AMLCC

Compliance | Risk Management | Education

Cryptocurrency and the UK legal sector

Working with

The Law Society

The background

The past decade has seen an explosive growth in cryptocurrencies. As of 2022, there was over 10,000 different cryptocurrencies in existence with a total market value of over $1 trillion.

Since the creation of Bitcoin in 2009, cryptocurrencies have transitioned from an obscure topic on internet forums to an asset class that draws significant interest from individuals, corporations, financial institutions and governments worldwide.

The adoption of cryptocurrencies has grown rapidly, especially in the UK: we're the most active jurisdiction for cryptocurrencies in Central, Northern and Western Europe.

While cryptocurrencies can enable fast, borderless transactions, these same properties can be exploited for criminal purposes like money laundering (ML), terrorist financing (TF) and proliferation financing (PF). And where these risks exist, there's a risk for regulated professionals becoming unwittingly involved.

Chainalysis, a U.S-based block chain analytics firm, estimated that in 2022 illicit transactions totalling $20.1billion were made using cryptocurrency. Transactions linked to sanctioned entities made up 44% this activity.

This guide aims to highlight the emerging risks of cryptocurrencies related to financial crimes for UK legal professionals. It examines the features of cryptocurrencies that present ML/TF/PF risks, as well as how they specifically impact the UK legal sector.

The basics of crypto

Cryptocurrency 3

Exchanges 3

Mixers 4

Wallets 5

Privacy coins 5

Cryptocurrencies and…

Money laundering 6

Terrorist financing 7

Proliferation financing 7

What's being done 8

Recommendations for legal professionals 9

The basics of crypto

Cryptocurrency

Cryptocurrency is a form of digital or virtual currency that uses cryptography for security. Cryptocurrencies work using blockchain, a decentralised technology that manages and records transactions in what are called 'blocks'.

They're often perceived as anonymous but most cryptocurrencies, including Bitcoin, are better described as pseudonymous. This means they provide a level of privacy by masking the true identity of the users with pseudo information, typically strings of alphanumeric characters that represent the sender and receiver in transactions.

While crypto transactions can be viewed by anyone, they don't automatically reveal identifiable information about the users making those transactions. The pseudonymous nature of cryptocurrencies makes them an ideal medium for illegal activities, such as money laundering.

Exchanges

Cryptocurrency exchanges provide a platform where users can buy, sell and trade. However, exchanges have also emerged as a major area of risk when it comes to money laundering and terrorist financing.

In the UK, exchanges are now regulated by the FCA. They're required to verify customer identities, monitor transactions and report suspicious activity to authorities. Exchanges that are non-compliant or located in high-risk jurisdictions, often have less stringent AML measures in place, which can facilitate illicit money flows.

Mixers

A cryptocurrency mixer, also known as a tumbler, is a service that aims to improve the privacy and anonymity of cryptocurrency transactions. These services work by pooling together funds from numerous sources and mixing them before redistributing them to the intended recipients.

The primary objective is to obscure the trail back to the funds' original source, making it challenging to trace the transaction path on the blockchain. By blending potentially identifiable or 'tainted' cryptocurrency with others, the mixer creates a complex web of transactions. This enhanced privacy means that it could be exploited for money laundering or other illicit activities.

Wallets

Crypto wallets are a digital tool that allows users to store, send and receive cryptocurrencies, providing a user interface to interact with the blockchain. Crypto wallets work by holding public and private keys.

Public keys are the same as your bank account number, which you share with others to receive funds. The private key is what protects your public keys, similar to a password or PIN. It's used to authorise transactions and prove ownership of your blockchain address. There are several types of crypto wallets.

Software wallets are apps that can be installed onto a computer or phone. They are divided into three primary categories: desktop wallets, mobile wallets and online wallets.

Hardware Wallets are physical devices that store cryptocurrency offline; they resemble USB drives and are considered very secure since they are not connected to the internet except when transactions are being made.

Paper Wallets are simply physical documents that record your public and private keys. They are considered a form of cold storage since they are not stored digitally.

Privacy coins

Cryptocurrencies like Monero and Zcash represent one area of emerging risk related to the use of cryptocurrencies for illicit financing. These cryptocurrencies utilise cryptographic techniques like zero-knowledge proofs to obscure transaction details and provide a high degree of anonymity for users.

While privacy coins aim to provide financial privacy, the anonymity they afford also makes them attractive for criminal and terrorist activity.

Cryptocurrencies and...

Money laundering

The anonymity of cryptocurrencies makes them attractive for money launderers. Cryptocurrency transactions are recorded on a public ledger but the parties involved are only identified by wallet addresses, not real identities. This provides a layer of anonymity.

Cryptocurrencies enable money laundering through:

- **Mixing services that obscure the source of funds**
- **Transaction hopping to disguise the money trail**
- **Integration with dark web marketplaces**
- **Conversion to privacy coins like Monero**

As we mentioned earlier, Chainalysis has estimated that illicit transactions totalling $20.1billion were made using cryptocurrency in 2022 alone, with 44% of these linked to sanctioned entities.

Law enforcement is ramping up blockchain analytics to track laundered funds, with the Government consulting with private entities like blockchain analysts Chainalysis on risks and how to tackle them. But cryptocurrency remains an attractive avenue for laundering due to speed, anonymity and lack of regulation compared to traditional finance.

