MONEY-LAUNDERING AND CRYPTO-ASSETS

Colonel t.SPEF Giuseppe Lopez

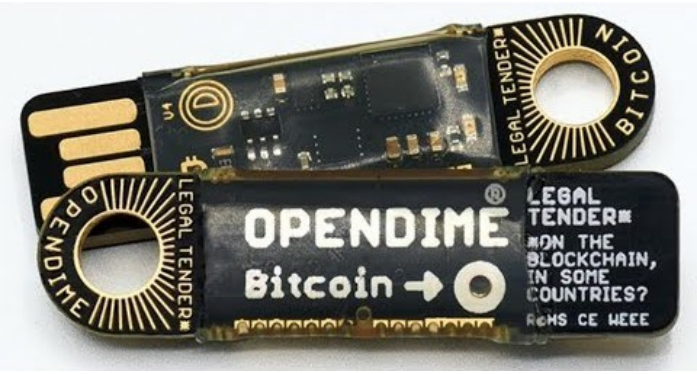
GUARDIA DI FINANZA

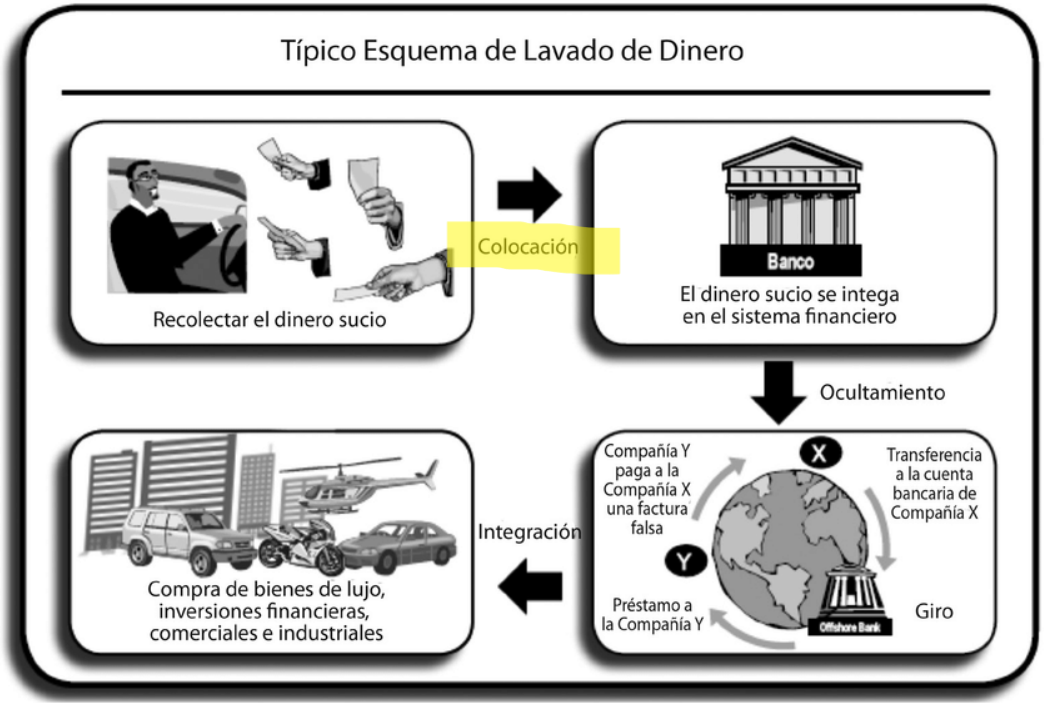
RESEARCH TECHNIQUES

By analyzing the different stages of a money laundering operation, we can understand how virtual currencies today represent an extraordinary opportunity for those seeking to reinvest illicit capital, offering a series of alternatives to traditional methods.

