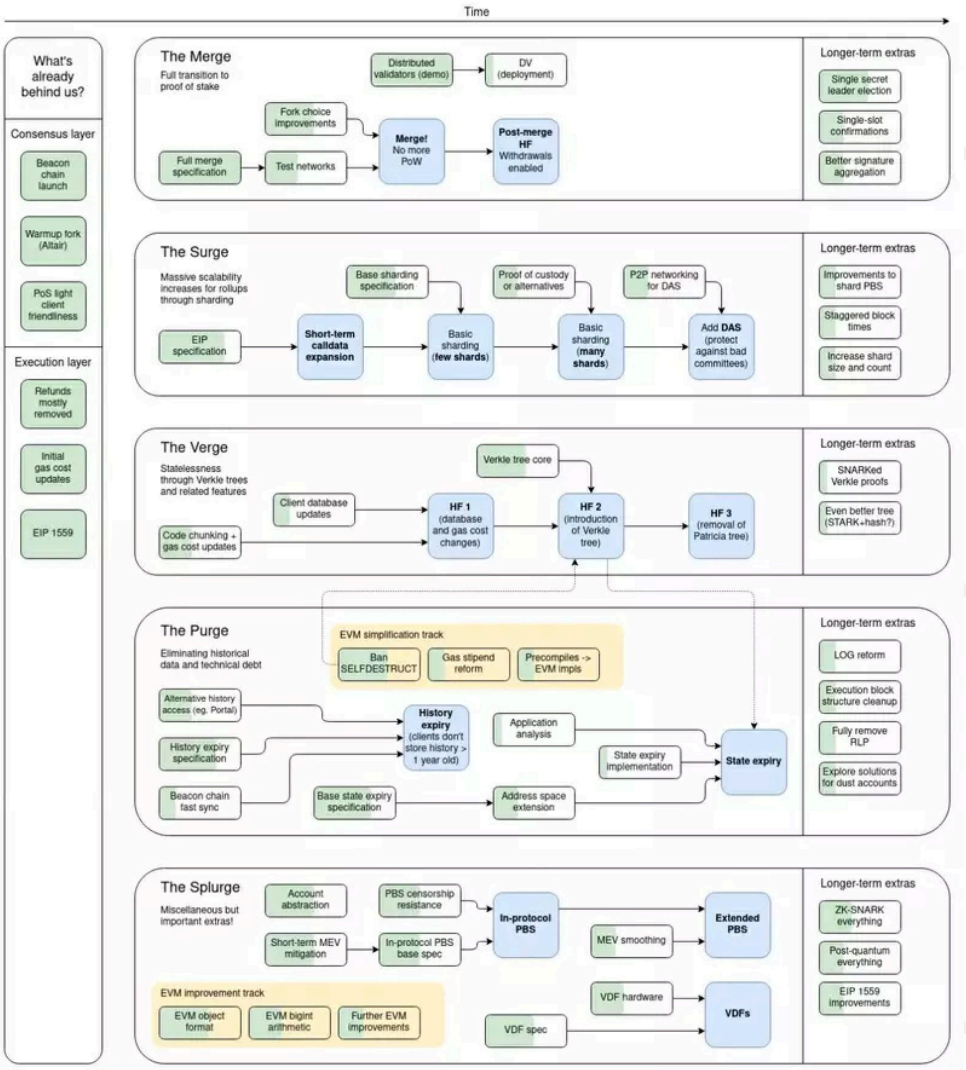


图54 以太坊合并路线图（以太坊联合创始人Vitalik Buterin）

5.6 事发 6 天后才发现，Ronin 被盗 6.25 亿美元

3月23日，链游 Axie Infinity 的以太坊侧链 Ronin Network 宣布遭遇黑客攻击[17]，黑客使用被黑的私钥伪造提款掠走大约 6.25 亿美元，成为迄今为止损失金额最大的一次 DeFi 黑客攻击。

值得注意的是，直到3月29日（攻击发生 6 天后），在用户反馈无法提取 5,000 ETH 后，项目方才发现了此次攻击。该漏洞影响了 Ronin Network 的 Sky Mavis、Axie Infinity 游戏的发行商和 Axie 去中心化自治组织（DAO）的验证节点。

当时，Ronin 侧链由 9 个验证器节点组成，要确认存款或取款，需要五个验证者签名。攻击者设法控制了 Sky Mavis 的四个 Ronin 验证器和一个由 Axie DAO 运行的第三方验证器。尽管 Ronin 使用的验证器密钥方案被设置为去中心化的，但攻击者仍通过无 Gas 费的 RPC 节点发现了一个后门，他们滥用该后门来获取 Axie DAO 验证器的签名。

