# Whole-of-Ecosystem Monitoring for Tokens and Stablecoins: A Supervisory and Risk-Management Framework

## Abstract

This paper sets out a framework for *whole-of-ecosystem monitoring*—a supervisory approach designed to provide continuous oversight across the entire lifecycle of a token, from **pre-issuance counterparty screening** to **secondary-market circulation**. Traditional monitoring models focus narrowly on address or transaction-level activity.

The proposed framework integrates these methods into a comprehensive structure encompassing four complementary layers:

- **Counterparty and distribution risk assessment** ,
- **Token and contract-level oversight**,
- **Entity and address-level surveillance** , and
- **Fund-flow tracing and investigation**, which enables the identification, classification, and documentation of illicit or high-risk value movements across chains and intermediaries.

Together, these components allow regulators and financial institutions to monitor how a token is created, distributed, and transacted within interconnected markets.

## 1. Introduction

This project was commissioned to explore *whole-of-ecosystem transaction monitoring* for tokens and stablecoins. The initiative seeks to establish practical mechanisms for continuous, data-driven supervision of digital-asset activity—covering how such instruments are created, distributed, traded, and held across interconnected networks and service providers.

**Fragmented tools and risk propagation**

Current monitoring systems capture risk only in fragments, for instance, exchange-based surveillance identifies activity within a single venue, while traditional blockchain analytics tools wallet or transaction-level behaviour. These methods do not connect events across the lifecycle of a token, leaving material gaps in oversight and accountability.

Risks associated with tokens and stablecoins are interlinked across actors and markets. Exposure can originate at the point of issuance, migrate through intermediaries and decentralised protocols, and re-emerge as market or compliance failures downstream. A token may be lawfully minted, pooled with illicit funds in a DeFi contract, and later re-introduced into the financial system through legitimate on-ramps—creating indirect exposure for regulated institutions.  Downstream risk arises when on-chain interactions (such as liquidity pooling, cross-chain swaps, or automated redemption) blur the line between compliant and non-compliant value, complicating AML and sanctions screening

### Need for holistic monitoring

These dynamics have led regulators to call for *whole-of-ecosystem monitoring*: a capability to observe and assess token activity across its full lifecycle. Such an approach recognises that AML/CFT and market-integrity risks propagate through several layers—

- **Issuers and distributors** – where token design, issuance controls, and counterparties establish the foundation for downstream exposure;
- **Trading venues and DeFi protocols** – where cross-chain bridges, custodial structures, and pooled liquidity can obscure beneficial ownership; and
- **Secondary markets** – where rapid circulation and price volatility can conceal layering, wash trading, or manipulation.

### Objective of this paper

This whitepaper outlines the policy rationale and technical foundations for that approach. It demonstrates how an integrated monitoring framework can enhance AML and market-integrity outcomes by combining counterparty verification, token-level analytics, and fund-flow intelligence within a unified supervisory model. The framework equips regulators, financial institutions, and token issuers to identify, assess, and mitigate emerging risks in real time as digital assets move across the broader ecosystem.

## 2. Regulatory Context and Problem Statement

Supervisory expectations for digital-asset activity have expanded rapidly. Early regulatory guidance centred on service providers—registration of exchanges, wallet screening, and transaction monitoring under anti-money-laundering and counter-terrorism-financing (AML/CFT) frameworks. Increasingly, regulators now view risk as **ecosystem-wide**, extending beyond individual intermediaries to the full circulation of a token across smart contracts, custodians, liquidity pools, and secondary markets.

In the United States, the **GENIUS Act (2025)** most clearly articulates this shift. It obliges payment stablecoin issuers to maintain the technical capability to **block, freeze, or burn illicitly held tokens**, affirming that compliance responsibilities continue beyond primary issuance and redemption. The Act acknowledges that risk persists in secondary-market transactions between third parties, where the issuer has no direct relationship but remains accountable for unlawful use of its tokens.

A similar direction is emerging under the **New York Department of Financial Services (NYDFS)** coin-listing and delisting guidance, which requires ongoing assessment of listed assets for **technical, operational, market-integrity, and illicit-finance risks**. The framework effectively embeds continuing due diligence as part of a token's life on trading platforms, recognising that risk characteristics evolve as tokens are transferred, traded, or re-deployed in decentralised applications.

The **European Union's Markets in Crypto-Assets Regulation (MiCA)** and the **Monetary Authority of Singapore's Stablecoin Regulatory Framework (2023)** adopt the same principle in different contexts: regulatory assurance must be supported by continuous verification of a token's circulation, counterparties, and usage. These developments collectively establish that effective oversight depends not only on institutional compliance, but on **visibility into how risk propagates through an entire token ecosystem**.

Whole-of-ecosystem monitoring responds directly to this regulatory direction, providing the analytical foundation for continuous, cross-platform supervision of tokens and stablecoins within a unified, data-driven framework.

## 3. Challenges and Risk Dimensions

Digital-asset ecosystems face a broad spectrum of risks, ranging from operational failures and governance weaknesses to volatility and market manipulation. While these factors collectively affect market integrity, this paper focuses on a narrower but critical dimension—**the monitoring of illicit-finance and related compliance risks across the token and stablecoin ecosystem**. The following sections outline where those risks emerge, why they are difficult to detect, and how existing monitoring tools fall short in providing regulators and financial institutions with a complete view of exposure.

## Challenge 1: Contract and Issuer Legitimacy

The earliest compliance risk arises at the point of token creation. A token's smart contract defines how it can be minted, transferred, or redeemed, and therefore sets the foundation for lawful circulation. When control over this contract is weak—or when administrative privileges can be exploited—large volumes of new tokens can enter the market without detection. For regulators and exchanges, verifying that a contract operates as declared, and that its issuer retains effective control, remains one of the most difficult aspects of digital-asset supervision.

