



## **”Follow the money”**

The use of BITCOIN-virtual currency and how it fuels the Human Trafficking Market – a particular challenge for law enforcement in solving THB cases





# Agenda **for today**

**01**

Let`s see the Romanian law!

**02**

The illicit income

**03**

Follow the illegal gain

**04**

Financial investigation of trafficking in human beings and the use of internet to trace financial flows

**05**

AMLD 5 solutions





# Incrimination of trafficking in human beings in Romanian law





# Romanian Law

## Romania has ratified

- United Nations convention against transnational organized crime and the protocols thereto
- Directive 2011/36/EU OF THE European Parliament and of the council on preventing and combating THB and protecting its victims

## Trafficking in, and exploitation of vulnerable persons

### Slavery art. 209 Penal Code

Pressing of keeping an individual in a state of slavery, as well as the trafficking in slaves shall be punishable by no less than 3 and no more than 10 years of imprisonment and a ban on the exercise of certain rights.

### Trafficking in human beings art. 210 Penal Code

(1) Recruitment, transportation, transfer, harboring or receipt of persons for exploitation purposes:

- a) by means of coercion, abduction, deception, or abuse of authority;
  - b) by taking advantage of the inability of a person to defend themselves or to express their will or of their blatant state of vulnerability;
  - c) by offering, giving and receiving payments or other benefits in exchange for the consent of an individual having authority over such person,
- shall be punishable by no less than 3 and no more than 10 years of imprisonment and a ban on the exercise of certain rights.

(2) Trafficking in human beings committed by a public servant in the exercise of their professional duties and prerogatives shall be punishable by no less than 5 and no more than 12 years of imprisonment.

(3) The consent expressed by an individual who is a victim of trafficking does not represent an acceptable defense.





# Romanian Law

## Trafficking in underage persons art. 211 Penal Code

(1) Recruitment, transportation, transfer, harboring or receipt of a juvenile for the purpose of their exploitation shall be punishable by no less than 3 and no more than 10 years of imprisonment and a ban on the exercise of certain rights.

(2) If such act was committed under the terms of Art. 210 par. (1) or by a public servant while in the exercise of their professional duties and prerogatives, it shall be punishable by no less than 5 and no more than 12 years of imprisonment and a ban on the exercise of certain rights.

(3) The consent expressed by an individual who is a victim of trafficking does not represent a acceptable defense.

## Pressing into forced or compulsory labor art. 212 Penal Code

An act of compelling a person, in cases other than the ones established by the legal stipulations, to work against their will or to compulsory labor shall be punishable by no less than 1 and no more than 3 years of imprisonment.

## Pandering art. 213 Penal Code

(1) The causing or facilitation of the practice of prostitution or the obtaining of financial benefits from the practice of prostitution by one or more individuals shall be punishable by no less than 2 and no more than 7 years of imprisonment and a ban on the exercise of certain rights.

(2) In the event that a person was determined to engage in or continue the practice of prostitution through coercion, the penalty shall be no less than 3 and no more than 10 years of imprisonment and a ban on the exercise of certain rights.

(3) If such acts are committed against an underage person, the special limits of the penalty shall be increased by one-half.

(4) Practicing prostitution means having sexual intercourse with various individuals for the purpose obtaining financial benefits for oneself or for others.





# Romanian Law

## Exploitation of beggary art. 214 Penal Code

(1) An act of an individual who causes a juvenile or a person having physical or psychic disabilities to resort repeatedly to the public's pity in order to ask for material help or benefits from financial benefits from such activity shall be punishable by no less than 6 months and no more than 3 years of imprisonment or by a fine.

(2) If such act is committed in the following situations:

- a) by a parent, guardian, curator or by the person under whose care the begging person is;
- b) by means of coercion,

it shall be punishable by no less than 1 and no more than 5 years of imprisonment.

## Use of underage persons for mendicancy art. 215 Penal Code

The action of a person who is of age and has the capacity to work, who resorts repeatedly to the public's pity in order to ask for material help, by using the presence of a juvenile for this purpose, shall be punishable by no less than 3 months and no more than 2 years of imprisonment or by a fine.

