



Web3 AML Solution

Prevent Money Laundering From Smart Contract Scams On Your Platform

Solidus Labs is changing the way crypto businesses approach AML risk. With HALO Threat Intelligence, crypto businesses can avoid being exposed to AML risk by continuously monitoring fraudulent funds derived from smart contract scams.

Reduce regulatory compliance risk exposure by uncovering hidden scams across smart contracts and liquidity pools. Deploy hyper-specialized crypto-native detection typologies uniquely developed by Solidus Labs to block malicious actors from off-ramping before they even enter your platform, eradicating risk with a fraction of the effort. Safeguard your crypto business and your users from this emerging on-chain threat.

Prevent the execution of scams on your platform

Identify scam addresses sending funds from hot wallets on your platform. Be alerted when a scam is taking place and an illicit actor is engaging with your platform.

Prevent money laundering of fraudulent funds on your platform

Identify and be alerted to scam addresses depositing funds to hot wallets on your platform to flag users that have executed scams and are laundering the proceeds.



What are Smart Contract Scams?

Smart contract scams are token smart contracts that have been coded to steal funds. They exist on the blockchain and are automatically executed. With the growing adoption of DeFi, smart contract scams have become more prevalent. They often go undetected, and serial scammers are able to execute thousands of small value scams without raising flags.

Crypto businesses are required by regulators to monitor their platforms to ensure they are not being used to facilitate money laundering or for illicit finance. Smart contract scams utilize these platforms to further their illicit activity as an off-ramp or as a means of money laundering. It is crucial that crypto businesses continuously monitor transactions to ensure they are not exposed to smart contract scams in order to meet regulatory requirements.



Identify Scams at Scale & Before Execution

Threats from fraudulent crypto tokens and smart contract scams often arise unexpectedly, and the strategies and schemes they use are continuously evolving. Traditional blockchain analysis companies identify smart contract scams **after** they have been executed. They are alerted to them by crypto businesses, victims, and law enforcement.

This approach makes it difficult for them to identify smart contract scams at a large scale and it is impossible for them to identify them before execution. Using our groundbreaking technology, HALO Threat Intelligence uncovers wallets and smart contract addresses for scams. It assesses hundreds of relevant data attributes, leveraging smart linking, to draw insights from over a billion historical transactions executed on our network.

This industry-first AML approach determines if addresses have deployed scam token contracts or if a scam exists but has yet to be executed. Flagging suspected addresses, continuously monitoring addresses of interest, and constantly enriching and updating our HALO Threat Intelligence database allow us to respond quickly to emerging threats & trends at scale.

A traditional Blockchain analysis tool did not properly identify any of the top 100 scams identified by Solidus Labs.



Identify scams at scale with smart contract screening technology



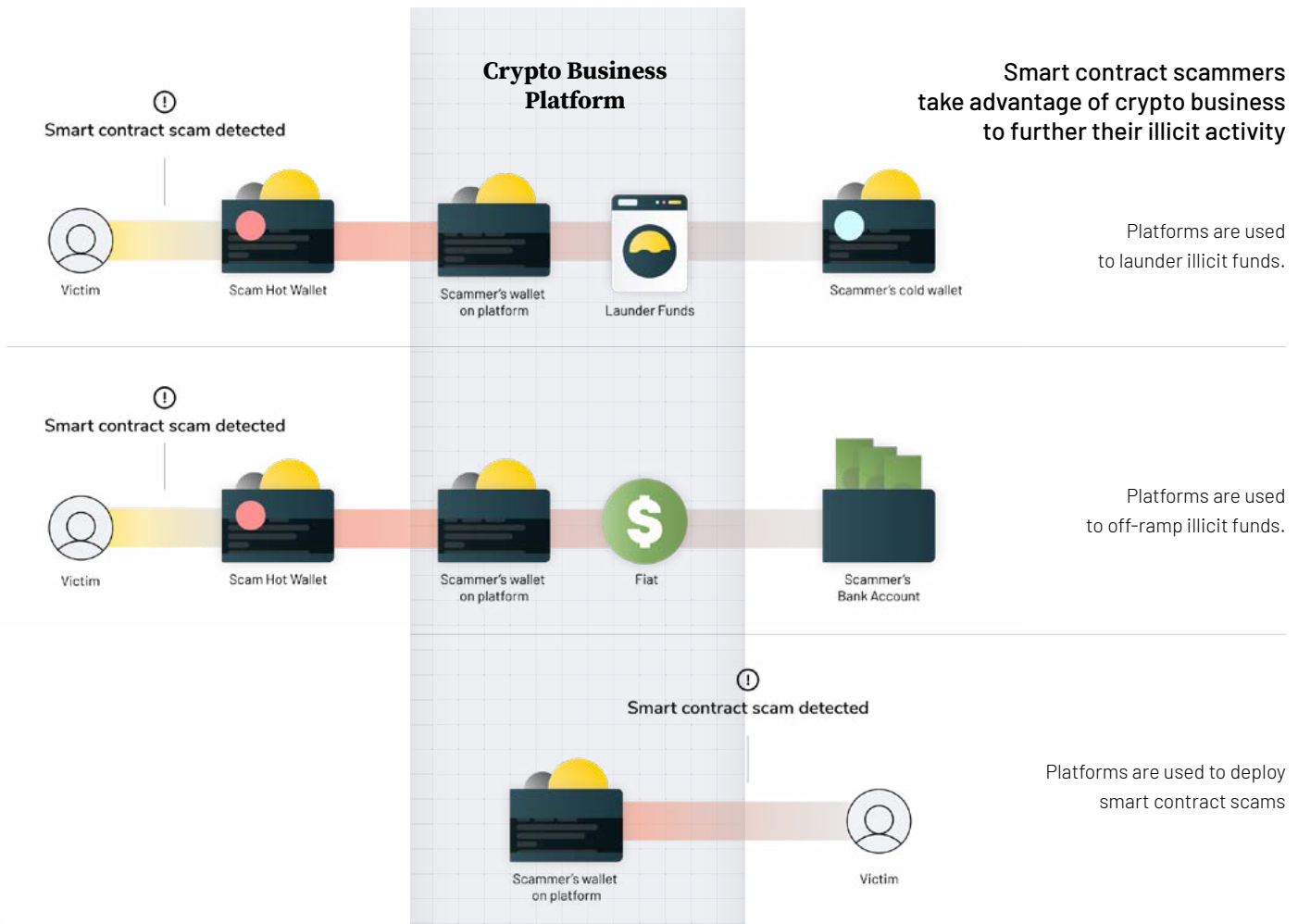
Proactively screen for scams before they are executed



Enrich your compliance tech stack with a first of its kind crypto-native AML approach



Ensure your platform is not being used by smart contract scammers



Seamlessly and Continuously Monitor Transactions on Your Platform for Smart Contract Scams

With HALO Threat Intelligence, crypto businesses can proactively protect themselves and their users from scams.