Ronin Network 被攻击后，其上的 ETH 和 USDC 已从其桥接合约中耗尽。历时半年，Ronin Network 攻击者将所盗资产转入 Tornado.Cash。

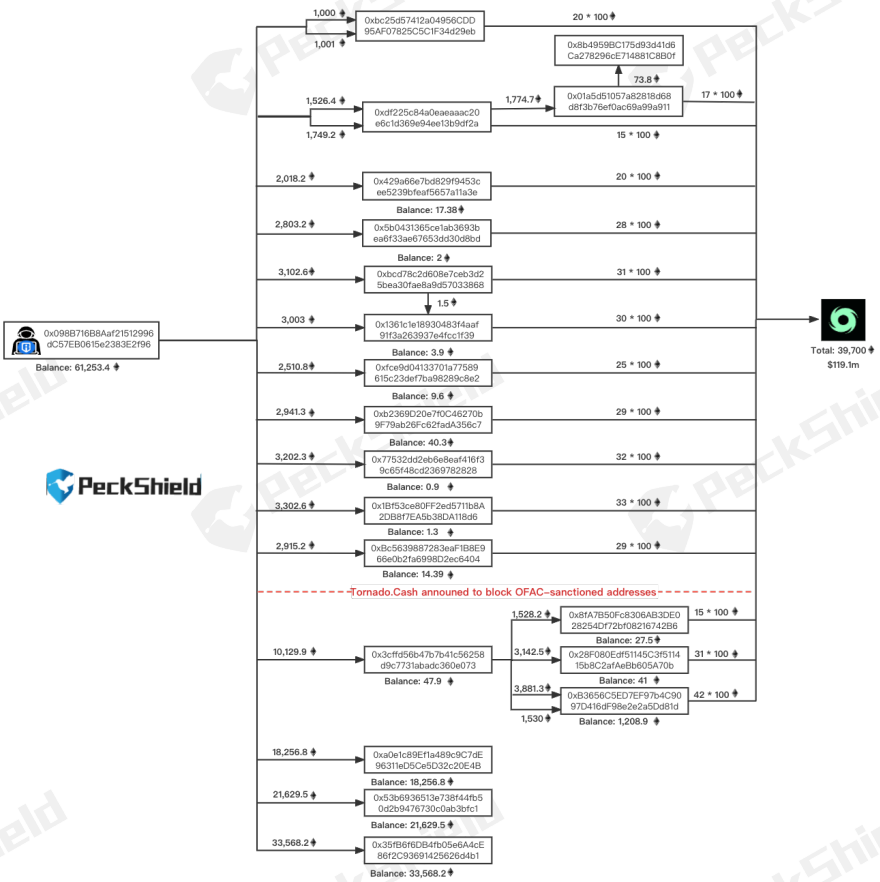


图55 Ronin Network 安全事件被盗加密资产链上流转图

5.7 多空双开操纵 Mango 价格，1 亿美元流动性被撬走

Solana 上的 DeFi 平台 Mango 于10月12日遭到攻击，攻击者通过操纵多个市场的 Mango 代币（下称“MNGO”）现货价格，使衍生品市场的仓位赚进大量收益，再一举将 Mango 金库中的加密资产借出。受此影响，Mango 平台的流动性几乎归零，损失超过 1 亿美元。

攻击者使用两个帐户用来进行攻击，在账户「A」上，攻击者最初使用价值 500 万美元的 USDC 购买了 4.83 亿枚 MNGO，以做空该代币。然后在账户「B」上，攻击者又使用500万美元购买了相同数量的 MNGO，总共使用了 1,000 万美元来有效对冲两个头寸。

