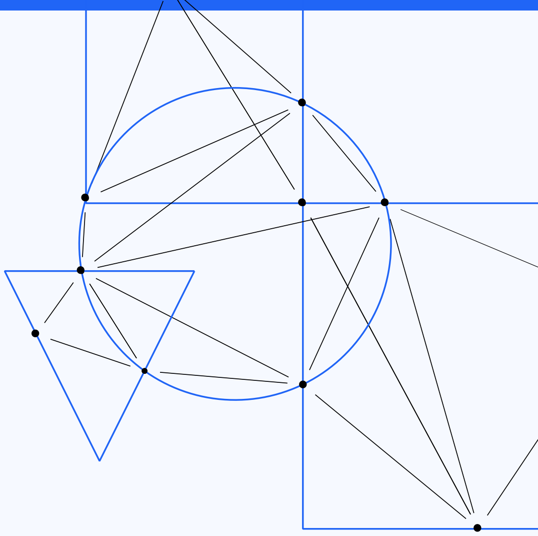
TRM



Blockchain Intelligence for Financial Regulators

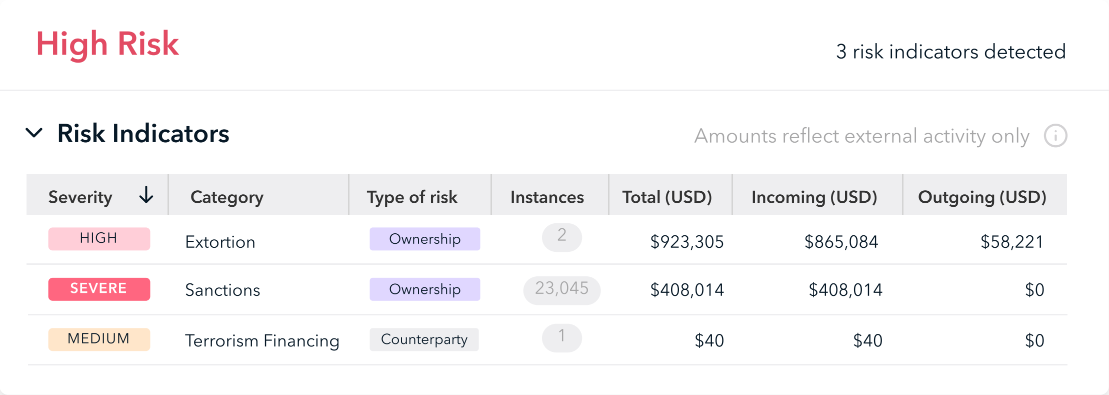
Digital asset exposure, and the number of firms facilitating activity in these assets, is increasing, adding challenges for regulatory bodies to evaluate, monitor and examine these organizations. As a result, supervisory and regulatory bodies around the world require unique analytics and intelligence to properly monitor this space. TRM's premier blockchain intelligence platform assists regulators in developing new methodologies for conducting this newfound, real-time supervision.

TRM provides critical insights to support regulators across key areas, including:

Targeted Risk Assessments & Licensing

On-Chain Risk Exposure

Understand the on-chain risk profile of VASPs applying for licenses to provide cryptocurrency services in your jurisdiction. Leverage risk indicator red flags to identify specific transactions indicative of control deficiencies and high risk exposure.



High Risk

3 risk indicators detected

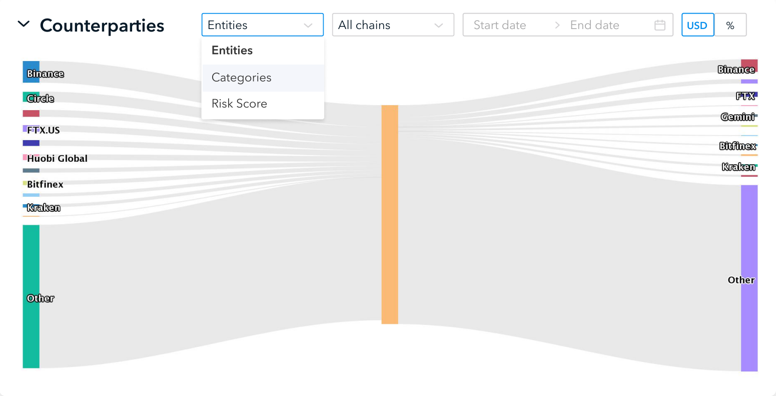
Risk Indicators

Amounts reflect external activity only

Severity ↓	Category	Type of risk	Instances	Total (USD)	Incoming (USD)	Outgoing (USD)
HIGH	Extortion	Ownership	2	$923,305	$865,084	$58,221
SEVERE	Sanctions	Ownership	23,045	$408,014	$408,014	$0
MEDIUM	Terrorism Financing	Counterparty	1	$40	$40	$0

