

## “MONEY LAUNDERING 3.0”

## HOW TO APPLY THE “FOLLOW THE MONEY” RULE IN THE CYBERSPACE

Avv. Emanuele Florindi



## INTRODUCTION: THE ROAD TO CYBER LAUNDERING

Most organized crime shares a financial motive as a common denominator: criminal activities aim to acquire profits, often referred to as “dirty money”, frequently in the form of cash. However, to utilize these funds, they must legitimize the profits through various channels.

Organized crime groups typically expand their assets and then attempt to integrate them into the legal economy through various money laundering schemes.

When we refer to “Money Laundering”, we are describing the process by which criminals “clean” the proceeds of their activities to conceal their illegal origin. Although it is challenging to measure money laundering on the same scale as legitimate economic activity, the magnitude of the problem is enormous.

The United Nations Office on Drugs and Crime (UNODC) estimates that between EUR 715 billion and 1.87 trillion is laundered each year (between 2 and 5% of global GDP).

Money laundering can take several forms, although most methodologies can be categorized into one of a few types and typically, it involves three steps: **placement**, **layering**, and **integration**.



First, the illegitimate funds are furtively introduced into the legitimate financial system. This is the placement phase and it is the most dangerous phase for the criminals. They need to physical place the money in the legal financial circuit to be allowed to use it so criminals need trusted men to transport the money and trusted banks directors who will not question the source of the money.

Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts. This is the **layering phase** (or the “cleaning” phase): money is cleaned through various services, such as friendly casinos or shell companies.

Finally, it is integrated into the financial system through additional transactions until the "dirty money" appears "clean". This is the **integration phase**: the clean money can now surface and be invested in legal activities. Tracing these assets means tracing the networks.

## FOLLOW THE MONEY

The Falcone Method was universally recognized as an innovative and revolutionary investigative technique based on 3 pillars:

- 1 Observing the phenomenon from above and then analysing it in detail like in a magnifying glass.
- 2 Identifying, tracking and dismantling the economic relations between the criminal organizations.
- 3 Making use of the collaboration of the "*pentiti*" as a key tool to understand the mafia dynamics.

This method became the *raison d'être* of the DIA (Direzione Investigativa Antimafia) in Italy: its functions were outlined by Falcone himself who advocated the creation of “*an agency in charge of judicial investigations and therefore a technical body*”, adding that the activities carried out by what he called “*the anti-crime police of the future*” would “*depend, to a greater extent, on the effectiveness of preventive investigations*”, which “*will allow greater flexibility in the intervention by law enforcement agencies, as urged on many sides*”.

## CYBER LAUNDERING VS LAUNDERING



**Cash is difficult to track, but it also has numerous disadvantages.**

- 1** It's heavy, cumbersome and difficult to hide and, if discovered, can be easily seized.
- 2** Must be physically placed in the banking circuit (placement) and requires direct contact to be delivered.



The March 2022, “International Narcotics Control Strategy Report” emphasizes that *“The rapid growth of virtual currencies supports the evolution of various crimes, including money laundering, posing new challenges for societies, governments, and law enforcement”*. Specifically exemplifying Italy, the report underlines the following: *“Law enforcement investigations have identified an increasing use of trade-based money laundering schemes and cryptocurrencies to disguise illicit proceeds and payments through legitimate trade transactions. Additionally, the arrest of over 100 Italian organized crime associates in September 2021 highlighted the increasing employment of cybercrime techniques to extort and steal income for the mafia”*. In a nutshell, organized crime is showing increasing interest in cryptocurrencies and alternative payment systems.

At present, common forms of money laundering include the banking system, cash couriers, bulk money smuggling, money service providers, alternative remittance systems, stores of value, trade-based money laundering, non-profit organizations, real estate, and front companies. However, even these methods are employed in more creative ways, such as utilizing unwitting frontmen who unwittingly act as money mules, responding to job offers. Additionally, commonly used tools like rechargeable cards, credit cards, contactless mobile phone payment systems, and money transfer systems outside the traditional banking system are exploited for money laundering purposes.



