fscom

Expertise that adds value.

AML in Crypto Handbook

A short introduction to Anti-Money Laundering in the context of cryptoassets

Contents

Introduction

Background

As of January 2022, more than 300 million people are using blockchain-based cryptocurrencies worldwide, and over 18,000 businesses accept cryptocurrency payments. According to market experts, the blockchain's market could grow from $3 billion in 2020 to $39.7 billion by the end of 2025.

The meteoric rise of cryptoassets has brought with it a new outlet for bad actors to launder funds. In 2020 criminals sent $3.5 billion from their addresses. Cryptocurrencies are coming under more and more scrutiny from regulators and VASPs need to understand the risks they face in this arena. This is where fscom can help.

Purpose of this handbook

This handbook aims to be the go-to guide for financial crime compliance professionals of any level of seniority who are starting out in the world of cryptoassets. Our in-depth experience of the industry has shown us that the fast-growing world of digital assets has posed a new and unprecedented challenge to the industry of financial crime compliance. Many courses and certifications on the topic of tackling money laundering in the world of digital assets are lengthy, often very technical, and offer very few practical insights that can be used in the day-to-day life of a compliance professional. This handbook aims to change that.

Within these pages, we want to provide a beginner's insight to cryptoassets from the point of view of an AML professional. We want to give you the absolute fundamentals and provide practical knowledge and insights that will help you do your job, without getting into the weeds of the technical aspects that developers and software engineers need to know. Whether it's crypto-relevant regulations, risk assessments, blockchain analysis or investigations, this handbook has got you covered. In short, this handbook is written by AML experts for AML experts.

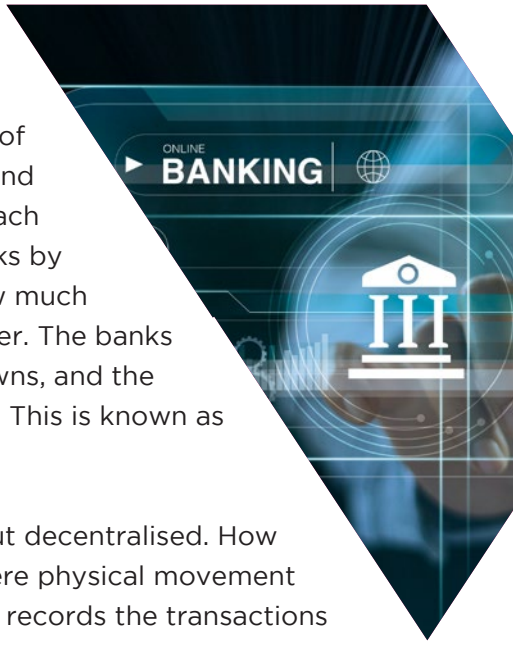
What Is Blockchain?

Distributed Ledger Technology (DLT)

Back to Basics

To begin understanding how financial crime risk can be tackled in the cryptoverse, our experience has shown us that we need to start with a fundamental understanding of the subject matter. The best to way to do this is to go back to basics and build up from the fundamental principles that guide financial activity.

Let's start with how a transaction works. Normal cash transactions can take place by one person handing cash to another person. The person on the other side of any transaction is called a counterparty.



The birth of the internet gave rise to additional complexity, but almost anyone with a bank account will have some knowledge in this area. Online, transactions obviously don't work by physical movement of cash. They work by the banks maintaining a private log of transactions, also known as a ledger, which comprises all the checks and balances that determines how much of the overall funds belongs to each account. To give a simple example, an interbank wire transaction works by instructions being sent from one bank to another bank to instruct how much currency should be deducted from one account and added to the other. The banks all maintain their own ledgers to keep track of how much everyone owns, and the ledgers are private – meaning no one outside the banks can see them. This is known as a 'general ledger', or 'centralized ledger' system.

Distributed Ledger Technology (DLT) is founded on the same idea, but decentralised. How does this work? DLT follows this internet-based transaction style, where physical movement of money is replaced by a complex ledger system, but the ledger that records the transactions is not housed within any institution like a government or a bank. This ledger is completely public, meaning everyone can see which accounts hold what amount of funds. This sounds risky – surely this public system would immediately be hacked? How can we know that no one has made a change to the public ledger to give themselves more funds?

