BLOCKSEC

# 2025 Crypto Crime Report

# CONTENTS

# Executive Summary

In 2025, cryptocurrency-related crime did not follow a single trajectory. Instead, it revealed a structural pattern: diversification at the generation stage and concentration at key financial aggregation points.

Across Ethereum and TRON, illicit proceeds originated from multiple crime types—including scams, hacks, drug trafficking, terrorist financing, human trafficking, and sanctions-related activity. While revenue generation mechanisms differed, laundering outcomes consistently converged toward a limited number of centralized liquidity hubs.

This concentration at the aggregation stage defines the primary enforcement leverage point: structural chokepoints where illicit funds consolidate and seek monetization.

Stablecoins emerged as a central variable in this landscape. Major centralized issuers functioned not merely as payment providers, but as enforceable regulatory interfaces capable of executing sanctions and law enforcement actions directly at the contract level.

In 2025, the scale of freezing activity underscored a structural shift—stablecoins increasingly operated as governance infrastructure rather than passive transactional tools.

Regional analysis further demonstrated adaptive resilience within illicit ecosystems. In Southeast Asia, organized scam compounds and labor brokerage platforms operated as industrialized systems supported by stablecoin-based settlement networks. Under sustained enforcement pressure, these networks restructured, migrated, and fragmented rather than disappeared.

Drug trafficking networks likewise exhibited structural financialization. Cryptocurrency—particularly stablecoins—became embedded within layered laundering architectures featuring role specialization and standardized on-chain workflows. Whether internally integrated or outsourced to specialized service providers, capital flows ultimately converged toward identifiable liquidity gateways.

Cryptocurrency-related crime in 2025 was therefore defined less by expansion in volume than by consolidation of financial infrastructure. Surface-level diversification persisted, but systemic dependence on stablecoin rails, centralized exchanges, and intermediary nodes remained intact. Effective disruption depends on identifying and constraining these structural concentration points rather than isolating individual transactions.

# Major Cryptocurrency Crime Trends in 2025

## Scope of Research

This report examines cryptocurrency-related criminal activity observed in 2025 across two primary blockchain networks: Ethereum and TRON. These networks were selected based on transaction scale, ecosystem adoption, and consistent involvement in illicit fund flows.

Ethereum and TRON occupy distinct but complementary roles within the illicit economy. Ethereum functions as a core environment for native on-chain applications and complex financial operations, while TRON operates as a primary settlement layer for stablecoin transfers and cross-border value movement. Together, they constitute the principal infrastructure through which illicit funds are generated, transferred, and laundered.

The analysis covers six major crime categories: scams; hacks and exploits; terrorist financing; human trafficking; drug trafficking; and sanctions-related activity. These typologies represent the most prevalent and operationally significant forms of cryptocurrency-enabled crime in 2025.

# Methodology

This analysis addresses two central questions:

1.How much illicit revenue was generated by each crime category in 2025?

2.Where did those funds ultimately flow during the laundering process?

## Estimating Illicit Revenue by Crime Category

Annual revenue is estimated by tracking on-chain inflows to addresses associated with identified illicit activity. Using the BlockSec AML labeling database, addresses are grouped by crime category, and inflows of major cryptoassets received during 2025 are aggregated and converted into U.S. dollar equivalents for comparability.

Several considerations apply:

• Not all illicit addresses are publicly identified or promptly labeled; actual volumes may therefore exceed reported figures.

• Internal transfers among related illicit addresses may introduce double counting. Where feasible, analysis mitigates this effect—for example, by using individual attack incidents as the primary unit of measurement within the hacks and exploits category.

• Some addresses are associated with multiple illicit typologies. While each address is assigned a primary classification where possible, overlap remains unavoidable in certain cases, particularly between general illicit activity and sanctions-related designations. The Lazarus Group represents a prominent example.

## Analyzing Laundering Destinations

Laundering patterns are analyzed using a fund flow modeling framework adapted from MFTracer. Rather than assessing addresses individually, all addresses associated with a given crime category are aggregated into a single analytical cluster. Outbound flows are then simulated at the cluster level to trace downstream movement.

Funds are followed until they reach identified service entities—such as exchanges, bridges, or other intermediaries—or converge at highly connected aggregation nodes. This cluster-level modeling captures coordinated activity across distributed address sets while reducing repeated attribution of downstream destinations.

As with any large-scale on-chain analysis, limitations apply:
• Automated simulations employ pruning strategies for computational feasibility, which may result in minor flow exclusions.

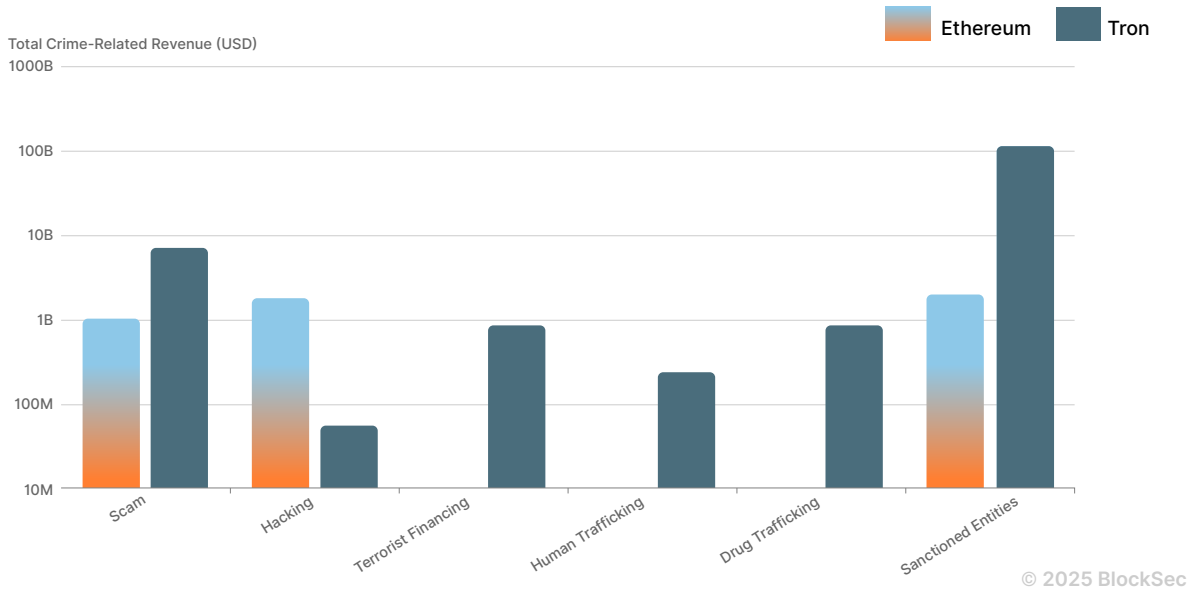
• Destination attribution depends on the BlockSec AML labeling database; flows entering unlabeled entities cannot always be further classified.

• Some service providers operate multiple business functions. In such cases, inflows are categorized under the entity's primary business type, which may introduce limited classification imprecision.

## Revenue by Crime Type

The figure below presents the distribution of illicit revenue across Ethereum and TRON in 2025 by crime category. Categories with negligible revenue on a given chain are displayed as zero to preserve scale clarity.

▸ **Crime-Related Revenue by Crime Type and Blockchain**



Terrorist financing, human trafficking, and drug trafficking revenue is overwhelmingly concentrated on TRON. These activities primarily depend on cryptocurrency for settlement and cross-border value transfer, making TRON's low transaction costs and operational efficiency structurally advantageous.

Scams and hacks, by contrast, generate substantial revenue on both networks. These crimes are more chain-native in nature: illicit proceeds typically emerge within the ecosystem where the underlying activity occurs. Hack-related revenue is materially higher on Ethereum, reflecting both its active DeFi environment—an ongoing target for smart contract exploitation—and the outsized impact of the Lazarus Group's 2025 attack on Bybit, which involved approximately $1.5 billion in ETH.

Sanctions-related activity increased sharply in 2025, with associated revenue rising by nearly $100 billion year-over-year. Two drivers account for most of this growth. First, the launch of the ruble-denominated stablecoin A7A5—reportedly designed to facilitate transactions outside traditional sanctions channels—generated approximately $70 billion in transaction volume across Ethereum and TRON. Second, entities such as Huione Group and BYEX Exchange were sanctioned for involvement in Southeast Asian scam and laundering networks, and their related flows were incorporated into sanctions totals.

Overall, revenue distribution reflects structural differences in blockchain selection. Settlement-oriented crimes gravitate toward low-cost, high-throughput networks, while chain-native offenses remain anchored to their originating ecosystems. These dynamics provide context for subsequent analysis of laundering pathways, concentration patterns, and regional illicit systems.

## Laundering Destinations by Crime Type

This section examines how illicit proceeds move across Ethereum and TRON during the laundering phase, focusing on the service entities that ultimately receive those funds.

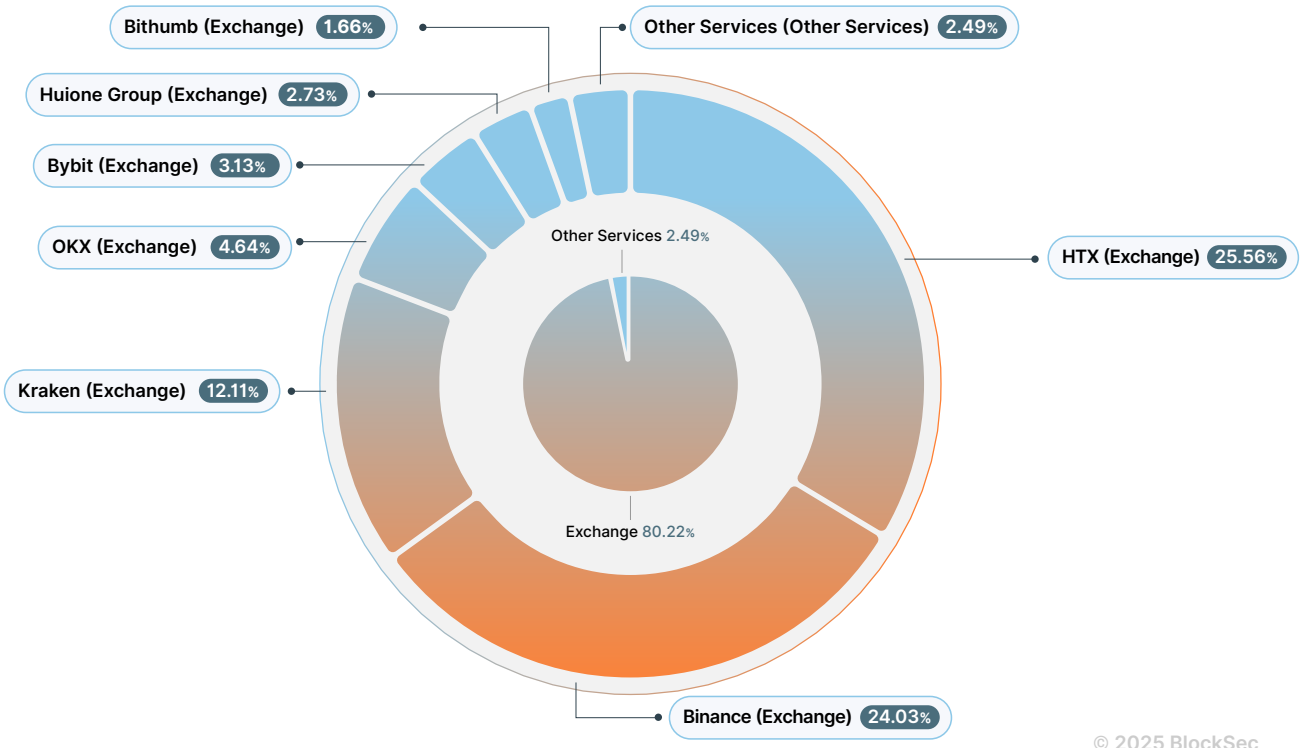
Sanctions-related activity is excluded from downstream destination analysis. Because sanctions designations encompass entities involved in diverse underlying conduct, aggregating all sanctioned addresses into a single typology would obscure meaningful distinctions in laundering behavior. Sanctions-related flows are therefore assessed in aggregate volume, but excluded from category-level pathway comparisons.

