Bloomberg Law

Securities Regulation & Law Report™

Financial Institutions

Law Enforcement Adapts to Using Cryptocurrency to Catch Criminals

Law enforcement agencies are turning to blockchain to track everything from financial crimes to drug trafficking, even as they're still learning how to use the distributed-ledger technology.

The accessible nature of a public blockchain — an open database that can exist on millions of computers designed to allow for reliable transactions among anonymous users — is particularly appealing to law enforcement, which doesn't need a subpoena or search warrant to access it.

But the nature of blockchain also makes it difficult to identify real-world users, particularly those who use sophisticated techniques to hide their identities or those who rely on more obscure cryptocurrencies that provide greater anonymity.

''Law enforcement is at the very beginning of the learning curve of dealing with these technologies,'' Jerry Brito, executive director of Coin Center, told Bloomberg BNA.

A blockchain is a distributed database that is used to maintain a continuously growing list of records, called blocks. Each block contains a link to a previous block and a time stamp.

Benefits Several aspects of blockchain, which allows Bitcoin and other digital cryptocurrency to exist, make it a useful law enforcement tool, said Jason Weinstein of the Blockchain Alliance, a partnership between cryptocurrency companies and federal agencies including the Justice Department, FBI, and the Commodity Futures Trading Commission.

Law enforcement doesn't have to worry about whether the data might disappear in the future since the blockchain ledger is permanent, Weinstein told Bloomberg BNA. The fact that the ledger is publicly accessible and exists across borders means no subpoena, search warrant, or permission from foreign governments is required to access the data.

''It lets us see, in a very public way, the movement of those funds, and it lets us trace those funds,'' former Assistant U.S. Attorney Kathryn Haun who served as the Justice Department's digital currency coordinator until departing the agency last month. Haun is now a member of the board of directors of Coinbase, an operator of cryptocurrency exchanges.

In addition to looking for suspicious transaction patterns, law enforcement can use blockchain software for evidence tracking. CryptoSeal, a technology owned by Chronicled, the San Francisco-based blockchain and connected device technology company, is a tamper-evident seal. The seal has a cryptographic chip within it, that when tampered with, will not verify through a blockchain.

Challenges The biggest challenge remains identifying criminals who are trying to stay anonymous. In the case of Bitcoin, for example, every user has a unique identity, but they aren't fully associated with a person's real-world identity.

''If somebody is making a drug buy on some dark corner and they're using cash, you're not going to have any way of tracking the use of that cash. That's not the case with the use of a cryptocurrency like bitcoin,'' Scott Dueweke, president of the Identity and Payments Association, told Bloomberg BNA.

Identifying Criminal Activity Software, like that made by Chainalysis and Elliptic, can be used to see if there are patterns in the movement of Bitcoin and if Bitcoin identities are connected to known persons. Those connections are usually made by following the blockchain to an outside regulated exchange where someone is exchanging Bitcoin for money. Those regulated exchanges typically have to know the real-world identity of the person.

Although law enforcement can figure that out on their own, software can make it faster for them to know which exchange to go to.

Using the Bitcoin blockchain, the FBI investigated Ross Ulbricht, the creator of the online black marketplace Silk Road, and Trendon Shavers, who ran a Ponzi scheme using Bitcoin.

Law enforcement in the Czech Republic and Japan have also charged Tomas Jiříkovský, who is suspected of laundering money through Bitcoin, and Mark Karpeles, who is charged with fraud and embezzlement.

The difficulty of identifying users is likely to become only more so as criminals turn to a newer generation of cryptocurrencies, like Zcash and Monero, which are designed to provide more privacy and anonymity, according to Dueweke.

''Law enforcement is going to be increasingly challenged to identify the users of those cryptocurrencies that are designed to be more anonymous than bitcoin,'' Dueweke said.

Training for Law Enforcement Law enforcement needs to adjust to using these new technologies by building up a workforce that can use and apply it, according to Alan Cohn, counsel to the Blockchain Alliance.

 ISSN 0037-0665

''One of the challenges is overcoming and realizing this is just like any other kind of evidence,'' Haun said. Part of the problem is that only the cyber units are getting trained on cryptocurrencies and the darknet, but that these issues affect other units that deal with narcotics and firearms, Haun said.

It's a ''question of shifting resources'' to teach more people about tracking cybercrime, Haun said at a June 8 hearing held by the House Financial Services Subcommittee on Terrorism and Illicit Finance.

BY SHIRA STEIN

To contact the reporter on this story: Shira Stein in Washington at sstein@bna.com

To contact the editor responsible for this story: Seth Stern at sstern@bna.com

  SRLR ISSN 0037-0665