2026 Crypto Crime Report

BITRACE

2026 Crypto Crime Report

2026.1

Content

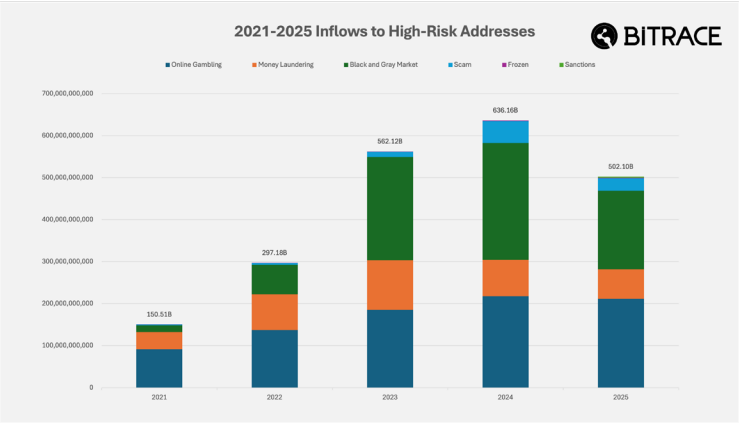
Introduction

The year 2025 was a crucial year for the cryptocurrency industry to see both regulatory transformation and structural progress.

The Trump administration has delivered on its political promise to provide clear regulatory pathways for the cryptocurrency sector through a series of pro-crypto initiatives. Key actions include the January 2025 Executive Order on “Strengthening American Leadership in Digital Financial Technology,” the March 2025 establishment of the Strategic Bitcoin Reserve, the signing of the GENIUS Act (establishing a federal framework for stablecoins) into law in July 2025, and continued progress on the CLARITY Act for broader digital asset market structure. Together, these steps have positioned the United States as the world's leading “cryptocurrency capital.”

These global policy tailwinds have accelerated adoption among retail investors, institutional participants, and sovereign entities alike. Bitcoin reached an all-time high of around $126,000, while the overall cryptocurrency market capitalization has held steady near $3 trillion, underscoring the sector's ongoing shift from marginal asset class to integral component of mainstream finance.

Nevertheless, amid this flourishing development and maturing infrastructure—including the broad uptake of decentralized exchanges (DEXs), cross-chain bridges, DeFi protocols, and diverse cryptocurrency instruments—cryptocurrencies' attributes of high liquidity, swift cross-border transfers, and relative pseudonymity have made them increasingly appealing to bad actors for illicit purposes.



As crypto assets and associated on-chain protocols gain broader mainstream integration, their abuse in select illicit and high-risk activities has grown more pronounced. Core infrastructure—such as decentralized exchanges (DEXs), cross-chain bridges, DeFi protocols, and diverse cryptocurrency instruments—serves principally as a conduit for value transfer, fund obfuscation (e.g., mixing), and storage of illicit proceeds in contexts including online gambling, money laundering, black/gray-market dealings, fraud schemes, and efforts to circumvent international sanctions. Regulatory bodies globally continue to monitor this evolving pattern with heightened attention.

Per Bitrace's ongoing monitoring and statistical analysis, blockchain addresses identified as high-risk across the ecosystem received an aggregate of $502.1 billion in illicit funds during 2025.

Tendency

Southeast Asian organized crime networks hit hard

In 2025, major countries around the world launched a series of crackdown operations targeting the fraud industry in Southeast Asia, marking a new stage in international cooperation. Despite the enormous scale of scam compounds, with annual output values reaching tens of billions of U.S. dollars, and the rapid relocation of criminal groups to new sites, multilateral law enforcement, sanctions, and repatriation actions have achieved significant progress.

This joint initiative has already been reflected on the blockchain. The United States and the United Kingdom jointly sanctioned the Cambodian Prince Group, seizing or freezing billions of dollars in cryptocurrency assets. This directly forced one of the central hubs of organized crime networks in the region, Huione Group, to temporarily suspend operations of its Huionepay payment service.