### Scams

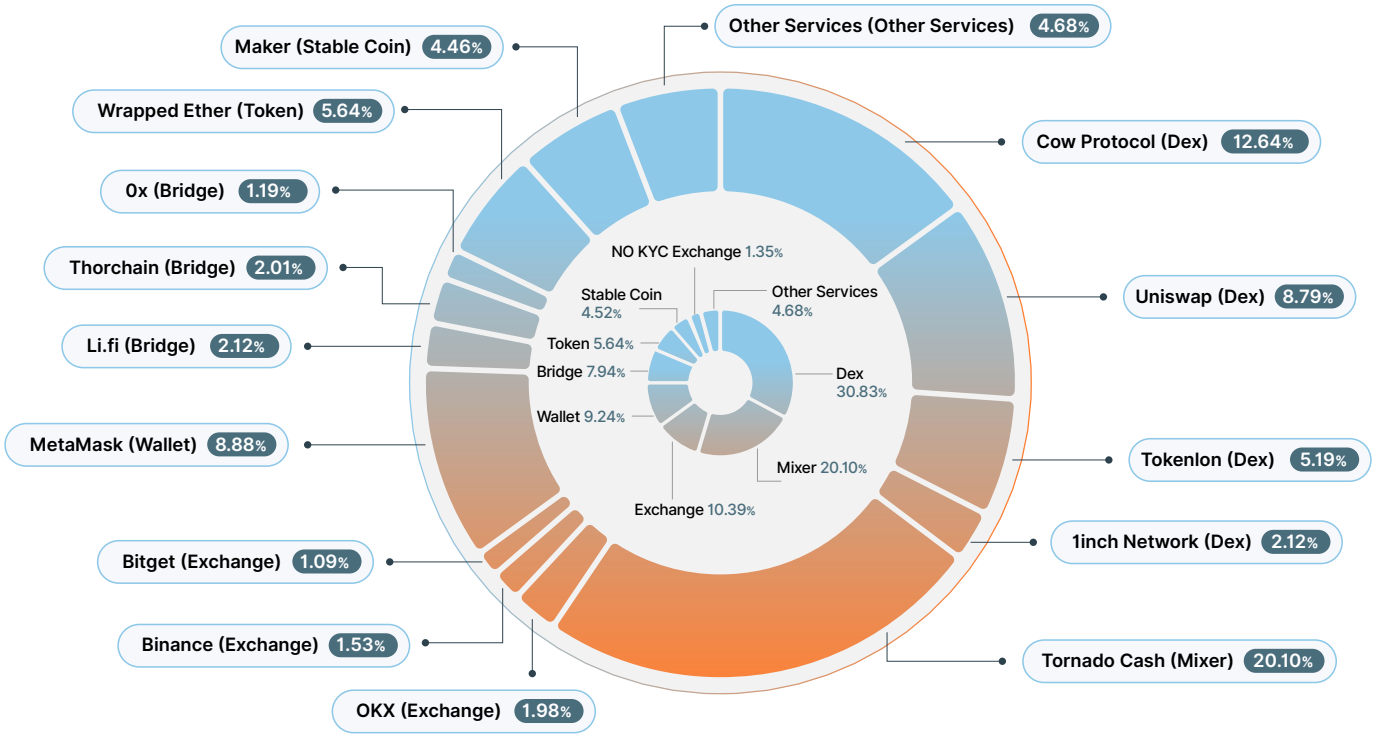
On TRON, scam proceeds follow a highly concentrated laundering pattern. More than 80% of outflows ultimately reach centralized exchanges.

HTX and Binance together account for roughly half of total flows, followed by Kraken, OKX, and Bybit. Huione Group represents approximately 2.73% of scam-related flows on TRON—consistent with FinCEN's designation of the entity as a key laundering node within Southeast Asian scam networks.

Outside exchanges and a small number of prominent entities, other service categories account for minimal volume. The structure is clear: scam operations on TRON prioritize rapid monetization, with centralized exchanges functioning as the dominant exit layer.



By contrast, Ethereum exhibits a markedly more diversified laundering structure. Decentralized exchanges (DEXs) account for roughly 30% of outflows but do not dominate the landscape. Mixer usage is substantially higher than on TRON, representing approximately 20% of flows, with Tornado Cash as the primary destination. Additional funds move through centralized exchanges, wallet services, cross-chain bridges, and stablecoin protocols, producing a more layered, tool-driven laundering architecture.



This divergence is rooted in asset composition and ecosystem design. On TRON, scam proceeds are overwhelmingly denominated in USDT, providing immediate liquidity and reducing the need for intermediate conversion. On Ethereum, proceeds are more heterogeneous, requiring consolidation and asset conversion before advancing through later-stage laundering steps—a dynamic examined further in Chapter 2.

Operational preferences also differ. On TRON, funds typically pass through multiple intermediary addresses before converging at exchanges for liquidation. On Ethereum, actors more frequently leverage the network's broader infrastructure—including mixers and DeFi mechanisms—to construct multi-stage obfuscation paths.

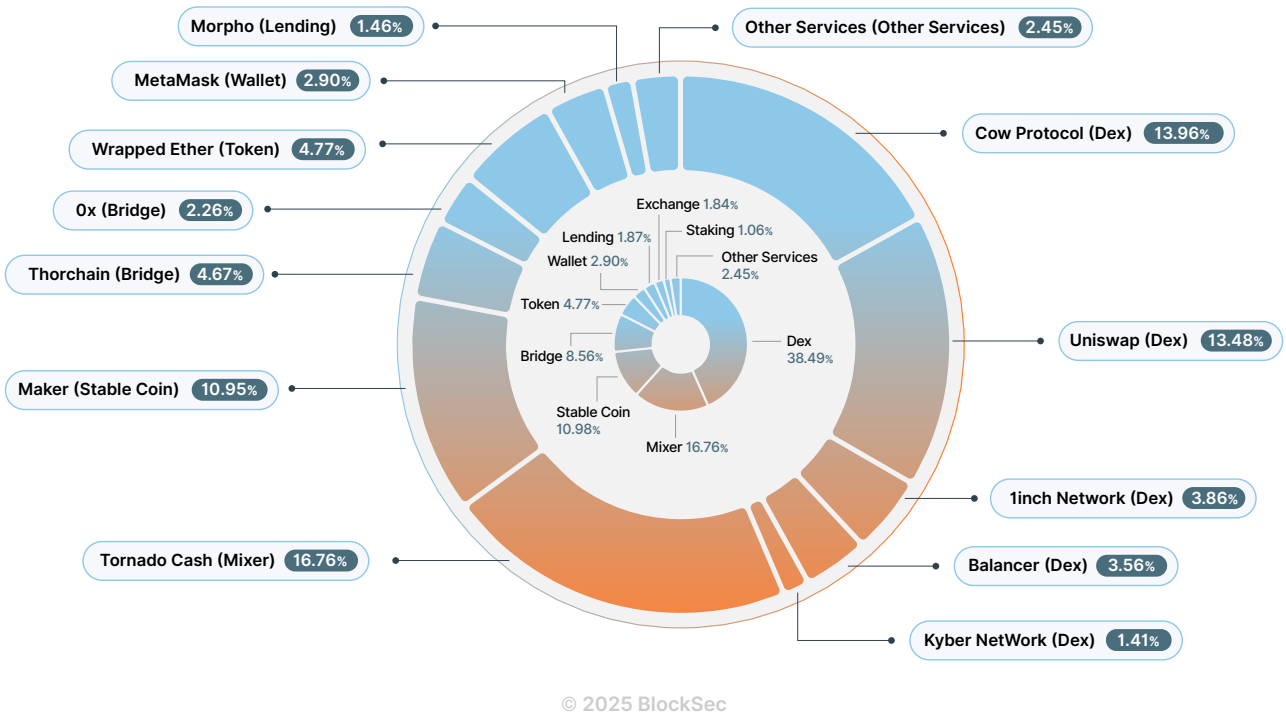
Taken together, scam-related laundering behavior demonstrates how ecosystem structure shapes illicit financial strategy. TRON reflects an exchange-centric liquidation model, while Ethereum enables layered, tool-based obfuscation. Despite these structural differences, the objective remains constant: minimize traceability while maximizing liquidity and exit efficiency.

## Hacks and Exploits

Before examining laundering destinations for hack-related proceeds, one clarification is necessary: flows attributed to the Lazarus Group are excluded from this section.

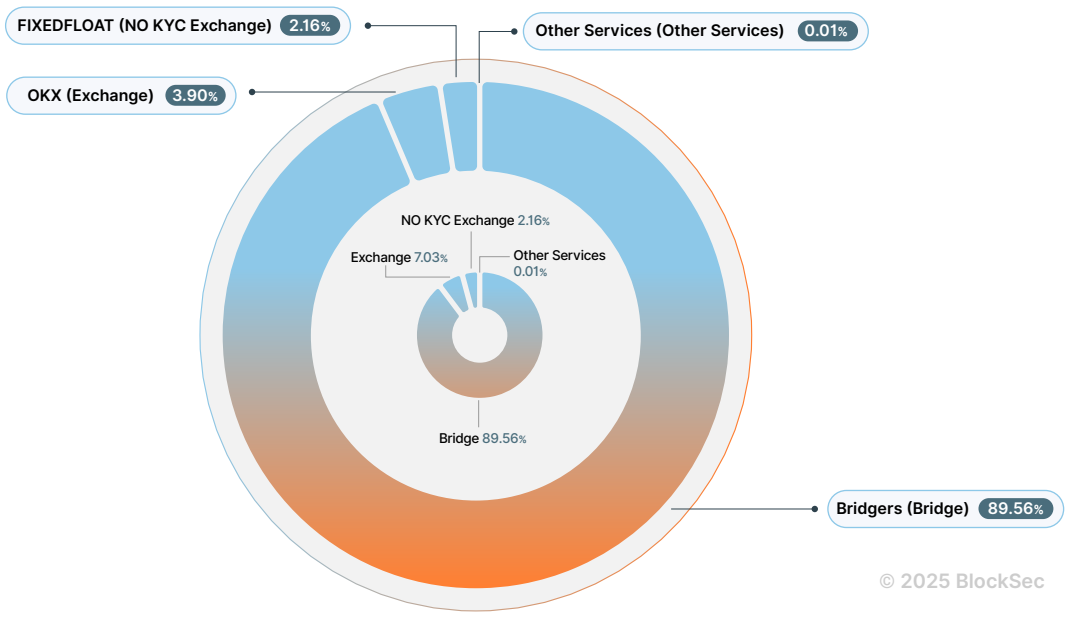
Given the scale of Lazarus-linked activity in 2025, inclusion would materially distort distributional patterns. Lazarus activity is therefore analyzed separately to preserve visibility into broader network-level dynamics.

On Ethereum, hack-related proceeds follow a highly diversified laundering structure. Decentralized exchanges account for 38.49% of outflows, primarily routed through Uniswap, Cow Protocol, 1inch, Balancer, and Kyber Network. Mixer usage represents 16.76% of flows, with Tornado Cash as the principal destination. Additional funds pass through cross-chain bridges, stablecoin protocols, wallet services, and lending platforms, reflecting a layered, multi-tool laundering architecture designed to increase obfuscation and tracing complexity.



By contrast, hack-related flows on TRON are overwhelmingly concentrated in cross-chain bridges. Approximately 90% of proceeds are routed through bridge services, predominantly via Bridgers. Outside of bridge activity, only marginal volumes reach centralized exchanges or no-KYC services.

The strategic contrast is clear. On TRON, attackers prioritize rapid network migration, transferring funds to external environments for subsequent laundering rather than constructing complex in-network pathways. Ethereum, by comparison, enables layered, infrastructure-intensive obfuscation within the ecosystem itself.

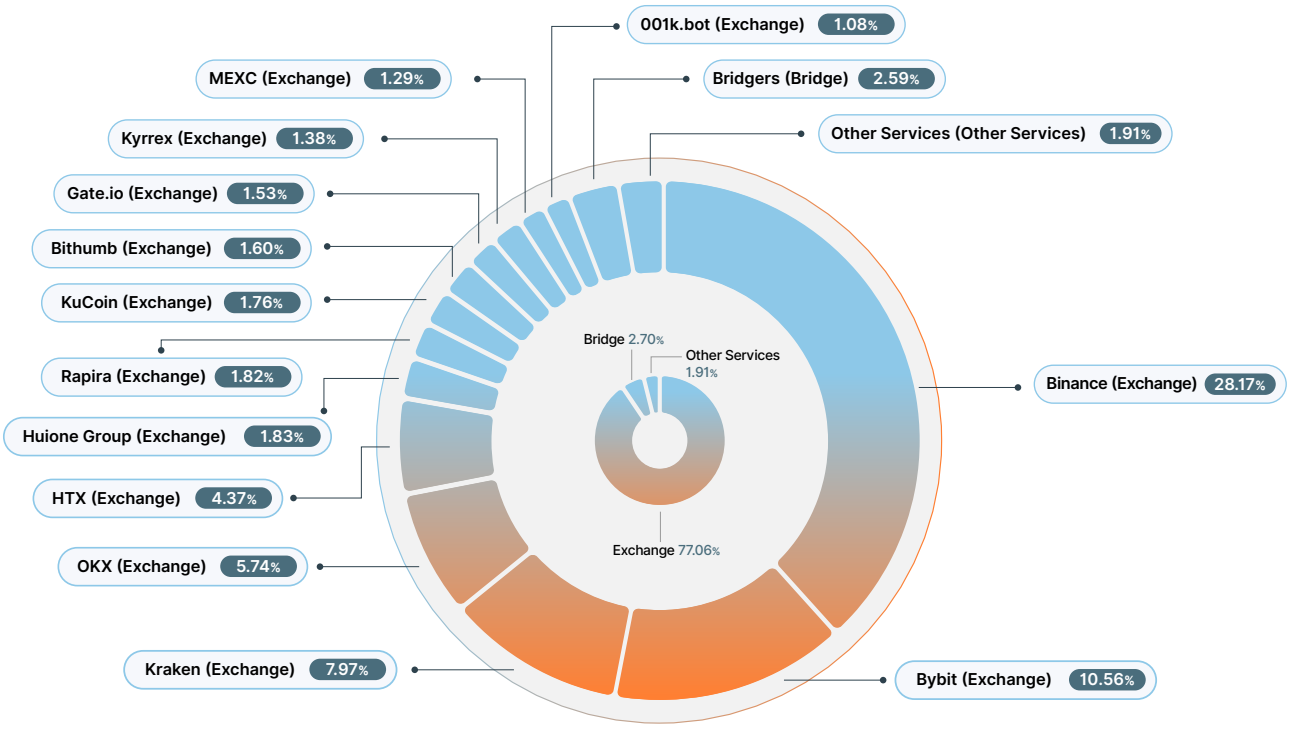



Taken together, hack-related patterns highlight a functional division of roles: Ethereum operates as an obfuscation-rich execution environment, while TRON functions primarily as a cross-chain transit layer.

