TRM

How Blockchain Intelligence Tools Help Detect and Prevent Money Laundering and Illicit Actors in Decentralized Networks

Financial institutions worldwide are in a state of experimentation with blockchain technology. As the institutionalization of this emerging technology grows, banks are investigating potential use cases and devising strategies to manage inherent risks.

One notable effort is Project Guardian, a pilot project by the Monetary Authority of Singapore and the financial sector, which focuses on the prospects of asset tokenization and decentralized finance (DeFi). While 'tokenization' has become a buzz word in the digital asset space, it fundamentally involves creating a digital counterpart of an asset, like a bond, on a blockchain. At its core, DeFi involves conducting economic activity, such as trades or lending, using software code to act as an automated market maker. Together, financial institutions are primarily interested in testing whether the combination of tokenization and DeFi technology can lower costs, reduce settlement times, and provide wider distribution for participants.

Leading financial institutions like HSBC, UBS, DBS Bank, and JP Morgan, are working on this and other tokenization projects ranging from digitally native structured product issuance to tokenized government bonds and foreign exchange transactions.

When it comes to financial service activities using DeFi applications, one of the key questions from financial institutions and regulators alike is how participating entities will mitigate financial crime risks. As policymakers debate whether and how to include DeFi within the regulatory perimeter, some DeFi protocols are proactively embracing compliance measures and demonstrating innovative ways to improve the ecosystem's overall compliance hygiene. TRM's wallet screening API, coupled with other traditional compliance tools, can boost visibility of the risks these applications face and assist in detecting illicit activity within the network.

The below case study demonstrates how one DeFi application in particular leverages TRM's risk management platform to identify and prevent illicit actors from using its services.

Summary Results:

- Nearly 10 million user wallets were screened for sanctions and AML risks between August 2022 and July 2023.
- Over that approximate time period, 590 high-risk addresses connected to illicit activity were blocked from transacting on the application interface.
- Blockchain intelligence tools like TRM enable clearer visibility of the exact risk typologies facing the platform including association with child sex abuse material (CSAM) vendors, scams, and hacked or stolen funds.

Overcoming Uncertainty through Proactive Compliance Solutions

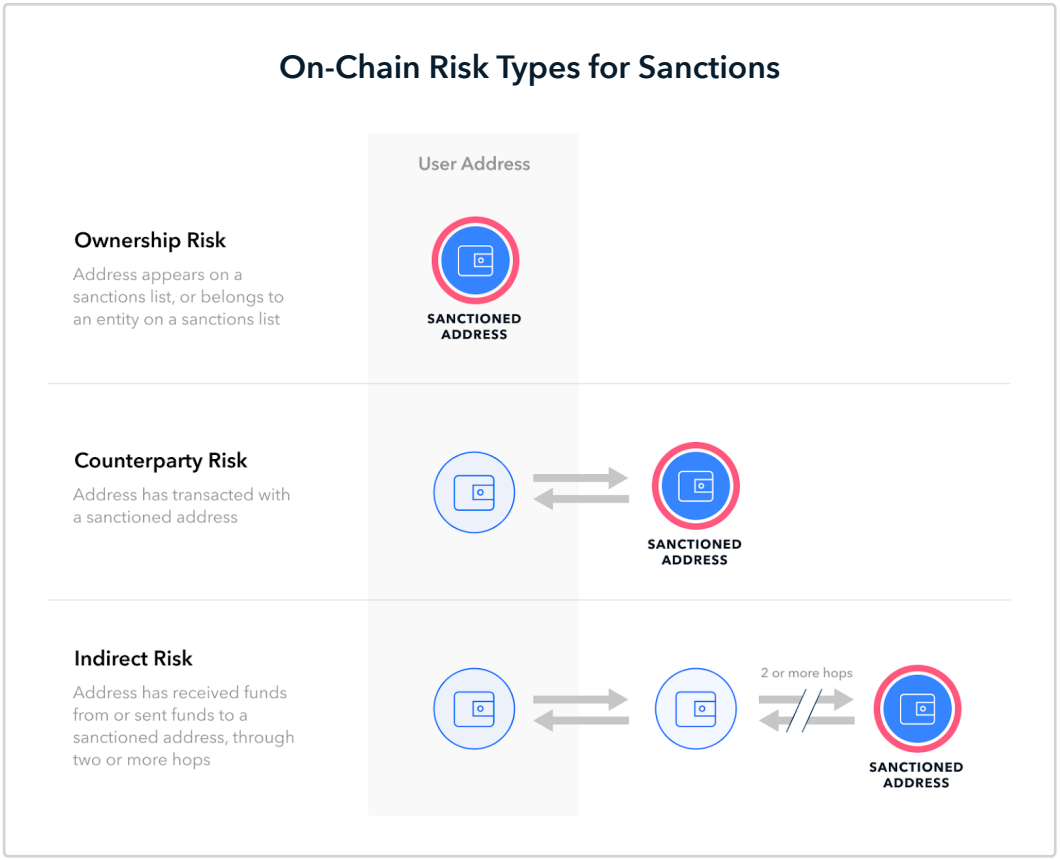
This application is among a cohort of DeFi protocols to be adopting proactive compliance measures as it looks to seize the mission to detect and prevent money laundering. The following is an example of how entities can partner with blockchain intelligence providers such as TRM to comply with sanctions and other applicable laws, limit the ability of threat actors to use DeFi networks for illicit activities and help shape the future regulatory environment.

Wallet Screening in Legacy Mode

Since many users interact with DeFi protocols from private wallets, one of the top priorities for a DeFi application is to identify AML and sanctions risks around its users, so that it can limit its exposure to risky actors and funds of potentially illicit origin. To that end, in August 2022 a DeFi protocol integrated TRM Wallet Screening, TRM Labs' on-chain AML and sanctions risks-detecting tool, to routinely screen user wallets connecting to these applications.