As one of the key infrastructures of the telecom fraud industry, illicit cross-border human trafficking operations have also been targeted. Channels of a series of human trafficking guarantee/trust platforms—led by Linghang Guarantee (领 航 担 保)—were shut down, and outbound funds from their operational addresses have been subjected to risk control measures by major mainstream trading platforms.

In addition, under pressure from neighboring countries, a number of telecom fraud compounds (scam parks) have been shut down, resulting in the repatriation of large numbers of individuals engaged in telecom fraud activities.

Online gambling users begin migrating to prediction markets

Online gambling was one of the earliest illegal industries to adopt cryptocurrency for business operations. Traditional online gambling platforms, by building their own settlement systems or integrating third-party payment tools, provided gamblers with cryptocurrency-based chip redemption services. Through this collaboration, online gambling platforms successfully circumvented crackdowns by certain countries or regions on fiat settlement systems targeting both gamblers and casinos. Thanks to this, the scale of cryptocurrency transactions related to online gambling has continued to increase over the past several years.

However, with the rise of the phenomenal prediction platform Polymarket in 2024, followed by the emergence of various competing products in 2025, traditional online gambling platforms have faced strong market share compression. Currently, the inflow of cryptocurrency funds into these platforms shows a downward trend, as gamblers begin shifting toward the new generation of prediction markets.

Tether's law enforcement cooperation activities were more active

As the issuer of Tether (USDT), the most widely adopted stablecoin at present, Tether Limited has, over the past several years, continuously carried out blacklist operations (Add Blacklist) against cryptocurrency addresses identified as receiving criminal funds, while collaborating with law enforcement agencies from major countries and regions worldwide.

In last year's crime report, Bitrace disclosed that Tether significantly increased its law enforcement collaboration activities in 2024, freezing a far greater number of blockchain addresses than in previous years. In 2025, this effort became even more proactive, with the number of addresses frozen exceeding that of 2024 by more than double, underscoring the company's heightened emphasis on compliance.

Geopolitical Conflicts under Cryptocurrency Sanctions

In 2025, the conflict between Israel and Palestine entered its third year. Against this backdrop, the former continued to target cryptocurrency channels suspected of providing funding to Hamas, Hezbollah, and entities linked to Iran.

According to monitoring by Bitrace, Israel's National Bureau for Counter Terror Financing (NBCTF) sanctioned at least 446 blockchain addresses or exchange accounts in 2025 alone, primarily involving USDT, Bitcoin, and others—far exceeding the number sanctioned by any other country.

Online gambling

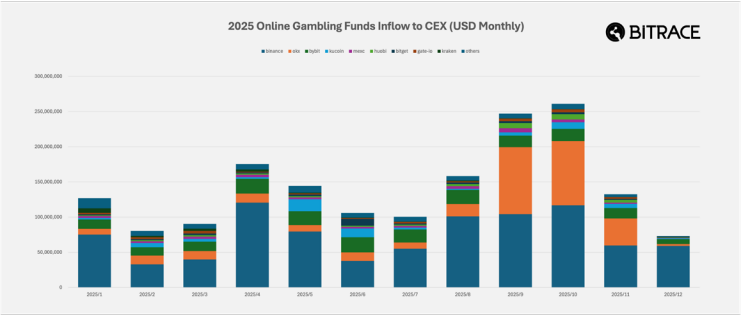
By establishing their own cryptocurrency settlement channels or integrating third-party cryptocurrency payment tools, online gambling platforms have achieved a business address structure similar to that of centralized cryptocurrency exchanges. Gamblers do not directly purchase or cash out betting chips through fiat currency; instead, they use cryptocurrency (especially stablecoins) as an intermediary, thereby achieving a high degree of anonymity.

In the past several years, this system has operated stably primarily on the Tron and Ethereum networks. Although lower than in previous years, high-risk addresses associated with online gambling still received $145.3 billion in 2025, down from $217.8 billion in 2024.

In addition, emerging prediction platform markets have shown significant growth, with known business addresses receiving fund inflows or bets totaling as high as $66.4 billion in the year, far exceeding the $16.7 billion recorded in the previous year.