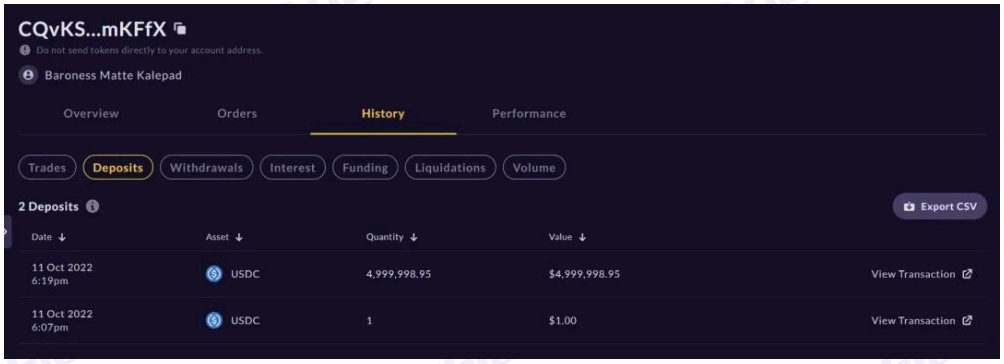


图56 Mango 攻击者创建的 A 账户

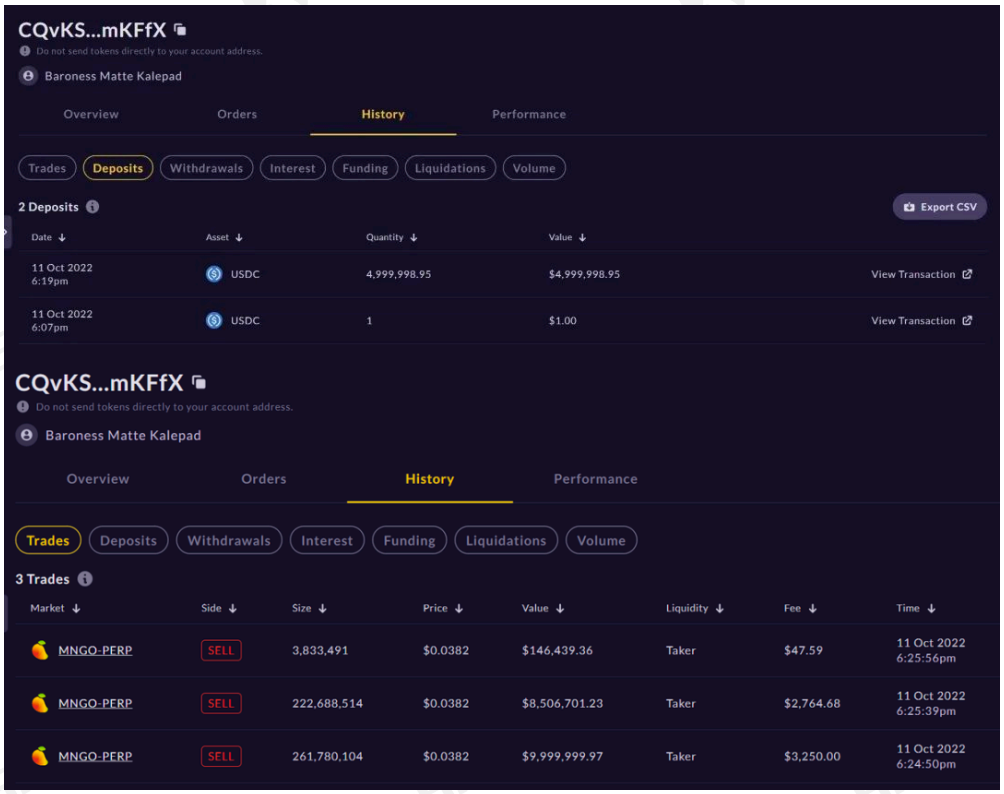


图57 Mango 攻击者创建的 B 账户

然后，攻击者使用更多资金购买现货 MNGO 代币，在 10 分钟内将其价格从 2 美分拉升至 91 美分。由于现货 MNGO 交易量少、流动性低，这使得黑客能够快速操纵价格。