CYBER VICTIM



VICTIM'S ACCOUNT

TRANSFER



MULE'S ACCOUNT



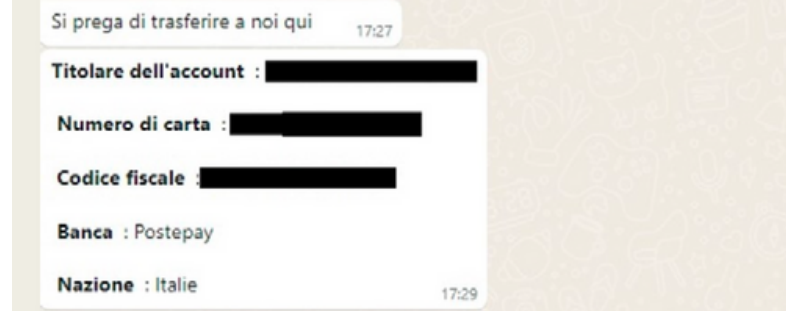
MONEY MULE



WIRE TRANSFER



CASH WITHDRAWAL



Esempio di money muling. Fonte: Europol.

PSA Into the Web of Profit: Tracking the Proceeds of Cybercrime


## Laundering Revenues

Guarda più Condividi

RSAC

### (ii) Traditional Means

- Shell companies; money mules; casino laundering; wire transfers
- In 2017, Western Union ordered to pay \$586m by DoJ
- Found to have enabled transfer of around \$632 million up to 2015 in relation to online lottery scams, romance frauds, 419 scams and so on.



ALTRI VIDEO

PSA Conference 2018

## THE CRIMINAL USE OF ALT COIN



*Cryptocurrencies should not be confused with other commonly available virtual currencies which are currently used in many criminal contexts, such as:*

- 1** Telephone recharge cards
- 2** Meal vouchers or points collection cards
- 3** Amazon vouchers or similar
- 4** Virtual currency linked to video games or virtual worlds such as, for example, Word of Warcraft e-gold or Second Life Linden Dollars



# SOME REAL CASES....



## Fake books sold on Amazon could be used for money laundering

Books of gibberish are listed on Amazon.com for thousands of dollars, with one author claiming his name was used to send almost \$24,000 to a fraudulent seller.



Tech > Phones & Gadgets

### CATCH ME IF YOU CAN Russian criminals are using Uber 'ghost rides' for money laundering

Fraudsters are using the app to create entire networks built on rides that never occur to extract real cash from stolen credit cards

## FBI Says ISIS use eBay to send terror cash

by vatfraud | Oct 4, 2019 | Latest News | 0 Comments

Products listed at astronomically high prices on eBay appear to be real transactions when sold but are in fact methods to launder and secretly send cash. This simple, popular ruse has been used by Islamic State to funnel cash to operatives in the Middle East.

U.S. investigators uncovered a global financial network run by a senior Islamic State official that funnelled money to an alleged ISIS operative in the U.S. through fake eBay transactions, according to a recently unsealed FBI affidavit.

## Inside Airbnb's Russian Money-Laundering Problem

PAYDAY

Russian crime forums have been using the home-sharing service to shuffle around cash under the table, sometimes with the help of legitimate Airbnb hosts.



Joseph Cox | Updated Nov. 27, 2017 5:37AM ET / Published Nov. 27, 2017 12:00AM ET



## Valve shuts down money laundering via CS:GO game

© 1 November 2019



Item Name	Count	Starting Price
Danger Zone Case Key	789	\$3.35 USD
Gamma Case Key	206	\$3.60 USD
Operation Phoenix Weapon Case	121,565	\$0.27 USD
Danger Zone Case	255,768	\$0.08 USD
Operation Wildfire Case Key	175	\$4.32 USD

Keys are widely traded on Steam's marketplace

Criminals have been laundering money via the popular Counter Strike: Global Offensive (CS:GO) video game, says creator Valve.



Имя: [Redacted]  
Регистрация: 25 Dec 2017  
Сообщений: 19  
Реакции: 12

13 Apr 2017

Вы автор данного материала? < #1

Доброго времени.

Если вы работаете в такой службе такси как Убер, и желаете заработать дополнительные деньги, вы попали по адресу.

Суть в следующем:

Вы пишете мне в телеграм, я вызываю вас и вы катаетесь по своим делам(естественно без пассажира), и вам капает деньги. Опытные водители работают со мной по такой схеме сразу в нескольких службах.

Вызвать без слета возможно по следующему сценарию:

Uber - поездка 2 часа, не важно, uberX или uberBlack

(цифры могут отличаться от действительности т.к. условия использования могут меняться убером)

Моя цена за любую поездку 700 рублей.

Постоянным клиентам скидка 20%

Т.к. я новичок на форуме, предлагаю хорошую скидку за отзыв.