Terrorist financing

Cryptocurrencies enable terrorist groups and other criminal organisations looking to raise and move money without detection. They give these groups the ability to solicit donations from around the world and transfer funds across borders rapidly without going through the regulated financial system.

ISIS has used Bitcoin to receive small donations from around the globe. While each individual donation may be small, combining thousands of transactions enables ISIS to accumulate sizeable war chests.

Likewise, in 2021 The Guardian reported that the far-right US extremist groups involved in the insurrection in Washington D.C. have used the video streaming platform DLive to raise nearly $1million in cryptocurrency donations.

The Economic Crime and Corporate Transparency Bill (updated in October 2023) amended the Proceeds of Crime Act 2002 (POCA) to support the recovery of crypto-assets and counter the misuse of cryptocurrencies by terrorists.

Proliferation financing

Cryptocurrencies have already been implicated in cases involving the evasion of sanctions. Transparency International found that every month 1000s of 'money mule' accounts at crypto-to-fiat payment providers are being sold on the dark web, so that sanctioned individuals can move money anonymously into cash.

There have been a number of elaborate schemes uncovered involving North Korean hackers stealing cryptocurrency to fund the regime's nuclear and ballistic missile programs. In one such heist, the hackers used doctored videos to trick employees at cryptocurrency exchanges and companies into opening Trojan Horse documents, which enabled the theft of over $600million.

Monitoring and restricting potential cryptocurrency transactions related to proliferation remains extremely challenging. While blockchain analysis can sometimes trace the flow of funds, cryptocurrency exchanges in other jurisdictions are not always required to collect identifying information about customers. And tools like mixers and tumblers can obscure transaction details.

What's being done

Governments and governing bodies are working to strike the right balance between anonymity and enabling legitimate usage versus tracking illicit activity. Techniques have emerged to identify cryptocurrency users, despite the privacy techniques in place. Chain analysis companies specialise in linking addresses and tracking cryptocurrency flows. Law enforcement agencies also employ blockchain forensics to de-anonymise users.

Regulations are also being amended to require more compliance from cryptocurrency exchanges and institutions to collect customer information and transaction data. As well as changes to UK legislation, the EU's transfer of funds regulation and FATF's travel rule require exchanges to collect and share originator and beneficiary data on transactions.

While services such as mixers provide greater anonymity, blockchain analysis continues to advance as well to keep pace with privacy techniques.

Recommendations for legal professionals

Policies, controls and procedures (PCPs)

Your PCPs may already contain specific details on how your business deals with cryptocurrencies, whether that's accepting them as payment or identifying them as a source of funds.

If not, develop and implement written PCPs that are tailored to cryptocurrency risks. Of course, as regulations change to keep up with the developing cryptocurrency industry, you'll need to go back and make changes to your PCPs too.

It's vital that all relevant employees are also educated on these PCPs, so that they're familiar with emerging cryptocurrency trends and risks, and know how to handle them.

Due diligence

Client due diligence (CDD) is already an essential part of your onboarding duties. The emergence of cryptocurrencies presents new challenges for legal professionals in mitigating ML/TF/PF risks during this process. While the regulatory landscape is still developing, there are ways that you can protect your firm from these risks.

LSAG specifically states that, when carrying out a matter-related risk assessment, legal professionals need to ask themselves: "Does the matter involve new sources of finance – anything unregulated e.g., involving crowd funding platforms or some aspects of bitcoin/cryptocurrencies?"

In many cases, you can do the necessary research on the sources of finance yourself, especially if the cryptocurrency is one of the more common ones, such as Bitcoin. In this case, as also recommended by the SRA, if you have the client's wallet or cryptocurrency details, you can use a search engine to track down transactions.

If you're unable to determine the origin of assets, it increases the risk there's an attempt to hide the source or to circumvent the sanctions regime.

Suspicious activity reports

With PCPs in place and ongoing vigilance, legal professionals can play a key role in guarding against illicit use of cryptocurrencies.

It doesn't matter whether the figures involved total hundreds, thousands or millions worth of cryptocurrency. A SAR must be submitted if you've formed a suspicion of criminal activity that has already, or may, generate proceeds from that crime.

Though 'suspicion' is referred to in case law, it's not defined in AML legislation. However, if you need to ask yourself whether you've formed a suspicion…you probably have.

Submitting a SAR to the NCA (or an internal SAR to your MLRO, if you're not the MLRO yourself) is the best way to protect yourself and your firm from any possible consequences of being involved in a criminal investigation.

AMLCC

Compliance | Risk Management | Education

AMLCC combines first-hand knowledge & the expertise of an international network of regulated professionals & authorities, to deliver an online platform that fulfils all your AML obligations. Richard Simms, MD of AMLCC, is a regulated professional & in-demand speaker & commentator on the evolving AML landscape.

Law Society members can claim 10% off the first year's annual subscription.

Learn more about AMLCC

The AML guidance for the legal sector is designed to help legal professionals and firms comply with the AML regime. Explore the guidance

+44 (0)1455 555468

enquiries@amlcc.com

@amlcc_global

@amlcc_global

Anti-Money Laundering Compliance Company Limited

Registered Address: Alma Park, Woodway Lane, Claybrooke Parva, Lutterworth, Leicestershire LE17 5FB

amlcc.com