Gate Research

黑客攻击的连锁反应

从 Mt.Gox 到 Bybit 等事件对加密市场的多重影响

摘要

- 2025 年，Bybit 交易所遭遇加密史上最大规模黑客攻击，损失超 14 亿美元，引发市场剧烈震荡，凸显中心化交易所的安全漏洞，并加速去中心化趋势。
- 加密市场黑客攻击频发，DeFi 项目攻击次数虽多，但中心化交易所（CEX）单次损失金额巨大；洗钱手段复杂化，跨链转移成为主要方式。
- 黑客事件往往引发主流币价格波动。例如，Mt. Gox 事件导致比特币单日暴跌 11.72%；Bybit 攻击后，BTC 和 ETH 当日最大跌幅分别达 4.44% 和 7.84%。
- 黑客攻击发生后，市场情绪指数下降，相关受影响项目代币价格暴跌。例如，Ronin 攻击后，其代币 RON 价格 24 小时内暴跌 20%。
- 黑客攻击导致市场剧烈波动，投资者恐慌性抛售加剧资金外流。例如，Bybit 事件后两天内净流出 57 亿美元，Ronin 桥攻击后其生态 TVL 两个月内暴跌 75.29%。市场对 CEX 的信任度下降，用户加速转向去中心化钱包和 DEX。
- 黑客攻击导致生态系统连锁反应，Bybit 攻击后造成恐慌性抛售导致 USDe 跌至 0.96 美元，Chainlink 预言机价格偏差引发 Aave 2,200 万美元清算。Ronin 桥攻击后导致资金外流导致 Ronin 生态系统 DeFi 业务大幅萎缩。
- 行业需构建“技术-监管-用户”三位一体的安全体系，包括技术防御升级（MPC 钱包、零知识证明）、合规与监管协同（KYC/AML）、运营透明化（储备金证明、保险机制）、用户教育（安全意识普及、漏洞赏金）和行业生态协作（跨链安全联盟、技术开源）。
- 历次重大黑客事件如 Mt. Gox、Poly Network、Ronin Bridge 和 Bybit 攻击，均推动行业反思和进化，加密行业在挑战中成长，通过技术、监管和社区共同努力，构建安全、透明和可持续的未来。

关键词：

Gate Research, Mt.Gox, Poly Network, Ronin

Gate 研究院：黑客攻击的连锁反应

- 从 Mt.Gox 到 Bybit 等事件对加密市场的多重影响

1 前言

2025 年 2 月 21 日，加密货币交易所 Bybit 遭遇史上最大规模安全漏洞事件，其以太坊冷钱包中约 14 亿美元资产被黑客盗取。此次攻击不仅打破了 Poly Network（2021 年，6.11 亿美元）与 Ronin Network（2022 年，6.2 亿美元）的历史记录，更引发市场剧烈震荡：比特币、以太坊等主流资产当日都有不同程度的下跌，加密货币总市值蒸发逾千亿美元，直至两日后方企稳于 96,500 美元与 2,700 美元关口。此次 Bybit 黑客入侵事件源于平台漏洞被利用，黑客成功盗取了超过 40 万枚 ETH 和 9 万枚 stETH，总价值超 14 亿美元。

48 小时后，跨链协议 Infini 也遭遇黑客攻击，黑客通过合约漏洞盗取 4,950 万 USDC 并全数兑换为 DAI，尽管两次事件并非由同一批黑客团队引发，但两次安全事件的接连发生进一步验证了安全威胁的持续性。这些黑客事件不仅造成了巨额财务损失，还暴露了加密货币行业基础设施中的安全漏洞，对市场稳定性构成威胁。从 2014 年的 Mt.Gox 到 2021-2023 年的跨链桥连环攻击，再到 2025 年的 Bybit 事件，黑客攻击愈演愈烈，行业持续面临安全挑战。

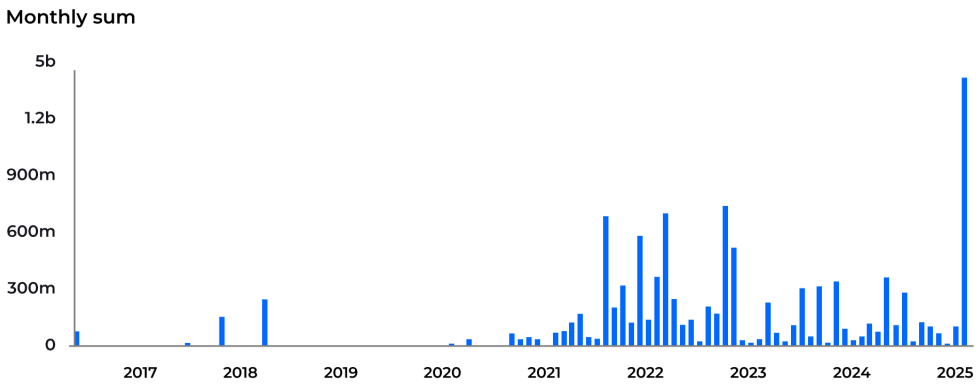
本文将深入探讨黑客攻击的现状，并基于影响极大的几起加密货币黑客事件，对加密市场的多方面影响进行详细分析，涵盖直接和间接影响，包括市场波动和投资者行为的变化。文章旨在警示加密市场可能面临的进一步风险，并展望未来可采取的应对策略。

2 加密市场黑客攻击现状

2.1 加密市场安全警报：DeFi 攻击频发，CEX 损失惨重

加密市场的去中心化特性使其易受到攻击，近年来频繁发生的黑客攻击事件不仅给市场参与者带来巨额损失，还对市场的信任度和安全性产生了严重负面影响。根据 DeFiLlama 的数据，从 2017 年至 2025 年 2 月，黑客攻击导致的资金损失呈指数级增长，总损失金额已高达 106.2 亿美元，且这一趋势仍在加剧，严重威胁到市场的长期发展。

图 一：2017 - 2025 年加密市场因黑客攻击损失金额

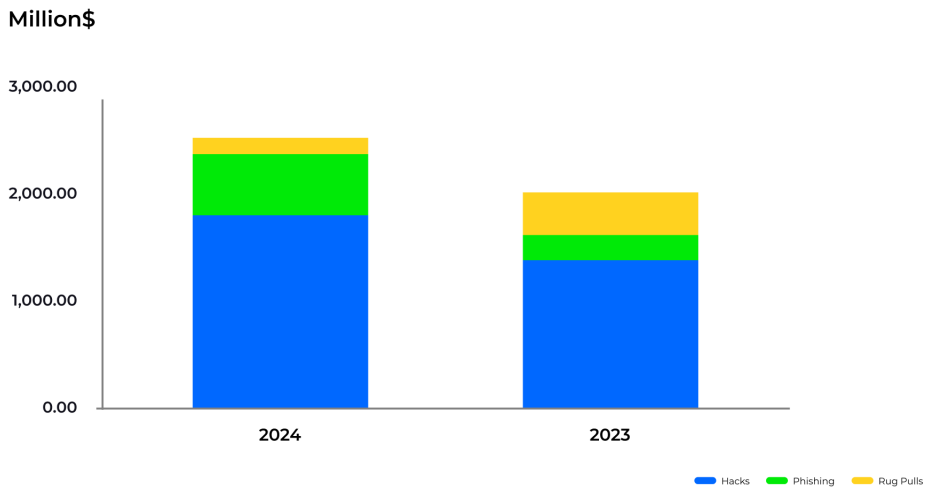


Gate Research, Data from: DefiLlama, 2025.2.21

具体来说，2024 年加密市场因黑客攻击损失的金额约为 12.72 亿美元，而 2025 年初仅两个月内，黑客攻击造成的损失就已达到 15.11 亿美元，已超过 2024 年全年损失的总和。然而，DeFiLlama 的数据主要统计了黑客攻击（Hacks）的损失，实际上，加密市场的安全事件并不限于黑客攻击。根据 Gate 研究院的报告《Gate 研究院：从黑客攻击到监管反思：2024 年加密货币安全现状分析》，历年安全事件可大致分为三类：黑客攻击（Hacks）、跑路（Rug Pulls）和钓鱼诈骗（Phishing）。

安全审计公司 Beosin 旗下 Alert 平台的监测数据显示，2024 年 Web3 领域因黑客攻击、钓鱼诈骗和项目方跑路造成的总损失高达 25.13 亿美元。其中，黑客攻击和钓鱼诈骗的损失金额较 2023 年显著上升，钓鱼诈骗的损失更是激增 140.66%。相比之下，项目方跑路事件的损失金额下降了约 61.94%。