Связь через telegram: @ [Redacted]

This article is more than 3 years old

## Counter-Strike trading found to be 'nearly all' money laundering

Valve says it has halted trading of some in-game items in multiplayer shooter

## SOME OPERATIONAL TIPS



**Pay attention to the presence of telephone rechargeable card; Amazon rechargeable card/vouchers.**



**Verify E-Bay transactions or other purchase sites, for example by verifying the sending and receipt of goods.**



**Check for inconsistencies in movements (bilocation or excessively rapid movements) via cell phones and GPS of vehicles or in the consumption of the rented apartments (no electricity / water / gas consumption)**



**Check for GPS spoofer in mobile phones.**



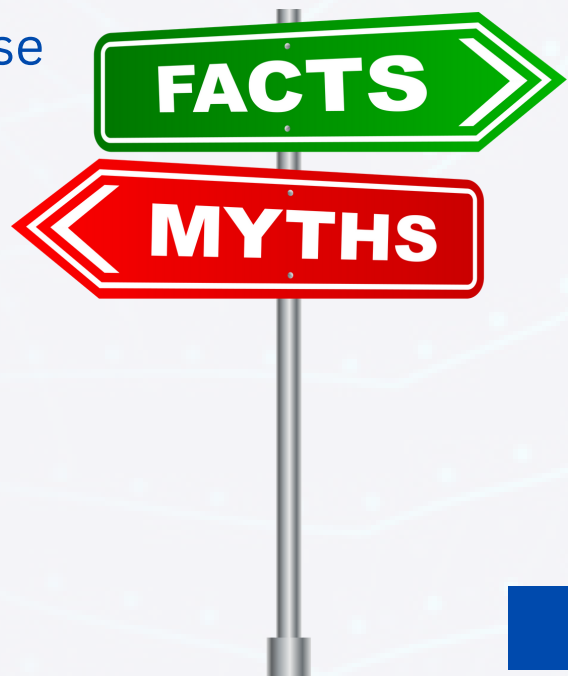
**Acquire Telegram and Signal accounts and verify contacts**



**A cryptocurrency, or crypto, is a digital currency designed to function as a medium of exchange through a computer network that does not rely on any central authority, such as a government or bank, to uphold or maintain it. There is a decentralized system for verifying that the parties involved in a transaction indeed possess the funds they claim to have.**

## Debunking some common myths about cryptos

- They are all anonymous
- They are only used on the dark web
- They are only used by criminals
- They are just a speculative bubble
- They have no practical use
- They are difficult to use



## WHAT DO WE MEAN WHEN WE TALK ABOUT CRYPTOCURRENCIES?

There are numerous types of cryptocurrencies, each exhibiting distinct characteristics, including variations in terms of anonymity.

**Blockchain:** A blockchain is a distributed ledger comprising growing lists of records (blocks) securely linked together through cryptographic hashes. Each block contains the cryptographic hash of the preceding block, a timestamp, and transaction data (typically represented as a Merkle tree, with data nodes depicted as leaves).

**Wallet:** A cryptocurrency wallet serves as a means to store the public and private "keys" (address) or seed, which can be utilized for receiving or spending the cryptocurrency (wallets do not contain crypto themselves). With the private key, it becomes possible to make entries in the public ledger, effectively spending the associated cryptocurrency. The public key allows others to send currency to the wallet. Various methods exist for storing keys or seeds in a wallet, ranging from paper wallets (where public, private, or seed keys are written on paper) to hardware wallets (specialized hardware for storing wallet information), digital wallets (computers with software hosting wallet information), to hosting your wallet through an exchange where cryptocurrency is traded, or by storing your wallet information on a digital medium such as plain text.

## PAPER WALLET

In a paper wallet, the private key is either written or printed onto the paper and then stored in a secure location for later retrieval. Physical wallets can also take the form of metal token coins with a private key accessible under a security hologram; the security hologram self-destructs when removed from the token, indicating that the private key has been accessed.

Creating and hiding a paper wallet is a straightforward process, It can be concealed in your wallet (though not recommended), in a book, in a safe, in a drawer... essentially, anywhere capable of holding a 5x10cm piece of paper.

**CAVEAT 1:** The private key is not saved anywhere, so if it is not identified during the search, there is no way to discover it.

**CAVEAT 2:** The adversaries may possess more than one copy of the paper wallet, so after a seizure, it is imperative to move the cryptocurrencies as soon as possible.



