2025 Crypto Crime Report

BITRACE

2025 Crypto Crime Report

2025.4

Content

Introduction

The year 2024 marks a milestone for the Web3 industry. Major financial hubs, including the United States and Hong Kong, have introduced a series of regulatory compliance policies, fostering the orderly growth of Web3 within their jurisdictions. Meanwhile, the industry has experienced explosive expansion through the tokenization of real-world assets (RWA), the launch of virtual asset spot ETFs, and the widespread adoption of meme culture. The entry of sovereign wealth funds and traditional publicly listed companies has further propelled the total market capitalization of crypto to unprecedented heights.

However, alongside the rapid growth of the crypto economy, criminal enterprises have increasingly leveraged crypto infrastructure to optimize their operations or develop new forms of crime. In the early, less-developed phase of the crypto industry, illicit actors had limited access to crypto infrastructure, assets, and market depth. In contrast, today's thriving crypto economy has seen significant advancements in decentralized exchanges (DEXs), cross-chain bridges, decentralized finance (DeFi), and stablecoins.

Stablecoins, designed to maintain value stability by pegging to a sovereign currency, offer unique advantages in storing value and facilitating payments. Their massive transaction volumes, diverse application scenarios, and inherent anonymity have also made them attractive to illicit industries such as online gambling, money laundering, illicit trade, and fraud. Criminals exploit stablecoins in various ways, including using them as a value transfer medium, a money-laundering tool, and a storage mechanism for illicit funds.

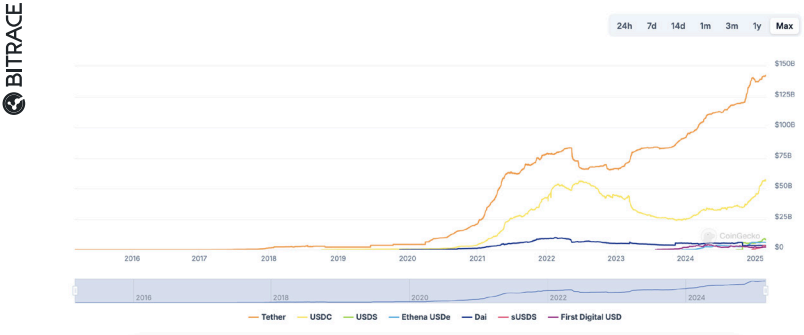


Figure 1: Stablecoin Market Capitalization Data Source: CoinGecko

According to data from the cryptocurrency aggregation platform CoinGecko, as of December 31, 2024, the total market capitalization of stablecoins has surpassed $229 billion. Among them, the two leading USD-pegged stablecoins—TetherUSD (USDT) and CircleUSD (USDC)—have reached market capitalizations of $142 billion and $57 billion, respectively.

This report aims to enhance the understanding of the crypto crime ecosystem and the risks associated with illicit stablecoins among government agencies and Web3 industry participants. By disclosing Bitrace's research findings on the relevant sectors, we seek to promote awareness and support the industry's path toward compliance.

The Ongoing Severity of Crypto-Related Crime

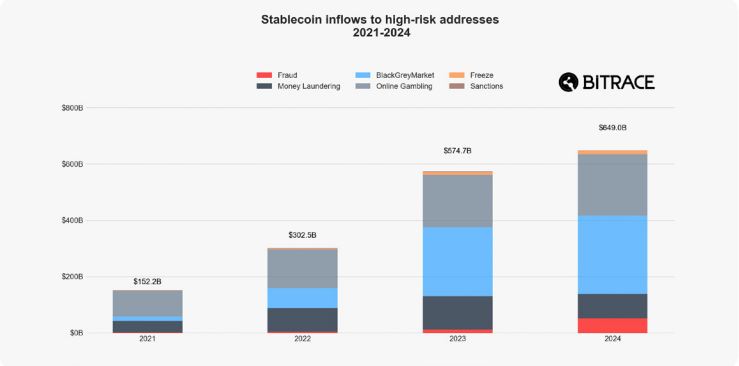


Figure 2: Stablecoin Inflows to High-Risk Addresses

Given that high-risk activities primarily occur on the Ethereum and TRON networks, Bitrace defines blockchain addresses used by illicit entities on these two networks to receive, transfer, or store stablecoins (ERC20_USDT, ERC20_USDC, TRC20_USDT, TRC20_USDC) as high-risk addresses. Over the course of 2024, the total incoming volume to such high-risk addresses reached $649 billion, slightly exceeding the amount recorded in the previous year.

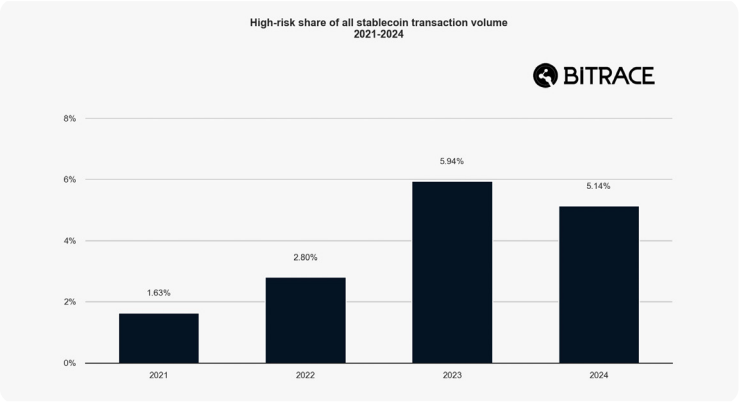


Figure 3: Proportion of High-Risk Activities in Total Stablecoin Transactions

Based on transaction volume, these high-risk activities accounted for 5.14% of the total stablecoin transactions in 2024, representing a 0.80% decrease compared to 2023. However, this proportion remains significantly higher than the levels observed in 2021 and 2022.

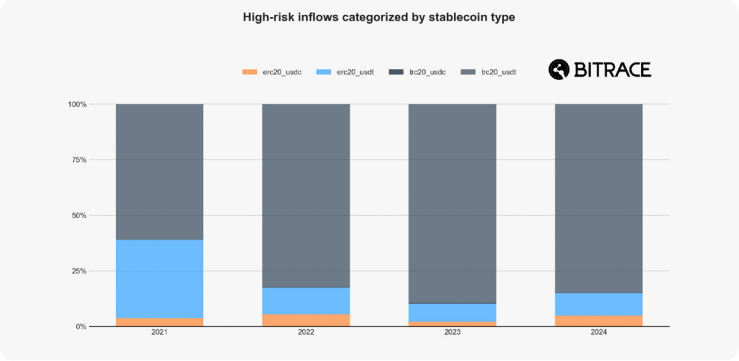


Figure 4: High-risk Inflows Categorized by Stablecoin Type

Analyzing by stablecoin type, USDT on the Tron network has consistently held the largest share from 2021 to 2024. However, in 2024, the share of both USDT and USDC on the Ethereum network saw an increase.

The Growing Scale of Illicit Transactions

Among high-risk address activities, the scale and proportion of stablecoin transactions related to illicit markets have shown a steady upward trend, with a particularly notable increase in 2024. This trend not only reflects the overall expansion of the stablecoin market but also underscores its growing role in illicit financial activities. The driving forces behind this phenomenon include both market demand and the internal evolution of illicit ecosystems.