## Terrorist Financing

Terrorist-financing activity observed in 2025 was overwhelmingly concentrated on TRON. Accordingly, laundering destination analysis in this section focuses exclusively on TRON-based flows.

Centralized exchanges function as the primary exit channel, accounting for 77.06% of outflows. Binance represents the single largest destination at 28.17%, followed by Bybit, Kraken, and OKX. Only 2.7% of funds are routed through cross-chain bridges—a markedly lower share than observed in hack-related activity.



While aggregation at the receiving stage is pronounced, transaction pathways themselves tend to be longer and more fragmented. Prior to reaching identified service entities, funds frequently traverse multiple intermediary addresses, requiring deeper tracing layers to establish final attribution.

This structure reflects a laundering strategy that prioritizes path elongation over tool diversification or cross-chain dispersion. Rather than increasing infrastructural complexity, actors appear to mitigate exposure risk by extending transaction chains before convergence.

### Human Trafficking

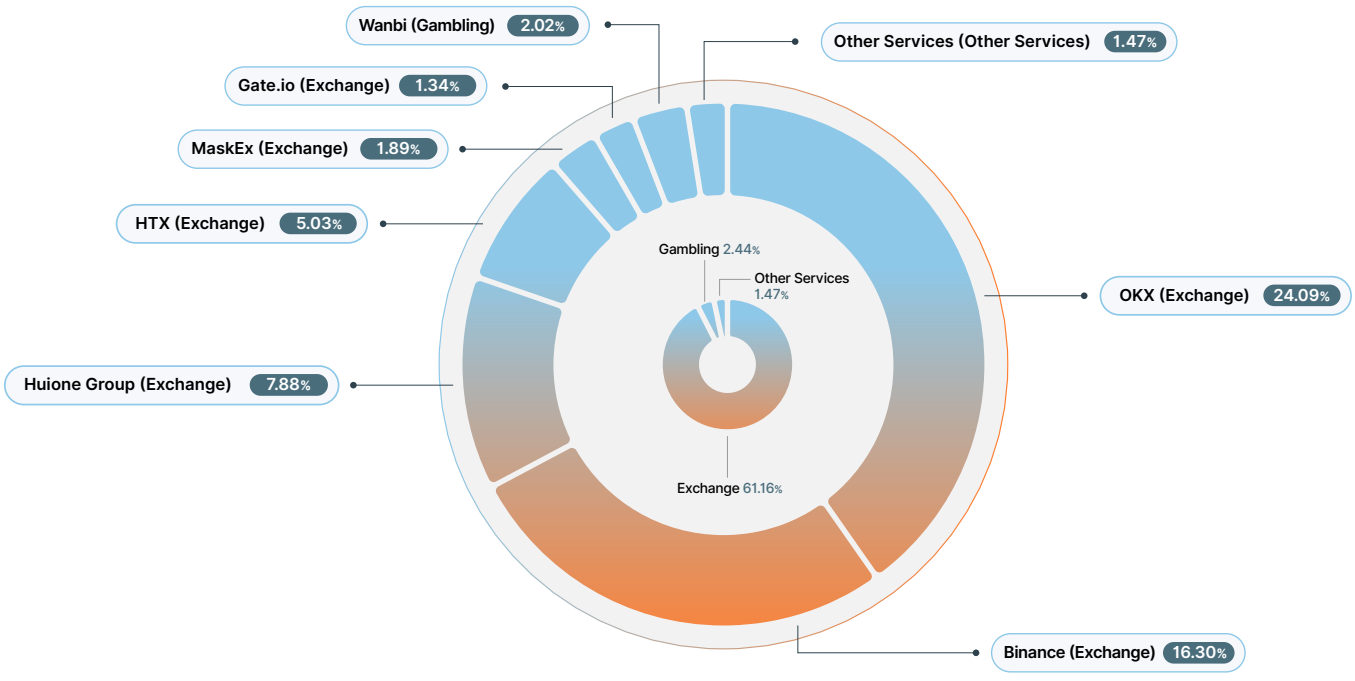
Human trafficking–related illicit funds are likewise heavily concentrated on TRON. The laundering analysis presented here therefore focuses on TRON-based flows.

Centralized exchanges constitute the primary exit channel, accounting for more than 60% of total outflows. Funds are distributed across multiple platforms, with OKX, Binance, and Huione Group representing the most significant destinations. Additional volumes flow to exchanges such as HTX, MaskEx, and Gate.io, though the overall structure remains centered on centralized exchange infrastructure.

A smaller share of funds is directed to gambling-related services. While limited in proportion, this channel is structurally noteworthy.

Its presence suggests an intermediate laundering layer in which funds circulate through high-liquidity transactional environments before converging on mainstream exchange-based exit points, potentially reducing attribution clarity.

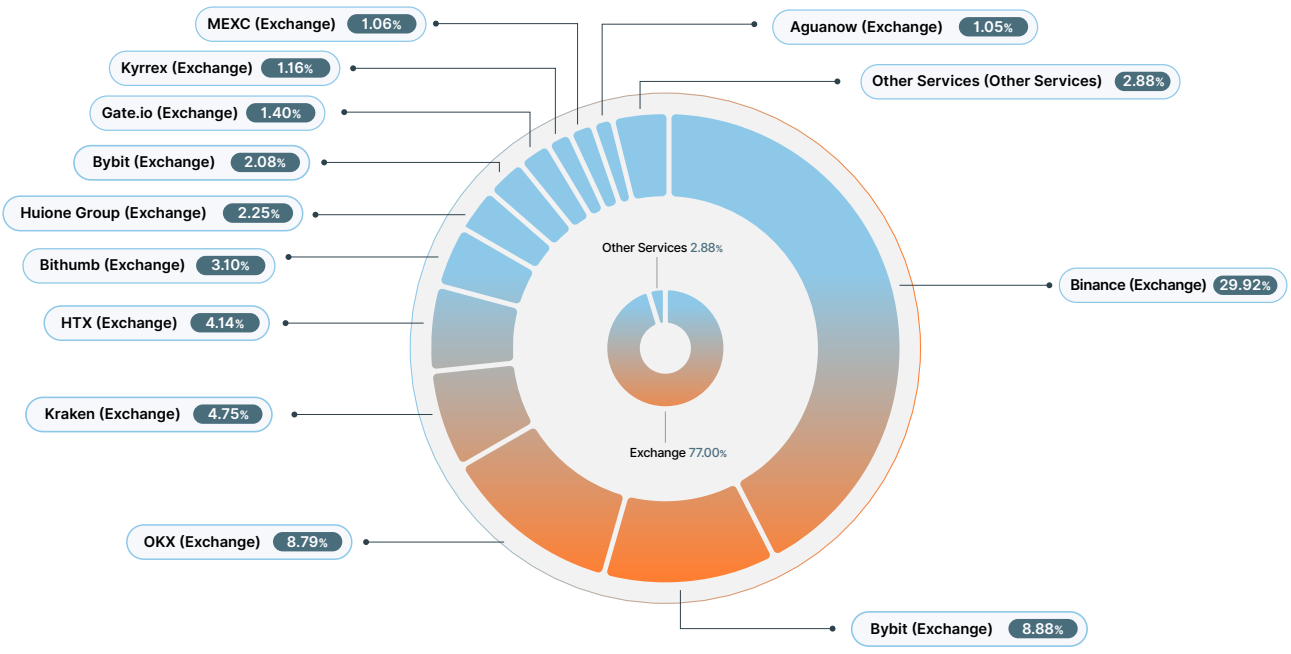
Taken together, human trafficking–related laundering activity remains predominantly exchange-centric, with only modest diversification beyond centralized liquidity hubs.



## Drug Trafficking

Drug trafficking–related illicit funds are likewise heavily concentrated on TRON, and the analysis presented here focuses on TRON-based flows.

Centralized exchanges remain the dominant exit channel. Approximately 77% of drug-related proceeds ultimately flow into exchanges, with Binance accounting for the largest share, followed by Bybit, OKX, and other major platforms. Despite multiple layers of on-chain transfers, exchanges continue to serve as the principal gateway through which drug-related proceeds enter the broader financial system.



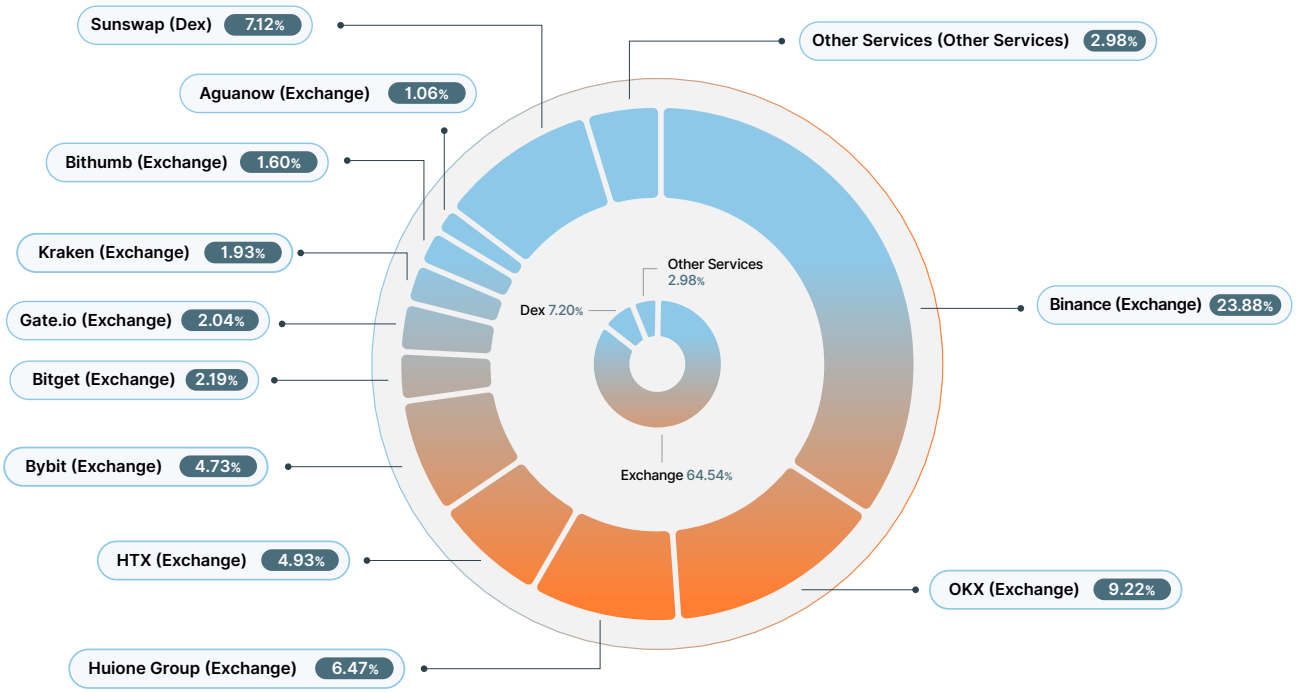
Relative to scams and hacks, drug-trafficking flows require deeper tracing layers before reaching identified service entities. Transaction chains are typically longer, involving a greater number of intermediary hops prior to exchange deposit. Funds undergo more extensive layering before converging at centralized liquidity hubs.

This configuration—highly concentrated exit points combined with elongated transaction paths—reflects a more mature and operationally risk-aware laundering model.