This is where the 'distributed' part comes in. DLT blockchains work by all parties to the system constantly validating and checking via an extremely complex set of mathematical encryptions (a system known as cryptography) to reach a consensus on the information stored in the ledger. This is called a 'Consensus Mechanism'. When a transaction happens, the information is distributed to parties across the entire network, and the networks must agree to validate the transaction. Once the transaction is validated, a new permanent record is created in the ledger. Transactions are organised into 'blocks', and each block forms a new link in the 'chain' of transactions. Therefore the 'blockchain' is the name of the digital ledger that keeps track of all these transactions. The blockchain is completely public and can be accessed by anyone with an internet connection. Some common blockchain explorers include Blockchain.com, Blockchair.com, Tokenview.com, etc.

One final thing to note. The rise of cryptocurrencies around the world has carved a divide between the old world of traditional finance and the new world of cryptographic finance. More and more commonly, the traditional banking system and the currencies tied to it are known as the 'fiat' system, in contrast to the new digital system often simply called 'crypto'.

Wallets, addresses and hashes

So far so good - we have a basic understanding of the system. Now for some jargon-busting. The meteoric growth of digital finance has brought with it a whole new vocabulary for navigating the cryptoverse. The table below shows some handy translations that we've found help people to get up to speed.

Traditional / Fiat	Digital / Crypto
Account	Wallet
IBAN, or Account number & sort code (routing number)	Address
Transaction ID	Hash
Financial institution (FI)	Virtual asset service provider (VASP)

If we imagine a traditional bank system, a client holds an account at a bank. In crypto, this account is known as a 'wallet', and it's where all the person's funds are stored. As you know if you've ever had a bank account, every account at a bank has its own unique account number and sort code (or routing number in the USA) to identify the account. In the world of crypto, this identifier is called an address. This is a long and complicated code that can look something like this:

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

If you know a cryptocurrency address, you can search for it using a blockchain explorer and see all the transactions it has ever carried out.

As we talked about above, each transaction with cryptocurrencies creates a new record in the digital ledger. And each transaction has a code to identify it. Just like a 'transaction ID' in the traditional banking system, every time anyone sends money on the blockchain, a new ID is created called a 'hash'. This can also be searched on a blockchain explorer to see details of the transaction, including the currency and the amounts and counterparties involved.

Finally, while it can often prove confusing, this space has gained many different names over the last decade. So, whether you're talking about crypto, cryptocurrencies, cryptoassets, digital assets, digital currencies, virtual assets, virtual money, crypto tokens, or digital coins – just know they're all referring to the same thing!

Custodial and non-Custodial

Banks maintain accounts on behalf of their clients and are therefore responsible for safeguarding and protecting the customer's accounts and their funds. But with

cryptocurrency, that responsibility can be taken out of the hands of a centralised organisation. A crypto wallet is secured using a 'public key' and a 'private key'. These basically act as passwords that, coupled with the address, grant access to the wallet. Crypto wallets whose owners hold their own keys are known as 'non-custodial' wallets.

The opposite of this is 'custodial' wallets, where a centralised financial institution holds the keys to the wallets, in a similar way to how banks guard their clients' accounts. There are many custodial wallet providers on the market but some of the most well-known are Coinbase, Crypto.com, etc.

Cryptoassets

Today there are over 6,000 cryptocurrencies that have been established using Distributed Ledger Technology. Some are common household names, whereas others are less well understood. Below are some of the most fundamental assets or asset classes in play in the cryptocurrency space.

Bitcoin

The first digital currency, also the largest by market cap and probably the most well-known by the general public. Launched in 2009, Bitcoin was founded by the mysterious and pseudonymous Satoshi Nakamoto.

Ethereum & ERC-20

Launched in 2015 by founder Vitalik Buterin, Ether has become the second-largest cryptoasset by market cap and Ethereum has paved the way for hundreds of new and innovative cryptoassets and crypto products to be built through its open-source, smart-contract-enabled blockchain. Ethereum Request for Comments (ERC-20) is the technical standard for new cryptoassets built on the Ethereum blockchain.

Stablecoins

Created to address the problem of price volatility in the original cryptoassets, stablecoins are pegged to the value of fiat assets such as the US dollar, to ensure their price remains stable. For this reason, stablecoins have become popular as a payment method as they benefit from the blockchain technology without suffering from erratic price volatility.

Decentralised Finance (DeFi)

DeFi products started being built on the Ethereum blockchain, taking advantage of its smart contracts feature. DeFi projects use code to offer financial services to cryptocurrency holders by removing the need for a trusted third party such as a broker or a bank. Clients can earn rewards for staking, acquire loans, or get access to exchange services through these products by leveraging the power of smart contracts.

Non-Fungible Tokens (NFTs)

Unlike fungible assets like Bitcoin and Ethereum, NFTs use cryptography to prove ownership of unique digital items which act as the online equivalent of art pieces. NFTs shot to fame in 2021 when a piece designed by digital artist Beeple sold for $69 million at auction.

