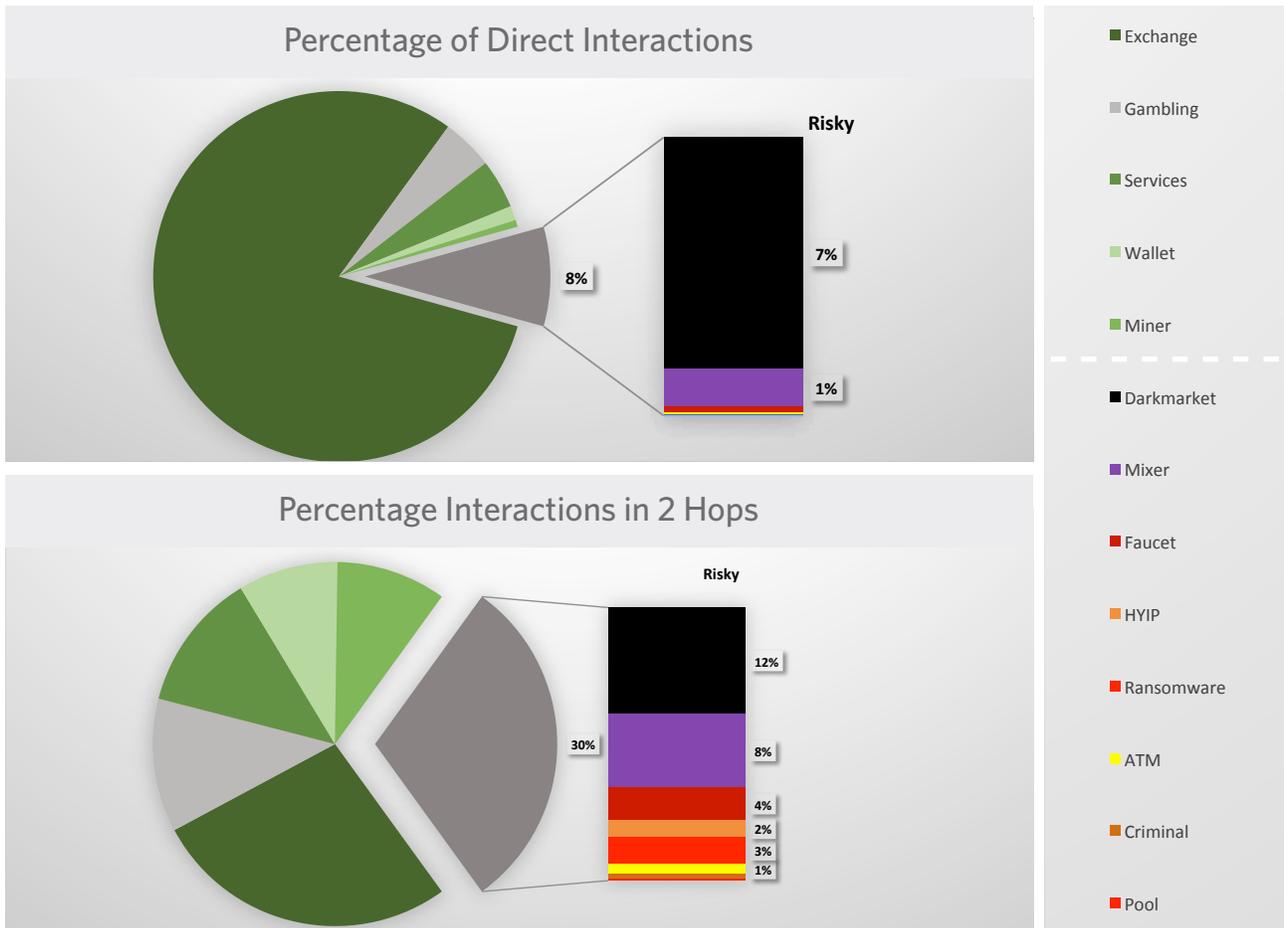


Benefits

- Understand entity risk trends
- Manage entity risk for regulators and banks
- Enforce compliance with Crypto AML/ATF regulations
- Automate supervisory tasks for regulators
- Detect transactions with illegal sources of funds
- Assure the trustworthiness of market participants

Powerful Macro View of Entity Risk

The CipherTrace Entity Monitoring Solution gives a broad, high-resolution view of the cryptocurrency transaction landscape, and uses this insight to provide risk-based intelligence to monitor and enforce regulations. It provides government regulators, banks and auditors with a powerful macro view of a crypto entity's degree of risk management, either currently or trending over time—i.e., is the exchange getting riskier, safer or staying the same. They can also access more granular views such as, for examples, monitoring the percentage of addresses that are high risk within an exchange or, within the high-risk addresses, tracking the top-10 risky activities sent and received.