### Lazarus Group

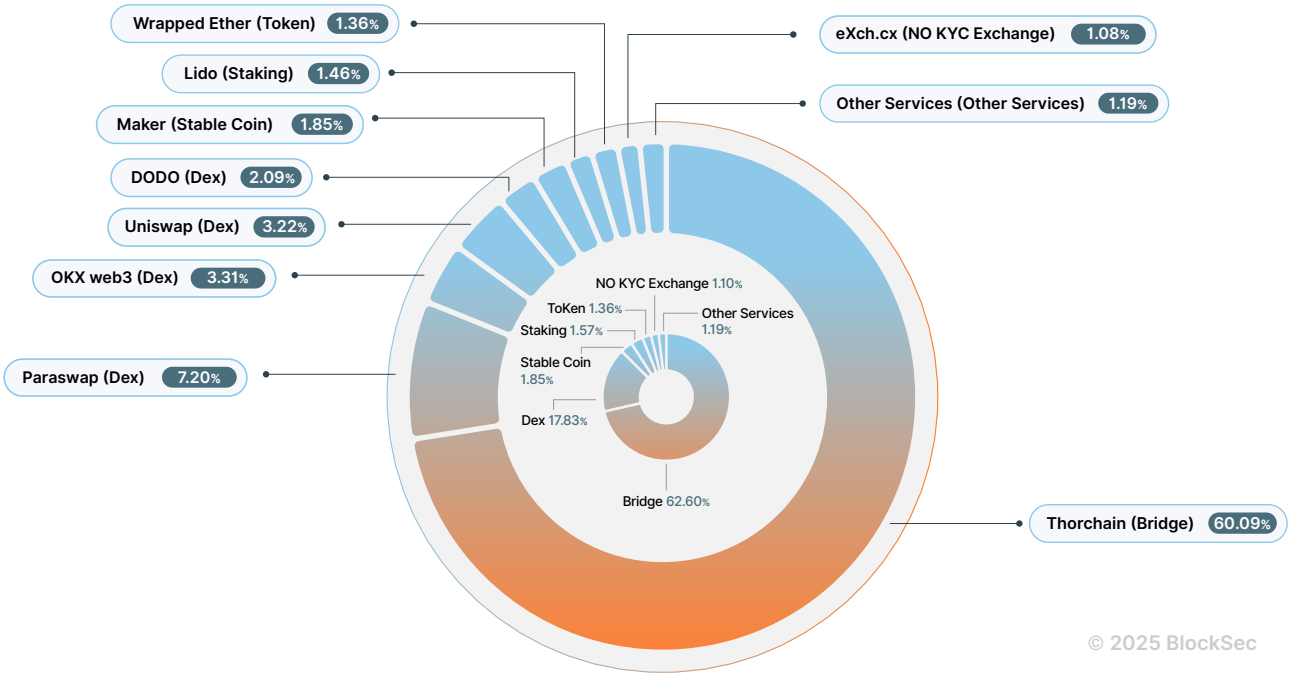
Lazarus Group was among the most consequential hack-related actors in 2025. Given the scale of its operations and their material impact on aggregate flow distributions, Lazarus-linked activity is analyzed separately to preserve structural clarity.

On TRON, Lazarus-associated funds are heavily concentrated in centralized exchanges. More than 60% of outflows ultimately reach exchange platforms, with Binance, OKX, Huione Group, and HTX representing the principal destinations. Activity outside exchanges remains limited.




On Ethereum, by contrast, flows follow a distinctly different configuration. Cross-chain bridges serve as the primary routing mechanism, with Thorchain functioning as the dominant outbound channel. Portions of funds are also routed through decentralized exchanges—including Paraswap, Uniswap, and OKX Web3—for asset conversion, while smaller volumes move into stablecoin protocols, staking services, and no-KYC trading platforms.

Ethereum-based laundering therefore emphasizes cross-chain migration and coordinated tool usage, producing significantly greater structural complexity than observed on TRON.




Taken together, Lazarus activity underscores a functional division of roles between networks: TRON operates as an exchange-centric consolidation layer, while Ethereum functions as the primary execution environment for cross-chain transfer and multi-stage operational sequencing.

## Key Findings

Laundering behavior in 2025 does not follow a uniform pattern across crime types. Distinct structural differences emerge in pathway design, tool usage, and network selection, reflecting adaptation to the functional characteristics of each blockchain ecosystem.

Scam-related activity centers on efficiency and monetization. On TRON, proceeds converge rapidly at centralized exchanges through relatively direct pathways. On Ethereum, structures are more diversified, with greater reliance on decentralized exchanges, mixers, and multi-stage asset conversion prior to exit.

Hack-related activity demonstrates more pronounced technical orchestration. Ethereum-based exploit proceeds move through layered combinations of decentralized exchanges, mixers, and cross-chain bridges, while TRON-based flows concentrate in bridge infrastructure to enable rapid network migration. High-impact exploit actors materially shape aggregate distributions and therefore warrant separate treatment.

Terrorist financing remains highly concentrated at centralized exchanges and is primarily observed on TRON. Transaction chains, however, tend to be longer, suggesting a preference for path elongation over infrastructural complexity as a means of mitigating exposure risk.

Human trafficking reflects relatively direct laundering structures centered on TRON and exchanges, with a limited but structurally relevant role for gambling services as transitional layers prior to exit.

Drug trafficking similarly converges on exchanges within TRON but is distinguished by deeper layering and longer transaction paths before deposit, indicating a comparatively mature laundering model.

The separate analysis of Lazarus Group reinforces the functional differentiation between networks: TRON operates as an exchange-centric consolidation layer, while Ethereum functions as a core execution environment for cross-chain transfers and multi-stage sequencing.

Overall, laundering in 2025 reflects diversification at the pathway level alongside persistent concentration at critical liquidity nodes. These structural dynamics provide a basis for identifying risk concentration points and frame subsequent analysis of enforcement leverage and ecosystem dependency.

# Risk Concentration and Enforcement Leverage

## Primary Sources of Illicit Proceeds

When evaluating cryptocurrency-related crime, total fund volume alone does not capture enforcement risk. Equally important is the distribution of proceeds—whether revenue is dispersed across many actors or concentrated among a limited set of high-impact entities.

Among distinct underlying crime types, scams and hacks remained the two largest sources of illicit proceeds in 2025. However, their concentration dynamics at the generation stage differ substantially.

Scam-related activity reflects a dual structure. A dispersed base of individuals and small groups contributes to aggregate volume, creating a fragmented threat landscape. At the same time, a smaller number of highly organized—often regionally concentrated—networks generate disproportionate proceeds. These actors function as structural hubs within the scam ecosystem and represent critical disruption points. Their operational models and geographic clustering are examined in later sections.

Hack-related activity, by contrast, exhibits pronounced revenue asymmetry. Although incident frequency remains high, aggregate proceeds are driven by a limited number of large-scale exploits. In some cases, a single event materially shapes annual category totals. Value generation in the hack domain is therefore concentrated among technically sophisticated, organizationally capable actors.

Concentration at the generation stage thus varies by crime type. Scam activity combines dispersion with selective concentration, whereas hack-related crime is dominated by event-level and actor-level asymmetry. Enforcement leverage follows accordingly: disruption of organized scam networks may generate ecosystem-wide effects, while in the hack domain, monitoring and rapid response to high-capability actors yields disproportionate impact.

## Concentration of Illicit Funds at the Laundering Stage

Risk concentration becomes more pronounced during laundering. Beyond identifying who generates illicit proceeds, it is critical to assess where those funds ultimately converge.

Despite variation in tool usage, cross-chain movement, and operational complexity, end-state aggregation is remarkably consistent. Centralized exchanges repeatedly function as primary consolidation hubs across scams, hacks, terrorist financing, and human trafficking.

Intermediate services—decentralized exchanges, bridges, and other on-chain infrastructure—primarily operate as transitional layers rather than final destinations. Following asset conversion or network migration, funds typically converge on exchange-based liquidity nodes.

This convergence indicates that greater technical sophistication does not meaningfully disperse systemic risk. Even with layered routing strategies, illicit funds remain structurally dependent on a limited set of intermediary nodes for consolidation and monetization. The receiving stage therefore represents the most stable and scalable point of enforcement leverage within the illicit ecosystem.

## Enforcement Implications

Taken together, cryptocurrency-related crime in 2025 reflects a persistent structural asymmetry: diversification at the generation stage and concentration at aggregation.

While concentration mechanisms differ at the source—from organized scam networks to high-impact exploit events—convergence at the receiving end is consistent. A limited set of service providers functions as liquidity gateways through which illicit proceeds ultimately pass.

Effective enforcement therefore depends less on tracking volume and more on identifying structural chokepoints. Leverage exists both in disrupting high-capability generators and in strengthening oversight of key receiving and transit nodes. Targeted intervention at these concentration points offers the potential for disproportionate systemic impact under constrained resources.

# Stablecoins as Enforceable Regulatory Infrastructure

As the cryptocurrency ecosystem has matured, stablecoins have evolved from payment and settlement instruments into a key interface between on-chain activity and regulatory authority. Unlike most cryptoassets, major stablecoins are issued and managed by centralized entities operating within established legal and compliance frameworks.

This design enables regulatory and enforcement actions to be executed directly at the protocol level.

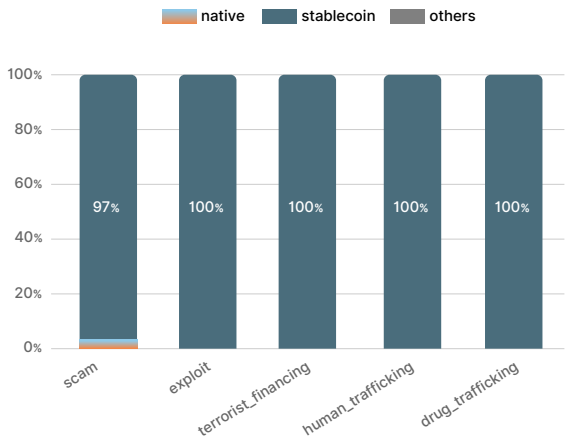
In practice, issuers can freeze addresses, restrict transfers, and conduct compliance interventions that materially alter the status of specific on-chain accounts. Sanctions designations and law enforcement requests are therefore no longer confined to exchanges or traditional financial intermediaries; they can be implemented directly within smart contract infrastructure.

This chapter examines how stablecoins have become an enforceable layer within digital asset markets and evaluates their implications for cryptocurrency crime governance.

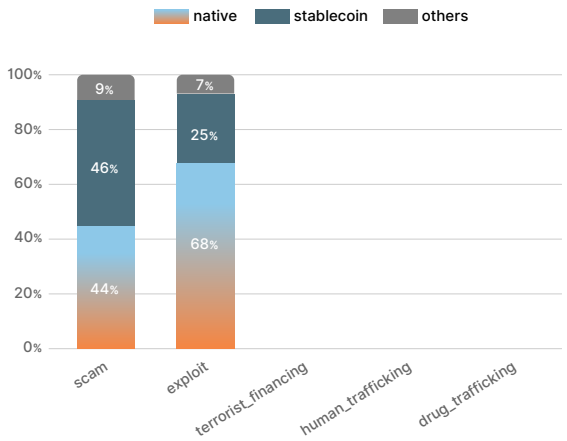
# The Central Role of Stablecoins in Illicit Activity

To assess stablecoin usage in illicit markets, revenue across crime types was analyzed by asset composition on Ethereum and TRON. Annual proceeds were categorized into native tokens, stablecoins, and other token types. Asset breakdowns were omitted where volumes fell below analytical thresholds.

▶ Revenue Asset Mix (Normalized) - TRON




▶ Revenue Asset Mix (Normalized) - ETH






Stablecoins now account for a substantial share of illicit revenue across networks, though concentration varies by ecosystem.

On TRON, revenue across nearly all analyzed crime types is overwhelmingly denominated in stablecoins, with shares approaching or reaching 100% in most categories. Illicit activity within the TRON ecosystem is therefore highly stablecoin-centric at the point of generation, with stablecoins functioning as the primary value layer rather than as transitional instruments.

On Ethereum, asset composition is more diversified. Native tokens retain relevance—particularly in exploit-related activity—yet stablecoins maintain a significant share across major crime types. Even within a more complex financial environment, stablecoins remain central to value storage and transfer in illicit operations.

Across both networks, stablecoins have become a structural component of illicit financial activity rather than a peripheral payment tool. This shift provides essential context for evaluating their enforcement potential and informs the subsequent analysis of freezing mechanisms and compliance interventions.

## Stablecoin Freezing Mechanisms: From Contract Privilege to Regulatory Execution

For centralized stablecoins, controllability is a defining architectural feature. To support compliance and law enforcement cooperation, stablecoin contracts embed privileged functions that allow issuers to manage supply and circulation. These controls also create a direct enforcement interface at the protocol level.

Using Tether's USDT on Ethereum and TRON as a case study, this section outlines the core contract mechanisms and their operational implications.

## Core Contract-Level Controls

The USDT contract includes three functions callable only by privileged addresses:

• **addBlackList:** Designates an address as frozen. The address can neither send nor receive USDT, rendering the balance non-transferable while remaining visible on-chain.
• **removeBlackList:** Restores transfer functionality to a previously frozen address.
• **destroyBlackFunds:** Permanently burns USDT held by a frozen address, reducing total supply.

Together, these controls form a graduated enforcement framework—from liquidity restriction to permanent asset removal—implemented directly at the contract layer without reliance on custodial intermediaries.

## Pathways to Freezing

Although Tether does not publish a comprehensive freezing policy, public disclosures and observable on-chain activity indicate three primary triggers.

### 1.Law Enforcement Requests

The most common pathway involves verified requests from law enforcement agencies. Authorities—including the FBI, U.S. Department of Justice, Secret Service, DEA, Europol, and over 275 partner agencies across 59 jurisdictions—may request freezes upon identifying suspect wallets.

Formal court orders are not always required; requests submitted through official channels and supported by legal justification may suffice. In urgent cases, temporary freezes may precede formal documentation. Public reporting indicates that more than 900 law enforcement requests have been processed in the past three years, including approximately 460 from U.S. authorities.

**2.Automated Sanctions Compliance**

Beginning in December 2023, Tether implemented proactive freezing of addresses listed on OFAC's SDN list without case-specific requests. Upon activation, 161 SDN-listed addresses were immediately frozen. This shift represents a transition from reactive, case-based enforcement to rule-driven, automated sanctions execution.

**3.Intelligence-Led Proactive Freezing**

Through cooperation with blockchain intelligence initiatives—most notably the T3 Financial Crime Unit (established in 2024 by TRON and TRM Labs)—Tether may freeze addresses linked to hacks, scams, or terrorist financing based on investigative findings, at times preceding formal enforcement requests. As of October 2025, T3-assisted actions had resulted in the freezing of more than $300 million in illicit assets across 23 jurisdictions.

