CIPHERTRACE

CipherTrace Armada

Full Suite of VASP Risk Monitoring and Due Diligence

Banks and other financial institutions now need to be aware of the pervasive presence of virtual asset service providers (VASPs) in their customer accounts and on payment networks. VASPs, as a class of financial institution, are experiencing intense regulatory pressure and scrutiny in the EU, US and other G20 countries.

CipherTrace Armada™ provides Financial Institutions (FIs) with the critical visibility into risky cryptocurrency blind spots, working with existing monitoring tools to identify transactions with digital asset entities and helps manage AML risks from. Its suite of investigative tools enables enhanced due diligence on VASPs.

Significance of VASPs in Bank Payment Networks and Customer Accounts

Under most AML regulatory regimes, money transmitters dealing in convertible virtual currency—such as cryptocurrency exchanges or Bitcoin ATM operators—are considered non-bank financial institutions (NBFIs). FATF identifies these digital asset entities as Virtual Asset Service Providers (VASPs). Although the complete definition of VASP extends beyond being a virtual asset money transmitter, the conversion between virtual assets and fiat makes these digital asset entities of particular interest to banks. It is important to both identify any VASP counterparties in customer transactions and the VASPs attempting to hide the fact that they are digital asset customers at your institution. Failure to identify these digital asset entities can lead to operational, legal, financial, reputational, and counterparty risks.

CipherTrace Armada ensures banks have insight into all digital asset entities that may be operating in their payment networks or transacting with their customers. Identifying previously undetected VASP third party transactions can significantly increase the volume of domestic wires, international wires, ACH and cross-border ACH transactions that now require increased monitoring or controls due to increased risk.

CipherTrace Armada Helps Mitigate VASP Risks

- Flags high-risk payments between banks and VASPs
- Reveals risk associated with hundreds of VASPs—including deep intelligence into their Know Your Customer (KYC) and AML practices
- Identifies illicit MSBs and P2P schemes using bank accounts
- Reveals dark market sales of bank cards, prepaid products, and compromised retail and corporate accounts
- Enables banks to manage risks related to VASP, which includes the ability to safely bank lucrative cryptocurrency exchange customers
- Highlights higher risk VASPs that trade privacy coins and fiat currency

Lack of Visibility Creates Payment Fraud and Compliance Exposure for Banks

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

55% of the top 400 VASPs lack good KYC.

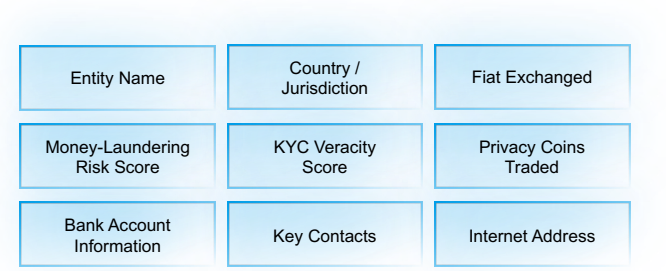
Full Suite of Virtual Asset Risk Feeds and Intelligence

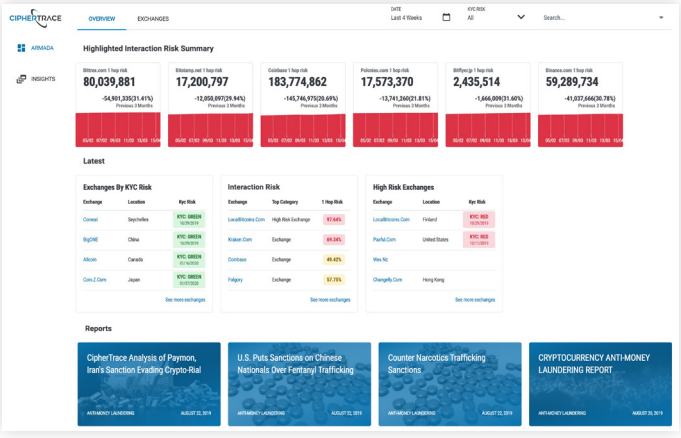
Powered by the world's leading cryptocurrency intelligence and blockchain analytics, CipherTrace Armada delivers a full suite of crypto-related monitoring solutions specifically developed for financial institutions. The Armada modules monitor risky third party transactions, flag money laundering and terrorist financing activities in your payment networks, and more.