AML/CTF in Crypto

This brings us to the focus of this handbook. Now we have a general understanding of the technology and some of the main cryptoassets available in the market today, it is important to understand the impact digital currencies have had on financial crime and the regulatory environment.

In this section, we'll lay out some of the key pieces of legislation and general guidance in this space that VASPs should be aware of. We will then take a deeper look at the specific risks associated with cryptoassets, and finally we'll look at the key parts of a firm's AML/CTF framework and controls environment required to mitigate the risks.

Regulation, Legislation and Guidance

FATF Guidance for a Risk-Based Approach to VAs and VASPs

In July 2019, the Financial Action Task Force (FATF) published this guidance on cryptoassets and VASPs. This brought cryptoassets under the purview of the FATF 40 Recommendations, including the application of Recommendation 16 to virtual currencies. This has since become known as the 'travel rule'.

"This includes the obligation to obtain, hold, and submit required originator and beneficiary information associated with VA transfers in order to identify and report suspicious transactions, take freezing actions, and prohibit transactions with designated persons and entities. The requirements apply to both VASPs and other obliged entities such as FIs when they send or receive VA transfers on behalf of a customer".

In short, it requires that VASPs must send account holder information with any outgoing transactions, in the same way that traditional banks must. Given that this is not built into the technology of cryptoassets, application of the 'travel rule' has been somewhat controversial. Nonetheless, it is likely that travel rule legislation across Europe is on the horizon for cryptoassets.

5th Anti-Money Laundering Directive (5AMLD)

The European Union (EU) first entered the 5AMLD into force in 2018, and one of the main updates was to bring virtual assets into scope for these regulations, with VASPs being brought into the definition of an 'obliged entity'. It additionally required that Member States register and regulate VASPs.

JMLSG Part II

In 2020, the Joint Money Laundering Steering Group first published sectoral guidance for VASPs in Part II, Section 22 of its Guidance. The guidance highlights specific cryptoasset risks and gives best practice guidance for tackling AML/CTF risk management in VASPs.

National Bans on Cryptocurrency

As of March 2022, eight nations (Egypt, Iraq, Qatar, Oman, Morocco, Algeria, Tunisia, Bangladesh, and China) have implemented a national ban on cryptocurrency. 42 additional jurisdictions, including Bolivia, Ecuador, Chad and Côte d'Ivoire, have put additional restrictions on VASPs and limited the ability for banks to deal with cryptoassets.

Risk and Typologies

Given that cryptocurrencies are a new type of asset and mode of value transfer, there are some risks which are inherent to the technology that we should consider. Of course, each different type of digital asset may present its own unique risks, but some general inherent risks to consider are laid out below:

Lower risks	Digital / Crypto
- Full audit trail	- Cross-border
	- Fast onward transmission
	- Anonymity
	- Irreversible transactions
	- Lack of central authority
	- Nascent technology

Fraud risk

Given cryptoassets are a relatively very new and largely poorly understood technology, there are many avenues for fraudsters to exploit. Some of the key fraud typologies are detailed below:

Private keys being lost, hacked or stolen through social engineering

Exchanges being hacked by bad actors

Deanonymisation of wallets leading to extortion or blackmail

Scam Initial Coin Offerings (ICOs), which lead to 'rug pulls' or 'pump and dump' scenarios

Pyramid or ponzi schemes

Money Laundering (ML) risk

The UK National Risk Assessment 2020 assessed the money-laundering risk in cryptocurrency as Medium. Online frauds in cryptocurrency can often be the predicate crimes that lead to money laundering. There are three key areas of ML risk detailed below to consider, which are (a) criminally derived funds, (b) channels for obscurity or obfuscation that mask the funds' origin, and (c) sources of funds that can be considered high risk for money laundering. Below is a non-exhaustive list of risks:

Criminal

Stolen funds | Scam | Malware/Ransomware | Dark markets | Child Abuse Material

Obscurity

Mixers/Coinjoin | Shielded Wallet | Burner wallets/Chain-peeling | Privacy tokens

High Risk

Crypto ATMs | P2P Exchanges | High-risk jurisdictions | High-risk exchanges | Gambling | ICOs

Terrorist Financing (TF) risk

The UK National Risk Assessment 2020 also assessed the terrorist financing risk in cryptocurrency as Medium. Given that cryptocurrency is an inherently quickly transmitted and cross-border technology with an increased capacity for anonymity, there is a clear terrorist financing risk associated. Blockchain monitoring solutions usually provide coverage for this within their products, but an increase in regulation and the introduction of the 'travel rule' for cryptoassets might be the key to significantly tackling this risk.

