Cryptocurrencies and money laundering investigations

Federico Paesano
Senior Financial Investigation Specialist

When I first started talking about cryptocurrencies and money laundering with my counterparts at INTERPOL and Europol back in 2014, the subject filled a tiny niche.

There was basically only one cryptocurrency (Bitcoin), only one case to discuss (Silk Road) and only 20 of us in a small room at the University of Basel. Regardless, we decided to co-found a Working Group on Cryptocurrencies and Money Laundering. We could sense something big was happening and law enforcement needed to be ready to face the challenge.

Today, thousands of people apply to attend our annual Global Conference on Criminal Finances and Cryptocurrencies. There are hundreds of new cryptocurrencies and other innovative forms of virtual asset – such as non-fungible tokens – and soaring numbers of money laundering cases that require investigators to enter the crypto sphere.

Global regulators are also taking the topic more seriously. The Financial Action Task Force (FATF), the global anti-money laundering watchdog, has issued updated standards and guidance on virtual assets and virtual asset service providers (VASPs), and is closely monitoring countries' progress in compliance.

What kind of crimes involve cryptocurrencies?

Cryptocurrencies have many legitimate uses and benefits, including their potential to provide a cheap, fast, accessible and international payment system to millions of unbanked people worldwide. But like any store of value, they can be misused.

Some cases involve criminals using cryptocurrencies to launder "normal" proceeds of crime or corruption. A simple example is a corrupt official receiving bribes and trying to hide the origin of the money by transferring money in and out of various cryptocurrencies and fiat currencies, such as dollars.

Mostly, though, we're talking about crimes that generate profits in cryptocurrency. As described in Europol's Internet Organised Crime Threat Assessment (IOCTA), cryptocurrencies are used to facilitate payments for various forms of illicit activity.

This includes the trade in drugs and other illegal goods on the dark web, ransomware like WannaCry, kidnapping and ransom payments, and cyber-crime.

Following the virtual money – easier in some ways, more challenging in others

The blockchain technology behind cryptocurrencies theoretically makes it easier for financial investigators to "follow the trail of the money". Why? Because each transaction is recorded permanently in a shared ledger – the blockchain – that cannot later be altered or falsified. The money trail will theoretically stay there forever, ready to become evidence even years later.

This is not the same for cash transactions, for example. It is impossible to rewind time and see who gave what to whom.

Bitcoin transactions include the time and amount of the transaction, plus the sender and receiver's addresses (pseudonyms in the form of long alphanumeric strings of characters). In contrast, smaller and more privacy-focused cryptocurrencies such as Monero and Zcash conceal this information.

What's tricky in all cases is *attribution*: linking transactions and addresses to real people in the real world. In other words, identifying potentially criminal transactions and the criminals behind them.

Breaking through the shield of anonymity

Luckily for investigators, there are techniques to penetrate the apparent anonymity of cryptocurrencies and link transactions and addresses to suspected criminals and money launderers.

For example, heuristics can be used to create clusters, i.e. groups of addresses which are likely controlled by the same entity. Special techniques are then applied to de-anonymise those clusters.

This is where blockchain analysis firms can help. For a fee, they can analyse addresses and transactions to obtain critical information such as geolocation data or the cryptocurrency exchange that was used to purchase the coins.

Investigators can then request further details from the exchange, just as they would from a bank or other payment provider. As the FATF's above-mentioned standards on VASPs are rolled out through national legislation, we hope and expect that more reliable data on their customers will be made available to competent authorities.

The cost of consulting a blockchain analysis firm could be a barrier in countries with limited resources for law enforcement.

However, in fact most investigations involving cryptocurrencies start with the suspect, not with a mysterious transaction or an anonymous address. Investigators are simply trying to find out which cryptocurrency addresses a suspect controls. This information can often be revealed through forensic analysis of the suspect's devices, without the need to consult a blockchain analysis firm.

Prosecuting cases – why expert witnesses are handy

The relatively new and fast-evolving nature of virtual assets means that blockchain technologies such as cryptocurrencies are not commonly understood.

This holds true among law enforcement and judicial officers, who may need to interpret evidence from blockchain analysis or digital wallets in order to convict a suspect.

In this case, it is helpful to call an expert witness to clarify and verify such evidence in court. Of course, a clear explanation of the investigative steps followed will also help to demonstrate to the court that the resultant evidence is just like any other evidence of financial crime.

Recovering stolen assets held in cryptocurrencies

Assets held in cryptocurrencies can be treated just like assets held in bank accounts or real estate. For example, a judge can issue an asset freezing

order on a cryptocurrency account, pending the outcome of the case.

Given that cryptocurrency transactions can be made in just a few minutes, however, international cooperation on asset freezing really needs to speed up. Even for regular bank transfers, in the time it takes to issue the freezing order, the money can have bounced around the world several times.

When it comes to confiscating and recovering assets held in cryptocurrencies, authorities – which still use national fiat currencies, although who knows what the future holds? – have a couple of options.

- One is to transfer the cryptocurrency into the relevant fiat currency through an exchange.
- Another is to hold an auction. The US Department of Justice recovered nearly USD 50 million by auctioning a hoard of illicit bitcoins after closing down the Silk Road online market in 2013.

Volatility in the value of cryptocurrencies is a headache for those in charge of recovering assets. The Silk Road auctions of 144,336 bitcoins would have generated around USD 6 billion if sold today.

What can law enforcement do?

At the 4th Global Conference on Cryptocurrencies and Criminal Finances in 2020, which was hosted by INTERPOL in cyberspace due to the pandemic restrictions, seven key recommendations emerged from the discussions.

In short, we see progress already, yet law enforcement still has a long road ahead.

A multidisciplinary approach

For example, Recommendation 5 encourages investigators to adopt a multidisciplinary approach. This translates to joint investigation teams that combine financial investigation, cybercrime and technical IT/forensic analysis expertise.

Yet many investigators still don't reach out to counterparts with such expertise, or else their institutions do not routinely convene multidisciplinary investigation or asset recovery teams. They should.

New technologies

Similarly, Recommendation 6 promotes new technologies to be applied to financial investigation of virtual assets.

Governments should support research and innovation on tools that facilitate the investigation and prevention of money laundering and terrorist financing through cryptocurrencies.

At the moment, this is mainly being done by private firms, which then charge a fee for their service to law enforcement.

Investigative strategies

Last, remember that cryptocurrencies are used by real people in the real world. Our 7th recommendation last year to adapt investigation strategies could include, for example, systematically searching suspects' premises for devices or documents that might contain details of cryptocurrency accounts.

And as the use of cryptocurrencies increases around the world, tracing transactions through the crypto sphere needs to become routine practice among investigators. For that, our law enforcement officers quickly need to upskill.

Originally published on 15 March 2021; updated 6 August 2021

All our Quick Guides are freely available on Basel LEARN in various languages. See: learn.baselgovernance.org

ISSN 2673-5229

Basel Institute on Governance
Steinenring 60
4051 Basel, Switzerland

+41 61 205 55 11
info@baselgovernance.org
baselgovernance.org

@BaselInstitute
Basel Institute

The Basel Institute on Governance is an Associated Institute of the University of Basel.