图58 MNGO 价格变化图

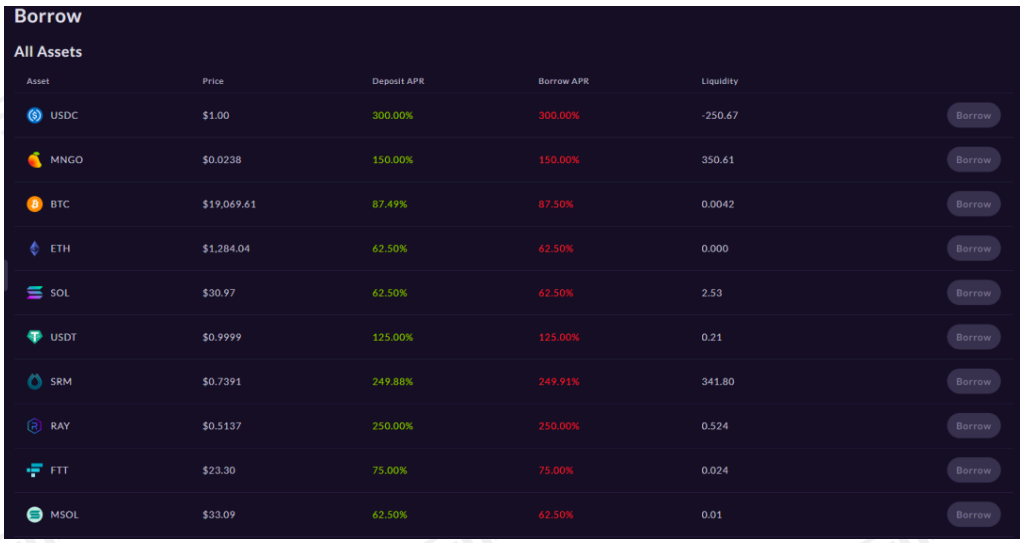


图59 攻击者从 Mango 金库中获得大量贷款

随着 MNGO 现货价格的上涨，「B」账户迅速积累了约 4.2 亿美元的未实现利润。然后，攻击者从 Mango 上所有可用的代币中提取了超过 1.16 亿美元的流动性，完成了整个攻击过程。

在事情发生不久后，攻击者在 Realms 上发布了一项新的治理提案：希望 Mango 官方使用国库资金（7,000 万美元）偿还用户坏账；如果官方同意，将返还部分被盗资金，同时希望免受刑事调查或冻结资产。攻击者计划送回的资产金额大约是 4,943 万美元，约为被盗资金的 42%，这意味着近半数的被盗资产被攻击者留下作为「漏洞赏金」。最终，Mango 社区与黑客达成协议，允许黑客保留 4,700 万美元作为漏洞赏金，且 Mango Markets 不会对此案提出刑事诉讼。

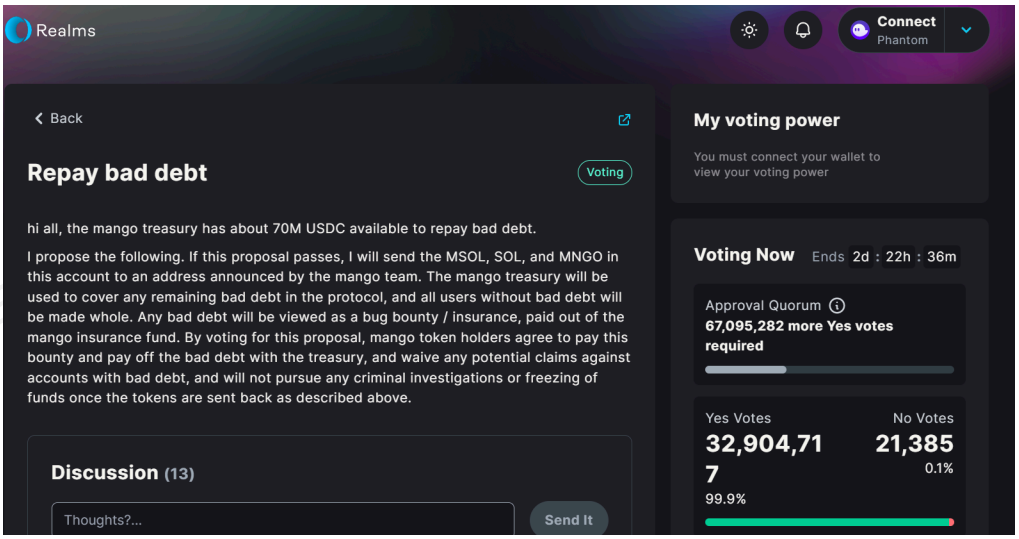


图60 攻击者在 Realms 上发布新的治理提案

5.8 Wintermute 被盗 1.6 亿美元，黑客成 3Crv 第三大持有者

9月20日，Wintermute 遭到黑客攻击，损失 1.6 亿美元。

此次被盗或因 Wintermute 被盗 EOA 钱包使用 Profanity 来创建的靓号钱包（开头 0x0000000）导致。攻击者掠走 6,927 枚 ETH（约 937 万美元）、671. 24 枚 WBTC （约 1,300 万美元）等超过 70 种 ERC-20 代币，总价值约 3,795 万美元。

事后为防止 Tether 和 Circle 对该地址进行封禁，黑客向 Curve.fi DAI/USDC/USDT 池中通过添加流动性获得 111,953,508 枚 3Crv。