The ways in which the three typical phases of a money laundering operation can be implemented are as follows:

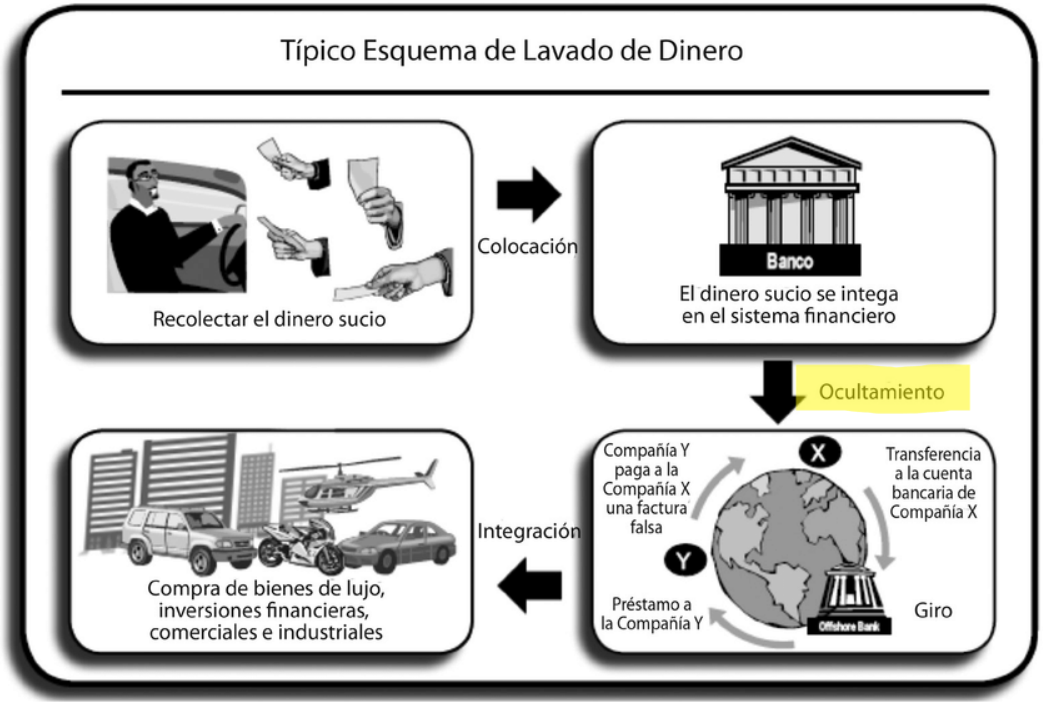
1. **placement** phase, a criminal in possession of cash proceeds from crime can easily **purchase the keys or credentials** of a *wallet directly* to exchange the banknotes for cryptocurrency (e.g., with an **Opendime**). In this case, the buyer of the virtual currency is not asked for any identity information during the transaction.





