Editor: Pavel Gladyshev, pavel.gladyshev@ucd.ie

Cryptocurrencies—A Forensic Challenge or Opportunity for Law Enforcement?

An INTERPOL Perspective

Giannis Tziakouris | INTERPOL

The anonymous and decentralized nature of cryptocurrencies has turned them into a powerful weapon in the cyber-arsenal of national and international criminal groups by facilitating their illicit activities while evading prosecution. This has baffled the international law enforcement community, with a large number of cryptocurrency-related investigation cases received on a monthly basis by INTERPOL.

Cryptocurrencies and Crime

Cryptocurrencies have been used extensively in darknet markets for receiving payments for illicit services such as distributed denial of service; malware binaries; botnets; and the purchase of illegal products including weapons, drugs, and falsified or stolen documents. In particular, darknet markets such as Silkroad, AlphaBay, and Hansa were reaping large profits, with the last reaching $3,000,000 between September 2015 and December 2016.[1]

Furthermore, it is important to note their use by extremist groups to facilitate the trade of illicit products (for instance, stolen antiquities, drugs, and firearms), remit money to areas that are under high financial scrutiny or embargo, and publicly crowd-fund their operations.

Money laundering through cryptocurrencies is another major challenge for law enforcement. A significant number of criminals have established cryptocurrency exchanges or initial coin offering (ICOs) with the goal of laundering illicit profits. A few well-known money laundering cases include the Bitcoin exchange OKCoin with hundreds of thousands of US dollars laundered[2] as well as the case of BitInstant, in which an estimated sum of more than $1,000,000 was laundered for Silk Road market customers.[3]

Moreover, cryptocurrencies have advanced the operations of various malware families such as ransomware, with CryptoLocker and CryptoWall receiving 133,045.9961 BTC and 87,897.8510 BTC, respectively;[4] cryptojacking, with Jenkins-Miner earning its operator over $3,000,000 worth of Monero;[5] and crypto-stealing Trojans, such as CryptoShuffler, which stole hundreds of thousands of US dollars by targeting the contents of volatile memory—that is, the clipboard.[6]

Another method through which criminals exploit the blockchain is by injecting arbitrary encoded data chunks (for instance, pictures) in non-standard Bitcoin transactions to disseminate child exploitation material.[7] The biggest challenge for law enforcement agencies here is

Copublished by the IEEE Computer and Reliability Societies

the immutable nature of the blockchain that disallows the removal of embedded illicit content.

Furthermore, there has been a significant rise in ICO exit scams where criminals persuade their victims to buy large numbers of fake coins, subsequently disappearing with millions of dollars.

Lastly, cryptocurrencies are used for sponsoring nation-state attacks, as a number of countries around the world are highly affected by the existence of contemporary hybrid-war strategies.

Adapting Law Enforcement and Criminal Strategies

As cryptocurrencies are associated with a plethora of crime types such as narcotics, firearms, money laundering, terrorism, and child exploitation, the international law enforcement community, including INTERPOL, has begun to focus on mastering the blockchain. In doing so, a significant amount of resources has been allocated for the exploration of the use of cryptocurrencies by criminals as well as the development of proprietary analytical tools for tracing cryptocurrency transactions.

In policing, two different schools of thought exist, with the first perceiving cryptocurrencies as a threat and the second viewing them as an investigational opportunity. The first group considers cryptocurrencies a disruptive solution enabling criminals to facilitate their illegal activities in the absence of policing, hence calling for its prohibition. On the other hand, a small yet growing law enforcement community views cryptocurrencies as an investigation opportunity where criminally associated information is now publicly and permanently indexed in the blockchain to be analyzed for the extraction of valuable forensic data that can lead to attribution and prosecution.

In recent years, there has been significant effort from both the industry and various law enforcement agencies, including INTERPOL, to develop forensic tools and methodologies for the analysis of various cryptocurrencies, with the majority focusing on the Bitcoin network. The vast focus on the analysis of Bitcoin transactions can be attributed to the substantial number of criminal cases affiliated with it, despite the existence of more anonymous cryptocurrencies. The increase in the value of Bitcoin and its wide adoption by markets (which offers easy entry and exit points) have played a catalytic role in boosting the magnitude of the criminal cases and trends associated to it. Despite the wide adoption of bitcoins by criminals, the recent success stories of contemporary analytical tools that allowed police investigators to partially de-anonymize the Bitcoin network and reveal the identity of criminals have caused a shift in the use of cryptocurrencies. An increasing number of criminals are using Bitcoin only as an entry and exit point; in the interim, they trade their bitcoins for more anonymous cryptocurrencies, in particular, Dash, Monero, Zcash, PIVX, Verge, and Namecoin.

It is imperative for law enforcement agencies to co-evolve with the current state of the art and identify and thwart online criminal activities that are linked to cryptocurrencies.

