CIPHERTRACE

CipherTrace Scout

Financial Investigations and Blockchain Forensics

Cryptocurrency De-anonymization Enables Successful Investigations and Prosecutions

CipherTrace provides a suite of powerful and easy-to-use de-anonymization tools for law enforcement. Investigators use this integrated platform to obtain solid evidence on individuals who use Bitcoin to launder money, finance terrorism, or carry out drug dealing, extortion and other crimes. The intuitive CipherTrace visual environment allows even non-technical agents and analysts to easily identify and trace criminals who attempt to use Bitcoin on the internet to conceal their illicit activities. The platform also supports de-anonymization for Ethereum.

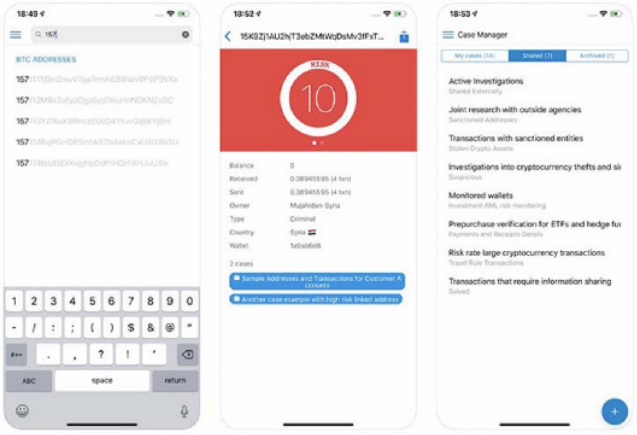
Investigate Potential Risks More Deeply

CipherTrace'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.

CipherTrace helps law enforcement follow digital money trails for crimes such as:

- Data extortion
- Money laundering
- Terrorist financing
- Cyber attacks
- Human Trafficking
- Weapon sales
- Drug transactions
- Ransomware schemes

Investigators simply enter any Ethereum or Bitcoin address into a search interface, and the mobile app determines if tokens are tainted through ransomware transactions, dark market purchases, or other criminal activities. The app instantly delivers a risk classification based on the relative risk of transactions related to the address. The app also displays the address balance, the amount received and sent, and the total number of transactions. Users can sort transactions by owner, type, and country, and investigators can tag specific individuals, companies or addresses according to their case status.

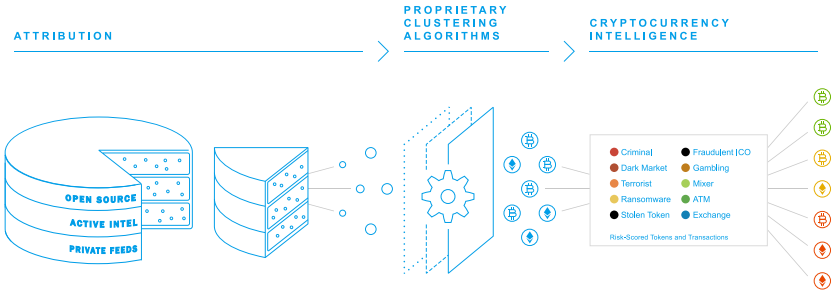


CipherTrace Scout instantly delivers cryptocurrency risk ratings to field agents.

Superior Attribution and More Accurate Threat Assessment

CipherTrace identifies risky attributes of crypto addresses, wallets, and related businesses participating in Bitcoin transactions—such as mixers, ransomware, and dark markets. This attribution requires applying sophisticated data science and big data analytics to blockchain-based transactions.

CipherTrace curates an enormous repository of attribution data, adding on average 1.5 million new data points each week. This data is derived from extensive open and closed-source intelligence gathering, which includes active participation in the crypto economy by CipherTrace researchers.



Proprietary clustering algorithms de-anonymizes crypto businesses to risk rate transactions.

High-Quality Attribution

Profile types and attribution collection methods include:

1. CipherTrace Crypto Asset Threats Labs
2. Active profiling of many blockchain ecosystem entities
3. Managing crypto money pots
4. Dark market sites and deep web sites
6. Monitoring investment scams and fraudulent ICOs
7. Tracing stolen cryptocurrencies
9. Confirmed attribution directly from CipherTrace trusted users
10. Anti-Phishing Working Group (APWG) eCrime Exchange

Risk-Scoring of Transactions and Entities Within the Global Blockchain Ecosystem

CipherTrace profiles hundreds of global exchanges, ATMs, mixers, money laundering systems, gambling services, and known criminal addresses. CipherTrace then assigns risk levels to transactions, wallets and entities based on known associations with suspicious addresses and nefarious geographic locations.

Advanced Algorithms Enable High-Quality Attribution

The CipherTrace high-quality attribution information platform applies advanced big data analytics—which leverages proprietary clustering algorithms—to cluster data points within the expansive attribution repository. The result is a broad, cataloged, high-resolution view of the cryptocurrency transaction landscape.

This CipherTrace high-quality attribution information platform can rapidly aggregate and correlate a variety of indicators, and then provide users with risk assessments and actionable intelligence. In addition, these extensive attribution capabilities help investigators gather implicating evidence more quickly.

Integrated Case Management

A Case Manager gives investigators a convenient way to save research, replay searches, export investigation reports, and collaborate with other agents. This feature also allows agents to perform bulk uploads of large quantities of cryptocurrency addresses for investigation.

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