Cooperation Programme between Latin America, the Caribbean and the European Union on Drug Policies

Funded by the European Union

COPOLAD

CFATF GAFIC

Financial Investigations and Analysis for Emerging Money Laundering Risks:

Criminal Use of Cryptocurrency

Financial Investigations and Analysis for Emerging Money Laundering Risks:

Criminal Use of Cryptocurrency

CFATF Secretariat

From February to March 2024, the Caribbean Financial Action Task Force (CFATF) and the COPOLAD III program collaborated to deliver a series of impactful training workshops on Financial Investigations and Analysis for Emerging Money Laundering Risks. These workshops provided financial investigators, analysts, and other stakeholders across the region with critical insights and tools to address the evolving challenges of money laundering, particularly the misuse of virtual assets. Building on the expertise shared during these sessions, COPOLAD III has developed this comprehensive training manual, which has been formally approved by the CFATF Heads of Financial Intelligence Units (FIUs). This manual serves as a vital resource for enhancing the region's capacity to combat money laundering, equipping practitioners with the knowledge and strategies necessary to navigate the complexities of the financial crime landscape.

COPOLAD III is a consortium formed by:

Collaborating partners:

COPOLAD III is a program financed by the European Union and is part of the growing co-operation between the EU and the countries of Latin America and the Caribbean in the field of the fight against drug trafficking. IILA[1] is part of the Consortium that manages the Program, together with the Spanish agency FIIAPP, the European Monitoring Center for Drugs and Drug Addiction (EMCDDA) and German Cooperation Agency (GIZ).

The Programme objective is to contribute to the reduction of the demand and supply of drugs in LAC countries facilitating the generation and application of anti-drug policies which are more balanced, evidence-based, comprehensive and, therefore, more effective, fully respecting the national sovereignty of the LAC countries in accordance with the principle of non-interference in the internal affairs of States.

The Caribbean Financial Action Task Force (CFATF), the Spanish agency FIIAPP and the IILA have signed a Memorandum of Understanding whose main objectives are:

1. **Strengthen** the exchange of information between LAC and European countries in the framework of financial and patrimonial investigations linked to crimes of drug trafficking.

2. **Improve** the capabilities of analysts and public officials in charge of the investigations related to money laundering.

3. **Support** the adoption, by CFATF member countries, of standards, procedures and regulations that strengthen the investigative capacity of money laundering crimes and the identification and recovery of assets coming from international drug trafficking.

1. The International Italian-Latin American Organization (IILA) is an intergovernmental organisation based in Rome, whose members are Argentina, Bolivia, Brazil, Colombia, Costa Rica, Cuba, Chile, Ecuador, El Salvador, Guatemala, Haiti, Honduras, Italy, Mexico, Nicaragua, Panama, Paraguay, Peru, Dominican Republic, Uruguay and Venezuela. Since its inception, IILA has played an important role in facilitating relations between Italy, Europe and Latin America, an action carried out operating in the cultural, socioeconomic, technical-scientific and cooperation areas, using tools such as: meetings with sector specialists, sponsorship of events and scholarships, promotion of congresses, conferences, exhibitions and other events, and execution of cooperation projects in Latin American countries.

This manual constitutes a summary of the key topics emanating from the course on "Financial Investigations and Analysis for Emerging Money Laundering Risks" held online between 29 January and 7 March 2024.
The information and opinions expressed in this manual do not necessarily reflect the official opinion of the European Commission. Neither the European Commission nor any person acting on behalf of the European Commission is responsible for any use that may be made of the following information.

The course saw the following speakers delivering lectures:

Michele SMALDONE
Maresciallo Maggiore of Carabinieri (Italy)

Ricardo Jorge DAVID
Officer of Polícia Judiciária, Portugal

RJ BERRY
Director, Financial Reporting Authority, Cayman Islands

Federico PAESANO
Expert on virtual asset (Italy)

Kisha SUTHERLAND
Director Regional Security System Asset Recovery Unit (RSS ARU)

Mirko LAPI
Expert consultant in OSINT

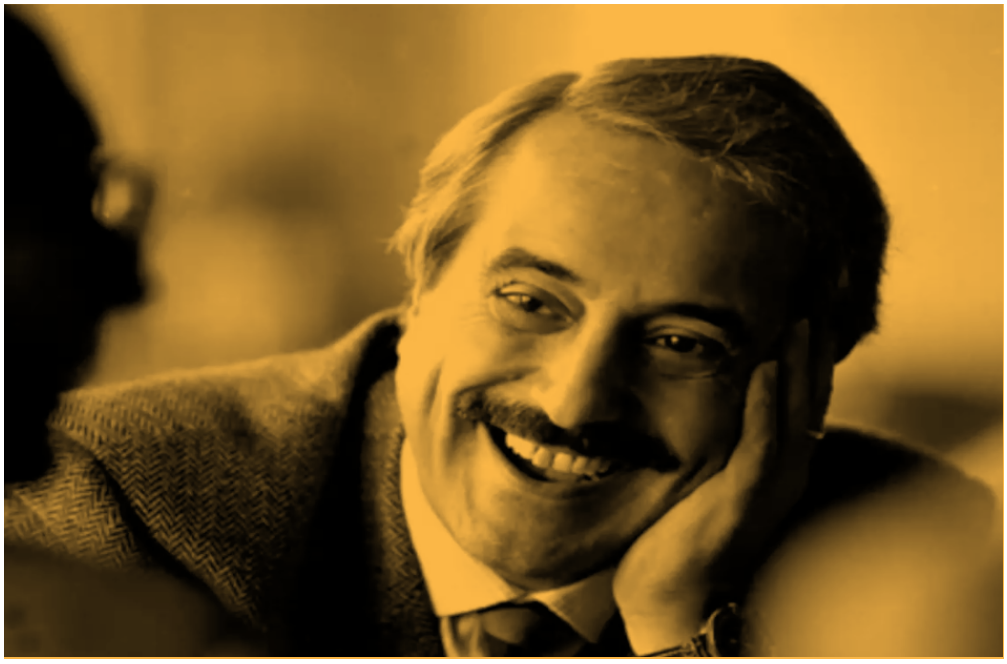
Content

1. Introduction

Giovanni Falcone, an Italian magistrate, devoted his life to combating organised crime and stood as one of the early proponents of global collaboration in this endeavour. Shortly before his tragic assassination on May 23, 1992, he took part in the inaugural session of the Commission on Crime Prevention and Criminal Justice in Vienna, established by the United Nations General Assembly. This marked the inception of a United Nations entity with a specific mission to address crime, laying the groundwork for more coordinated international efforts against organised crime.

Motivated by an exceptional sense of duty, Falcone pioneered an innovative investigative approach focused on "following the money" in financial inquiries involving banks and financial institutions both in Italy and abroad. This method proved instrumental in tracing the movement of suspicious assets and establishing their connections to organised criminal activities. The legacy of Falcone's approach endures globally to combat organised crime.

Follow the money... and criptocurrancy!



This can be interpreted, today, as "follow the cryptocurrency"

In recent years, the financial landscape has witnessed an unprecedented surge in technological advancements, particularly in electronic payment methods. While these innovations offer convenience, they also raise concerns about money laundering and terrorist financing, as criminals can exploit these advanced channels for illicit activities. Technology evolves rapidly, whereas legislative frameworks often lag behind, creating a gap that criminals readily exploit, especially in the realm of global money movement.

Traditional financial transactions, once reliant on cash or cash-related instruments, now embrace new technologies like the Internet, mobile payments, and card systems, rapidly gaining global acceptance. These advancements not only impact existing investigative techniques and financial crime prevention strategies but also challenge the effectiveness of past practices, such as cash, cheques, and bank accounts, which heavily relied on stringent Know Your Customer (KYC) protocols.

Recent developments in digital currencies further complicate the landscape, offering criminals avenues to obfuscate the origins of their proceeds and transfer funds across borders clandestinely. Numerous recent successful investigations underscore criminal organizations' utilization of digital currencies for money laundering. However, these instances also reveal that tracing ownership of digital currencies, albeit challenging, is not impossible.

Digital currency networks typically maintain transaction records on a distributed public ledger, allowing analytical monitoring tools to flag suspicious activities. Every digital transaction leaves a trace, and with proper scrutiny, the veil of secrecy can be lifted, enabling authorities to identify, locate, and seize assets associated with illicit activities.

However, this amount of information is useless if we don't know how to use it properly; it's crucial for law enforcement to understand cryptocurrencies in order to:

1. **Prevent illicit activities**: cryptocurrencies are increasingly being used by criminals for various illicit activities such as money laundering, drug trafficking, terrorism financing, and cybercrime. Law enforcement agencies need to understand how these digital currencies work to prevent and combat such criminal activities effectively.
2. **Investigating Financial Crimes**: As criminals turn to cryptocurrencies to conceal their illicit proceeds, law enforcement must possess the knowledge and tools to investigate and track these transactions. Understanding the underlying technology and the methods used by criminals helps authorities trace and prosecute those involved in financial crimes.

In order to prepare for the future, law enforcement must acquire knowledge about cryptocurrencies, the dark web, and encryption techniques; they should be able to recognize indicators of cryptocurrency involvement, such as the presence of cryptocurrency wallet icons on electronic devices, the use of wallets, visits to cryptocurrency

ATMs and kiosks, and transactions between individuals of interest and cryptocurrency exchanges.

This handbook serves as a comprehensive resource, equipping law enforcement personnel with the knowledge, tools, and best practices necessary to effectively investigate and address crimes involving cryptocurrencies, ultimately safeguarding communities and upholding the rule of law in the digital age.

2. Understanding Cryptocurrencies

This chapter provides an in-depth exploration of the foundational aspects and distinctive attributes of cryptocurrencies, offering readers a thorough comprehension of these innovative digital assets. Central to this discussion are the fundamental principles that underpin cryptocurrencies, serving as the building blocks upon which their operation and significance rest.

One of the key concepts emphasized is the decentralized nature of cryptocurrencies, which distinguishes them from traditional forms of currency controlled by central authorities. This decentralization is facilitated by blockchain technology, a distributed ledger system that records and verifies transactions across a network of nodes, ensuring transparency, security, and immutability.

In addition to exploring the technical aspects of cryptocurrencies, the chapter introduces readers to the dynamic international legislative landscape governing these digital assets. This includes an overview of regulatory frameworks, compliance requirements, and jurisdictional considerations that impact the use, trading, and taxation of cryptocurrencies across different jurisdictions.

2.1. Basic structure and characteristics

Cryptocurrencies represent digital assets facilitating remote and semi-autonomous transactions, eliminating the need for a centralized intermediary. Unlike traditional currencies issued and regulated by governments or financial institutions, cryptocurrencies operate on decentralized networks. These networks consist of voluntary participants, including individuals and organizations, running computer servers that collectively manage transactions through a shared governance protocol, typically implemented as a software algorithm.

This decentralized structure ensures that no single entity or individual can exert control over the entire system. Consequently, there is no centralized authority or intermediary for law enforcement agencies to engage with in cryptocurrency transactions. Instead, users seeking to engage in transactions require access to specific software known as a wallet, along with a unique alphanumeric code called a private key. The private key

serves as a password-like authentication mechanism, enabling users to securely access and manage their cryptocurrency holdings. For many users, wallets are accessible through smartphone applications, which not only facilitate transactions but also manage private keys and wallet addresses.

Expanding on the nature of cryptocurrency transactions, it's essential to highlight the cryptographic principles underlying their security. Transactions are encrypted and authenticated through complex mathematical algorithms, ensuring the integrity and confidentiality of each transaction. This cryptographic layer provides a robust level of security, mitigating the risk of unauthorized access and fraudulent activity.

Furthermore, the decentralized nature of cryptocurrency networks fosters transparency and cooperation among network participants. Each transaction is recorded on a public ledger known as the blockchain, which is distributed across multiple nodes within the network. This distributed ledger ensures transparency and immutability, as transactions cannot be altered or manipulated once recorded.

In October 2008, an innovative paper surfaced on the Internet, credited to an entity named 'Satoshi Nakamoto.' This paper, titled *Bitcoin: A Peer-to-Peer Electronic Cash System*[2], presented a groundbreaking concept: the use of a peer-to-peer network to establish a decentralized system for electronic transactions, eliminating the need for intermediaries and fostering trustless transactions. This revolutionary idea introduced the world to Bitcoin, a digital currency designed to operate independently of traditional financial institutions and centralized authorities. Satoshi Nakamoto's vision outlined a framework where individuals could securely and directly transact with one another, bypassing the need for third-party oversight.