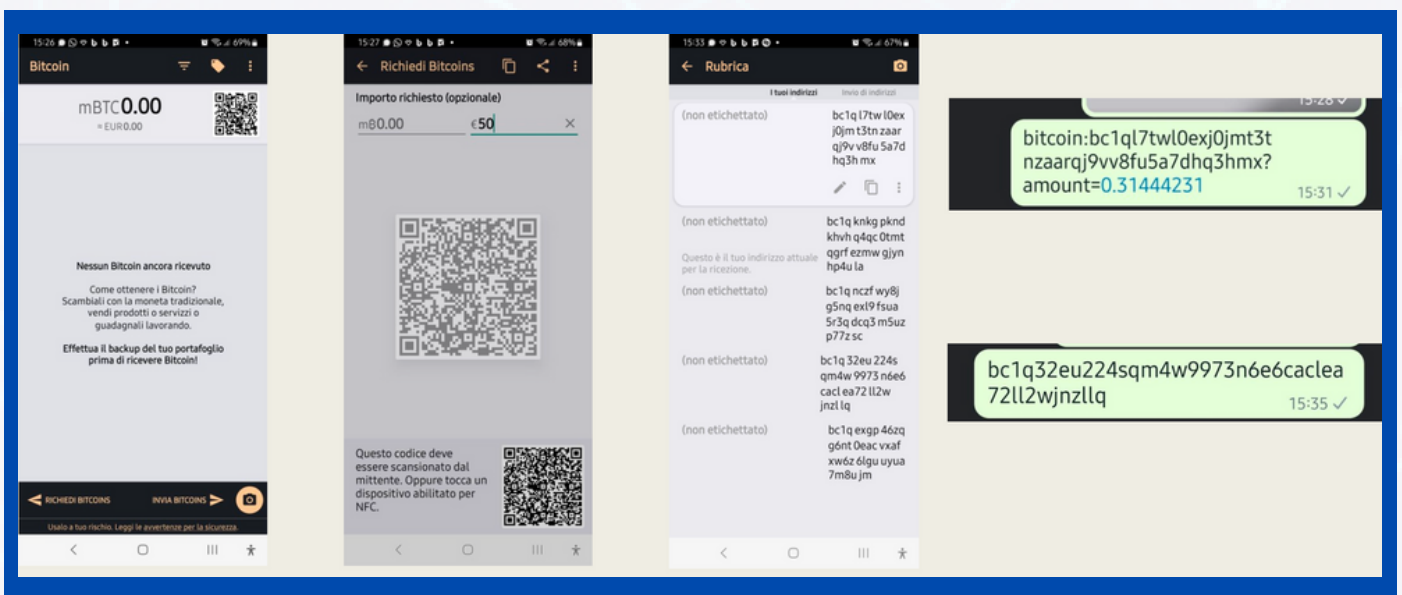
The image shows a paper wallet for Bitcoin, divided into two main sections: a yellow/orange left side and a green right side. The left side features a QR code labeled 'PUBLIC ADDRESS' and the text 'DEPOSIT / VERIFY' below it. The right side features a QR code labeled 'PRIVATE KEY' and the text 'WALLET IMPORT FORMAT' below it. The Bitcoin logo and the word 'bitcoin' are centered between the two sections. The public address is printed at the top and bottom of the left side, and the private key is printed at the top and bottom of the right side.

Your **public** key is: `15kid6yqKFXF4G1csj5ippLtaJoovF85cZ`  
Receive bitcoin to your wallet using your PUBLIC key.

Your **private** key is: `5J7uS4xLxfoaVDmXvzAiGToD4aY26MU8Az2hNwVtanxqTUKest4`  
Access bitcoin in your wallet using your PRIVATE key.