One key factor is that as the stablecoin market matures, the scale of illicit transactions involving stablecoins has grown accordingly. Since 2021, fueled by the rise of DeFi protocols, the influx of institutional investments, and the expansion of cross-border payments, stablecoin issuance has surged—USDT, for instance, grew from approximately $25 billion in 2021 to around $125 billion in 2024. This massive liquidity market has inevitably been contaminated by illicit transactions. Whether

for online gambling, black-market trading, or fraud, criminals favor stablecoins for their stability and anonymity, making them central tools for money laundering, fund transfers, and settlement. The covert growth of this demand, intertwined with the expansion of the legitimate market, has further driven the continued issuance of stablecoins.

Another critical factor is the increasing industrialization and specialization within illicit ecosystems. In recent years, illicit activities have evolved from scattered individual operations into highly structured, efficiently coordinated criminal networks. For example, specialized "technology providers" develop phishing websites for fraud rings, "money mules" handle cross-border laundering, and "guarantee platforms" facilitate transaction matching and provide credibility endorsements. This division of labor has not only significantly increased the total illicit revenue and operational efficiency of these networks but has also led to a substantial rise in the volume of financial transactions within their infrastructure.

Sharp Decline in Money Laundering Activities

2024 marked a pivotal year for the crypto industry's transition toward compliance, driven by the intensive rollout of regulatory policies across multiple regions and a series of major law enforcement actions that led to a decline in crypto transactions linked to money laundering.

The U.S. and Hong Kong, among other key jurisdictions, demonstrated a heightened focus on crypto regulation in 2024 by introducing a series of landmark policy frameworks. These regulations covered Virtual Asset Service Provider (VASP) licensing, stablecoin oversight, Real-World Asset (RWA) tokenization guidelines, and compliance requirements for crypto spot Exchange-Traded Funds (ETFs). These measures set clear compliance standards for industry infrastructure, with Anti-Money Laundering (AML) obligations emerging as a core requirement.

At the same time, global enforcement efforts intensified significantly in 2024. The U.S. led an unprecedented crackdown on illicit activities within the crypto industry, signaling a zero-tolerance stance from regulators and a commitment to deterring potential violations through aggressive enforcement. In Asia, regions such as Hong Kong and Taiwan tightened their oversight following the end of the VASP licensing transition period. Several non-compliant VASPs were ordered to cease operations, and some license applications were revoked. Additionally, law enforcement agencies

carried out multiple coordinated actions against fraudulent crypto platforms, effectively removing bad actors from the market.

The combined impact of these regulatory and enforcement efforts has, to some extent, curbed the use of stablecoins for illicit fund laundering.

Fluctuations in Illicit Stablecoin Activity on Ethereum

In 2021, the Tron network rapidly emerged as a dominant player in the stablecoin market due to its deep partnerships with major exchanges and early competitive pricing advantages. This strategic positioning allowed Tron to quickly capture a significant share of stablecoin transactions, gradually eroding Ethereum's market dominance over the following two years.

However, by 2024, the competitive landscape of the stablecoin market underwent a significant shift. Consecutive technical upgrades on the Ethereum network alleviated congestion issues, resulting in lower transaction fees. Meanwhile, Tron adjusted its operational strategy by increasing transaction fees multiple times. This divergence in fee structures prompted some industry participants and users to reassess the cost-effectiveness of Ethereum, leading to a partial migration of stablecoin transactions back to the Ethereum network.

Illicit actors, who are particularly sensitive to transaction costs, were also affected by this shift. As a result, stablecoin transactions associated with illegal activities on the Ethereum network began to rise again, reversing the previous downward trend.

Online Gambling

Online gambling platforms are websites or applications that offer gambling services over the internet, allowing users to participate in various forms of betting without the need to visit physical casinos.

The legality of online gambling varies by country or region, with some jurisdictions enforcing strict regulations or differing classifications for certain aspects of the online gambling industry. However, as a long-standing non-economic activity, gambling is deeply embedded in nearly every nation or region, and the crypto world is no exception.

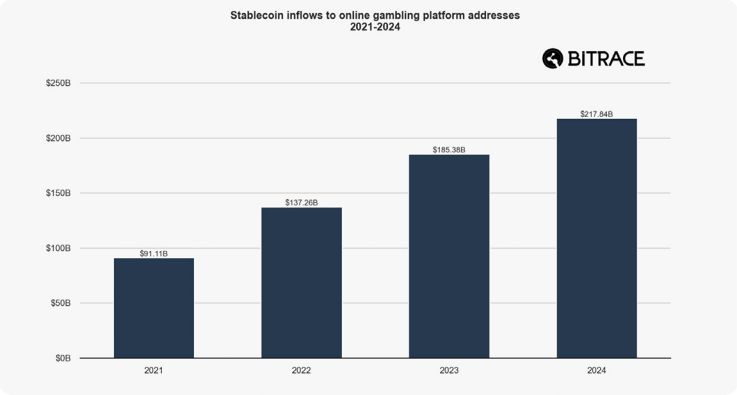


Figure 5: Stablecoin Inflows to Online Gambling Platforms Addresses

In 2024, the total fund flow involving online gambling platforms and the payment service providers facilitating their deposits and withdrawals reached $217.8 billion, marking an increase of over 17.50% compared to 2023.

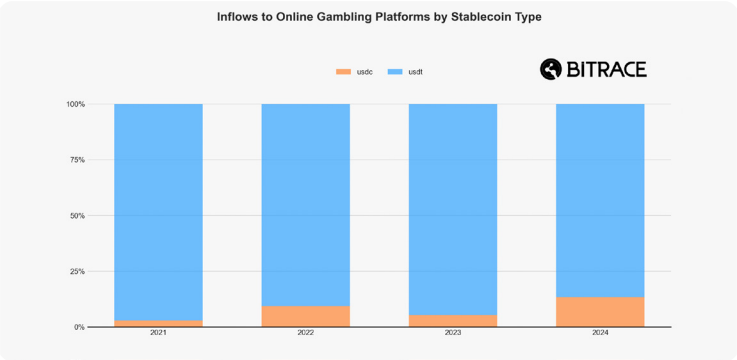


Figure 6: Inflows to Online Gambling Platforms by Stablecoin Type

An analysis of the stablecoins used by these platforms reveals a significant increase in the share of USDC, which accounted for 13.36% of transactions in 2024—more than double its 5.22% share in 2023.

Stablecoin Transfer Model in Online Gambling Platforms

For typical online gambling platforms and their agents, these entities primarily facilitate fund settlements for gamblers through self-built centralized cryptocurrency deposit, trading, and withdrawal systems, or by integrating cryptocurrency payment tools. Due to the anonymous nature of cryptocurrencies, government agencies find it challenging to regulate or enforce actions against such activities.