On January 3, 2009, the Bitcoin network officially commenced operations with the release of the inaugural open-source Bitcoin client software and the creation of the first bitcoin. This marked the genesis of a new era in finance, where decentralized digital currencies gained prominence and challenged conventional notions of monetary exchange and trust. The emergence of Bitcoin not only introduced a novel approach to financial transactions but also sparked a global phenomenon, inspiring the creation of numerous alternative cryptocurrencies and blockchain-based projects.

The network's software operates on an open-source basis, meaning its code is freely accessible to the public, inviting contributions and enhancements from developers worldwide. Unlike proprietary systems, this software is not owned or governed by any single entity but rather by a collaborative community of individuals dedicated to its maintenance and improvement.

In *proof of work-based* cryptocurrencies, the management and validation of transactions, as well as the creation of new coins, are carried out collectively by participants

2. Available at https://bitcoin.org/bitcoin.pdf

in the network, who voluntarily contribute the computational power of their machines. This collective effort, known as *mining,* involves the verification and recording of transactions onto a public ledger, referred to as the blockchain. This ledger serves as a permanent and immutable record of every transaction ever conducted within the network. Through the process of mining, network participants are incentivized to validate transactions and maintain the integrity of the blockchain. In exchange for their contributions, miners are rewarded with newly generated bitcoins, as well as transaction fees associated with processed transactions. This reward mechanism not only incentivizes active participation in the network but also ensures the security and stability of the decentralized system.

Crypto peer-to-peer transactions typically involve the use of unique identifiers known as *addresses*, strings of alphanumeric characters such as 12c6DSiU4Rq3P4ZxziKxzrL5LmMBrzjrJX[3].

When a user installs a crypto application or initialise a wallet, the software automatically generates a number of addresses along with a corresponding cryptographic key pair. Cryptocurrency users have the flexibility to generate multiple addresses as needed. To enhance privacy, users often use addresses only once before discarding them. Each transaction recorded in the blockchain associates a balance with a specific address and its corresponding public-private key pair.

The ownership and control of crypto assets are tied to possession of the private key associated with a particular address. Similar to using a password to access a bank account, individuals can spend cryptocurrency by signing transactions with their private keys. Transactions can be initiated and completed using client software installed on various devices, including computers, smartphones, tablets and dedicated hardware.

When a user initiates a transaction, the information is broadcast to the network, where it undergoes validation. The network verifies the validity of the transaction by confirming that it has been properly signed with the correct private key and that the transferred value has not been previously spent. Since the balance associated with an address is essentially a record of past transactions stored in the public ledger (blockchain), there are no physical 'coins' involved, and the client software used for transactions does not store any monetary value.

It's important to note that cryptocurrencies exist purely as entries in the blockchain, and ownership is contingent upon possession of the private key necessary to authorize transactions. This concept presents significant challenges and concerns in cases where bitcoins associated with criminal activities need to be seized, as the digital nature of cryptocurrencies complicates traditional asset seizure procedures.

---

3. All addresses and private keys mentioned in this manual are for learning purposes only and should never be used in practice. Sending cryptocurrencies to the addresses mentioned or using the private keys displayed may result in the permanent loss of the coins sent.

2.2. Different cryptocurrencies exist

In the wake of Bitcoin's inception over a decade ago, a plethora of new cryptocurrency variants have surfaced, contributing to the diverse landscape of digital assets available today. Pinpointing an exact count proves challenging, given the dynamic and ever-evolving nature of the cryptocurrency market. However, even conservative estimates suggest that the number of distinct cryptocurrencies currently in circulation spans into the thousands. Cryptocurrencies operate on distinct platforms, each with its own blockchain infrastructure, and they generally cannot be directly interchanged without intermediary mechanisms like bridges. This inherent separation implies that you cannot, for instance, transfer Ethereum to a Bitcoin address or send Bitcoin to an Ethereum address. Attempting to do so would result in the loss of the assets involved. To ensure the successful transfer of funds, it's imperative to use the appropriate cryptocurrency address corresponding to the specific ledger or blockchain network.

To prevent mistakes, it might be useful to have a look at the most common cryptocurrencies and their address format.

Bitcoin

Originating from a white paper released in 2008, stands as the inaugural cryptocurrency globally recognized. It retains its position as the most prominent form of digital currency. Operating on its dedicated blockchain, bitcoin transactions undergo verification by a decentralized network of miners who also generate new bitcoins, adhering to a predetermined and fixed cap (21 million bitcoin will be created in total).

In the Bitcoin network, *proof of work* (PoW) is the consensus mechanism used to validate transactions and secure the blockchain. In essence, certain nodes in the network, called *miners*, compete to create a new block by solving a complex mathematical puzzle. This puzzle, known as the "hash puzzle," involves repeatedly hashing[4] the block's data until a hash value is found that meets a certain difficulty target set by the network. Once a miner finds a hash value that meets the difficulty target, they broadcast the new block to the network. This block contains the transactions that the miner has verified and grouped together. The miner who successfully mined the block is rewarded with a certain number of newly created bitcoins, as well as any transaction fees included in the block. This serves as an incentive for miners to expend computational resources and secure the network.

> Addresses always start with **1, 3, or bc1.** Their length varies between 26 and 35 characters; example: **bc1q0v4qz095ftv72mcgql0yy39783keztj9fptupv.**

4. Hashing is the process of converting data — text, numbers, files— into a fixed-length string of letters and numbers. Data is converted into these fixed-length strings, or hash values, by using a special algorithm called a hash function.

Ethereum

Ether is the cryptocurrency that runs on the Ethereum blockchain. Ether operates on its own blockchain—but unlike Bitcoin, Ether is uncapped, meaning that an infinite number of coins can theoretically be created. Ethereum also supports smart contracts, which are programs that run on the Ethereum blockchain and are executed automatically when certain conditions are met.

The Ethereum blockchain, through smart contracts, allows the creation of other cryptocurrencies (fungible tokens), known as ERC-20 tokens. Developers can create smart-contract-enabled tokens that can be used with other products and services.

Ethereum and smart contract enable the creation of another type of tokens, known as ERC-721 or non-fungible tokens (**NFTs**): these tokens are non-fungible, meaning that they cannot be exchanged on a one-to-one basis due to their unique properties. They are similar to units of blockchain currency, except that they are connected to unique digital files, so that individual tokens can be considered to have a meaningful distinction from others. This distinguishability provides NFTs with unique characteristics and use cases, such as:

1. **Possession:** ERC-721 empowers users to securely own, transfer, and oversee unique digital assets, ensuring transparent and verifiable records of ownership.
2. **Compatibility:** This standard guarantees seamless interaction of NFTs with various Ethereum network marketplaces, wallets, and decentralized applications (dApps), enriching their functionality and accessibility.
3. **Rarity and Distinctiveness:** In contrast to fungible tokens, ERC-721 NFTs epitomize singular items with distinct attributes, rendering them highly prized among collectors and creators alike.
4. **Protection of Intellectual Property:** ERC-721 NFTs serve as a safeguard for intellectual property rights by furnishing artists and creators with immutable documentation of their creations, alongside mechanisms for monitoring usage and subsequent sales.
5. **Fractionalized Possession:** NFTs constructed according to the ERC-721 standard can be fragmented into smaller, tradable portions, opening avenues for a broader audience to invest in high-value assets.
6. **Inter-Platform Compatibility:** Leveraging a shared standard facilitates the seamless utilization of NFTs across diverse platforms and applications, broadening the scope of potential applications and utility.

The Etherum (and other compatible) blockchain also allow the creation of **Stablecoins**, cryptocurrencies whose value is pegged, or tied, to that of another currency, commodity, or financial instrument. Stablecoins aim to provide an alternative to the high volatility of the most popular cryptocurrencies. Examples are Tether (USDT), USD Coin (USDC), Dai (DAI), Binance USD (BUSD).

Ethereum maintains and expands its blockchain of transactions through a system which is completely different from the one used by Bitcoin. Proof of Stake (PoS) is a consensus mechanism to achieve agreement on the state of the network and validate transactions. Unlike PoW, which relies on computational power and energy-intensive mining activities, PoS operates on the principle of staking cryptocurrency holdings to secure the network. In a PoS system, validators are chosen to create new blocks and validate transactions based on the amount of cryptocurrency they hold and are willing to lock up as collateral, known as their stake. Essentially, the more cryptocurrency a validator stakes, the higher the probability they have of being chosen to create a new block and earn rewards.

> Ethereum addresses always start with **0x** and are made up of 40 characters. Ethereum-compatible networks like Polygon, BNB Chain, Fantom, and Avalanche also use this format. Example: **0x675bB023e268dCC43F543620577bCacB73047f08**.

Monero

Monero is a privacy-focused cryptocurrency that prioritizes anonymity, security, and decentralization. It was launched in April 2014 as a fork of Bitcoin. Monero's development is guided by principles aimed at ensuring the confidentiality of transactions and the privacy of its users. Through the use of advanced cryptographic techniques, such as ring signatures, ring confidential transactions (RingCT), and stealth addresses, Monero obfuscates transaction details such as sender, recipient, and amount. This ensures that transactions on the Monero blockchain are private and unlinkable, and make it a tool that more and more criminals are using to launder proceeds of crime.

> Monero addresses always start with either **4 or 8**, and are 95 characters long.
> Example: **888tNkZrPN6JsEgekjMnABU4TBzc2Dt29EPAvkRxbANsAnjyPbb3iQ1YBRk1UXcdRsiKc9dhwMVgN5S9cQUiyoogDavup3H**.

2.3. Crypto Wallets and how to manage crypto-transactions

Cryptocurrency wallets, whether in the form of software applications or physical devices, serve as secure repositories for the cryptographic keys necessary to access and manage one's digital assets within a specific blockchain network. Unlike traditional wallets that hold physical currency, crypto wallets safeguard the vital keys required for storing and transferring cryptocurrencies; in essence, they take care of safely and securely store **private keys**. As digital assets residing solely on blockchain technology, cryptocurrencies are associated with public and private keys upon wallet registration.

These keys serve as cryptographic credentials, validating ownership of crypto coins and facilitating access to the associated assets.

Ensuring the security and integrity of these keys is paramount, as they are the linchpin of cryptocurrency ownership and transaction authorization. Owners must take great care to securely store their keys and protect their crypto wallets through robust security measures and diligent management practices. Safeguarding these keys against unauthorized access, loss, or theft is essential to safeguarding one's digital assets. Therefore, employing stringent security protocols and exercising caution in managing crypto wallets is imperative for maintaining the integrity and accessibility of one's cryptocurrency holdings.

It is crucial for law enforcement to understand what cryptocurrency wallets are due to their central role in facilitating and managing digital assets. Wallets contain valuable information that can aid law enforcement in criminal investigations. Transactions' history and wallet addresses can provide critical insights into illicit financial transactions, money laundering schemes, and other criminal activities. Law enforcement personnel with knowledge of cryptocurrency wallets can leverage this information to build cases, identify suspects, and disrupt criminal networks. Moreover, understanding how cryptocurrency wallets operate enables authorities to navigate the process of seizing and recovering illicitly obtained funds effectively.

Broadly speaking, crypto wallets fall into two categories: hot wallets and cold (or hardware) wallets. Hot wallets exist solely in digital form and are constantly connected to the internet, making them more susceptible to hacking and phishing attacks. On the other hand, hardware wallets, a subset of cold wallets, are physical devices that operate offline, providing an added layer of security against malicious intrusions.

Hot wallets offer the convenience of digital accessibility from any internet-connected device. Most of them are free to download and available as mobile-based applications or browser extensions. Exodus and Trust Wallet are two examples of this type of virtual currency wallet. A key advantage of such wallets is the user-friendly interface. On the other hand, a cold storage wallet is a type of cryptocurrency wallet designed to store private keys offline, providing an added layer of security against hacking, malware attacks, and other security threats. Private keys are used to access and manage cryptocurrency assets. By storing them offline, cold wallets make it more difficult for malicious actors to gain access to your digital assets.

The simplest form of **cold storage** is known as a **paper wallet**, which is essentially a physical document containing both the address and its private key. Anyone can generate and print the document using one of the existing online paper-wallet tools[5], utilizing an offline printer for added security. Typically, the paper wallet includes a QR code, allowing for easy scanning and signing to execute transactions.

5. For example, see http://www.bitaddress.org/

However, one significant drawback of this method is the risk of loss, damage, or destruction of the paper. If the paper wallet is misplaced, becomes unreadable, or is damaged, the user may permanently lose access to the funds stored at the associated address. Therefore, it is imperative for individuals opting for this approach to ensure secure storage of the paper wallet, such as utilizing a safe box or another reliable storage method.