**Where monitoring fails**

- **Contract upgrades and proxy patterns** – A single contract address can be upgraded or replaced through proxy mechanisms without changing its visible identity on-chain. Existing monitoring tools treat the address as unchanged, missing the introduction of new mint or transfer privileges.
- **Hidden administrative controls** – Many token contracts include "owner-only" or "pause/mint" functions. These appear dormant until triggered and therefore do not generate anomalies in transaction-based analytics.
- **Issuer identity vs. contract operator** – The entity deploying or managing the contract may differ from the legal issuer named in disclosures, creating

a disconnect between corporate accountability and on-chain authority. Current compliance datasets rarely link these identities.

- **Absence of behavioural baselines** – Without continuous monitoring of contract inflows and outflows, early warning signals—such as rapid depletion of reserves, sudden spikes in token minting, or abnormal counterparties interacting with the contract—go unnoticed until after the damage has spread through the ecosystem.

**Example:**

**Ankr Exploit (December 2022):** A compromised deployer key was used to upgrade the aBNBc contract and remove access controls from its mint function, enabling unrestricted token creation. The unauthorised tokens were sold through decentralised exchanges within minutes, with the event visible only as a surge in liquidity rather than as a flagged anomaly.

**Ordinals Finance (April 2023):** An attacker used a proxy-admin function to reassign ownership of staked assets, draining funds without breaching consensus rules. Because the activity involved normal contract calls, most analytics tools flagged no anomaly. A contract-level monitoring layer could have detected the rapid outflow of assets and the interaction of previously unseen wallets with the staking contract—signals consistent with illicit-finance typologies rather than user behaviour.

Both incidents show how failures at issuance and contract-management stages can create cascading illicit flows that only become visible when funds reach exchanges or liquidity pools. For ecosystem-level oversight to be effective, monitoring must include the behaviour of deployed token contracts themselves—not just the transactions that follow.

## Challenge 2 – Distribution and Counterparty Risk

After a token or stablecoin is created, its movement into circulation depends on who first receives it and under what conditions. Counterparty verification at this stage determines whether illicit value is introduced into the market or whether exposure remains confined to regulated entities. In practice, the challenge appears in two distinct forms:

### A. Regulated Stablecoin Issuers – Secondary-Market Counterparty Risk

**Nature of the challenge**

Regulated issuers distribute new supply only through approved exchanges, custodians, and institutional clients that have completed full KYC and AML checks. This model effectively mitigates primary-market risk. However, once tokens leave those trusted rails and begin circulating across decentralized protocols, OTC desks, and cross-chain bridges, the issuer's visibility and control end.

**Why it matters**

Even when all direct counterparties are verified, the next tier of transactions—counterparties of counterparties—can re-introduce illicit funds into the system. Stablecoins redeemed or swapped through DeFi pools can commingle with proceeds of crime or sanctioned assets, creating tainted liquidity that later re-enters regulated exchanges. Supervisors cannot easily differentiate between compliant and contaminated supply once these tokens move into open circulation.

**Example**

Following the *Harmony Bridge* exploit in 2022, a portion of the stolen funds was converted into USDT and bridged across multiple networks before reaching centralised venues. Although USDT was originally issued to compliant institutions, its later circulation connected regulated supply to illicit activity—illustrating the secondary-market exposure that persists beyond issuer controls.

**B. Unregulated or Decentralised Token Projects – Primary-Market Counterparty Risk**

**Nature of the challenge**
For unregulated token issuers, the problem emerges at inception. New tokens are often distributed through launchpads, private sales, or automated market-maker pools without counterparty due diligence. Early participants may include affiliated insiders or wallets linked to previous frauds. Because these addresses have no verified identity or historical tags, they enter the market appearing clean.

**Why it matters**
Once unverified wallets seed initial liquidity, the taint spreads instantly across trading venues. By the time a token lists on an exchange, the original source of funds is untraceable, leaving institutions exposed to laundering and sanctions-evasion risks. Regulatory intervention then becomes reactive—limited to post-incident tracing. For instance, the ***Squid Game Token*** **collapse in 2021** showed how anonymous counterparties can corrupt an asset from launch. Early liquidity was provided by wallets previously involved in rug-pull schemes. Because no distribution-stage monitoring existed, those addresses were not identified until after the token's failure, by which point illicit proceeds had been recycled through other projects.

While new tokens distributed in permissionless environments can be exploited in multiple, distinct ways, the following patterns are particularly relevant to supervisors and compliance teams:

**Rug-pulls and exit scams** — Malicious developers seed liquidity and then drain the pool once retail buys in.

- ***When:*** Immediately after listing or first liquidity provisioning.

- ***Why it matters:*** Investors lose funds; tainted proceeds are recycled into other projects; exchanges and intermediaries listing the token face reputational and AML exposure.
- ***Why hard to detect:*** Owner-controlled wallets appear legitimate until the drain occurs; liquidity movement is rapid and can be split across many small transactions to evade thresholds.

• **Wash trading and fake volume** — Coordinated trading across wallets or venues to create an appearance of demand.

- *When:* During and after initial listing to attract capital or qualify for exchange listing.
- *Why it matters:* Artificial volumes mislead market participants and can be used to launder value by creating plausible on-chain movement.
- *Why hard to detect:* Cross-venue coordination and algorithmic bot activity mimic normal market making; standard address tags do not reveal collusion.

**Pump-and-dump and coordinated hype** — Groups use social media, private chats, and bots to inflate prices then sell.

- ***When:*** Shortly before or after listing; reruns whenever liquidity permits.
- ***Why it matters:*** Rapid inflows and outflows create layering opportunities for illicit gains and draw retail funds into risky positions.
- ***Why hard to detect:*** Off-chain coordination drives on-chain behavior; sentiment signals must be fused with transaction patterns to detect coordination.

**SafeMoon and other "meme-token" surges (2021–2023)**

During several meme-token cycles, including SafeMoon (2021) and PEPE (2023), groups of affiliated promoters used Twitter, Telegram, and Discord channels to coordinate price spikes. Large holders injected liquidity and simultaneously launched social-media campaigns to drive retail inflows.

Once volumes rose, these same wallets began selling into the liquidity they had created—realising profits while leaving retail participants exposed to rapid losses.