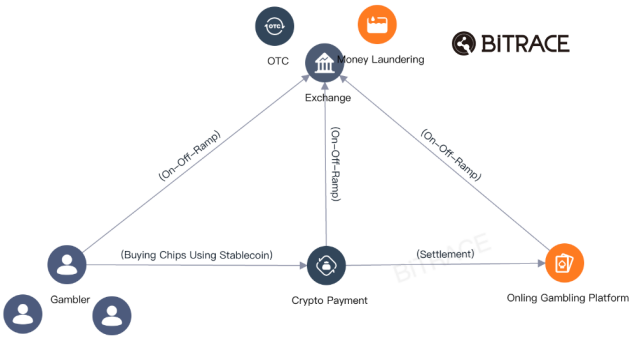


Figure 7: Usage of Stablecoins by Online Gambling Platforms

Taking an online gambling platform that uses a third-party cryptocurrency payment platform for user deposits and withdrawals as an example, the payment platform assigns individual cryptocurrency deposit addresses to gamblers. The payment platform manages these addresses and periodically aggregates funds. When a user requests a withdrawal, the payment platform reviews the request and processes the transfer. The payment platform and the gambling platform then regularly settle funds between them.

USDC, U.S. Elections, and the Rise of Polymarket

As a symbol of regulatory stability, USDC seized the dual opportunities presented by changes in the U.S. regulatory landscape and the growing demand for compliant stablecoins in the DeFi market. Its circulating supply skyrocketed from around $24.4 billion at the beginning of 2024 to $43.9 billion by the end of the year, with its market share rising from 18% to approximately 22%. This growth significantly influenced the online gambling industry, particularly platforms like Polymarket that use USDC for settlement.

The 2024 U.S. Presidential Election marked a key turning point. Donald Trump's promise to "make America the cryptocurrency capital" spurred a shift in regulatory attitudes. Compared to the SEC's tough stance under President Biden's administration, the new government appeared more supportive of the development

of compliant digital assets. USDC, issued by Circle, quickly became the favorite stablecoin among regulators due to its transparent reserve management and stringent compliance standards. After the U.S. approved a Bitcoin spot ETF in early 2024, institutional demand for compliant stablecoins surged, benefiting many compliant trading platforms. Meanwhile, USDT lost some trust due to regulatory uncertainties, further opening space for USDC.

In the DeFi sector, USDC's rise was equally significant. With its expansion to 16 blockchain networks (such as Solana and Ethereum) in 2024, and its higher security and liquidity, the multi-chain ecosystem reduced transaction friction, making USDC the preferred stablecoin in DeFi protocols.

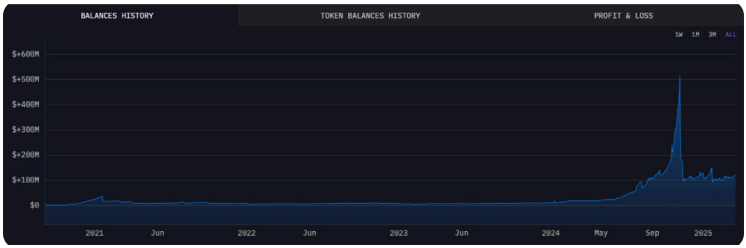


Figure 8: Polymarket Address Balances Data Source: Arkham

Polymarket, a decentralized prediction platform that uses USDC for settlements, saw substantial growth. During the 2024 U.S. election, the platform gained popularity as users placed bets on election outcomes and policy directions. It even predicted a 60% chance of Trump winning, surpassing traditional polls in accuracy. This blend of the real world and crypto economy not only increased USDC's frequency of use but also pushed its total transaction volume to over $9 billion in 2024.

This factor further accelerated the adoption of USDC in the stablecoin market and explains why USDC's share in the online gambling industry expanded in 2024.

New Changes: Vigilance Against the Threat of Compliant Stablecoin Funds

In 2024, the market share of compliant stablecoins, particularly USDC, saw significant growth. Emerging prediction platforms have begun to accept USDC as a tool for exchanging chips, and the payment companies providing services for these platforms

are also adopting USDC for fund settlements. Given the regulatory policies on the crypto industry under the leadership of the Trump administration, the adoption of USDC is expected to continue increasing and will likely be further leveraged by the online gambling industry.

Moreover, with USDC's deep integration into new blockchains and DeFi protocols, more native on-chain USDC, non-native bridged USDC, and other USDC-pegged tokens are continuously emerging. This presents greater challenges for security companies focused on threat perception and fund tracking, demanding more robust and sophisticated solutions.

For cryptocurrency companies, it's crucial to enhance your Know Your Transaction (KYT) programs by incorporating more threat intelligence sources related to USDC. Security firms, on the other hand, must upgrade their tracking tools to support multi-chain functionality and improve threat intelligence integration to recognize real-time changes in fund settlement patterns within the online gambling sector, thus adapting to the rapid evolution of fund flows in the gambling industry.

This proactive approach will help ensure better oversight, compliance, and the ability to mitigate potential risks associated with the increasing adoption of compliant stablecoins like USDC in illicit activities.

Black and Gray Market Transactions

Black and gray market transactions refer to illegal or illicit trading activities conducted on the internet, where individuals or organizations use various technical means to facilitate or assist in criminal acts. These transactions are characterized by their focus on obtaining unlawful economic benefits or disrupting the order of the digital ecosystem to achieve specific goals. Black and gray market activities span traditional internet areas, but with the rise of blockchain and cryptocurrency, their methods and forms are continually evolving, becoming more complex and covert.

In traditional online environments, black and gray market transactions often involve the use of cryptocurrency for illegal activities, or advanced encryption tools replacing traditional methods to increase secrecy and deception. For example, criminals may use cryptocurrency's anonymity to facilitate ransomware payments, dark web transactions, or money laundering, reducing the chances of detection or sanction by law enforcement. This method not only improves the efficiency of illegal activities but also creates technical barriers that increase the difficulty of regulation and tracking.

In contrast, the emerging blockchain-based black and gray market activities showcase distinct industry-specific characteristics. These activities no longer simply use cryptocurrency as a tool; they directly target the digital assets of cryptocurrency investors or institutions within the crypto industry, forming illegal acts endemic to the ecosystem. Examples include hackers using phishing attacks, exploiting smart contract vulnerabilities, or conducting DeFi platform scams to steal crypto assets from users' wallets or manipulate the market to create fake trading volumes for profit. These black and gray market activities make full use of the decentralized nature of blockchain, its immutability, and the automation features of smart contracts, deeply embedding criminal actions within the crypto ecosystem. Compared to traditional black and gray markets, blockchain-based black and gray markets are more specialized, involve higher technical barriers, and often collaborate with cross-border criminal networks, further complicating enforcement efforts.

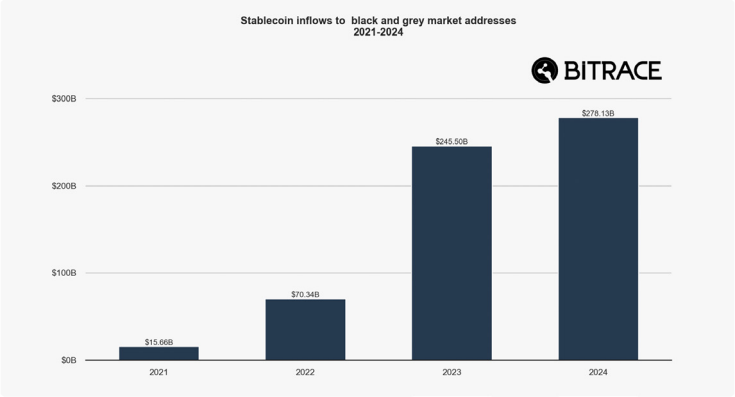


Figure 9: Stablecoin Inflows to Black and Gray Market Addresses

In 2024, business addresses associated with illicit and gray-market transactions on the Ethereum and TRON networks collectively received over $278.1 billion, slightly exceeding the amount recorded in 2023. The transaction volumes in both years far surpassed those of 2021 and 2022. As highlighted earlier in this report, the growth in illicit transaction volume has closely paralleled the rapid expansion of the stablecoin market.