TRM's API enable this entity to query data about an on-chain address or transaction and flag relevant risks across various threat areas. These include sanctions, terrorist financing, hacked or stolen funds, known hacker groups, ransomware, scams, human trafficking, and child sexual abuse material (CSAM). In requesting this data from TRM, the protocols sends only the blockchain address – and no further identifiers – to TRM, whose API returns a risk scoring to indicate:

- Whether an address is owned or associated with a sanctioned entity or other forms of illegal activity ("ownership risk");
- Whether an address has transacted with a sanctioned address or one that is associated with other forms of illegal activity ("counterparty risk").

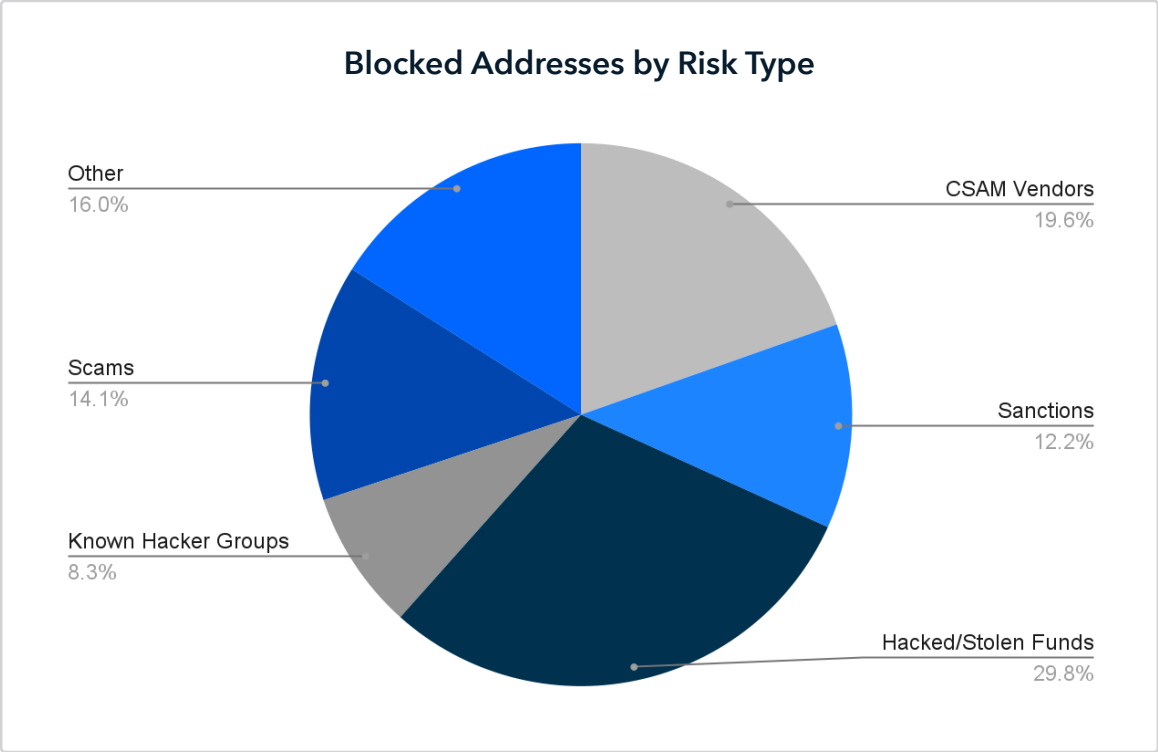


Based on the risk factors detected by TRM's API around any specific wallet address, the protocol can proactively and automatically block the user in question from connecting to the service. In essence, the protocol is performing a form of transaction monitoring, with the added advantage of never permitting illicit actors from conducting financial transactions in the first instance. This stands as an interesting analogy and distinction to traditional fiat-based transaction monitoring, which is generally done retroactively after transactions have already been effected.

Improved Safety Profile and Enhanced Visibility of Risk Landscape

The DeFi application's implementation of compliance tools across its products and services is transforming its visibility of financial crime risks associated with its users and their funds, as well as the overall security of its platform. Before implementing TRM's Wallet Screening, illicit actors could access its platform to trade assets. However, between August 2022 and July 2023, TRM's API screened more than 9.7 million user wallets, which resulted in the interface blocking 590 addresses from accessing its services. blocked addresses, according to the DeFi network's data.

TRM Wallet Screening also sharpens the DeFi network's understanding of the exact types of risks associated with funds and users connecting to its interface. While traditional financial institutions attempt to do this in annual risk assessments, it is challenging and often involves speculative assumptions. Among the various risks detected by TRM's API, those linked to child sex abuse material vendors, scams, hacked and stolen funds were the most prevalent among the addresses that were ultimately barred from the interface. Ownership and/or counterparty risks linked to these threat areas accounted for almost 64% of the risks identified around the blocked addresses, according to the DeFi network's data.



Next Steps for Compliance Programs

Despite successfully banning hundreds of bad actors from its platform, the DeFi network is currently exploring further ways it can uplift its compliance program to protect its business from tainted funds and contribute to a safer DeFi system as the regulatory environment takes shape. Options under consideration include the possible adoption of additional transaction monitoring controls and investigation software, with a view to potentially obtaining a VASP license further down the line.

As financial institutions grapple with increasing scrutiny and evolving regulatory obligations with blockchain technology, this DeFi network's proactive approach is a reminder of how industry can lead the way to help define its future operating context and embark on a path of continued compliance improvement.