Another method of cold storage involves the use of **hardware wallets**, which utilize an offline device or smart card to generate private keys in an offline environment. An exemplar of this approach is the Ledger USB Wallet, which employs a smart card to enhance the security of private keys. Other notable hardware wallets include TREZOR and KeepKey. Functioning akin to a USB drive, these hardware wallets require a computer and an application to manage and store private keys offline. The devices vary in complexity, ranging from standard USB storage drives to sophisticated devices equipped with features such as batteries, Bluetooth connectivity, and specialized software.

Similar to paper wallets, it is imperative to store hardware wallets and smart cards securely to mitigate the risk of loss or damage, as any such occurrence could result in permanent loss of access to the stored cryptocurrency assets. Thus, users must exercise diligence in safeguarding these devices and implementing appropriate security measures to protect their digital wealth.

Most of the wallets, and all the ones mentioned above except made for the paper wallet, are secured by **recovery seeds**.

A seed phrase serves as a critical security measure for recovering lost or damaged cryptocurrency wallets, consisting of a sequence of either 12 or 24 randomly generated words. Also known as a mnemonic phrase, it acts as a safeguard for digital assets held in personal custody. Both hot and cold wallets can employ a seed phrase for recovery purposes, making it a versatile tool in the realm of cryptocurrency security. Analogous to a master password, the seed phrase serves as the gateway to accessing all cryptocurrency associated with the wallet that generated it, even in cases where the wallet itself has been deleted or lost. Essentially, it functions as a password manager for cryptocurrencies, providing a secure means of retrieval in times of need. To enhance memorability, seed phrases consist of simplified, randomly generated words chosen from a predetermined list of 2048 options. This design choice ensures that users can easily recall their seed phrases without the need for complex numerical or special character sequences.

The following is an example of a 12-word seed phrase:

> *"regret, difficult, shy, planet, child, anxiety, typical, alternative, humanity, never, loose, cry"*

2.4. Legislative framework

In the past decade, cryptocurrencies, also known as virtual assets (VAs) or Crypto Assets (CAs), have transcended their niche origins to become a widespread phenomenon with profound implications for the traditional financial landscape. Both individuals and companies are increasingly adopting VAs for various purposes, reflecting a growing acceptance and integration of digital currencies into mainstream finance. Worldwide, this trend is underscored by the rising number of financial institutions offering VA-related services, contributing to the emergence of virtual asset service providers (VASPs).

However, alongside this surge in legitimate usage, there has been a corresponding rise in illicit activities exploiting the anonymity and borderless nature of cryptocurrencies. Criminal elements have swiftly recognized the potential of VAs as a tool for conducting a broad spectrum of illegal activities, ranging from basic theft and fraud to sophisticated transnational crimes like money laundering and terrorist financing. These nefarious activities present significant challenges for all stakeholders involved in anti-money laundering (AML) efforts, including regulatory authorities, law enforcement agencies, financial institutions, and cryptocurrency service providers.

As VAs continue to gain traction in the mainstream economy, the need for robust AML measures and effective regulatory oversight becomes increasingly pressing. Addressing the illicit use of cryptocurrencies demands collaborative efforts from all stakeholders to develop comprehensive strategies, enhance detection capabilities, and implement stringent compliance measures.

One of the main international bodies that has tried to regulate the world of VAs is the Financial Action Task Force (FATF). The FATF, also known by its French name, Groupe d'Action Financière (GAFI), is an intergovernmental organisation founded in 1989 on the initiative of the G7 to develop policies to combat money laundering and to maintain certain interest. In 2001, its mandate was expanded to include terrorism financing. It sets international standards that aim to prevent these illegal activities and the harm they cause to society. The FATF Recommendations provide a comprehensive framework of measures to help countries tackle illicit financial flows. These include a robust framework of laws, regulations and operational measures to ensure national authorities can take effective action to detect and disrupt financial flows that fuel crime and terrorism, and punish those responsible for illegal activity. The Recommendations are the basis on which all countries should meet the shared objective of tackling money laundering, terrorist financing and the financing of proliferation. The FATF calls upon all countries to effectively implement these measures in their national systems.

The FATF has also regional bodies, like the Caribbean Financial Action Task Force (CFATF), an organisation of states and territories of the Caribbean basin which have agreed to implement common counter-measures against money laundering and terrorism financing, or the Financial Action Task Force of Latin America (GAFILAT).

In October 2018, the Financial Action Task Force (FATF) made a significant stride by providing its inaugural definitions of VAs and VASPs, aiming to delineate them from the previously employed term 'virtual currency'. These novel definitions were incorporated into FATF Recommendation N. 15, which pertains to 'New technologies', with the primary objective of elucidating the regulatory expectations imposed on these emerging asset classes and their service providers:

> *A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations*[6].

At the same time, the FATF gave a broad definition of VASPs as follows:

'Virtual asset service provider' means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

> i. *exchange between virtual assets and fiat currencies;*
> ii. *exchange between one or more forms of virtual assets;*
> iii. *transfer of virtual assets;*
> iv. *safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and*
> v. *participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.'.*

The FATF Recommendations serve as a vital framework for the regulation and oversight of financial institutions, encompassing cryptocurrency exchanges among other entities. These recommendations play a pivotal role in establishing robust anti-money laundering protocols, thereby safeguarding the integrity of the financial system and deterring illicit activities. Moreover, they create the framework within law enforcement agencies can seek and obtain vital information from VASPs.

Cryptocurrency exchanges play a crucial role in identifying and reporting suspicious activities to the appropriate authorities. They are mandated to implement procedures for detecting and reporting transactions that raise concerns about potential money laundering, terrorist financing, or other illicit conduct. Through timely reporting of such activities, exchanges actively support broader initiatives aimed at combating financial crimes.

6. FATF, *The FATF Recommendations*, February 2023, p. 135

2.5. Virtual Assets Red flags indictors

In the early days of the crypto industry, transparency was not a top priority for crypto firms. However, the current landscape sees a significant shift, with crypto businesses now placing great importance on Know Your Customer (KYC) procedures and compliance measures. The heightened scrutiny from national and international authorities has prompted crypto firms to implement stringent screening processes. They are now required to have robust KYC systems to authenticate customers' identities, addresses, and the sources of their funds. Additionally, monitoring transactions and assessing risks have become integral parts of their operational requirements. The implementation of such measures often necessitates the overhaul of existing processes or the development of new programs.

Despite the challenging journey to achieve regulatory compliance, some exchanges opt to avoid necessary improvements and continue to operate without adhering to KYC standards. This non-compliance leaves them vulnerable to criminal actors, both from traditional finance and the crypto space, who actively seek platforms lacking proper KYC mechanisms to engage in fraudulent activities. Engaging with non-compliant crypto exchanges poses risks for customers, as their funds may be at stake in the event of a mandatory shutdown. Furthermore, these non-compliant exchanges may lack adequate security measures to safeguard user funds and personal information, making them susceptible to various types of attacks.

For individuals employed in conventional financial institutions, the concept of virtual assets and transactions conducted through VASPs might appear perplexing. However, the signs of illicit activity closely resemble those observed in traditional financial transactions. The red flags in virtual asset transactions mirror the indicators recognised by anti-money laundering investigators and transaction monitoring systems in fiat transactions. Detecting and addressing these red flags is crucial for risk mitigation.

There are six main red flag indicators identified by FATF[7]:

- **Red flag indicators related to Transactions**: configure VA transactions for small amounts or amounts below record-keeping or reporting thresholds; making multiple high-value transactions; depositing VAs to an exchange and then immediately withdraw them; accepting funds suspected of being stolen or fraudulent;

- **Red Flag Indicators Related To Transaction Patterns**: to start a new relationship with a VASP, make a large initial deposit and fund the entire stake on the first day of opening; operations involving the use of more than one VA without a correct and plausible explanation; making frequent transfers to the same VA account by more than one

7. FATF (2020), Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets, FATF, Paris, France. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf

person, by one or more people from the same IP address, or by large amounts of money in a specified period;

- **Red Flag Indicators Related to Anonymity**: abnormal transaction activity of VAs converted to cash on exchanges from wallets associated with the P2P platform without any logical explanation; VAs transferred to or from wallets showing previous activity patterns related to the use of VASPs mixers or P2P platforms; transactions using mixing services suggesting the intention to move illegal fund between known wallet addresses and darknet markets; users who register Internet domain names on the VASP platform through proxies to hide or remove domain name owners; receiving or sending money to VASPs whose CCD or KYC processes are weak or absent;

- **Red Flag Indicators about Senders or Recipients**: to create separate accounts under different names to circumvent the restrictions on trading or withdrawal limits imposed by VASPs; transactions initiated from untrusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously marked as suspicious; frequent attempts to open an account within the same VASP from the same IP address; missing or insufficient KYC information or a client denying requests for KYC documents, or questions regarding source of funds;

- **Red Flag Indicators for Fund or Wealth Source**: transactions arising from or for online gambling services; lack of transparency or insufficient information about the source and owners of funds, such as funds placed in the Coin Offerings (ICO) or online payment system with credit / prepaid cards followed by instant withdrawal; using one or more cards linked to a VA wallet to withdraw large amounts of fiat money;

- **Red Flag Indicators Related to Geographical Risks**: the client's funds originate from or are sent to an exchange that is not registered in the client's jurisdiction; the customer sends money to VASPs operating in jurisdictions that do not have VA regulations or implement AML / CFT controls; the client sets up or moves offices in jurisdictions that do not have or legal regulations governing VAs.

2.6. Travel Rule

Of particular importance for cryptocurrencies, is the implementation of Recommendation N. 16, which extends the so-called travel rule to VAs. It mandates that VASPs obtain and disclose precise details pertaining to the sender and recipient of a virtual asset transfer to counterpart VASPs or financial institutions, either during the transaction or prior to it. By gathering this data, authorities can pinpoint suspicious behavior, such as funds transfers involving individuals or entities linked to criminal endeavors, and subsequently undertake necessary measures to thwart or prosecute unlawful actions.

Because the personal information of the parties involved in transactions accompanies their transfers, this regulation has been dubbed the "Travel Rule". The FATF suggests[8]

that countries implement a de minimis threshold of 1,000 USD/EUR for VA transfers, while acknowledging that there would be relatively fewer requirements for VA transfers below this threshold compared to those above it.

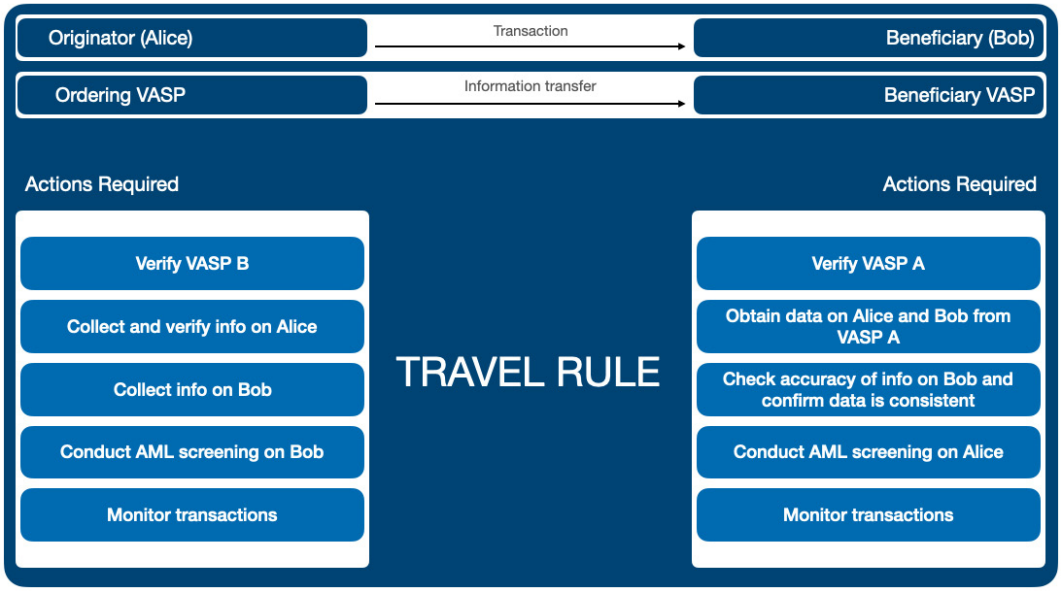
For VA transfers falling under the threshold, VASPs are required to gather:

- The names of both the originator (sender) and the beneficiary (recipient)
- The Virtual Asset (VA) wallet address for each transaction or a unique transaction reference number.

Verification of such information is not obligatory unless suspicious circumstances related to Money Laundering/Terrorist Financing (ML/TF) are observed, in which case customer information should be verified.