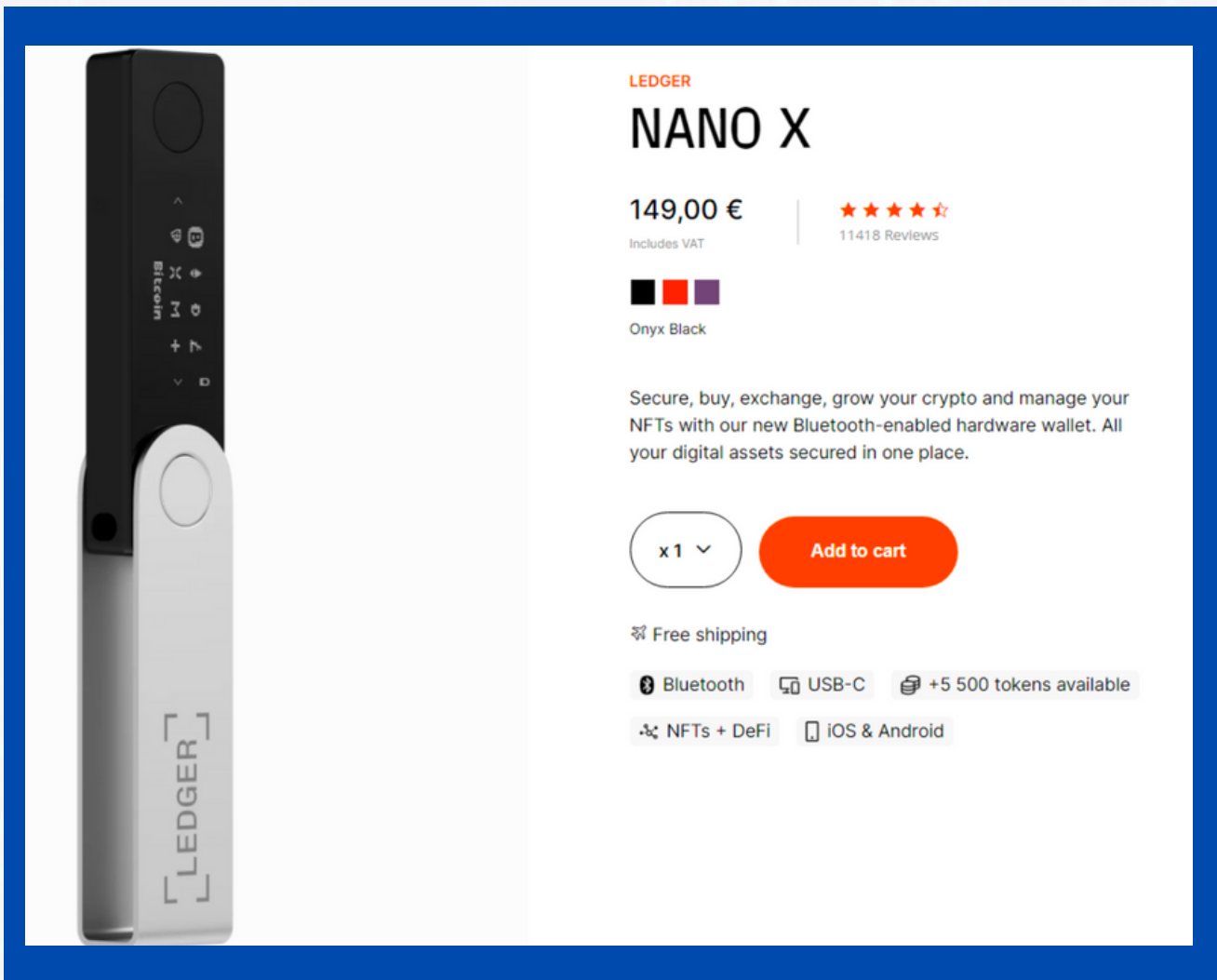
# SOFTWARE WALLET

The wallet software is an application that can be downloaded on a PC, tablet, or smartphone. Usually, when a new wallet is created using wallet software, the application either generates or requests a private key, which it keeps hidden to protect against any trojans. Simultaneously, it generates a 12-word phrase, commonly known as a seed phrase. Typically, this passphrase is written down and concealed to facilitate wallet recovery. A notable feature of many software wallets, in contrast to simple paper wallets, is that they generate a new public key for each payment. This design ensures that each payment received appears to be from different users each time, enhancing privacy protection. Additionally, it is possible to create customized QR codes for specific amounts.



# HARDWARE WALLET

A hardware wallet consists of a simple, non-overwritable USB stick containing a set of private keys for each supported cryptocurrency. The primary advantage of a hardware wallet is its potential usability even on a security-compromised computer. However, the main disadvantage is that being a physical object, it is susceptible to theft or seizure



The image shows a screenshot of the Ledger Nano X product page. On the left is a vertical image of the device, which is black and silver, with the Ledger logo at the bottom. The right side of the page contains the following information:

- LEDGER** (brand name)
- NANO X** (product name)
- 149,00 €** (price), including VAT
- ★★★★☆ (5-star rating) and 11418 Reviews
- Color selection: Onyx Black (selected)
- Description: "Secure, buy, exchange, grow your crypto and manage your NFTs with our new Bluetooth-enabled hardware wallet. All your digital assets secured in one place."
- Quantity selector: x1
- Add to cart** button
- Free shipping icon and text
- Feature tags: Bluetooth, USB-C, +5 500 tokens available, NFTs + DeFi, iOS & Android

## SOME OPERATIONAL TIPS



Be vigilant about the presence of QR codes in or around surveillance areas; a drug dealer could sell illicit substances without the need for physical meetings by following a simple series of steps:



*The customer makes payment through a QR code placed in various locations.*

*Communicate the payment via Telegram or Signal.*



*Receive the GPS position of the location where the goods are located.*



During search activities, be alert to "unusual" hardware devices or sheets with QR codes or strings of characters.