From a compliance perspective, these episodes illustrate how **off-chain coordination produces on-chain anomalies**: a sharp increase in small new wallets, repeated cyclical buy-sell activity, and abnormal transaction clustering within a short time window. None of these movements necessarily violate blockchain protocol rules, so they pass through ordinary transaction-monitoring filters. Detecting such manipulative activity requires combining **sentiment analysis and token-flow metrics** to correlate social-media hype with sudden on-chain inflows and liquidity withdrawals.

**Liquidity-pool laundering (mixing via AMMs)** — Illicit assets are paired with project tokens in AMMs to obscure provenance; subsequent swaps reintroduce value into "clean" chains.

- ***When:*** After initial distribution once liquidity pools exist.
- ***Why it matters:*** Pools instantly commingle clean and illicit value, undermining wallet-level risk scores and creating fungible exposure.
- ***Why hard to detect:*** Pool tokenization hides origin of constituent assets; tracing requires de-pooling and multi-step flow analysis across swaps.

**Airdrop abuse and Sybil schemes** — Creation of thousands of addresses to claim tokens, then use them to launder or manipulate metrics.

- ***When:*** At token launch or marketing distribution events.
- ***Why it matters:*** Inflates holder counts  obscures real ownership and enables coordinated sell-offs or wash patterns.

- ***Why hard to detect:*** New wallets are expected at launches; distinguishing genuine early adopters from Sybil clusters needs behavioural baselines and linkage analysis.

### Arbitrum Airdrop (March 2023)

Ahead of the Arbitrum token launch, analysts and the project's own Sybil-filtering partners identified tens of thousands of wallets created solely to qualify for the airdrop. Many were controlled by single operators using scripted activity—small bridge transfers, token swaps, and governance interactions—to mimic real user behaviour. Despite multiple screening rounds, an estimated 10–20 % of the distribution still reached coordinated clusters of Sybil wallets. Within hours of the airdrop, those clusters consolidated and sold their allocations through decentralised exchanges, distorting liquidity data and short-term holder metrics.

For supervisors, this illustrates the detection challenge: **the behaviour of Sybil wallets is indistinguishable from legitimate new users until after consolidation occurs.** Each wallet meets the eligibility rules, and all transactions are valid on-chain; the manipulative pattern emerges only when multiple addresses act in synchrony. Identifying such clusters requires temporal and network-graph analysis rather than static wallet screening, which most existing AML and compliance systems are not designed to perform.

**Governance capture and bribery** — Buying or bribing large token holdings to change protocol parameters or approve malicious proposals.

- ***When:*** After token distribution once governance is active.
- ***Why it matters:*** Can enable theft, change mint/burn rules, or relax protections without on-chain alarms.
- ***Why hard to detect:*** Governance votes appear procedurally valid; identifying economic coercion or off-chain inducements requires cross-evidence beyond chain data.

**Backdoor minting / hidden supply mechanisms** — Tokenomics that permit later inflation or phantom supply increases (e.g., hidden mint addresses, privileged bridges).

- ***When:*** Post-deployment when privileged functions are exercised.
- ***Why it matters:*** Undermines asset integrity and creates sudden sell pressure used to convert illicit proceeds.
- ***Why hard to detect:*** Static code analysis would reveal this best; behavioural monitoring only sees effects (sudden supply changes) after they occur.

**Flash-loan enabled manipulation** — Use of large, temporary capital to manipulate or drain liquidity and then unwind within a block.

- ***When**:* At any time if lending markets and DEX composability allow it.
- ***Why it matters:*** Enables exploitation and rapid value extraction tied to other illicit flows.
- ***Why hard to detect:*** Happens within atomic transactions; requires high-granularity, on-the-fly analysis to flag.

**Implication for monitoring design**

These patterns show that primary-market counterparty risk is not a single failure mode but a set of behaviours that exploit distribution mechanics, composability, and off-chain coordination. Effective detection therefore requires: (a) early screening of distribution pathways and initial liquidity recipients, (b) rapid behavioural baselining that flags anomalous issuance/distribution events, and (c) fusion of on-chain telemetry with off-chain signals (exchange KYC, social media, launchpad identity) to differentiate legitimate activity from abuse.

## Challenge 3 – DeFi and Cross-Chain Obfuscation

DeFi composability and cross-chain bridges enable rapid, automated movement of tokens and stablecoins across networks and pooled contracts. That capability both fragments provenance and multiplies points at which illicit value can be commingled with legitimate liquidity. As a result, funds can traverse regulatory perimeters within minutes, undermining single-venue transaction monitoring and creating significant AML and sanctions risks.

Technically, this is hard to monitor because the environment combines multiple, reinforcing obstacles: ledgers are heterogeneous (different standards, identifiers and event schemas), tokens exist in multiple representations (native, wrapped, synthetic) with distinct contract addresses, and DeFi operations often bundle many transfers into single atomic transactions that hide intermediate holders. On top of that, automation (bots, flash loans, multi-router swaps) executes high-frequency, multi-leg sequences whose behavioural signatures closely resemble legitimate market making until viewed at scale and across chains.

Put together, these factors mean that illicit actors can (for example) bridge stolen assets, perform dozens of small swaps across AMM routes to break lineage, and bridge out to another chain or exchange before single-chain monitors detect anything anomalous. Incidents such as the Harmony and Ronin bridge compromises illustrate how quickly cross-chain layering converts a theft or sanctionable inflow into effectively untraceable proceeds when multi-chain, time-correlated analysis is not available.

## Challenge 4 – Custodial and Market-Structure Risk

Risk does not end at issuance or distribution. Even when tokens and stablecoins are managed by compliant issuers, vulnerabilities can emerge through how reserves are held and how liquidity moves across custodians, exchanges, and DeFi pools. These market-structure dynamics can quietly erode confidence or transmit risk across chains before any formal disclosure occurs.

### Why it matters

Custodians and large exchanges often control a disproportionate share of circulating supply and reserves. Their operational decisions—redeeming, re-minting, or reallocating holdings—directly affect liquidity and price formation. If one custodian withholds redemptions, delays transfers, or redeploys assets to maintain yield, stress can ripple through the market long before regulators receive reports. Likewise, coordinated market-making or wash activity can create a false appearance of liquidity, masking shortfalls or concealing flows from illicit sources.

