

2025 年度 加密犯罪报告





2025 年度加密犯罪报告

2025.4

目录

介绍	01
加密货币犯罪态势依然严峻	02
黑灰产交易规模逐步增加	04
洗钱规模骤降	04
以太坊非法稳定币活动占比先降后升	05
网络赌博	06
网赌平台的稳定币转移模式	07
USDC、美国大选与 Polymarket 的崛起	08
新的变化：警惕合规稳定币资金威胁	09
黑灰产交易	10
作为黑灰产交易产业核心的加密货币交易担保平台	11
案例研究：好旺交易担保 (Huione Guarantee)	12
不变的趋势：黑灰产交易市场不受加密行情影响	13
欺诈	14
加密欺诈规模增加	14
从 CEX 流入欺诈平台的资金	15
Bitrace 推出反欺诈手册	16
KYT 程序能够抑制加密欺诈活动	16
洗钱	17
CEX 流入洗钱资金数据	18
去中心化协议：更加严峻的洗钱态势	19
稳定币冻结	20
案例研究：好旺支付 (HuionePay) 被冻结 2962 万美元稳定币	21
稳定币发行商的链上冻结是强大的反洗钱武器	22
制裁	23
Tornado Cash 被 OFAC 制裁	24
对加密实体的制裁收效甚微	24

Crypto 监管态势及其影响	26
合规政策让香港加密实体资金风险降低	26
明确的监管框架减少法律不确定性	27
打击非法活动减少系统性风险	27
用数据为 Web3 带来合规与信任	29
联系我们	29

介绍

2024 年对 Web3 行业而言，是里程碑式的一年。这一年包括美国、香港等在内的主要金融中心推出了一系列监管合规政策，帮助 Web3 行业在本土有序生长；借由现实世界资产 (RWA) 上链、虚拟资产现货 ETF、Meme 文化传播等方式，行业规模得到爆炸式增长；主权国家基金与传统上市公司的入场，更是将 Crypto 总市值推到了前所未有的高度。

然而伴随着加密经济的蓬勃生长，犯罪产业也开始更多利用 Crypto 基础设施对其业务进行优化或创造新的犯罪范式。在加密行业的蛮荒年代，不法分子可利用的加密设施、币种、交易深度均有限，而在加密经济爆发的当下，去中心化交易平台 (Decentralized Exchange)、跨链桥 (Cross-Chain Bridge)、去中心化金融 (Decentralized Finance)、稳定币 (Stablecoin) 等基础设施均得到长足发展。

其中稳定币通过锚定某个现实国家的法定货币来实现币值的稳定，在储值与支付方面具备得天独厚的优势，同时巨大的交易规模、丰富的应用场景以及匿名特性，使得其也被网络赌博、洗钱、黑灰产交易、欺诈等非法产业所利用，利用方式包括将稳定币作为价值传输工具、资金清洗工具、资金存储工具等。

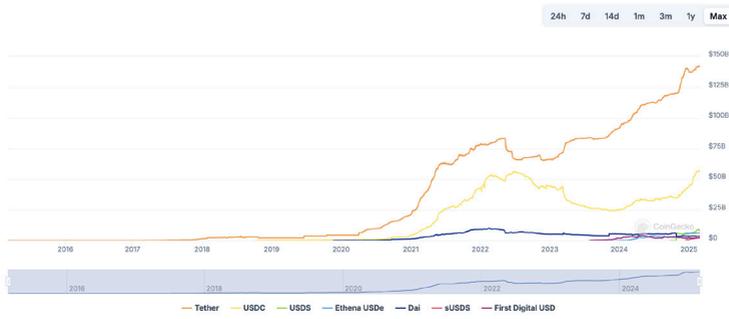


图 1 稳定币市值 数据来源：CoinGecko

根据加密货币数据聚合平台 CoinGecko 的数据，截至 2024 年 12 月 31 日，稳定币市值规模已经超过 2290 亿美元，其中两个头部美元稳定币——TetherUSD (USDT)、CircleUSD (USDC) 市值分别达到 1420 亿美元与 570 亿美元。

这篇报告旨在通过披露 Bitrace 对相关产业的调研数据，提高政府部门与 Web3 从业者们对加密犯罪生态的了解，以及对风险稳定币危害的认知，以帮助行业迈向合规。

加密货币犯罪态势依然严峻

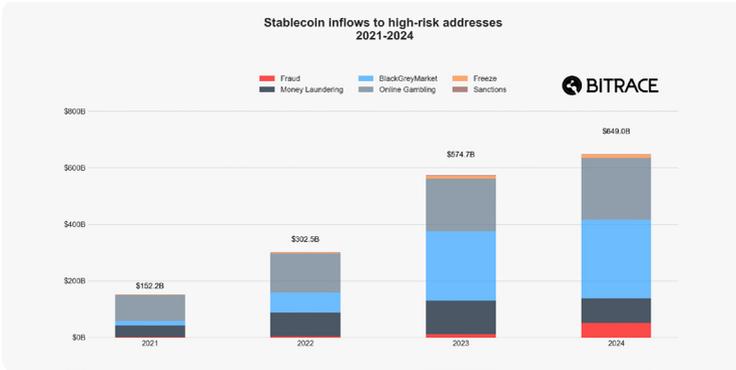


图 2 高风险地址收取稳定币数量

考虑到风险活动主要发生在以太坊、波场网络中，Bitrace 将非法实体在这两个网络中用于接收、传输、存储稳定币 (erc20_usdt、erc20_usdc、trc20_usdt、trc20_usdc) 的区块链地址定义为高风险地址，在过去的 2024 年里，这类高风险地址总的收款规模达到 6490 亿美元，略高于上年。

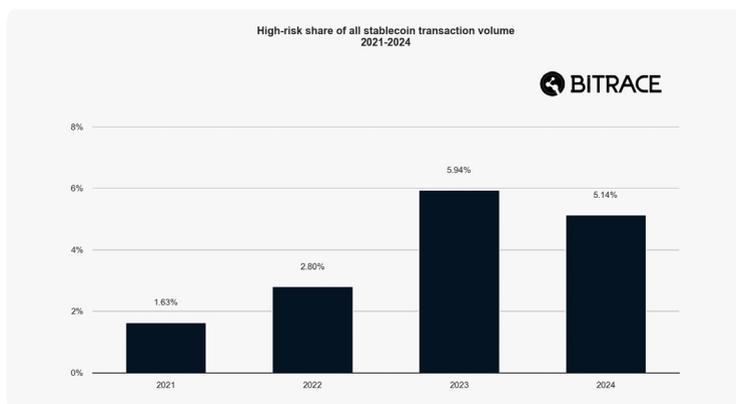


图 3 高风险活动占稳定币总交易规模比例

按照交易量进行计算，这部分高风险活动占当年稳定币总交易活动的 5.14%，相比 2023 年减少 0.80%，但仍然显著高于 2021 年与 2022 年。

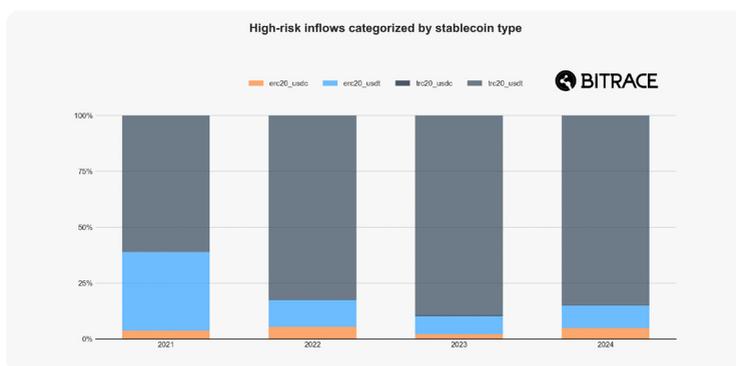


图 4 高风险地址收取稳定币分类

按照稳定币类型进行计算，在 2021-2024 年，波场网络中的 USDT 都占据了最主要份额。但在 2024 年，以太坊网络中的 USDT、USDC 份额均有所提升。