For transfers surpassing the threshold, VASPs are obliged to collect:

- Originator's name
- Originator's account number for the account used to process the transaction (e.g., wallet address)
- Originator's physical (geographical) address; national identity number; customer identification number (i.e., not a transaction number) that uniquely identifies the originator to the ordering institution; or date and place of birth
- Beneficiary's name
- Beneficiary's account number for the account used to process the transaction (e.g., wallet address)



8. *FATF (2022) Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs*, FATF, Paris, France, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf

Recommendation 16 pertains to VASPs whenever their transactions, involving either fiat currency or virtual assets, encompass:

- Traditional wire transfers
- VA transfers between a VASP and another obligated entity (such as between two VASPs or between a VASP and another obligated entity like a bank or financial institution)
- VA transfers between a VASP and a non-obligated entity (i.e., an unhosted wallet)[9].

As the FATF refrains from endorsing any particular data sharing technology, there isn't a singular protocol or network designated for data transfer. Consequently, several networks for encrypted data transfers are already in existence, such as OpenVASP, Shyft, and Trisa. Nevertheless, challenges persist with these networks, such as protocol compatibility.

Later on, we'll delve into how this legal framework empowers LEAs to track anonymous criminal transactions on the blockchain until they reach a juncture where subpoenas can be issued, information obtained, and assets seized.

9. This scenario is unique, as the FATF does not anticipate that VASPs, when initiating a VA transfer, would furnish the required information to individuals who are not obligated entities (for instance, to an unhosted wallet). Only a few jurisdictions have implemented this part.

3. Criminal use of cryptocurrency

Within the intricate landscape of cryptocurrencies, a contentious issue looms large: their exploitation by criminals for illicit activities. This chapter delves into the multifaceted dynamics of how cryptocurrencies serve as a conduit for nefarious endeavors, shedding light on the myriad challenges confronting law enforcement agencies. The ascent of crypto assets has coincided with a surge in their utilization for money laundering activities, providing criminals with a cloak to veil the origins and destinations of illicit funds. Moreover, this chapter explores the intricate web of obfuscation techniques employed by criminals, further complicating the task of tracking financial misdeeds. As cryptocurrencies continue to permeate global financial systems, the need for effective strategies to combat their misuse becomes increasingly pressing.

3.1. Drug trafficking and Money Laundering

Drug traffickers exploit virtual currency and peer-to-peer mobile payments due to the relative anonymity they afford, thereby complicating detection efforts. These transactions, shielded by a veil of anonymity (or, as we will see, pseudonymity), present significant challenges for law enforcement agencies striving to uncover illicit activities. Virtual assets are increasingly utilized on platforms that facilitate drug trafficking, amplifying the complexity of combating this heinous crime.

In 2023, the US Justice Department made headlines with charges against four sons of the incarcerated Mexican drug lord Joaquin "El Chapo" Guzman. The indictment alleged their involvement in laundering profits from a US fentanyl smuggling operation through the use of "untraceable cryptocurrency". Simultaneously, US authorities announced the apprehension of a wanted money launderer in Guatemala on the same day. According to authorities, the individual had ties to the cartel and was accused of collecting $869,000 in drug profits, subsequently depositing the funds into cryptocurrency wallets. These high-profile cases underscore the growing trend of drug cartels and crime syndicates in Latin America embracing virtual currencies as a means to launder money, facilitate payments, and peddle narcotics on the darknet.

In tandem with the proliferation of virtual currencies, online marketplaces have emerged as hubs for the trafficking of sex and illegal goods. These marketplaces, often nestled

within the recesses of the "dark web," represent a clandestine corner of the internet accessible via specialized software like Tor, fostering an environment of heightened anonymity for users engaging in illicit transactions. The dark web's cloak of secrecy shields participants from scrutiny, minimizing the risk of detection by law enforcement.

Dark web markets are online platforms within the dark web that facilitate the buying and selling of various goods and services. These markets operate on anonymised networks and are known for providing a degree of anonymity to both buyers and sellers through encryption and privacy-focused technologies. While some items on these markets may be legal, many are associated with illegal activities, especially drugs, leading to concerns about the facilitation of criminal enterprises.

Which are the characteristics that make dark web markets useful from criminal activity?

- **Anonymity:** Dark web markets operate on the Tor network, which allows users to access websites with increased anonymity;
- **Cryptocurrency Transactions:** transactions on dark web markets are usually conducted using cryptocurrencies like Bitcoin, Monero, or other privacy-focused coins. This adds an additional layer of anonymity to financial transactions;
- **Product Variety:** Dark web markets offer a wide range of products and services, both legal and illegal. Legal items might include privacy-focused tools, digital goods, or niche products. However, many dark web markets are notorious for facilitating the trade of illegal items such as drugs, firearms, hacking tools, stolen data, and counterfeit documents;
- **Escrow Services:** Many dark web markets use escrow services to facilitate transactions. In this process, the funds are held by a third party (escrow) until the buyer receives the product or service and is satisfied, after which the funds are released to the seller;

Dark web markets pose difficult challenges to Law Enforcement due to the anonymity of users and the use of cryptocurrencies. However, law enforcement agencies worldwide are actively working to track and apprehend individuals involved in illegal activities on these platforms and we have many successful investigations that took down dark web markets like SilkRoad, Hydra, Monopoly, Wall Street Market, and many more.

On the bright side, these new technologies and the growth of digital information available, investigators now have access to vast amounts of data, including digital activity, internet traffic, browsing data, phone records, social media activities, emails and, finally, blockchain activity. While this abundance of information can be valuable, it also poses significant challenges. Information overload in criminal investigations refers to the overwhelming amount of data and information that investigators have to sift through while trying to solve a crime.

The overload causes several concerns:

- **Volume of Data:** The sheer volume of data generated in modern society can be immense. Collecting, organising, and analysing this data is a time-consuming process, and investigators may struggle to keep up with the ever-increasing amount of information available;
- **Technological Challenges:** Law enforcement agencies may face challenges in terms of technological infrastructure, tools, and expertise. The rapidly evolving nature of technology makes it necessary for investigators to stay updated on the latest tools and techniques for handling digital evidence;
- **Time Constraints:** Criminal investigations often have time constraints, and investigators may not have sufficient time to thoroughly examine all available data. This can lead to the possibility of overlooking crucial information.

To counter those problems, analysts and investigators will pay attention to follow the information cycle, which is the continuous and dynamic process of gathering, analysing, and disseminating information throughout the various stages of an investigation. It involves the systematic flow of information from different sources, both internal and external, and it plays a crucial role in solving crimes.

The information cycle typically includes the following stages:

- **Planning:** identify tasks, source of information and plan the different phases of the investigation;
- **Collection:** analysts and investigators collect a wide range of data and evidence related to the crime. This can include witness statements, physical evidence, surveillance footage, forensic analysis, and information obtained from various databases and other sources;
- **Evaluation:** not all the evidence collected is useful or relevant; Law Enforcement must focus on what can provide the solution to the case
- **Analysis:** the collected data is then analysed to identify patterns, connections, and potential leads. This stage also involves the identification of any gaps or inconsistencies.
- **Integration:** this step involves the organisation and analysis of various pieces of data and evidence from multiple sources to create a comprehensive and coherent understanding of a criminal investigation. Integration is a critical aspect of modern law enforcement, especially given the diverse and often complex nature of information available in criminal cases;
- **Diffusion:** law enforcement agencies often collaborate and share information with each other to benefit from collective expertise and resources. This collaboration may involve local, state, or federal agencies, as well as other relevant entities.

CASE STUDY: ANALYSIS EXERCISE IN INTERNATIONAL DRUG INVESTIGATION	
Evaluate strengths	A criminal organisation is selling drugs in the dark web, using its members as sellers
Evaluate weaknesses	By setting up a fake buyer account, investigators can gather information about the sellers and identify crypto addresses used by the criminal organization. Transactions can be followed on the blockchain to understand which exchange the gang is using
Opportunity	Instead of simply arresting drug sellers, we can dismantle a criminal organisation
Threat	The criminal gang is highly organised and structured
Sustainable option	Create different teams, each with a specific task (technical team, financial analysis team, etc)
Desirable possibility	The investigation will provide leads to a bigger organised criminal group
Catastrophic theory	A leak alerts the criminals who are able to flee before being arrested
Investigative project	The start of the investigation
Operational organisation	Teams will open accounts with the darkweb market
Operational objectives	Arrest all members of the criminal group, charging them with both drug trafficking and money laundering, identifying and seizing all their assets
Consideration and proposals	Consider the use of seized assets for social purposes
Results	Completion of all the planned tasks

3.2. Obfuscation Techniques

As previously elaborated, the blockchain technology serves as a paradigm shift in record-keeping, offering unparalleled transparency, immutability, and accessibility. This decentralized ledger system meticulously documents every transaction, rendering it

publicly available for scrutiny. Each transfer is accompanied by comprehensive metadata, including timestamps, transaction amounts, and the specific crypto assets utilized. While the identities associated with blockchain addresses remain concealed behind cryptographic pseudonyms, it's crucial to acknowledge the existence of methodologies capable of unraveling these pseudonyms, a topic we'll explore in greater detail later.

In light of the inherent transparency of blockchain transactions, particularly concerning the movement of illicit funds, criminal actors have innovated sophisticated strategies and obfuscation techniques. These maneuvers are meticulously designed to thwart investigative efforts aimed at tracing nefarious activities within the public blockchain ecosystem. Ranging from complex mixing services to intricate layering techniques, these strategies introduce formidable obstacles for law enforcement agencies and regulatory bodies tasked with combating blockchain-enabled crimes.

Given the multifaceted nature of these evasion tactics, traditional investigative approaches may find themselves ill-equipped to effectively navigate the intricacies of blockchain-based criminal activities. As such, there exists a pressing need for the continuous evolution and adaptation of investigative methodologies to effectively address the challenges posed by the rapidly evolving landscape of blockchain-related crimes.

Before delving into more intricate obfuscation techniques, it's important to emphasize that, beyond their utilization by criminals and criminal organizations, there exist numerous legitimate use cases for these methods. These legitimate applications underscore the versatility and value of obfuscation techniques in various contexts, showcasing their adaptability and significance in addressing a wide array of challenges and requirements. These include:

1. **Protection Against Surveillance:** In an era where digital privacy is increasingly under threat, the ability to conduct private transactions provides individuals with a shield against pervasive surveillance. Without privacy protections, every financial transaction becomes subject to monitoring, potentially compromising personal and financial autonomy.

2. **Preservation of Financial Confidentiality:** Just as individuals expect privacy in their traditional financial transactions, the same expectation applies to cryptocurrency transactions. Preserving financial confidentiality is crucial for maintaining trust and safeguarding sensitive information from unauthorized access or exploitation.

3. **Prevention of Discrimination and Profiling:** Without privacy safeguards, individuals risk being subjected to discriminatory practices or profiling based on their transaction history. The ability to conduct private transactions helps mitigate the risk of such discrimination and ensures equitable treatment for all participants in the cryptocurrency ecosystem.

4. **Enhanced Security:** Privacy features in cryptocurrency transactions not only protect against external surveillance but also enhance security by reducing the risk of identity

theft, fraud, and targeted attacks. By obscuring transaction details, privacy measures help mitigate the potential for malicious actors to exploit vulnerabilities and compromise sensitive information.

Mixers and Tumblers

Crypto mixers, alternatively referred to as Crypto tumblers or Crypto blenders, are services operating within the Crypto realm. Their function is to obscure the origins and destinations of crypto transactions by blending them randomly with other legitimate transactions. This process ensures transaction anonymity, making it difficult for any third party, including Law Enforcement, to trace them easily.

Mixers accept crypto assets from multiple origins; these coins are then distributed to different addresses before reaching the final destination, effectively severing the connection between the source and destination of funds. Utilizing algorithms, mixers create distinct pools and facilitate the exchange of various cryptocurrencies. By obscuring sender and receiver information, mixers make it challenging for investigators to identify the source and destination addresses.

Different kind of mixers exist: centralized mixers are operated by private third-party services that users rely on to mix their crypto assets, whereas decentralized mixers function as peer-to-peer protocols with an automated mixing process.

When using centralized mixers, users transfer their funds to wallet addresses controlled by these mixers, pay a service fee, and specify the destination. Upon receipt of these funds, the mixer combines them with funds from other users in a pool and redistributes them. Centralized mixers, however, pose the additional risk of placing trust in a third party. There is a potential risk of losing funds if the network or the company ceases operations. Additionally, due to the significant volume of funds they handle, centralized mixers become prime targets for hackers and may also present risks of malicious behavior from the company itself. Some centralized mixers may even store user information privately, compromising the anonymity they aim to provide. The efficiency of centralized mixers increases with more users, as a larger user base reduces the likelihood of detection.

