Gate Research

从黑客攻击到监管反思：2024 年加密货币安全现状分析

摘要

- 自 2012 年至 2024 年 11 月，区块链生态共发生 1,740 起公开安全事件，造成约 337.44 亿美元损失；
- 2024 年，区块链行业安全事件频发，共发生 369 起，导致约 23.08 亿美元损失，黑客攻击构成主要威胁；
- 2024 年，私钥泄露事件造成高达 11.99 亿美元的损失，占所有黑客攻击损失的 62.3%，凸显了私钥安全在行业中的重要性；
- 2024 年前三季度，合约漏洞攻击最为频繁，其中业务逻辑漏洞、重入漏洞和访问控制漏洞造成了最严重的损失；
- 中心化交易所（CEX）遭受的损失最为严重，而 DeFi 是最易受到攻击的领域；
- 以太坊由于生态的成熟和庞大的资金规模，成为黑客的首要目标。BSC 和 Arbitrum 等快速发展的新兴生态也成为黑客攻击的新选择；
- 2024 年被盗资金中，约 25.3% 被冻结或追回，但仍有 58.7% 留在了黑客地址；
- 各国监管机构正通过加强 KYC 和稳定币监管等措施，积极应对加密货币领域的洗钱和欺诈活动，保护投资者利益。

关键词：

Gate Research, 安全事件, 黑客攻击, 反洗钱

从黑客攻击到监管反思：2024 年加密货币安全现状分析

1 前言

在比特币突破 9 万美元，创下历史新高的同时，Meme 币也备受市场关注，GOAT、PUNT、BAN 等一众 Meme 币巨大的财富效应引爆了市场热情。然而，正当投资者沉浸在暴富的幻想中时，一场突如其来的黑客攻击事件打破了市场的狂欢。去中心化交易所 DEXX 遭遇黑客入侵，大量用户资产被盗，多个相关 Meme 币价格暴跌。此次事件再次凸显了加密货币市场安全的重要性。

DEXX 事件暴露了去中心化交易所在安全方面存在的诸多问题，也警示我们，在享受加密货币带来的便利的同时，必须高度重视安全问题。事实上，随着加密货币市场的快速发展，安全问题日益凸显。黑客们利用各种手段，如系统漏洞、钓鱼攻击、智能合约漏洞等，对加密资产发起攻击，导致用户遭受巨额损失。

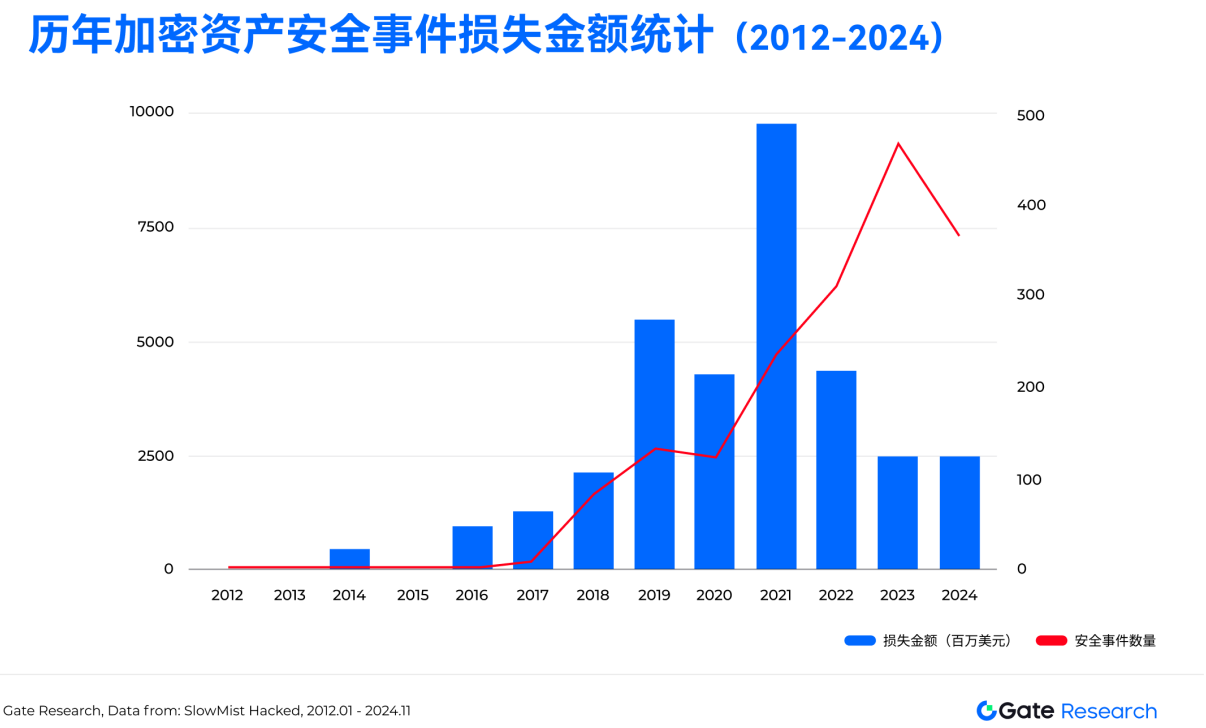
本文将深入剖析 2024 年加密货币安全领域的现状与趋势。我们将对这一年发生的重大安全事件进行回顾，分析攻击者的常用手法、攻击目标以及造成的损失。同时，我们也将探讨历史上的经典案例，总结其中的经验教训。此外，本文还将展望未来加密货币安全领域可能面临的挑战和机遇，并探讨监管机构和行业参与者如何共同应对这些挑战，构建更加安全可靠的加密货币生态系统。

2 历年加密安全事件总览

根据 SlowMist Hacked 的不完全统计，自 2012 年至 2024 年 11 月，全部区块链生态被公开的加密安全事件 1,740 起，损失总金额约 337.44 亿美元。从整体趋势来看，加密安全事件的数量和造成的损失金额呈现出逐年上升的态势，尤其在 2021 年和 2022 年达到高峰。

每年被统计到的加密安全事件数量从 2012 年的 32 起逐年攀升，并在 2021 年达到峰值，随后略有回落，但到 2024 年仍达到 369 起。随着加密货币市场规模的扩大和加密资产价值的攀升，针对区块链生态的攻击愈发频繁。损失金额与事件数量的变化趋势高度一致，从 2012 年的 597 万美元激增至 2022 年的 439.8 亿美元，增长了数万倍。每一次攻击造成的损失金额不断攀升。加密市场的高速发展吸引了大量参与者，但也成为黑客的“聚宝盆”。尤其在 2021 年和 2022 年加密市场最为火热时，加密资产价格大幅上涨，引来了大量投机者和黑客。不过，2023 年的数据显示，安全事件数量和损失金额较 2022 年有所回落，这可能与加密市场整体降温以及行业对安全的重视程度提升有关。

图 一：历年加密资产安全事件损失金额统计（2012-2024）

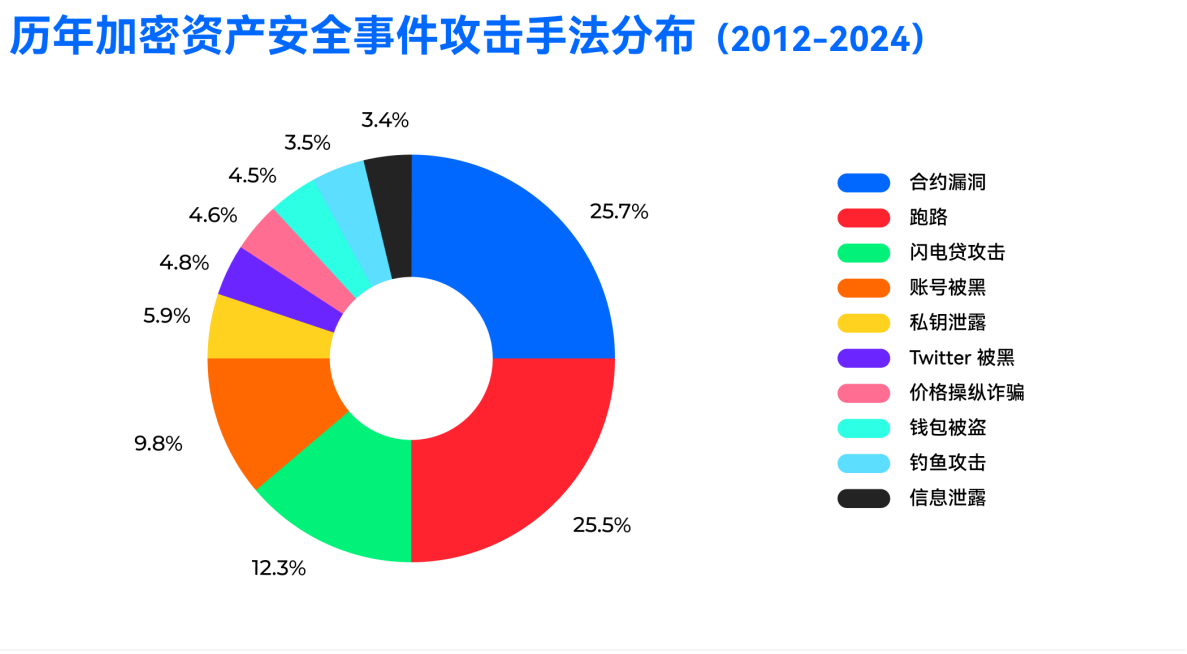


从攻击手法来看，历年加密安全事件主要集中在十种类型上，分别是：合约漏洞、跑路（Rug Pull）、闪电贷攻击、账号被黑、私钥泄露、Twitter 被黑、价格操纵诈骗、钱包被盗、信息泄露和钓鱼攻击。其中，合约漏洞、跑路和闪电贷攻击是近年来最常见的攻击手法，三者合计占比超过 50%。具体来看，合约漏洞占比最高，达到 25.7%；其次是跑路，占比 25.5%；闪电贷攻击占比 12.3%。智能合约的安全性、项目方的信誉以及 DeFi 协议的设计缺陷是当前加密领域最主要的风险点。