黑灰产交易规模逐步增加

在高风险地址的活动中，与黑灰产交易相关的稳定币交易规模与占比呈现逐年提升的趋势，这一现象在 2024 年尤为显著，不仅反映了稳定币市场整体的扩张，也揭示了其在非法领域中日益重要的角色。这种现象的背后，既有市场需求的驱动，也有黑灰产生态自身演变的推动。

其中一个关键原因在于，随着稳定币市场的日趋成熟，黑灰产对稳定币的利用规模也同步增加。自 2021 年起，受惠于 DeFi 协议的繁荣、机构投资的涌入以及跨境支付的普及，稳定币发行量开始大幅增加，例如 USDT 从当年的约 250 亿美元增长至 2024 年的约 1250 亿美元。这一庞大的流动性市场不可避免被黑灰产交易相关资金所污染，无论是网络赌博、黑灰产交易还是诈骗，不法分子都青睐稳定币的稳定性与匿名性，将其作为洗钱、资金转移和结算的核心工具。这种需求的隐秘增长，与合法市场的繁荣交织在一起，推动了稳定币发行规模的持续扩张。

另一个重要原因源于黑灰产生态内部的产业化与高度分工化趋势。近年来，黑灰产已从零散的个体作案演变为结构严密、协作高效的产业链条。例如，专门的“技术提供商”为诈骗团伙开发钓鱼网站，“资金搬运工”负责跨国洗钱，而“担保平台”则提供交易撮合与信任背书。这种分工不仅显著提升了行业的整体非法所得和犯罪效率，也大幅增加了内部基础设施的资金交易规模。

洗钱规模骤降

2024 年是加密行业整体迈向合规的重要一年，主要体现在多个地区监管政策的密集出台，以及当地执法部门连续开展重大执法行动，导致与洗钱有关的加密交易规模降低。

其中以美国和香港为代表的政策主体在 2024 年展现出对加密货币监管的高度重视，出台了一系列具有里程碑意义的政策框架。这些政策涵盖了虚拟资产服务提供商（VASP）许可制度、稳定币监管法案、现实世界资产（RWA）代币化规范，以及加密货币现货交易所交易基金（ETF）的合规要求等多个领域。这些监管措施对行业基础设施提出了明确的合规标准，其中反洗钱（AML）义务成为核心要求之一。

与此同时，2024 年全球执法力度显著增强，尤其是美国在加密行业的执法活动达到历史巅峰，这不仅反映了监管机构对行业乱象的零容忍态度，也彰显了其通过高强度执法震慑潜在违规行为的决心。在亚洲地区，香港和台湾等地也因 VASP 许可制度的过渡期结束，采取了更为严格的监管措施。多家未能满足合规要求的 VASP 被勒令停止运营，部分机构的许可申请被撤回。此外，针对涉嫌欺诈的交易平台，当地执法部门开展了多起联合行动，有效清除了市场中的不良参与者。

上述监管与执法的协同作用，在一定程度上遏制了非法实体利用稳定币进行资金清洗的趋势。

以太坊非法稳定币活动占比先降后升

波场网络在 2021 年凭借与各大交易平台的深度合作以及早期具有竞争力的价格优势，迅速在稳定币市场崛起，成为行业中的重要参与者。这一战略布局使其在短时间内占据了稳定币交易的主导地位，并在此后的两年内持续挤占以太坊网络在稳定币市场的份额。

然而，到了 2024 年，稳定币市场的竞争态势发生了显著变化。以太坊网络因连续的技术升级，极大缓解了其网络拥堵问题，进而带来了较低的网络费率。与此同时，波场网络却因运营策略调整，多次上调了交易费用。这一费率差异使得部分行业实体和用户重新审视以太坊网络的成本效益，开始回归以太坊进行稳定币交易的结算。

利用加密货币进行违法犯罪活动的群体作为对价格最敏感的一类群体，这一变化同样对其造成了影响，进而导致以太坊网络中与非法活动有关的稳定币交易活动的增加。

网络赌博

网络赌博平台是通过互联网提供赌博服务的网站或应用，它们允许用户在全球范围内进行各种赌博活动，而无需前往传统的陆基赌场。

赌博的合法性因国家或地区而异，部分区域对网络赌博有严格的管制，或者对网赌产业链中的特定部分存在不同的认定。但作为一项历史悠久的非经济活动，网赌产业根植于几乎所有的国家或地区，这一点在加密世界也不例外。

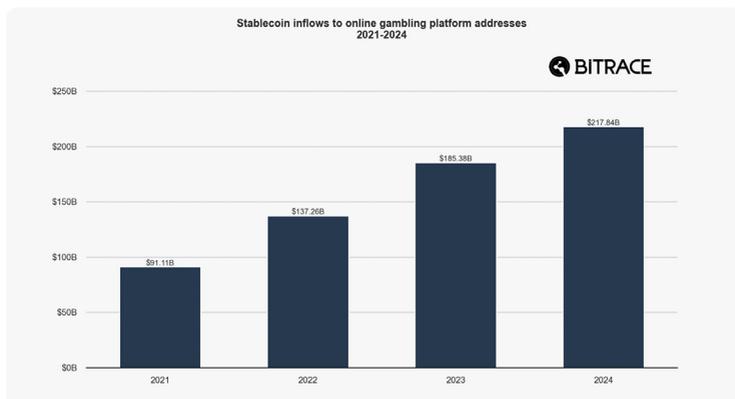


图 5 网赌平台收取稳定币数量

2024 年网络赌博平台以及为其提供出入金服务的支付平台的资金规模达到 2178 亿美元，相比 2023 年的规模增加超过 17.50%。

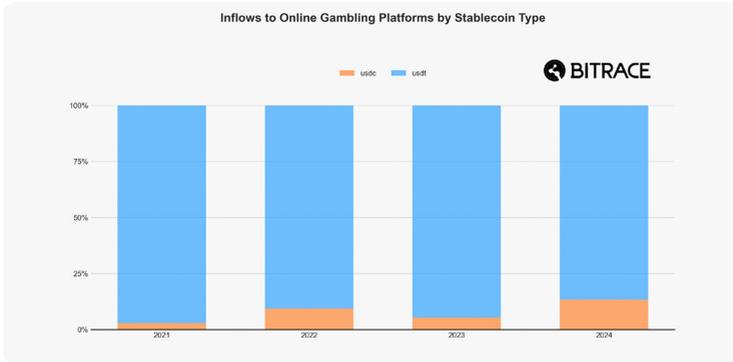


图 6 网赌平台收取稳定币分类

对网赌平台所采用的稳定币分类型进行统计，2024 年的 USDC 份额占比提升明显，达到 13.36%，远高于 2023 年的 5.22%。

网赌平台的稳定币转移模式

对于典型的网赌平台及其代理，这类机构主要通过自建中心化的加密货币充值、交易、提现系统或接入加密货币支付工具的形式帮助赌客进行资金结算，由于加密货币的匿名特性，政府部门将难以对这类行为进行监管或执法。