### Freezing vs. Seizure

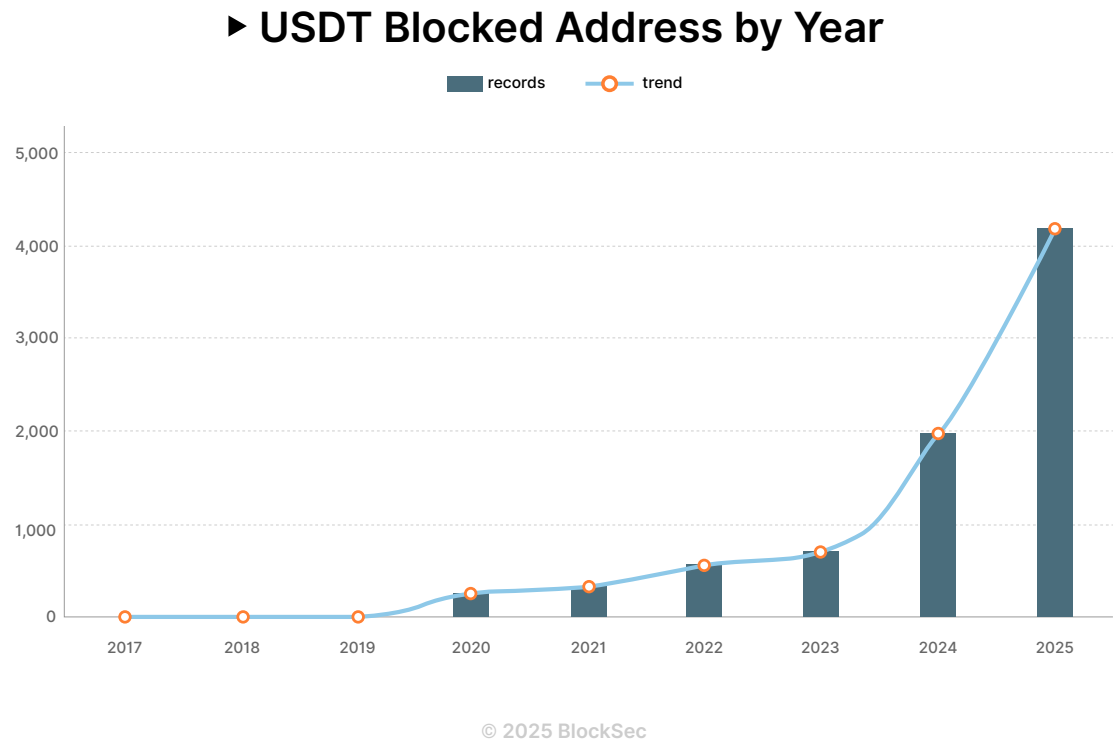
Freezing and seizure differ materially at both legal and technical levels.

A freeze, executed via addBlackList, temporarily restricts transferability and does not itself constitute asset confiscation.

A seizure occurs when destroyBlackFunds is invoked, permanently burning the frozen USDT and reissuing an equivalent amount to a government-controlled wallet. This destroy-and-reissue process typically follows civil asset forfeiture procedures and requires judicial authorization, representing formal transfer of control.

## The Scaled Execution of USDT Freezing

Stablecoin freezing has evolved from sporadic case-based intervention into a normalized enforcement mechanism. Since 2017, the number of USDT-linked addresses added to blacklists has risen steadily, accelerating in the past two years. Freezing authority has transitioned from exceptional use to routine operational practice.

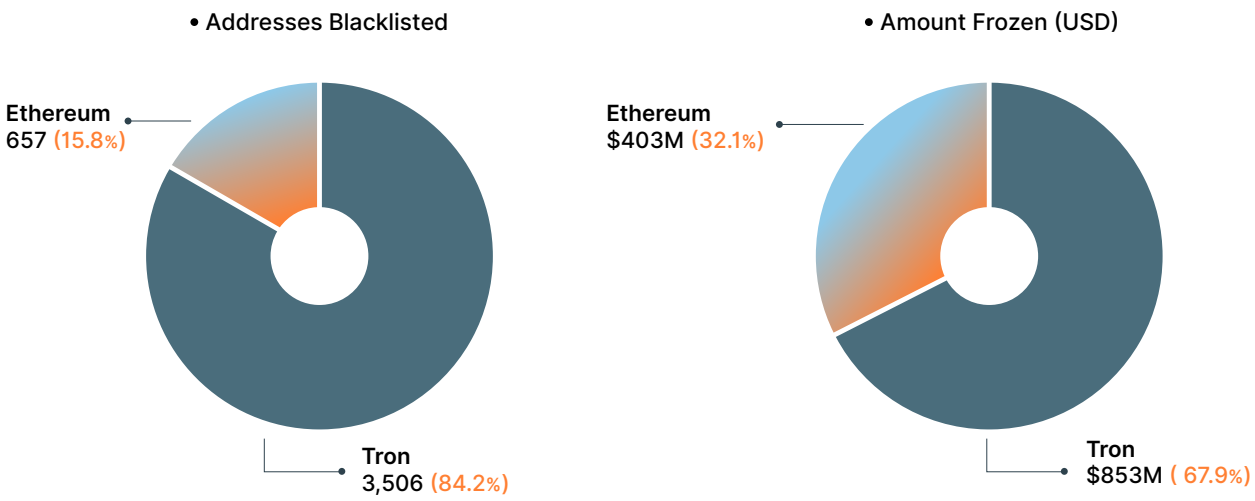



In 2025 alone, Tether blacklisted 4,163 addresses, freezing approximately $1.26 billion in USDT. More than half—roughly $698 million—was subsequently destroyed. Under Tether's framework, destroyed funds are typically reissued to victims or transferred to law enforcement-controlled wallets, completing formal asset takeover.

Network distribution reveals meaningful asymmetry. TRON accounted for more than five times as many frozen addresses as Ethereum, with correspondingly higher aggregate volume.

Ethereum, however, exhibited higher average balances per frozen address. These patterns mirror broader ecosystem dynamics: TRON is associated with high-frequency, high-volume flows, while Ethereum more commonly hosts larger, structurally complex transactions.

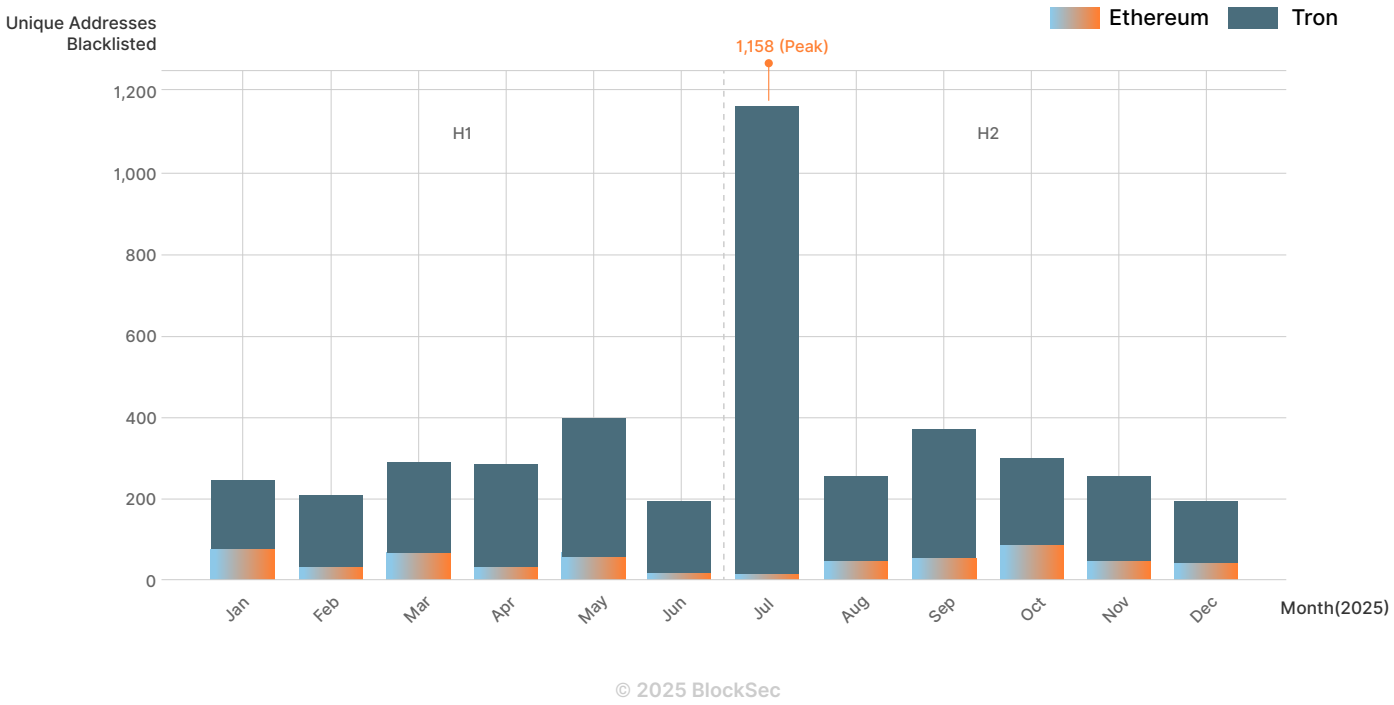
### ▸ USDT Blacklist 2025: Chain Distribution






Freezing activity in 2025 unfolded in waves rather than evenly across the year, with July marking a peak in both address count and volume. This episodic clustering aligns with external enforcement actions, indicating increasing synchronization between issuer execution and regulatory operations.

▶ **Monthly USDT Blacklisted Addresses by Chain (2025)**

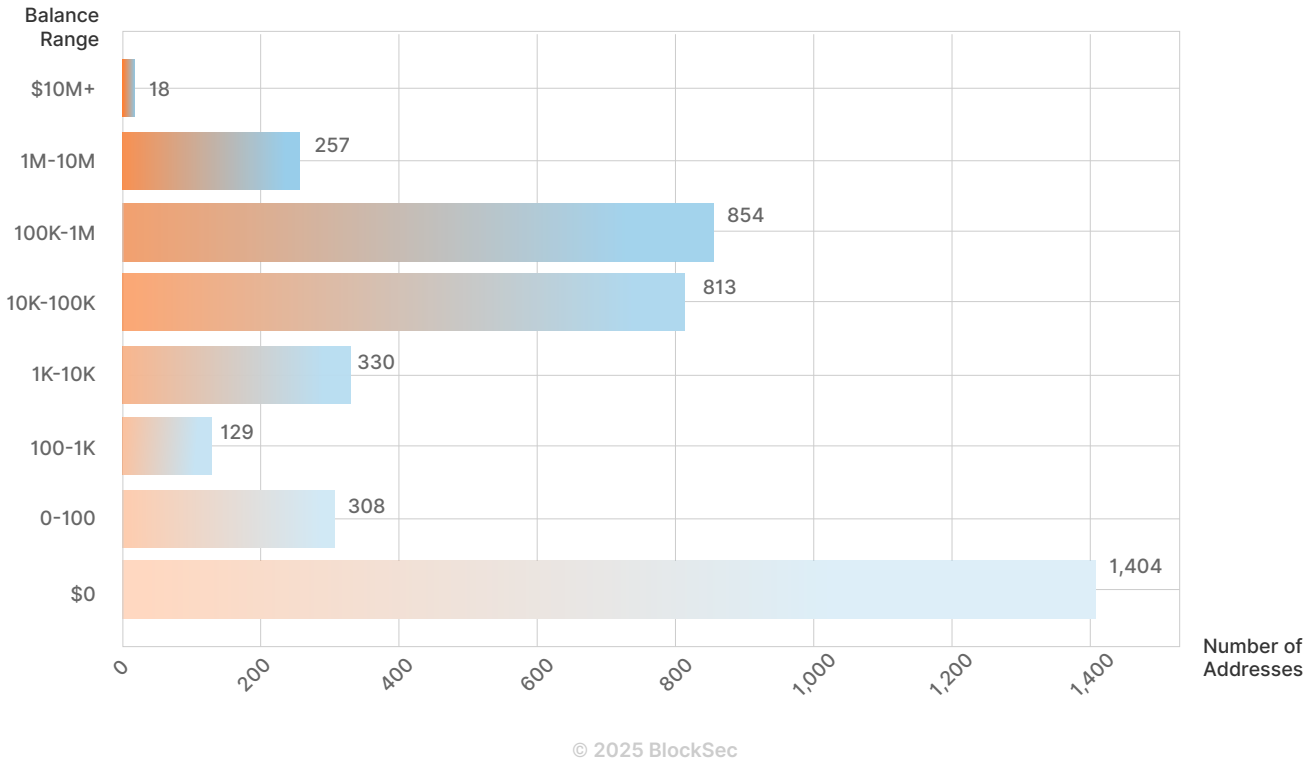





Balance concentration is similarly pronounced. Approximately 75% of frozen funds were held in just 275 addresses with balances exceeding $1 million. Freezing therefore disproportionately constrains high-value nodes within illicit networks.

At the same time, the broader base of lower-balance freezes reflects a complementary strategy. Large accounts linked to major investigations face direct capital removal, while widespread freezes of smaller wallets disrupt intermediary and laundering infrastructure. Together, these dynamics illustrate a layered enforcement model targeting both core actors and supporting network components.