- Rug Pull（跑路）是一种常见的加密欺诈手段。骗子通过制造虚假繁荣，创建一个看似前景广阔的加密项目，吸引投资者大量投入资金。一旦资金积累到一定程度，项目方就会卷款潜逃，留下毫无价值的代币，或者直接关闭项目，导致投资者遭受巨大损失。
    - Thodex，这家总部位于土耳其的加密货币交易所，于 2021 年 4 月突然关闭，其创始人 Faruk Fatih Özer 卷款数十亿美元潜逃，导致近 39.1 万用户蒙受超过 20 亿美元的损失，成为加密货币史上最严重的跑路事件之一。
- 智能合约漏洞是指智能合约代码中存在的安全隐患，黑客可以利用这些漏洞发起攻击，从而导致用户资产遭受损失。
    - 2016 年 6 月，黑客利用 The DAO 智能合约中的重入漏洞，通过不断调用合约的提款功能，实施了重入攻击，成功窃取了约 360 万 ETH，折合当时市值约 5,000 万美元。

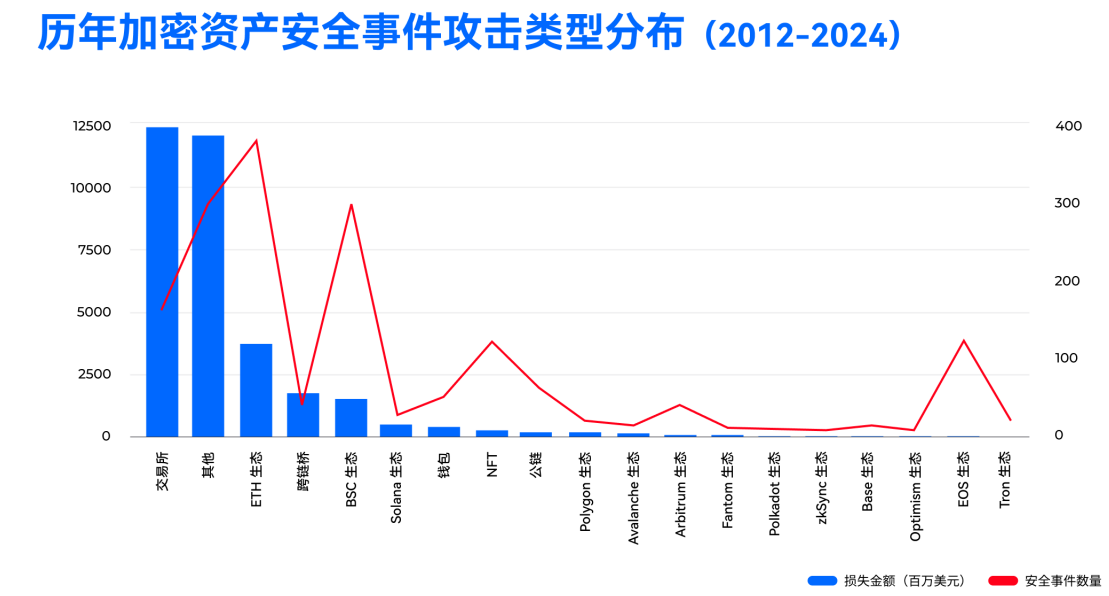
- 闪电贷攻击是一种利用 DeFi 平台/协议的瞬时借贷功能，在同一笔交易中借入大量资金，随后通过操纵市场价格或利用价格差异进行套利，以获取不当利益的攻击方式。
    - 2023 年 3 月 13 日，DeFi 借贷协议 Euler Finance 遭受了闪电贷攻击。攻击者通过借入巨额闪电贷，实施高倍杠杆操作，触发协议的清算机制，最终盗取了约 1.97 亿美元的资金。

图 二：历年加密资产安全事件攻击手法分布（2012-2024）



从攻击造成的损失金额来看，交易所无疑是黑客的首要目标。数据显示，交易所的损失金额高达 123.74 亿美元，远超其他类别。这主要是因为交易所集中存储了大量的用户资产，一旦被攻破，损失将极为惨重。此外，ETH 生态和跨链桥等高度合作、资金流动频繁的生态系统，也成为了黑客的重点关注对象。其中，ETH 生态因其发展历史较长、项目众多，安全事件数量高达 379 起，位居首位。

图 三：历年加密资产安全事件攻击类型分布（2012-2024）



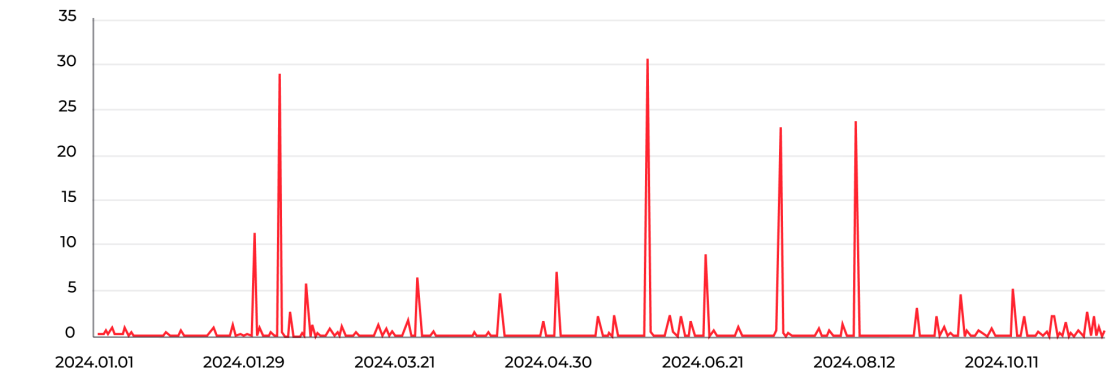
Gate Research, Data from: SlowMist Hacked, 2012.01 - 2024.1

Gate Research

3　2024 年加密安全事件态势概述

根据 SlowMist Hacked 的不完全统计，2024 年全部区块链生态被公开的加密安全事件 369 起，损失总金额约 23.08 亿美元。这一数字表明，加密资产安全问题不容忽视，频繁的安全事件给行业带来了巨大的经济损失。

图 四：2024 年加密资产安全事件损失金额统计



Gate Research, Data from: SlowMist Hacked, 2024.01 - 2024.11

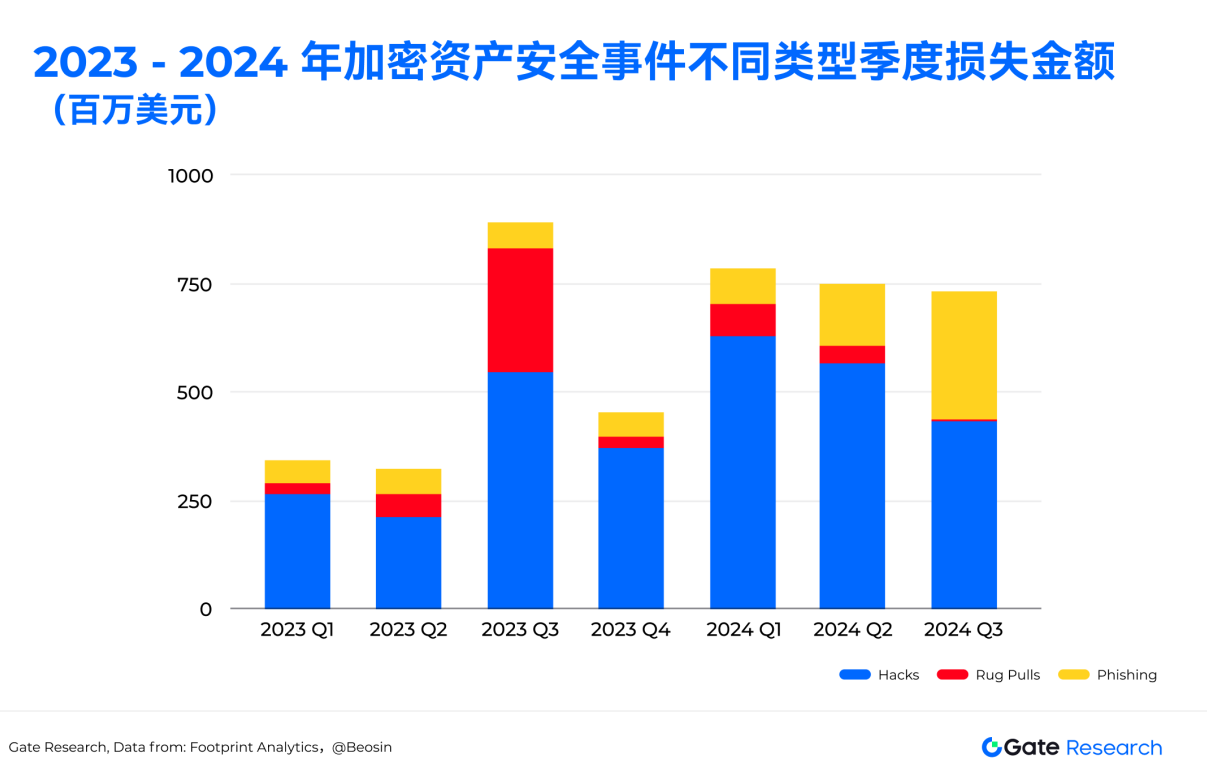
Gate Research

3.1 安全事件类型分析

我们将上述历年攻击手法中的合约漏洞、闪电贷攻击、账号被黑、私钥泄露、Twitter 被黑、钱包被盗、信息泄露等，统称为黑客攻击；钓鱼攻击和价格操纵诈骗，则统称为钓鱼诈骗。因此，可以将历年攻击手法大致分为黑客攻击 (Hacks)、跑路 (Rug Pulls) 和钓鱼诈骗 (Phishing) 三大类型。