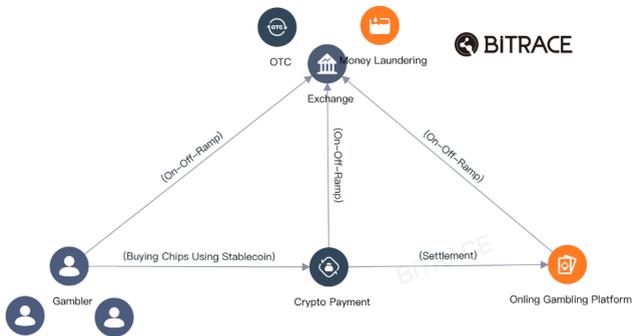


图 7 网赌平台对稳定币的采用方式

以通过接入第三方加密货币支付平台实现用户出入金的网赌平台为例，支付平台会为赌客分配独立的加密货币充值地址，支付平台拥有该地址的管理权限并定期归集资金，当用户提出提款申请时，再由支付平台审核打款，支付平台与网赌平台之间则定期结算资金。

USDC、美国大选与 Polymarket 的崛起

作为合规性稳定的代表，USDC 在 2024 年抓住了美国监管环境变化与 Defi 市场合规稳定币需求的双重机遇，流通量从年初的约 244 亿美元激增至年末的 439 亿美元，市场占比从 18% 攀升至约 22%，并深刻影响了以竞猜平台 Polymarket 为代表的网络博彩行业。

美国 2024 年总统大选成为关键转折点。特朗普“将美国打造为加密货币之都”的承诺推动了监管态度的转变。相比拜登时期 SEC 对加密行业的强硬执法，新政府倾向于支持合规数字资产发展。USDC 作为 Circle 发行的稳定币，凭借透明的储备管理和严格的合规标准，迅速成为监管青睐的对象。2024 年初，美国批准比特币现货 ETF 后，机构投资者对合规稳定币的需求激增，诸多合规交易平台直接受益于这一热潮。与此同时，USDT 因监管不确定性失去部分信任，进一步为 USDC 让出空间。

在 DeFi 领域，USDC 的崛起同样显著。2024 年得益于其扩展至 16 个区块链网络（如 Solana 和以太坊），以及更高的安全性和流动性，多链生态降低了交易摩擦，使 USDC 成为 DeFi 协议中的首选稳定币。

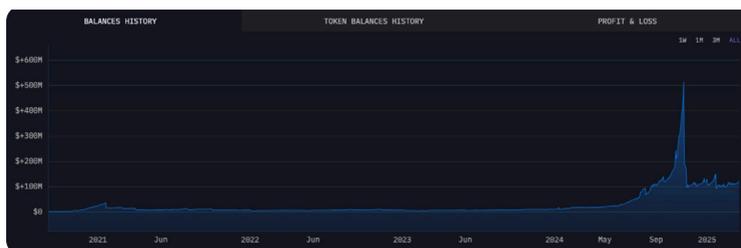


图 8 Polymarket 地址余额 数据来源：Arkham

Polymarket 等以 USDC 为结算工具的去中心化竞猜平台业务量巨大增长，则是在监管环境与市场需求下的行业缩影。2024 年美国大选期间异军突起，用户通过 USDC 押注选举结果、政策走向等事件，平台甚至预测特朗普胜率高达 60%，准确性超越传统民调。这种现实世界与加密经济的结合，不仅提升了 USDC 的使用频率，也推动其交易总量在 2024 年突破 90 亿美元。

这个因素推动了 USDC 在稳定币市场的应用，也解释了为何 2024 年，USDC 在网络赌博行业份额占比的扩张。

新的变化：警惕合规稳定币资金威胁

在 2024 年，合规稳定币 USDC 的市场份额获取了较大的提升，当前新型的竞猜平台开始接纳 USDC 作为换取筹码的工具，为其提供服务的支付公司也开始采用 USDC 作为资金结算工具。考虑到特朗普政府领导下的加密行业合规政策，USDC 的采用度还会继续提升，并进一步被网赌产业所利用。

此外，由于 USDC 在新公链与 DeFi 协议中的高度集成，更多链上原生 USDC、非原生桥接 USDC、其他 USDC 锚定代币正在不断涌现，这对致力于威胁感知、资金追踪的安全厂商提出了更高的要求。

对于加密企业而言，应在了解你的交易 (KYT) 程序里，增加更多与 USDC 相关的威胁情报来源；对于安全厂商而言，应升级追踪工具确保多链支持，增强威胁情报整合识别实时出现的网赌平台资金结算模式，以适应网赌产业快速变化的资金流动特征。

黑灰产交易

黑灰产交易是指在网络空间中，以牟取不正当利益为根本目的，通过多样化的技术手段实施或协助实施违法犯罪活动所形成的规模化、链条化的交易行为。这类活动的本质在于追求非法经济利益，或通过破坏网络生态秩序来达成特定目标。黑灰产不仅覆盖了传统互联网领域，随着区块链和加密货币的兴起，其形态和手段也在不断演变，呈现出更加复杂和隐蔽的特征。

在传统网络环境下，黑灰产交易往往通过将加密货币引入非法活动，或以先进的加密工具替代原有的技术手段，来提升活动的隐蔽性和欺骗性。例如，犯罪分子可能利用加密货币的匿名性进行勒索软件支付、暗网交易或洗钱操作，从而减少上下游活动被政府执法部门侦测或制裁的可能性。这种方式不仅提高了非法行为的执行效率，还通过技术屏障增加了监管和追踪的难度。

与之相对，新型的区块链黑灰产交易则展现出鲜明的行业原生特性。这类活动不再仅仅是将加密货币作为工具，而是直接以加密货币投资者或机构的数字资产为攻击目标，构成加密行业内部滋生的违法犯罪行为。例如，黑客通过钓鱼攻击、智能合约漏洞利用、去中心化金融（DeFi）平台诈骗等手段，直接窃取用户钱包中的加密资产，或通过操控市场制造虚假交易量来牟取暴利。这类黑灰产充分利用了区块链技术的去中心化特性、不可篡改性以及智能合约的自动化执行机制，将犯罪活动与加密生态深度绑定。与传统黑灰产相比，新型区块链黑灰产的链条更加专业化，涉及的技术门槛更高，且往往伴随着跨国犯罪网络的协作，进一步加大了打击难度。