Sample crypto exchange risk profile for direct interaction and interactions with two degrees of separation

Banks and other financial institutions can use these views to accept DAB customers so they are free to accept avoiding the need to turn away, de-risk, lucrative corporate banking customers in the crypto sector. Examiners and auditors can use this crypto intelligence to advise clients on risk levels associated with customers or potential customers.

Attribution Information Provides an Accurate, 360-Degree View of Risk

CipherTrace analysts integrate both open- and closed-source intelligence—while the solution’s automated crypto intelligence leverages machine learning algorithms to aggregate and correlate a variety of indicators—and then rapidly provide users with actionable analytics. This capability helps government regulators and banks to efficiently react to potentially dangerous entities, including digital asset businesses, and monitor risky sources of funds.

CipherTrace analysts add, on average, more than 1.5 million attributions each week. The solution integrates attribution data from CipherTrace’s intelligence gathering and analyst team, private intelligence sources, and open-source intelligence, OSINT. This data is collected from:

- Proprietary CipherTrace discovery algorithms and analysts
- Public sources
- Honeypots and other active capture sources
- Trusted communities, including law enforcement and regulators
- CipherTrace Crypto Recovery Network
- APWG eCrime Exchange (eCX)



CipherTrace intelligence identifies and scores a variety of AML risks

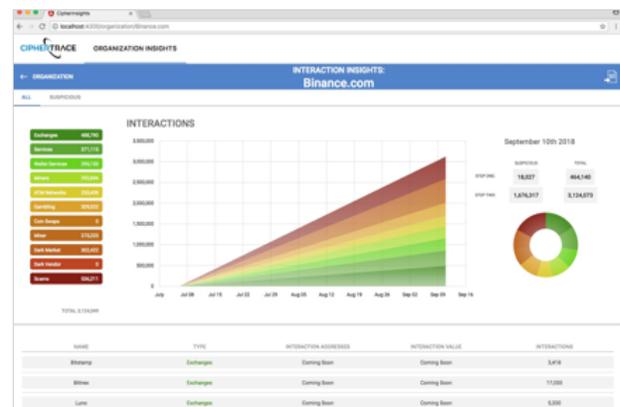
CipherTrace Crypto Intelligence Analyzes and Scores a Variety of AML/ATF Risks

Machine learning algorithms, advanced statistical analysis, and clustering techniques distill meaning from this massive data lake, resulting in a high-resolution view of the cryptocurrency risk landscape. This view spans everything from dark markets to hundreds of global exchanges, delivering actionable intelligence for AML/ATF investigation and compliance monitoring.

CipherTrace’s big data, machine learning, and advanced analytics automate risk scoring of transactions and exchanges. For government regulators and auditors, the solution provides an easy-to-use graphic interface that allows non-technical users to see the level of crypto risk and the causes of the high risk scores.

Calculate Risk Levels for Transactions and Rate the Risk of Crypto Exchanges

CipherTrace algorithms calculate risk levels for exchanges, addresses, wallets and other entities based on associating suspicious addresses and wallets. CipherTrace also profiles hundreds of global exchanges, ATMs, mixers, money laundering systems, gambling services, and known criminal addresses to score transactions and assess risk. It then assigns risk levels to transactions based on activity related to suspicious addresses and wallets.



About CipherTrace | CipherTrace develops cryptocurrency Anti-Money Laundering, bitcoin forensics, and blockchain threat intelligence solutions. Leading exchanges, banks, investigators, regulators and digital asset businesses use CipherTrace to trace transaction flows and comply with regulatory anti-money laundering requirements fostering trust in the crypto economy. Its quarterly CipherTrace Cryptocurrency Anti-Money Laundering Report has become an authoritative industry data source. CipherTrace was founded in 2015 by experienced Silicon Valley entrepreneurs with deep expertise in cybersecurity, eCrime, payments, banking, encryption, and virtual currencies. US Department of Homeland Security Science and Technology (S&T) and DARPA initially funded CipherTrace, and it is backed by leading venture capital investors. For more information visit www.ciphertrace.com or follow us on Twitter @ciphertrace.