Such patterns rarely breach protocol rules; they appear as ordinary transfers until viewed in aggregate. Yet they influence multiple risk layers simultaneously: destabilising secondary markets, distorting cross-chain liquidity, and enabling tainted value to migrate between regulated and unregulated venues.

### On-Chain Behavioral Patterns to watch out for

1. **Custodial concentration** – A rising share of total supply held by a few exchange or custodian clusters, signalling dependency on limited counterparties.
2. **Unexplained issuance or redemption surges** – Sudden increases or decreases in supply without corresponding market demand or reserve disclosures.
3. **Liquidity migration** – Large, rapid outflows from known custodians or regulated exchanges into unverified DeFi pools or newly deployed bridge contracts.
4. **Circular or internal trading** – Repetitive transfers among affiliated wallets that inflate apparent trading volume or obscure real end-users.
5. **Price-volume divergence** – Sharp volume spikes unaccompanied by growth in unique holders, often preceding de-pegs or artificial rallies.
6. **Sustained divergence across markets** – Token prices deviating between exchanges or chains, suggesting uneven reserve deployment or market manipulation.

## Challenge 5 – Market Conduct and Smart-Contract Behaviour

Most token and stablecoin activity eventually concentrates in the secondary market, where thousands of automated agents—bots, arbitrage scripts, and trading contracts—interact continuously. These mechanisms drive liquidity and price discovery but can also conceal manipulation or illicit profit-taking. Direct prevention of such conduct sits outside transaction monitoring; however, several **behavioural indicators** can still be observed on-chain and integrated into ecosystem-level surveillance.

### Why it matters

Manipulative or exploitative trading distorts market integrity and can reintroduce illicit value into the ecosystem. Wash trading, coordinated volume inflation, and front-running through miner-extractable value (MEV) practices all produce artificial liquidity and rapid fund turnover that obscure real flows. Smart-contract vulnerabilities or governance manipulation can drain assets and then disperse them through the same trading infrastructure, blending stolen funds with legitimate activity.

### Patterns visible through monitoring

- **Cyclical buy–sell loops** between the same wallet clusters, inflating volume without genuine counterparties
- **Large transfers into newly deployed or unaudited contracts**, often preceding exploit activity.
- **Abnormal trading bursts** following oracle updates or social-media-driven price spikes.
- **Rapid concentration or dispersion of liquidity** across multiple DEX pools within short intervals.

These are not full proof of misconduct but can serve as **early indicators** of manipulation or post-exploit laundering.

### Illustrative case

During the July 2023 **Curve Finance exploit**, vulnerabilities in Vyper-compiled contracts drained several stablecoin pools. The attacker then executed rapid swaps and bridging transactions through newly created contracts to disguise origin and inflate apparent trading volume. While the exploit itself stemmed from contract logic, the resulting liquidity migration and abnormal transaction clustering were observable on-chain—precisely the type of secondary symptom that ecosystem-wide monitoring can surface.

### Supervisory implication

Monitoring tools cannot eliminate or prevent smart-contract or conduct risk, but they can highlight **patterns of market stress or manipulation** early enough for regulators or exchanges to intervene. Integrating these indicators into a broader token-ecosystem framework ensures that even when the cause is technical or behavioural, its financial-crime consequences are visible within the same supervisory perimeter.

---

## PROPOSED SOLUTION

Token Monitoring Toolkit – A Lifecycle Framework for Ecosystem-Level Risk Supervision

Effective oversight of tokens and stablecoins demands visibility that extends across their **entire lifecycle**—from **issuance and distribution** to **secondary-market circulation**.

Merkle Science’s Token Monitoring Toolkit brings these stages together under one architecture. Each module performs a distinct supervisory function, but collectively they form a **single data and analytics layer** for AML/CFT, sanctions, and market-integrity monitoring at ecosystem scale.

## 1. Pre-issuance screening (before onboarding distributors and liquidity partners)

**Objective.** Establish a risk-controlled foundation for token issuance by vetting ecosystem participants and technical controls prior to mint, consistent with the gaps identified in Challenges 1 and 3 above.

**Scope.** Applies to issuers, distributors, market-makers, custodians providing seed liquidity, and the smart-contract stack governing mint, treasury, and transfer logic.

*Risk assessment components*

1. **Counterparty due diligence (KYBB).**
    a. Identity, beneficial ownership, licensing/registration status, sanctions/PEP screening, adverse-media reports
    b. Jurisdictional exposure mapping (home state, operational footprint, cross-border servicing).
    c. Historical wallet behavior and cluster linkages based patterns (source of funds/wealth indicators, prior exposure to high-risk categories).
    d. Risk scoring with configurable weights; evidence requirements tied to score bands.
2. **Liquidity and Distribution Safeguards**
    a. Evaluate minting contracts, spot exposure to high-risk actors, and analyze systemic risks such as liquidity concentration or distribution imbalances
3. **Go/No-Go Gate**
    a. Minting proceeds only after all mandatory onboarding and exposure checks are completed. Approved entities and addresses are loaded into downstream monitoring modules (Smart Contract Watchlist) to

ensure continuity between pre-issuance screening and live supervision.