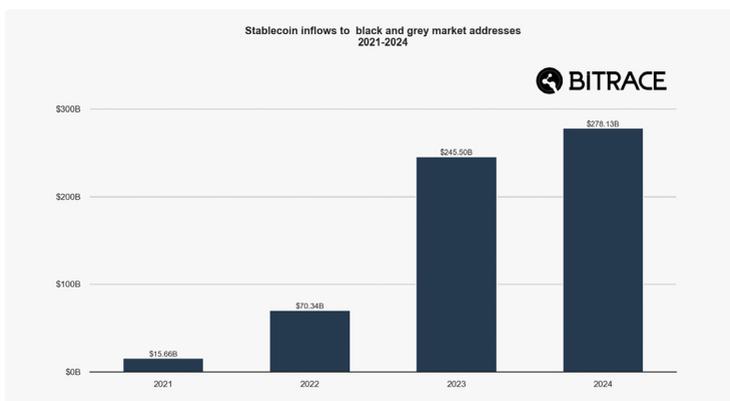


图 9 黑灰产交易地址收取稳定币数量

2024 年以太坊网络与波场网络中，与黑灰产交易相关的业务地址共收取资金超过 2781 亿美元，略高于 2023 年，而这两年的交易规模远超 2021 年与 2022 年。正如本报告前文所述，黑灰产交易规模的增长，与稳定币市场规模的快速爆发是同步的。

作为黑灰产交易产业核心的加密货币交易担保平台

交易担保平台是一种旨在为交易双方提供安全保障的第三方服务机制，通过充当中介或利用自动化技术，确保交易过程中的资金安全和履约义务得到执行。这种平台广泛应用于需要建立信任的场景，尤其是在买卖双方互不熟悉或交易存在一定风险的情况下。

交易担保平台的运作通常遵循以下基本步骤：

- ① 交易发起：买家将资金支付至平台指定的托管账户，而不是直接支付给卖家。
- ② 履约监督：卖家根据交易要求提供商品、服务或资产，并提交相关证明（如物流单号或数字资产转移记录）。
- ③ 条件验证：平台核实交易条件是否达成，例如买家确认收到商品或服务无误。
- ④ 资金释放：条件满足后，托管资金被转给卖家；若未达成，资金可能退回买家。
- ⑤ 纠纷处理：如双方对交易结果有异议，平台会根据规则或人工介入进行裁决。

在传统金融中，这种机制常见于基于法币支付体系的“第三方支付”或“托管服务”，但在以匿名为特征的加密货币交易担保平台，这一机制往往通过加密货币支付工具或智能合约来实现。这种模式结合了传统金融中的担保交易理念与区块链技术的去中心化特性，旨在降低交易中的信任风险和欺诈可能性。

也正因如此，通过将加密货币担保交易平台纳入业务流程，黑灰产业在一定程度上实现了去信任化与高度匿名。

以时下流行的加密货币浪漫骗局为例，这一骗局旨在通过塑造网络人设，与目标对象发起网恋，并诱骗对方参与虚假加密货币投资，进而骗取钱财。在整个行骗过程中，欺诈团伙需要购买大量潜在受害人个人信息、定制对应的人设与话术、订阅手机短信 / 电子邮件群发服务、购买并部署欺诈网站、清洗非法获取的加密货币，所有的服务或物资，都是通过加密货币交易担保平台进行的购买。

目前，加密货币担保平台已经成为犯罪产业链的核心，通过挖掘平台的客户与商家，能够追溯到大量与非法活动相关联的加密资金。

案例研究：好旺交易担保 (Huione Guarantee)

好旺集团（曾经的汇旺集团 Huione Group）是一家位于柬埔寨的大型金融集团，旗下拥有包括加密货币钱包、支付、交易担保、保险、加密货币交易所等在内的业务板块。其最核心的支付与担保业务大量采用了 USDT，根据 Bitrace 的标记数据，HuionePay、HuioneGuarantee 的官方及用户地址数超 18 万个，是当地规模最大的加密企业，影响力辐射至整个东南亚乃至东亚地区。

因东南亚系不法分子利用加密货币进行非法活动的高发区域，且好旺担保无需商家或客户匿名，因此其业务地址在一定程度上遭到风险资金的污染。

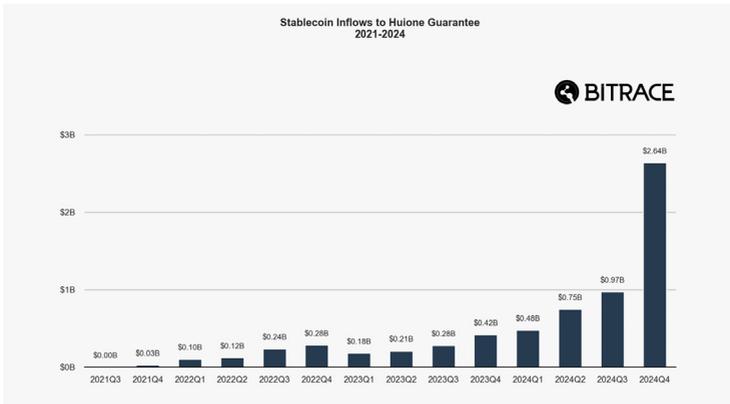


图 10 好旺担保收取稳定币数量

好旺担保以及其在东南亚的竞争对手们的崛起，是伴随着稳定币在当地真实经济活动中的逐渐普及而展开的，这一趋势在 2024 年尤为明显，当年四季度其业务规模已经扩张至 26.4 亿美元。

不变的趋势：黑灰产交易市场不受加密行情影响

2021 年是黑灰产生态开始利用加密货币开展业务的元年，而后几年里，其市场规模逐年增加，即使是在加密市场行情极为低落的 2022 年，其交易规模也相对 2021 年增长巨大，更不必说之后的 2023 年与 2024 年的加密牛市年份。

因此可预见的是，只要全球多个加密犯罪高发地没有从根本上铲除犯罪温床或者采取法律措施对其进行限制，那么即使未来两年是加密熊市，也不会对利用加密货币黑灰产交易市场的增长造成太大负面影响。

欺诈

加密货币欺诈是指利用数字货币或区块链技术进行的各种欺诈活动，相对于传统的欺诈，加密货币欺诈在原有的欺诈流程中加入了加密货币，或者基于区块链技术特点创造出新的骗术，包括但不限于钓鱼诈骗、投资欺诈、假交易所等。

由于结合了加密货币，这类骗术也更难以被识别，损失更难以被挽回，包括——

- 匿名性：交易无需实名，黑客或欺诈者难以追踪。
- 不可逆性：转账后无法撤销，受害者难以追索资金。
- 缺乏监管：全球范围内法规不统一，导致部分案件囿于当地司法管辖权限制而无法追查，给了欺诈者可乘之机。
- 技术复杂性：普通用户缺乏相关技术知识难以辨别真伪。

这使得加密货币欺诈成为了一个全球性的威胁。

加密欺诈规模增加

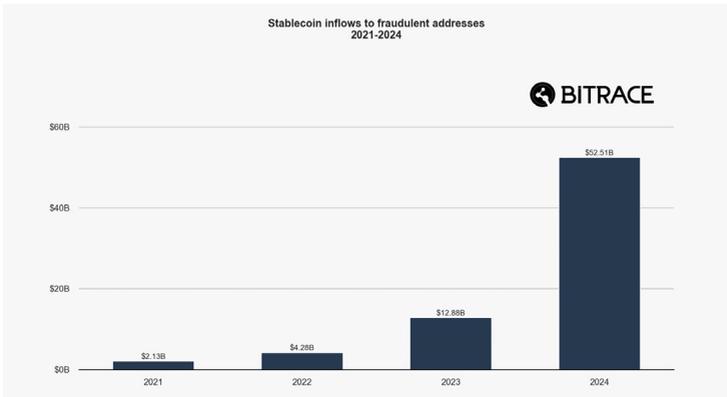


图 11 欺诈地址收取稳定币数量

2024 年与欺诈活动相关联的区块链地址，稳定币收取规模出现了爆炸式的增长。相比于 2021 年 -2023 年，当年的资金规模已经达到 525 亿美元，超过历年总和。