Beosin Alert 数据显示，2024 年前三季度 Web3 领域安全事件频发，导致总损失高达 22.76 亿美元，同比增长 45%。其中，黑客攻击损失最为严重，达 16.24 亿美元，同比增长 59.18%。黑客攻击手段日益复杂，对 Web3 生态系统的安全构成严重威胁。钓鱼诈骗损失也同比增长 191.26%，达到 5.28 亿美元。2024 年上半年，钓鱼诈骗损失显著上升，表明黑客越来越擅长利用用户心理弱点，通过伪造网站或信息诱骗用户泄露私钥或转账。相较之下，2024 年 Rug Pull 事件损失有所下降，仅为 1.22 亿美元，同比下降 66.54%。这可能与社区对 Rug Pull 事件警惕性提高，以及相关监管措施加强有关。

图 五：2023 - 2024 年加密资产安全事件不同类型季度损失金额

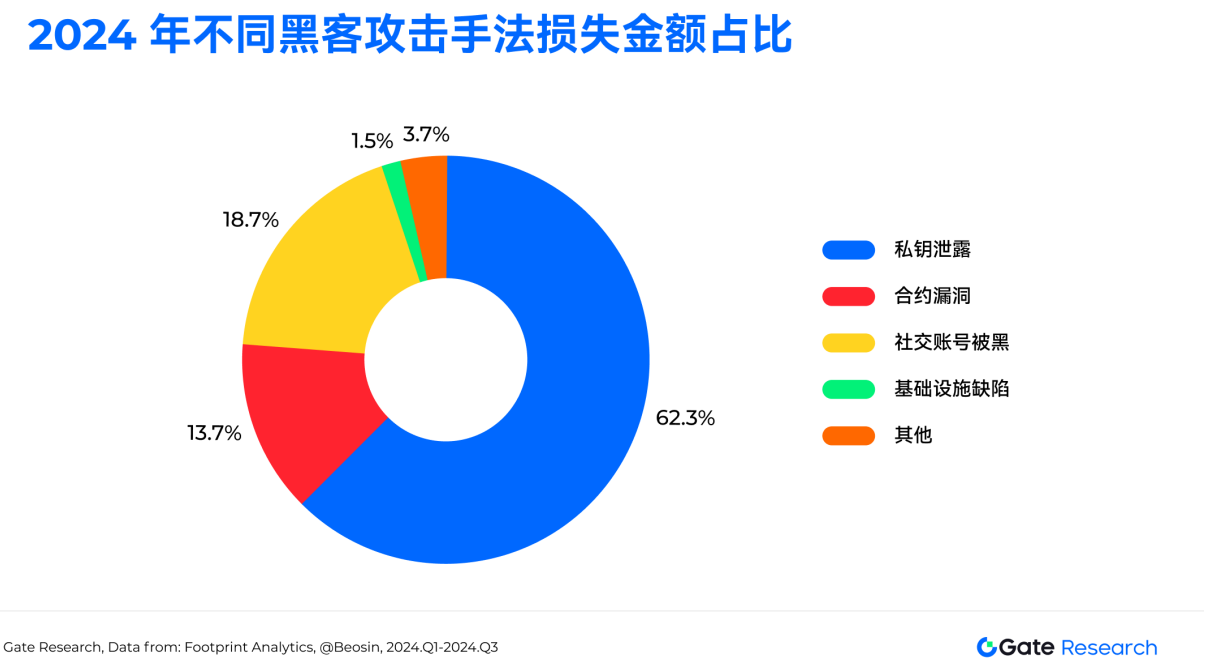


3.2 黑客攻击手法分析

2024 年前三季度，私钥泄露事件造成 11.99 亿美元的损失，在所有黑客攻击损失中占比 62.3%，与 2023 年相似，私钥泄露事件依旧是所有黑客攻击类型中损失最高的。其次是通过攻击社交账户信息造成的损失，合约漏洞利用则排名第三，占比 13.7%。

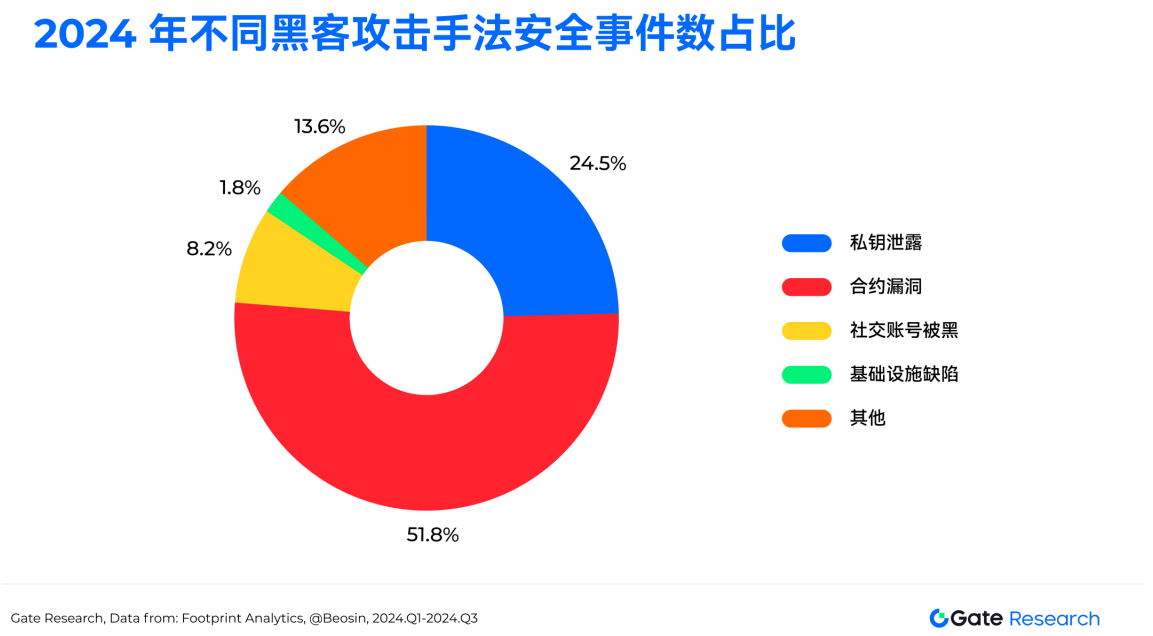
2024 年，DMM Bitcoin（3.08 亿美元）、PlayDapp（2.9 亿美元）、WazirX（2.3 亿美元）、Ripple 联合创始人 Chris Larsen（1.12 亿美元）、BtcTurk（5,500 万美元）、BingX（4,500 万美元）和 Indodax（2,200 万美元）等多个平台和个人因私钥泄露遭受了重大损失。这些事件表明，私钥安全问题仍然是加密货币行业面临的最大挑战之一。

图 六：2024 年不同黑客攻击手法损失金额占比



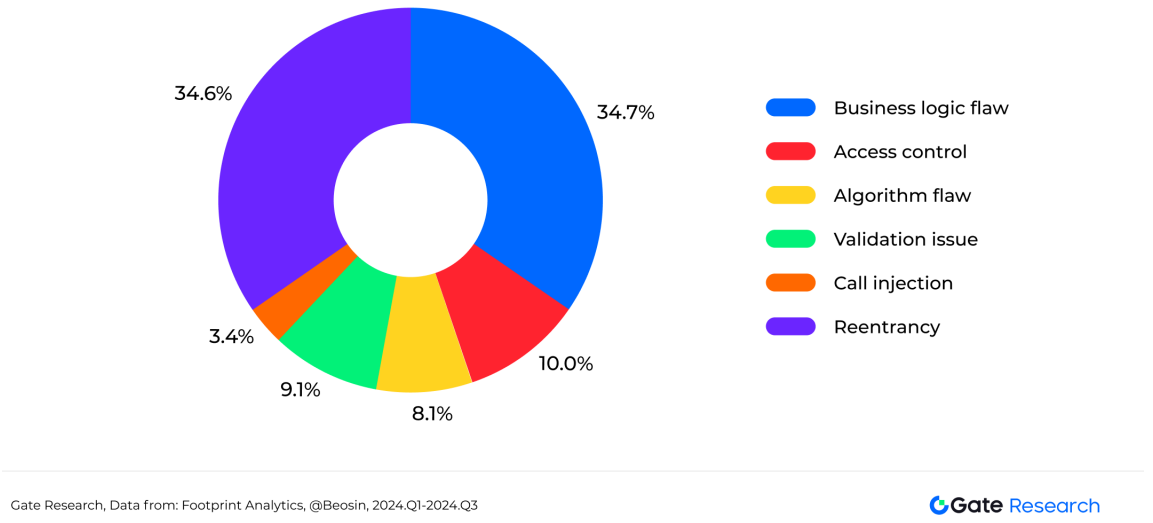
从安全事件数量来看，2024 年前三季度，合约漏洞攻击最为猖獗，占比高达 51.8%。黑客通过利用智能合约代码中的漏洞，实施各种攻击手段，窃取用户资产。尽管合约漏洞造成的直接经济损失（占比 13.7%）不及私钥泄露严重，但其高发的态势不容忽视。部分项目由于合约设计存在诸多缺陷，极易成为黑客攻击的目标。

图 七：2024 年不同黑客攻击手法安全事件数占比



从漏洞类型来看，2024 年前三季度造成损失最大的前三种漏洞分别是：业务逻辑漏洞（Business logic flaw）、重入漏洞（Reentrancy）及访问控制漏洞（Access control），分别占比 34.7%、34.6%、10%。出现次数最高的漏洞也为业务逻辑漏洞，其次是验证问题（Validation issues）。