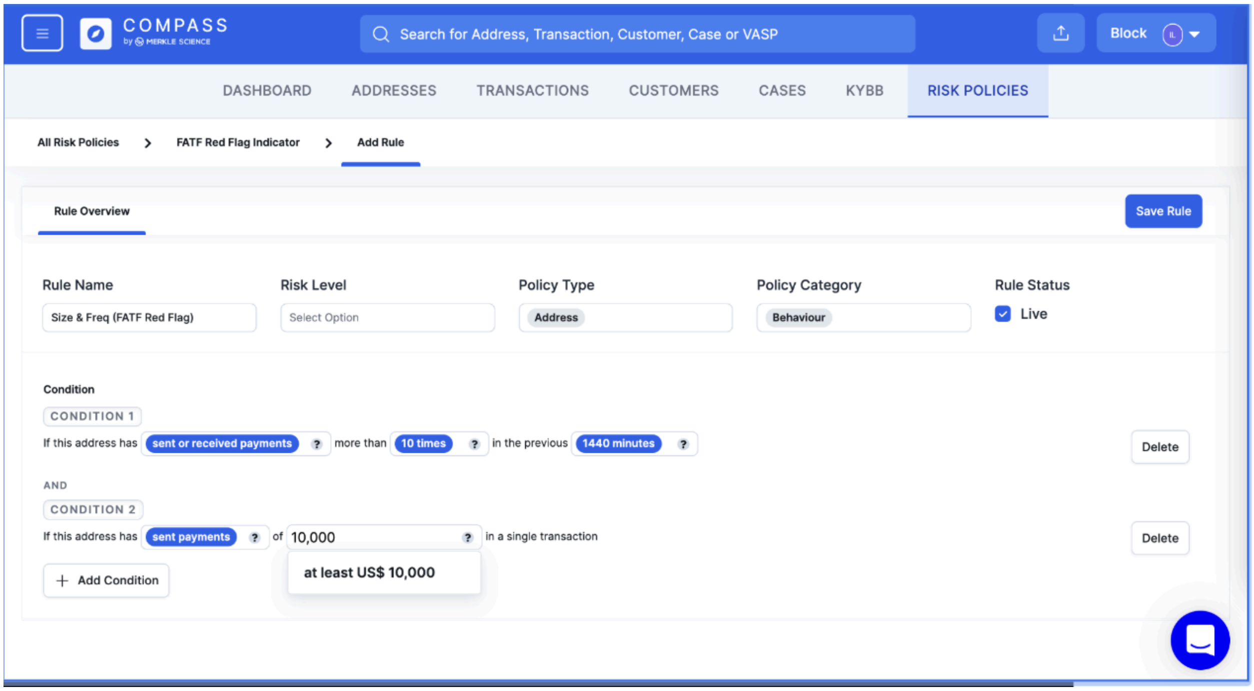
### 2. Circulation and Ecosystem Activity: Compass – Cross-Merchant Risk Detection

Once tokens enter circulation, risk no longer sits neatly within one institution. Wallets move across exchanges, custodians, and DeFi protocols, creating behavioral patterns that individual monitoring systems cannot detect. **Compass** provides both a cohesive and  micro view of those movements.

**Purpose**
Delivers continuous, rule-based monitoring of transactions across the ecosystem. Instead of observing a single merchant's customers, Compass maps how high-risk wallets interact across multiple regulated and unregulated venues within the same network.

**Behavioral Challenges Addressed**
Compass rules can detect and flag patterns that were previously invisible to siloed monitoring systems, including:

- **Multi-venue velocity:** wallets transacting with several merchants in short timeframes.
- **Liquidity fragmentation:** tokens cycling rapidly between exchanges, OTC desks, and pools.
- **Coordinated movement:** related addresses shifting funds simultaneously across entities.
- **High-risk contagion:** exposure chains linking compliant participants to sanctioned or illicit wallets.
- **Round-tripping and wash patterns:** repeated transfers between common counterparties to inflate volume or obscure source of funds.



| Rule Name | Risk Level | Policy Type | Policy Category | Rule Status |
|---|---|---|---|---|
| Size & Freq (FATF Red Flag) | Select Option | Address | Behaviour | ☑ Live |

Condition

CONDITION 1

If this address has sent or received payments ? more than 10 times ? in the previous 1440 minutes ?

AND

CONDITION 2

If this address has sent payments ? of 10,000 ? in a single transaction

at least US$ 10,000

*Custom Risk Rule for Stablecoin Activity: A stablecoin issuer sets a rule to flag addresses that send or receive more than 10 transactions above $10,000 in a 24-hour window. This may indicate structured transfers, layering, or potential mule activity—triggering alerts for further review before tokens circulate deeper into the ecosystem.*

## Additional Key Capabilities

- **Cross-Merchant Activity Dashboard:** Consolidates address and transaction data from all participating entities, showing shared counterparties, token-specific exposure, and alert categories. This feature aims to provide a full ecosystem view,  for instance , a network operator such as Mastercard can see stablecoin activity across all connected issuers and venues, while an individual issuer can track its own tokens' circulation and counterparties in the same shared environment.
- **Configurable Rule Engine:** Supports policies such as "flag addresses transacting with three or more merchants within 24 hours above threshold."
- **Real-Time Alerts and Escalation:** Generates immediate notifications when risky activity crosses institutional boundaries.
- **Audit-Ready Recordkeeping:** Maintains immutable alert histories for regulator or independent review.

**Supervisory Value**

Transforms fragmented institutional monitoring into coordinated ecosystem oversight, giving supervisors a clear view of how risk propagates while preserving each merchant's data confidentiality.

### 3. Contract-Level Assurance: Smart Contract Watchlist

Smart contracts automate value transfer, but they also remove the human checkpoints that traditionally enforce AML and sanctions controls. Once deployed, they execute whatever logic is coded—irrespective of who interacts with them. The **Smart Contract Watchlist** closes that gap by embedding continuous screening directly at the contract level.

