

SUBSCRIBE

FINANCIAL

As cryptocurrencies grow, so does the demand to track their users

(Duncan Rowlinson / Flickr)



Patrick Howell O'Neill Nov 13, 2017 | CyberScoop

If bitcoin is a roller coaster ride with dizzying heights and rapid drops, one thing is clear: The original cryptocurrency carnival keeps attracting new riders. The price is up, trade volume is rising and new money buys in daily.

As a result, the business of bitcoin surveillance is booming. Governments are just barely coming to terms with how bitcoin works, but they want track newer cryptocurrencies like Monero and Zcash that were designed for anonymity beyond what's available with bitcoin.

Elliptic, a United Kingdom-based financial technology startup, launched with one basic goal: Trace bitcoins, identify illegal activity and sell ongoing visibility to governments and private companies to track the currency's movement.

This is possible because bitcoin is inherently transparent, with every unique transaction published on a public ledger, known as the blockchain, that anyone can access. Successfully analyzing the blockchain has become big business.

Police use Elliptic's technology to investigate crime. Banks use it for compliance so they can more comfortably do business with bitcoin exchanges while watching for money laundering and other illicit activity. The company took a \$5 million [investment](#) round last year. Chainalysis, the other big player in cryptocurrency forensics, is contracted by the IRS to sniff out bitcoin-using tax cheats.

As newer cryptocurrencies begin to creep up, law enforcement agencies want the same capabilities targeting the newer technology.

Launched in 2014, Monero is a cryptocurrency built fundamentally built to be private and untraceable. Zcash, a much-hyped 2016 addition to the cryptocurrency world, [boasts](#) similar privacy goals and is designed by a team of highly-respected academics in the U.S. and Israel.

“I absolutely think Monero is going to change how cybercriminal payments are made,” Flashpoint analyst Olivia Rowley told CyberScoop. “In terms of actually bringing cybercriminals to court, it’s all about privacy. That’s the whole point of Monero. It’s going to make investigations a lot trickier.”

“Monero in particular [is gaining adoption],” said Andrew Lewman, previously the director of Tor and now a vice president at the dark net intelligence firm Dark Owl. “One or two [criminal] marketplaces have played with Zcash but Monero is becoming much more popular and there is a marketplace that only does Monero now because bitcoin is easy to trace through the blockchain.”

Bitcoin remains by far the king of cryptocurrency. The price of one bitcoin now tops \$7,000 and the total market cap is nearing \$115 billion. Newer cryptocurrencies are rising, however, because they offer truly distinct technology: increasingly private transactions that appeal to a range of users including, unmistakably, cybercriminals.

“The vast majority of illicit activity in cryptocurrencies is still taking place in bitcoin,” Tom Robinson, Elliptic’s co-founder and chief data officer, told CyberScoop. “Having said that, we are seeing growing interest in more anonymous cryptocurrencies. Dark marketplaces are beginning to accept Monero in particular, as are some strains of ransomware. The Shadow Brokers hacker group, which infamously released exploits developed by the NSA, has sold further exploits for Zcash and Monero.”

Before police shut it down, AlphaBay made history as perhaps the biggest dark web marketplace to accept Monero. Now some markets, like Libertas, accept only Monero. At other sites, users have been calling on market administrators to offer newer, more private cryptocurrency options.

In recent months, Elliptic has been giving talks and pitching potential government customers on the new generation of cryptocurrencies.

“This is naturally leading to increased interest from law enforcement agencies, and we are working with them to address these threats,” Elliptic’s Robinson said.

It’s still early days for both Monero and the companies that exist to track it. The trajectory is clear but law enforcement, who are still largely grappling with bitcoin, will need time to grasp the newer coins hitting the markets.

“I think [rise in demand] is just started,” DarkOwl’s Lewman said. “The most sophisticated national agencies know what bitcoin is and how to use it but the vast majority of law enforcement still thinks bitcoin is ransomware or just some criminal thing that they don’t really understand yet.”

Despite the many advantages the more anonymous cryptocurrencies can offer, the fact they remain far less popular than bitcoin is a major hurdle. Tracking the specific coins and transactions is difficult, but it’s far easier to spot when a coin like Monero is bought in the first place. Once you do buy it, Robinson says, it’s bound to attract attention.

Another underlying problem is the only way for most people to buy Monero is to use bitcoin. That brings us back to square one with bitcoin surveillance and forensics which just so happens to be Elliptic's core focus and big money maker.

"I believe that the biggest challenge for the privacy-focused cryptocurrencies will be to achieve and maintain sufficient scale and liquidity," Robinson said.

"At the moment simply using one of these currencies puts you at risk of being suspected of illicit activity, to a greater extent than for a user of bitcoin. Regulators are beginning to appreciate that cryptocurrencies are not all alike, and have varying risk profiles when it comes to money laundering and illicit use. I suspect that some exchanges have already chosen not to list these currencies, for compliance reasons."

It's a cycle with no foreseeable end. As bitcoin becomes more popular, governments' and banks' interest intensifies, and they pay for better tracking technology. As bitcoin's inherent transparency becomes more obvious, some people become increasingly interested alternative coins that "fix" the transparency problem. The direct result is governments and private firms becoming more interested in tracking technology for those coins.

-In this Story-

[Andrew Lewman](#), [bitcoin](#), [Chainalysis](#), [dark web](#), [Elliptic](#), [Flashpoint](#), [Libertas](#), [Monero](#), [Tom Robinson](#), [Zcash](#)

RELATED NEWS

FINANCIAL

Day trader indicted for...

by **Patrick Howell O'Neill** • 6 days ago

FINANCIAL

Survey: About a quarter...

by **Shaun Waterman** • 1 week ago

FINANCIAL

Whole Foods says it has...

by **Zaid Shoorbajee** • 3 weeks ago

[ABOUT](#)

[SPONSOR](#)

[RSS](#)

© 2017 Scoop News Group | All Rights Reserved