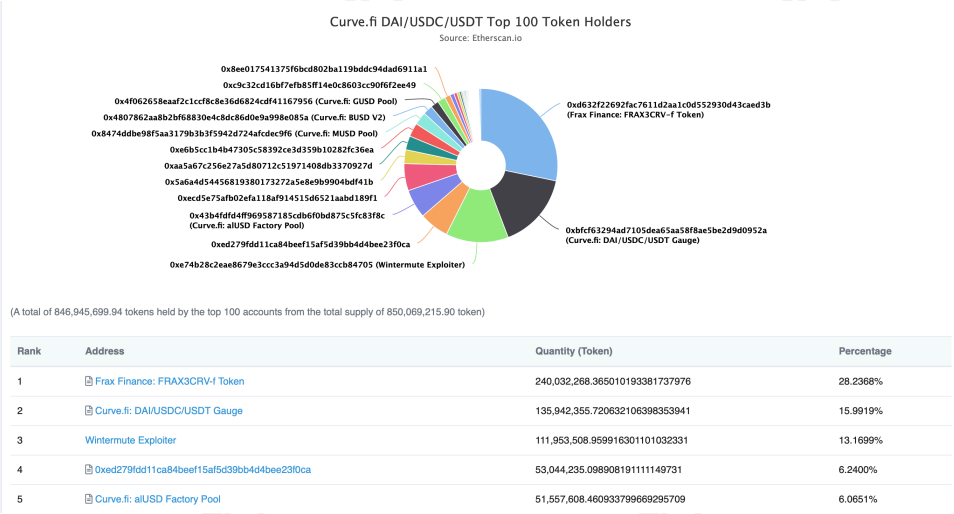


图61 攻击者在 Curve.fi DAI/USDC/USDT 池中的排名情况（Eetherscan）

5.9 约 2,000 万枚 OP 遭窃，攻击者发百万给 V 神

以太坊第二层解决方案 Optimism 在完成治理代币 OP 空投不久后，于2022年6月9日凌晨四点左右遭到黑客攻击[18]。

加密资产做市商 Wintermute 发布声明表示，因「技术性失误」攻击者已窃取该平台 2,000 万枚 OP（当时价值约 1,660 万美元）。据悉，这些代币是空投两周前 Optimism为了让空投后欲购买 OP 的用户获得更好的流动性，向 Wintermute 提供的贷款。

图62 Wintermute 攻击者链上资金流转图

Wintermute 在声明中解释，此次攻击之所以发生是因为团队犯了一个严重错误，他们提供的地址是尚未部署到 Optimism（Layer2）的 Ethereum（Layer1）多签地址，导致团队无法进行访问。虽然在意识到问题后，已立即开始恢复行动，但攻击者已先一步发现漏洞并进行攻击。

图63 Wintermute 攻击者向 V 神的钱包转入了 100 万枚 OP

链上数据显示，得手后攻击者将 100 万枚 OP 转入混币器 Tornado.Cash，且引人注意的是，攻击者还向 V 神的钱包转入了 100 万枚 OP。受攻击影响，OP 代币的价格快速下跌，从 0.93 美元的高点一度跌破 0.7 美元，四小时内重挫 25%。最终，社区与黑客达成协议，黑客归还所盗 OP。

5.10 冒名发行「五粮液」同名数字藏品，携款跑路

北京时间8月11日凌晨12时左右，与五粮液同名的 NFT 项目 Wuliangye，在不到一周的运营后，突然关闭官网和其社交媒体平台，同时注销了在海外社交平台的账号，疑似项目方卷款 75 万元人民币跑路[19]。