Decentralized mixers utilize open-source protocols like CoinJoin to facilitate an automated and permissionless mixing process. They rely on multiple users participating in the protocol, consolidating their funds into a single large transaction and directing different Bitcoins to various destination addresses.

In noncustodial mixers, a common feature involves the utilization of publicly verifiable and transparent smart contracts or secure multi-party computation to replace the need for a trusted mixing entity. The process of noncustodial mixing typically involves two steps. Initially, users deposit an identical amount of Ether (ETH) or other tokens into a mixer contract from an address. Subsequently, following a user-defined time interval,

they are able to withdraw their deposited coins via a withdrawal transaction to a new address; in the meantime, the cryptocurrencies are tumbled in a number of different ways.

To address these challenges, nations worldwide have implemented regulatory measures targeting crypto mixers due to their involvement in financial transactions. In the United States, for instance, the Financial Crimes Enforcement Network (FinCEN) mandates that all mixers must comply with registration requirements outlined in the Bank Secrecy Act.

Furthermore, in the year 2022, the United States Office of Foreign Assets Control ("OFAC") took decisive action by imposing sanctions on prominent crypto mixers such as Tornado Cash and Blender.io. OFAC administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States.

According to statements from the U.S. Treasury, Tornado Cash was allegedly utilized in the laundering of over 7 billion dollars since its inception, while Blender.io was purportedly involved in facilitating money laundering activities linked to a North Korean hacker group.

These sanctions go beyond merely prohibiting individuals in the U.S. from conducting business with the aforementioned services; they also involve freezing any assets held by these entities within the United States. This aggressive stance underscores the global commitment to combating illicit financial activities facilitated by crypto mixers and serves as a deterrent against their misuse in the future.

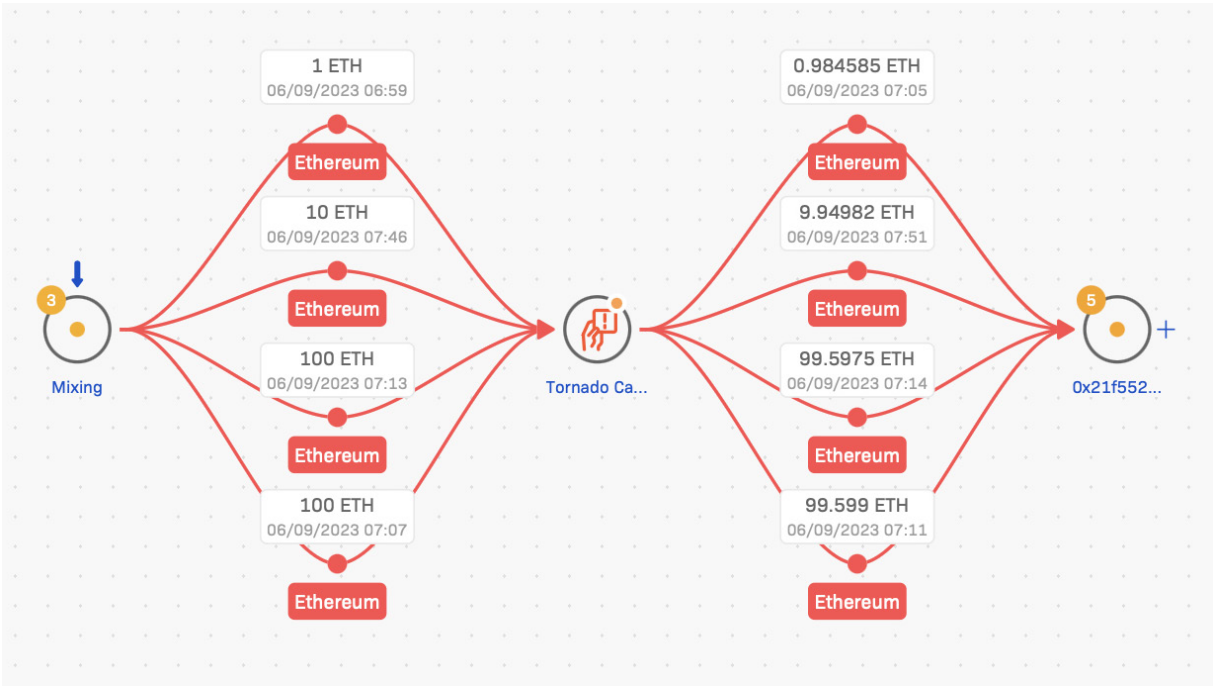


Figure 1- Example of funds going through a decentralised mixer (Tornado Cash) and de-anonymised using Crystal Expert, a blockchain analytic tool by Crystal Intelligence

Privacy coins and chain hopping

Privacy coins such as Monero, Dash and Zcash have garnered significant attention in recent high-profile criminal investigations. A vast majority of darknet marketplaces, including the now-defunct AlphaBay, readily accept Monero as payment for goods and services. Additionally, recent actions taken by the OFAC highlight the increasing use of privacy coins by cybercriminals in their illicit operations.

However, it's important to note that not all privacy coins carry the same level of risk in terms of facilitating money laundering and terrorist financing (ML/TF). While Monero boasts robust privacy features that make it resistant to blockchain analytics, other privacy coins like Zcash lack such built-in privacy measures. Consequently, transactions involving these coins can be scrutinized by blockchain analytics experts, allowing for the detection of potential illicit activities, similar to transactions involving non-privacy coins.

A common strategy employed by criminal actors, often in conjunction with privacy coins, is the practice of chain hopping. This tactic involves moving funds between different cryptocurrencies and blockchains to obfuscate the trail of transactions. The FATF highlighted this emerging risk in 2022, underscoring its potential impact on anti-money laundering efforts and the need for enhanced regulatory oversight.

The prevalence of chain hopping has surged in recent years, largely driven by the proliferation of decentralized exchanges and "coinswap" services. These platforms facilitate peer-to-peer transactions and crypto-to-crypto exchanges with minimal or no know-your-customer checks, enabling participants to maintain a higher level of anonymity. This trend poses significant challenges for law enforcement and regulatory authorities in their efforts to combat financial crim es facilitated by privacy coins and decentralized financial services[10].

10. https://crystalintelligence.com/thought-leadership/how-to-investigate-emerging-risks-related-to-cross-chain-crime/

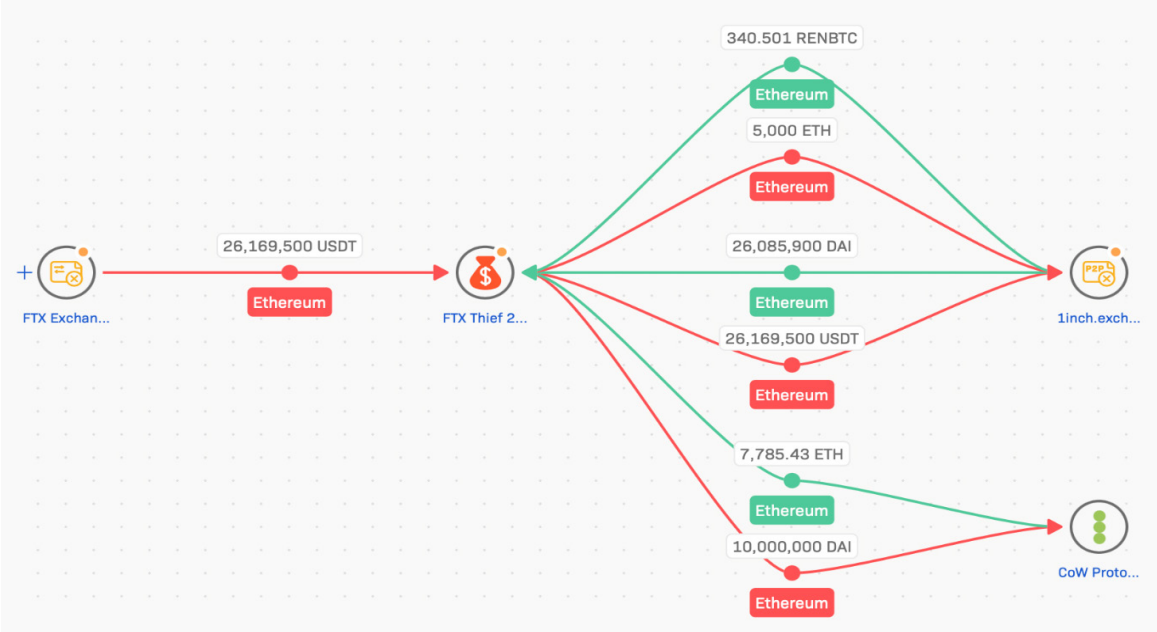


Figure 2 - Funds stolen from a prominent exchange and swapped through different cryptocurrencies. Visualisation by Crystal Intelligence's Expert tool

Blockchain analytics tools play a crucial role in investigating chain hopping by providing insights into the movement of funds across different cryptocurrencies and blockchains. Here's how these tools can aid in the investigation:

1. **Transaction Tracking:** Blockchain analytics tools can track transactions across multiple blockchains, allowing investigators to follow the flow of funds as they are moved from one cryptocurrency to another. By analyzing the transaction history and associated addresses, investigators can uncover patterns and connections between different crypto assets involved in chain hopping.

2. **Address Clustering:** These tools employ sophisticated algorithms to cluster together addresses belonging to the same entity or wallet. By identifying clusters of addresses involved in chain hopping activities, investigators can gain a comprehensive view of the entities involved and their transaction patterns across various cryptocurrencies.

3. **Pattern Recognition:** Blockchain analytics tools can detect patterns indicative of chain hopping, such as rapid and frequent exchanges between different cryptocurrencies or the use of specific decentralized exchange platforms known for facilitating such activities. By recognizing these patterns, investigators can flag suspicious transactions for further analysis.

4. **Risk Scoring:** Some blockchain analytics tools offer risk scoring capabilities that assess the likelihood of transactions being associated with illicit activities. By assigning risk scores to transactions involved in chain hopping, investigators can prioritize their efforts and focus on high-risk transactions that warrant closer scrutiny.

5. **Visualization:** Visualization features in blockchain analytics tools enable investigators to visualize the flow of funds across different cryptocurrencies and blockchains. By creating visual representations of transaction networks and relationships, investigators can gain insights into the complexity of chain hopping activities and identify key nodes or entities involved.

It is crucial to choose the right tool for the investigation, depending on the circumstances and taking into account the blockchains involved.

- The tool should support a wide range of cryptocurrencies and blockchains from the most popular like Bitcoin and Ethereum to the ones most used by criminals like Tron;
- Must be able to provide robust analytics, including transaction tracing, address clustering, and wallet identification. Features like graph visualizations are essential and can help illustrate complex relationships,
- A user-friendly interface is crucial, especially for investigators who may not be blockchain experts. The tool should offer intuitive navigation and clear visualizations;
- Real-time monitoring and alerts for suspicious activities can be vital for timely investigations;
- Evaluate the pricing model to ensure it fits within budget constraints while offering the necessary features;
- Research the tool's reputation within the industry, including user reviews and case studies, to assess its reliability and effectiveness.

Layer 2 Solutions

So-called "layer 2 solutions" in the context of blockchain refer to technologies or protocols that are built on top of an existing blockchain network (which constitute Layer 1, such as Bitcoin or Ethereum). The primary goal of Layer 2 solutions is to enhance the scalability, efficiency, and speed of the blockchain without compromising its security or decentralization.

These solutions handle transactions off the main blockchain, reducing the load and congestion on Layer 1 while still benefiting from its security features. This also means that often transactions performed on Layer 2 are not visible, or not entirely, on Layer 1.

Key Characteristics of Layer 2 Solutions

- **Off-Chain Processing:** Transactions or computations are moved off the main chain (Layer 1) to a secondary layer. This off-chain processing reduces the data burden on the main blockchain, increasing its overall speed and efficiency.
- **Enhanced Scalability:** By processing many transactions outside the main chain, Layer 2 solutions can significantly increase the number of transactions per second that a blockchain network can handle.
- **Reduced Transaction Fees:** Since fewer transactions are processed directly on the main blockchain, the fees for each transaction are often lower on Layer 2 solutions.
- **Security Benefits:** Although transactions are processed off-chain, the security of these solutions still relies on the underlying Layer 1 blockchain. In case of a dispute or need for validation, the transaction details can be referred back to the main chain.

Different types of layer 2 solutions exists, with different characteristics. The most common solutions include:

State Channels (Bitcoin's Lightning Network, Ethereum's Raiden Network): state channels allow two parties to create a multi-signature wallet and conduct many transactions off-chain. These transactions are only recorded on the blockchain when the channel is closed, reducing the load on the main chain.