Clearly, prediction markets are rapidly capturing market share from traditional online gambling platforms.

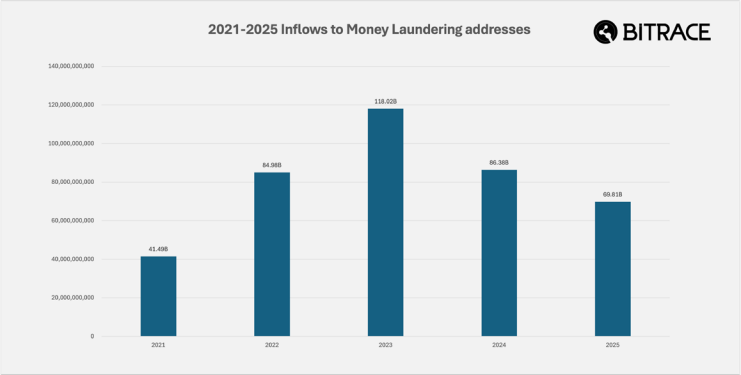
In 2025, statistics on the activity of prediction platforms show that, in addition to Polymarket maintaining steady growth, Opinion—launched in the fourth quarter—as well as the established compliant platform Kalshi, both experienced rapid expansion and achieved an overtake of Polymarket.



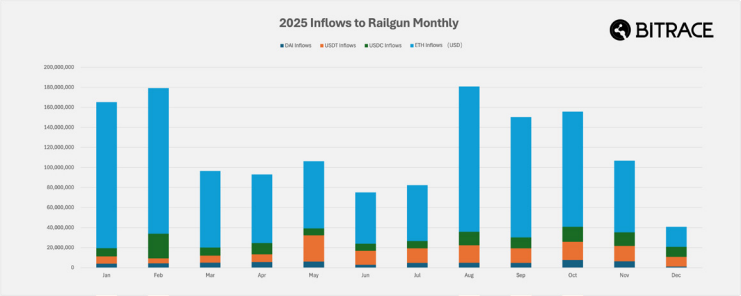
Statistics on the counterparties receiving outbound funds from addresses associated with traditional online gambling platforms show that in 2025, at least $1.7 billion in USDT or USDC was directly transferred to exchange user addresses, of which 82.40% flowed into the three major platforms: Binance, OKX, and Bybit.

Money laundering

Money laundering remains the primary area of illicit use of cryptocurrency, and it is mainly concentrated on the Tron network and the Ethereum network, achieved through the receipt and payment of USDT.

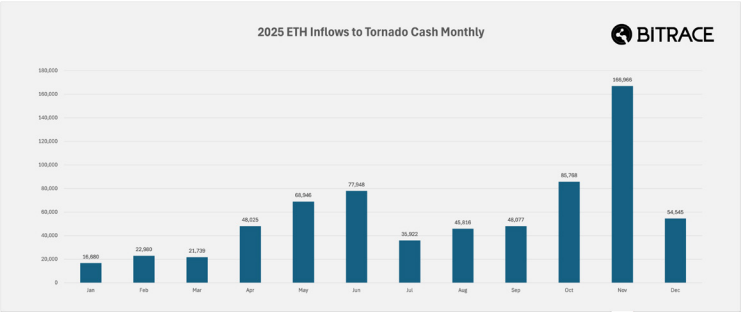


In 2025, high-risk addresses associated with money laundering collectively received funds totaling $69.8 billion. Among these, money laundering activities related to USDT on the Ethereum and Tron networks amounted to $5.7 billion and $60.2 billion, respectively.



In addition to traditional money laundering channels, the business scale of privacy transfer and coin mixing protocols has also been included in this statistics.