但这一惊人的增长趋势或许并不是完全准确的，因为统计值受限于安全厂商的统计方式以及非法实体欺诈水平的提升。例如随着安全厂商对诸多新型公链的支持，更多的犯罪事件才会被观察，这意味着过去发生的事件或许并未被纳入统计；发生在中心化机构内以及未经受害人主动披露的案件，也无法被纳入统计。

随着统计方式的改进与案件披露的增加，在下一年的调查报告里，这批数据会进一步增长。

从 CEX 流入欺诈平台的资金

类似假交易所矿池挖矿欺诈、浪漫欺诈等针对新手投资者的骗局，中心化交易平台（CEX）在其中都起到了非常大的作用，因为受害者必须先从 CEX 中购买稳定币，并将资金提现至欺诈者提供的区块链收款地址。通过监控交易所热钱包地址向欺诈地址的转账活动，能够在一定程度上衡量这类欺诈对新手用户造成的损害。

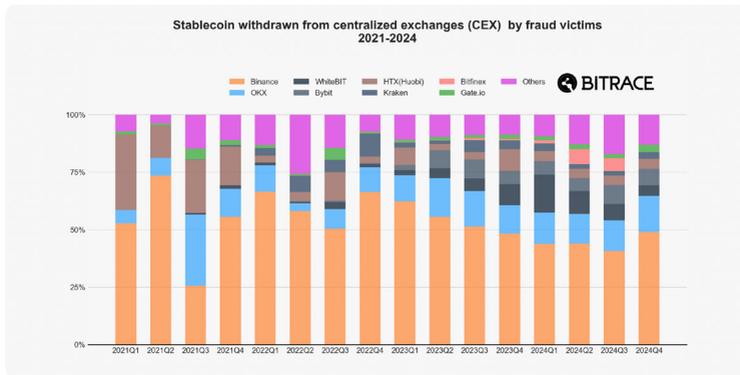


图 12 主要中心化交易平台向欺诈地址转账稳定币规模占比

综合而言，CEX 向欺诈地址的转账活动规模，基本与其业务规模成正比。例如 FTX、HTX 在 2021 年至 2022 年期间相当活跃，出现了较多受害人提款，而在破产或清退用户后这一数值快速降低；此外欺诈活动在亚洲尤其东南亚地区更加猖獗，因此 OKX、Bybit、Gate 等亚洲背景交易所，相对于其体量呈现出更高比例的欺诈资金转出。

Bitrace 推出反欺诈手册

基于几千起真实涉币案件（Crypto Crime）的调查经验，Bitrace 于 2024 年推出了面向普通加密货币投资者的反欺诈手册。

Content

Introduction	01	The End of Industrial Specialization: The Rise of Crypto	
Unreliable Information Sources: You Might Have Been Misled		Drainers	34
from the Beginning	03	The Stolen Wallets Affiliate Model	34
Video QR Code Scams	03	The Phishing Affiliate Model	35
Social Media Scams	05	OTC Fraud: The Weakest Link in Crypto Transactions	37
Romance Scams: A Hybrid of Investment and Romantic		Exchange Merchant Fraud	37
Fraud	07	In-Person Trading Scams	38
Mismanagement of Assets: A Major Pitfall at the Start of the		In-Person Multisignature Fraud	39
Crypto Journey	09	Security Recommendations for Navigating the Crypto Space	41
Fake Wallet Apps: A Trap for Asset Theft	10	Don't Let Emotions Like Fear and Greed Control Your	
Multisig Case: A New Breed of Crypto Theft	12	Decisions	41
Payment Authorization Scams: A Growing Threat to Wallet		Don't Blindly Trust—Always Verify	42
Security	13	Most Crypto Scams are Variants of Traditional Scams	42
Fake Telegram Scams: Targeting Crypto Investors with		Sunk Costs Are Not Costs	43
Counterfeit Apps	15	What to Do After Falling Victim to a Crypto Scam	44
Hardware Wallet Fraud: A Social Engineering Scheme	16	Mitigate Losses Immediately	44
When You Begin Trading Crypto	17	Preserve the Crime Scene and Report the Incident	44
High-Yield Exchange Investment Scams	17	Seek Assistance from Relevant Parties	45
Honeypot Token Scams: The "Buy-Only, No-Sell" Trap	19	Final Thoughts	46
Fake Binance Mining Pool Scam: A Sophisticated		About Bitrace	48
Deception Targeting Crypto Users	21	Disclaimer	49
Fake OKX Public Chain Scam: "Hold USDT to Earn OKT"	23		
Liquidity Withdrawal Scams: Exploiting AMM Mechanisms			
for Profit	26		
Phishing: The Viral Growth of Deceptive Tactics	28		
Address Poisoning	28		
Advertising Tokens	30		
Fake Exchange Clearance SMS	32		



图 13 Bitrace 反欺诈手册

该手册介绍了不同层级投资者会遇到的欺诈类型，并详细介绍了欺诈手法，旨在帮助读者识别与规避欺诈，以减少财产损失。

KYT 程序能够抑制加密欺诈活动

KYT 程序通过分析区块链上的交易数据，能够追踪每笔交易的资金来源和流向。区块链的公开账本特性使得每一笔交易都可以被记录，而 KYT 利用这一特性，通过关联地址和交易模式，识别出资金是否来自非法渠道，或者即将进入非法地址，从而阻止欺诈资金的进一步流通。

在实践中，KYT 已经在加密货币交易所、钱包服务和金融合规领域得到广泛应用。例如，部分中心化加密交易所使用 KYT 技术，根据用户行为模式和资金流向进行风险评级，对高风险交易采取限制措施。但这一程序在钱包、DEX、加密支付平台中尚未得到普及，对欺诈事件的反制还有很大的进步空间。

洗钱

洗钱 (Money Laundering) 是一种将非法所得合法化的行为，主要指将违法所得及其产生的收益，通过各种手段掩饰、隐瞒其来源和性质，使其在形式上合法化。其行为包括但不限于提供资金账户、协助转换财产形式、协助转移资金或汇往境外。而加密货币——尤其是稳定币——因其低廉的转账成本，去地理化的特质以及一定的抗审查特性，在相当早的时间便已经被洗钱活动所利用。

加密货币洗钱活动往往会利用加密货币场外交易市场，进行从法币到加密货币，或从加密货币到法币的兑换，其中洗钱场景不同，形式也多样化，但不论如何这类行为的本质都是为了阻断执法人员对资金链路的调查，包括传统金融机构账户或加密机构账户。

