Cryptocurrencies and money laundering

Federico Paesano
Senior Financial Investigation Specialist

When I and the other founding members of the Working Group on Cryptocurrencies and Money Laundering first started talking about blockchain and anti-money laundering/countering terrorist financing (AML/CFT) back in 2014, it was a tiny niche.

There was basically only one cryptocurrency around (Bitcoin), only one case of money laundering to discuss (Silk Road) and only 20 of us in a room at the University of Basel.

Now there are hundreds of people attending our annual Global Conference on Criminal Finances and Cryptocurrencies, dozens of new cryptocurrencies and soaring numbers of cryptocurrency-related money laundering cases uncovered every week.

What kind of money laundering cases involve cryptocurrencies?

Some cases involve criminals using cryptocurrencies to launder “normal” proceeds of crime or corruption. A corrupt official receiving bribes and trying to hide the origin of the money through a maze of transactions in bitcoins, for example.

Most often, though, we’re talking about crimes that generate profits in cryptocurrency. The trade in drugs and other illegal goods on the dark web. Ransomware like WannaCry. Kidnapping and ransom payments. Terrorist financing: Europol’s Virtual currencies and terrorist financing report in May 2018 describes how the terrorist group ISIS used Bitcoin and Zcash to collect donations.

More widespread awareness of how cryptocurrencies work could help financial institutions, FIUs and law enforcement authorities detect more cases more quickly – and choke off a fast-growing avenue for criminals to both gather and launder the proceeds of their crimes.

Following the (virtual) money

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 that cannot later be altered or falsified. The money-trail will theoretically stay there forever, ready to become evidence even years later.

Bitcoin transactions include the time and amount of the transaction, whereas smaller and more privacy-focused cryptocurrencies such as Monero and Zcash conceal this information.

What’s tricky in all cases is linking transactions and user accounts to real people in the real world. In other words, identifying potentially criminal transactions and the criminals behind them. It is the so-called “attribution” problem: heuristics are used to create clusters, i.e. groups of transactions which are likely done by the same entity, and then techniques are applied to de-anonymise those clusters.

Everyone can learn it – and should

Blockchain, cryptocurrencies, AML… it’s a fast-changing field, with new tools constantly being developed and upgraded to help law enforcement stay one step ahead of the criminals. The Financial Action Task Force – the inter-governmental body responsible for AML/CFT policies and supervision – is actively focused on clarifying how the standard risk-based approach to money laundering applies to virtual assets.

But for those on the front line of financial crime – police officers, compliance professionals, financial institutions – you don’t need to be an

expert. In fact, it is surprisingly quick and easy to gain the knowledge you need to detect risks and red flags involving cryptocurrencies and escalate them. Once you know what to look for, you can detect the criminal activity and take the first steps towards securing the ill-gotten funds and preserve the evidence.

And you really, really do need to know this.

Because here's the thing: whatever form cryptocurrency-enabled crime takes in the future, it is here to stay.

Want to learn more?

Full disclosure: I co-lead a two-day FinTech AML Compliance Training course in collaboration with Swiss law firm MME. It's designed to help financial institutions and FinTech/RegTech management, policymakers and compliance professionals detect and prevent the use of cryptocurrencies for illicit activities.

But however you choose to learn about blockchain, cryptocurrencies and the risks around AML/CFT, please do. Otherwise, at the next Global Conference on Criminal Finances and Cryptocurrencies in 2021, there'll be hundreds of thousands of cases, if not more.

Published on 15 March 2019
baselgovernance.org/blog/federico-paesanos-quick-guide-cryptocurrencies-and-money-laundering

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.

Basel Institute on Governance
Steinenring 60
4051 Basel, Switzerland

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

@BaselInstitute
Basel Institute