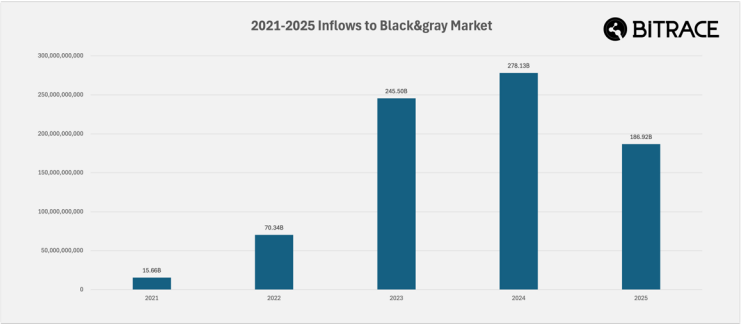
Railgun began to be heavily adopted by cryptocurrency practitioners this year, with inflows of DAI, USDT, USDC, and ETH tokens exceeding $1.4 billion in USD terms, of which the majority of the transaction volume was supported by ETH tokens.



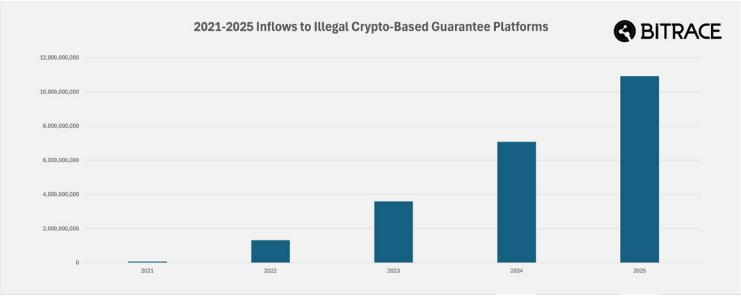
The well-known coin mixing protocol Tornado Cash, after having its OFAC sanctions lifted, has continued to operate. In 2025, it received a total of over 690,000 ETH tokens, equivalent to $2.5 billion.

Black and gray market

Organized crime networks in East Asia and Southeast Asia have illicitly adopted cryptocurrency, constituting the world's largest market for illicit cryptocurrency transactions. This portion of funds is utilized by entities such as transaction guarantee platforms, illicit cross-border human trafficking operators, telecom fraud compounds, and online or physical casinos for their business activities.

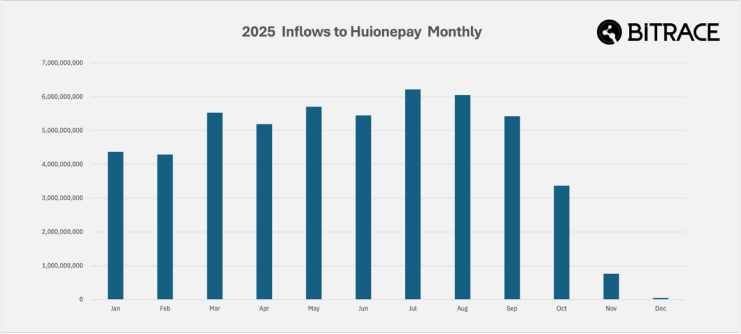


These stablecoin adoption activities occurred almost entirely on the Tron network. In 2025, addresses flagged as high-risk for Black and Gray Market transactions collectively received $186.9 billion, of which $186.7 billion was on the Tron network.



Although the overall scale of the Black and Gray Market has declined compared to the previous year, cryptocurrency-based illicit transaction guarantee platforms have continued to grow despite intense crackdowns by law enforcement agencies in various countries. According to Bitrace statistics, in 2025, the deposit addresses of various illicit transaction guarantee platforms collectively received 10.9 billion USDT.

Due to the differing guarantee rules across platforms, this figure cannot fully reflect the true scale of illicit transaction business. The actual transactions occur on the business addresses of the guarantee operators, and the scale should far exceed the deposit amounts.