**Purpose**

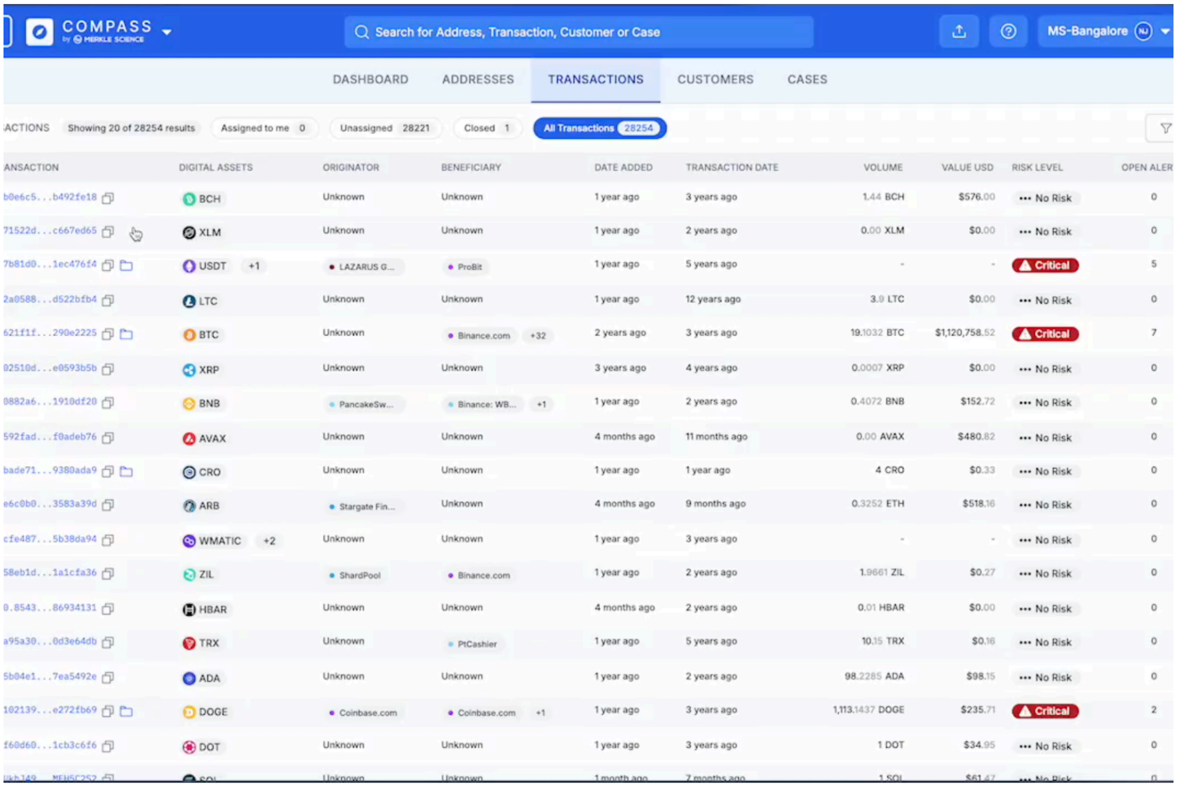
Monitors designated smart-contract addresses—such as token contracts, liquidity pools, and staking vaults—to ensure that all inflows and outflows comply with applicable AML and sanctions policies.

**Key Features**

- **Continuous screening:** Every transaction involving the monitored contract is screened in real time.
- **Risk classification:** Originator and beneficiary wallets are automatically classified based on sanctions, exposure history, and typology flags.
- **Policy-aligned alert thresholds:** Rules detect activity inconsistent with supervisory expectations, such as inflows from mixers or sanctioned entities.
- **Auditable transaction log:** Each screened interaction is recorded for later verification by auditors or regulators.

**Supervisory Value**

Bridges the gap between smart-contract automation and regulatory oversight. By integrating screening at the protocol layer, the Watchlist allows supervisors and issuers to maintain compliance assurance without disrupting on-chain execution or compromising user privacy.



| ANSACTION | DIGITAL ASSETS | ORIGINATOR | BENEFICIARY | DATE ADDED | TRANSACTION DATE | VOLUME | VALUE USD | RISK LEVEL | OPEN ALER |
|---|---|---|---|---|---|---|---|---|---|
| b0e6c5...b492fe18 | BCH | Unknown | Unknown | 1 year ago | 3 years ago | 1.44 BCH | $576.00 | No Risk | 0 |
| 71522d...c667ed65 | XLM | Unknown | Unknown | 1 year ago | 2 years ago | 0.00 XLM | $0.00 | No Risk | 0 |
| 7b81d0...1ec476f4 | USDT +1 | LAZARUS G... | ProBit | 1 year ago | 5 years ago | - | - | Critical | 5 |
| 2a0588...d522bfb4 | LTC | Unknown | Unknown | 1 year ago | 12 years ago | 3.9 LTC | $0.00 | No Risk | 0 |
| 621f1f...290e2225 | BTC | Unknown | Binance.com +32 | 2 years ago | 3 years ago | 19.1032 BTC | $1,120,758.52 | Critical | 7 |
| 02510d...e0593b5b | XRP | Unknown | Unknown | 3 years ago | 4 years ago | 0.0007 XRP | $0.00 | No Risk | 0 |
| 0882a6...1910df20 | BNB | PancakeSw... | Binance: WB... +1 | 1 year ago | 2 years ago | 0.4072 BNB | $152.72 | No Risk | 0 |
| 592fad...f0adeb76 | AVAX | Unknown | Unknown | 4 months ago | 11 months ago | 0.00 AVAX | $480.82 | No Risk | 0 |
| bade71...9380ada9 | CRO | Unknown | Unknown | 1 year ago | 1 year ago | 4 CRO | $0.33 | No Risk | 0 |
| e6c0b0...3583a39d | ARB | Stargate Fin... | Unknown | 4 months ago | 9 months ago | 0.3252 ETH | $518.16 | No Risk | 0 |
| cfe487...5b38da94 | WMATIC +2 | Unknown | Unknown | 1 year ago | 3 years ago | - | - | No Risk | 0 |
| 58eb1d...1a1cfa36 | ZIL | ShardPool | Binance.com | 1 year ago | 2 years ago | 1.9661 ZIL | $0.27 | No Risk | 0 |
| 0.8543...86934131 | HBAR | Unknown | Unknown | 4 months ago | 2 years ago | 0.01 HBAR | $0.00 | No Risk | 0 |
| a95a30...0d3e64db | TRX | Unknown | PtCashier | 1 year ago | 5 years ago | 10.15 TRX | $0.16 | No Risk | 0 |
| 5b04e1...7ea5492e | ADA | Unknown | Unknown | 1 year ago | 2 years ago | 98.2285 ADA | $98.15 | No Risk | 0 |
| 102139...e272fb69 | DOGE | Coinbase.com | Coinbase.com +1 | 1 year ago | 3 years ago | 1,113.1437 DOGE | $235.71 | Critical | 2 |
| f60d60...1cb3c6f6 | DOT | Unknown | Unknown | 1 year ago | 3 years ago | 1 DOT | $34.95 | No Risk | 0 |
| Ukh149...MEH5C252 | SOL | Unknown | Unknown | 1 month ago | 7 months ago | 1 SOL | $61.47 | No Risk | 0 |

*Smart Contract Watchlist interface showing live inflow/outflow screening and automated alerts on high-risk contract interactions.*

## 4. Ecosystem Oversight: Token Monitoring Dashboard

Once circulation is underway, regulators and issuers need to look beyond individual alerts to understand structural risks building across the ecosystem. The **Token Monitoring Dashboard** provides this macro-level perspective—translating on-chain metrics into indicators of systemic stability and policy exposure.