图 八：2024 年不同黑客攻击漏洞类型安全事件数占比

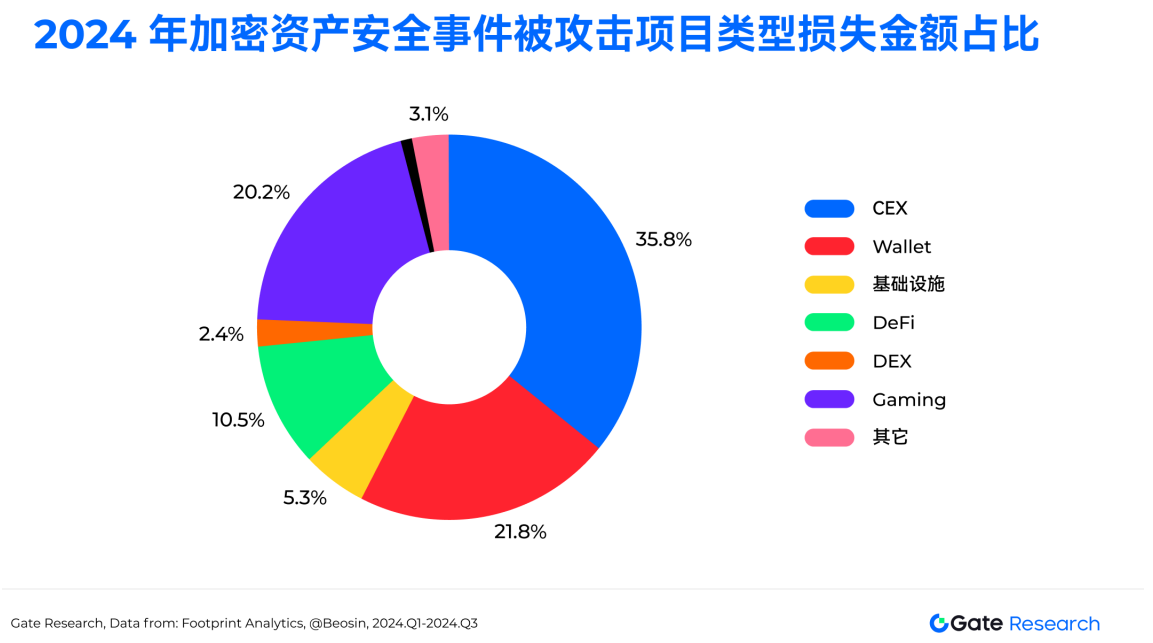


3.3 被攻击项目类型分析

从项目赛道来看，2024 年前三季度，中心化交易所（CEX）遭受的损失最为严重，占比高达 35.8%，累计损失达 6.88 亿美元。其中，DMM Bitcoin 事件最为严重，损失金额高达 3.08 亿美元，是加密货币黑客攻击史上受害金额排名第七的安全事件，也是 2024 年损失最大的安全事件。此次 DMM Bitcoin 事件是继 2014 年 Mt.Gox 事件和 2018 年 Coincheck 事件后，日本发生的第三大加密货币交易所盗窃案。因为 CEX 集中了大量用户资产，更易于成为黑客的重点目标。虽然 CEX 的安全事件发生频率相对较低，但单次事件造成的损失往往巨大，对整个交易所生态的安全性构成了极大的威胁。

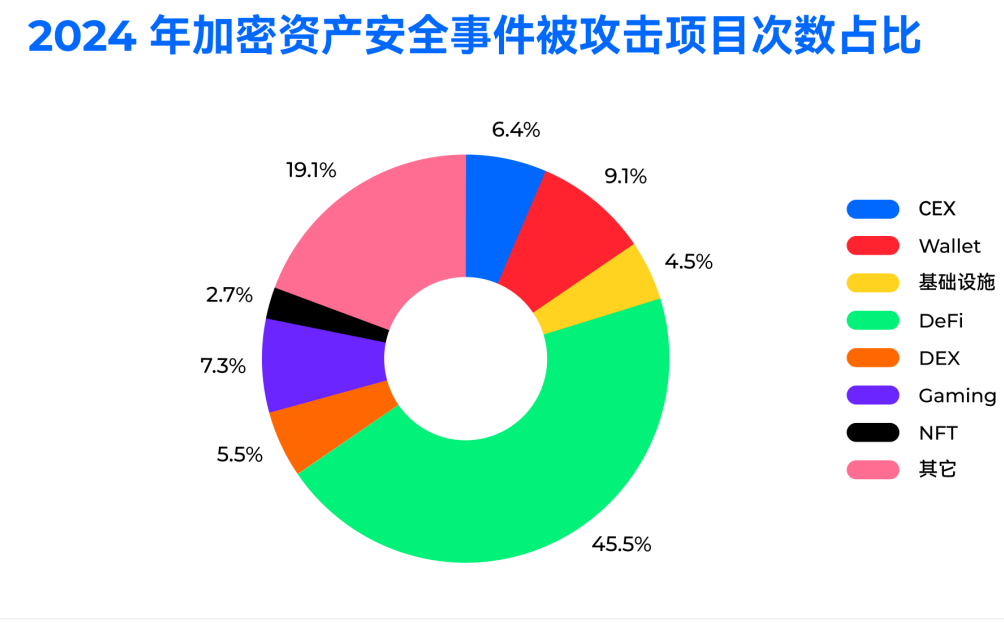
其次，钱包和游戏类项目也遭受了较大损失，分别占比 21.8% 和 20.2%。钱包作为用户存储加密资产的首选，一旦被攻破，损失往往惨重。而游戏类项目因其庞大的用户基数和大量的虚拟资产交易，也成为黑客攻击的高风险领域。以 5 月 20 日 Gala Games 受到攻击为例，攻击者通过铸造大量代币，然后迅速将其兑换为其他主流加密货币，给平台造成了巨大的损失。

图 九：2024 年加密资产安全事件被攻击项目类型损失金额占比



从被攻击项目次数来看，DeFi 是最易受到攻击的领域。根据 Beosin Alert 的数据，2024 年前三季度，DeFi 项目的攻击次数占比高达 45.5%，成为黑客的重点目标。DeFi 协议的复杂性、资金集中度高以及安全漏洞频发是其屡遭攻击的主要原因。相较之下，中心化交易所（CEX）和钱包项目虽然也受到攻击，但由于采用了多重安全措施，攻击次数相对较少。不过，DeFi 项目被攻击频率最高，但由于单笔交易额相对较小，导致的直接经济损失可能低于 CEX。这是因为 CEX 存储了大量用户资产，一旦被攻破，造成的损失往往更为严重。

图 十：2024 年加密资产安全事件被攻击项目次数占比



Gate Research, Data from: Footprint Analytics, @Beosin, 2024.Q1-2024.Q3

Gate Research

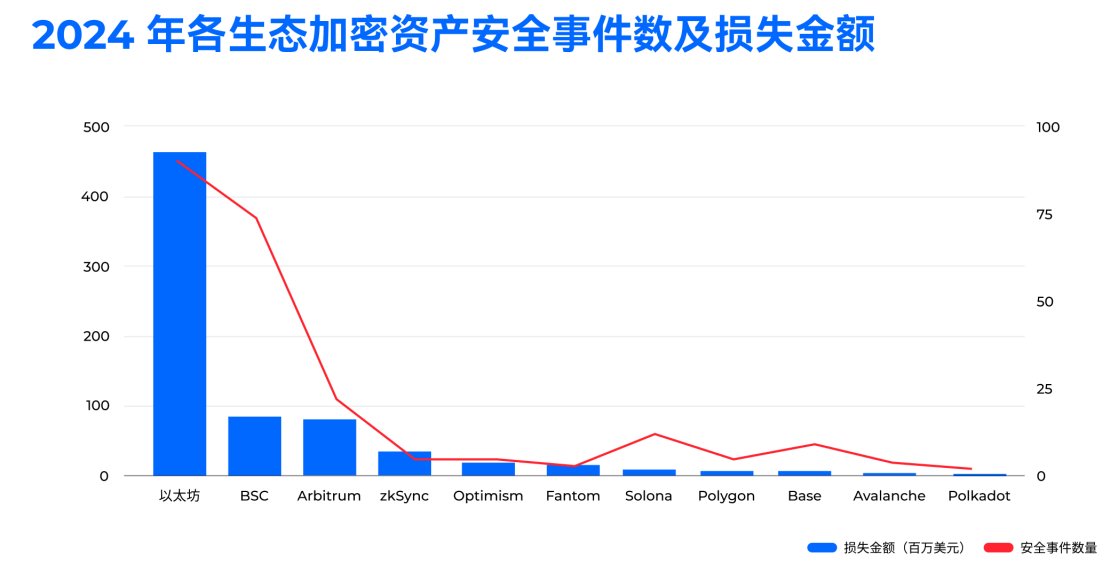
3.4 被攻击生态分析

从被攻击生态来看，2024 年，以太坊仍然是损失金额最高的公链，达到 4.6 亿美元；紧随其后的是 BSC，损失约 8,608 万美元，其次是 Arbitrum，约 8,323 万美元。以太坊之所以成为黑客攻击的首选目标，主要是因为它是目前最大的智能合约平台，拥有丰富的生态和庞大的资金体量。BSC 作为以太坊的竞争对手，也面临大量攻击，损失金额仅次于以太坊。

值得注意的是，Solana 生态在 2024 年的快速发展也使其成为了黑客的关注焦点。例如，5 月 16 日，基于 Solana 的代币启动器 pump.fun 遭遇了一起利用闪电贷的攻击，损失高达 8,000 万美元。这起事件凸显了 Solana 生态在安全方面仍存在较大的挑战。

此外，随着 Layer2 解决方案（如 Arbitrum 和 Optimism）的兴起，这些生态的安全性也受到了越来越多的关注。尽管这些生态在技术上进行了诸多优化，但仍不可避免地遭受了黑客攻击。