Rollups: a process that bundles multiple transactions into a single batch that is processed off-chain. The data or proof of these transactions is then submitted to the main chain in a compressed form.

Sidechains (Polygon): independent blockchains that run in parallel to the main blockchain (Layer 1). They have their own consensus mechanisms and can operate autonomously. Transactions on sidechains can be periodically settled on the main blockchain for added security.

Layer 2 solutions address the scalability trilemma in blockchain technology, which suggests that it is challenging to achieve scalability, security, and decentralization all at the same time. By focusing on scalability while leveraging the security and decentralization of the underlying Layer 1 chain, Layer 2 solutions make blockchains more practical for mass adoption, especially for use cases like payments, decentralized finance (DeFi), and NFTs.

While enhancing blockchain scalability and transaction speed, these solutions can introduce significant challenges and opacity issues for law enforcement and regulators, due to the way Layer 2 networks operate in relation to the underlying blockchains. State channels, for example, like the Bitcoin Lightning Network, involve two parties conduct-

ing transactions privately until they close the channel and settle the balance on the main blockchain. All intermediate transactions are hidden from the blockchain. Since they can handle their transactions off-chain, those are not immediately recorded on the main blockchain, significantly reducing transparency.

To mitigate this problem, LE Agencies should partner with firms that specialise in blockchain analysis, which can help in tracing those transactions and understanding how they interact with the underlying blockchain and other networks.

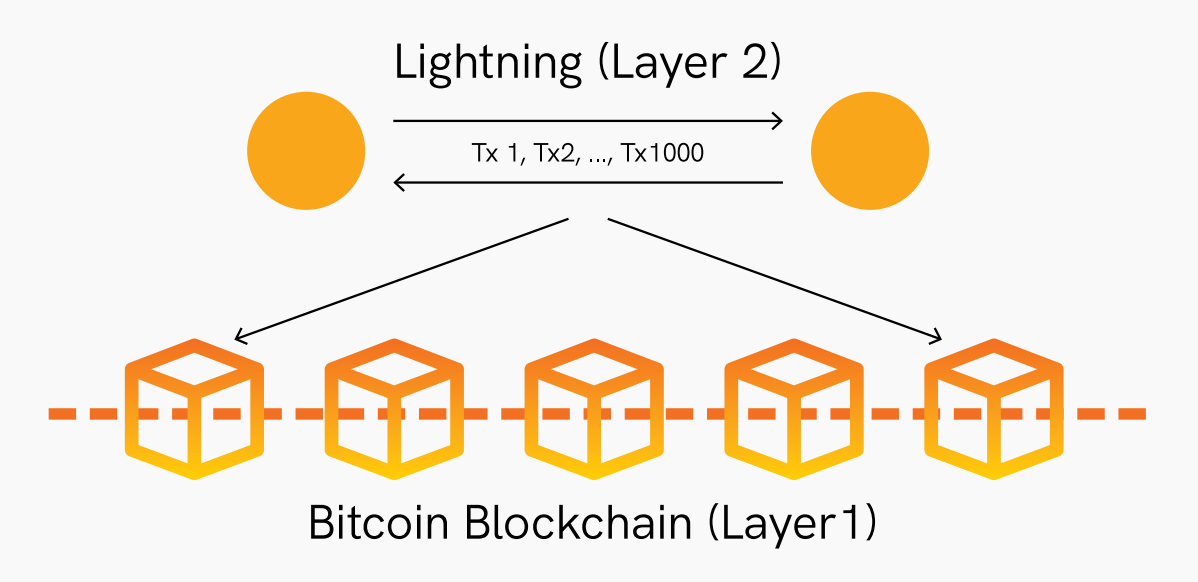


Figure 3 - Representation of the Bitcoin Lightning Network

4. Investigating cryptocurrency

As the use of cryptocurrencies proliferates, so too do illicit activities ranging from money laundering and fraud to drug trafficking and terrorism financing. In response, law enforcement entities face the daunting challenge of navigating this complex and decentralized ecosystem to uphold justice and maintain the integrity of financial systems.

This chapter delves into the intricate world of cryptocurrency investigations, offering law enforcement professionals a comprehensive roadmap to effectively navigate the nuances of this digital realm.

Navigating the labyrinth of cryptocurrency investigations requires a multifaceted approach that integrates technical expertise, legal acumen, and collaboration across jurisdictions. By deciphering the intricate web of blockchain transactions and identifying patterns indicative of illicit activity, law enforcement can disrupt criminal networks and hold perpetrators accountable.

Furthermore, this chapter explores the evolving legal landscape surrounding cryptocurrencies and their seizure, shedding light on the emerging trends and regulatory challenges.

Ultimately, the fight against cryptocurrency-enabled crime demands a proactive and collaborative effort, where law enforcement agencies from different jurisdictions, VASPs, and industry stakeholders work in tandem to fight criminal activities involving crypto assets. Through continuous education, innovation, and cooperation, we can unravel the complexities of cryptocurrency investigations and uphold the rule of law in the digital age.

4.1. Investigation security

When investigating criminal activity that involve any use of the internet, it is crucial to seek and preserve security and, in some cases, anonymity. Virtual machines play a crucial role in this process for several reasons, providing investigators with valuable tools and capabilities and allow them to run an operating system and all its applications on a virtualised environment that operates independently their actual physical computer.

Which are the main reasons to use Virtual Machines? There are especially two that are important in criminal investigations:

- Isolation and Containment: they allow investigators to create isolated and contained environments for analysing potentially malicious or suspicious software, files, data or websites. This prevents the spread of malware or any harmful effects to the investigator's actual operating system, and prevent the criminals under scrutiny to locate and identify the investigating actors;
- Safe Interaction with Malicious Content: In cases where investigators need to interact with potentially harmful content, such as phishing emails, malicious websites, or suspicious files, VMs provide a safe and controlled environment for doing so without compromising the investigator's actual system.

Another crucial aspect of this kind of criminal investigations is the preservation on the investigator's identity and location. What helps in those cases is the use of a VPN, a Virtual Private Network, which is a tool that enables secure and private communication over the internet. It establishes a secure connection, often referred to as a tunnel, between your device (such as a computer, smartphone, or tablet) and a server operated by the VPN service provider. This tunnel encrypts the data traveling between your device and the server, ensuring the confidentiality and integrity of the information, something that Investigators often need when communicating and sharing sensitive information.

Moreover, by masking your real IP address with the IP address of the VPN server, a VPN helps anonymise any online activity. This adds a layer of privacy and is crucial when conducting online investigations, as it makes it more challenging for suspects or adversaries to trace the investigators back to their actual locations.

Should investigator use the many available free VPN services available online, or should they go for subscription-based version? The choice between the two, especially in investigations, depends on several factors, and there are pros and cons associated with both options.

Free VPNs have the obvious advantage of being free of charge, which can be appealing for investigators working within budget constraints. They are also readily available, and users can quickly download and start using them without the need for payment. On the other hand, free VPNs often come with limitations on features, bandwidth, and server locations and may compromise user privacy by logging and selling user data to third parties. They can also experience downtime, have slower connection speeds, or lack customer support, impacting their reliability.

Paid VPNs provide better security features, including strong encryption, no-logs policies, and advanced security protocols and typically offer better server infrastructure, leading to faster and more reliable connections. This is crucial for investigators who

need consistent and secure access to online resources. They often provide customer support, which can be essential for investigators who may encounter technical issues or have specific requirements and are more likely to have transparent privacy policies and a commitment to protecting user data, reducing the risk of unauthorised data sharing.

When investigating over the internet, LEs should also pay careful attention to not disclosing their personal or working email addresses: many websites require authentication or registration, and an email address is also among the mandatory data requested. Therefore, a newly created email address can be used in those situations.

Metadata is also something every investigator must keep in mind when they want to stay anonymous. Metadata refers to information about the file itself rather than the actual content within the file. Metadata provides valuable information about a file, helping users and applications organize, manage, and understand the characteristics of the data.

Some common types of file metadata include file name and type, size, date and time stamp (including timestamp of last access or last modification), owner and permissions. In case of pictures, that would also include phone model, brand and geolocation.

4.2. Looking for OSINT

OSINT (Open Source Intelligence) plays a crucial role in cryptocurrency investigations: the decentralised, pseudonymous, and global nature of cryptocurrencies makes traditional investigative methods less effective, but OSINT may offer valuable data to track, trace, and analyse blockchain activity and associated entities. While blockchain explorers or professional tools can be used to map out transaction paths and identify clusters of wallet addresses controlled by the same entity, OSINT techniques are effective in linking those cryptocurrency wallet addresses to identifiable individuals or organisations. Investigators can use data from public forums, social media platforms, or online marketplaces where users might have exposed their wallet addresses. Below we will explore some of the instances where OSINT becomes crucial in a crypto investigation.

- **Blockchain Transparency:** although cryptocurrency transactions are pseudonymous, the blockchain ledger is public and immutable. As we will see later, OSINT techniques can be used to trace transactions and analyze patterns on the blockchain to link wallet addresses with real-world entities, using also data from public forums, social media platforms, or online marketplaces where users might have exposed their wallet addresses.

- **Exchange Accounts and KYC Data**: many cryptocurrency exchanges require users to go through Know Your Customer (KYC) processes. OSINT can help identify the exchanges that a wallet is associated with, making it possible to request additional data from these exchanges through legal channels.

- **Phishing and Scam Analysis**: OSINT can identify common patterns and tactics used in cryptocurrency-related scams, such as phishing websites that imitate legitimate crypto services. By analyzing the domain registrations, website content, and user complaints, investigators can trace these scams to their origins. Similarly, they can be used to detect signs of Ponzi schemes, investment frauds, or pump-and-dump schemes in crypto communities by tracking suspicious activities, promotions, and sudden spikes in trading volumes.

- **Dark Web Marketplaces**: criminal activities involving cryptocurrencies often occur on the dark web. OSINT techniques allow investigators to monitor these marketplaces and forums to track illicit transactions, money laundering schemes, or even ransom payments.

- **Social Media Intelligence**: users often share cryptocurrency addresses on social media platforms, either knowingly or unknowingly, which can be crucial in linking accounts to real-world identities. Investigators will look for discussions around cryptocurrency transactions that relate to scams, frauds, or hacks.

4.3. Investigative techniques

While we have seen that the use of cryptocurrency provides criminals with a certain level of anonymity and can frustrate investigators trying to locate proceeds of crime or trying to discover the origin of certain transaction, techniques exist that may help Law Enforcement to utilise blockchain data and other clues to pierce the veil of anonymity.

Like in old style investigations, simulated undercover purchases still constitute a useful method. Whether is a dark web market or any other service accepting cryptocurrency, a controlled purchase will expose at least one address under the criminals' control: in order to receive funds, at least one receiving address must be provided to the buyer and that would be the investigative starting point.

Heuristics can then be applied to create a cluster of addresses that are under the control of the same suspect. Once a cluster is identified, the investigators' job will be to follow those transactions, in both directions (transactions sending coins to the target cluster but also sent from the cluster) until an address is found which is controlled by an entity that can provide clues about the identity of the receiver (or sender) of those transactions.

Among the most common heuristics, we can find:

- **Multi input or Common Input Ownership:** is one of the core heuristics used by chain analysis companies to determine the owner of specific UTXOs. This heuristic currently assumes that all inputs of a given transaction are owned by the same owner. This heuristic has never offered certainty, and as Bitcoin continues to evolve, it is becom-

ing less reliable. Technologies such as CoinJoin, CoinSwap, regular multisig, and, in the future, MuSig transactions all contradict this heuristic by accepting inputs from many different parties.

- **Change address detection:** the change address detection heuristic relies on the attributes of UTXOs. Since sending the exact specified amount of funds to the receiver is challenging, any surplus funds are typically returned to the sender via a change address. Therefore, detecting change addresses is essential as they are integral to the entity's operations.

While following and tracing transactions on the blockchain, investigators must keep in mind their ultimate goals: to identify suspects, when they are not already known to them, and secure their convictions but also, and this aspect is becoming more and more important, to locate and seize their assets.

Free tools exist that allow investigators to surf the blockchain and follow the money. Arkham is one of those tools; they allow a quick overview of different blockchains and to follow transactions from one address to another. Often, a basic clustering is applied, allowing the detection of transfer to VASPs. What they often lack, however, is a proper visualisation and a verifiable source of the information used to cluster addresses.

4.4. Blockchain Analysis Tools

On the other hand, Law Enforcement are increasingly using blockchain analytics provider's tools which provide a comprehensive, powerful and reliable way to extract information. Blockchain analytics tools offer visibility into blockchain transactions. Information recorded on the blockchain is encoded and verified within publicly accessible and immutable records. These tools monitor these records and structure the data to illustrate the connections between various cryptocurrency wallets.

