

Crypto Threat-Intel™ for Banks

Expose Emerging Money Laundering Risks and Concealed Cryptocurrency Threats

Whether it is unnoticed in your ACH, SWIFT, wire or credit card payments, transferred to clients' offshore accounts, or received from unregistered money service businesses (MSBs), you need to recognize your cryptocurrency risk exposure. Every day, bad actors funnel illegal gains through hundreds of unregulated cryptocurrency service businesses and into the banking system. Essentially, this new asset class is more pervasive—and the ecosystem more diverse and geographically dispersed—than most traditional financial services companies are aware. By leveraging years of research and relationships with regulators and law enforcement, CipherTrace Crypto Threat-Intel™ delivers powerful insights to help you discover, mitigate, manage, and properly report this unwanted or illegal activity.

Accurately accessing crypto asset risk exposure is essential for financial institutions to thrive. However, once cryptocurrency enters into the equation, banks and other financial institutions face a completely new set of challenges, including:

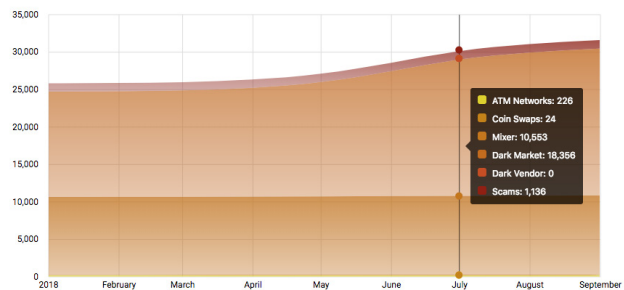
- Limited visibility into how much fiat currency flows to and from the various cryptocurrency exchanges
- Banking customers acting as *defacto* unregistered MSBs using cryptocurrencies
- Difficulty verifying the source of funds by individual or by country
- Deposits of funds derived from cybercrime activities
- Transfers of cryptocurrency to exchanges located in risky countries
- Difficulty identifying higher-risk cryptocurrency customers
- Monitoring employees' participation in crypto asset markets

CipherTrace Crypto Threat-Intel

CipherTrace Crypto Threat-Intel delivers a threat intelligence service for financial institutions that includes:

- Anti-money laundering (AML) data feed for use in ACH, SWIFT, wire and credit card networks
- Details on emerging cryptocurrency-related malware and ransomware threats
- Details on Dark Market product sales that target banks
- Risk ratings of 400+ cryptocurrency exchanges and the countries where they operate

PAYMENTS



Risky payments to a representative cryptocurrency exchange

Mitigating cryptocurrency-related business risk also requires a completely new form of intelligence to address this aggressive and hidden threat vector. Years of research, blockchain surveillance, cybercrime prevention and cryptocurrency investigation make CipherTrace uniquely positioned to deliver this intelligence. As an active participant in the blockchain ecosystem, CipherTrace maintains deep relationships with law enforcement and regulators around the globe.

CipherTrace helps banks, brokerages and funds understand and reduce risks associated with this pervasive yet nearly invisible new asset class.

Enhanced cryptocurrency transaction filtering

One challenge common to most financial service companies is identifying cryptocurrency exchanges that rapidly come and go. In this “Wild West” of the emerging crypto economy, banks and financial institutions have trouble ensuring they are not inadvertently sending funds to or receiving funds from unregistered money service businesses.

As a leader in crypto AML solutions, CipherTrace curates the most comprehensive database of cryptocurrency exchanges and their operational status. This includes sourcing risk data by opening and operating accounts at exchanges globally, making it possible for CipherTrace to provide first-hand assessments of their respective Know Your Customer (KYC) and AML practices. In addition, CipherTrace analysts continuously scour open, dark and deep web sources for fresh information on new exchanges and money laundering services in the cryptocurrency ecosystem—a rough-and-tumble environment that is evolving in blockchain time.

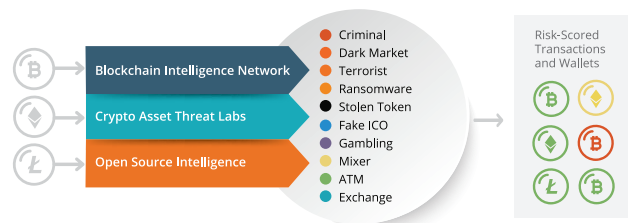
Good intelligence on bad actors

CipherTrace Crypto Threat-Intel provides threat intelligence about criminal actors who use cryptocurrency to sell stolen credentials, credit card dumps, ATM skimmers, malware, zero-day exploits and phishing kits that may impact a bank or its customers. This intelligence includes information such as their websites, handles, IP addresses and even locations.

CipherTrace researchers also actively participate in the dark side of the blockchain ecosystem by paying ransomware and dissecting malware code. The information gleaned from these activities is augmented with open and private data feeds that are carefully curated by expert analysts.

Crypto AML data feed mitigates cryptocurrency risks latent in funds transfers

Often banks are not aware of cryptocurrency flows in their networks that may involve money laundering. CipherTrace Crypto Threat-Intel features an AML data feed for the ACH, SWIFT, wire and credit card payments of a bank’s business to identify funds being transferred from or to cryptocurrency businesses—which may include money laundering services.



CipherTrace Crypto Threat-Intel identifies and scores a variety of AML risks.

The Crypto Threat-Intel service complements this data feed with risk ratings of businesses involved in cryptocurrencies for use in the existing AML and compliance side of the business. Plus, the CipherTrace service gives subscribers quarterly reports. These deep dives examine the most pressing threats such as, for example, enumerating the characteristics of most known forms of ransomware extortion and malware.

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.