**Purpose**

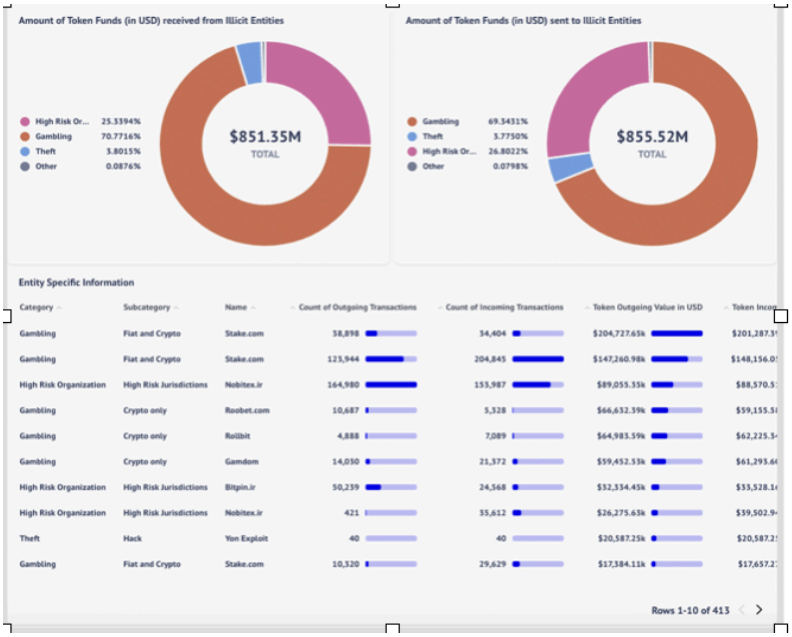
Delivers an ecosystem-wide analytical view of token behaviour, liquidity distribution, and risk concentration to support early warning and comparative supervision.

**Core Capabilities**

- **Liquidity and Concentration Analytics:** Aggregates transaction volumes, holder distribution, and liquidity by venue to identify concentration and fragmentation trends.
- **Systemic Anomaly Detection:** Flags sudden liquidity migration, de-pegs, and rapid supply changes that may indicate market or reserve stress.
- **Illicit-Use Mapping:** Quantifies the share of token activity linked to high-risk categories such as sanctioned entities, darknet markets, or mixers.
- **Cross-Chain Exposure Tracking:** Maps how token flows move between networks and identifies where systemic risk may propagate.
- **Custom Ecosystem Views (on request):** Enables deeper monitoring of token price, market cap, DeFi versus CEX liquidity, DEX–CEX spreads, and contract-level anomalies (unusual mint/burn patterns or high-risk pools).

**Example Use Case:** For a stablecoin issuer, the dashboard surfaces shifts in exchange liquidity and counterparty exposure; for a network operator or regulator, it benchmarks the ecosystem's aggregate risk posture and highlights emerging contagion channels.

**Supervisory Value:** Transforms raw blockchain data into policy-relevant intelligence. The Dashboard allows supervisors to detect structural vulnerabilities before they escalate—supporting proactive, data-driven oversight across markets, venues, and chains.



Entity Specific Information

| Category | Subcategory | Name | Count of Outgoing Transactions | Count of Incoming Transactions | Token Outgoing Value in USD | Token Incom |
|---|---|---|---|---|---|---|
| Gambling | Fiat and Crypto | Stake.com | 38,898 | 34,404 | $204,727.65k | $201,287.3 |
| Gambling | Fiat and Crypto | Stake.com | 123,944 | 204,845 | $147,260.98k | $148,156.0 |
| High Risk Organization | High Risk Jurisdictions | Nobitex.ir | 164,980 | 153,987 | $89,055.35k | $88,570.5 |
| Gambling | Crypto only | Roobet.com | 10,687 | 5,328 | $66,632.39k | $59,155.5 |
| Gambling | Crypto only | Rollbit | 4,888 | 7,089 | $64,983.59k | $62,225.3 |
| Gambling | Crypto only | Gamdom | 14,050 | 21,372 | $59,452.53k | $61,293.6 |
| High Risk Organization | High Risk Jurisdictions | Bitpin.ir | 50,239 | 24,568 | $32,334.45k | $33,528.1 |
| High Risk Organization | High Risk Jurisdictions | Nobitex.ir | 421 | 35,612 | $26,275.63k | $39,502.9 |
| Theft | Hack | Yon Exploit | 40 | 40 | $20,587.25k | $20,587.2 |
| Gambling | Fiat and Crypto | Stake.com | 10,320 | 29,629 | $17,384.11k | $17,657.2 |

Rows 1-10 of 413

*Example: Entity-Level Risk Intelligence: Visualize value flowing through illicit categories like scams, gambling, and high-risk jurisdictions—across both inbound and outbound directions, enabling proactive review of suspicious token circulation.*

## 5. Escalation and Investigation: Tracker

When high-risk activity is detected, supervisors must move from monitoring to evidence-building. The **Tracker** module supports this transition by tracing the complete movement of value—across wallets, exchanges, and chains—to generate defensible, audit-ready cases.