▶ Balance Distribution of Blacklisted Addresses(2025)




Once blacklisted, USDT becomes immediately non-transferable. Freezing alters asset functionality in real time: enforcement is not merely signaled but encoded directly into contract-level usability.

## A Structural Turning Point in Stablecoin Compliance

Viewed over a longer horizon, 2025 does not represent an isolated spike in freezing activity, but the convergence of several structural developments. The intensification of stablecoin enforcement reflects both regulatory formalization and the evolving role of stablecoins within illicit financial flows.

First, regulatory clarity strengthened the institutional basis for enforcement. In July 2025, the United States enacted the GENIUS Act, establishing a federal framework for stablecoin oversight. The legislation formally brought issuers within the financial regulatory perimeter, mandating compliance with anti-money laundering, counter–terrorist financing, and sanctions requirements, alongside the operational capacity to execute lawful freezing and asset disposition orders. For foreign issuers with material U.S. exposure, compliance shifted from cooperative practice to statutory obligation. Transitional provisions were included, but the direction was clear: scalable and sustained enforcement became an expectation.

Second, stablecoins' central position within illicit value flows elevated their importance as control points. By 2025, stablecoins accounted for the majority of illicit cryptocurrency transaction volume. This dominance does not stem from inherent vulnerability, but from their function as a universal liquidity layer across legitimate and illicit markets alike. Consequently, stablecoin exposure became a structural feature of compliance engagement rather than an exceptional circumstance.

Third, enforcement patterns confirm institutionalization. On-chain data shows a multi-year expansion in USDT freezing activity, culminating in a 2025 peak exceeding one billion dollars in a single year. Cumulative freezes since 2023 now total multiple billions. Freezing no longer reflects episodic intervention; it operates as a sustained enforcement capability.

Taken together, 2025 marks a turning point not because of headline figures, but because three developments aligned: regulatory codification, stablecoin centrality, and scalable execution capacity. Stablecoins have shifted from assets subject to regulation to mechanisms through which regulation is executed.

Freezing is therefore no longer peripheral to compliance architecture. It functions as a direct interface between regulatory intent and on-chain asset state—reshaping risk calculations within illicit networks and reinforcing the integration of blockchain systems into formal supervisory regimes.

# Southeast Asia's Organized Scam Ecosystem: Labor, Platforms, and Adaptive Dynamics

Organized scam activity in Southeast Asia has evolved from dispersed criminal clusters into a regionally embedded system. Rather than revolving around a single offense type, the ecosystem now combines industrialized scam compounds, structured labor recruitment and control mechanisms, intermediary-style guarantee platforms, and stablecoin-based settlement networks.

Over time, these components have become mutually reinforcing. Online fund flows are closely tied to offline labor control structures, enabling both operational scale and cross-border replication. What has emerged is not simply geographic concentration, but a coordinated model in which recruitment, transaction routing, and liquidity management operate as linked stages of the same process.

In 2025, international enforcement and regulatory coordination intensified across the region. This chapter examines how the ecosystem functions under that pressure—and how it adjusts in response. Drawing on on-chain analysis and case-level observation, we trace the formation of labor supply chains, the intermediary role of guarantee platforms, and the measurable shifts in transaction behavior that accompany sustained enforcement activity.

# Scam Compounds and Labor Brokerage: The Formation of a Human Supply Chain

## Industrialized Scam Compounds

Scam compounds in Southeast Asia have evolved from dispersed or temporary criminal sites into industrial-scale operational hubs. In Myanmar, Cambodia, Laos, and neighboring regions, large compounds operate in concentrated clusters, featuring defined hierarchies, stable staffing structures, and enclosed living and working environments.

These facilities typically include dormitories, office space, and logistical support infrastructure. Entry and exit are tightly controlled, creating highly restricted operating zones. The figures below illustrate a large compound under construction in Shwe Kokko and an aerial view of KK Park.

Geographically, compounds are not randomly distributed. They cluster along border corridors—particularly in areas with limited enforcement capacity and complex cross-border transit routes. Regulatory gaps and political instability in these regions provide conditions conducive to long-term entrenchment and scaled operations.

Internally, operations are highly standardized. Scam activity is structured into parallel "product lines", including fraudulent investment schemes, romance scams, impersonation of law enforcement officials, and online gambling. Target populations are primarily overseas. Workflows are decomposed into repeatable procedures, scripts are continuously optimized, and victim outreach is quantified through performance metrics.

### Labor Supply Mechanisms: Recruitment, Control, and Resale

If scam compounds function as production facilities, their sustainability depends on a stable and replaceable labor force. Investigative materials indicate that labor acquisition generally unfolds in three stages: recruitment or deception, coercive control, and internal transfer or resale.

Recruitment commonly occurs under the guise of high-paying jobs, overseas employment opportunities, or online entertainment companies. Targets are often economically vulnerable individuals with limited access to reliable information.

Once transported abroad, initial promises collapse: passports are confiscated, movement is restricted, and employment conditions shift into coercive labor arrangements.

A more systematized pattern has emerged beyond initial recruitment. Controlled workers are frequently transferred or resold between compounds. Individuals who fail to meet performance quotas or are deemed insufficiently productive may be sold to other operations. This internal circulation transforms compounds from isolated crime sites into components of a closed labor marketplace. The image below shows workers rescued during the February 2025 raid on KK Park, illustrating the scale of labor demand.

## Labor Guarantee Platforms: Platformization of Human Trafficking

Within this environment, a new intermediary structure has accelerated labor trafficking at scale: labor guarantee platforms. Unlike traditional trafficking arrangements—often reliant on direct coercion and informal negotiation—these platforms formalize transactions through rule-based coordination and escrow-style settlement mechanisms.

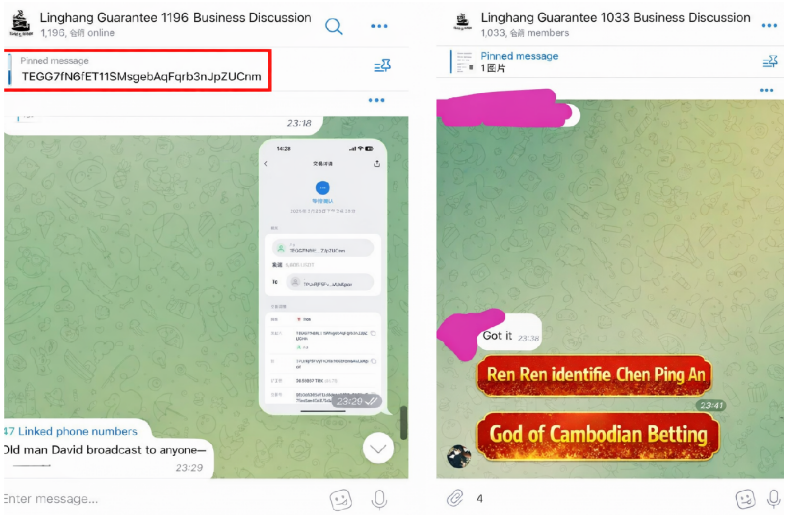
Labor guarantee platforms connect two market participants: scam compounds with ongoing labor demand and traffickers responsible for recruitment, transportation, and delivery. Acting as guarantors, platforms reduce counterparty risk through a "deposit plus final payment" structure and collect coordination fees.

In practice, compounds pay an upfront deposit to confirm demand. Once delivery is verified, the platform releases the final payment to the trafficker. Structurally, this resembles escrow-based transactions common in e-commerce. Platform rules and reputation signaling foster repeated interactions, reducing friction and uncertainty in high-risk illicit exchanges.

## Communication and Settlement Infrastructure: Telegram and Stablecoins

Operationally, labor guarantee platforms depend on two critical infrastructures: encrypted messaging applications and stablecoin payment networks.

Communication occurs primarily via Telegram. Small private groups negotiate transaction details—such as delivery location, pricing, and verification procedures—while larger public groups serve promotional and reputation-building functions. Participants share chat screenshots, transaction confirmations, and on-chain transfer records to signal reliability and speed, thereby attracting additional participants into the ecosystem. The figure below illustrates promotional content posted in a public Telegram group, displaying transaction discussions and blockchain confirmations sourced from smaller private groups.



Settlement is predominantly conducted in USDT on the TRON network. Platforms control designated receiving addresses; compounds transfer deposits and final payments to these addresses, and funds are subsequently distributed to traffickers, completing the escrow cycle. The low cost, cross-border efficiency, and speed of stablecoin transfers enable this transnational network to scale and automate settlement operations.

## On-Chain Behavior of Labor Guarantee Platform Suppliers

Building on the preceding analysis of scam compounds and labor brokerage mechanisms, this section turns to on-chain data. We examine a labor guarantee platform that has maintained sustained operational visibility within relevant Telegram communities. By combining transaction records with publicly observable group activity, we construct a behavioral profile of supplier-side participants and analyze transaction frequency, value distribution, and downstream fund flows.

### Supplier Scale and Transaction Frequency: Repeat Participation as the Norm

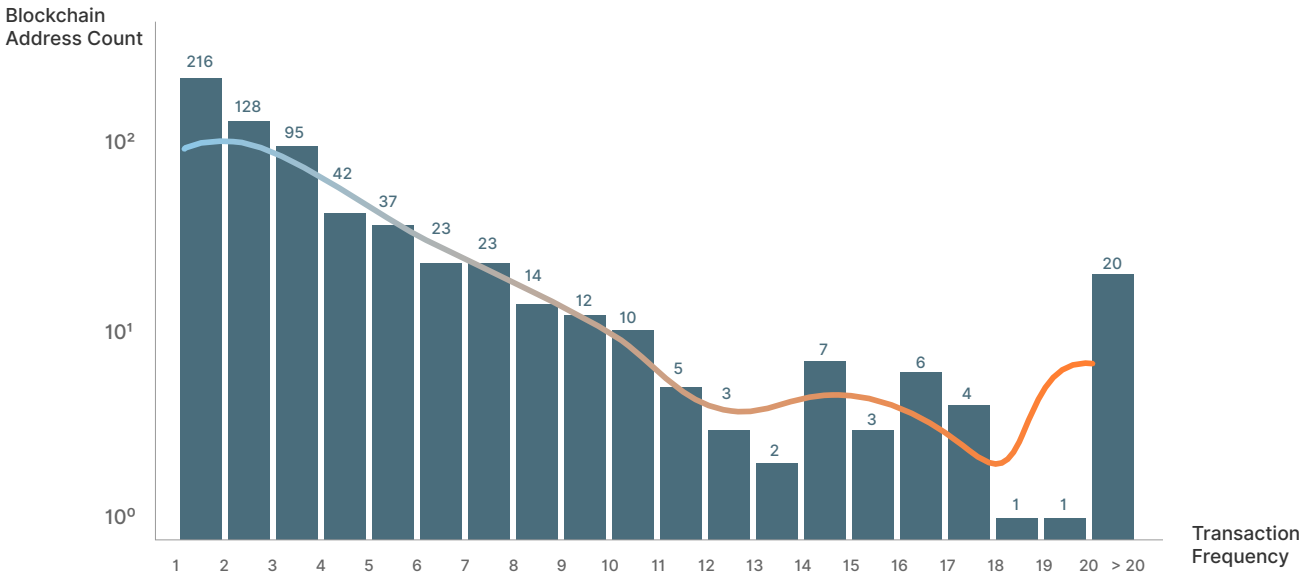
Across the analyzed platform, 652 supplier addresses linked to labor trafficking were identified, with cumulative transaction volume of approximately $14.58 million.

Repeat participation is the dominant pattern. Only 216 addresses (33.1%) engaged in a single transaction, meaning that more than two-thirds participated in multiple transfers. Approximately one-third recorded four or more transactions, indicating sustained engagement rather than one-off involvement.

In extreme cases, a small subset of addresses conducted more than twenty transactions, reflecting ongoing operational participation.

This distribution suggests that the platform does not merely match sporadic actors. It sustains a recurring supplier base, lowering coordination costs and reinforcing operational continuity.

### ▸ Distribution of Transaction Frequency



### Transaction Value Distribution and Pricing Ranges

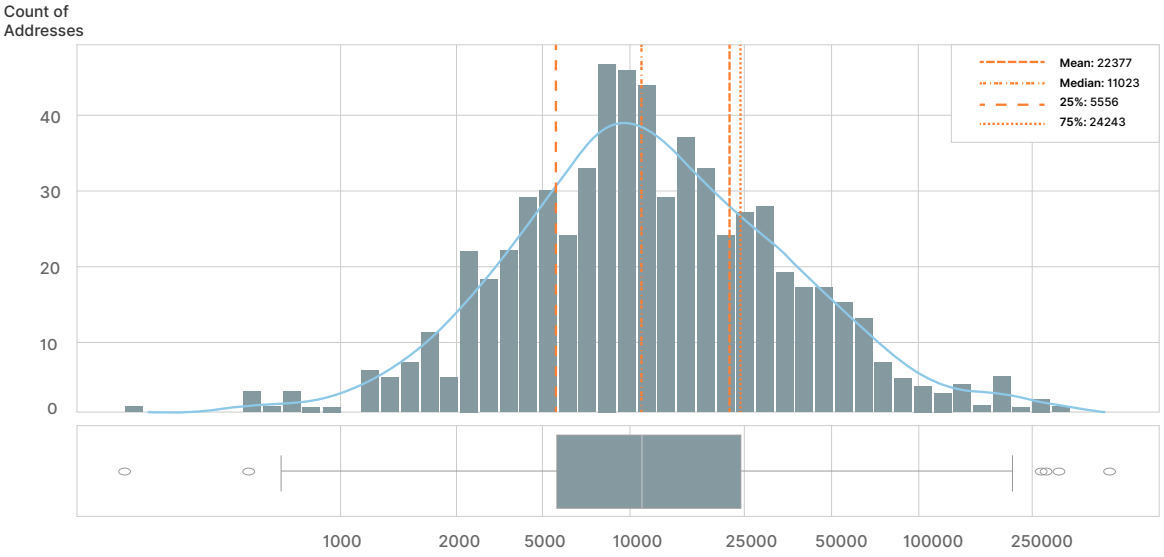
We analyzed total USDT revenue earned by each supplier address through the platform. The resulting distribution clusters within a relatively narrow range rather than being driven by extreme outliers.