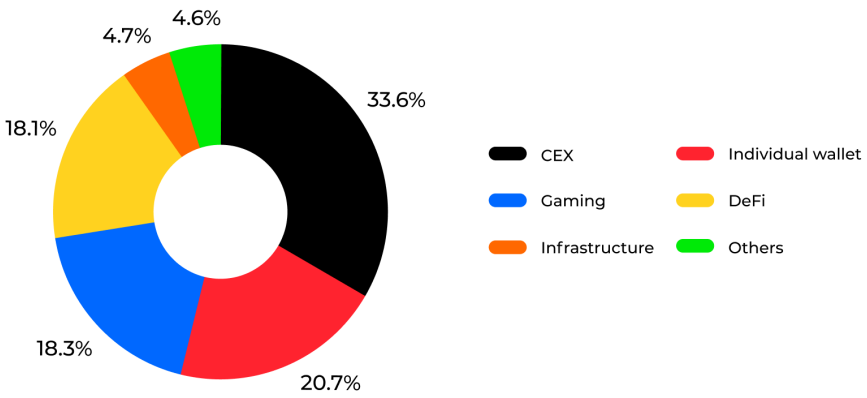
图 二：2023 - 2024 年不同类型加密资产安全事件损失金额



Gate Research, Data from: Footprint Analytics，@Beosin

从被攻击的项目类型来看，尽管黑客攻击事件涉及的项目类型非常广泛，但 DeFi 项目仍然是攻击频率最高的领域，其遭受的攻击次数占所有攻击事件的 50.7%。然而，DeFi 项目的总损失金额仅占全部损失的 18.1%，位列第四。相比之下，中心化交易所（CEX）虽然攻击次数较少，仅占所有攻击事件的 6.8%，但其造成的损失金额却占全部损失的 33.6%，成为损失最严重的领域。这表明，尽管 DeFi 项目是攻击频率最高的目标，但 CEX 因安全事件导致的单次损失更为严重，交易所安全仍然是 Web3 生态面临的最大挑战。

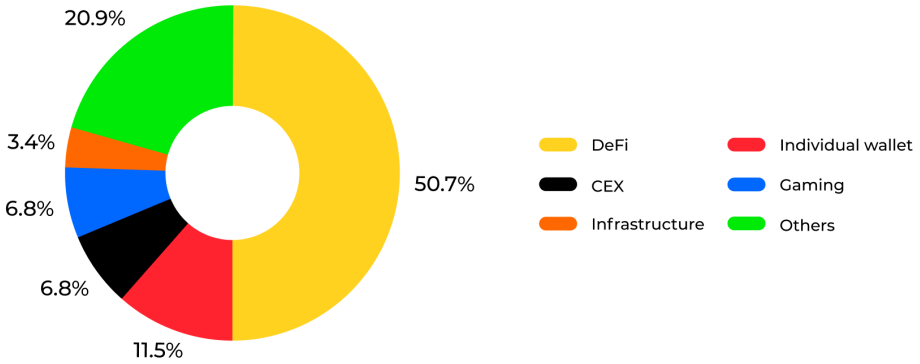
图 三：2024 年被攻击项目类型损失金额占比



Gate Research, Data from: Footprint Analytics，@Beosin

Gate Research

图 四：2024 年被攻击项目类型遭受攻击次数占比



Gate Research, Data from: Footprint Analytics，@Beosin

Gate Research

2025 年初的数据进一步印证了这一趋势。根据 DeFiLlama 梳理的 2025 年黑客攻击事件（不完全统计），DeFi 项目占了一半，但 CEX 攻击的损失金额高达 14.85 亿美元，占总损失的 98%。

这一数据凸显了中心化交易所在安全防御上的薄弱环节，以及黑客攻击对市场造成的巨大冲击。

图 五：2025 年黑客攻击事件（截至 2025 年 2 月 21 日）

名称	损失金额	分类	日期	攻击方式	相关链接
Bybit	14 亿美元	CEX	2025-02-21	钱包被盗	https://x.com/benbybit/status/1892963530422505586
Cardex	40 万美元	GameFi	2025-02-22	安全漏洞攻击	https://x.com/0xCygaar/status/1891948692204368122
Four.Meme	18.3 万美元	Meme发射平台	2025-02-23	业务逻辑漏洞	https://x.com/peckshieldalert/status/1889210001220423765
zkLend	955 万美元	DeFi	2025-02-24	合约漏洞	https://x.com/zkLend/status/1889515118368829559
Ionic Protocol	400 万美元	DeFi	2025-02-25	社会工程	https://x.com/CyversAlerts/status/1886829735130407065
DogWif Tools	1,000 万美元	Meme	2025-02-26	部署恶意软件	https://x.com/kookcapitalllc/status/1884285558635323437
Phemex	8,500 万美元	CEX	2025-02-27	热钱包被攻击	https://ktromedia.com/152490/
Orange Finance	78.7 万美元	DeFi	2025-02-28	多签配置错误	https://x.com/0xorangefinance/status/1876863611458801890
Moby	250 万美元	DeFi	2025-03-01	黑客修改合约	https://x.com/Moby_trade/status/1877096336140677458
MoonHacker	30万美元	DeFi	2025-03-02	闪电贷攻击	https://x.com/dedaub/status/1874838342485102852

Gate Research, Data from: DefiLlama, 2025.2.21

Gate Research

2.2 黑客洗钱手段加剧市场的不稳定性和信心动摇

频繁的黑客攻击事件不仅带来直接的经济损失，还对加密市场的安全性和稳定性造成严重冲击。其中，中心化交易所（CEX）的高额损失暴露了资产托管和安全管理的漏洞，加剧了市场的波动性，并削弱了投资者信心。

在成功窃取巨额资金后，黑客通常会通过复杂的洗钱手段来隐藏资金来源、规避监管追踪。这些洗钱方式包括利用去中心化混币服务、跨链桥技术、OTC 脱敏交易以及多链资金转移等手段，构建起一条隐蔽而高效的资金清洗链条。这种行为阻碍了执法机构和项目方的资金追踪，也对市场的流动性和合规性构成了重大威胁。

目前，黑客在窃取加密货币后，会采取以下方式来模糊资金来源，并最终完成套现：

1. 兑换为流动性高的代币（如 ETH、USDT）；
2. 分散资金至多个钱包，降低单一地址暴露风险；

3. 使用混币器或混合服务，阻断资金追踪路径；

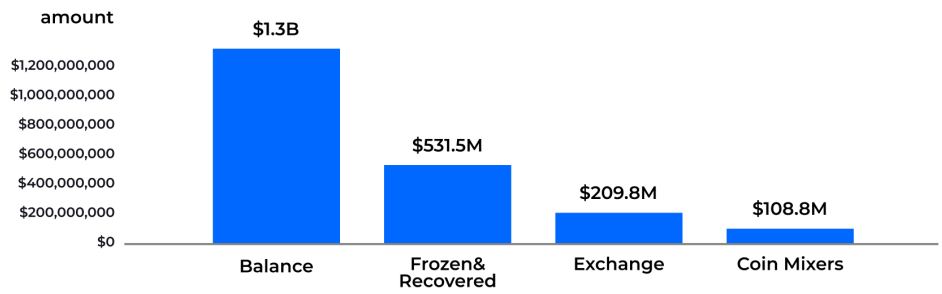
4. 跨链转移并通过 DEX 进行资金拆分，增加追踪难度；

5. 兑换为稳定币或其他匿名资产，增强隐匿性；

6. 通过 OTC 或法币渠道提现，最终实现资金合法化。

基于上述洗钱手法，黑客洗钱涉及工具大致为混币器（Mixers/Tumblers）、跨链桥和去中心化金融平台（DEX/DeFi）、场外交易（OTC）及集中化交易所（CEX）、隐私币转换（如 Monero、Zcash）、NFT 交易及其他新型工具等。尽管黑客采用了多种洗钱手段，但仍有大量被盗资金分散在黑客控制的地址中。根据 Beosin 的数据显示，2024 年被盗资金总额中，约 13.12 亿美元仍存于黑客地址（包括跨链转移和多钱包分散），占总被盗资金的 52.20%。其中，部分资金通过跨链工具进行了拆分。