What makes a blockchain analysis tool a good one?

- **Coverage:** tools must be able to parse and track an extensive portfolio of digital assets and blockchains.
- **User Interface:** an intuitive and user-friendly interface facilitates the analysis of transactions and makes it intuitive to follow transactions and identify entities.
- **Updated information:** tools need to monitor transactions on different blockchains in real time. They also need to be updated on the latest sanction lists.

11. https://platform.arkhamintelligence.com

- **Case management:** tools will provide an easy way for investigators to share information, analysis and graphs internally and externally.
- **Transparent and reliable source of information:** analytics tool must provide the information that led them to make a particular attribution of ownership, as this information can be double checked, supported by other sources, and will be critical in court.
- **Visualisation tools:** graphs make it very easy to understand activity on the blockchain and interactions between addresses, and provide evidence in court that will clearly illustrate the steps taken by criminals.

Using those tools, investigators will typically follow the funds on the blockchain, moving from address to address, and sometimes from blockchain to blockchain, until their location is known and identified. Here they will face two possible scenarios: either funds are held into private, or unhosted wallets, or they have reached a VASP or a similar service, with the aim of being converted to fiat and cashed out. Depending on which solution has been used by criminals, investigators will adapt their investigative strategies accordingly.

4.5. Unhosted (private) wallets

While following transactions on the blockchain, often times investigators will face this situation: after a number of hops (a hop means a transaction moving funds from one address to the next) funds reach an address and don't move any further. Some tools will visualize them as "unspent" or "settled": the result is the same, funds are sitting within an address which seems, according to the tools used, privately held; the funds have not been deposited with an exchange or any other service which could be subpoenaed. More importantly for the investigations, the suspect is the one holding the private keys.

An unhosted wallet is often referred to as cold storage or self-custody and enables users to manage their cryptocurrency balance independently of an exchange, similar to keeping cash in a personal wallet. Examples include hardware wallets like Ledger or Trezor, mobile apps, or software solutions such as Electrum. In contrast, a hosted wallet is one managed by a third-party platform, such as verified exchanges like Coinbase, Crypto.com, or Binance.

In this situation, in order to seize the proceeds of crime and the funds connected to the illicit activity, investigators will need to locate the private keys and take control of them, before moving forward to the next step.

> A private key looks like this:
>
> **KxRpTxdFnmanomZzq8YVt5NcfJQbi19xDTDkmLV1D8fHEKFyqBmT** (Bitcoin)

2410FD14C3AA9340E57FE64B25CDCDE514A85CB1B46E157E11B3232264254373
(Bitcoin – hexadecimal)

DC38EE117CAE37750EB1ECC5CFD3DE8E85963B481B93E732C5D0CB66EE6B0C9D
(Ethereum – hexadecimal)

A private key is, essentially, a long string of number and letters: it can be stored, therefore, in numerous different places, physical and digital. In the following examples, we will consider different scenarios and for each one, we will locate the private keys.

Mobile applications

The most common typology of self-custody, is a mobile wallet, a software application installed on a phone or tablet that allow users to receive, send and store cryptocurrency.

There are two primary types of cryptocurrency wallets: custodial and noncustodial. Custodial wallets are managed by a third party that holds and secures your private keys on your behalf. These third parties often provide robust, enterprise-level data security systems to protect your assets, similar to how businesses safeguard their sensitive information. Many cryptocurrency exchanges, such as Coinbase or Binance, offer custodial wallets to their users, ensuring that their funds are stored with advanced security measures.

In contrast, noncustodial wallets give you full control and responsibility over your private keys. This means you are solely responsible for the security and management of your cryptocurrency. Noncustodial wallets are typically used on personal devices, such as smartphones or computers. The use of a noncustodial wallet, provides a person with direct access to funds without relying on a third party.

In this situation, once a similar software/application is found, investigators can initiate a transaction directly from it, moving the funds to a controlled address.

Hardware wallets

A hardware wallet is a physical device designed to securely store the private keys. Unlike software wallets seen before, hardware wallets provide an extra layer of security by keeping the private keys offline, reducing the risk of them being exposed to malware or hackers.

Key features of hardware wallets include:

1. **Offline Storage:** Private keys are stored on the device itself and never leave it, even when connected to a computer or mobile device. This ensures that your keys remain secure even if your computer is compromised.

2. **Secure Transactions:** When one needs to send or receive cryptocurrency, the transaction is signed within the hardware wallet itself. This means the private keys are never exposed to your connected device or the internet.

3. **PIN Protection:** Hardware wallets are typically protected by a PIN code, adding an extra layer of security. Even if the device is lost or stolen, the PIN helps prevent unauthorized access.

4. **Backup and Recovery:** Hardware wallets usually come with a recovery seed, a list of words that can be used to restore the wallet (see next paragraph).

5. **Compatibility:** Most hardware wallets are compatible with various cryptocurrencies and can be used with multiple wallet applications, allowing for flexibility in managing different digital assets.

Popular examples of hardware wallets include Ledger and Trezor. Investigators would first need to physically obtain the hardware wallet. This typically occurs through search warrants or raids: law enforcement can execute search warrants to seize physical hardware wallets from a suspect's property.

Like in the previous example of mobile wallets, in this situation investigators can seize the wallet and initiate a transaction from it to move the funds to a controlled wallet. Once the hardware wallet is in custody, accessing the funds requires the use, if this function is enabled, of the device PIN or passphrase: authorities might compel the owner to provide the PIN or passphrase through legal means, such as court orders or plea bargains.

Seed Phrases

Whether the suspects have used a mobile or an hardware wallet, they have an important feature in common: they both use a form of protection, called "seed phrase".

A seed phrase, also known as a recovery phrase or mnemonic phrase, is a sequence of words generated by a cryptocurrency wallet that gives the user access to the wallet's funds. It serves as a backup mechanism, allowing the user to recover their wallet and its contents if the wallet is lost, damaged, or otherwise inaccessible.

Typically, a seed phrase consists of 12, 18, or 24 randomly generated words. These words are selected from a standardized list (such as the BIP-39 word list) to ensure uniformity and compatibility across different wallets.The use of common words instead of complex strings of characters makes it easier for users to write down and store the phrase securely. When a new wallet is created, the wallet software generates a seed phrase and instructs the user to write it down and store it safely. This seed phrase is linked to the wallet's private key through a deterministic algorithm, allowing the regeneration of the private keys from the seed phrase.

Even if a wallet is not found during a search on the suspect, the retrival of the seed phrase is sufficient to take control of the assets and move them to a controlled address. Investigators will create a new wallet, or use one in their possession, and will then input the seed phrase into the wallet software. The software uses the phrase to regenerate the private keys and associated addresses, giving the investigators access to their cryptocurrency holdings.

Steps involved:

- Download the wallet software or obtain a new hardware wallet.
- During the setup process, choose the option to restore a wallet.
- Enter the seed phrase accurately when prompted.
- The wallet software will regenerate the private keys and addresses, giving you access to your funds

Planning ahead the capture of an unhosted wallet

As law enforcement preparing for a search and seizure of unhosted wallets (such as hardware or software wallets), it is essential to approach the operation with meticulous planning and adherence to legal protocols. Due to the peculiarities of seizing cryptocurrencies, the operation should be planned in advance to make sure all the following points are taken into account and covered properly.

Obtain Proper Warrants: Secure a search warrant that explicitly authorizes the seizure of digital assets, including hardware wallets, software wallets, and any related devices. Ensure the warrant details the specific locations to be searched and the types of items to be seized to avoid overstepping legal boundaries.

Consult Experts: Engage with cybersecurity and cryptocurrency experts to understand the technical aspects of unhosted wallets and how they can be accessed or seized.

Operational Planning: Use surveillance and informants to gather information about the suspect's properties and potential hiding spots for hardware wallets. Analyze the suspect's digital footprint, including social media, online transactions, and communications, to identify possible locations of digital assets.

Prepare Specialized Equipment: Equip the team with forensic tools designed to handle and analyze hardware wallets and encrypted devices. Have data recovery tools ready to extract information from seized devices. Make sure to have technical support personnel are on hand to assist with any unexpected technical challenges during the operation.

Execution of the Search: Secure the area to prevent the suspect from destroying or hiding devices during the search and move quickly to prevent the suspect from using

self-destruct mechanisms or encryption tools to erase data. Collect all devices that might store or have access to digital assets, including computers, smartphones, tablets, USB drives, and written notes that might contain seed phrases.

Handle Devices Carefully: handle all devices carefully to avoid data destruction. For hardware wallets, ensure they remain powered off to prevent any remote wipe commands. Record the location and condition of each seized item, including serial numbers and any visible identifiers.

4.6. Hosted wallets

A hosted wallet, also known as a custodial wallet, is a type of cryptocurrency wallet where a third party (such as a cryptocurrency exchange or wallet service provider) holds and manages the user's private keys on their behalf. This third party is responsible for securing the funds and providing various services related to the wallet's management and transactions.

Most hosted wallet providers perform Know Your Customer (KYC) procedures as part of their regulatory compliance efforts. KYC is a process used by financial institutions, including cryptocurrency exchanges and wallet providers, to verify the identity of their customers and assess the risk of illegal activities, such as money laundering and terrorism financing. In this phase, users are required to provide personal information, such as their full name, date of birth, address, banking details, government-issued identification documents (e.g., passport, driver's license) and place of residency.

It is usually good news when, while following transactions on the blockchain, investigators can see funds landing on an address controlled by a service provider like a VASP: it means that now investigators can, through the appropriate mechanisms, obtain information from the service regarding the identity of the person controlling the account and ask the service to freeze the crypto assets (or fiat currency) held in the name of the customer.

It is fundamental for investigator to understand that, once they see on the blockchain a transaction reaching a service like a VASP, they should stop following the chain of the subsequent transactions. When users deposit cryptocurrency with a service, they will be provided with a deposit address, meaning the crypto address to which they can send money to in order to credit their account. After crediting the user with the corresponding amount, services will usually move those funds to other internal wallets and use those funds for other operations that have nothing to do with the user depositing the money. If and when, at a later stage, users want to move and withdraw the funds they have deposited, for example to an unhosted wallet or to another provider, the funds will come from a completely unrelated address which is different from the deposit address initially used. The only way to understand the internal transactions and determine which address has been used to withdraw funds (and consequently to determine the receiving address), is to receive this information from the service provider.

What kind of information is the service provider capable of providing to the requesting law enforcement?

- **User's depositing address:** this is the address assigned to the user to deposits crypto assets. This address may remain the same, even in case of multiple deposits, or change in time.
- **User's withdraw address:** if crypto assets are moved out from the VASP to a self hosted wallet, a service or another VASP, this information can be made available to the investigators.
- **KYC:** all data related to the customer, including full name, date of birth, address, government-issued identification documents, place of residency and banking details. If the customer is a legal entity, this data will include incorporation documents.
- **2FA:** 2FA stands for Two-Factor Authentication. It is a security measure used to add an extra layer of protection to online accounts and services. The second factor is something the user possesses, such as a mobile device, security token, or hardware key. This may provide investigators with a mobile number used by the suspect.

A subpoena to a VASP works similarly to a subpoena issued to any other financial institution or service provider. However, a few aspects should be taken into account by law enforcement agencies before submitting a request.

- **Correct language:** the crypto sphere has developed its own set of specific jargon and terminology over the years. This jargon is often used by cryptocurrency enthusiasts, traders, developers, and other participants in the crypto ecosystem, but has also become widely accepted and can be very specific. Writing a subpoena to a service provider will require investigator to become familiar with the terminology used, or will incur the risk of the request not being completely and thoroughly understood.
- **Use of text files:** as we have seen before, addresses, private keys and transactions' identifier are long string of numbers and letters, likely prone to mistakes and typos if one has to read and type from a pdf document. It is good practice to send this information in a file format that allows copy-pasting, like doc or txt files.
- **Informal contacts:** VASPs have, in recent years, expanded their teams dedicated to assist law enforcement with their requests. Moreover, some actions are time-sensitive and require immediate actions. Establishing informal contacts with VASPs, even before a formal request is served, helps speeding up the process in several ways: a draft request can be reviewed and amended if needed, avoiding lengthy back and forth; VASPs can assess whether all the required information has been provided; in time-sensitive occasions, VASPs can take urgent actions, like preventing any transactions from the account under scrutiny, while waiting for the formal subpoena.

5. International cooperation

As criminals increasingly operate across borders, leveraging the global reach of blockchain technology, the need for international cooperation in cryptocurrency criminal investigations has never been more critical. Law Enforcement need to explore the complexities of tracing illicit transactions that span multiple jurisdictions and highlight the essential mechanisms and frameworks that facilitate cross-border cooperation among law enforcement agencies, regulatory bodies, and financial institutions.