Crypto Currency Transaction Guarantee Platforms: Core to the Black and Gray Market

A crypto transaction guarantee platform is a third-party service mechanism designed to provide security for both parties involved in a transaction. Acting as an intermediary or using automated technologies, these platforms ensure the safety of funds and fulfillment of obligations during the transaction process. These platforms are widely used in scenarios where trust needs to be established, particularly when buyers and sellers are unfamiliar with each other or when the transaction carries certain risks.

The typical operations of a transaction guarantee platform follow these basic steps:

① Transaction Initiation: The buyer deposits funds into a designated escrow account on the platform, rather than directly paying the seller.

② Performance Supervision: The seller provides goods, services, or assets according to the transaction terms and submits relevant proof (such as shipping tracking

numbers or digital asset transfer records).

③ Condition Verification: The platform verifies whether the transaction conditions have been met, such as the buyer confirming receipt of the goods or services as agreed.

④ Funds Release: Once conditions are met, the escrowed funds are released to the seller. If the conditions are not met, the funds may be refunded to the buyer.

⑤ Dispute Resolution: If there is a dispute regarding the transaction's outcome, the platform will mediate the situation according to its rules, or through manual intervention.

In traditional finance, such mechanisms are common in "third-party payment" or "escrow services" based on fiat currency payment systems. However, in crypto transaction guarantee platforms—characterized by anonymity—this mechanism is typically achieved through cryptocurrency payment tools or smart contracts. This model combines traditional financial escrow concepts with the decentralized nature of blockchain technology, aiming to reduce trust risks and the possibility of fraud during transactions.

Because of this, black and gray market industries have managed to introduce de-trust and high anonymity features into their operations through cryptocurrency guarantee transaction platforms. These platforms help eliminate the need for trust and enhance operational privacy in criminal activities.

For example, in the case of popular cryptocurrency romance scams, the fraudsters create fake online personas to initiate internet relationships and lure victims into participating in false cryptocurrency investment schemes, ultimately scamming them of money. During the scam, the fraudsters need to purchase large amounts of personal data of potential victims, customize fake identities and scripts, subscribe to SMS/email marketing services, create fraudulent websites, and launder illegally obtained cryptocurrency. All of these services or goods are typically acquired through cryptocurrency transaction guarantee platforms.

Currently, crypto transaction guarantee platforms have become central to criminal industry chains. By investigating the platform’s customers and merchants, a large amount of crypto funds linked to illicit activities can be traced.

Case Study: Huione Guarantee

Huione Group is a large financial group based in Cambodia, with business sectors that include cryptocurrency wallets, payments, transaction guarantees, insurance, and cryptocurrency exchanges. Its core payment and guarantee business heavily uses USDT, and according to Bitrace's tagged data, the official and user addresses for HuionePay and HuioneGuarantee exceed 180,000, making it the largest crypto enterprise in the region, with influence extending across Southeast Asia and East Asia.

Due to Southeast Asia being a hotspot for illegal activities involving cryptocurrencies, and since Huione Guarantee does not require merchants or customers to remain anonymous, its business addresses have, to some extent, been contaminated by risky funds.

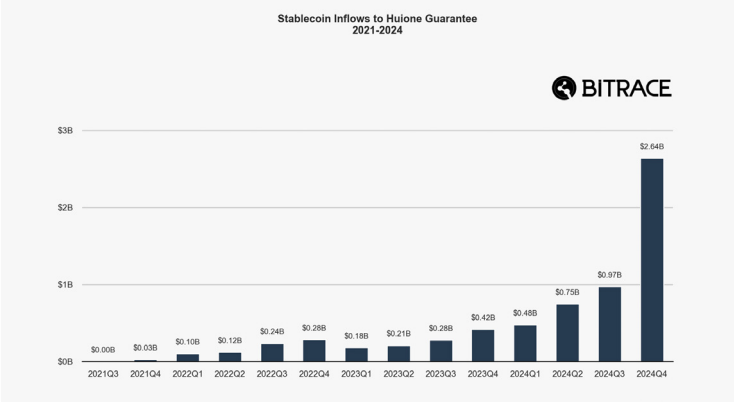


Figure 10: Stablecoin Inflows to Huione Guarantee

The rise of Huione Guarantee and its competitors in Southeast Asia has coincided with the gradual adoption of stablecoins in the region's real economic activities. This trend became particularly evident in 2024, with its business scale expanding to $2.64 billion in the fourth quarter of the year.

Unchanging Trend: The Black and Grey Market for Crypto Transactions Unaffected by Market Conditions

2021 marked the beginning of the black and grey market ecosystem utilizing cryptocurrencies for business operations. In the years that followed, the market scale continued to grow year by year. Even during the severe downturn of the crypto market in 2022, the transaction volume still saw significant growth compared to 2021, not to mention the crypto bull market years of 2023 and 2024.

Therefore, it is foreseeable that as long as multiple regions with high crypto-related crime rates globally fail to fundamentally eradicate the criminal activities or take legal measures to limit them, the growth of the black and grey market for crypto transactions will not be significantly affected, even if the next two years see a crypto bear market.

Fraud

Cryptocurrency fraud refers to various fraudulent activities carried out using digital currencies or blockchain technology. Compared to traditional fraud, cryptocurrency fraud incorporates cryptocurrencies into existing fraudulent processes or creates new scams based on the unique characteristics of blockchain technology. These include, but are not limited to, phishing scams, investment fraud, and fake exchanges.

Because of the involvement of cryptocurrencies, these scams are more difficult to identify, and the losses are harder to recover. The reasons include:

- Anonymity: Transactions do not require real names, making it difficult to trace hackers or fraudsters.
- Irreversibility: Once a transfer is made, it cannot be undone, leaving victims with little recourse to recover funds.
- Lack of Regulation: Global regulations are not unified, and some cases may be restricted by local jurisdiction, preventing proper investigation and providing fraudsters with opportunities to exploit the system.
- Technical Complexity: Ordinary users may lack the technical knowledge to distinguish between legitimate and fraudulent activities.

These factors make cryptocurrency fraud a global threat.

Surge in Crypto-Related Fraud

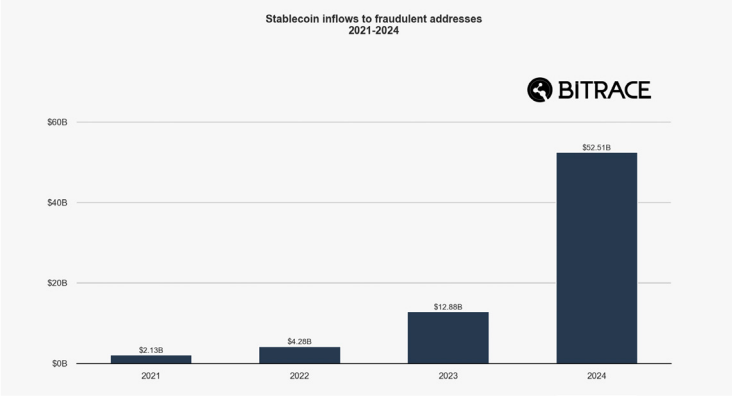


Chart 11: Stablecoin Inflows to Fraudulent Addresses

In 2024, blockchain addresses associated with fraudulent activities saw an explosive increase in stablecoin inflows. The total volume reached $52.5 billion, surpassing the combined figures of 2021 through 2023.