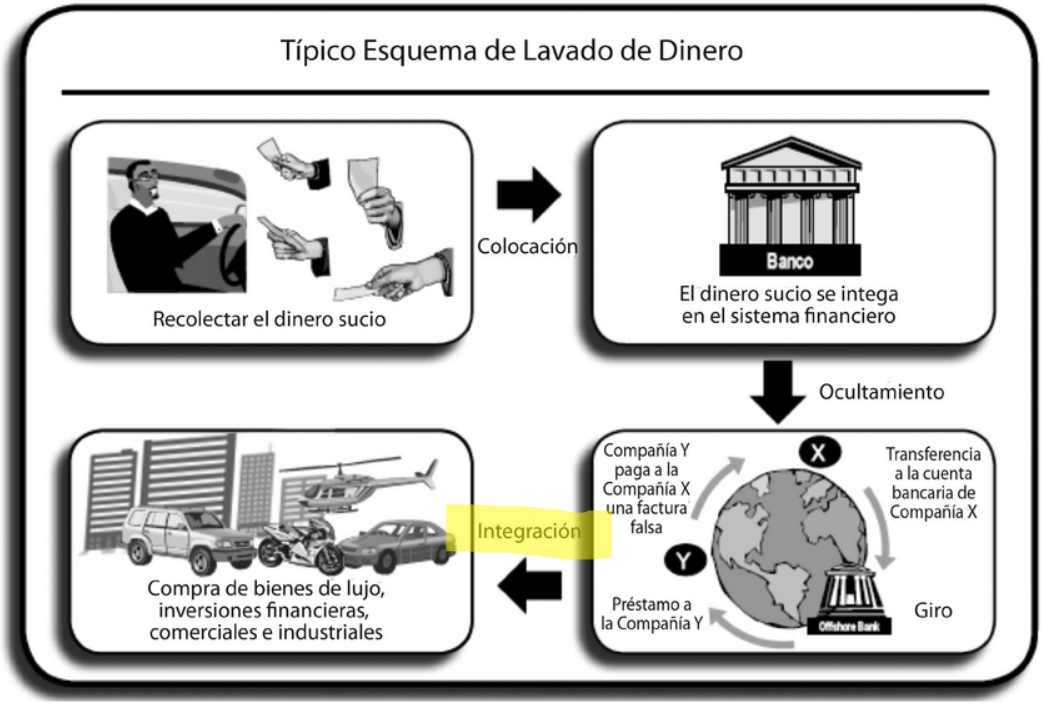
RESEARCH TECHNIQUES

2. In the next phase, **concealment**, in which the illicitly accumulated sums must be divided, it is possible to create **different cryptocurrency *wallets***, dividing the original amount into many smaller parts and thus obscuring the traceability of the transactions. Movements from one *wallet* to another, combined with maintaining anonymity, can erase evidence of the illicit origin of the money. In fact, for every exchange of virtual currency between users, there is a step between different *wallet addresses.* To carry out these operations, criminal organizations often use so-called ***money mules***, individuals recruited to act as intermediaries in the money laundering phases. All they have to do is transfer the received sums of money to third parties, receiving a percentage of the transferred amount. Often, the people carrying out these operations are not even aware that the transferred money represents the proceeds of an illicit crime, but they nevertheless play a crucial role in the money laundering process.



RESEARCH TECHNIQUES

3. In the final phase, i.e. the **integration phase**, the money launderer could retain the illicit proceeds in the form of cash to invest in future transactions, also by creating websites or *online front companies* .
   In fact, one of the most frequent cases is the creation of companies **e-commerce** capable of offering services or marketing goods fraudulently or not.
   In addition, you can create an ***online* gaming site**, By purchasing cryptocurrency, using fake identities or nominees to transfer funds. This way, after investing the virtual currency, the gambling site's earnings appear completely legitimate.
   Another widespread practice at this stage is to collect cash from services where cash had originally been exchanged for virtual currencies, by performing multiple split **transactions (CryptoATM)**.



RESEARCH TECHNIQUES

There are certain methods designed to circumvent, or at least hinder, the investigation techniques provided by so-called ***mixing*** services (*mixer/tumbler*).
This definition refers to services offered by third parties that "mix" the cryptocurrencies sent to further anonymize them and possibly make them "clean". The mixing operation It is relatively simple and is based on the movement (***switching***) of "money" from one "address" to another not connected to the first, except through algorithms that are internal to the service itself.

Specifically, the user sends the amount they wish to "clean" to the *tumbler*, which, once received, will pay it to the destination address indicated by the user, but for this payment, it will use "codes" that refer to other "customers."
This way it will be very difficult, if not impossible (unless the internal details and history of the *mixer are known*), to reconnect the two addresses indicated by a simple analysis of the blockchain, since technically the transaction sent by the user will reach the recipient through one or more different users.
In addition, more sophisticated *mixers* offer other "solutions" intended to increase the anonymity of transactions, such as: **time delays** and **transaction decomposition**.
Obviously, the service has a cost, albeit a limited one: a small fee is applied to the transaction, which is also anonymized in various ways within the process.

RESEARCH TECHNIQUES

It is plausible to believe that, with respect to research objectives, the Bitcoin system and its derivatives can offer a double advantage, considering that:

a. The underlying **transaction record** (*cryptoledger*) is **public and immutable**, therefore "suitable" for conducting investigative activities;
b. In-depth analysis and intelligence activities can be carried out on transactions published in the register using the "***follow the money***" technique.

The purposes of research in the Bitcoin field can be different:

1. **the identification of suspects;**
2. **bitcoin movements and traceability to specific subjects;**
3. **the seizure of crypto assets.**

The cryptocurrency address can be known and is usually provided to the victim to deposit funds into in case of extortion or fraud.

