

CipherTrace Armada™

Cryptocurrency Risk Controls for Banks

In 2021, bank examiners and FinCEN will focus on virtual currency exposure when assessing the effectiveness of bank AML programs. Financial institutions must be able to identify institutional and peer-to-peer virtual currency-related transactions and understand how their institutions interact with emerging virtual asset service providers (VASPs).

Virtual currency money laundering risk mitigation requires specialized tools to identify and report potentially suspicious activity.

“...banks must be thinking about their crypto exposure as well...If banks are not thinking about these issues, it will be apparent when examiners visit. ”

-FinCEN Director Blanco, September 2020

CipherTrace Armada™ provides critical visibility for banks to reduce risks and:

- Monitor payments to and from over 1,100 VASPs
- Onboard and manage VASP customer risks
- Detect more than 3,700 digital asset customers
- Adopt a risk-based approach to virtual currency AML
- Implement policies based on VASP KYC deficiencies and money laundering risk

CipherTrace cryptocurrency intelligence delivers the highest quality competitive advantage on two critical dimensions—superior data and advanced analytics.

CipherTrace anti-money laundering analysts collect and collate hundreds of millions of blockchain data points to produce the most extensive attribution data on over 800 cryptocurrencies. This attribution data is continuously processed by advanced analytics to de-anonymize legitimate, higher-risk and illicit businesses. CipherTrace blockchain analytics then accurately traces crypto flowing through exchanges, bitcoin ATMs, peer-to-peer services, money laundering services, dark markets, and ransomware.

\$2 Billion in crypto-related transactions move annually on the payment networks of a typical top 10 US bank.

Monitor for Crypto Payments with Traditional Transaction Tools

CipherTrace Armada is tightly integrated with leading AML tools including Nice Actimize, Caseware Alessa, BAE, Worldsys and Featurespace to identify VASP payments without installing additional software. CipherTrace cryptocurrency intelligence feeds can be in rapidly added to most modern transaction monitoring deployments. With thousands of digital asset companies emerging, financial institutions cannot afford not to have the most comprehensive cryptocurrency intelligence available.

Grading VASP KYC Processes

By analyzing and probing the Know Your Customer (KYC) processes of over 800 VASPs in more than 80 countries, CipherTrace identifies VASPs with demonstrably deficient KYC processes that could be exploited by money launderers, criminals, and extremists. The CipherTrace Attribution Team tests all VASPs using a standardized criterion and rates them as weak, porous, or strong based on how easy it would be to launder money through the VASP after opening an account.

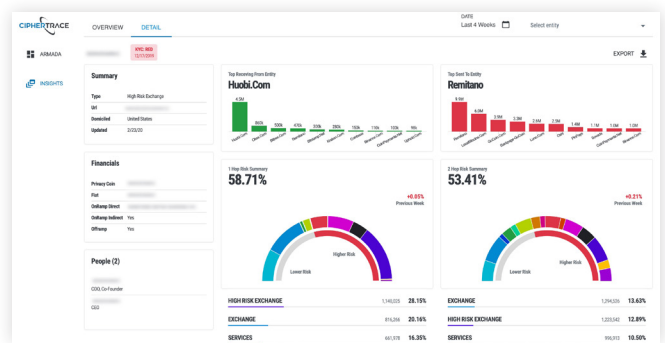
66% of the Top 800 VASPs Have Demonstrably Weak KYC

Many digital asset entities obscure the nature of their business to avoid de-risking by banks. Unregistered MSBs and P2P schemes selling crypto for fiat using bank accounts frequently falsify Merchant Category Codes and provide incorrect industry details, making them challenging to detect. Armada data feeds accurately match payments to higher risk VASPs and peer-to-peer MSBs using legal identifiers, aliases, and bank account numbers to produce the highest catch rate.

VASP Risk Monitoring

CipherTrace Armada™ visually displays VASP risk profiles based on KYC effectiveness, risky transactions, illicit activity and enables enhanced due diligence on VASPs.

- Profile VASP KYC and money laundering risks
- Audit and monitor transaction risk exposure
- Perform enhanced due diligence on digital asset businesses
- Make risk-based decision based on how well VASPs know their own customers



Armada VASP Risk Insights creates risk profiles for each VASP and monitors for interactions with high risk entities, such as dark markets and criminal actors.

Crypto Risk Advisories and Darknet Crypto Exposure Feeds

CipherTrace provides customized payments fraud intelligence on bad actors using cryptocurrencies to sell stolen account credentials, prepaid cards, credit card dumps, ATM skimmers, and phishing kits. Stay up to date with actionable advisories on emerging crypto crime, cryptocurrency-related malware and ransomware threats to your financial institution.

8/10 top US banks unknowingly harbor illicit crypto MSBs.

About CipherTrace | CipherTrace develops cryptocurrency anti-money laundering (AML)/counter-terrorist financing (CTF), blockchain forensics, crypto threat intel and regulatory solutions. Leading exchanges, banks, auditors, regulators and digital asset businesses use CipherTrace to comply with regulatory requirements, investigate financial crimes, and foster trust in the crypto economy. Founded in 2015 by experienced Silicon Valley entrepreneurs with deep expertise in cybersecurity, eCrime, payments, banking, encryption, and virtual currencies, CipherTrace is backed by top venture capital investors and by the US Department of Homeland Security. For more information, visit: www.ciphertrace.com