图 六：2024 年被盗资金流向

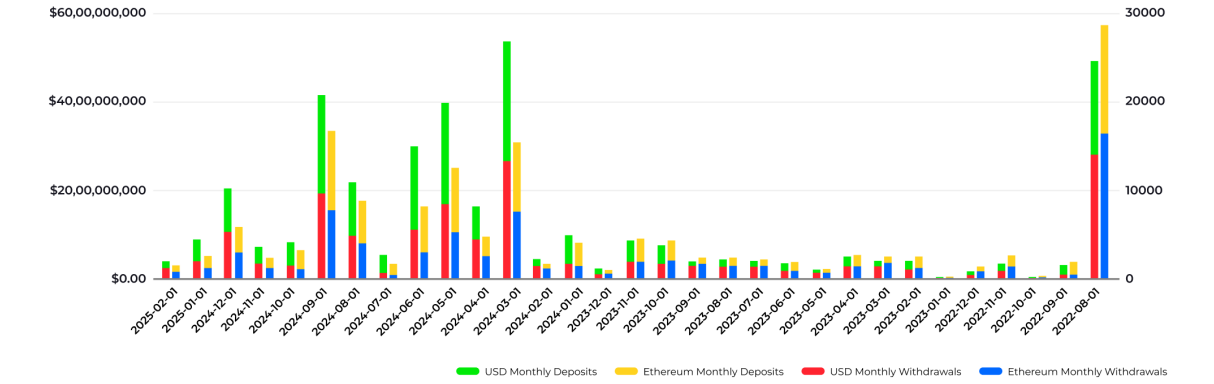


Gate Research, Data from: Footprint Analytics，@Beosin

Gate Research

自 2022 年 8 月美国 OFAC 对 Tornado Cash 实施制裁以来，被盗资金转入该混币器的金额大幅下降。如下图所示，自 2022 年 9 月起，Tornado Cash 的转入和转出金额出现断崖式下跌，直至 2024 年 3 月才略有回升。然而根据 Beosin 的数据显示，2024 年仅有约 1.09 亿美元的被盗资金转入混币器，占总被盗资金的 4.34%。相比之下，2023 年和 2022 年这一比例分别为 23.6% 和 38.7%，显示出显著下降趋势。

图 七：近三年 Tornado Cash 转入及转出金额



Gate Research, Data from: Dune，@legionx

Gate Research

总体来看，黑客通过多次跨链、混币器转换和资金拆分等方式，使得资金流向的追踪变得更加困难，市场合规性面临严峻考验。黑客洗钱不仅仅是单个项目的损失问题，而是影响整个市场安全性与稳定性的系统性风险，同时也为监管机构和项目方提出了新的挑战。

3 黑客攻击对加密市场的影响分析

黑客攻击对加密市场的影响是多维度的，不仅造成直接的经济损失，还会影响市场信心、推动监管介入、加速技术革新，并重塑行业生态格局。这些攻击往往会引发投资者恐慌、加剧市场波动，并促使各国政府加强对加密行业的监管。

3.1 直接影响：巨额财务损失，受害者范围扩大

近年来，黑客攻击频发，累计造成了数百亿美元的资金损失。从 2014 年的 Mt. Gox 交易所事件到 2025 年的 Bybit 事件，单次攻击的损失往往高达数亿美元。其中，朝鲜黑客组织 Lazarus Group 是加密行业最活跃的黑客群体之一，过去几年间多次发动攻击，目标涵盖交易所、跨链桥、DeFi 协议及个人钱包，累计盗取资金超过数十亿美元。值得注意的是，朝鲜黑客从加密平台窃取的资金规模可能比已知统计数据更为庞大。

图 八：历年朝鲜黑客加密市场攻击次数及盗取金额

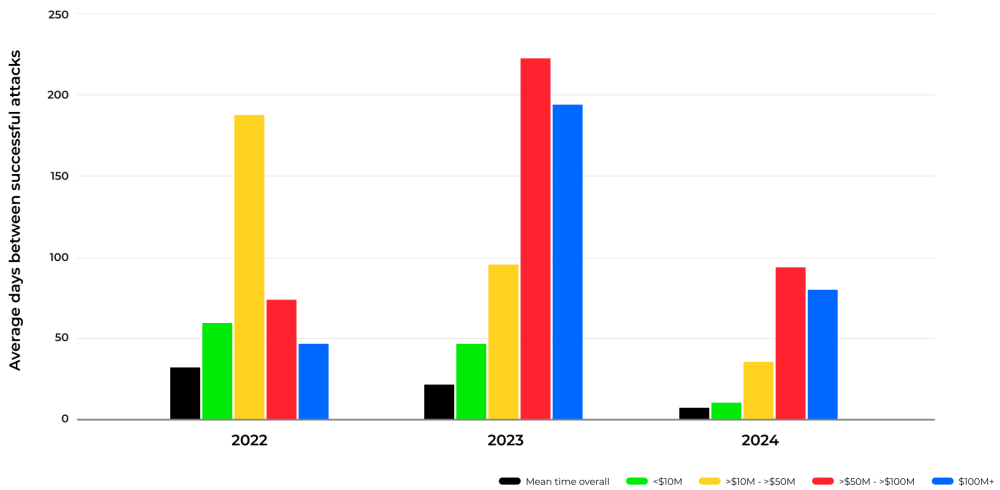
年份	攻击次数	盗取金额
2016	1	200 万美元
2017	5	2,900 万美元
2018	10	5.22 亿美元
2019	9	2.71 亿美元
2020	4	3 亿美元
2021	7	5.06 亿美元
2022	15	11 亿美元
2023	20	6.6 亿美元
2024	47	13.4 亿美元（增幅 102.88%）

Gate Research, Data from: chainalysis

Gate Research

朝鲜的加密货币攻击的范围正在逐步扩大。2024 年，朝鲜黑客组织针对 5,000 万至 1 亿美元以及超过 1 亿美元资产的攻击比 2023 年更为频繁，表明其对高额目标的攻击效率显著提升，这将导致更多用户和机构遭受损失。与此同时，小额攻击（如 1 万美元级别）的数量也在上升，显示普通投资者同样可能成为攻击目标，朝鲜黑客的策略正在向更广泛的目标群体扩展。此外，朝鲜黑客的攻击密度也在增加，尽管部分攻击的金额较低，但其频率和覆盖面显著扩大。

图 九：历年朝鲜黑客加密市场不同攻击规模分布



Gate Research, Data from: chainalysis

Gate Research

3.2 间接影响：市场信心与投资者行为

黑客攻击发生后，市场通常会迅速反应，相关资产（如 BTC、ETH 及受攻击项目代币）在短期内往往出现下跌。市场情绪指数在事件后普遍下降，但其影响程度取决于黑客攻击的规模与范围。

我们分析了过去几年发生的四起被盗金额排名前五的加密货币黑客事件，并研究了其对 BTC 和 ETH 价格的影响。数据显示，尽管 BTC 在黑客攻击后通常会出现一定跌幅，但下跌的时间和幅度可能有所不同：有时是攻击当天直接引发市场下跌，有时则是攻击事件发酵后，因信任危机蔓延而导致的延迟下跌。下文将基于这四个案例，深入分析黑客攻击对加密市场的间接影响：

图 十：四起大额黑客攻击加密安全事件详情

时间	攻击目标	被盗金额	攻击方式
2014 年 2 月 24 日	Mt. Gox（当时全球最大的比特币交易所）	约 85 万枚 BTC（当时价值 4.7 亿美元，按当前价格约 800 亿美元）	交易所私钥泄露 + 交易重放漏洞（Transaction Malleability）
2021 年 8 月 10 日	Poly Network	约 6.1 亿美元	私钥泄露 / 多链跨链合约漏洞
2022 年 3 月 23 日	Ronin Bridge（Axie Infinity 侧链）	6.24 亿美元（173,600 枚 ETH + 2,550 万 USDC）	私钥泄露（社交工程攻击）
2025 年 2 月 21 日	Bybit 的 ETH 冷钱包（中心化交易所，假设性案例）	14 亿美元（ETH 及相关衍生资产）	多签系统漏洞 + 恶意合约钓鱼

