Cryptocurrencies and money laundering investigations

Federico Paesano
Senior Financial Investigation Specialist

It has been an incredible journey so far. I first heard about Bitcoin in 2010 at a cybercrime conference. We didn't know much yet, except that it was a new form of money – completely decentralised since it was not issued or controlled by any government – and that it could potentially help criminals to move and launder their proceeds across borders undetected.

How can money be decentralised? Are criminals able to convert their ill-gotten funds into bitcoins and back to fiat? Is it game over for law enforcement if the adoption of Bitcoin grows exponentially? These were our questions at the time.

The answer to the last question seemed to be a big "yes", as criminal activity in this field had begun to be detected and it still seemed impossible to investigate crypto flows on the blockchain. The use of Bitcoin appeared to be the ultimate anonymity tool.

Growing attention

When the Basel Institute on Governance decided to sit down with Europol, Interpol and another small group of investigators from different parts of the world, 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 set up a Working Group on cryptocurrencies and money laundering. We could sense that something big was happening and law enforcement needed to be ready to face the challenge.

But what a change in just a few years! 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 Central Bank Digital Currencies, and soaring numbers of money laundering cases that require investigators to enter the crypto sphere.

Global regulators are also taking the issue 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.

And in June 2023, the European Union witnessed the adoption of the most extensive regulatory framework for digital assets to date: the Markets in Crypto-Assets Regulation (MiCA).

What kind of crimes involve cryptocurrencies?

Cryptocurrencies have many legitimate uses and benefits, including the potential to provide a cheap, fast, accessible and international payment system for 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 who receives bribes and tries 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 being 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 such as Rhysida or Abyss Locker, 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 permanently recorded in a shared ledger – the blockchain – that cannot be altered or falsified later. The money trail will theoretically remain forever, ready to become evidence even years later.

The recent prosecution of an individual who stole more than 50,000 bitcoins from the defunct crypto exchange called MtGox back in 2012 illustrates this process clearly. The immutability of the blockchain gave law enforcement the ability to follow the money, identify the perpetrator and recover a record-breaking USD 3.36 billion in assets almost 10 years after the fact.

This would not be possible with 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, as well as the addresses of the sender and receiver (pseudonyms in the form of long alphanumeric strings of characters). However, smaller and more privacy-focused cryptocurrencies such as Monero 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

Fortunately 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 – groups of addresses which are likely controlled by the same entity. Special techniques are then applied to de-anonymise these 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 aforementioned 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 the investigating authorities.

The cost of consulting a blockchain analysis firm could be a barrier in countries with limited resources for law enforcement. However, most investigations involving cryptocurrencies start with the suspect, not with a

mysterious transaction or an anonymous address. Investigators are simply trying to determine 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 rapidly evolving nature of virtual assets means that blockchain technologies such as cryptocurrencies are not widely 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 the same as 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.

However, given that cryptocurrency transactions can be made in a matter of minutes, 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 may have bounced around the world several times.

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

- One is to exchange the cryptocurrency into the relevant fiat currency.

- 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 responsible for recovering assets. The Silk Road auctions of 144,336 bitcoins would have generated around USD 4.2 billion if sold today.

What can law enforcement do?

At the 6th Global Conference on Cryptocurrencies and Criminal Finances in 2022, which was co-organised by the Basel Institute and Europol and attended by more than 2,000 participants in person and remotely, five recommendations emerged from the discussions.

1. **Break down silos between "traditional" and "crypto"** – not treating crypto as a separate area, but operating across the physical and virtual domains (as the criminals do).

2. **Regulate broadly and make full use of existing laws** – to ensure that crypto assets are treated like any other asset for the purposes of AML/CFT supervision, enforcement and asset recovery.

3. **Take advantage of the blockchain to disrupt organised crime** – since the blockchain offers numerous opportunities to investigate and disrupt crime and money laundering schemes, gather intelligence and freeze and confiscate illicit assets.

4. **Raise crypto literacy through capacity building and clear communication** – cutting out the jargon and acronyms and extending basic training to wider groups of staff.

5. **Increase public-private cooperation** – since law enforcement can gain a lot from the technical skills of blockchain analysis and asset tracing companies as well as cooperate with crypto asset service providers to speed up freezing orders and information sharing.

Originally published on 15 March 2021; updated 11 August 2023.
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