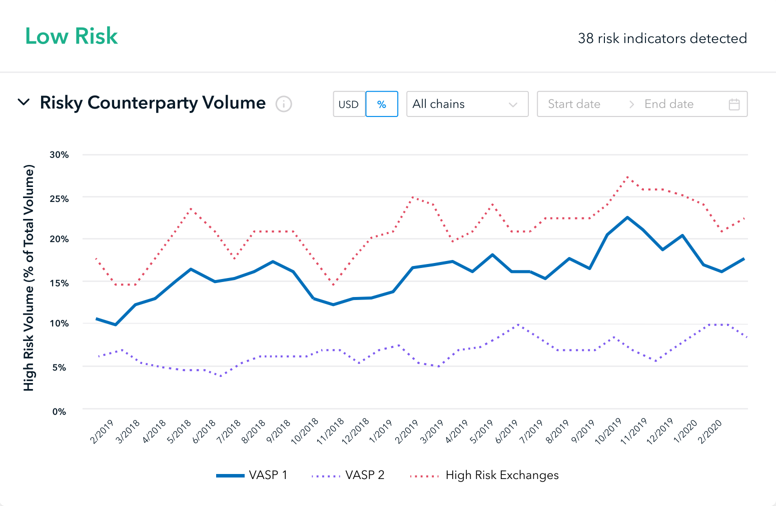
Counterparty flows

Understand a VASP's counterparty exposure, flows between affiliated entities, changes in asset flows over time and other associated risks.



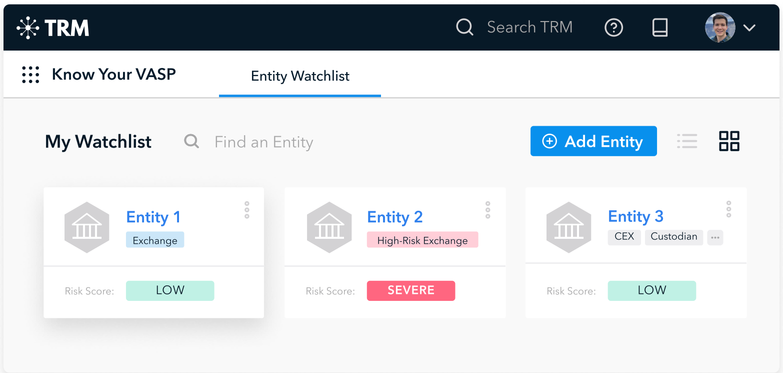
VASPs Benchmarking

Benchmark risk levels against cohorts of other VASPs.



Risk Monitoring

Monitor a VASP on an ongoing basis for changes in risk exposure or other deviations from expected activity.



Use Cases

TRM also provides the ability to view a VASP's asset token listing, jurisdictions of operations, fiat currency supported and actual level of KYC controls in order to assess:

Does the VASP's risk assessment include jurisdictions to which they may have exposure?

Example: the VASP supports Turkish currency conversions but doesn't acknowledge high-risk jurisdiction customers in risk assessment

Do the VASP's transaction monitoring controls cover all the assets they support?

Example: some crypto businesses will support new assets without first including in risk assessment or notifying regulators.

Does the VASP have other legal entities in jurisdictions that indicate connectivity or exposure to countries with sanctions implications?

Example: a crypto business may have an Eastern European entity that has exposure to Russian entities

Real-time Monitoring

Determine whether a licensee remains compliant on an ongoing basis when performing a periodic review or evaluating whether the licensee meets threshold conditions to maintain a licensed status.

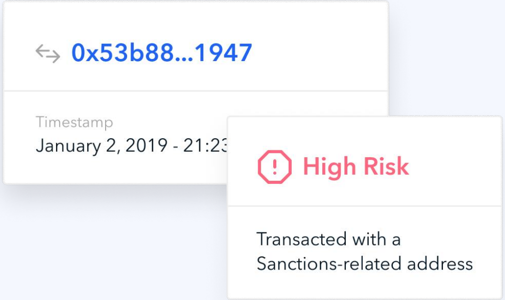
Monitor VASPs' transactions associated with illicit cryptocurrency activity such as sanctions, terrorist financing, darknet markets, child and sexual abuse materials, and more.

Risk-rate the entities you supervise to inform reports, onsite inspections, annual MLRO report and audits. If a spike in high-risk activity is detected, identify the root causes and provide industry guidance.

Easily identify, monitor and investigate whether regulated entities have exposure to nested activity associated with high-risk exchanges.

Rather than asking for transaction monitoring alert samples, pinpoint and target exact transactions that appear to be high-risk in order to inform your requests for information.

Assess VASPs' filing effectiveness by comparing VASPs' risky transactional activity to actual Suspicious Transaction Reports filed.



0x53b88...1947

Timestamp
January 2, 2019 - 21:23

High Risk

Transacted with a Sanctions-related address

- ✓ We enable monitoring across 1,000,000+ digital assets and 28 blockchains – including all ERC-20 tokens, popular stablecoins and DeFi tokens
- ✓ Our threat intelligence team proactively monitors changes in SDN lists and other embargo lists to ensure you are screening against the latest information
- ✓ TRM's Real Time Supervision module enables regulators to scan across all supervised entities and take a risk-based approach to supervise the virtual asset space, utilizing limited internal resources more effectively

Training and Certifications

TRM Academy

Extensive self-serve digital course library

- ✓ Product guides and tutorials
- ✓ Case studies and drills
- ✓ Timely micro-learnings on recent events or new product features

TRM Cryptocurrency Fundamentals Certification (TRM-CFC)

2-day course; 4 hours/day

A comprehensive orientation to the crypto ecosystem and key concepts related to crypto-based fraud and financial crime.

Academy access is complimentary for all TRM licensed users. Certifications priced separately.

TRM provides blockchain intelligence tools to help financial institutions, crypto businesses and governments combat cryptocurrency fraud and financial crime.

Request a demo:
contact@trmlabs.com | www.trmlabs.com