Gate Research

3.2.1 Mt. Gox 交易所攻击（2014 年）

Mt. Gox 曾是全球最大的比特币交易所，掌控了超过 70% 的全球比特币交易量。然而，2014 年 2 月 24 日，该交易所遭受了灾难性的黑客攻击，导致约 85 万枚比特币被盗（当时约 4.5 亿美元，按当前价格约 800 亿美元），最终迫使 Mt. Gox 申请破产。然而，这并非 Mt. Gox 首次出现安全漏洞。早在 2011 年，该交易所已损失 2.5 万枚比特币。2014 年 3 月，Mt. Gox 宣布找回约 20 万枚比特币，但仍有 65 万枚下落不明。事实上，Mt. Gox 事件的真实原委至今仍是未解之谜。尽管存在监守自盗、外部入侵、里应外合等多种猜测，但核心问题依然悬而未决：被盗的大量比特币至今未能全部追回。

3.2.1.1 价格下跌与市场恐慌

BTC 在事件发生后单日下跌 11.72%，并在事发后两个月内，于 4 月 11 日最低跌至 340 美元，跌幅 36%。短期内，市场情绪剧烈波动，部分持币者可能选择抛售以规避潜在风险。然而，这种

恐慌性抛售的实际影响可能被高估。

图 十一：Mt. Gox 交易所攻击前后 BTC 价格走势

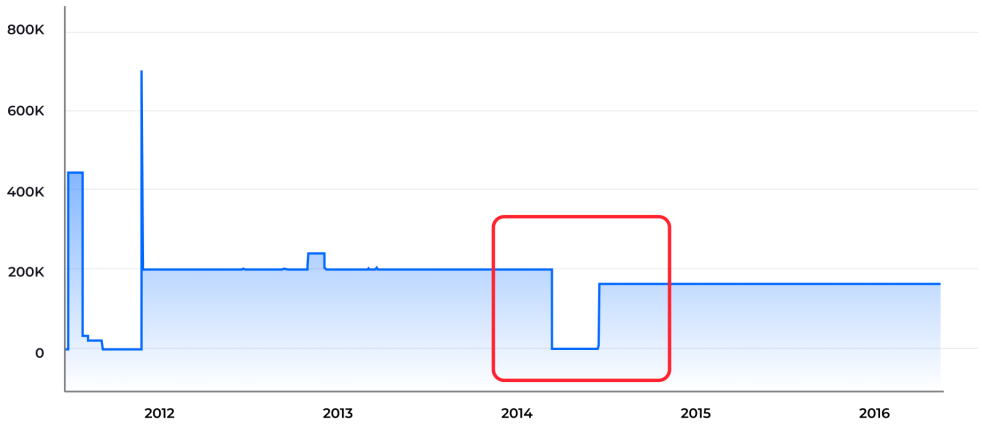
Gate Research, Data from: Gate.io

Gate Research

3.2.1.2 流动性危机与资金异动

Mt. Gox 事件发生时，全球宏观经济环境正处于不稳定时期。美联储的利率政策和 CPI 数据对加密货币市场产生了一定影响。当时，美联储的量化宽松政策导致美元贬值，一些投资者将目光转向加密货币，以寻求资产保值和增值。然而，Mt. Gox 事件的爆发严重打击了投资者对加密货币的信心。链上数据分析显示，在 Mt. Gox 停止提现前，大量比特币出现异常流出，部分大户和敏感投资者提前转移资金，进一步加剧了市场的不稳定性。随后，交易所全面暂停提现，比特币交易流动性骤降，市场一度陷入停滞。

图 十二：2012 - 2016 年 Mt. Gox 交易所 BTC 持有数



Gate Research, Data from: intel.arkm

Gate Research

3.2.1.3 信任崩塌与行业形象受损

这次黑客攻击影响深远，不仅引发比特币价格剧烈波动，还严重削弱了全球加密货币社区的信任。该事件对投资者信心造成了长期冲击，加密社区的信任度降至冰点，许多投资者开始重新评估加密货币的安全性和可靠性。Mt. Gox 事件成为加密生态系统中最臭名昭著的安全事故，其阴影至今仍深刻影响着人们对数字资产交易平台风险的认知。

主流媒体普遍将 Mt. Gox 事件描绘为加密货币行业“不成熟”和“高风险”的典型案例，进一步延缓了机构投资者的入场步伐。同时，部分传统投资者对加密货币的认知固化，将其与“黑客”“诈骗”等负面标签联系在一起，影响了行业的整体形象和未来发展潜力。

3.2.1.4 法律诉讼与监管介入

事件发生后，受害用户和投资者纷纷提起法律诉讼，要求赔偿损失；2015 年，前 CEO Mark Karpeles 被捕并面临多项指控，尽管部分指控最终未成立，但这一系列法律行动显著推动了监管机构对加密市场的介入。日本警方和金融厅对 Mt. Gox 事件展开了详细调查，试图查明比特币丢失的具体原因和责任人，这些调查揭示了平台管理层在处理用户资金和安全问题上的严重失职。Mt. Gox 的倒闭成为监管部门完善加密货币交易所管理规定的重要契机，并推动了各国加密监管政策的逐步形成。

3.2.1.5 后续进展与影响

Mt. Gox 事件不仅敲响了安全警钟，而且加速了整个行业规范化进程。一方面，它促使投资者更加重视加密货币交易平台的安全问题，从而推动平台加强安全技术研发和管理。Mt. Gox 的惨痛教训使整个行业重新审视交易所安全和资产托管机制，进而推动了多重签名钱包、资产储备证明等安全技术的普及。另一方面，该事件引起了监管机构的高度关注，促进了加密货币监管政策的不断完善。事件发生后，日本政府迅速制定了《支付服务法》，要求所有加密交易所必须注册并接受金融监管，其他国家也相应加强了监管要求。

2024 年，Mt. Gox 宣布开始偿还 BTC 和 BCH，比特币价格在消息公布后再次震荡，并引发了短期恐慌性抛售。在 5 月 28 日至 7 月 5 日期间，比特币价格从 7 万美元的高点回落，最低跌破 5.4 万美元，累计跌幅达 22%。尽管市场出现波动，现金偿还的宣布为受影响的投资者带来了一线希望，标志着这一长期未解决的问题终于取得了实质性进展。

3.2.2 Poly Network 攻击（2021 年）

Poly Network 是由 Neo、Ontology、Switcheo 基金会共同作为创始成员，分布科技作为技术提供方共同发起的跨链组织。2021 年 8 月 10 日，Poly Network 遭遇了一次规模空前的黑客攻击，

损失高达约 6.12 亿美元，涉及以太坊、BSC 和 Polygon 等多个生态资产。黑客利用源链上的无效攻击交易，通过中继器将其错误地纳入 Alliance Chain 的 Merkle 树并签名，随后在目标链上篡改了 keepers 权限，最终在多条公链上解锁并转移资产。此次事件成为当时最大的 DeFi 黑客攻击，也引发了市场对跨链互操作性安全性的广泛关注。攻击发生后，黑客先后归还了约 2.58 亿美元的资金，但仍有约 3.42 亿美元未被追回，事件一度引发对“白帽”动机的猜测，认为攻击可能旨在促使 Poly Network 正视自身的安全漏洞。

3.2.2.1 市场信心与用户损失

Poly Network 事件发生后，比特币的日跌幅为 1.47%，整体主流币市场情绪保持稳定。受牵连的以太坊生态下跌 0.66%，波动幅度也不显著。

图 十三：Poly Network 攻击前后 BTC 价格走势

Gate Research, Data from: Gate.io

Gate Research

图 十四：Poly Network 攻击前后 ETH 价格走势

Gate Research, Data from: Gate.io

然而，受此次事件冲击最深的是依赖跨链聚合器 O3 Swap 进行挖矿的用户。由于 O3 Swap 的跨链功能基于 Poly Network 构建，该平台因此暂停了跨链相关服务。事发前，O3 Swap 在 Polygon 等链上的稳定币池年化收益率超过 20%，而一些短期单币池的年化收益甚至高达数百分之数百，这样的高收益吸引了大量 DeFi Famer。然而黑客攻击发生后，这些高收益挖矿者最终血本无归。据 CoinGecko 数据显示，O3 Swap 代币在 2021 年 6 月 20 日曾达到历史最高点 8.20 美元，但受到事件影响后，该代币价格大幅下跌，进一步反映出市场对跨链服务安全性的担忧。

图 十五：Poly Network 攻击前后 O3 价格走势

Gate Research, Data from: CoinGecko

3.2.2.2 跨链桥市场萎缩与 DeFi 生态结构变化

尽管整个 2021 年 DeFi 生态市值变化不大，但自 Poly Network 事件发生后，跨链桥和相关协议

的市场份额出现了明显下滑。事件发生于 8 月 10 日，而整体跨链桥的总锁仓价值直到 8 月 26 日才明显下跌。总锁仓价值由事发当天的 115.3 亿美元，最低于 8 月 28 日下跌至 28.7 亿美元，跌幅 75%，显示出市场对跨链安全性的担忧。