Sanctions risk

Blockchain addresses were first added to sanctions lists in 2018. Blockchain monitoring solutions provide coverage for sanctioned wallets within their products, but firms should also consider blacklisting sanctioned addresses to ensure their clients are unable to send funds to a sanctioned wallet.

Strategy and Framework

There are many areas of a firm's AML/CTF strategy and framework that will need to consider and cater to the additional risks that cryptoasset-focused products and services carry. Below are some of the most important aspects to consider in tackling this risk within the firm.

Risk Assessments

Cryptoasset-related risks must be considered as part of a VASP's whole firm risk assessment (WFRA). The WFRA should be informed by the Supranational and National Risk Assessments, and the assessment should consider the specific granular risks that the firm's cryptoasset products and services present.

The customer risk assessment should consider any use of crypto products and acknowledge their inherently higher risk. Custodial VASPs should seek to understand the purpose of any wallet they open for a client and consider the risks of offering multiple different cryptoassets at the same time.

Additionally, regulators increasingly want to see evidence that VASPs have risk assessed the cryptocurrencies they list before deciding to offer them. Token assessments can include:


Legal review on whether the token may be classed as a security


Capacity for anonymity and other relevant risks


Review of entities that issue the token


Potential for coverage through blockchain monitoring

Due Diligence

The nature of the blockchain technology can influence the due diligence steps firms need to take in order to ensure they apply appropriate due diligence measures that are proportionate to the risk. For example, firms should consider additional enhanced due diligence (EDD) measures which may include acquiring transaction receipts and taking steps to ensure clients provide proof of ownership of their digital wallets.

Proof of wallet ownership can be evidenced by acquiring statements from another VASP, for example, or by requesting the client take action with their cryptocurrency wallet. This can entail sending a very small amount of currency to the VASP to prove ownership (known as a 'Satoshi test' in Bitcoin), or they can sign and verify a message, which is a more technical method of proving ownership of a non-custodial address.

Finally, firms should consider that they will need to ensure their policies and procedures regarding source of funds (SOF) and source of wealth (SOW) evidence are appropriate. SOF and SOW proofs may also be supplemented by verification on the blockchain.

Blockchain Monitoring

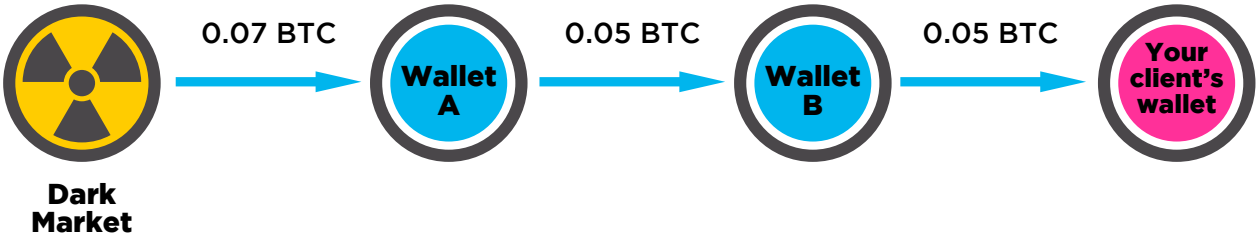
Blockchain monitoring is an additional control firms can use to supplement their transaction monitoring infrastructure. Providers of this service gather information to deanonymise cryptocurrency addresses to help VASPs understand the risk exposure posed to their firm by ingoing and outgoing cryptoasset transactions. Most services allow for bespoke risk rules to be implemented, and also provide visualisation and investigation tools to assist with suspicious activity investigations.

If a firm chooses to employ a third party blockchain monitoring solution, they should ensure to conduct due diligence on the provider, and may need to seek additional training for compliance staff.

Investigations

As with any normal financial crime alert in a traditional financial institution, an alert generated by a blockchain monitoring solution should result in an investigation. Investigations best practices will vary from firm to firm, but investigations staff should have sufficient training to be able to carry out a review into potentially suspicious activity involving cryptocurrency, with a focus on the risks identified in the sections above.