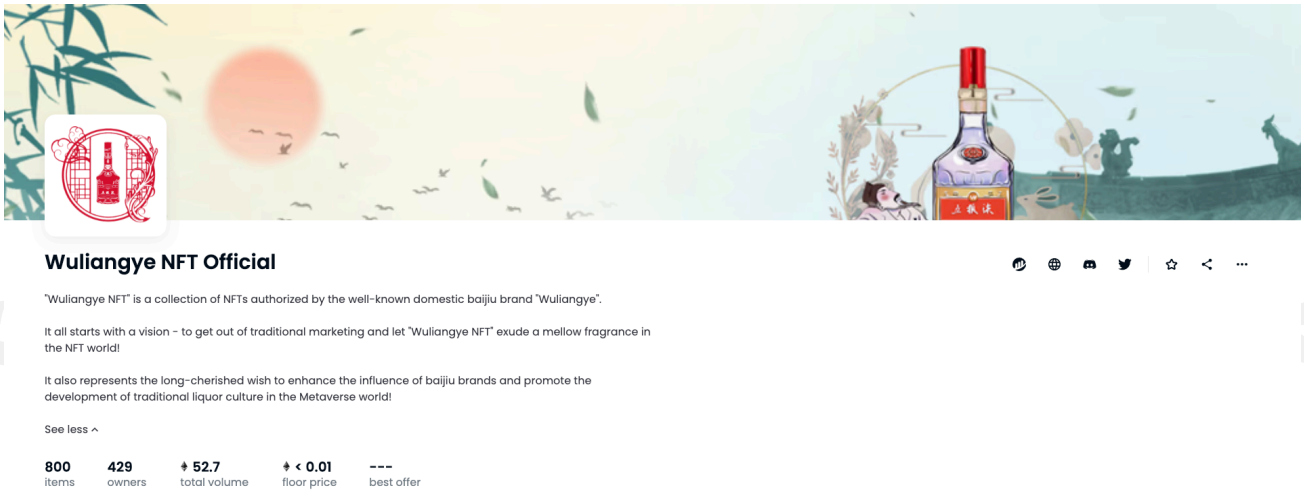


图64 与五粮液同名的 NFT 项目「Wuliangye」官网

Wuliangye NFT 的快速蹿红，得益于挂靠中国知名酒商名义的成功叙事，投资者在 FOMO（害怕错过）情绪的促使下，因未做尽调盲目入局而引发的诈骗事件。

据悉，该项目方曾多次以五粮液官方的名义发布宣传文章故意混淆概念，借着五粮液的名气营销。该项目曾自称已完成由成都商通时代数字科技有限公司（简称：时代数科）等公司领投的 A 轮融资。时代数科为新浪集团在成都投资孵化的为高端酒业提供加密资产运营服务的科技公司，臻久网隶属于该公司，也是五粮液官方指定数字酒证运营平台。但经证实，臻久网曾多次辟谣与该 Wuliangye NFT 项目的关系。

PeckShield「派盾」通过分析链上资金流向发现，Wuliangye NFT 部署者（Wuliangye: Deployer）于2022年7月29日从 Binance（币安）加密资产交易所转入约 0.5 ETH（合约 800 美元）创建合约 Wuliangye NFT (WLY)，近 600 个地址认购约 700 个 Wuliangye NFT，获利

约 70.5 ETH。

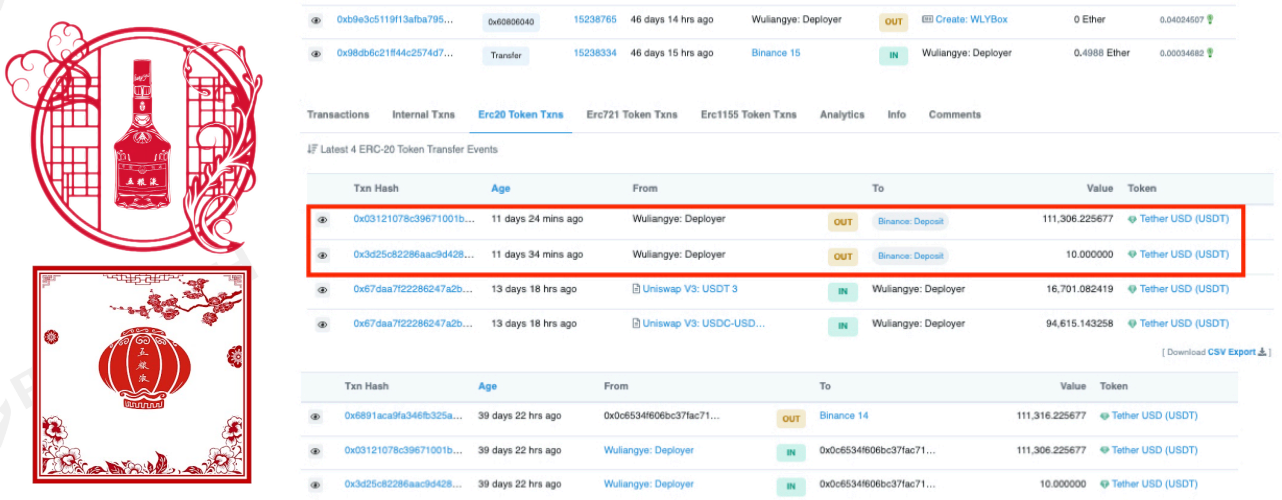
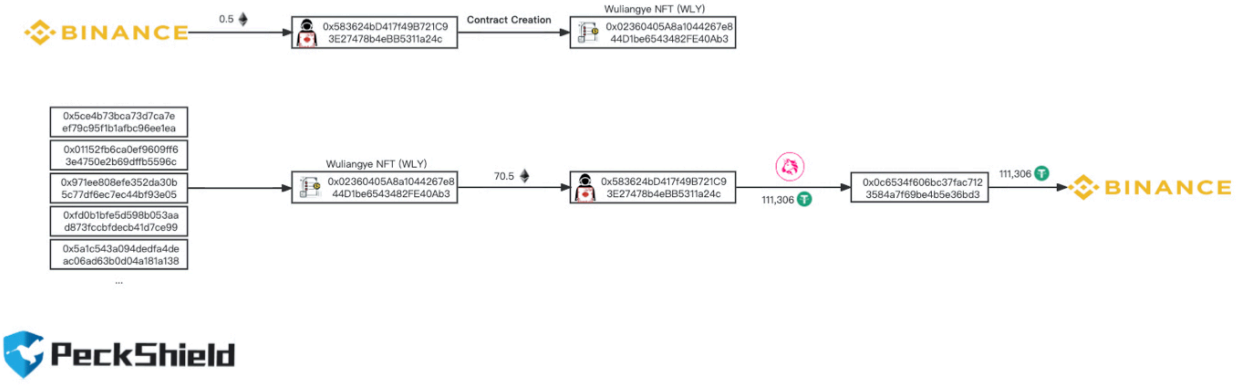