图 十六：2021- 2022 年跨链桥 TVL 走势

Gate Research, Data from: DefiLlama

Gate Research

在 2021 年第四季度，去中心化交易所、预言机和借贷平台等部分 DeFi 平台市值分别下降了约 9%，累计减少了约 15 亿美元，而收益率聚合器和保险行业则成为了最大的赢家，部分资金从高风险跨链协议转向更安全的 DeFi 产品。

图 十七：2021 年第四季度 DeFi 细分领域市值变化

占比 2021年Q4 的市值占比	分类	季度变化
	DeFi总市值	0.0%
49.4%	去中心化交易所	-0.3%
16.9%	预言机	-8.5%
17.4%	借贷	-4.4%
6.1%	衍生品	-9.0%
7.5%	收益聚合器	64.2%
2.1%	保险	31.5%
0.4%	资产管理	-36.7%
0.3%	固定收益	-17.1%

Gate Research, Data from: CoinGecko

Gate Research

3.2.2.3 行业警示与安全反思

Poly Network 事件暴露了跨链协议和智能合约安全中的诸多薄弱环节，促使整个 DeFi 领域在安全审计和技术防护上加快了升级步伐。许多跨链项目和聚合器（例如 O3 Swap）因此被迫暂停相关服务，迫使业界深入反思并改进安全措施。该事件成为 DeFi 安全领域的重要案例，促使众

多跨链项目在事件后对智能合约进行安全升级，采用形式化验证工具（如 Certora）以防范类似漏洞。与此同时，政府和监管机构也加强了对 DeFi 领域的监管力度，推动 KYC、AML 以及其他安全标准的严格执行。

3.2.3 Ronin 桥攻击（2022 年）

Axie Infinity 运行在名为 Ronin 的以太坊侧链上，旨在解决以太坊网络的可扩展性问题。为实现 Ronin 与以太坊之间的高效、低成本资产转移，平台引入了 Ronin Bridge，使用户能够在两个区块链之间轻松转移以太币 (ETH) 和 USDC 等资产。

2022 年 3 月 23 日，攻击者利用 Ronin Bridge 的安全漏洞，通过盗取的私钥伪造提款交易。仅通过两次交易，攻击者便从 Ronin Bridge 中窃取了 173,600 枚 ETH 和 2,550 万 USDC，总价值约 6.24 亿美元。到 3 月 29 日，部分用户发现无法通过 Ronin Bridge 提取 ETH，这才让其团队意识到，攻击者已在上周将大部分资金抽走。为应对此次攻击，团队暂停了 Ronin Bridge 和侧链上的 Katana 交易所，并迅速迁移了节点基础设施，与执法部门、大型加密交易所和 Chainalysis 紧密合作，追踪和包围攻击者。

3.2.3.1 生态相关代币价格暴跌

黑客攻击后（2022 年 3 月 23 日），BTC 日涨幅达到 1.24%。然而，直到 2022 年 3 月 29 日，用户才意识到 Ronin 桥遭遇黑客攻击。此后，从 2022 年 4 月初开始，比特币（BTC）呈现下跌趋势，但该趋势并非完全由 Ronin 桥攻击单独引起。当年还发生了其他重大事件，如 Terra（LUNA）崩盘导致 BTC 跌至 3 万美元、Celsius（CeFi 借贷平台）破产以及美联储 9 月加息等因素共同作用，致使 BTC 在 4 月至 9 月期间从 47,000 美元下跌至约 18,500 美元，跌幅接近 60%。

图 十八：Ronin 桥攻击前后 BTC 价格走势

Gate Research, Data from: Gate.io

Gate Research

受此次攻击影响，RON 代币价格在 2022 年 3 月 29 日至 3 月 30 日暴跌超过 20%，从 2.2 美元跌至 1.7 美元。随后市场恐慌情绪加剧，投资者抛压不断，一个月内最低触及 1.23 美元，以最低价来算，事件发生后一个月跌幅 43%。若以收盘价 1.36 美元算，事件发生后一个月跌幅为 39%。

图 十九：Ronin 桥攻击前后 RON 价格走势

Gate Research, Data from: Gate.io

Gate Research

此外，Axie Infinity 相关代币如 AXS 的价格也遭受重挫，事件发生后，AXS 从 52 美元跌至 45 美元，跌幅 13%。

图 二十：Ronin 桥攻击前后 RON 价格走势

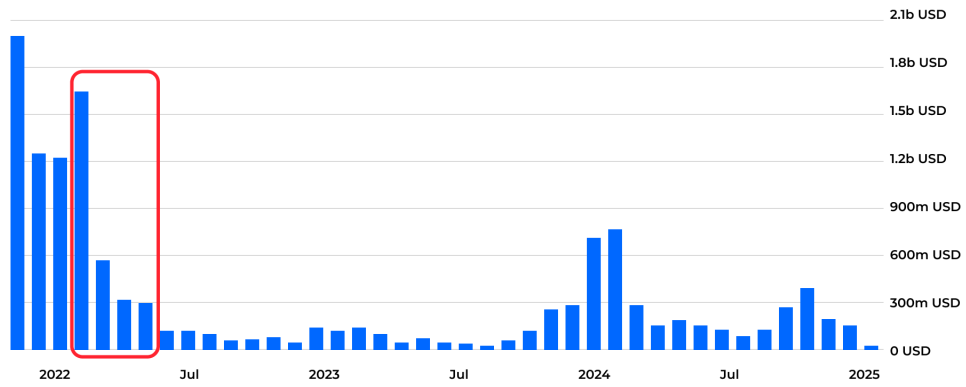
Gate Research, Data from: CoinGecko

Gate Research

3.2.3.2 生态系统崩盘与资金外流

此次攻击的影响十分明显，不仅造成了巨额资金损失，还导致 Ronin 生态的用户活跃度和链上交易量大幅下降。从 Ronin 链上 DEX 月交易量可以看出，2022 年 3 月黑客攻击后，相关指标值骤减。叠加 2023 年加密寒冬的影响，Ronin 似乎陷入了长时间的低迷期。

图 二十一：2022- 2025 年 Ronin 链 DEX 月交易量



Gate Research, Data from: DefiLlama

Gate Research

Ronin 链的总锁仓价值（TVL）早在 2022 年初就因 Axie Infinity 经济崩溃、加密市场下行和 P2E 模型失效而大幅下降。然而，Ronin 桥的攻击进一步加剧了资金外流，导致其 TVL 从 2022 年 3 月 29 日的约 3.36 亿美元在两个月内（2022 年 5 月 29 日）跌至 8,300 万美元，跌幅约为 75.29%。值得注意的是，Ronin 生态主要围绕 Axie Infinity 构建，其 DeFi 部分较小，主要应用集中在 Katana DEX，而非借贷协议，因此此次攻击并未直接引发大规模 DeFi 清算。

图 二十二：2021- 2022 年 Ronin 链 TVL 走势

Gate Research, Data from: DefiLlama

Gate Research

3.2.3.3 行业安全与监管的后续反应

Ronin 攻击对跨链协议及其安全性提出了严峻挑战，加剧了资金外流，动摇了投资者信心，并引发了行业对安全和监管标准的深刻反思。此次事件推动了 Web3 安全措施的升级：为了降低单点控制风险，Ronin 将验证者节点数量从 9 个增加到了 21 个，而整个 DeFi 生态系统也开始普遍采用去中心化多重签名（MPC）和去信任验证机制（如 ZK-Rollups）来提升安全性。此外，美国政府进一步加大了对黑客行为的打击力度，虽然 OFAC 对 Tornado Cash 的制裁曾被推翻，但美国执法机构依然加强了对朝鲜 Lazarus Group 相关钱包地址的监控，并联合交易所冻结了可疑资金。