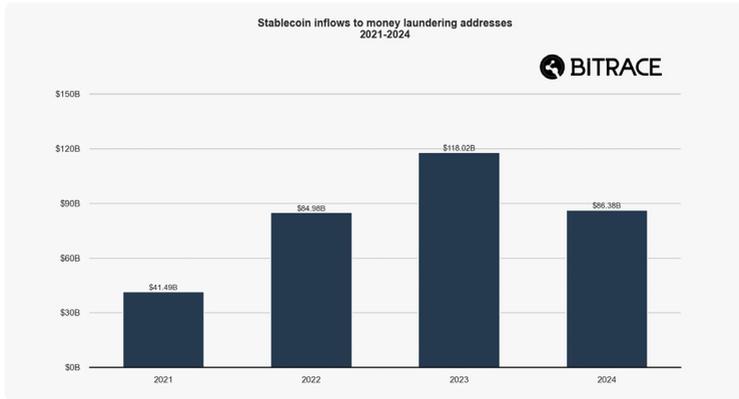


图 14 洗钱地址收取稳定币数量

2024 年与洗钱活动有关的区块链地址共计收取价值 863 亿美元的稳定币，略低于 2023 年，与 2022 年持平。这一数值可能表明，发生在过去两年的重大执法活动以及主要政策主体的监管立法活动，已经对加密行业的洗钱犯罪态势造成了有效抑制。这部分内容将在本报告的监管政策解读章节中详细展开。

CEX 流入洗钱资金数据

而随着加密行业基础设施的逐渐完善，去中心化交易平台（DEX）、跨链桥（Bridge）、混币平台（Mixer）越发在加密洗钱活动中展现出巨大的作用，不法分子往往不会再将涉案资金直接转入中心化交易平台进行资金倾销，而是选择在链上进行资金混淆，再择机变现，令资金变得更加难以追踪。

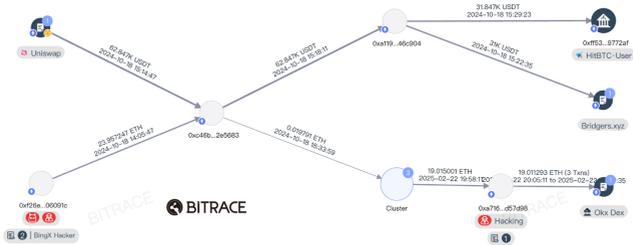


图 15 BingX 黑客洗钱手法

发生在 2024 年四季度的 BingX 被攻击案，目前已经能够确认是朝鲜黑客组织拉撒路（Lazarus）的所作所为。该组织在非法获取受害交易平台的资金后，迅速进行了链上洗钱活动。在这过程中，他们大量使用了去中心化交易平台、去中心化交易聚合器、跨链桥、中心化交易平台，尽管这些加密实体努力进行了资金拦截，但收效甚微，绝大多数被盗资金仍然未能挽回。

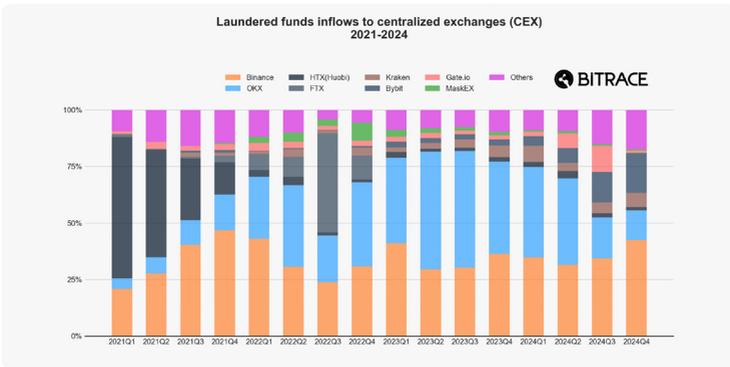


图 16 主要中心化交易平台收取洗钱稳定币规模占比

考虑到中心化交易所在资金变现方面相对于其他实体，具备得天独厚的优势而更容易受到洗钱团伙的青睐，Bitrace 对主要的中心化加密货币交易平台的热钱包地址进行了资金审计。结果与欺诈章节的调查类似，平台收取洗钱资金的规模总体与其业务规模成正比，但 OKX 在最近几个季度的占比显著降低，这可能是其合规经营的结果。

去中心化协议：更加严峻的洗钱态势

随着区块链技术的普及与去中心化协议的易用性提升，越来越多的不法团伙能够以极低的技术门槛对加密资金进行混淆、清洗、隐匿，已经对政府监管部门与加密实体的风控部门构成了巨大的威胁。

在当前，各主要政策主体正在对以虚拟资产场外交易商（Virtual Asset Over-the-Counter Trading Service Provider | VAOTC）与虚拟资产交易平台（Virtual Asset Trading Platform | VATP）为主的虚拟资产交易服务商（Virtual Asset Service Provider | VASP）立法实施监管，但对部署在区块链上的去中心化协议的监管进程缓慢，在未来的数年里，行业将面临更为严峻的洗钱态势。

稳定币冻结

中心化机构发行的稳定币除了具备其他加密货币的匿名转移、无许可使用特性外，代币系统也赋予了发行方巨大的调度权限，使得开发者能够定向增发、销毁某个地址的稳定币，或者限制特定地址对稳定币的操作权限，也即业界所称的稳定币冻结。

这类中心化的冻结活动通常由全球各国政府部门的执法请求所触发，旨在对已知的利用稳定币进行的违法犯罪活动进行阻止，并对受损资产进行拦截，防止损害扩大化。

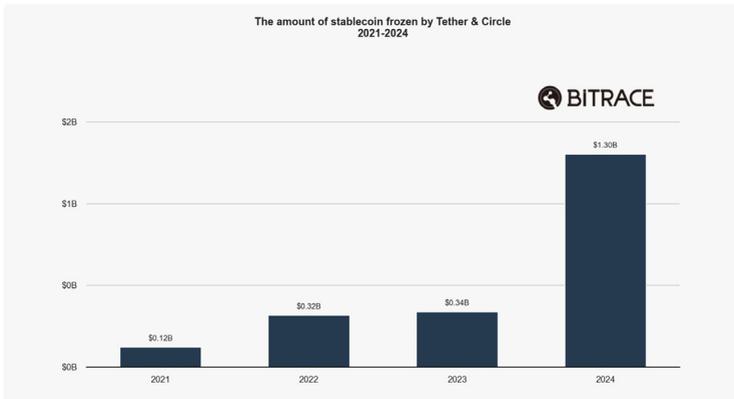


图 17 Tether 与 Circle 冻结的稳定币数量

2024 年是稳定币发行商们积极配合执法的一年，泰达（Tether）与 Circle 公司共在以太坊及波场网络中冻结价值超过 13 亿美元的稳定币，是之前三年冻结规模的两倍。

