



Cryptocurrency risk mitigation for financial institutions and regulators

Ciphertrace Armada helps financial institutions, payment providers, and regulators identify and mitigate risk associated with crypto-related transactions in and out of Virtual Asset Service Providers (VASPs) by providing detailed VASP information, a anti-money laundering (AML) risk score, KYC grade, and in-depth analysis. Armada empowers institutions to uncover virtual currency-related transactions for use in AML risk and fraud models by mapping legal names and bank account numbers associated with VASPs. With Armada, users can view, filter, sort and drill down on VASP risk- and fraud-related data points, such as customer identification (KYC) processes, domiciled location and transactional risk profiling.

Complete crypto counter-party intelligence, including bank accounts and credit card identifiers

Ciphertrace Armada associates a wealth of legal names, bank account numbers and credit card identifiers to hundreds of VASPs. Though financial institutions have policies in place to prevent their clients from interacting with risky crypto entities, Ciphertrace routinely uncovers billions of dollars in crypto-related transactions every month.

Comprehensive risk assessments based on real interactions

Ciphertrace's team of expert analysts interact with hundreds of VASPs opening accounts, depositing funds, running transactions and withdrawing funds. Through these interactions, Ciphertrace gains unique insight into the risks presented by these VASPs. Ciphertrace evaluates KYC practices, support of privacy assets, fiat on- and off-ramps, domiciled locations, and regulatory data, each contributing substantially to risk.

Analysis of counter-party relationships for enhanced due diligence

Ciphertrace's immense repository of attribution data ties crypto addresses to real-world organizations, sanctioned entities and events. Armada aggregates this data to reveal top custodial VASP counterparties and the percentage of VASP client funds flowing to and from risky entities, such as criminals, dark markets and gambling sites.

Powerful, easy to use VASP Risk Monitor application

Armada's VASP Risk Monitor allows users to view, filter, sort and drill down on VASP risk data points. Easy-to-understand, exportable reports enable users to analyze historical data and trends to inform future decision-making. Armada also contains components that educate as you go, revealing details of geographic risk, terms definitions and other information.

AML and fraud detection

Ciphertrace Armada provides data feeds that can be easily integrated into NICE Actimize, SAS, NetReveal, SIRON, Alessa, FeatureSpace and other leading fraud and AML solutions, helping better identify potentially suspicious and fraudulent activity.

Mobile-friendly interface

Ciphertrace Armada supports Chrome, Firefox, Safari and Edge browsers on any screen size, including mobile iOS and Android devices.

A complete solution

Ciphertrace is the only crypto-analytics company to provides a complete, native crypto compliance and forensic solutions suite. Armada complements and enhances Ciphertrace Sentry, Inspector, and Traveler to identify counterparty risks, comply with compliance regulations, perform required counterparty due diligence and perform detailed investigations. Armada is also used to extend and provide additional insights for Mastercard Crypto Secure clients, allowing them to dig deeper into risk factors and explore broader crypto and fraud ecosystems. Ciphertrace is a 314(b) certified organization.

The screenshot displays the Ciphertrace Armada interface for a specific VASP. The interface is divided into several sections:

- Summary:** Shows KYC status as Green, Category as Exchange, and Active status as 12/31/2008. It also lists the domiciled region as North America.
- Top Received From (BTC):** A bar chart showing the top 10 sources of BTC received, with Binance.com being the largest at 43 BTC.
- Top Sent To (BTC):** A bar chart showing the top 10 destinations for BTC sent, with Binance.com being the largest at 100 BTC.
- Received High Risk (BTC):** A donut chart showing 3.71% of received BTC is high risk. A table below lists categories like Exchange (92.51%), Services (2.78%), and Criminal (1.94%).
- Sent High Risk (BTC):** A donut chart showing 4.36% of sent BTC is high risk. A table below lists categories like Exchange (89.79%), High Risk Exchange (3.39%), and Wallet (3.17%).
- Banks:** A section for bank account details including bank name, account number, and routing.
- Crypto Assets:** A table of asset types with Yes/No indicators for Custodial, Privacy Coin, Fiat, Direct Onramp, Indirect Onramp, and Offramp.
- People (1):** A list of individuals, including the Chief Executive Officer.

About Ciphertrace

Ciphertrace, a Mastercard company, delivers scalable crypto asset intelligence solutions that help identify and mitigate crypto risk across the entire ecosystem. Powered by fully auditable and independently verified data attribution, our insights help make crypto safe and secure, while navigating ever-changing global regulations.