However, this dramatic surge may not fully reflect the actual growth in fraud, as the statistics are influenced by the methodologies used by security firms and the evolving sophistication of illicit actors. For example, as security vendors expand coverage to newer blockchains, more criminal activities are detected, meaning that incidents from previous years may have gone unrecorded. Additionally, cases occurring within centralized institutions or those not voluntarily disclosed by victims are often excluded from the data.

With continued improvements in data collection and increased transparency through case disclosures, the figures in next year's report are expected to rise even further.

Funds Flowing from CEX to Fraud Platforms

Fraud schemes targeting novice investors, such as fake exchange mining pool scams and romance frauds, rely heavily on centralized exchanges (CEX). Victims are required to first purchase stablecoins from CEXs and withdraw the funds to blockchain addresses provided by the fraudsters. By monitoring the transfer activities from the exchange's hot wallet addresses to fraudulent addresses, we can measure

the extent of the damage caused by such scams to novice users.

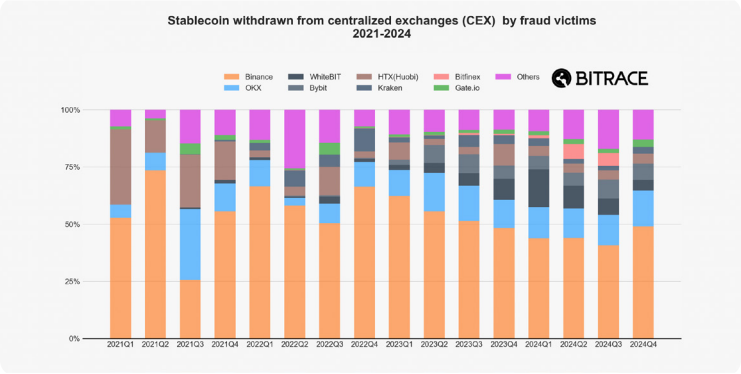


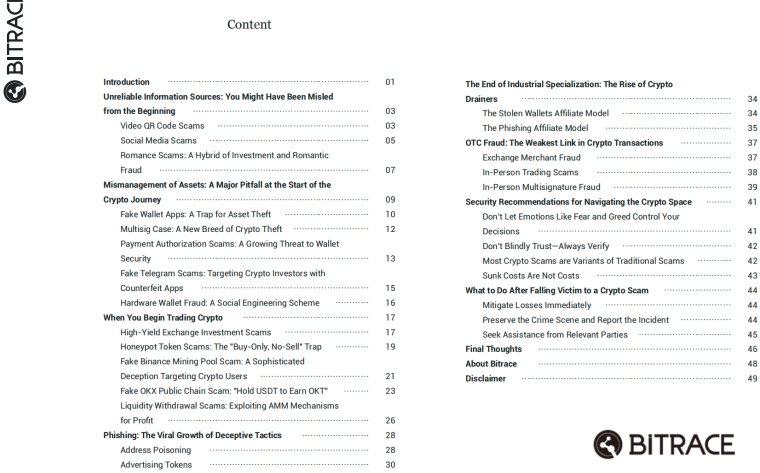
Figure 12: Proportion of Stablecoin Transfers from Major Centralized Exchanges to Fraudulent Addresses

Overall, the volume of transfers from centralized exchanges (CEXs) to fraudulent addresses has generally been proportional to the scale of their business operations. For instance, FTX and HTX were notably active between 2021 and 2022, with a high number of victim withdrawals observed during that period. However, following their bankruptcy or user offboarding, these figures declined rapidly.

Moreover, fraud-related activity has been particularly rampant in Asia, especially in Southeast Asia. As a result, exchanges with strong regional ties—such as OKX, Bybit, and Gate—have exhibited a disproportionately higher share of outflows to fraudulent addresses relative to their overall transaction volume.

Bitrace Launches Anti-Fraud Handbook

Based on investigations of thousands of real cryptocurrency-related cases (Crypto Crimes), Bitrace launched an anti-fraud handbook in 2024 aimed at regular cryptocurrency investors.



Content

Figure 13: Bitrace Anti-Fraud Handbook

The handbook outlines the various types of fraud that different investors may encounter and provides detailed descriptions of fraudulent techniques. Its goal is to help readers recognize and avoid fraud, thereby reducing financial losses.

KYT Can Effectively Prevent Crypto Fraud Activities

The KYT (Know Your Transaction) program analyzes blockchain transaction data to track the source and flow of funds in each transaction. The public ledger feature of blockchain ensures that every transaction is recorded, and KYT leverages this feature to identify whether funds originate from illegal sources or are about to enter illicit addresses, preventing the further circulation of fraudulent funds.

In practice, KYT has been widely adopted in cryptocurrency exchanges, wallet services, and financial compliance fields. For example, some centralized exchanges use KYT technology to assess risk by monitoring user behavior patterns and fund flows, imposing restrictions on high-risk transactions. However, the application of this program is still limited in wallets, decentralized exchanges (DEX), and crypto payment platforms, leaving significant room for improvement in countering fraud events.

Money Laundering

Money laundering refers to the process of legitimizing illicit funds, primarily by disguising or concealing their source and nature through various methods, so that they appear to be legal. This activity includes, but is not limited to, providing funding accounts, assisting in the conversion of assets, and helping to transfer funds or remit them abroad. Cryptocurrencies—especially stablecoins—have been exploited for money laundering activities due to their low transaction costs, geographical neutrality, and certain censorship-resistant properties, making them attractive for illicit use early on.

Cryptocurrency money laundering often involves off-chain trading markets, where exchanges between fiat and cryptocurrencies, or vice versa, take place. These laundering scenarios vary in form, but their essence remains the same: to obstruct law enforcement's ability to trace the flow of funds, including both traditional financial institution accounts and cryptocurrency exchange accounts.

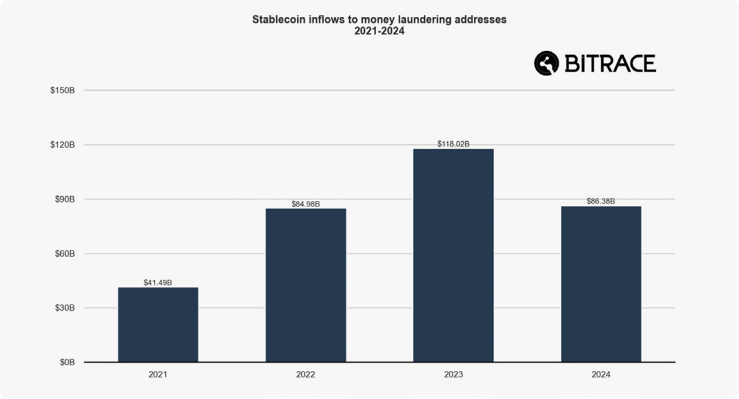


Figure 14: Stablecoin Inflows to Money Laundering Addresses

In 2024, blockchain addresses associated with money laundering activities received a total of $86.3 billion in stablecoins—slightly lower than in 2023 and on par with 2022. This stabilization may indicate that major enforcement actions and regulatory

initiatives over the past two years have had a tangible deterrent effect on money laundering in the crypto space. A more detailed analysis of this trend will be provided in the Regulatory and Policy Insights section of this report.