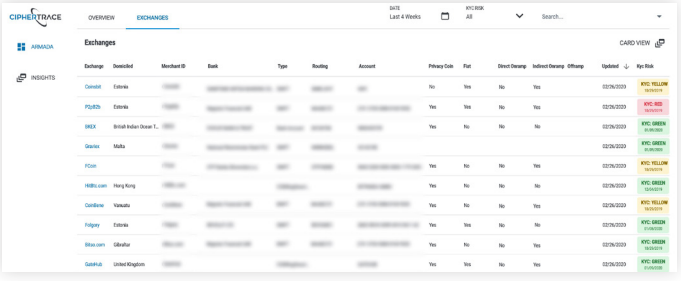
VASP Risk Feed

CipherTrace VASP Risk Feeds help your institution reveal and monitor hidden payments to and from VASPs in order to enhance your AML and Know Your Customer (KYC) compliance. These feeds are delivered via CSV for easy integration with your existing transaction monitoring system.

- A comprehensive CipherTrace knowledgebase and matching file allows you to match your internal transactional and customer records to detailed profiles of hundreds of VASPs, including CipherTrace's exclusive KYC/AML practices rating, domiciled jurisdiction, percentage of interactions done with risky entities, fiat on- and off-ramp capabilities, acceptance of privacy coins, key personnel, and other dimensions of risk.
- Works with your existing systems to link SWIFT and IBAN routing numbers and Bank Account Numbers and Merchant IDs, so that banks can reveal hidden inflows and outflows linked to the crypto-world
- Highlights risky transactions with VASPs
- Flags VASPs for enhanced due diligence
- Scores AML risk and KYC processes of VASP customers and counterparties (Know Your Customer's Customer)
- Monitor Payments and quantify Transfers with risky VASPs. Crypto transactions can be identified and linked to credit card, debit card, ACH, and Wire systems.





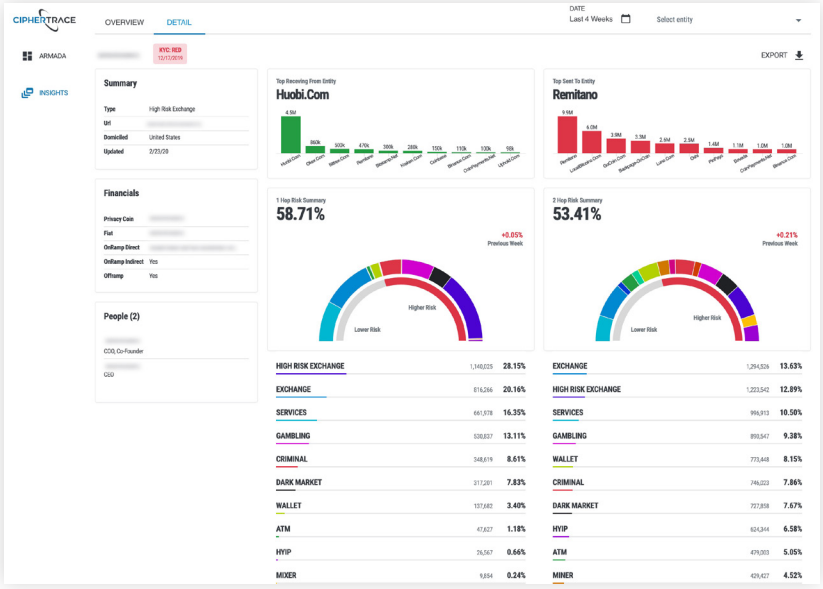


VASP Risk Monitoring and Reports

Comprehensive and timely risk monitoring on over 500 VASPs allows banks to easily see the evolving risk profile of any VASP.

This data includes the top entities with which each VASP has engaged, the percentage of top interactions to and from each entity, and the number and percentage of "risky" entity interactions, such as those with criminals, dark markets, gambling sites (which are often used for money laundering), high-risk cryptocurrency exchanges, HYIPs, Mixers, and Malware and Ransomware-associated addresses. By mapping blockchain addresses to real-world entities, CipherTrace de-anonymizes many transactions on the blockchain, thus providing much-needed visibility into an institution's participation in the crypto economy.