图65 Wuliangye NFT 部署者链上资金流转

随后，部署者（Wuliangye: Deployer）通过去中心化交易所 Uniswap 将所获 70.5 ETH 兑换为 111.3k USDT（合约 11 万美元），并转入中转地址 0x0C65……6bD3，最终转入 Binance「币安」加密资产交易所地址（标记为 Binance 14）。



PeckShield

图66 冒名发行五粮液同名数字藏品跑路链上资金流转

七、结论

综上所述，PeckShield「派盾」安全团队通过分析2022年 Web3 行业的发展态势，整理和统计各类安全事件，追踪、监控相关典型案例链上资金流转，得出如下三个合规:

7.1 FTX 遭挤兑，CEX 透明度备受诟病，凸显 DeFi 稳健发展

在加密资产行业发展的十余年间，CEX 曾多次因财务不透明、随意挪用用户资产等问题备受诟病。由于缺乏对传统金融行业具体的外部监管政策和成熟的风险预防、管控机制，以 CEX 为主的 CeFi 领域仍极大程度地依附于行业自律的模式进行运转，但很多时候道德抵不过市场诱惑，不透明的财务管理令用户的加密资产风险系数增大。

在第一次牛熊周期中（2012年到2015年），受到当时全球第一家交易所 Mt.Gox 因黑客事件破产的影响，各 CEX 通过出具储备证明来重拾用户信心。进入第二次牛熊周期（2015年至2018年末），由于 DeFi 领域尚处于探索阶段，用户仍主要依附于透明度不高的 CeFi 作为主要入场通道。随着2020下半年 DeFi 生态的蓬勃发展，以透明算法驱动交易，规避资金托管风险的 DEX 赛道加速建设与飞速扩张。当诸如 FTX 等中心化加密巨头溃败的黑天鹅事件来临时，行业发展不再受到中心化交易所的掣肘，用户获得将资产掌握在自己手中的有效方案。

2022年熊市期间，「浮华」退却，行业发展逐步回归理性，泡沫逐渐出清，DeFi 的真实价值逐步凸显。这有利于 DeFi 生态乃至整个 Web3 行业进一步完善基础设施建设，以 DEX 为代表的赛道在纵横方向继续延扩，等待下一叙事周期的到来。

7.2 Tornado.Cash 受制裁，DeFi 监管和合规需求日益增长

2022年8月 Tornado.Cash 遭 OFAC 制裁，反映出各主要国家对 DeFi 监管的需求提升，一系列针对 DeFi 领域的监管框架或将逐步出台。除美国外，欧盟也将在明年推出针对 DeFi 的欧盟加密资产市场监管框架（MiCA）。未来这种监管可能不单单是某个协议，而是从整个区块链应用层完全监控起来。除了需要完善相关的法律法规，相关加密机构也亟需引入新的合规工具和技术，主动拥抱监管，规避风险。

PeckShield「派盾」建议钱包软件服务商、DAO 组织、DeFi 平台、稳定币发行商、Web3 基础设施提供商、挖矿和抵押奖励池等中心化加密机构和去中心化加密组织，尽快引

入链上调查筛选和调查工具来持续审查、识别具有受制裁风险地址的历史信息或其他识别信息，主动规避潜在受制裁风险的资金。

7.3 Web3 行业安全事件持续高发，安全风控亟待加强和完善

2022年 Web3 行业共发生重大安全事件 1,637 起，其中诈骗事件 1,377 起，同比增长 585%，较前两年呈抛物线式飙升。NFT、GameFi 等垂直行业的兴起使得钓鱼攻击在 Web3 行业肆虐。DeFi 黑客攻击掠走 30 亿美元，造成损失同比增长 39%，DeFi 领域成为黑客攻击主要目标，其中跨链桥安全事件造成损失 19.2 亿美元，损失金额同比增长 3,740%（不计入白帽攻击），占2022年 DeFi 生态系统因黑客攻击被盗金额的 59%。

骤增的安全事件凸显出亟待完善跨链桥赛道「安全风控」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 生态的稳定和安全。