Funds Flowing from CEX to Money Laundering-Related Addresses

With the gradual improvement of the cryptocurrency industry's infrastructure, decentralized exchanges (DEX), cross-chain bridges, and mixing platforms have shown a significant role in cryptocurrency money laundering activities. Perpetrators are increasingly avoiding direct fund dumps into centralized exchanges (CEX) and are instead opting to obfuscate the funds on-chain, making them harder to trace before converting them into cash.

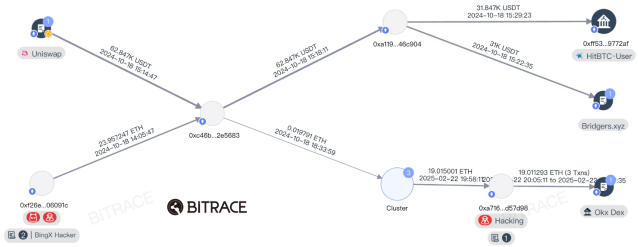


Figure 15: BingX Hacker Money Laundering Techniques

An example of this trend can be seen in the BingX hack incident in Q4 2024, which has now been confirmed as the work of the North Korean hacker group Lazarus. After illicitly obtaining funds from the victimized exchange, the group quickly engaged in on-chain money laundering activities. During this process, they extensively used decentralized exchanges, decentralized trading aggregators, cross-chain bridges, and centralized exchanges. Despite these cryptocurrency entities' efforts to intercept the funds, the results were limited, with most of the stolen funds remaining unrecovered.

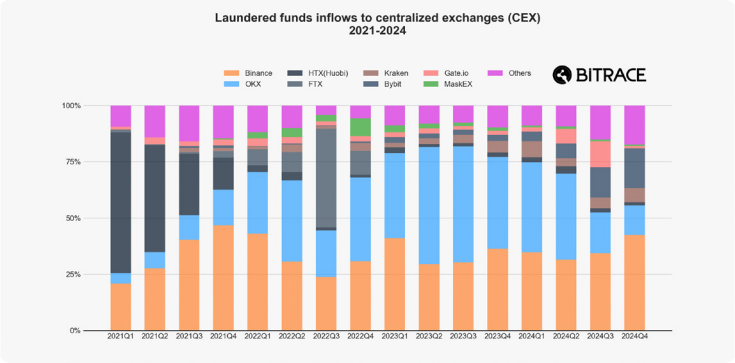


Figure 16: Proportion of Stablecoin Amounts Received by Centralized Exchanges in Money Laundering Activities

Considering that centralized exchanges have inherent advantages over other entities in terms of fund monetization, they are more likely to be targeted by money laundering syndicates. Bitrace conducted a fund audit on the hot wallet addresses of major centralized cryptocurrency exchanges. The results, similar to those in the fraud section, show that the amount of money laundering funds received by these platforms is generally proportional to their business scale. However, OKX's share of such funds has notably decreased in recent quarters, which may reflect its improved compliance practices.

Decentralized Protocols: A More Severe Money Laundering Situation

With the widespread adoption of blockchain technology and the increased ease of use of decentralized protocols, more and more criminal organizations are able to obfuscate, launder, and conceal crypto funds with very low technical barriers, posing a huge threat to government regulatory agencies and the risk control departments of crypto entities.

Currently, major regulatory bodies are implementing legislation and regulation for virtual asset service providers (VASPs), mainly focusing on Virtual Asset Over-the-Counter Trading Service Providers (VAOTCs) and Virtual Asset Trading Platforms (VATPs). However, the regulatory progress for decentralized protocols deployed on the blockchain is slow. Over the next few years, the industry will face an even more severe money laundering situation.

Stablecoin Freezing

Stablecoins issued by centralized institutions, in addition to possessing the anonymity and permissionless usage features of other cryptocurrencies, also grant the issuers significant control over the token system. This allows developers to issue or burn stablecoins for specific addresses or restrict certain addresses from performing operations with stablecoins, a process known in the industry as stablecoin freezing.

Such centralized freezing activities are typically triggered by law enforcement requests from governments worldwide, aimed at blocking illegal activities conducted using stablecoins and intercepting affected assets to prevent further damage.

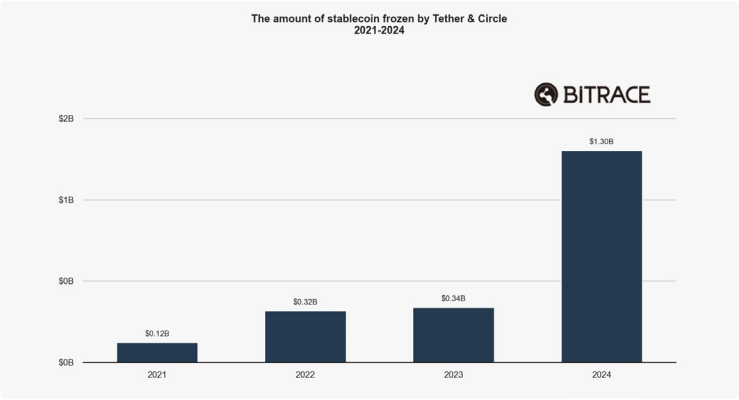


Figure 17: Amount of stablecoins frozen by Tether and Circle

2024 was a year where stablecoin issuers actively cooperated with law enforcement. Tether and Circle together froze over $1.3 billion worth of stablecoins on the Ethereum and TRON networks, which is double the amount frozen in the previous three years.

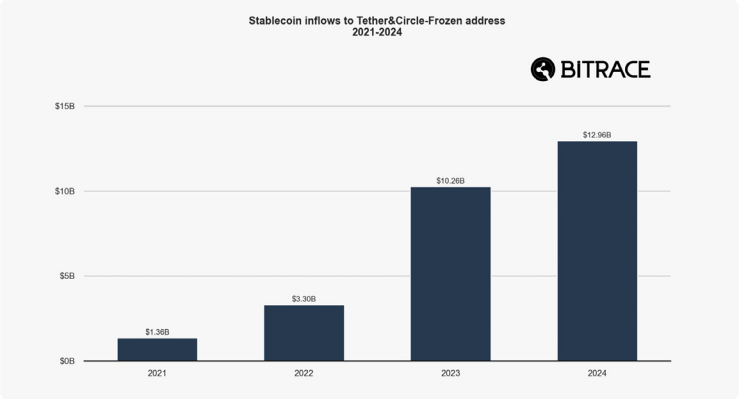


Figure 18: Stablecoins Inflows to Tether & Circle Blacklisted Addresses

An analysis of fund transfers involving frozen addresses reveals that the transaction volume in 2024 reached $12.9 billion, remaining largely consistent with 2023. This suggests that illicit on-chain crypto activities had been active for several years, but it wasn't until 2024 that effective enforcement and countermeasures began to take significant effect.