3.2.4 Bybit 交易所攻击（2025 年）

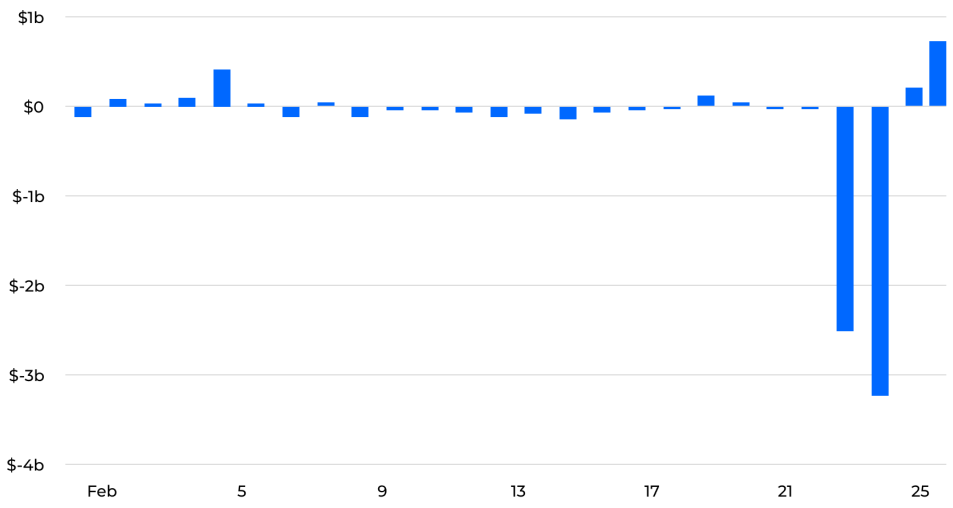
2025 年 2 月 21 日，加密货币交易所 Bybit 遭遇重大黑客事件，造成约 14 亿美元的损失。当晚 23:44（UTC+8），Bybit 执行长在推特上确认了此次攻击，称至少约 401,000 ETH（事发时价值约 14 亿美元）被转移至不明地址。Bybit 表示，仅有一个 ETH 冷钱包受到攻击，其余所有钱包均完好无损，提现功能依然正常。

此次事件的关键在于，黑客针对多签系统发动了攻击。当时，Bybit 正在进行 ETH 冷钱包与热钱包之间的例行转账，在通过 Safe 交易签署时，黑客利用先前部署的恶意合约，成功升级交易合约并提取了资金。有关该事件的详细数据追踪可参考Gate Research 的 Dune 数据看板，本文将重点分析此次攻击对市场的影响。

3.2.4.1 市场恐慌及流动性危机

黑客攻击发生后，市场波动骤增，用户恐慌性提款导致 Bybit 的资产储备大幅下降，投资者纷纷采取措施保护资产。数据显示，2 月 22 日和 23 日，Bybit 分别净流出加密资产 25 亿美元和 32 亿美元。到 2025 年 2 月 24 日，Bybit 的 BTC、USDT 和 USDe 储备分别净流出 21,248 BTC、17.6 亿美元 USDT 和 2.1747 亿美元 USDe，使得其主要资产储备从攻击时的 108 亿美元下降至 65 亿美元，总计流出 43 亿美元。这些数据表明 Bybit 的流动性遭受严重消耗，进一步加剧了市场对中心化交易所安全性的担忧。

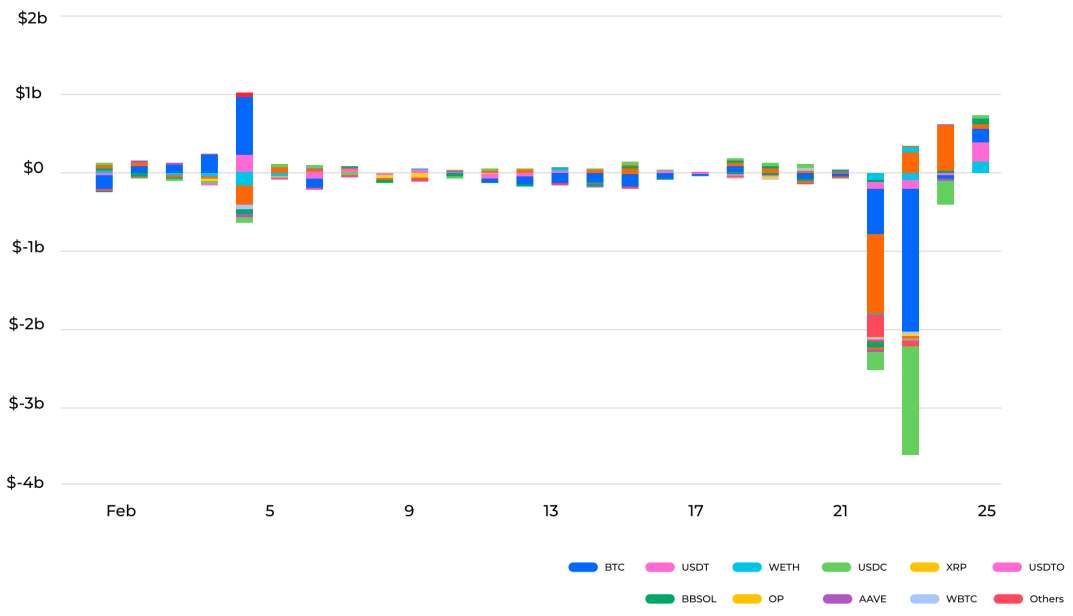
图 二十三：2025 年 2 月 Bybit USD 流入



Gate Research, Data from: DefiLlama

Gate Research

图 二十四：2025 年 2 月 Bybit 各 Token 流入



Gate Research, Data from: DefiLlama

Gate Research

3.2.4.2 市场疲软，加速市场下跌

在事件发生当日，比特币（BTC）最大跌幅达到 3%，最低价格为 94,924.1 美元；到 2 月 26 日，比特币价格进一步下探，跌至约 86,000 美元，当月累计跌幅近 13%。以太坊（ETH）当天最大

跌幅为 6%，最低价格为 2,617.03 美元；随后价格持续下行，月初收盘价为 3,117 美元，2 月 28 日收盘价为 2,237 美元，当月累计跌幅约 28%。此次价格大幅下跌不仅逆转了数月来的上涨趋势，充分暴露出市场信心的脆弱性。

图 二十五：Bybit 攻击前后 BTC 价格走势

Gate Research, Data from: Gate.io

Gate Research

图 二十六：Bybit 攻击前后 ETH 价格走势

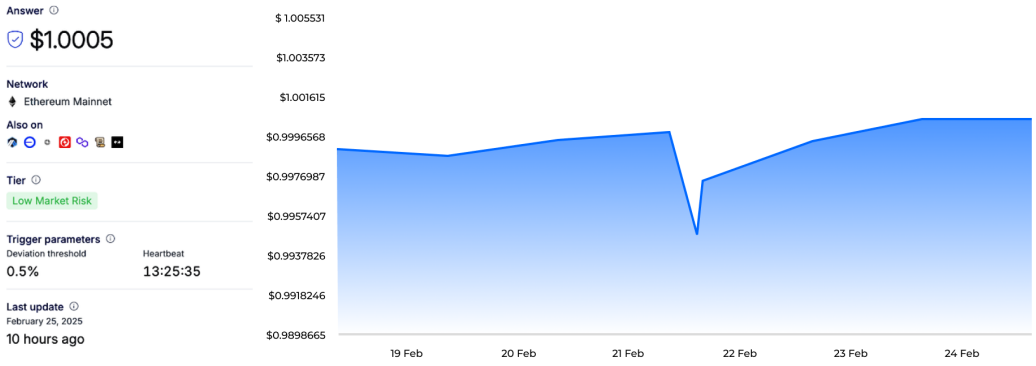
Gate Research, Data from: Gate.io

Gate Research

相比 BTC 、ETH 等主流币，Bybit 事件发生后，其平台币 MNT 受到了显著冲击，最大跌幅达 22.05%，最低触及 0.8231 美元。

此外，由于 Ethena 在 Bybit 存有大量资产（据 Chaos Labs 创始人兼 CEO @omeragoldberg 披露，Bybit 占比 21%，仅次于 Binance 的 36%），Bybit 事件对 Aave、Ethena Labs 及 USDe 稳定币价格产生了连锁反应。由于市场恐慌性抛售，Bybit 交易平台上的 USDe/USDT 一度跌至 0.96 美元。Chainlink 的 USDe/USD 预言机价格因二级市场剧烈波动而出现偏差，最低跌至 0.977 美元。这一价格偏差直接导致 Aave 平台上约 2,200 万美元的资产被清算，加剧了市场动荡。总体来看，由于市场流动性下降、现货需求降温以及抛售压力加剧，进一步引发了更广泛的市场调整。