- Works together with the VASP risk feeds to provide even deeper insight into potential direct and indirect exposure to aid KYC efforts
- Reveals the effectiveness of VASPs' AML and KYC practices
- Enables FIs to make more informed decisions for actions on customer payments coming to or from higher-risk VASPs
- Empowers banks to commercialize relationships with low risk VASPs



Banking Details on Unregistered MSB Feed

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

The CipherTrace unregistered MSB Feed identifies unregistered MSBs and P2P vendors using bank accounts. Many vendors on legitimate P2P exchange sites operate as Money Service Businesses (MSBs), typically unlicensed and often with no KYC, AML, record keeping or reporting. Illicit money transmitters often hide themselves behind a personal or corporate account with a misleading name and cover story. In fact, CipherTrace research recently revealed that 8 out of 10 top US banks unknowingly harbor illicit cryptocurrency MSBs.

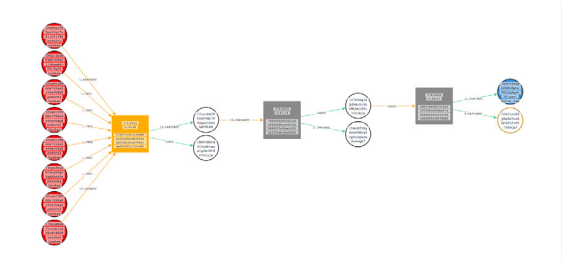
These illicit MSBs typically accept payment for cryptocurrency directly through deposits or wires into their bank account, and then transfer the crypto value to corresponding accounts at cryptocurrency exchanges. CipherTrace data identifies bank account numbers linked to illicit MSB transactions.

By providing these unregistered MSB feeds to banks, CipherTrace Arnada enables banks to work together with their existing AML systems and processes, thus helping map the account numbers and names of crypto money services businesses that may be obscuring their true nature through different false names or incorrect business models.

CipherTrace Inspector

CipherTrace Inspector's interactive user interface allows non-technical users to quickly perform deeper investigation and visualize cryptocurrency transaction flows. This capability enables investigators to follow virtual money trails without having to become cryptocurrency or blockchain experts.

- Trace movement of cryptocurrency visually
- Identity flows of illicit funds
- Monitor wallets for activity
- Create and share cases
- Perform due diligence on virtual asset customers and other virtual asset entities
- Produce admissible evidence



The CipherTrace platform's intuitive graphical interface makes it easy for both technical and non-technical users to access state-of-the-art investigation tools and analysis capabilities.

Alerts and Advisories

A subscription to the CipherTrace Crypto Threat Advisories, as well as CipherTrace's renowned Quarterly Cryptocurrency AML Reports give a financial institution visibility into the latest major trends and threats impacting the crypto asset community and financial institutions as the relationship between the two becomes increasingly intertwined.

- Receive customized payments fraud intelligence on bad actors using cryptocurrencies to sell stolen account credentials, prepaid cards, credit card dumps, ATM skimmers, and phishing kits
- Receive actionable advisories on emerging crypto crime, cryptocurrency-related malware and ransomware threats to your financial institution
- Receive advisories on hacked VASPs that may be transacting with bank customers
- Receive updates on various crypto regulation changes around the world
- Receive updates on recent sanctions and enforcement actions regarding the lack of crypto AML processes at other financial institutions

Why CipherTrace Armada for Virtual Asset Risk Mitigation?

Years of research have gone into developing the world's most complete and accurate cryptocurrency intelligence and forensics tools, covering over 100,000 virtual currencies and over 2000 digital asset entities, including 500 VASPs. This visibility into both blockchains and virtual asset businesses helps protect banks and cryptocurrency exchanges from cryptocurrency money laundering risks. CipherTrace also works with government agencies to bridge the gaps between regulation and the world of cryptocurrencies. Relying on our expert intelligence and industry-leading research ensures that Financial Institutions are enables to accurately identify and mitigate cryptocurrency risks their payment systems, allowing for informed decisions around security and compliance.

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