**Purpose**

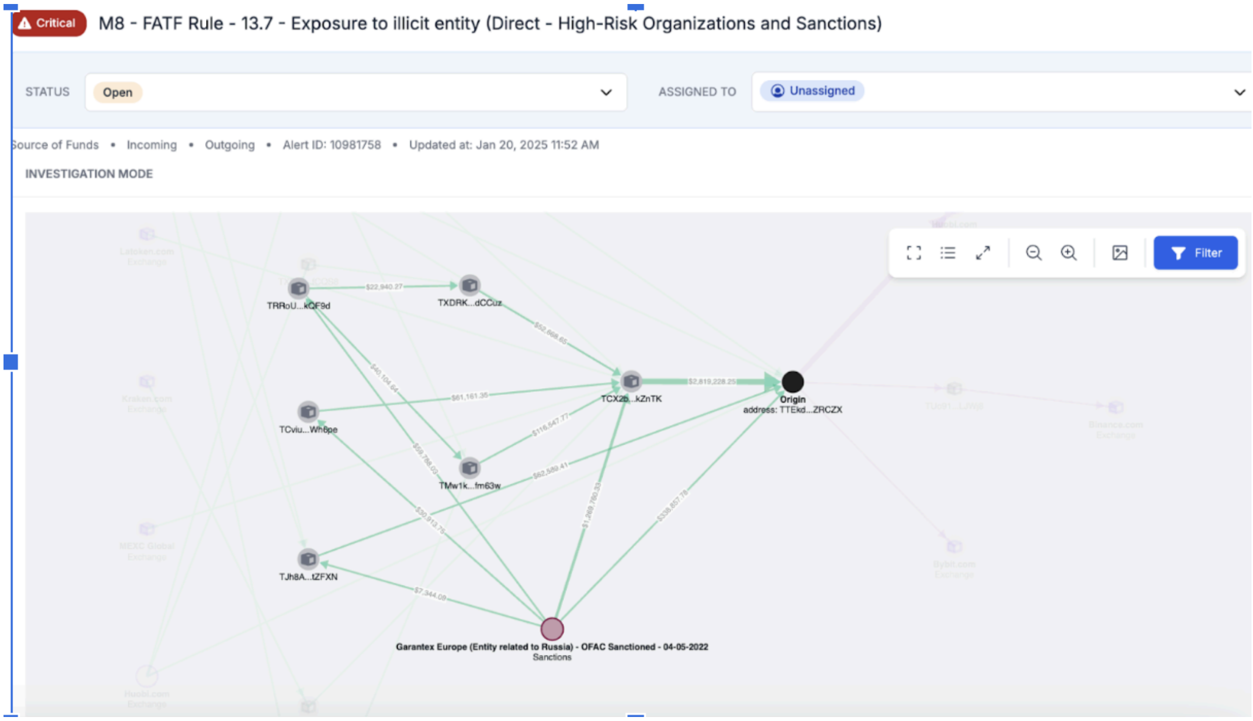
Converts alerts from Compass or the Smart Contract Watchlist into actionable investigations, allowing compliance teams to trace, document, and quantify exposure with precision.

**Core Capabilities**

- **Cross-Chain Tracing:** Follows the flow of funds through wallets, bridges, and DeFi protocols, reconstructing movement across multiple blockchains.
- **Transaction Intelligence:** Surfaces hashes, internal transactions, and method IDs to identify mixers, peel chains, or obfuscation patterns.
- **Entity Attribution:** Maps counterparties to clusters or known exchange identifiers to reveal laundering pipelines or exploit infrastructure.
- **Reporting:** Packages findings into structured, audit-ready reports suitable for regulators or law-enforcement referral.

**Supervisory Value**

Provides a forensically sound path from alert to enforcement. Tracker enables regulators and compliance officers to freeze, block, and escalate with confidence—linking behavioral detection to verifiable investigative outcomes.



Critical M8 - FATF Rule - 13.7 - Exposure to illicit entity (Direct - High-Risk Organizations and Sanctions)

STATUS Open

ASSIGNED TO Unassigned

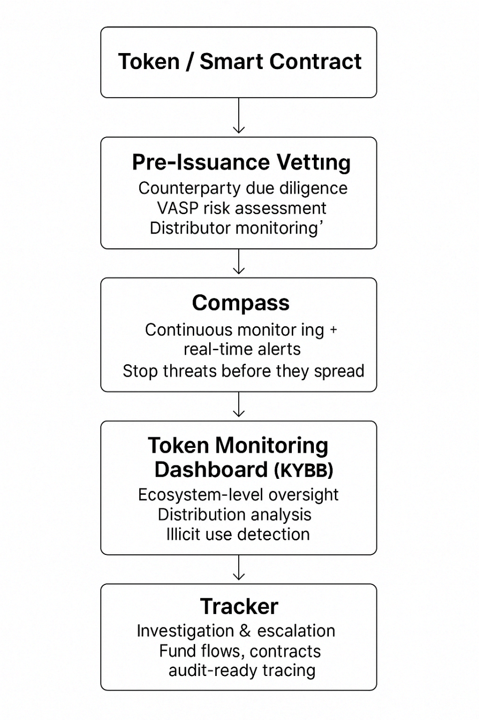
Source of Funds • Incoming • Outgoing • Alert ID: 10981758 • Updated at: Jan 20, 2025 11:52 AM

INVESTIGATION MODE

*Example: Analysts can trace fund movement from origin to OFAC-sanctioned entities like Garantex, uncovering intermediaries and transaction history to support enforcement, freezing, or reporting workflows.*

## 6. Integrated Monitoring Architecture

Across these modules, the toolkit operates as a **layered compliance infrastructure**:



Information flows seamlessly between modules: an alert in Compass can trigger investigation in Tracker; results can feed back into network-level analytics. This architecture supports both **preventive and investigative supervision** while minimising redundancy across participants.

## Outcome for MAS and Ecosystem Supervisors

The combined toolkit offers regulators and ecosystem administrators a structured, data-driven model for monitoring token integrity and financial-crime risk without imposing disproportionate reporting burdens on individual participants. It enables **continuous supervision at three levels**:

- **Micro (entity)** – each merchant’s direct interactions.
- **Meso (ecosystem)** – aggregated risk across participants.

- **Macro (market)** – systemic trends and anomalies.

This layered approach converts compliance from a series of isolated merchant checks into a **coordinated ecosystem-risk-management system**, aligning with MAS's objective of whole-of-ecosystem transaction monitoring for tokens and stablecoins.