Law enforcement considers the aforementioned cryptocurrencies highly disruptive due to their enhanced anonymity, which makes them an effective weapon for criminals. Dash and Zcash enable users to keep their activity history and balances private, which ultimately restricts law enforcement investigators from identifying and tracing suspicious transactions. Similarly, Monero uses ring signatures, ring confidential transactions, and stealth addresses to obfuscate the origins, amounts, and destinations of transactions. Furthermore, PIVX implements the Zerocoin protocol that converts public PIV into anonymous PIV (aka zPIV) to conceal the pseudo-identity of the sender or any traces that can lead to the real identity of the sender. Verge is another anonymous cryptocurrency that leverages the wraith protocol to enable its users to switch between public and private ledgers. When the wraith protocol is turned on, the transaction data is hidden. Finally, Namecoin does not share the same strong anonymity characteristics or goals as the cryptocurrencies above but is still identified as a potential threat to policing due to its feature that allows criminals to anonymously register illegal websites without providing any personal information, thus preventing investigators from identifying the administrators behind these pages.

As an extra layer of protection (despite the enhanced level of privacy offered by the aforementioned cryptocurrencies), many criminals use crypto-mixing/tumbling services or decentralized P2P exchange markets to "clean" their "tainted" coins, making it increasingly difficult for police investigators to follow their transactions.

To counteract the illicit use of cryptocurrencies, law enforcement is now focusing on the development of advanced solutions for tracing criminally linked transactions. In particular, police agencies work toward developing forensic tools for the analysis of various computing

devices for the identification of cryptocurrency-related artefacts, such as wallets, and cryptocurrency hashes; fingerprinting tools for identifying the use of mixers/tumblers in cryptocurrency transactions; clustering solutions for the aggregation of the addresses belonging to the same criminal actors for better attribution; and cross-ledger tracing tools to support the association of suspicious transactions in different blockchains.

In addition to the current work by law enforcement on a national level, INTERPOL acts as an information hub on the international level by bringing police investigators from various nations, researchers, and blockchain developers together to share best investigation practices and forensic tools for cryptocurrencies. Moreover, INTERPOL works toward developing the investigation capabilities of its member countries by delivering advanced hands-on trainings on cryptocurrencies. INTERPOL strives for innovative solutions by seeking partnerships with the public and private sectors, including cybersecurity and cryptoanalytic companies. INTERPOL held its first international Darknet and Cryptocurrencies Working Group in March 2018 to further stimulate discussions surrounding policing solutions for cryptocurrency-related crimes, identifying Altcoins and cross-ledger investigations as the biggest challenges for law enforcement.

Despite the numerous challenges that the international law enforcement community faces when investigating cryptocurrencies, a number of investigation opportunities do exist. The blockchain is here to stay due to the wide use of cryptocurrencies by investors, adopters, and pioneers. While it is anticipated that a large number of its characteristics will significantly adapt in the near future to overcome critical technological shortcomings such as its size and scalability, its use for illicit activities will only continue to grow. It is imperative for law enforcement agencies to co-evolve with the current state of the art and identify and thwart online criminal activities that are linked to cryptocurrencies. For better efficacy in combatting cryptocurrency-related crime, an implementation of an international understanding and a legal framework to regulate it should be considered; this will enable law enforcement to access information for criminally linked transactions and urge cryptomarkets and exchanges to enforce strong KYC (know your client) policies. However, while its purpose is to apprehend criminals, actions taken by policing should not tamper with the confidentiality, integrity, and availability attributes of the blockchain and the development of other innovative solutions. ■

References

1. "OnionScan Report: Reconstructing the Finances of Darknet Markets through Reputation Systems," Mascherari Press, 2018; https://mascherari.press/onionscan-report-forensic-finances-dark-markets.
2. "Bitcoin Exchange OKCoin Fined in Money Laundering Case," Gautham, 15 Aug. 2016; https://www.newsbtc.com/2016/08/15/china-okcoin-exchange-fined.
3. J. Pagliery, "Bitcoin Exchange CEO Arrested for Money Laundering," CNN Tech, 28 Jan. 2014; http://money.cnn.com/2014/01/27/technology/security/bitcoin-arrest.
4. M. Conti, A. Gangwal, and S. Ruj, "On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective," arXiv: 1804.01341v4 [cs.CR], 27 Apr. 2018.
5. M. Osena, "Cryptocurrency-Mining Malware: 2018's New Menace?," Trend Micro blog, 28 Feb. 2018; https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-malware-2018-new-menace.
6. "CryptoShuffler: Trojan Stole $140,000 in Bitcoin," Kaspersky Lab Daily, 31 Oct. 2017; https://www.kaspersky.com/blog/cryptoshuffler-bitcoin-stealer/19976.
7. R. Matzutt et al., "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin," RWTH Aachen University, Germany.

Giannis Tziakouris is a digital crime analyst at INTERPOL. Contact at g.tziakouris@INTERPOL.INT.