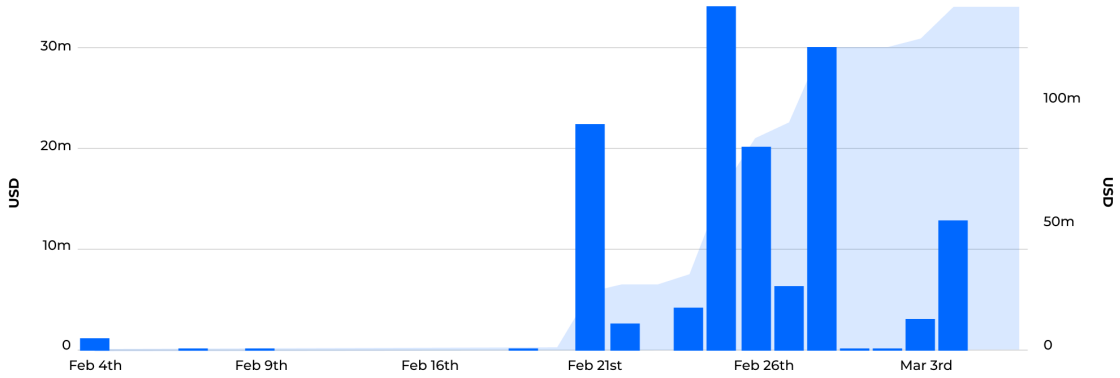
图 二十七：Bybit 攻击前后 USDe/USD 预言机价格



Gate Research, Data from: Chainlink

Gate Research

图 二十八：Bybit 攻击前后 AAVE V3 以太坊清算量



Gate Research, Data from: Dune, @KARTOD

Gate Research

3.2.3.3 去中心化趋势加速与监管加强

Bybit 虽然强调自身偿付能力，但本次被盗资金占其总储备的 8.64%-9.28%，引发了市场对中心化交易所（CEX）安全性的强烈质疑。此次事件颠覆了“冷存储绝对安全”的传统认知，促使投资者加速转向去中心化钱包和 DEX，以降低集中化管理带来的风险。

与此同时，各国监管机构可能加强对 CEX 资产管理的要求。日本、韩国等国早已实施交易所多重签名、冷存储比例披露及第三方审计等措施，此次攻击或推动更多国家效仿，进一步收紧对交易所安全标准的监管。此外，投资者信心受挫，也可能促使行业对交易所储备透明度、智能合约安全及资产保险机制进行更深入的探讨和改进。

3.3 小结

黑客攻击最直接的影响就是巨额资金损失，除此之外，还对市场情绪和投资者信心产生深远影响，导致市场信心崩塌与投资者行为异化，进而推动行业生态重塑与监管升级。通过总结上述案例中黑客攻击对加密市场的影响，可以归纳为以下几点：

3.3.1 市场剧烈波动

- 黑客事件往往引发市场剧烈波动。例如，Mt. Gox 事件导致比特币单日暴跌 11.72%；Bybit 攻击后，BTC 和 ETH 当日最大跌幅分别达 4.44% 和 7.84%。
- 尽管主流币短期波动受多重因素影响（如 Terra 崩盘、美联储加息），但黑客事件无疑加剧了市场的脆弱性。

3.3.2 投资者行为异化

- **恐慌性抛售：**攻击发生后，BTC、ETH 及相关受影响项目代币通常会短期下跌，市场情绪指数下降。例如，Ronin 攻击后，其代币 RON 价格 24 小时内暴跌 20%；一个月内最低触及 1.23 美元，以最低价来算，事件发生后一个月跌幅 43%。
- **流动性风险：**黑客攻击可能导致交易所暂停提现，引发市场恐慌，加剧资金外流。交易所或相关 DeFi 平台会遭遇大规模资产外流，用户撤回资金以规避风险。例如，Bybit 两天内净流出 57 亿美元。Ronin 桥 TVL 从 2022 年 3 月 29 日的约 3.36 亿美元在两个月内（2022 年 5 月 29 日）跌至 8,300 万美元，跌幅约为 75.29%。
- **生态系统连锁反应：** Bybit 攻击后造成恐慌性抛售导致 USDe 跌至 0.96 美元，Chainlink 预言机价格偏差引发 Aave 2,200 万美元清算。Ronin 桥攻击后导致资金外流导致 Ronin 生态系统 DeFi 业务大幅萎缩。

– **行业信任受损：**历史上，Mt. Gox、Poly Network、Ronin Bridge 等事件均导致市场对加密行业的信任度降低，使机构投资者更加谨慎。

3.3.3 行业生态重塑与监管升级

– **行业安全标准升级：** Poly Network 促使 DeFi 项目加强合约安全审计。Ronin 桥提高验证者数量，减少单点控制风险。Mt. Gox 事件后，交易所广泛采用多重签名钱包和资产储备证明（PoR）。Bybit 事件暴露了多签系统的潜在漏洞，可能促使行业对 MPC 钱包、硬件签名等方案进行升级。

– **监管加强：**每次重大黑客事件都会促使监管机构介入，推动交易所和 DeFi 项目加强安全措施，如多重签名钱包和资产储备证明。KYC/AML 要求提升。Mt. Gox 促使日本政府制定《支付服务法》，对加密交易所进行监管。Ronin 桥（2022）事件后，美国政府加强对朝鲜 Lazarus Group 相关钱包的监控。2022 年美国 OFAC 制裁 Tornado Cash，阻止黑客使用该平台洗钱（2025 年法院裁定撤销）。

总的来说，黑客攻击如同一面镜子，既暴露加密行业的脆弱性，也折射其进化潜力。短期看，事件冲击市场信心并引发动荡；长期看，它们倒逼行业技术升级与制度完善。

4 行业启示与建议

加密行业面临着多重安全挑战，这些挑战既来自技术本身的复杂性，也涉及人为因素以及监管与合规性问题。首先是技术层面的复杂性与潜在漏洞，由于区块链技术仍在快速发展，不可避免地存在尚未被发现的脆弱性，加之智能合约审计不足，使得项目容易遭受攻击，甚至基础区块链技术本身也可能存在安全隐患。其次，人为因素是另一个重要挑战，包括用户普遍存在的弱密码和不良习惯，以及缺乏安全最佳实践的教育，此外，内部管理漏洞也可能导致员工作恶，从而威胁平台安全。最后，监管与合规方面也存在诸多问题，缺乏有效的监管监督，反洗钱机制面临困境，如跨链转移的复杂性、地址分散以及 DeFi 协议的匿名性，再加上无 KYC 交易所的滥用，都为黑客攻击和洗钱活动提供了可乘之机。要应对这些挑战，加密行业防范黑客攻击、保障加密安全需从技术、风险分散、用户教育和监管等多方面入手，构建多层次的安全防护体系。

4.1 技术防御升级

为了提升加密资产安全性，行业必须在多个层面加强防护措施。首先，在私钥管理与验证机制方面，应采用去中心化密钥管理解决方案，例如多方计算（MPC）钱包，这可以有效消除单点私钥泄露的风险，并确保交易必须经过多方授权。同时，使用硬件安全模块（HSM）或硬件钱包（如 Ledger）存储私钥，可将私钥与网络攻击隔离开来。此外，通过增加验证节点数量（例如 Ronin 将验证者从 9 个增至 21 个），可以构建动态验证机制，进一步降低单点控制的风险。

在智能合约与协议安全方面，采用形式化验证工具（如 Certora 和 OpenZeppelin）对智能合约进行数学证明级的审计，有助于确保代码逻辑无漏洞，从根本上降低安全风险。同时，部署零知识证明技术（例如 ZK-Rollups）来验证跨链交易，可以替代传统的多签机制，提升匿名性和安全性。模块化架构设计（例如采用 Celestia）通过将数据可用性与执行层分离，也能够有效降低系统性风险。

最后，在实时监控与应急响应方面，建议部署链上分析平台（如 Chainalysis 和 TRM Labs），以实时追踪异常交易和大额资金流动，从而及时发现潜在威胁。同时，通过设定风险阈值，触发自动熔断机制（例如在 Ronin 攻击后暂停跨链桥提现或交易功能），可以在风险扩大前及时切断攻击路径，保护用户资产安全。