图 十一：2024 年各生态加密资产安全事件数及损失金额

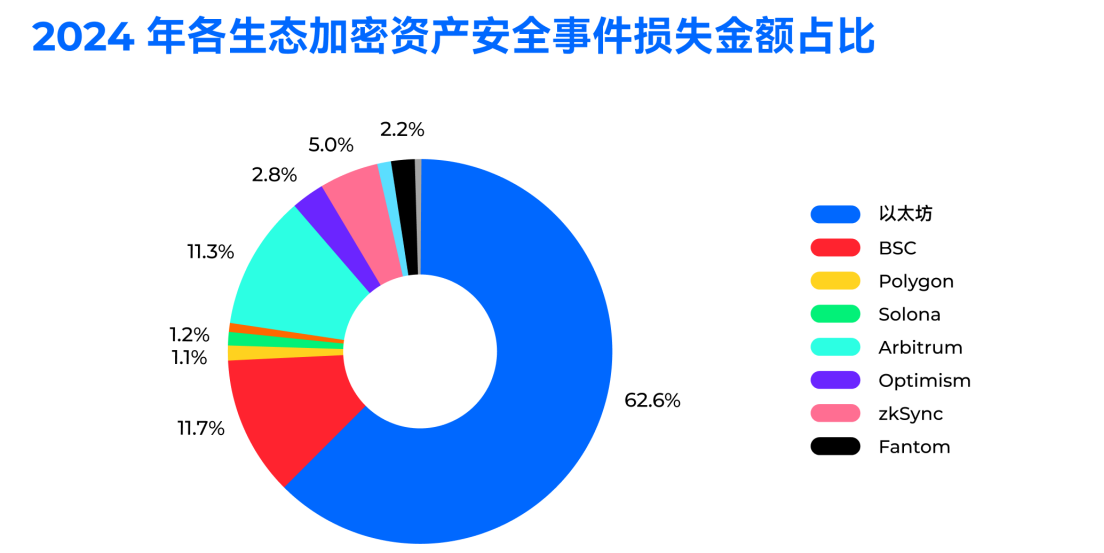


Gate Research, Data from: SlowMist Hacked, 2024.01 - 2024.11

Gate Research

此外，对比 2024 年各生态加密资产安全事件的损失金额和事件数量占比，我们可以发现：以太坊生态的损失金额占比高达 62.6%，远高于其他生态。虽然其安全事件发生次数占比仅为 39%，但单次攻击造成的损失却远高于其他生态。这可能与其作为最大的智能合约平台，拥有丰富的 DeFi 生态和庞大的锁仓资金量有关。一旦被攻击，损失往往更为惨重。相比之下，BSC 生态的安全事件发生次数与以太坊不相上下，占比达 32%，但损失金额占比仅为 11.7%，表明其虽然事件频发，但单次攻击造成的损失相对较小。

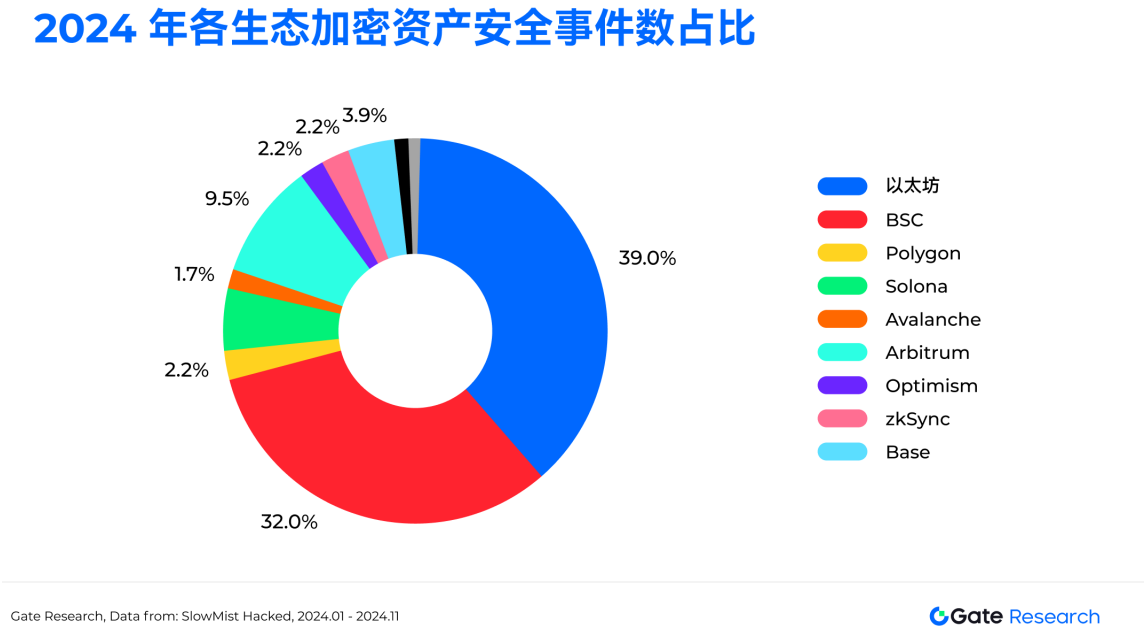
图 十二：2024 年各生态加密资产安全事件损失金额占比



Gate Research, Data from: SlowMist Hacked, 2024.01 - 2024.11

Gate Research

图 十三：2024 年各生态加密资产安全事件数占比



3.5 2024 年攻击事件回顾

2024 年，加密货币行业面临严峻的安全形势，黑客攻击事件频繁发生，给行业造成了巨大的经济损失。以下汇总了 2024 年前三季度的一些重大安全事件，涵盖了不同的攻击手法和显著的损失金额。

图 十四：2024 年加密安全部分典型攻击事件

2024 年加密安全部分典型攻击事件

事件名称	损失金额	攻击方式	事件描述
DMM Bitcoin	3.08 亿美元	私钥泄露	5 月 31 日，日本加密货币交易所 DMM Bitcoin 遭到攻击，盗取了价值约 3.08 亿美元的比特币。黑客将盗取的资金分散到 10 多个地址。
PlayDapp	2.9 亿美元	私钥泄露	2 月 9 日，区块链游戏平台 PlayDapp 遭黑客攻击，黑客铸造了 2 亿枚PLA代币，价值 3,650 万美元。2 月 12 日，在与黑客谈判失败后，黑客继续铸造了 15.9 亿枚 PLA 代币，价值达 2.539 亿美元。
WazirX	2.3 亿美元	钱包被盗	加密交易所 WazirX 发布初步调查结果，称其一个多重签名钱包遭到攻击，导致资金损失超过 2.3 亿美元。
BtcTurk	5,500 万美元	私钥泄露	土耳其加密货币交易所 BtcTurk 承认遭受黑客攻击，影响了包括多种加密货币的十个热钱包。交易所暂停了存款和取款，积极与执法部门合作。
Hedgey	4,470 万美元	闪电贷攻击	Hedgey Finance 遭受两次攻击，包括在以太坊和 Arbitrum 网络上的攻击，导致总损失。
FixedFloat	2,610 万美元	第三方漏洞	加密货币交易所 FixedFloat 确认遭到黑客攻击，资金被盗，正在努力提高安全性并进行调查。
Gala Games	2,180 万美元	私钥泄露	2024 年 5 月 20 日，Web3 游戏平台 Gala Games 遭攻击，攻击者铸造并迅速抛售了大量 GALA 代币。
Thala	2,550 万美元	安全漏洞	Aptos 生态 DeFi 项目 Thala 因安全漏洞导致资产被盗，已采取措施暂停合约并协商恢复用户资产。
DEXX	2,100 万美元	未知	链上交易终端 DEXX 的多名用户资金被盗，损失规模达 2,100 万美元。
BingX	4,500 万美元	未知	BingX 的安全系统检测到针对一个热钱包的未经授权的入侵。
U.S. Government-Controlled Wallet	近 2,000 万美元	未知	美国政府控制的钱包疑似转移了近 2,000万 美元的代币，随后有部分资金被返还给政府地址。