The information can be "exploited" by operators to continue research activities, using specific tools such as:

a. *Blockchain explorer*, useful for selectively consulting the *blockchain;*
b. *walletexplorer.com, to carry out " follow the money"* activities;
c. cryptoasset tracking systems.

RESEARCH TECHNIQUES

Bitcoin (like other cryptoassets) is not completely anonymous but rather **pseudonymous**. This means that despite having no connection between the real identity of the perpetrator and the address/public key that received the payment, it is possible to examine the *blockchain* where all transactions are indelibly stored and identify and track the movement of Bitcoin in this network of connections.

Forensic operations can track bitcoin payments.
In some respects, it is possible to trace the financial transaction more easily than banking transactions (which require a **court order**) and even more complex if the banking transaction is carried out by **banks located in so-called "rogue" and/or uncooperative states**.

Therefore, the task involves identifying and examining the transactions involved in the crime. Try to aggregate addresses and understand which addresses belong to the same person and which ones, on the other hand, might represent *exchanges* where the user has an identity and where it's possible to investigate and request information.

RESEARCH TECHNIQUES

For example, computer research systems have been developed on three processes:

a. labeling;

b. clustering;

c. mixnet recognition.

Labeling activity uses *web crawling* and *scraping* engines: The *crawling* process analyzes entire websites and indexes all their content. A *crawler*, also known as a *spider*, is specialized *software.* It takes all the content of a web page and follows its various links to analyze linked websites or subpages. Once all the pages have been collected, they are analyzed using the *scraping process*. *Web scraping*, also known as *web data extraction*, is a technique, usually automated, that involves taking individual pieces of data from a set of web pages and compiling them into databases or files for further analysis.

We search within web pages by matching the text of the page with a regular expression, for strings that can represent bitcoin addresses. The address found is associated with the web page where it appears and any email addresses, nicknames, or pseudonyms, in order to trace the identity of the bitcoin address's owners.

Unfortunately, the number of addresses that can be tagged in this way is much smaller than the total number of existing addresses. This requires *clustering*.

RESEARCH TECHNIQUES

Clustering activity It uses heuristics to extend the label to all addresses considered to have the same owner. In fact, the Bitcoin protocol suggests, though not requires, the use of a new address each time a user makes a transaction.
This means that a diligent user has dozens, hundreds, or even thousands of addresses, collected in one or more *wallets*. To group all cryptocurrency addresses under the same owner, several heuristics are used. The most widespread is the multiple-input heuristic, which assumes that in a transaction with n addresses, all n input addresses belong to the same user. With this heuristic, it is possible to group approximately 70% of the addresses.

Mixnet recognition activity, it should be noted that it is the most complex activity and still requires considerable research efforts for its profitable use. In this context, the most common *mixing services were analyzed.* acquaintances to understand how it works and create a "sample" scheme that will be used to recognize other *mixing activities* among all transactions present in the blockchain.