Median total revenue per address is approximately $11,023, with an average of $22,377. Roughly 54.2% of addresses fall within the $5,000–$25,000 range, with the $5,000–$10,000 and $10,000–$25,000 bands each accounting for close to one-quarter of observations. These ranges broadly align with publicly discussed per-person pricing in associated Telegram groups.

Importantly, the distribution is not dominated by a handful of unusually large transactions. Its relative stability suggests the emergence of consistent pricing bands shaped by supply-demand dynamics, delivery risk, and transaction costs.

The presence of standardized pricing indicates reduced transactional uncertainty and a degree of structural normalization within what would otherwise be fragmented black-market exchanges.

▸ Distribution of Transfer Amount with Boxplot






## Downstream Flows and Cash-Out Pathways

The conversion of stablecoin proceeds into usable funds is central to the persistence of supplier-side activity.

We conducted downstream tracing on approximately 120 supplier addresses that collectively received about $624,600 in USDT. At least 54.3% of traced proceeds ultimately flowed into centralized exchanges for cash-out across multiple major platforms. Certain exchanges absorbed a disproportionately large share of these flows, underscoring their structural role within the settlement chain.

Two broad behavioral patterns emerge. In the first, suppliers exhibit limited laundering sophistication: funds pass through few intermediary hops before reaching exchanges, and in some instances exchange deposit addresses are used directly. In the second, suppliers adopt more deliberate obfuscation strategies, fragmenting transfers, extending transaction paths, and distributing funds across multiple exchanges.

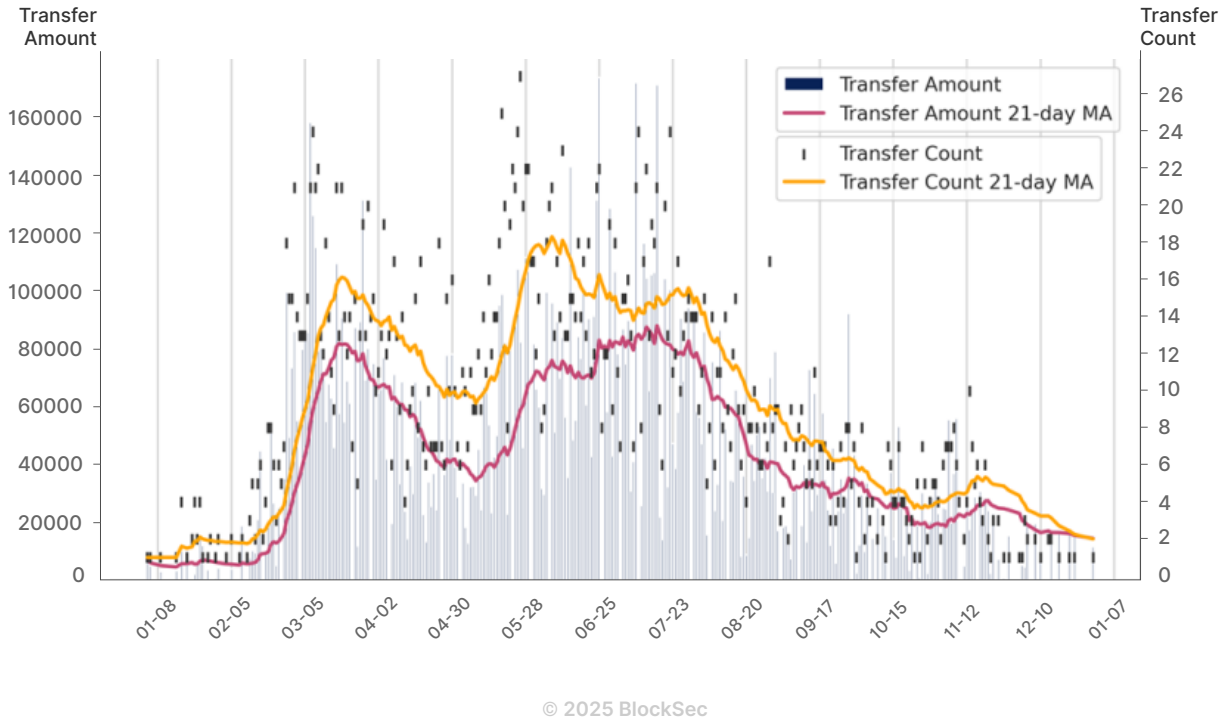
Extrapolating the observed exchange-outflow ratio across the platform's total recorded supplier volume of $14.58 million suggests that more than $7.9 million in supplier proceeds likely exited through exchange infrastructure.

While this estimate assumes proportional behavior across the broader address set, it underscores a consistent structural dependence on centralized liquidity providers. Despite the clandestine nature of labor trafficking, its financial endpoints remain closely tied to exchange-based settlement channels.

## On-Chain Transactional Responses Under Enforcement Pressure

To assess how labor guarantee activity responds to enforcement pressure, we analyzed Linghang Guarantee's on-chain transaction count and volume across 2025 and mapped their evolution over time.

### ▸ Transfer Amount and Count Over Time




The observed trend reflects how enforcement and governance measures propagate through financial and platform channels into measurable shifts in black-market activity.

Across 2025, Linghang Guarantee's activity unfolds in three phases: a marked contraction in April–May, a partial rebound in June–July, and a sustained decline from August onward.

## Short-Term Contraction Under Multi-Layered Pressure

The first notable decline appears in April–May. Rather than being driven by a single event, this downturn reflects the cumulative impact of compound-level crackdowns combined with financial and platform-level regulatory actions. Together, these measures increased transaction friction and temporarily compressed labor guarantee activity.

At the compound level, enforcement intensified along the Thai–Myanmar border beginning in early 2025. Restrictions on electricity, fuel, and telecommunications disrupted scam center operations. Reuters reported in March 2025 that coordinated cross-border efforts led to victim rescues and repatriations. These interventions affected both sides of labor guarantee transactions: they raised the logistical cost and uncertainty of delivering individuals to compounds while dampening public recruitment and visible transaction activity.

At the financial and platform level, FinCEN designated Cambodia-based Huione Group as a "primary money laundering concern" on May 1 and proposed restrictions limiting its access to the U.S. financial system. The designation explicitly referenced its role in scam and laundering ecosystems. Shortly thereafter, Telegram removed accounts and channels linked to Huione Guarantee and Xinbi Guarantee networks.

Although Linghang Guarantee was not directly targeted, ecosystem-wide enforcement actions elevated perceived risk across the network. Participants delayed transactions, reduced public signaling of completed deals, and limited visible activity—corresponding with the observed decline in both transaction count and volume.

### Adaptation and Reorganization Following Initial Shock

Transaction volume and count partially rebounded in June–July. This pattern aligns with broader observations of cross-border scam and labor brokerage ecosystems: enforcement spikes rarely eliminate activity outright. More commonly, they prompt relocation, restructuring, and adaptive reorganization.

Regional reporting indicates that following intensified scrutiny in areas such as Myawaddy, certain groups shifted operations to adjacent compounds or alternative sites. The Irrawaddy reported that after KK Park became a focal point of enforcement and media attention, some networks relocated to nearby areas. The United Nations Office on Drugs and Crime (UNODC) similarly noted in its 2025 Mekong regional report that organized crime groups respond to enforcement pressure through diversification strategies, operational adjustments, and reconstruction of financial pathways.

Within the labor guarantee ecosystem, these adaptations manifested in observable forms: dismantled compounds were replaced by newly established sites; banned public channels were rapidly reconstituted; and blockchain addresses attracting attention were abandoned in favor of new address clusters and modified routing structures.

The June–July rebound reflects a transition from disruption to adaptive stabilization. Activity did not disappear; it reorganized under revised risk conditions.

### Gradual Structural Decline Under Sustained Pressure

From August through year-end, activity follows a sustained downward trajectory rather than a sharp collapse. This pattern is consistent with structural adjustment under prolonged regulatory pressure.

At the regulatory level, U.S. measures extended beyond the initial May designation. In October, FinCEN finalized rules further restricting Huione Group's access to the U.S. financial system, converting proposed measures into durable constraints. The cumulative effect reinforced expectations of rising long-term risk, contributing to sustained compression of visible transaction activity.

Platform governance also deepened. Public channels associated with guarantee ecosystems were repeatedly removed, constraining recruitment, matchmaking, and reputational signaling in open environments. Under these conditions, activity migrated into smaller private networks or fragmented across alternative intermediaries and dispersed address structures, reducing exposure tied to identifiable platforms.

Notably, platform bans did not produce immediate cessation of activity. After Linghang Guarantee's public channels were removed, associated blockchain addresses continued to receive sporadic payments between September and December. This divergence—public coordination channels disrupted while fund flows persisted—indicates a shift from high-visibility coordination toward lower-frequency, fragmented settlement patterns.

The overall trajectory reflects gradual attenuation and migration under sustained governance pressure rather than abrupt disappearance.

## Chapter Summary and Implications

Across 2025, Linghang Guarantee's transaction patterns demonstrate adaptation rather than disappearance under enforcement pressure.

Multi-layered interventions temporarily reduced visible activity by increasing operational friction. Yet over time, participants relocated, rebuilt communication channels, and adjusted transaction behavior to restore continuity.

Sustained regulatory and platform actions did not immediately dismantle the ecosystem. Instead, they altered its structure. Public coordination declined, activity shifted into smaller and more private networks, and on-chain flows became less concentrated and more fragmented.

This case illustrates a broader principle: enforcement pressure is more effective at reshaping operational structure and increasing costs than at producing immediate cessation. Assessing long-term governance effectiveness therefore requires attention not only to volume reduction, but to how illicit systems reorganize under constraint.

# The Financial Restructuring of Drug Trafficking: From Cash Smuggling to On-Chain Laundering Networks

The primary enforcement challenge in contemporary drug trafficking extends beyond intercepting shipments or dismantling retail distribution networks. It increasingly centers on identifying and constraining the financial systems that sustain cross-border capital continuity.

Historically, narcotics operations depended on cash smuggling, informal value transfer systems, and fragmented underground banking channels. These methods imposed logistical constraints and operational risk, limiting scalability. As cryptocurrency infrastructure matured—particularly stablecoin-based settlement networks—drug trafficking organizations began integrating digital assets directly into their capital management frameworks.

This development represents more than the adoption of an alternative payment mechanism. It marks a structural shift in financial organization. Cryptocurrency now serves to standardize settlement, coordinate cross-jurisdictional transfers, and separate operational roles within criminal enterprises.

Laundering, in turn, increasingly functions either as an internalized specialized division or as an outsourced professional service operating independently of any single trafficking group.

Stablecoins are central to this transformation. Their price stability, liquidity depth, and cross-border utility allow narcotics proceeds to circulate within a unified accounting layer, mitigating volatility while enabling scalable transfer. In this context, cryptocurrency operates less as an anonymity device and more as programmable financial infrastructure.

The two cases analyzed in this chapter demonstrate how drug-related illicit finance has evolved from ad hoc concealment toward structured, repeatable laundering architectures. This restructuring shifts enforcement focus: rather than targeting isolated transactions, effective intervention requires identifying centralized control nodes, intermediary settlement layers, and liquidity exit channels embedded within on-chain networks.

## Case Study I: Laundering Architecture of a Violent Drug Trafficking Organization

The Ryan James Wedding case provides a detailed illustration of how drug trafficking networks systematically integrate cryptocurrency into structured laundering and capital coordination systems.

The indictment describes a cocaine trafficking organization operating across Canada, the United States, Mexico, and parts of Latin America. Its scale, role differentiation, and reliance on digital assets reflect a mature transnational network. Unlike cases in which cryptocurrency serves merely as an auxiliary settlement tool, digital assets here were embedded within the organization's core financial operations.

According to the indictment, narcotics proceeds were laundered through U.S. dollars, Canadian dollars, and cryptoassets. At the digital layer, large sums were repeatedly subdivided, routed across multiple USDT wallets, and ultimately consolidated into a central wallet controlled by Ryan James Wedding. Judicial filings identify Sokolovski, Hossain, and Canastillo-Madrid as key operational actors within the laundering process, alongside other associates collectively described as members of the "Wedding Organization."

