Using Blockchain Analysis to Fight Crime

Criminals and rogue nations may believe they can hide behind cryptocurrency and blockchain transactions, but blockchain analysis makes that more difficult. **Don Spies,** *Director of Market Development for Chainalysis, discusses how law enforcement agencies can use this cutting-edge technology to fight crime.*

What opportunities do blockchains present for law enforcement agencies?

Cryptocurrency offers an unprecedented opportunity to quantify and investigate financial crime. Cryptocurrencies are the first global payment system outside of any single organization's control, and their blockchains create permanent public records, or ledgers, of illicit activity. Although crime makes up a small subset of a much larger cryptocurrency market — one percent — it remains significant. For example, cryptocurrency is used for money laundering, terrorist financing, darknet markets, child abuse material, ransomware, scams and more. Fortunately, the transparency afforded by blockchains helps law enforcement weed out bad actors. This will help build trust in blockchains and pave the way for mainstream uses of cryptocurrencies.

What is blockchain analysis and how are law enforcement agencies using it?

Blockchain analysis helps people interpret the public blockchain ledgers. With Chainalysis tools, government agencies can understand which real-world entities transact with each other on these public ledgers. For example, we can show that a given transaction took place between two different cryptocurrency exchanges or between a cryptocurrency exchange and an illicit entity, such as one conducted by a sanctioned individual or organization. With blockchain analysis tools and exchanges' know your customer (KYC) information, law enforcement can gain transparency into blockchain activity in ways that aren't possible in traditional finance.

Discuss the use of blockchain analysis in other areas of the justice system.

It's a burgeoning field, and use cases are still being discovered. The unique nature of this is that blockchains are completely open. Anyone can go to a blockchain ledger website and see all the data that's there. Depending on the scenario and the blockchain analysis tools used, organizations can follow the money on the blockchain, monitor transactions for suspicious activity and anti-money laundering compliance, and obtain profiles of cryptocurrency businesses. Information gleaned from blockchain analysis can be used in a court of law.

Are there hacking or other security issues associated with blockchains and cryptocurrency?

To my knowledge, no one has ever hacked the major coins, such as Bitcoin. Hacking the technology underlying cryptocurrency, which is the blockchain, would require an amount of computing that doesn't exist right now. What's important to understand is there are on-ramps and off-ramps in coin infrastructures like exchanges that can be compromised if they're not properly configured. Having said that, stolen funds can be traced. You literally can see where funds go on the blockchain, because everything is open.

What should organizations look for in a blockchain analysis solution?

It comes down to having the right data and making it actionable. Specifically, law enforcement should be interested in a partner with data attributing services, which attribute addresses to the clusters — that is, the entities — that control them. In this case, that would be clusters associated with criminal activity and their cashout points.

The historical data behind this capability is an important differentiator. Chainalysis is the only company that has systematically collected information that links real-world entities to blockchain transactions since 2014. This allows the software to accurately distinguish different clusters of entities and attribute more data than can be seen on the blockchain.

What is the biggest misconception about cryptocurrency?

Cryptocurrency's decentralized, semi-autonomous nature makes it uniquely appealing to criminals, and their embrace of the technology has helped shape its overall reputation. But in fact, unlike cash and other traditional forms of value transfer, cryptocurrency is inherently transparent and easier to trace. Every transaction is recorded in a publicly visible ledger. With the right tools, we can see how much of all cryptocurrency activity is associated with illicit activity.

Learn more at **Carah.io/Law-Enforcement-Chainalysis**

Myth: Cryptocurrency is untraceable.
Fact: Chainalysis empowers investigators to follow illicit funds on the blockchain.

Chainalysis helps identify the services behind the majority of transactions on cryptocurrency blockchains. Law enforcement and intelligence agencies have used Chainalysis to take down notorious darknet markets, a child exploitation ring, and help address national security threats around the world.
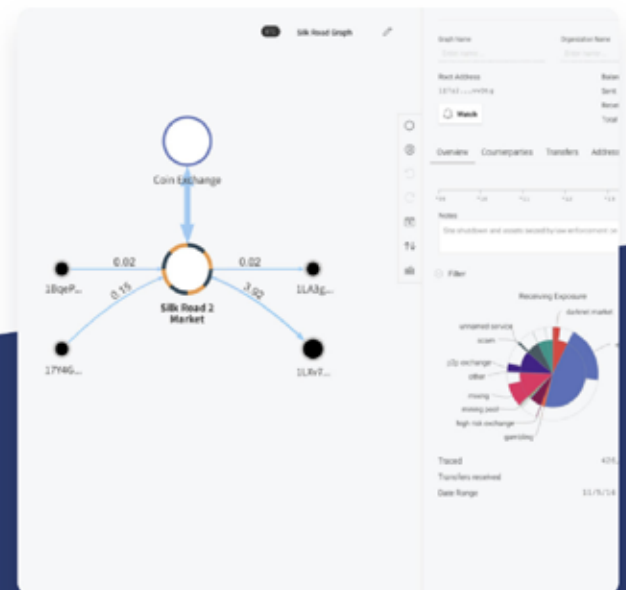
🔍 Enter an address, a transaction, or service name to understand who controls funds

⌥ Create graphs showing cryptocurrency activity using our intuitive interface

Ⓑ Conduct investigations covering 90% of cryptocurrency market value, with new coins added all the time

For more info, or to request a demo email: naps@chainalysis.com