## Use of an exploited person's services art. 216 Penal Code

The action of using the services listed under Art. 182, provided by a person about whom the beneficiary knows that they are a victim of trafficking in human beings or of trafficking of underage persons, shall be punishable by no less than 6 months and no more than 3 years of imprisonment or by a fine, unless such action is a more serious offense.

## Punishing the attempt art. 217 Penal Code

The attempt to commit the offenses set forth by Art. 209-211 and Art. 213 par. (2) shall be punishable.





# Romanian Law

## Child pornography art. 374 Penal Code

- (1) The production, possession for display or distribution, the purchase, storage, display, promotion, distribution and supplying, in any manner, of child pornography shall be punishable by no less than 1 and no more than 5 years of imprisonment.
- (2) If the acts set out in par. (1) are committed using a computer system or other means of data storage, it shall be punishable by no less than 2 and no more than 7 years of imprisonment.
- (3) The act of unlawfully accessing child pornography through computer systems or other means of electronic communication shall be punishable by no less than 3 months and no more than 3 years of imprisonment or by a fine.
- (4) Child pornography means any material that shows a juvenile displaying a sexually explicit behavior or that, even if not presenting a real person, simulate a juvenile with such behavior in a credible manner.
- (5) The attempt shall be also punishable.

## Trafficking in migrants art. 263 Penal Code

- (1) Recruitment, instructing, guiding, transporting, transferring or harboring individuals for the purposes of fraudulently crossing Romania's state border shall be punishable by no less than 2 and no more than 7 years of imprisonment.
- (2) When the act was committed:
  - a) in order to obtain material gain, directly or indirectly;
  - b) using means that endanger the life, integrity or health of the migrant;
  - c) by subjecting migrants to inhuman or degrading treatment,it shall be punishable by no less than 3 and no more than 10 years of imprisonment and a ban on the exercise of certain rights.
- (3) The attempt shall be also punishable.





# Romanian Law

## Creation of an organized crime group art. 367 Penal Code

(1) The act of initiating or creating an organized crime group or of joining or supporting such a group in any way shall be punishable by no less than 1 and no more than 5 years of imprisonment and a ban on the exercise of certain rights.

(2) When the offenses included in the purpose of an organized crime group are punished by life imprisonment or by a term of imprisonment exceeding 10 years, it shall be punishable by no less than 3 and no more than 10 years of imprisonment and a ban on the exercise of certain rights.

(3) If the acts set out in par. (1) and par. (2) were followed by the commission of an offense, the rules on multiple offenses shall apply.

(4) No penalty shall apply to the individuals who committed the acts set out in par. (1) and par. (2) if they report the organized crime group to the authorities before it was discovered and before the commission of any of the offenses included in the purpose of the group.

(5) If the perpetrator of one of the acts referred to in par. (1) - (3) facilitates, during the criminal investigation, discovery of the truth and the prosecution of one or more members of the organized crime group, the special limits of the penalty are reduced by one-half.

(6) An "organized crime group" means a structured group, made up of three or more persons, which exists for a certain period of time and acts in a coordinated manner for the purpose of perpetrating one or more offenses.







**The illicit income:  
FIAT currency vs.  
cryptocurrency**

# Main purpose of the THB offenders

## Obtaining large benefits in a short time

- Usually, the offender will try to hide the illicit income by committing other crimes, like money laundering for disassembling the transactions.
- Traditional FIAT currencies and the scriptural ones have become more easy to trace by the investigators, usually leaving clues, as they are regulated and manipulated through institutions that are subject to governmental regulation. We should not take into consideration for this discussion the organised crime groups that have "cash carriers" or the ones that trade using "HAWALA" methods.
- "HAWALA" is an informal transfer system usually used by migrant smugglers.
- So, as the traffickers search for anonymity, they usually trade with new currencies, using cryptocurrencies.