4.2 合规与监管协同

在全球监管框架建设方面，日本《支付服务法》的经验值得借鉴，强制要求交易所披露冷热钱包资产比例，并实施多重签名和第三方安全审计，以确保平台安全性。同时，建立跨国链上数据共享网络，实现反洗钱协作，追踪黑客资金流向（如美国对朝鲜 Lazarus Group 钱包的监控），进一步强化行业整体安全监管。对于 DeFi 合规化，应推动各协议整合 KYC/AML 模块，对用户身份进行严格验证，防止匿名账户滥用。此外，推广监管沙盒试点，为创新项目在受控环境中测试提供机会，从而平衡安全与效率，这一模式可参考新加坡 MAS 的监管框架。

4.3 运营透明化与风险分散

为了增强用户信任并降低系统性风险，加密行业需在资产透明化和保险机制覆盖方面采取有效措施。首先，为了提升资产透明度，交易所应定期发布储备金证明（PoR）（如 Gate.io 就定期发布储备金证明报告），DeFi 平台可以公开链上储备地址和审计报告，证明其资产足额托管，从而消除用户对资金安全的疑虑。此外，采用去中心化预言机进行多源数据验证，能够有效避免价格操纵和清算漏洞（如 Bybit 事件中的 USDe 偏差），确保交易和清算过程的公平性与准确性。

其次，保险机制可以在风险防范中发挥关键作用。交易所和 DeFi 平台可以通过设立协议保险基金，为潜在的黑客攻击损失提供资金保障。同时，与第三方保险平台合作，为用户资产投保，能够进一步分散系统性风险，确保在极端情况下用户资金仍能得到赔付。这些措施不仅提升了平台的安全性，也可以增强用户对加密生态的信任。

4.4 用户教育与社区协作

为了提升加密行业的安全水平，安全意识普及和白帽黑客激励是不可或缺的环节。首先，安全意识普及是防范安全事件的基础。通过向用户提供安全操作指南，普及冷钱包使用、钓鱼攻击识别、合约授权风险等知识，能够帮助用户更好地保护自己的资产。此外，定期开展模拟攻击活动（如“红队演练”），以测试平台防御能力，及时发现并修复安全漏洞。与此同时，通过设立漏洞赏金计划（例如 Immunefi 平台提供的高额奖励）鼓励白帽黑客积极提交漏洞报告，从而加速问题修复。最后，借助 DAO 等社区治理机制，让社区成员参与安全升级方案的投票决策，增强共识和信任，共同推动平台安全标准的不断提升。

4.5 行业生态协作

为了提升跨链安全和整个加密生态的稳健性，建立跨链安全联盟至关重要。通过组建行业安全联盟，如区块链安全联盟（BSA），可以实现共享攻击情报，实时同步黑客攻击手法与防御策略，从而提升整个行业的防御能力。同时，推动跨链通信协议（如 IBC）的标准化，可以减少兼容性漏洞，确保不同链之间的安全互操作。此外，技术开源与生态互操作性也是关键。鼓励项目公开核心模块代码，如以太坊客户端，接受社区审查，可以增强代码的透明度和安全性。通过 LayerZero 等协议实现多链资产互操作，降低单链依赖风险，也能有效分散潜在风险，提升整体生态的抗风险能力。

通过上述举措，加密行业可以构建一个“技术-监管-用户”三位一体的安全体系。技术升级是这一体系的基石，通过零知识证明（ZK）、多方计算（MPC）等先进工具，能够有效抵御日益复杂的攻击。合规协作则是不可或缺的框架，它确保全球监管与反洗钱网络能够有效运作，形成强大的合力。用户信任是这一体系的核心，通过透明化运营和持续的用户教育，可以显著提升社区的整体韧性。

5 总结

加密货币市场在追求创新与效率的道路上，始终与安全风险如影随形。2025 年加密货币市场面临的安全挑战前所未有，以 Bybit 交易所遭受的巨额黑客攻击为代表，不仅揭示了中心化交易所安全防护的薄弱环节，也凸显了整个行业在技术、监管、用户教育等方面的短板。黑客攻击手法的不断升级，洗钱手段的日益复杂，以及由此引发的市场恐慌和投资者行为异化，都对加密市场的稳定性和可持续发展构成了严峻威胁。

然而，每一次危机也都是一次进步的契机。从 Mt.Gox 的信任崩塌到 Poly Network 的跨链危机，再到 Bybit 的冷钱包沦陷，每一次攻击都在倒逼行业进化。通过对历次重大黑客事件的深入分析，我们得以洞察行业生态的脆弱性，并从中汲取经验教训。为了应对这些挑战，加密行业必须构建一个多层次、全方位的安全防护体系。这包括：

- **技术防御升级：**采用去中心化密钥管理、形式化验证、零知识证明等先进技术，从根本上提升智能合约和协议的安全性。
- **合规与监管协同：**建立全球统一的监管框架，加强反洗钱协作，推动 DeFi 合规化，平衡创新与安全。
- **运营透明化与风险分散：**提升资产透明度，建立完善的保险机制，增强用户信任。
- **用户教育与社区协作：**普及安全知识，鼓励白帽黑客参与，构建强大的社区安全防线。
- **行业生态协作：**建立跨链安全联盟，推动技术开源与生态互操作性，提升整体生态的抗风险能力。

加密行业正处于一个关键的转折点。只有通过技术、监管和社区的共同努力，才能构建一个更加安全、透明和可持续的未来。每一次黑客攻击都是一次警醒，促使我们不断反思和改进。唯有如此，加密市场才能在挑战中成长，在变革中前行，最终实现其真正的潜力。

作者：Ember

6 参考资料

1. https://defillama.com/hacks
2. https://dune.com/legionx/tornadocashstats
3. https://www.footprint.network/@Beosin/Footprint-Beosin-2024-Web3-Security-Report#type=dashboard
4. https://www.footprint.network/@Beosin/Footprint-Beosin-2023-Web3-Security-Report#type=dashboard
5. https://peckshield.com/static/pdf/2020_2.pdf
6. https://www.slowmist.com/report/2024-Blockchain-Security-and-AML-Annual-Report%28CN%29.pdf
7. https://sussblockchain.com/review-of-the-anti-money-laundering-analysis-of-the-web3-blockchain-security-situation-in-the-first-half-of-2023/
8. https://news.qq.com/rain/a/20250225A05C7R00?suid=&media_id=
9. https://www.theblockbeats.info/news/56981
10. https://arxiv.org/abs/2305.14748
11. https://cdn.prod.website-files.com/6082dc5b670562507b3587b4/67a66929a076faf602d64b4c_TRM%202025%20Crypto%20Crime%20Report.pdf
12. https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/
13. https://cdn.prod.website-files.com/6082dc5b670562507b3587b4/67a66929a076faf602d64b4c_TRM%202025%20Crypto%20Crime%20Report.pdf
14. https://zh.wikipedia.org/wiki/Mt._Gox
15. https://www.gate.io/trade/BTC_USDT
16. https://intel.arkm.com/explorer/entity/mt-gox
17. https://cn.cointelegraph.com/news/poly-network-hacker-returns-258m-conducts-ama-on-how-it-went-down
18. https://www.odaily.news/post/5171470
19. https://www.gate.io/trade/ETH_USDT
20. https://www.coingecko.com/en/coins/o3-swap
21. https://defillama.com/protocols/Bridge
22. https://www.aicoin.com/zh-Hans/article/289899
23. https://foresightnews.pro/article/detail/1683
24. https://defillama.com/chain/Ronin
25. https://abmedia.io/us-court-overturns-tornado-cash-sanctions
26. https://dune.com/gate_research/bybit-security-breach-tracker#according-to-on-chain-analysis-the-stolen-assets-primarily-include
27. https://defillama.com/cex/bybit?usdInflows=true&tvl=true&twitter=false#tvl-charts

28. https://data.chain.link/feeds/ethereum/mainnet/usde-usd
29. https://dune.com/KARTOD/AAVE-Liquidations
30. https://x.com/omeragoldberg/status/1893440510682964012

相关链接

Gate研究院社媒

往期研究报告

关于 Gate 研究院

Gate 研究院是专注于区块链产业研究的专业机构，长期致力于深入研究区块链产业发展趋势， 为从业人员和广大区块链爱好者提供专业、前瞻性的产业洞察。我们始终秉持着普及区块链知识的初心，力求将复杂的技术概念转化为通俗易懂的语言，透过对海量数据的分析和对市场趋势的敏锐捕捉，为读者呈现区块链行业的全貌，让更多人了解区块链技术，并参与这个充满活力的产业。

research@gate.me