Gate Research, Data from: SlowMist Hacked

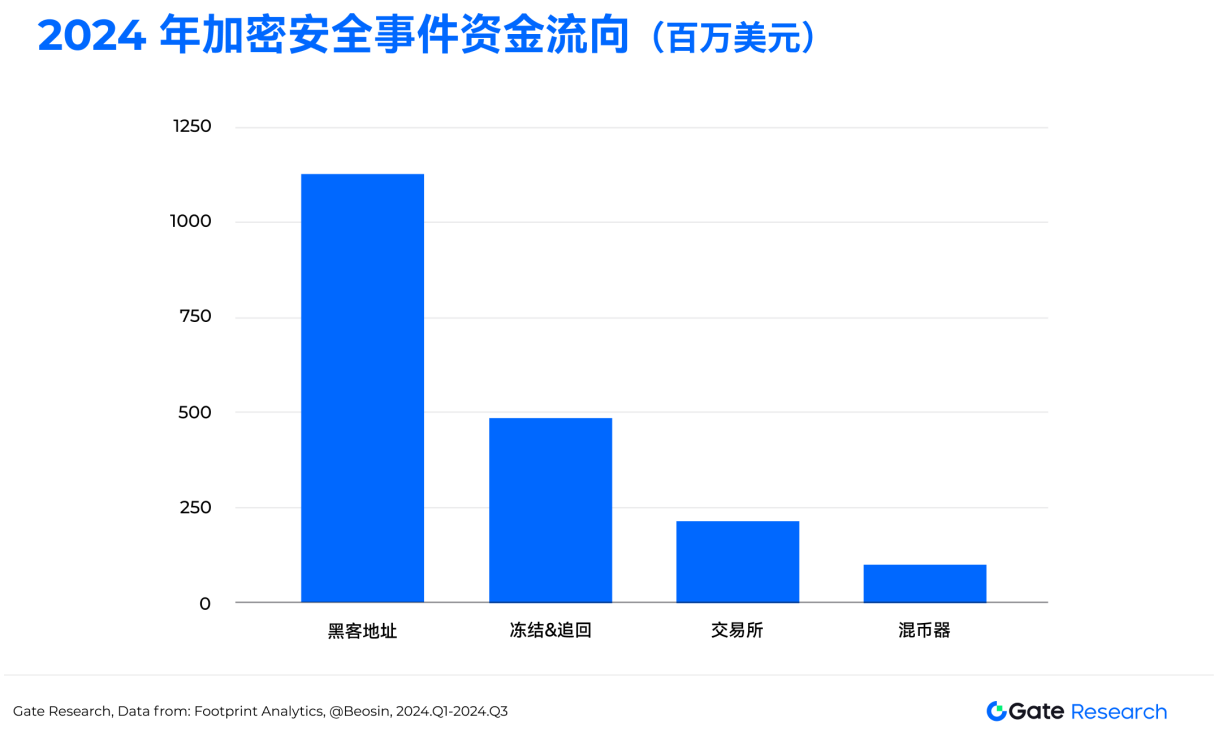
Gate Research

4　2024 年加密安全事件资金流向

4.1　被盗资金流向分析

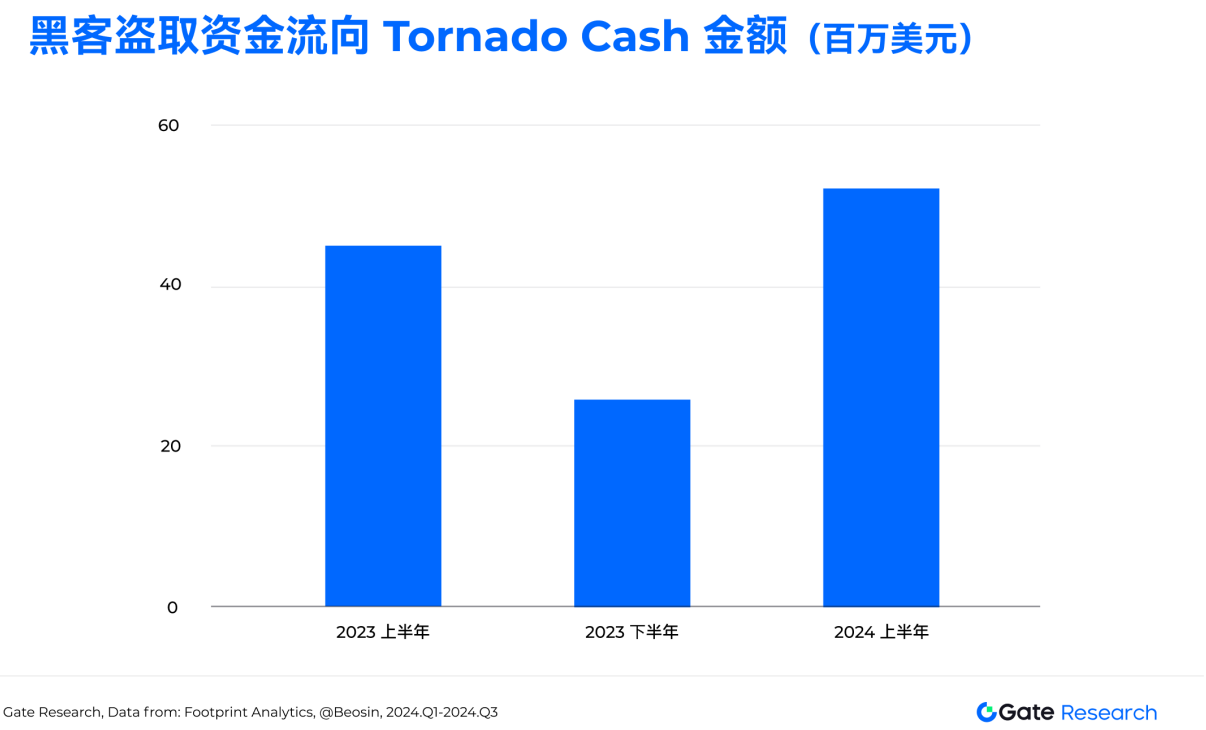
据 Beosin KYT 数据显示，2024 年被盗的资金中，约 25.3%（4.86 亿美元）被冻结或追回，较 2023 年显著提升。约 58.7%（11.29 亿美元）仍保留在黑客地址。随着全球监管机构反洗钱力度的加大，黑客清洗赃款难度增加，因此，黑客通常会先将盗取的资金转移到链上地址，以方便后续操作。约 10.9%（2.09 亿美元）的被盗资金转入交易所，比例高于 2023 年。仅有 5.1%（约 9,800 万美元）转入混币器，通过混币器清洗的被盗资金大幅减少。

图 十五：2024 年加密安全事件资金流向（百万美元）



通过上述数据可以看出，黑客盗取资金后去向主要有四种：被冻结或追回、保留在黑客地址、转入交易所以及通过混币器清洗。其中，Tornado Cash 是最常用的混币器之一。它允许用户通过混合交易提高交易隐私性，但同时也可能被用于非法活动，如洗钱。Beosin KYT 数据显示，2024 年上半年，黑客利用 Tornado Cash 洗钱的金额较 2023 年大幅增长，分别比上半年增长 15.42%，比下半年增长 103.42%，这表明黑客越来越依赖 Tornado Cash 来掩盖其资金来源。

图 十六：黑客盗取资金流向 Tornado Cash 金额（百万美元）



随着犯罪分子利用 Tornado Cash 等混币器进行洗钱活动，监管机构对加密货币混合服务的关注度日益升高。2022 年 8 月，美国财政部对 Tornado Cash 实施制裁的举措标志着监管层对加密货币隐私与反洗钱之间平衡的严厉态度。这一事件引发了整个行业的广泛关注，合规性和风险管理已成为加密平台的重中之重。各国政府纷纷加强对加密货币混合服务的监管，以防止洗钱和恐怖融资活动。

4.2 被盗资金的洗钱方式

近年来，加密货币被盗资金的洗钱手法日益复杂多样。黑客们不断创新，通过多层转账、混币服务、DEX 交易和匿名币等手段，极力掩盖资金来源。其中，朝鲜黑客组织 Lazarus Group 尤为活跃，多次对金融机构和加密货币交易所发动网络攻击，造成巨额损失。例如 Axie Infinity Ronin 攻击和 DMM Bitcoin 的攻击都与 Lazarus Group 密切相关，这两起事件都是加密货币史上规模最大的攻击之一。

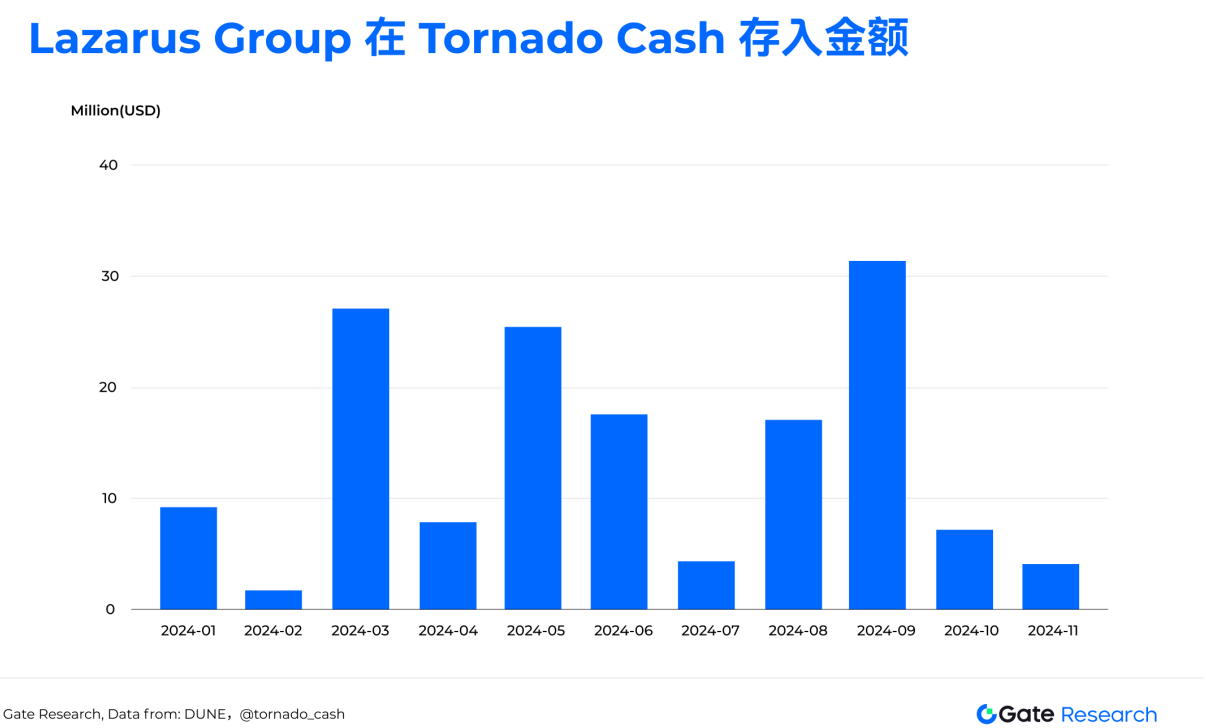
Lazarus Group 的洗钱策略经过多年演变，已形成一套成熟且复杂的体系。他们通常采取以下步骤：

1. 初始混淆：将盗取的加密货币存入 Tornado Cash 等混币器，切断交易链条，实现初步匿名化。
2. 跨链转移：利用 Thorchain 等跨链协议，将资金转换为不同加密货币，增加追溯难度。

3. 资金混淆：Lazarus Group 通过多个地址进行了资金混淆。例如，部分资金通过跨链到比特币链上，再利用 tBTC 协议将资金转移到以太坊，进一步增加洗钱的复杂性。
4. 分散存储：将资金分散到多个地址，并转移至监管较少的链，如 TRON 链。
5. 场外交易：通过 Paxful、Noones 等平台进行场外交易，将加密资产转换为法币或其他加密货币，规避 KYC 审查。

行业分析普遍认为，Lazarus Group 与 Tornado Cash 的资金流入量密切相关，这表明 Tornado Cash 在黑客洗钱活动中扮演着不可或缺的角色。数据显示，Lazarus Group 通过 Tornado.Cash 存入的 ETH 数量呈现出波动上升的趋势，表明其洗钱活动持续活跃。尽管监管部门不断加强对 Tornado Cash 的监管，但 Lazarus Group 通过不断创新洗钱手法，如多层转账、跨链转移等，成功规避监管，增加了执法难度。针对黑客组织的洗钱活动，监管部门需要与时俱进，加强国际合作，才能更有效地打击加密货币犯罪。