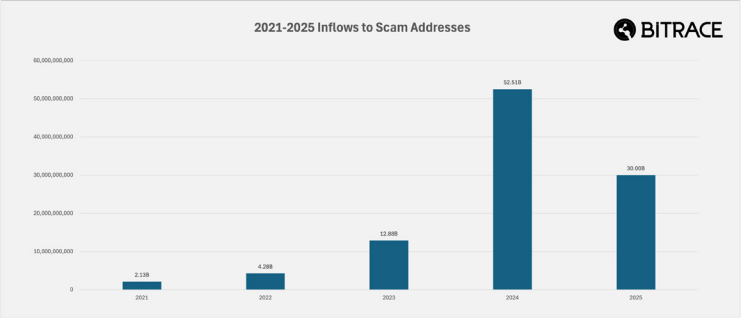


Due to the joint sanctions announced by the United States and the United Kingdom against the Cambodian Prince Group and Huione Group, Huione Group was compelled to temporarily suspend operations of its primary business—Huionepay. According to Bitrace statistics, Huionepay received a total of 52.4 billion USDT during the year, but chain activity had almost completely ceased by December.

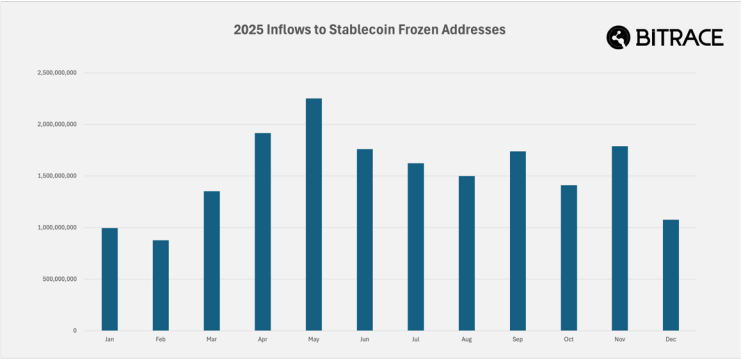
This event caused disruption in the local Black and Gray Market, with some operators unable to withdraw funds from Huionepay. The industry lost a stable and secure payment tool. Combined with ongoing enforcement actions from various countries and crackdowns on Telegram, organized crime networks in East Asia and Southeast Asia are currently in a state of chaos and disorder.

Fraud

Cryptocurrency fraud encompasses both direct financial scams targeting native cryptocurrency users and investment/lending scams directed at non-crypto investors. Both categories of illicit fraudulent activities remain key focal points for law enforcement agencies in various countries.



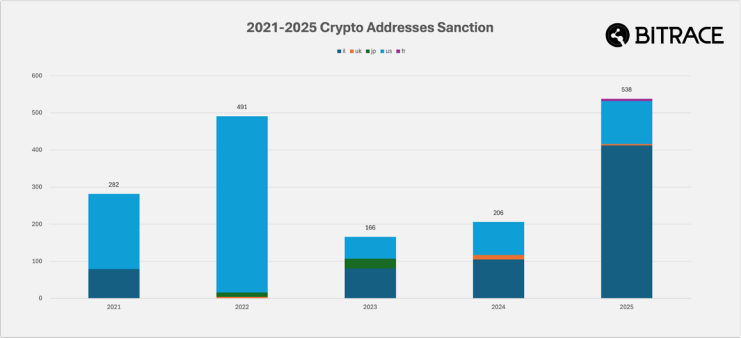
In 2025, the scale of funds associated with addresses tracked by Bitrace—involving real fraud cases, stablecoin freezes, address poisoning, and related activities—reached $30 billion, representing a significant decline compared to 2024.



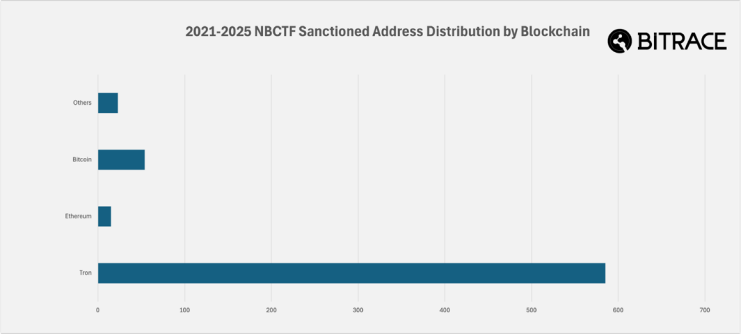
Among these, accompanied by the increase in law enforcement collaboration activities by Tether and Circle, the scale of stablecoin activities related to frozen addresses also reached an all-time high. In 2025, these addresses collectively received stablecoins valued at $18.3 billion.