RESEARCH TECHNIQUES

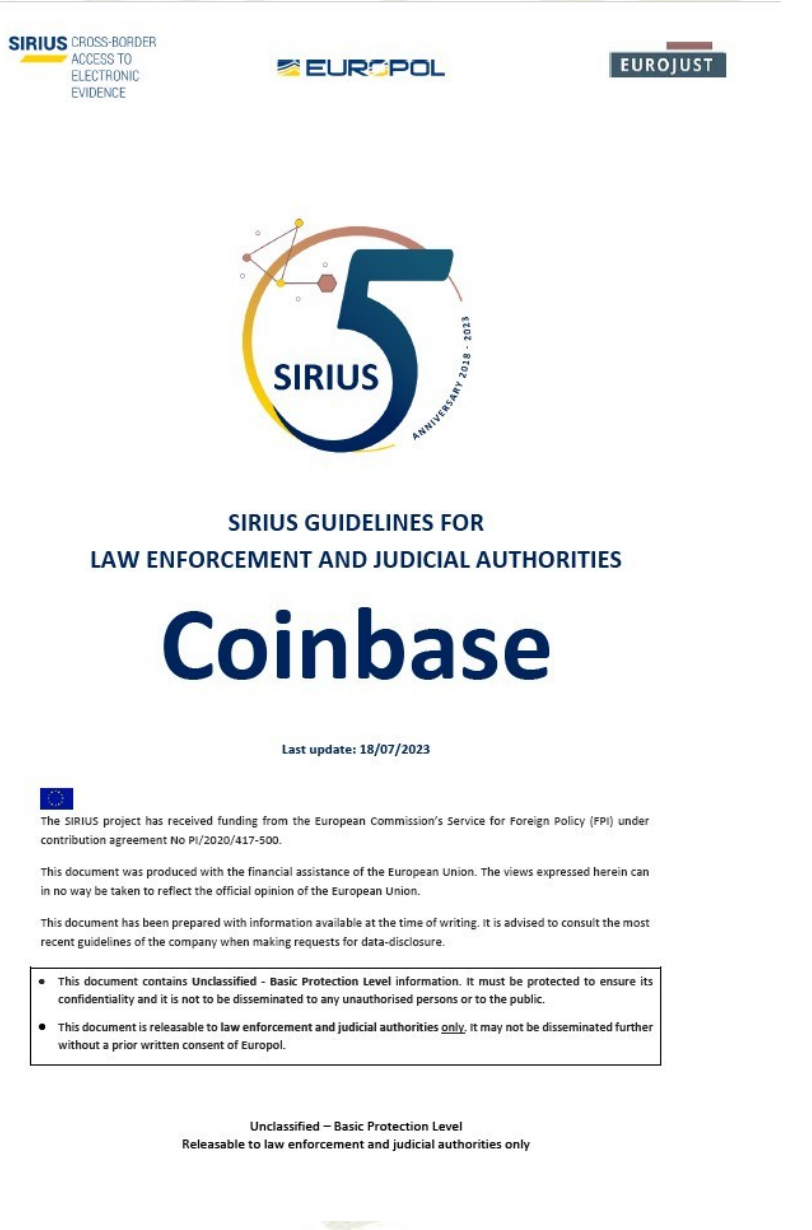
https://bitcointalk.org/
https://www.chainabuse.com/
https://www.bitcoinwhoswho.com/
https://www.walletexplorer.com/
https://blockchair.com/it/
https://oxt.me/
https://blockchain3d.info/
https://graphsense.info/

EUROPOL

EPE - EUROPOL PLATFORM FOR EXPERTS

https://epe.europol.europa.eu/group/sirius/home

SIRIUS CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE


SIRIUS CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE

EUROPOL

EUROJUST

SIRIUS GUIDELINES FOR
LAW ENFORCEMENT AND JUDICIAL AUTHORITIES

Coinbase

Last update: 18/07/2023

The SIRIUS project has received funding from the European Commission's Service for Foreign Policy (FPI) under contribution agreement No PI/2020/417-500.

This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

This document has been prepared with information available at the time of writing. It is advised to consult the most recent guidelines of the company when making requests for data-disclosure.

- This document contains **Unclassified - Basic Protection Level** information. It must be protected to ensure its confidentiality and it is not to be disseminated to any unauthorised persons or to the public.
- This document is releasable to **law enforcement and judicial authorities** only. It may not be disseminated further without a prior written consent of Europol.

Unclassified – Basic Protection Level
Releasable to law enforcement and judicial authorities only

RESEARCH TECHNIQUES

First of all, during the search phase, it is of fundamental importance to search for **private keys** (an alphanumeric string or a QR code in a *paper wallet*), as well as ***login* data in the *exchange* platform** or **physical *wallet*** that can take different forms. We could also find the **Seed Phrase**, a series of words randomly drawn from a vocabulary of 2,048 English words, which allows for recovering access to and use of cryptocurrencies.

RESEARCH TECHNIQUES

We will also investigate **software or *applications used for cryptocurrency and*** **credit card** management that directly allow cryptocurrency spending with contextual conversion to FIAT currency.

coinbase

bitpanda

BINANCE

kraken

SpectroCoin
PART OF BANCERA

RESEARCH TECHNIQUES

To proceed with the physical seizure, it is necessary **to generate a new address and a new private key** to transfer the availability of the suspect's cryptocurrency to the Judicial Authority, to prevent others from accessing it thanks to a copy of the keys.

The public key and the private key of the address generated from zero and containing the transferred assets will be kept in a sealed and sealed envelope at the disposal of the Judicial Authority.