图 十七：Lazarus Group 在 Tornado Cash 存入金额



4.3 2024 年加密安全案例资金去向追踪

4.3.1 DMM Bitcoin 被盗资金跟踪：疑似 Lazarus Group 所为

4.3.1.1 背景介绍

日本知名加密货币交易所 DMM Bitcoin 于 2024 年 5 月遭遇了一场严重的网络攻击，导致大量比特币被盗。由于黑客攻击造成的巨大损失，DMM Bitcoin 决定停止运营。12 月 2 日，公司宣布将所有用户账户及公司资产转移至 SBI 集团旗下的 SBI VC Trade，这一资产转移计划预计将于 2025 年 3 月完成。

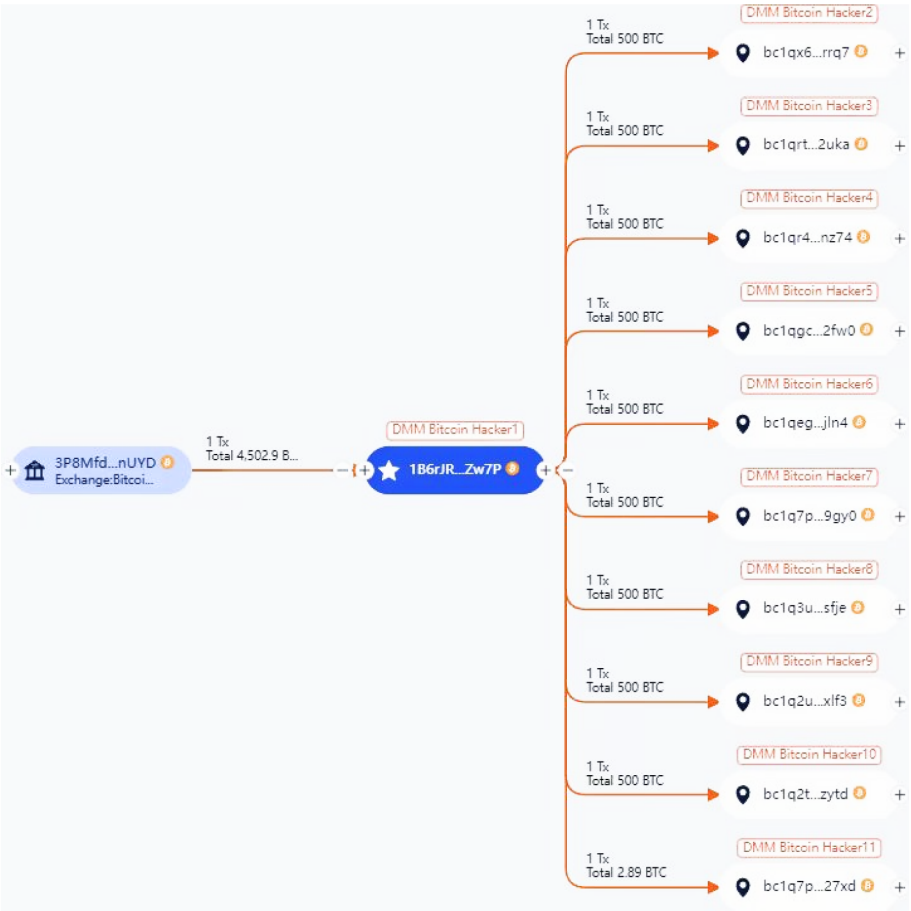
2024 年 5 月 31 日，黑客入侵 DMM Bitcoin 平台，盗取了 4,502.9 枚比特币，价值约 3.08 亿美元。截至 12 月 2 日，这些被盗比特币的价值已上涨至超过 4.29 亿美元。事件发生后，DMM Bitcoin 为减轻损失，对平台的提款和加密货币购买进行了限制。然而，这些措施未能阻止损失扩大，反而对用户服务造成了负面影响。

4.3.1.2 资金路径

区块链安全专家分析发现，被盗的比特币迅速分散至多个钱包，并通过可疑平台 Huione Guarantee 等进行洗钱。攻击手法和洗钱模式高度疑似为朝鲜国家支持的黑客组织 Lazarus Group 所为。

Beosin Trace 的追踪显示，被盗的 4,502.9 枚比特币已被分散至 10 个新地址。区块链侦探 ZachXBT 的调查显示，Lazarus Group 已通过柬埔寨的 Huione Guarantee 洗白了超过 3,500 万美元的 DMM Bitcoin 盗窃资金。

图 十八：DMM Bitcoin 被盗资金路径



Gate Research, Data from: BEOSIN

Gate Research

4.3.1.3 监管挑战

此次事件引发了市场对加密货币交易所安全的广泛关注。DMM Bitcoin 的停运凸显了交易所面临的严峻安全挑战，并引发了监管机构的密切关注。日本金融厅（FSA）的调查结果显示，该公司在风险管理方面存在严重缺陷，包括缺乏独立审计、安全职能集中化以及违反加密货币交易法规。

调查发现，DMM Bitcoin 未建立健全的风险管理体系，内部审计形同虚设，未能有效防范加密资产流失。公司未指派专人负责风险管理，相关职责被集中在少数人员手中。此外，公司未保存有助于调查盗窃事件的关键日志，违反了相关规定。FSA 已向公司发出“业务改善命令”，并强调公司在系统风险管理和应对加密资产泄漏风险方面存在严重问题。

此次事件是 2024 年最重要的加密货币盗窃案之一，也是日本历史上第二大非法加密货币流出事

件。它凸显了数字资产领域不断升级的网络安全威胁，并引发了对加密货币交易所监管的广泛关注。DMM Bitcoin 的遭遇再次警示我们，加密货币交易所正面临着巨大的安全风险。为了保护用户资产，交易所必须不断加强安全防护措施。同时，监管机构也应加强对加密货币市场的监管，以维护市场秩序，防止类似事件再次发生。

4.3.2 土耳其加密庞氏骗局：被盗资金跟踪

4.3.2.1 背景介绍

2024 年 5 月 30 日，土耳其警方对一个名为 Smart Trade Coin（STC）的加密货币项目进行了大规模突击行动，逮捕了 127 名涉嫌诈骗的嫌疑人，并查获了大量资产和枪支。

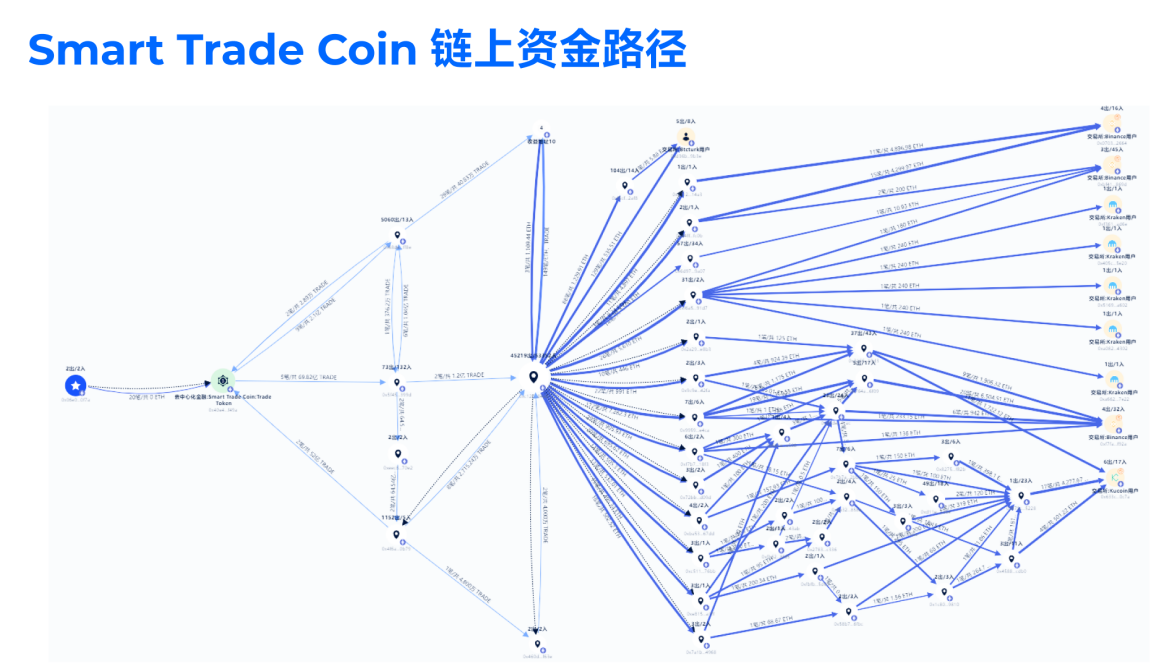
STC 项目自 2021 年推出以来，以其能够连接多个加密货币交易所、统一管理多个交易账户的高额回报承诺，吸引了大量土耳其投资者。然而，随着时间的推移，越来越多的投资者开始怀疑该项目是一个庞氏骗局。受害者律师表示，有高达 5 万名土耳其投资者深陷其中，总损失金额可能超过 20 亿美元。许多用户报告损失了 95% 的积蓄，并且无法核实这些资金是否被 STC 团队挪用。

4.3.2.2 资金路径

Beosin KYT 基于项目名称 Smart Trade Coin 的链上资金追踪分析显示，STC 代币合约通过 0x5f45 地址将大部分资金转出，并最终流入 0xc12c 地址。进一步追踪发现，0xc12c 地址进行了大量 ETH 的单向转出交易，转出金额巨大，接近公布的预计损失金额。而且，所有涉及 ETH 转出的交易手续费均由 0xc12c 地址支付，这进一步佐证了该地址被用于分发被盗资金。

下图仅展示了部分资金流向，0xc12c 地址涉及的转出交易超过 2 万笔。从已跟踪的交易数据来看，被盗资金在分发后，一部分被直接转入各大交易所，另一部分则通过拆分、合并、混淆等复杂操作，最终流入交易所。