Always check for the presence of electronic devices (mobile phones, tablets, computers).



Obtain Telegram and Signal accounts and verify contacts.



## CRIME AND CRYPTOCURRENCIES: FATAL ATTRACTION?

Currently, the criminal use of cryptocurrencies remains relatively limited. However, as revealed in the Report to Parliament on information security policy for the year 2020 (AA.VV., 2021), criminal organizations have undergone transformation, adapting to new technologies, especially in the realm of agile and secure money transfer systems. In this context, it is essential to reference the action plan of the EU Commission on combating money laundering and the financing of terrorism (AML/CFT - Anti-Money Laundering and Countering Financing of Terrorism of 07/20/21). The European Parliament, in point number 4, emphasizes the urgent changes needed to establish an effective European framework. The Commission is urged to expand the single regulatory body on AML/CTF, broadening the scope of obligated entities. This expansion includes incorporating new and disruptive market sectors, technological innovation, and the evolution of international standards. The Commission is also tasked with ensuring that the regulation of services aligns with the regulation of goods. Addressing the risks associated with crypto-assets is emphasized, with a broad application of the "Know Your Customer" principle. It is not coincidental that the transparency of blockchain technology makes it relatively unattractive to criminals. The Bitcoin blockchain, in particular (not all blockchains are the same), is highly transparent. As exemplified, it can be utilized to reconstruct the network of contacts and the associated transfer of funds.

## WILL CRIMINALS USE CRYPTOS?

### YES BECAUSE

- 1** They allow for relatively fast and cheap payments to and from anywhere in the world.
- 2** Due to the lack of centralized control, cryptocurrencies cannot be shut down by any country.
- 3** They are safe from "capital controls".
- 4** They are safe from "currency controls" that restrict the free use or exchange of currencies.
- 5** They guarantee a high level of confidentiality.
- 6** They are easy to store and hide.
- 7** There are excellent and cheap "washing" systems.

## CRYPTOS: FRIENDLY OR FOE?

The cryptosphere is not solely associated with crime; on the contrary, it primarily comprises honest participants envisioning a global economic future in cryptocurrencies. An interesting perspective on this matter emerged during the conference led and organized by Europol on digital assets and organized crime. The event recognized that the features of blockchain could be leveraged by the police for investigative purposes.

In essence, cryptocurrencies could prove highly valuable in combating organized crime to the extent that they are described as 'fundamental for fighting organized crime.'

## SEIZING CRYPTOS: DIFFICULTIES TO OVERCOME

First, it is crucial to distinguish between "content" and "container." This involves the seizure of cryptocurrencies and the confiscation of wallets, each varying based on whether it is a paper wallet, software wallet, or physical wallet. Following this, it becomes imperative to comprehend how to "follow the flows." Companies such as Chainalysis, TRM Labs, and Elliptic have developed software designed to track and analyze the cryptocurrency ecosystem. Upon identifying illicit funds, the next step is to determine the feasibility of proceeding with the seizure. This multifaceted process involves not only understanding the nature of the digital assets but also employing advanced tools and technologies developed by specialized companies in the field.

## SEIZURE: SOLUTION AND DOUBTS

Physical wallets, encompassing paper and hardware, pose theoretical challenges such as conservative, preventive, or probative seizures. In probative seizures, the focus is on the wallet and digital traces to establish its existence and transactions. Preventive seizures aim to hinder asset availability, requiring identification of virtual currency and rendering it unavailable to the owner. The seizure of virtual currency involves transferring it to a specially ordered wallet controlled by judicial authorities. Operational solutions include moving assets to a judicially controlled wallet or converting them into fiat currency, though the latter faces challenges due to virtual currency volatility. Entrusting the wallet to an exchanger is discouraged. Importantly, seizures directly impact cryptocurrency codes (private keys), demanding clear operational instructions.



BIGOSINT Countering THB through  
BIG DATA & OSINT Analysis  
This project is co-funded by the  
European Commission, Directorate-  
General for Migration and Home  
Affairs under Grant number:  
101038761