However, the question of **how to deal with seized virtual currencies seems more controversial**. On the one hand, if a conversion to legal tender is carried out, it will be necessary to take into account the *mining action* that will separate a ***transaction fee***, so the value of the initial currency, which has already changed at the time of the seizure, will suffer a further decrease; on the other hand, if a possible conversion to legal tender is not considered, there will be a risk that the currency's value will change over time due to its **volatility**. In any case, by deciding to convert virtual currencies, you expose yourself to the risks arising from price instability based on market valuation.
Under Italian law, conversion requires an **explicit ruling from a judge**, who, if he believes the **volatility** of the seized cryptocurrencies is so high as to jeopardize their value, can order their sale.
Ultimately, in the event of cryptocurrency seizure, the Judicial Police must provide the Judicial Authority with all the necessary information to take action to convert the virtual currencies into cash.

RESEARCH TECHNIQUES

Another possibility of monetizing seized cryptocurrencies is to hold **a judicial auction**.

In this way, it is possible to obtain legal tender in exchange for cryptocurrencies, without resorting to third-party intermediaries (*exchangers*).

The U.S. Marshall Service, for example, auctioned off more than 4,000 bitcoins from various operations carried out by various agencies, including the DEA, and the same solution was also adopted by European law enforcement agencies.

RESEARCH TECHNIQUES

SEIZURE CAN ONLY BE CARRIED OUT IF INVESTIGATORS TAKE POSSESSION OF THE PRIVATE KEY

SEIZURE MUST BE MADE BY CREATING A SPECIFIC FINANCIAL TRANSACTION

THE TRANSACTION MUST BE PERFORMED QUICKLY TO PREVENT SUGGESTED OR THIRD PARTIES, BY BECOMING AWARE OF THE POSSESSION OF THE PRIVATE KEY BY THE JUDICIAL POLICE, FROM OBSTACLING THE SEIZURE

BEFORE THE TRANSACTION , A SPECIFIC WORK ENVIRONMENT MUST BE PREPARED AND A PRE-IDENTIFIED *WALLET TYPE MUST BE USED* FOR THE GENERATION OF A NEW PRIVATE KEY (TO BE MANAGED BY THE JUDICIAL POLICE)

THE SEIZURE OPERATION, HOWEVER, RESULTS IN A DECREASE IN THE VALUE OF THE INITIAL CURRENCY, DUE TO THE INTERMEDIATION OF VARIOUS PARTIES (*MINERS, EXCHANGERS, WALLET PROVIDERS, ETC.*)

THE NEW PRIVATE KEY (OF THE JUDICIAL POLICE) MUST BE KEPT IN A SEALED ENVELOPE - BLACK AND SEALED - AND CONCENTRATED IN THE CUSTODY ROOM OF THE COMPETENT PROSECUTOR OR , ALTERNATIVELY, IN THE EVIDENCE DEPOT OF THE APPLICABLE POLICE AGENCY

AT THE END OF OPERATIONS, THE WORK ENVIRONMENT MUST BE MADE SECURE TO AVOID LEAVING TRACES OF THE PRIVATE KEY IN THE POSSESSION OF THE JUDICIAL POLICE

TO CONVERT THE SEIZED VIRTUAL CURRENCY INTO LEGAL TENDER (EVEN IN THE EVENT OF SUBSEQUENT CONFISCATION), A SECOND FINANCIAL TRANSACTION MUST BE CARRIED OUT, RESULTING IN A FURTHER DECREASE IN THE INITIAL VALUE OF THE SEIZED CURRENCY. THE CONVERTED CURRENCY WILL THEN BE PAID INTO THE SINGLE JUSTICE FUND.

IF IT IS NOT POSSIBLE TO PROCEED WITH THE TRANSFORMATION OF THE SEIZED VIRTUAL CURRENCY INTO LEGAL TENDER, IT SHOULD BE CONSIDERED THAT THE FIRST IS VOLATILIZED AND, OVER TIME, SUBJECT TO UNPREDICTABLE OSCILLATIONS - POSITIVE OR NEGATIVE

Thanks for your attention

Col. t.SPEF Giuseppe Lopez