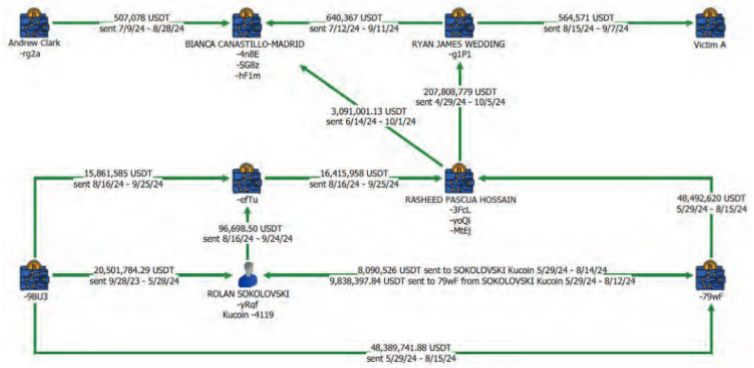
Laundering of Drug Proceeds

d. The Wedding Criminal Enterprise would conceal the significant proceeds of its cocaine sales in U.S. and Canadian dollars and cryptocurrencies.

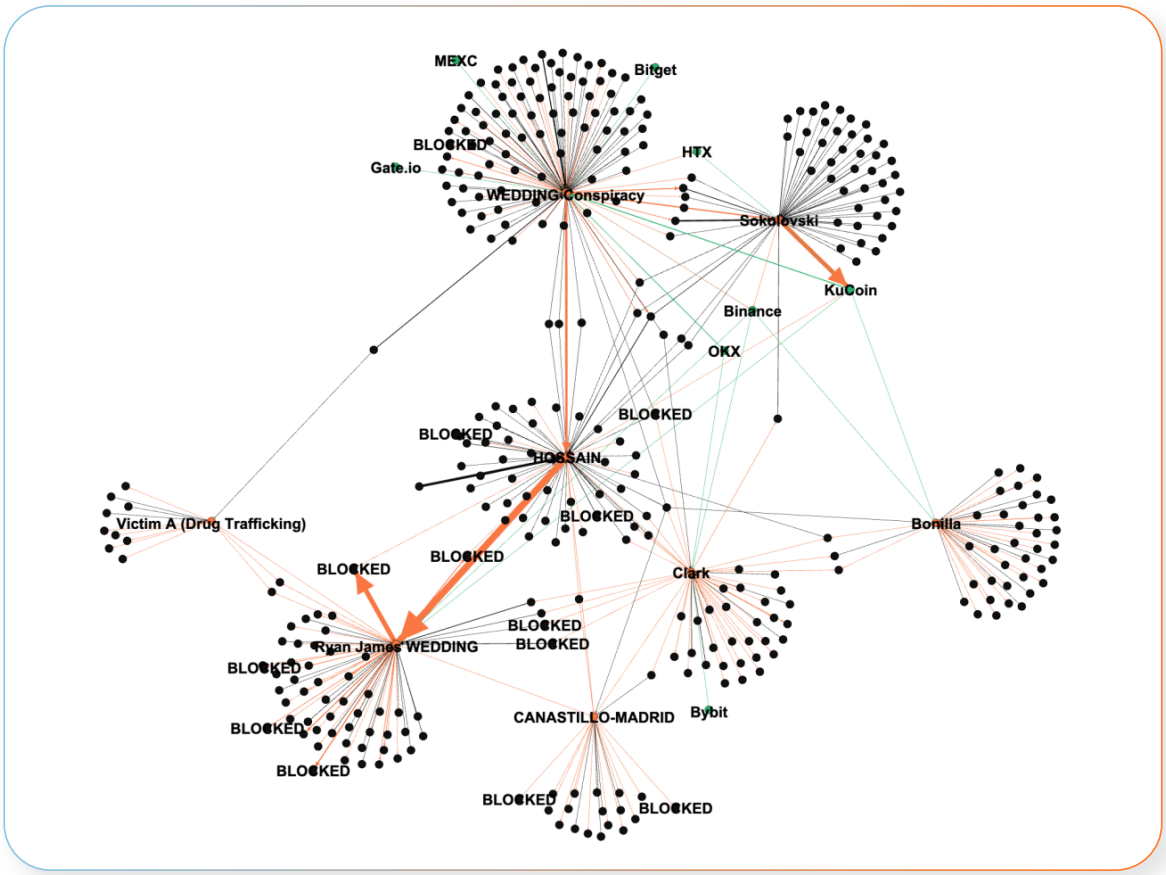
e. With respect to the use of cryptocurrencies, to obscure the original source of the funds, members and associates of the Wedding Criminal Enterprise would use a sophisticated Tether network to: (1) break large amounts of money into smaller transfers and (2) quickly use intermediary USDT wallets to move funds before ultimately reaching a hub Tether wallet controlled by defendant WEDDING.

f. Defendants SOKOLOVSKI, HOSSAIN, and CANASTILLO-MADRID, and others known and unknown to the Grand Jury, would serve members and associates of the Wedding Criminal Enterprise, namely, defendant WEDDING and Clark, by concealing their drug trafficking proceeds and by using those proceeds to facilitate and further the objectives of the enterprise. A truncated flow chart illustrating this laundering system is depicted in the diagram below.





Joint analysis of court records and on-chain data reveals a clearly tiered laundering architecture. Upstream address clusters directly associated with drug transactions functioned as initial receipt and rapid dispersion nodes. Funds were fragmented and redistributed within short intervals, reducing exposure at any single address and preparing flows for downstream consolidation.



At the midstream layer, laundering activity exhibited explicit role specialization. At least two parallel but functionally distinct pathways are observable. One pathway, centered on Sokolovski-controlled addresses, focused on aggregation and off-ramping, with substantial volumes flowing into centralized exchanges such as KuCoin for conversion into fiat or highly liquid assets. The second pathway, involving Hossain and related nodes, extended multi-stage on-chain transfers before consolidating funds into wallets controlled by Wedding.

This dual-channel structure created operational complementarity: one branch emphasized liquidity realization, while the other preserved centralized capital control and allocation. The indictment further indicates that laundering responsibilities were organizationally distinct from core trafficking operations, reflecting professionalized specialization within the network.

Stablecoins played a structural role in this system. Court filings and on-chain analysis show extensive use of USDT across multiple stages of fund movement and settlement. Relative to more volatile cryptoassets, USDT provided a stable accounting unit across extended laundering cycles while maintaining deep liquidity at major exchanges. The selection appears driven by stability, liquidity, and execution efficiency rather than anonymity alone.

The Wedding case therefore illustrates a structured, role-differentiated laundering architecture anchored around stablecoin-based capital coordination. In this context, cryptocurrency functions not merely as a circumvention mechanism, but as embedded financial infrastructure sustaining transnational drug operations.

## Case Study II: A Professionalized On-Chain Laundering Service Network

Unlike the Wedding case, where laundering functions were embedded within a trafficking organization, this case reveals a comparatively autonomous and specialized laundering network. Rather than serving a single drug trafficking group, the network operated as a service provider, offering capital cleansing, cross-border transfer, and settlement services to multiple illicit actors, including narcotics distributors.

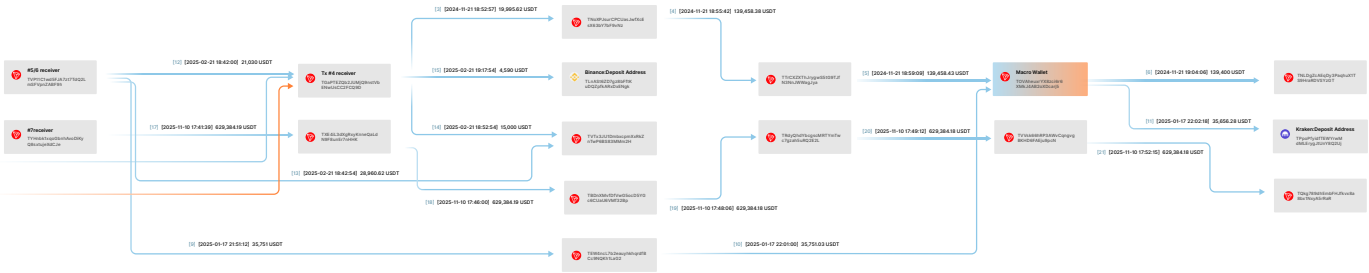
Within this structure, cryptoassets were not the endpoint of criminal proceeds. Instead, they formed part of a multi-stage, cross-jurisdictional underground financial process, functioning as instruments of value intermediation and capital coordination. Investigative materials indicate a stable client base, clearly differentiated roles, and reusable operational workflows—hallmarks of a professionalized service model rather than an ad hoc arrangement.

## Organizational Design: From Distributed Intake to Centralized Control

Sworn affidavits describe a structurally convergent architecture.

At the upstream stage, funds were received through numerous intermediary addresses associated with different regions and illicit revenue sources, including drug trafficking. These addresses handled intake and preliminary dispersion. Before reaching core nodes, funds typically underwent multiple rounds of subdivision, recombination, and short-interval transfers, extending transactional paths and reducing exposure at any single address.

In contrast to the dual-path structure observed in the Wedding case, this network emphasized sustained convergence toward a single control node. Repeated references to a "Macro Wallet" identify it as the central consolidation and command point. Controlled directly by the principal laundering operator, this wallet served as the ultimate aggregation hub, coordinating capital allocation and external settlement. It represented both operational authority and concentrated systemic risk within the structure.



## Functional Role of the Central Wallet

Investigative transaction descriptions indicate that the central wallet functioned as a capital management hub rather than a passive receiving address. Its responsibilities included:

• Aggregating funds that had already undergone upstream layering;
• Executing batch-level allocations based on client demand and timing;
• Converting funds into fiat or equivalent assets through OTC channels, liquidity providers, or alternative financial conduits.

This design externalized complexity to upstream layers while concentrating control within a limited number of key nodes. Controlled transaction records demonstrate the network's capacity to receive, segment, confirm, and deliver large sums within compressed timeframes—evidence of procedural standardization and operational maturity.

continued: “We clean that wallet. The one I received from him. Those USDTs are going to transit through seven more wallets. From one network to another before it arrives to our macro-wallet.” **FIGUEIRA** then explained that from that “macro-wallet,” **FIGUEIRA** sends the money to a liquidity provider, which exchanges the USDTs for dollars, and transfers the dollars to **FIGUEIRA**’s bank accounts.

## Stablecoins as a Standardized Settlement Layer

As in the Wedding case, USDT was widely used across multiple stages of the laundering cycle. Its function extended beyond price stability.

Affidavit records include direct statements from the defendant citing cross-border usability, settlement efficiency, and operability within constrained financial environments as primary reasons for selecting USDT. The emphasis was practical rather than anonymity-driven. Stablecoins enabled smoother cross-jurisdictional transfers while reducing repeated exposure to traditional banking scrutiny.

47. **FIGUEIRA** continued to explain the benefits of working with USDT. **FIGUEIRA** stated: "Basically, it is used for what we are doing. It is used to transfer money in a quick way, even to make it get to jurisdictions that have some type of issues, etcetera. For example, to send it to China. It is not that easy to pay in China. Or, let's say it because I'm from there, to bring resources from Venezuela, and to pay different accounts not only in the United States but also in other parts of Europe and Asia, through USDT, because Venezuela doesn't have the liberty to interact with the international financial institutions because of the sanctions."

Upstream funds often originated across multiple jurisdictions and were subject to foreign exchange controls, sanctions regimes, or compliance oversight. USDT provided a relatively neutral intermediary layer, enabling cross-border transfers without reliance on domestic banking infrastructure while limiting volatility risk over extended laundering cycles.

More significantly, stablecoins functioned as a standardized settlement layer. Illicit proceeds from diverse origins could be consolidated, fragmented, and reallocated under a unified unit of account before entering downstream channels. This standardization reduced operational complexity and enabled the network to service multiple clients without restructuring settlement mechanisms for each revenue source.

## Structural Financialization of Drug Trafficking

The two cases analyzed in this chapter illustrate a structural transformation in how drug trafficking organizations manage capital. Cryptocurrency is no longer used episodically for settlement convenience; it is increasingly embedded within coordinated laundering architectures defined by role specialization, procedural repeatability, and centralized capital management.

Two organizational patterns emerge. In some instances, laundering functions are integrated within trafficking groups through differentiated pathways and internal capital control. In others, laundering is outsourced to specialized intermediary networks operating as professionalized underground financial service providers. Despite these structural differences, both models rely on standardized workflows and cross-border liquidity mobility enabled by stablecoin-based settlement layers.

From an on-chain perspective, this financialization manifests in longer transaction chains, deeper address layering, and systematic convergence toward consolidation nodes and exchange off-ramps. Capital movement becomes process-driven rather than opportunistic. Drug proceeds circulate within structured financial circuits designed for continuity, scalability, and risk distribution.

This transformation does not eliminate operational exposure; it redistributes it. Risk shifts from physical transportation of value to the integrity of intermediary financial infrastructure.

## Governance Implications

As drug trafficking capital flows migrate into structured on-chain systems, enforcement leverage increasingly resides in financial architecture rather than commodity interception alone.

Disruption strategies must therefore prioritize identification of consolidation nodes, monitoring of intermediary laundering service networks, and oversight of exchange-based liquidity gateways. Stablecoin ecosystems, in particular, represent a central coordination layer where compliance capacity and enforcement execution intersect.

The strategic challenge is no longer limited to tracing individual transactions. It lies in mapping and constraining the infrastructure that enables capital continuity across jurisdictions. Effective intervention depends on structural targeting—focusing on chokepoints, control hubs, and settlement rails—rather than episodic case-based disruption.