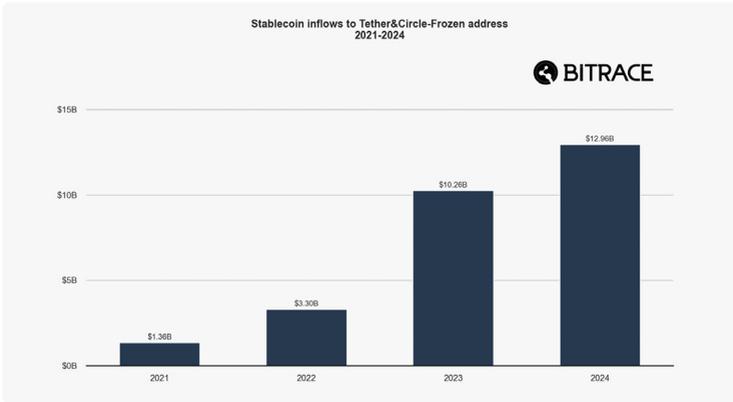


图 18 冻结地址当年收取稳定币数量

对被冻结地址在当年的资金转账活动进行统计，2024 年的交易规模达到 129 亿美元，并且与 2023 年基本持平，这表明链上加密犯罪活动在数年前就已经开始活跃，但直到 2024 年才开始被有效打击。

案例研究：好旺支付（HuionePay）被冻结 2962 万美元稳定币

好旺支付同样是好旺集团旗下主要产品之一，与好旺担保共同为东南亚地区用户提供加密服务，系当地头部支付与担保公司。2024 年 7 月 13 日，Tronscan 显示好旺支付热钱包地址遭到泰达公司限制，高达 2962 万 USDT 被冻结无法转移。

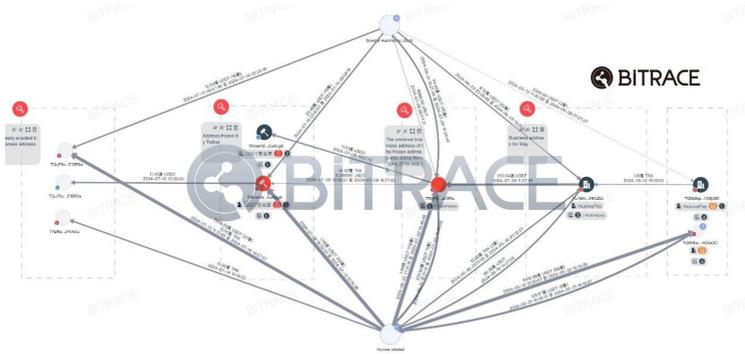


图 19 好旺支付被冻结 2962 万美元

其原因系日本中心化加密货币交易平台 DMM 被拉撒路黑客攻击，发生价值超过 6 亿美元的比特币损失，黑客所获取的 tBTC、BTC.b 等资产在 avalanche、ethereum 等链兑换为价值相当于 3182 万美元的 USDT、USDC、DAI 等资产后，经跨链兑换至 TRON 网络，最终其中大约 1400 万进入好旺支付的业务地址，进而导致冻结。

这起事件因其巨大的冻结金额与东南亚特殊实体身份而颇受行业关注，表明了加密洗钱的跨国特性。

稳定币发行商的链上冻结是强大的反洗钱武器

区块链的透明性结合稳定币发行商的制裁能力，可以快速识别和冻结可疑资金。与传统金融系统相比，链上制裁无需经过繁琐的跨国银行协调，能在几秒钟内生效。这种速度对于阻止洗钱资金快速转移至关重要。

目前最大的稳定币发行商泰达正在推进其合规计划，而第二大稳定币发行商 Circle 已经是包括美国地区在内的合规实体，在这两家机构的协助下，链上冻结将成为强大的反洗钱武器。

制裁

政府制裁是指一国政府或国际组织通过实施经济、贸易、金融、外交或其他形式的限制措施，对特定国家、实体、个人或活动进行惩罚或施压，以达到政治、经济或安全目的。随着非法实体对加密货币的采用度提升，与受制裁主体相关联的区块链地址也被纳入制裁范围。

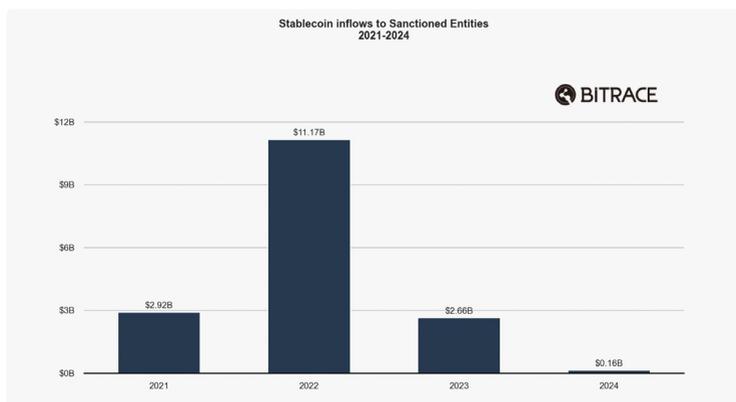


图 20 OFAC 与 NBCTF 制裁实体关联地址收取稳定币数量

美国财政部下属的外国资产控制办公室（OFAC）和以色列国家反恐融资局（NBCTF）是两个与制裁和反恐融资相关的机构，在打击恐怖主义融资和与恐怖组织（如哈马斯）相关的金融网络方面存在较多合作，对这两个组织披露的与受制裁实体相关的区块链地址进行资金统计，整体资金规模在 2022 年达到最高，此后逐年下降。

其原因在于 2022 年 OFAC 制裁了一家俄罗斯中心化交易平台 Garantex，后者被指控为俄罗斯最大的暗网交易市场 Hydra Market 提供资金清洗服务。此后 Garantex 为规避业务地址遭稳定币发行商的执法协作，开始高频率更换业务地址，受限于统计方法与统计范围，使得难以准确统计其资金规模，导致了图表中统计值的降低。

Tornado Cash 被 OFAC 制裁

Tornado Cash 是一种运行在以太坊区块链上的去中心化混币服务 (cryptocurrency mixer)，于 2019 年推出。它通过智能合约技术，将用户的加密货币存款与其他用户的资金混合后重新分配，从而模糊资金的来源和去向，以增强交易隐私。这种设计既吸引了追求隐私的合法用户，也为非法活动提供了便利。

其中以拉撒路黑客组织为主的非法团伙多次利用 Tornado Cash 进行资金清洗，引起了美国政府的高度关注。美国财政部认为，Tornado Cash 未采取有效措施防止非法资金流动，违反了反洗钱 (AML) 和制裁合规要求，成为恶意行为者规避美国制裁的工具。

2022 年 8 月 8 日，美国财政部外国资产控制办公室 (OFAC) 宣布对 Tornado Cash 实施制裁，将其列入“特别指定国民和受阻人士名单” (SDN 清单)。这是 OFAC 首次针对一个去中心化智能合约而非实体或个人采取制裁行动。具体措施包括：

- 冻结 Tornado Cash 在美国境内或美国人控制下的所有资产。
- 禁止美国公民和实体与 Tornado Cash 进行任何交易，包括与其相关的以太坊地址。
- 将制裁理由定为 Tornado Cash“为朝鲜支持的恶意网络行为者洗钱提供了便利”。

此外，部分主要的中心化交易平台与 DeFi 平台也开始与 Tornado Cash 用户进行隔离，禁止收到相关资金的地址访问平台官方前端网页或者将资金转入平台等。

尽管在 2024 年 11 月 26 日，美国第五巡回上诉法院作出里程碑式裁决，推翻了 OFAC 对 Tornado Cash 的制裁。法院认为，这些合约“无法被拥有或控制”，不属于 IEEPA 定义的“财产”，因此 OFAC 越权，但 Tornado Cash 的行业声誉与交易规模均不复从前。