Sanction

Bitrace mainly counts the national sanctions activities of the United States, Japan, Britain, Israel and France.



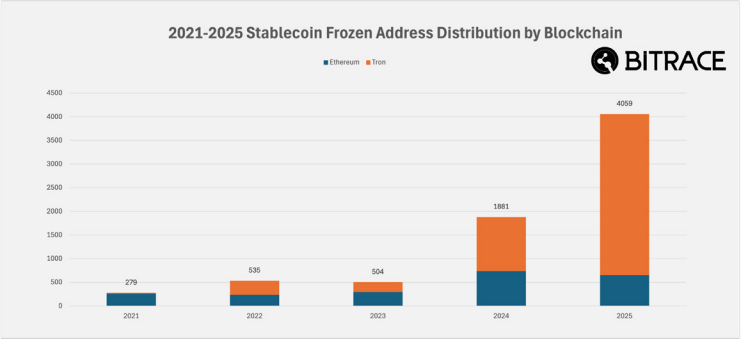
During the period from 2021 to 2025, five countries (excluding centralized cryptocurrency exchange accounts) imposed sanctions on at least 1,683 blockchain addresses in total, with the United States' OFAC accounting for the largest number, followed by Israel's NBCTF. The majority of Israel's sanctions occurred during the conflict period and were primarily directed at cryptocurrency addresses suspected of providing funding to Hamas, Hezbollah, and entities linked to Iran.



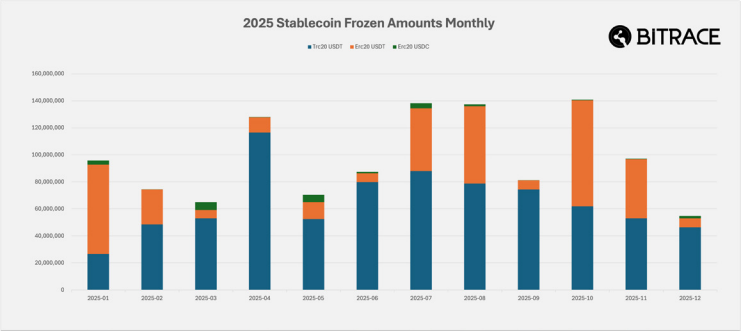
Further analysis of Israel's NBCTF sanctions activities between 2021 and 2025 shows that Tron network addresses have a total of 585, far exceeding other networks, indicating that current terrorist financing is making extensive use of the assets of Tron networks.

Stablecoin Blacklist

Limiting the operational permissions of specific blockchain addresses with respect to USDT or USDC is the primary means of law enforcement collaboration employed by the two major stablecoin issuers, Tether and Circle.



After excluding certain contract addresses and anomalous addresses, the number of frozen addresses in 2025 still reached a record high of 4,059, surpassing the total of 3,199 frozen addresses over the previous four years combined. Among them, 653 Ethereum addresses were frozen, while 3,406 Tron addresses were frozen—the latter almost entirely executed by Tether.



Further statistics on the amounts frozen by addresses show that in 2025, Tether successfully froze more than $1.1 billion in USDT, while Circle successfully froze more than $23 million in USDC. Circle's law enforcement collaboration activities were significantly lower than those of Tether.

Bring compliance and trust to Web3 with data

Bitrace is a regulatory technology (RegTech) company centered on cryptocurrency risk data analysis. We are dedicated to leveraging AI and big data technologies to more accurately and efficiently identify and monitor on-chain risks and criminal activities, providing clients with leading regulatory, compliance, and investigative tools, products, and service support.

We focus on the field of cryptocurrency crime investigations. To date, we have collaborated and connected with law enforcement agencies in multiple countries and Web3 enterprises, supported thousands of cases, cumulatively monitored hundreds of billions in risk funds, and successfully recovered billions of dollars in losses.

Contact us

Official website: bitrace.io
Mailbox:bd@bitrace.io
Twitter: @Bitrace_teamm
LinkedIn: @ Bitrace Techh