频发的 RugPull 和钓鱼攻击，推动整个生态加速完善针对诈骗和钓鱼的防范和整治方法。例如，引入疑似 RugPull 高危预警，钓鱼网站实时警告 C 端工具。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。

参考文献

[1] Aidan Arasasingham & Gerard DiPippo, Cryptocurrency's Role in the Russia-Ukraine Crisis, CSIS, 2022-03-15, https://www.csis.org/analysis/cryptocurrencys-role-russia-ukraine-crisis

[2] The White House, Executive Order on Ensuring Responsible Development of Digital Assets, whitehouse.gov, 2022-03-09, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/

[3] Salvador Rodriguez,《Twitter 推出 NFT 头像功能，进军数字商品业务》，华尔街日报，2022-01-24，https://cn.wsj.com/articles/twitter推出NFT头像功能-进军数字商品业务-11642721742

[4] 0x137,《8400 万美元撬动 400 亿金融帝国，UST 崩盘始末》，区块律动 BlockBeats, 2022-05-11, https://www.theblockbeats.info/news/30504

[5] 0x137,《从 Celsius 到三箭：加密百亿巨头们的多米诺，史诗级流动性的枯竭》，区块律动 BlockBeats, 2022-06-16, https://www.theblockbeats.info/news/30901

[6] U.S. DEPARTMENT OF THE TREASURY, READOUT: Secretary of the Treasury Janet L. Yellen's Meeting with the President's Working Group on Financial Markets, the OCC, FDIC and CFPB on Stablecoins, 2022-06-30, home.treasury.gov, https://home.treasury.gov/news/press-releases/jy0843

[7] U.S. DEPARTMENT OF THE TREASURY, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash, home.treasury.gov, 2022-08-08, https://home.treasury.gov/news/press-releases/jy0916

[8] ethereum.org, What was The Merge?, ethereum.org, https://ethereum.org/en/upgrades/merge/

[9] 司林威，《火币交易所控股股东变为百域资本，创始人李林抽身离场》，界面新闻，2022-10-08, http://finance.ce.cn/stock/gsgdbd/202210/08/t20221008_38148899.shtml

[10] Paulina Villegas, Bankman-Fried is ready to 'face the music,' prison official says, The

Washington Post, 2022-12-17, https://www.washingtonpost.com/nation/2022/12/17/sbf-prison-bahamas/

[11] Nikhilesh De, CFTC Alleges Market Manipulation Against Mango Markets Exploiter, CoinDesk, 2023-01-10, https://www.coindesk.com/policy/2023/01/09/cftc-alleges-market-manipulation-against-mango-markets-exploiter/

[12] Vitalik Buterin, Having a safe CEX: proof of solvency and beyond, vitalik.ca, 2022-11-19, https://vitalik.ca/general/2022/11/19/proof_of_solvency.html

[13] Arriva,《请把这份 NFT 防盗指南转发给周杰伦》，区块律动 BlockBeats, 2022-04-01, https://www.theblockbeats.info/news/29967

[14] PeckShield,《派盾：在 BAYC Instagram 攻击事件中黑客还盗取了 765.3 枚 ETH》, PANews, 2022-04-26, https://www.panewslab.com/zh/articledetails/1650956105854171.html

[15] Osato Avan-Nomayo, Lido staked ether (stETH) discount drops to 5% for second time in one month, The Block, 2022-06-10, https://www.theblock.co/post/151380/lido-staked-ether-steth-discount-drops-to-5-for-second-time-in-one-month

[16] Dirty Bubble Media, Celsius Liquidated User Assets to Pay DeFi and FTX Loans, Dirty Bubble Media, 2022-10-27, https://dirtybubblemedia.substack.com/p/celsius-liquidated-user-assets-to

[17] Ronin Network, Community Alert: Ronin Validators Compromised, Ronin's Newsletter, 2022-03-29, https://roninblockchain.substack.com/p/community-alert-ronin-validators?s=w

[18] The Optimism Foundation, A Message to the Community from the Optimism Foundation, 2022-06-09, https://plaid-cement-e44.notion.site/A-Message-to-the-Community-from-the-Optimism-Foundation-f49b913bb0974d8a854a8bdd409a9dd6

[19] 史玉宁，《冒名发行"五粮液"同名 NFT 项目方跑路，卷款约 75 万人民币》，蓝鲸财经, 2022-08-12, https://finance.sina.com.cn/blockchain/roll/2022-08-12/doc-imizirav7864046.shtml

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、青岛、北卡罗来纳州罗利，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 加密资产反洗钱系统，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加密资产相关的犯罪案件，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