Case Study: HuionePay Frozen $29.62 Million USDT by Tether

HuionePay, another major product under the Huione Group, along with Huione Guarantee, provides cryptocurrency services to users in Southeast Asia and is a leading payment and guarantee company in the region. On July 13, 2024, Tronscan displayed that HuionePay's hot wallet address was restricted by Tether, resulting in $29.62 million worth of USDT being frozen and unable to be transferred.

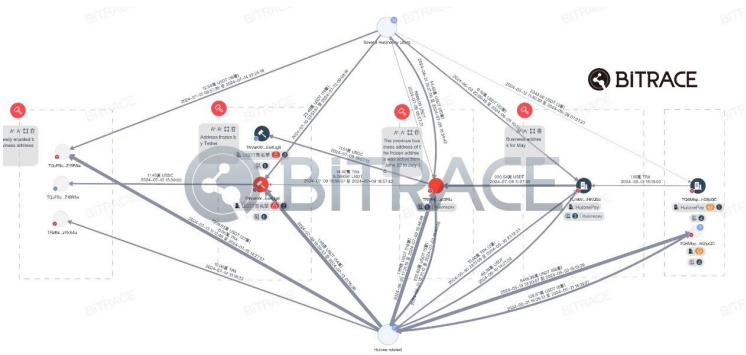


Figure 19: HuionePay Frozen Case Fund Analysis

The cause was an attack on the centralized Japanese cryptocurrency exchange DMM by the Lazarus hacker group. The attack led to over $600 million in Bitcoin losses. The stolen assets, such as tBTC and BTC.b, were swapped on chains like Avalanche and Ethereum into USDT, USDC, and DAI worth approximately $31.82 million. After cross-chain swaps, about $14 million of this amount ended up in HuionePay's business address, resulting in the freezing of funds.

This incident garnered significant attention in the industry due to the large amount of frozen funds and the special nature of Southeast Asian entities, highlighting the cross-border characteristics of crypto money laundering.

On-chain Freezing by Stablecoin Issuers: A Powerful Anti-Money Laundering Tool

The transparency of blockchain, combined with the sanctioning power of stablecoin issuers, allows for the quick identification and freezing of suspicious funds. Compared to traditional financial systems, on-chain sanctions can take effect within seconds without the need for cumbersome cross-border bank coordination. This speed is crucial in preventing money laundering funds from rapidly being transferred.

Currently, the largest stablecoin issuer, Tether, is advancing its compliance program, while the second-largest stablecoin issuer, Circle, is already a compliant entity, including in the U.S. With the assistance of these two institutions, on-chain freezing will become a powerful anti-money laundering weapon.

Sanctions

Government sanctions refer to economic, trade, financial, diplomatic, or other restrictive measures imposed by one country or international organization to punish or exert pressure on specific countries, entities, individuals, or activities in order to achieve political, economic, or security objectives. As illicit entities increase their use of cryptocurrencies, blockchain addresses associated with sanctioned parties are also brought under sanction.

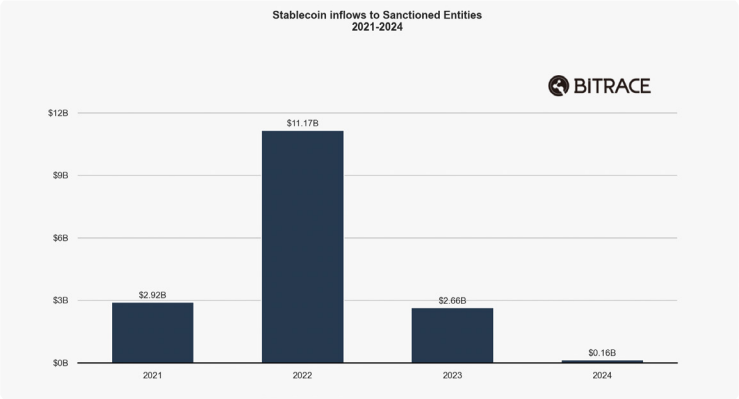


Figure 20: Stablecoin Inflows to Blockchain Addresses Associated with Sanctioned Entities (OFAC and NBCTF)

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and Israel's National Bureau for Counter-Terrorism Financing (NBCTF) are two key institutions involved in sanctions and counter-terrorism financing. These organizations have a significant focus on combating terrorism financing and financial networks associated with terrorist groups such as Hamas. When examining the blockchain addresses associated with sanctioned entities disclosed by these two organizations, the overall funds received reached their peak in 2022 and have declined year over year since then.

The reason for this decline is due to the 2022 OFAC sanctions against the Russian

centralized exchange, Garantex, which was accused of providing money laundering services for Russia's largest darknet marketplace, Hydra Market. Following these sanctions, Garantex began frequently changing its business addresses to evade enforcement cooperation from stablecoin issuers. Due to limitations in the methods and scope of the statistics, it became difficult to accurately track the scale of its funds, resulting in the decrease observed in the chart.

Case Study: Tornado Cash Sanctioned by OFAC

Tornado Cash is a decentralized cryptocurrency mixer operating on the Ethereum blockchain, launched in 2019. It uses smart contract technology to mix users' cryptocurrency deposits with funds from other users and redistributes them, thereby obfuscating the source and destination of funds to enhance transaction privacy. While this design attracted legitimate users seeking privacy, it also facilitated illicit activities.

Among the many groups exploiting Tornado Cash for money laundering, the Lazarus hacking group was particularly notable, which drew significant attention from the U.S. government. The U.S. Treasury Department believed that Tornado Cash failed to take effective measures to prevent illegal funds from flowing, violating anti-money laundering (AML) and sanctions compliance requirements, and became a tool for malicious actors to evade U.S. sanctions.

On August 8, 2022, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) imposed sanctions on Tornado Cash, adding it to the "Specially Designated Nationals and Blocked Persons List" (SDN List). This marked the first time OFAC had imposed sanctions on a decentralized smart contract, rather than on an entity or individual. The specific measures included:

- Freezing all assets of Tornado Cash within the United States or under U.S. control.
- Prohibiting U.S. citizens and entities from engaging in any transactions with Tornado Cash, including those involving associated Ethereum addresses.
- Justifying the sanctions on the grounds that Tornado Cash "facilitated money laundering for malicious cyber actors supported by North Korea."

Additionally, some major centralized exchanges and DeFi platforms began isolating Tornado Cash users, blocking addresses that received related funds from accessing the platform's official front-end or transferring funds into the platform.

However, on November 26, 2024, the U.S. Fifth Circuit Court of Appeals made a landmark ruling, overturning OFAC's sanctions on Tornado Cash. The court ruled that these contracts "cannot be owned or controlled" and therefore do not constitute "property" as defined by the International Emergency Economic Powers Act (IEEPA), deeming OFAC's actions as overreach. Nonetheless, Tornado Cash's reputation and transaction volumes have not returned to their previous levels.

This sanction event underscores the vulnerability of DeFi protocols when facing regulatory scrutiny and highlights the significant influence government decisions can have on the operations of entities within the cryptocurrency industry.