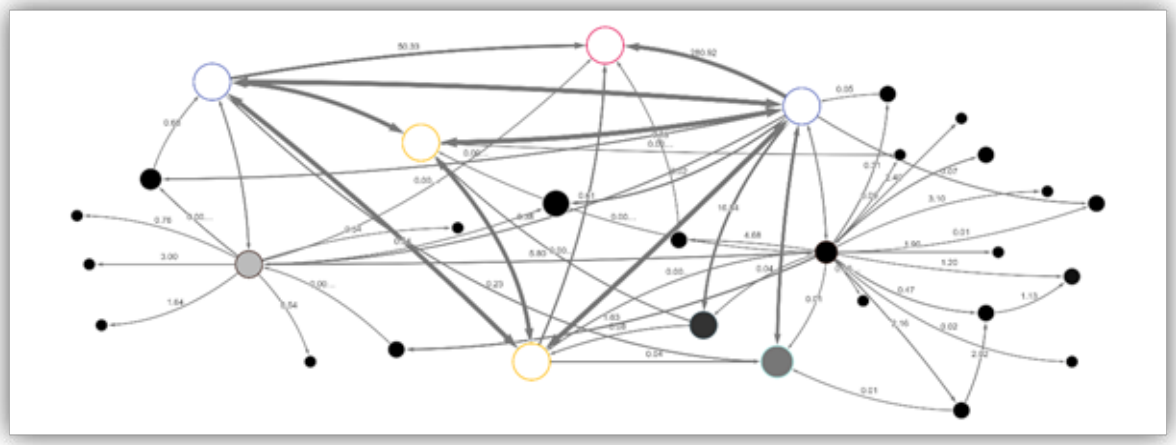
Investigations will usually begin with identifying the reason for the alert, followed by an in-depth review to determine whether the alert is a True or False Positive. Most of today's blockchain monitoring solutions will include a form of transactions visualiser. This will help the investigator to visualise the movement of funds and assess the risk exposure. Each bubble represents an address or group of addresses. A basic example is shown below:



In the above example, your client received 0.05 bitcoin from Wallet B, which received those funds from Wallet A, which originally received 0.07 bitcoins from a dark market. In the context of AML investigations into cryptoassets, each of these movements of funds is commonly known as a 'hop'. So, in the visualisation above, there are 3 hops between your client and the dark market source. No AML investigation can be completely prescriptive, but some common things to consider as part of any blockchain monitoring investigation include:

- How many hops are there between the client and the suspicious source/destination? Is it likely that your client is aware of the exposure?
- Are there any clear changes of ownership of the funds?
- Is there a pattern of this type of activity in the customer's transaction history?
- Are there any other suspicions in the customer's profile which could corroborate the risk?
- Does an open-source intelligence search return any suspicions on the client?

While some investigations will be as simple as the one above, some will reach a much deeper level of complexity. For example, a detailed investigation into the Twitter hack incident of July 2020 is shown below:



Reporting

Cases of suspicion involving cryptoassets should be reported to the relevant FIU in the normal way. Most FIUs have issued additional guidance for VASPs on reporting via SARs/STRs. For example, the UK FIU has issued a SAR code to be used for virtual assets (XXVAXX) and has added the currency codes for the main cryptoassets to the transactions section.

VASPs should also know they are unable to block incoming transactions into their cryptocurrency wallets. The risk of fast onward transmission of suspicious assets means that funds can be quickly converted for the purposes of laundering. To combat this, firms should seek to automate account blocks, asset freezes or cool-down periods if they receive suspicious funds.

Training

Cryptocurrency is a new class of asset, and as such poses a wide variety of additional financial crime risks that firms will need to be aware of. With the rapid growth of the digital currencies sector, the AML industry is facing a lack of experience in managing risks associated with cryptoassets.

To address this, MLROs should consider adding specific cryptoasset-focused trainings to their onboarding and annual AML training courses. Furthermore, additional blockchain investigations training and in-depth cryptoasset risk training should be considered for compliance staff.

Expertise that adds value

If you would like to find out more about any of the information in this handbook, please contact Chris Vaughan or any of the financial crime team today.

Chris Vaughan
Senior Compliance Associate
chris.vaughan@fscom.co

Chris Vaughan is a Senior Compliance Associate in the financial crime team in fscom. He is an ACAMS-certified financial crime risk and compliance expert with over 5 years of experience in anti-financial crime-focused roles in the e-commerce, payments and cryptoasset industries. Chris is a risk assessment specialist with extensive experience in business-wide, jurisdictional and cryptoasset financial crime risk assessments.

A former financial crime risk manager in the cryptoassets fintech industry, he has a background in fraud and AML/KYC operational environments, with extensive experience in process optimisation in investigations, SARs procedures and transaction monitoring.

fscom
Expertise that adds value.

Let's start a conversation.

Have a compliance question?

+44(0)28 9042 5451

info@fscom.co

fscom.co

+353 (1) 640 1986

@fscom1

@fscom-limited