这一制裁事件充分表明了 DeFi 协议在面对监管时的脆弱性，政府部门的决策对加密行业的经营实体影响力巨大。

对加密实体的制裁收效甚微

尽管政府部门的监管措施会对受制裁实体的业务造成巨大影响，但对于利用这些基础设施进行非法活动的犯罪团体而言，却收效甚微，因为加密技术的匿名与无需可特性决定了这类实体难以被制裁并且高度可替代。

例如 Tornado Cash。尽管 OFAC 的制裁举措足够强硬，但合约部署在去中心化的区块链网络中，即使官网前端被屏蔽，使用者仍然可以直接调用区块链合约进行资金清洗，后续发生的多起安全事件中，攻击者便是从该协议中获取手续费并清洗非法所得。

此外，加密行业内的隐私协议众多，即使 Tornado Cash 被制裁，也还有更多同类型产品作为替代，为需要隐私的用户提供资金混淆服务。2025 年 2 月发生的 Bybit 被攻击事件同样是拉撒路的手笔，这次清洗过程中，黑客大量使用了 Thorchain 与 Li.Fi 两个协议，而非 Tornado Cash。

因此，制裁只是对遭利用加密实体的惩罚，而对实施犯罪的不法分子收效甚微，监管部门应当对加密犯罪开展更加深入的调查，并对犯罪团伙采取相应的执法行动。

Crypto 监管态势及其影响

2024 年是加密行业加速合规的一年，从全球范围来看，主要的监管机构对加密货币的态度从观望转向更积极的介入，推动行业向更规范、更透明的方向发展，其中——

欧盟的加密资产市场法规 (MiCA) 于 2024 年 12 月 30 日全面生效，对加密资产发行、交易和服务提供商 (如 CASPs) 实施统一监管，要求获取许可证、遵守 AML/KYC 规则，并对稳定币发行商设定银行级别的资本和风险管理要求；

2024 年，美国国会讨论了多项法案 (如 FIT 21 法案和稳定币法案)，SEC 批准了比特币和以太坊现货 ETF，标志着一定程度的认可；

日本强化了 AML 措施，日本金融厅 (FSA) 进一步收紧加密交易所的客户信息共享规则，以防止洗钱，同时继续将加密货币视为合法财产，支持其交易和发展；

韩国 2024 年进一步落实虚拟资产用户保护法，要求交易所提高透明度和记录保存标准，金融当局计划在年中发布虚拟资产上市指南；

香港金融管理局推出稳定币发行商监管沙盒，鼓励创新并测试合规性，同时加强对加密交易所的许可要求；

英国 2024 年继续制定稳定币相关立法，计划将其纳入金融监管框架，同时通过数字证券沙盒支持区块链技术发展。

这些政策反映了全球对加密货币的态度从宽松转向规范，重点在于反洗钱、消费者保护和金融稳定，同时部分地区 (如欧盟、香港) 试图在监管与创新间找到平衡。

合规政策让香港加密实体资金风险降低

Bitrace 认为香港的合规政策降低了当地加密实体的资金风险，主要是因为其监管框架在平衡创新与风险管理方面采取了较为严格且清晰的措施。

明确的监管框架减少法律不确定性

香港自 2022 年起逐步完善加密货币监管体系，特别是通过《反洗钱及反恐融资条例》（AMLO）的修订，将虚拟资产服务提供商（VASP）纳入监管范围。2023 年 6 月，香港证券及期货事务监察委员会（SFC）正式实施针对加密货币交易所的牌照制度。

合规政策要求加密实体（如交易所、托管服务商）取得 SFC 牌照，需满足反洗钱（AML）、反恐融资（CFT）和客户资金保护等严格标准。这一明确的法律框架减少了加密实体因政策模糊而面临的潜在法律风险（例如突发的禁令或罚款），从而降低了因监管不确定性导致的资金冻结或流失风险。

打击非法活动减少系统性风险

香港的合规政策严格打击洗钱、恐怖融资和规避制裁的行为，要求 VASP 实施“了解你的客户”（KYC）、了解你的交易（KYT）和交易监控措施。

SFC 与香港警方和国际机构（如 FATF）合作，追踪并冻结非法资金流，通过清理不合规的加密实体（如 Garantex 那样的制裁规避平台），使香港减少了因非法活动引发的系统性金融风险。同时与 Bitrace 等加密安全企业合作，对部分涉币案件进行协作调查，减少了事件中受害人的损失。

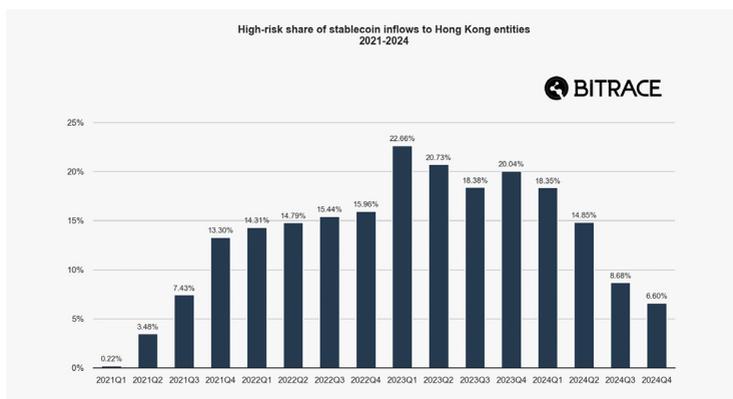


图 21 香港 Web3 实体稳定币收入中的高风险资金占比

对主要服务香港客户的 VATP 与 VAOTC 地址进行资金分析，数据显示在 2023 年三季度之后，流入当地的风险稳定币占比急剧减少，这表明在合规政策发布以及若干标志性涉币案件后，当地与风险活动相关的稳定币交易活动得到了有效抑制。

总结来说，香港的合规政策通过明确的法律要求、客户资金保护、打击非法活动、吸引机构资金以及与国际标准接轨，构建了一个更安全、可控的加密生态。这不仅减少了黑客攻击、平台破产或法律处罚导致的直接资金损失，也通过提升市场信任和稳定性降低了间接风险。对于加密实体而言，合规成本虽然短期内增加，但长期来看显著降低了资金暴露于不可控风险的可能性。

用数据为 Web3 带来合规与信任



Bitrace 是一家以加密货币风险数据分析为核心的监管科技 (Regtech) 企业, 我们致力于运用 AI 与大数据技术更准确高效地识别、监测链上的风险和犯罪活动, 为客户提供领先的监管、合规、调查工具产品与服务支持。

我们聚焦于加密犯罪调查领域, 目前已与多国执法机构、Web3 企业进行协作与对接, 完成数千起案例服务支持, 累计监测数千亿风险资金, 并成功挽回数十亿美元的损失。

联系我们

官网 : bitrace.io

邮箱 : bd@bitrace.io

Twitter: [@Bitrace_team](https://twitter.com/Bitrace_team)

LinkedIn: [@Bitrace Tech](https://www.linkedin.com/company/bitrace-tech)

Telegram: [@BitraceBD](https://t.me/BitraceBD)