图 十九：Smart Trade Coin 链上资金路径



Gate Research, Data from: BEOSIN

Gate Research

4.3.2.3 监管挑战

此次事件凸显了土耳其加密货币市场监管的严重不足。尽管政府一直鼓励创新，但缺乏有效的监管框架，导致不法分子有机可乘，损害了广大投资者的利益。地方政府应尽快建立健全的监管体系，以保护投资者权益，促进加密货币行业健康发展。

土耳其的经验表明，单纯追求加密货币自由并不可取。在鼓励创新发展的同时，必须加强监管，建立合规、透明的市场环境。只有这样，加密货币才能真正发挥其价值，成为促进经济发展、对冲风险的有效工具。政府和行业应共同努力，制定完善的监管法规，加强市场监管，提高行业透明度，共同营造一个安全、可靠的加密货币投资环境。

5 加密安全事件反洗钱监管

加密货币领域的洗钱活动愈演愈烈，严重威胁着金融安全。2024 年以来，为应对这一挑战，全球范围内针对加密货币的监管力度不断加强。各国监管机构要求虚拟资产服务商加强 KYC/AML 合规，并积极参与国际监管合作。然而，如何在保护投资者利益的同时，不扼杀创新，是监管机构面临的一大难题。加密货币行业也需要积极适应监管环境，在合规与业务发展之间寻求平衡。

各国在反洗钱监管方面的实践呈现出多样性。以中国香港、新加坡、美国、欧洲、日本、加拿大、澳大利亚、韩国、土耳其和马来西亚为例，这些地区均出台了相应的监管政策，主要集中在以下几个方面：一是加强对虚拟资产交易平台的监管，要求取得相关牌照；二是强化反洗钱和反恐融资措施，如实施 Travel Rule (资金移动规则：该规则要求处理加密资产转移的金融机构将客户信息传递给下一个机构，该信息应包括发件人和收件人的姓名和地址)，加强 KYC 认证；三是关注稳定币的监管，要求提高透明度和资本储备；四是保护投资者权益，打击欺诈和网络犯罪。这些监管举措表明，全球范围内正形成一种共识，即需要加强对加密货币市场的监管，以维护金融稳定和保护投资者利益。

图 二十：各国加密货币反洗钱监管措施

各国加密货币反洗钱监管措施

国家/地区	监管机构	主要监管措施
中国香港	1.香港金融管理局 2.香港证券及期货事务监察委员会	1.设立虚拟资产场外交易服务（OTC）发牌制度，要求所有相关服务必须获得牌照。 2.推出稳定币开发和发行的监管沙盒。 3.香港证券及期货事务监察委员会（SFC）：负责监管加密货币交易所、证券型代币等，确保符合证券法和反洗钱法规。
新加坡	新加坡金融管理局	1.修订支付服务法案，增加对 DPT（数字支付代币）服务提供商的要求，涉及反洗钱和金融稳定性。 2.推出稳定币监管框架，符合要求的稳定币发行人可申请“ MAS 监管的稳定币”标签。
美国	1.SEC 2.OFAC（海外资产控制办公室） 3.FinCEN（金融犯罪执法局） 4.OCC 和联邦储备 5.各州级监管机构	1.从事加密货币、虚拟资产、或者数字货币交换服务的加密货币机构，需要申请并获得 MSB（Money Services Business）牌照才能合法运营。 2.SEC 针对加密借贷产品和欺诈案件提起诉讼，强调投资者保护。 3.OFAC 制裁逃避制裁的俄罗斯实体和网络犯罪组织。 4.FinCEN：负责加密货币的反洗钱和客户身份验证。 5.OCC 和联邦储备：负责金融机构处理加密货币的合规性。 6.稳定币监管要求更高的透明度和资本储备，以提升市场透明度和保护投资者。
欧洲	1.欧洲证券和市场管理局（ESMA） 2.欧洲央行（ECB） 3.各国金融监管机构	1.加强反洗钱和反恐融资法律，设立反洗钱局（AMLA）监督高风险实体。 2.欧盟正在通过《市场加密资产法规》（MiCA）来创建统一的加密货币监管标准，2023 年 6 月生效，并在逐步普及。MiCA主要涉及加密货币发行、交易、钱包服务以及反洗钱等方面的规定。 3.欧盟各国通过金融牌照监管：德国BaFin金融牌照、法国 AMF 和 ACPR 牌照等。 4.英国，加密货币交易所、钱包提供商等从事加密货币相关活动的公司，都需要在英国金融行为监管局（FCA）注册，并符合相应的监管要求。
日本	日本金融厅	1.日本强制实施 Travel Rule，要求加密货币交易所等机构在处理交易时，必须收集并传递交易双方的身份信息，以实现对加密货币交易的追踪。 2.监管虚拟货币交易所，日本金融厅在 2017 年通过了《虚拟货币法》 3.加密货币相关的金融服务需要获得金融厅（FSA）的批准
加拿大	1.加拿大证券管理局（CSA） 2.加拿大金融交易与报告分析中心（FINTRAC） 3.投资行业监管组织（IIROC） 4.各省证券委员会	1.规范加密资产的证券交易，要求某些加密货币交易平台注册为证券交易商。 2.要求加密平台注册为“货币服务业务”（MSB）并遵守AML/ATF法规。 3.加拿大 MSB牌照（Money Services Business牌照）
澳大利亚	1.澳大利亚证券和投资委员会（ASIC） 2.澳大利亚交易报告和分析中心（AUSTRAC） 3.澳大利亚储备银行（RBA）	1.若加密货币被视为金融产品（例如某些代币、稳定币），相关服务商需要获得 AFSL 牌照，以便合法提供这些加密资产的投资或交易服务。 2.根据 AUSTRAC 的规定，所有提供加密货币交易、钱包管理、托管、兑换等服务的公司必须向 AUSTRAC 注册并遵守 AML/CTF 规定。 3.若加密货币用于支付服务，需要获得支付牌照并接受澳大利亚储备银行（RBA）的监督。
韩国	1.金融服务委员会（FSC） 2.韩国金融情报局（KFIU）	韩国国会通过了《特定金融交易信息法》的修正案，要求所有虚拟资产服务提供商（VASPs）向金融服务委员会（FSC）注册，并遵守反洗钱（AML）和了解客户（KYC）规定。
土耳其	资本市场委员会、银行监管和监督局	未经授权的加密服务提供商面临 3 至 5 年监禁，严重者可判处最高 22 年监禁。 资本市场委员会负责提供商的授权与监管。
马来西亚	1.马来西亚国家银行（BNM） 马来西亚证券监督委员会（SC）	马来西亚已将加密货币交易纳入《反洗钱法》监管范围，要求交易所严格执行 KYC，并上报可疑交易。

通过对比各国监管措施，我们可以发现一些共同点和差异点。共同点在于，各国都将反洗钱和反恐融资作为监管重点，并要求加密货币交易平台加强 KYC 认证以及牌照获取。差异点在于，各国对稳定币的监管要求、对投资者保护的力度以及对区块链技术的支持程度等方面存在差异。这些差异反映了各国在平衡创新与监管之间的不同取向。

6 结语

2024 年，加密资产的安全形势依然严峻。黑客攻击手段不断更新，给行业发展带来了显著挑战。尽管 Rug Pull、智能合约漏洞和私钥泄露等老问题仍然存在，但用户安全意识的薄弱以及新兴攻击手段的层出不穷，使得加密资产的安全防护变得更加复杂。多起重大安全事件揭示了去中心化交易所及其他平台在资产保护方面的脆弱性，凸显了加强安全措施的迫切需求。

DMM Bitcoin 事件和土耳其加密庞氏骗局等安全事件敲响了警钟，迫使各国监管机构加速了对加密货币市场的监管步伐。通过强化反洗钱和 KYC 措施，监管机构旨在保护投资者权益，打击金融犯罪，维护市场稳定。目前，全球范围内，各国纷纷采取了发放牌照、加强反洗钱、保护投资者、监管稳定币等措施。例如，中国香港推出了虚拟资产 OTC 发牌制度，新加坡加强了对数字支付代币服务提供商的监管。美国 SEC 对加密借贷产品加强了监管，欧洲则通过了《市场加密资产法规》（MiCA），为加密货币市场提供了统一的监管标准。这些监管举措旨在平衡创新与风险，为加密货币行业构建一个更加安全、透明和合规的生态环境。

未来，加密货币行业仍需要在创新与安全之间寻求平衡。只有通过提升技术手段、加强安全防护和完善法律框架，才能有效应对日益复杂的网络威胁。此外，各国监管部门之间的国际合作至关重要，这将促进信息共享和协调一致的监管策略，共同构建一个更加安全、透明的加密货币生态系统。如此，才能实现长期的可持续发展，为投资者创造更安全的投资环境。

作者：Ember

参考资料

1. https://hacked.slowmist.io/zh/statistics/?c=all&d=all
2. https://hacked.slowmist.io/zh/statistics/?c=all&d=2024
3. https://www.footprint.network/@Beosin/Footprint-Beosin-Q1-2024-Web3-Security-Report
4. https://www.footprint.network/@Beosin/Footprint-Beosin-Q3-2024-Web3-Security-Report
5. https://www.footprint.network/@Beosin/Footprint-Beosin-H1-2024-Web3-Security-Report
6. https://dune.com/queries/3446964/5791304
7. https://www.bbc.com/news/world-europe-66752785
8. https://www.gemini.com/cryptopedia/the-dao-hack-makerdao
9. https://www.pwc.tw/zh/news/press-release/press-20240131.html
10. https://www.deheheng.com/content/31030.html
11. https://cointelegraph.com/news/japanese-exchange-dmm-loses-bitcoin-private-key-hack
12. https://home.treasury.gov/news/press-releases/jy0916
13. https://beosin.com/resources/more-than-300-million-in-losses-analysis-of-45029-btc-abnormal-outflow-on-dmm-bitcoin-exchange
14. https://beosin.com/resources/over-100m-involved-and-127-suspects-detained-analysis-of-turkeys-crypto-ponzi-scheme

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