Unlike traditional financial systems, which are often regulated and monitored within specific jurisdictions, the decentralized and pseudonymous nature of cryptocurrencies enables perpetrators to obscure their identities and locations effectively.

Several typologies of criminal activity involving cryptocurrencies are particularly transnational in nature, including:

- **Money Laundering:** Criminals use cryptocurrencies to launder money by converting illicit funds into digital assets, which can then be moved across borders and exchanged for fiat currency in different jurisdictions, making the funds harder to trace.
- **Fraud and Scams:** Fraudulent schemes such as Ponzi schemes, phishing attacks, and investment scams can target victims in multiple countries simultaneously, exploiting the anonymity of cryptocurrency transactions to evade detection and prosecution.
- **Ransomware Attacks:** Cybercriminals deploy ransomware to lock victims' data and demand payment in cryptocurrencies. These attacks are often orchestrated from one country, target entities in another, and route payments through various international exchanges to obfuscate the money trail.
- **Terrorism Financing:** Terrorist organizations have increasingly turned to cryptocurrencies to fund their activities, taking advantage of the ability to transfer value across borders without the oversight typical of traditional banking systems.

One of the most significant challenges in combating transnational cryptocurrency crimes is the issue of jurisdiction. Law enforcement agencies are typically confined to

operating within their national borders, while cryptocurrency transactions can easily cross these borders without any physical presence. This disconnect creates several problems:

- **Jurisdictional Overlap:** Multiple countries may claim jurisdiction over a single cryptocurrency crime, leading to conflicts and inefficiencies in investigation and prosecution.
- **Lack of Jurisdiction:** In some cases, no single country may have clear jurisdiction, especially if the criminal and victim are in different countries, and the servers or exchanges used are located in yet another set of jurisdictions.
- **Legal Inconsistencies:** Different countries have varying laws and regulations regarding cryptocurrencies, leading to inconsistencies in how crimes are defined, investigated, and prosecuted. This can create loopholes that criminals exploit to avoid justice.

5.1. International cooperation Mechanisms

International cooperation in cryptocurrency criminal investigations relies on a variety of mechanisms designed to facilitate effective collaboration among nations. These mechanisms enable the sharing of information, resources, and expertise, making it possible to tackle complex and transnational cryptocurrency crimes more efficiently.

Mutual Legal Assistance Treaties (MLATs)

MLATs are bilateral or multilateral agreements between countries that provide a framework for requesting and exchanging evidence in criminal investigations and prosecutions. MLATs are crucial for obtaining information that is beyond the reach of domestic law enforcement agencies.

- **Process:** When a country needs assistance from another jurisdiction, it submits an MLAT request through designated central authorities, typically the Ministry of Justice or a similar entity. The request outlines the nature of the investigation, the specific assistance required, and the legal basis for the request.
- **Benefits:** MLATs facilitate the collection of evidence, such as transaction records from foreign cryptocurrency exchanges, witness statements, and digital forensics. They ensure that evidence is obtained legally and can be admissible in court.
- **Application:** In a high-profile case, the a country in South America might use an MLAT to request transaction data from a European cryptocurrency exchange to trace funds linked to a ransomware attack. This cooperation is essential for building a robust case against the perpetrators.

Joint Investigative Teams (JITs)

JITs are collaborative groups formed by law enforcement agencies from multiple countries to work on specific cases involving transnational crime. JITs allow for real-time information sharing and coordinated actions.

- **Process:** Countries involved in a transnational investigation agree to establish a JIT through a formal agreement. Members of the JIT, which can include police, prosecutors, and other specialists, work together, often in a single location, to pool their resources and expertise.
- **Benefits:** JITs enhance operational efficiency, reduce duplication of efforts, and enable synchronized actions such as simultaneous arrests and searches in different countries. They foster trust and close cooperation among international partners.
- **Application:** A JIT might be formed between agencies in the United States, the United Kingdom, and Australia to investigate a global cryptocurrency fraud scheme. By working together, the team can swiftly share intelligence, coordinate interviews with suspects and witnesses, and conduct simultaneous raids to dismantle the criminal network.

Information-Sharing Platforms

Information-sharing platforms, such as the Egmont Group and Europol's Secure Information Exchange Network Application (SIENA), facilitate the rapid exchange of intelligence and data between countries.

- **Process:** Participating agencies share information through secure, standardized channels. These platforms provide a framework for submitting and responding to information requests, ensuring data integrity and confidentiality.
- **Benefits:** Information-sharing platforms enable timely access to critical data, such as suspicious transaction reports, which can be pivotal in identifying and disrupting criminal activities. They also support analytical tools that help in tracing cryptocurrency transactions and uncovering criminal networks.
- **Application:** Through the Egmont Group, a financial intelligence unit (FIU) in Canada might alert its counterparts in Japan and Germany about suspicious cryptocurrency transactions linked to a money laundering operation. This prompt exchange of information allows for a coordinated response and the freezing of illicit assets.

INTERPOL and Europol

International policing organizations like INTERPOL and Europol play a vital role in fostering international cooperation in cryptocurrency investigations.

- **Process:** INTERPOL and Europol provide platforms for law enforcement agencies to collaborate on investigations, share intelligence, and access specialized resources. They also organize training sessions, conferences, and joint operations.
- **Benefits:** These organizations enhance global law enforcement capabilities by offering expertise in digital forensics, cybersecurity, and cryptocurrency tracing. They also facilitate cross-border investigations through coordination and support.
- **Application:** Europol's European Cybercrime Centre (EC3) might lead a coordinated effort involving multiple European law enforcement agencies to dismantle a dark web marketplace dealing in illegal goods and services paid for with cryptocurrencies. INTERPOL can issue international alerts, such as Red Notices, to locate and apprehend suspects globally.

5.2. Challenges and obstacles in International Cooperation

Despite the frameworks and mechanisms in place to facilitate international cooperation in cryptocurrency criminal investigations, numerous challenges and obstacles remain. These barriers can significantly hinder the effectiveness of cross-border efforts to combat cryptocurrency-related crimes.

One of the primary challenges in international cooperation is the issue of jurisdictional conflicts. Different countries have varying legal systems, laws, and regulations concerning cryptocurrencies, which can lead to conflicts and complications in investigations and prosecutions. For instance, a cryptocurrency fraudster operating from one country, targeting victims in another, and using an exchange in a third country to launder proceeds can create a complex scenario where determining jurisdiction becomes contentious. Developing international agreements and frameworks that clearly define jurisdictional boundaries and protocols for resolving conflicts can help mitigate these issues.

Moreover, the lack of uniformity in legal and regulatory approaches to cryptocurrencies across different jurisdictions presents significant challenges for international cooperation. Countries have different definitions of what constitutes a cryptocurrency crime, varying standards for evidence, and disparate regulations for cryptocurrency exchanges and financial institutions. Such inconsistencies can create legal loopholes that criminals exploit to evade justice. For example, operating an unregistered cryptocurrency exchange might be a criminal offense in one country while only resulting in a fine in another. Promoting international harmonization of cryptocurrency regulations and adopting global standards, such as those recommended by the FATF, can help create a more cohesive legal environment.

Lastly, the rapid evolution of cryptocurrency technology poses a significant challenge, as law enforcement agencies worldwide often struggle to keep up with the latest developments and techniques used by criminals. Technological disparities and varying levels of expertise among countries result in uneven enforcement capabilities. Some countries may lack the necessary tools, resources, or trained personnel to effectively investigate and prosecute cryptocurrency crimes. For instance, a country with limited technological infrastructure and expertise may be unable to trace sophisticated cryptocurrency transactions or recover digital evidence, impeding the overall investigation. Enhancing international collaboration on capacity-building initiatives, including training programs, technical assistance, and resource sharing, can help bridge these gaps. Establishing international centers of excellence for cryptocurrency forensics and cybersecurity can provide ongoing support and knowledge dissemination.

6. Recommendations

The recommendations provide a detailed framework of strategies and best practices aimed at addressing the misuse of crypto assets and related services. They focus on preventing the exploitation of digital currencies for criminal purposes, including the creation, concealment, and laundering of illegal funds. By establishing clear guidelines, these Recommendations guide organizations and authorities in implementing robust measures to detect, trace, and disrupt illicit financial activities within the cryptocurrency ecosystem.

Obtain the right tools:

The crypto space is rapidly advancing, together with the strategies used by criminal actors. As a consequence, investigators are encountering greater challenges in tracking illicit crypto assets. Moreover, the rise of decentralized finance (DeFi) platforms and smart contracts, presents more significant hurdles. Blockchain analytics tools are crucial for law enforcement because they enable the tracking, tracing, and analysis of cryptocurrency transactions, turning the transparency of blockchain technology into a powerful crime-fighting tool. These tools help link suspicious wallet addresses to real-world identities, detect money laundering techniques, and identify fraud patterns, even in decentralized finance (DeFi) environments. They also support ransomware investigations, provide admissible evidence in legal proceedings, and enhance collaboration between international agencies and financial institutions. By automating investigative processes and adapting to evolving obfuscation methods, blockchain analytics tools allow law enforcement to respond effectively to the dynamic nature of crypto-related crime.

Expand knowledge through training:

Training is vital for law enforcement in crypto crime investigations because it builds the knowledge and skills needed to handle the complexities of blockchain technology and evolving criminal tactics. It provides officers with a solid understanding of how cryptocurrencies work and how to use specialized blockchain analytics tools to trace illicit transactions and link them to real-world identities. As crypto-related crime evolves with new innovations like decentralized finance (DeFi), mixers, and privacy coins, training ensures that investigators stay up-to-date with the latest methods criminals use to

hide their tracks. Training also emphasizes legal compliance, teaching officers how to handle digital evidence properly so that it remains admissible in court, strengthening their ability to build strong legal cases. Additionally, well-trained officers can conduct investigations more efficiently, reducing errors and increasing the speed and accuracy of their work. Training promotes better collaboration between law enforcement agencies, both domestically and internationally, allowing for effective information sharing in the global fight against crypto crimes. Ultimately, ongoing training is crucial for enabling law enforcement to keep pace with the fast-changing crypto landscape, adapt to new challenges, and successfully prevent and prosecute digital financial crimes.

Increase cooperation:

Collaboration between national and international agencies is crucial for effective crypto crime investigations, as these often span multiple jurisdictions and require coordination across different areas of expertise. National agencies, such as financial intelligence units, play a key role by providing clear, actionable intelligence based on data from virtual asset service providers. Investigators and prosecutors may also rely on asset recovery agencies to ensure that electronic evidence, like access to cryptocurrency private keys, is properly gathered and admissible in court. On the international level, organizations like Europol facilitate cross-border cooperation by coordinating efforts between jurisdictions. The global and transparent nature of blockchain technology further supports this collaboration, allowing more advanced jurisdictions to detect and share information on potential crypto-related crimes and money laundering, promoting faster and more spontaneous exchanges of intelligence between countries.

7. Conclusions

In conclusion, navigating the complex landscape of cryptocurrency financial investigations requires law enforcement agencies to be equipped with robust tools, comprehensive knowledge, and a collaborative spirit. As digital currencies continue to evolve and integrate into the global economy, so too must the strategies and methodologies employed to combat illicit activities. By embracing advanced technologies, fostering international cooperation, and continuously enhancing regulatory frameworks, law enforcement can effectively safeguard the integrity of the financial system.

The challenges posed by cryptocurrency crimes are significant and multifaceted, encompassing jurisdictional conflicts, legal inconsistencies, technological gaps, and issues of trust and sovereignty. Addressing these challenges necessitates a concerted and coordinated effort at both national and international levels. Law enforcement agencies must prioritize ongoing education and training to stay abreast of the latest developments in cryptocurrency technology and criminal tactics. Leveraging tools such as blockchain analytics and engaging with specialized cybersecurity units will be critical in staying one step ahead of perpetrators.

Ultimately, the fight against cryptocurrency-related crimes requires a proactive and adaptive approach. Law enforcement agencies must remain vigilant and innovative, continually refining their strategies to address the evolving landscape of digital financial crime. By embracing a holistic and integrated approach, we can ensure that the promise of cryptocurrencies is not overshadowed by their misuse, maintaining a secure and just environment for all. Through dedication, collaboration, and innovation, law enforcement can effectively counteract the threats posed by cryptocurrency crimes, protecting the financial system and upholding the rule of law in the digital age.

Federico Paesano

Financial Investigations and Analysis for Emerging Money Laundering Risks:

Criminal Use of Cryptocurrency

Funded by the European Union

COPLAD