Ineffectiveness of Sanctions on Cryptocurrency Entities

While regulatory measures imposed by government agencies can have a significant impact on the operations of sanctioned entities, they have little effect on criminal groups utilizing these infrastructures for illegal activities. This is primarily due to the anonymity and permissionless nature of cryptocurrency technology, which makes it difficult to sanction such entities and highly replaceable.

Take Tornado Cash as an example. Although the sanctions imposed by OFAC were stringent, the contract was deployed on a decentralized blockchain network. Even if the official front-end was blocked, users could still directly interact with the blockchain contract to launder funds. In subsequent security incidents, attackers accessed the protocol to collect fees and launder illicit proceeds.

Moreover, the cryptocurrency industry hosts many privacy protocols. Even if Tornado Cash were sanctioned, other similar services remain available as alternatives, offering users fund obfuscation services. In the February 2025 Bybit hack, which was also attributed to Lazarus, the hackers extensively used Thorchain and Li.Fi protocols instead of Tornado Cash.

Therefore, sanctions only punish the cryptocurrency entities being exploited, and have minimal impact on the criminals carrying out the illicit activities. Regulatory authorities should conduct more in-depth investigations into cryptocurrency-related crimes and take appropriate enforcement actions against criminal groups.

Crypto Regulatory Trends and Their Impact

The year 2024 marked a significant shift toward compliance in the cryptocurrency industry. Globally, major regulatory bodies moved from a wait-and-see approach to more active intervention, steering the industry toward greater transparency and standardization. Key developments include:

- European Union (EU): The Markets in Crypto-Assets (MiCA) regulation fully came into effect on December 30, 2024, imposing unified oversight on crypto asset issuers, trading platforms, and service providers (CASPs). MiCA mandates licensing, AML/KYC compliance, and bank-level capital and risk management requirements for stablecoin issuers.
- United States: Congress debated multiple bills, including the FIT 21 Act and the Stablecoin Act, while the SEC approved Bitcoin and Ethereum spot ETFs, signaling a degree of regulatory recognition.
- Japan: The Financial Services Agency (FSA) tightened AML measures, enhancing customer information-sharing requirements for crypto exchanges to prevent money laundering while continuing to recognize crypto as legal property.
- South Korea: The country implemented the Virtual Asset User Protection Act, enforcing stricter transparency and record-keeping standards for exchanges. Authorities plan to release crypto asset listing guidelines in mid-2024.
- Hong Kong: The Hong Kong Monetary Authority (HKMA) introduced a stablecoin issuer regulatory sandbox, balancing innovation with compliance, while strengthening licensing requirements for crypto exchanges.
- United Kingdom: The UK continued developing stablecoin regulations, integrating them into its financial framework while launching a digital securities sandbox to support blockchain technology.

These policies highlight a global shift from lenient oversight to stricter regulations, focusing on AML, consumer protection, and financial stability. Some regions, such as the EU and Hong Kong, are seeking a balance between regulation and innovation to foster sustainable industry growth.

Hong Kong's Compliance Policies Reduce Crypto Entities' Financial Risks

Bitrace believes that Hong Kong's compliance policies have effectively lowered financial risks for local crypto entities by establishing a clear regulatory framework that balances innovation and risk management.

Clear Regulations Reduce Legal Uncertainty

Since 2022, Hong Kong has progressively refined its crypto regulatory framework, particularly by amending the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) to bring Virtual Asset Service Providers (VASPs) under formal supervision. In June 2023, the Securities and Futures Commission (SFC) officially implemented a licensing regime for crypto exchanges.

Under these regulations, crypto entities such as exchanges and custodians must obtain an SFC license, requiring strict adherence to AML, CFT, and customer fund protection measures. This well-defined legal framework reduces regulatory uncertainty, mitigating risks associated with sudden bans, fines, or operational disruptions. As a result, the likelihood of fund freezes or outflows due to unclear policies has significantly decreased.

Crackdown on Illicit Activities Reduces Systemic Risk

Hong Kong's compliance policies actively combat money laundering, terrorist financing, and sanction evasion, requiring VASPs to implement Know Your Customer (KYC), Know Your Transaction (KYT), and transaction monitoring measures.

The SFC collaborates with Hong Kong law enforcement and international bodies such as the Financial Action Task Force (FATF) to track and freeze illicit funds. By eliminating non-compliant entities, such as sanction-evading platforms like Garantex, Hong Kong has reduced systemic financial risks linked to illicit activities. Additionally, partnerships with crypto security firms like Bitrace enable cooperative investigations, minimizing losses for victims in crypto-related fraud cases.

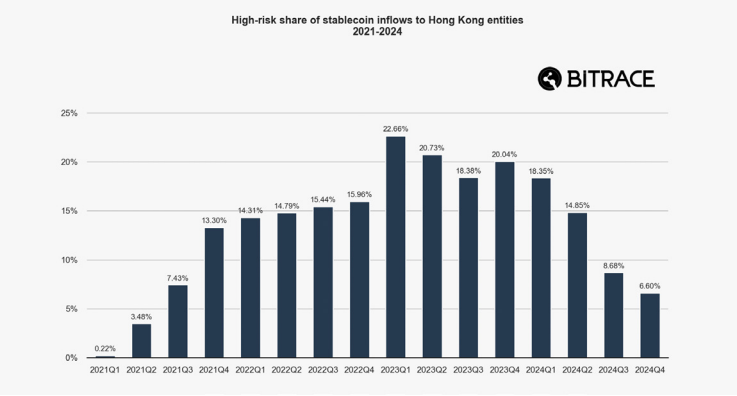


Figure 21: Proportion of High-Risk Funds in Stablecoin Inflows of Hong Kong Web3 Entities

An analysis of fund flows related to VATP and VAOTC addresses primarily serving Hong Kong customers indicates that after Q3 2023, the proportion of high-risk stablecoins flowing into the local market dropped sharply. This suggests that following the introduction of compliance policies and several high-profile crypto-related cases, stablecoin transactions associated with risky activities have been effectively curbed in Hong Kong.

In summary, Hong Kong's compliance policies—through clear legal requirements, customer fund protection, crackdown on illicit activities, institutional capital attraction, and alignment with international standards—have fostered a safer and more controlled crypto ecosystem. This not only reduces direct financial losses from hacks, platform bankruptcies, or legal penalties but also lowers indirect risks by enhancing market trust and stability. While compliance costs may rise in the short term, they significantly reduce the likelihood of crypto entities being exposed to uncontrollable financial risks in the long run.

Driving Web3 Compliance and Trust with Data

Bitrace is a Regtech company specializing in cryptocurrency risk data analysis. We are dedicated to utilizing AI and big data technologies to more accurately and efficiently identify, monitor, and investigate risks and criminal activities on the blockchain. Our mission is to provide customers with leading regulatory, compliance, and investigative tools and services.

We have collaborated and interfaced with LEs and Web3 enterprises in multiple countries, completing 1000+ case services, monitoring 700B+ USD in risk/criminal funds, and successfully recovering 1B+ USD in losses.

Contact us

Website: bitrace.io
Email: bd@bitrace.io
Twitter: @Bitrace_team
LinkedIn: @Bitrace Tech
Telegram: @BitraceBD