**Follow the illegal  
gain**

# Let`s discover the Bitcoin



"The one thing that is missing, but will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B, without A knowing B or B knowing A"

*1999, Milton Friedman, awarded in Nobel Memorial Prize in Economic Sciences*



Bitcoin was not the first virtual currency. Centralised digital currencies have been coming and going since the 1990s. Yet, its popularity over the last few years has been so great that many people have started using the terms 'virtual currency' and 'bitcoin' interchangeably.

In 2009, bitcoin emerged as the first decentralised digital currency. This meant that for the first time in history, one person could send a secure payment directly to another without using a third party as an intermediary. To date, bitcoin remains the most important cryptocurrency that boasts over €10 billion in market value. Its increasing adoption allows for a practical legitimate use including investment, trade, person-to-person transactions or payment for goods or services online.

Bitcoin is based on a combination of several technologies, one of which is a public key cryptography dictating that two different keys are required to send and receive transactions. A public key can be distributed to anyone in order to receive a payment while the private key that should only be known to its owner is used to create a signature for a transaction that cannot be forged.

Public key cryptography solves two fundamental problems all digital currencies face:

- It allows users to uniquely identify their addresses in the system.
- It prevents users to spend coins they do not own.

## Key addresses vs. wallets

Both the private and public keys are stored in a bitcoin wallet. One person can possess any number of bitcoin wallets and each wallet can store any number of private keys. These private keys are used to generate public keys. A public key, when hashed, turns into a bitcoin address.

A private key acts as a lock for the bitcoin addresses. The owner of a private key has access to the funds stored on the corresponding bitcoin address. Private keys and bitcoin addresses are commonly stored in a wallet within a **wallet.dat file**. Both file and private keys are perfectly portable. The file can be copied from one drive or USB key to another and the private key can be exported to another bitcoin wallet. All of the above fundamentals apply not only to bitcoin but to other cryptocurrencies as well.

The vast majority of bitcoin addresses are between 30 and 35 characters long and start with a number 1. However, those who have already spent some time looking at the blockchain may also have noticed bitcoin addresses starting with number 3. These addresses are called pay-to-script (P2SH) hash addresses.

For an investigator, it is enough to know that by far the most popular example of a pay-to-script hash address is a multi-signature transaction, where multiple keys have to sign a transaction to release funds — for example, **3KgtbGgaX2ngstNpvyv7LwpHSweVeqGbpM**



# Strings to watch for at the crime scene/ in the suspect's computer



There are three most common representations of the private key:

1. Hex:

1E79423A4ED27608A15A2616A2B0E5E52CED330AC530EDCC32C8F  
FC6A520AED1

2. Private key is longer than the bitcoin address and starts with number 5:

5J3hzQ41KoJX64H5YRTqS9YB9LVGacU2qusL37Ys1eVpJTgnr4u

3. Compressed private key may look similar but starts with either K or L:

KyoPrwwmvSZymMrJLRhePV6jTFFpGU6uMVLv5nQhkMM4dpDKaMgG

In addition, there are three most common representations of the public key or a bitcoin address.

A public key is rarely found. What is usually discovered is a bitcoin address:

1. Public key:

04e2ff72520d37  
d88c61d0bac1c  
aa6fccec4ffefd3  
72d22247686aff  
a1ebdeea52d0  
dd2135

2. Normal bitcoin address:

13mE8VYvGym8Rj  
9ddHoagcNxmDs1  
SAxbNJ

3. Pay-to-script hash bitcoin address:

3KgtbGgaX2ngst  
Npvyv7LwpHSwe  
VeqGbpM

*During the house search, any notes, printed documents or electronic evidence containing strings resembling those above should be collected.*



# Inspecting a suspect's wallet



01

The IP addresses of the nodes the client is connecting to can be found in the standard Bitcoin Core client (Help -> Debug Window -> Peers on both PC and Mac wallet)

02

When inspecting the suspect's wallet, the remote node with the earliest connection time may give the investigator an idea of how long the suspect's wallet was open.

If there is a sign of a recent outgoing transaction, the RAM should be preserved as a priority. It is likely that the password is still stored in the RAM. Since there is no currently way of circumventing the password protection, extraction of the password from RAM significantly increases probability of bitcoin seizure.

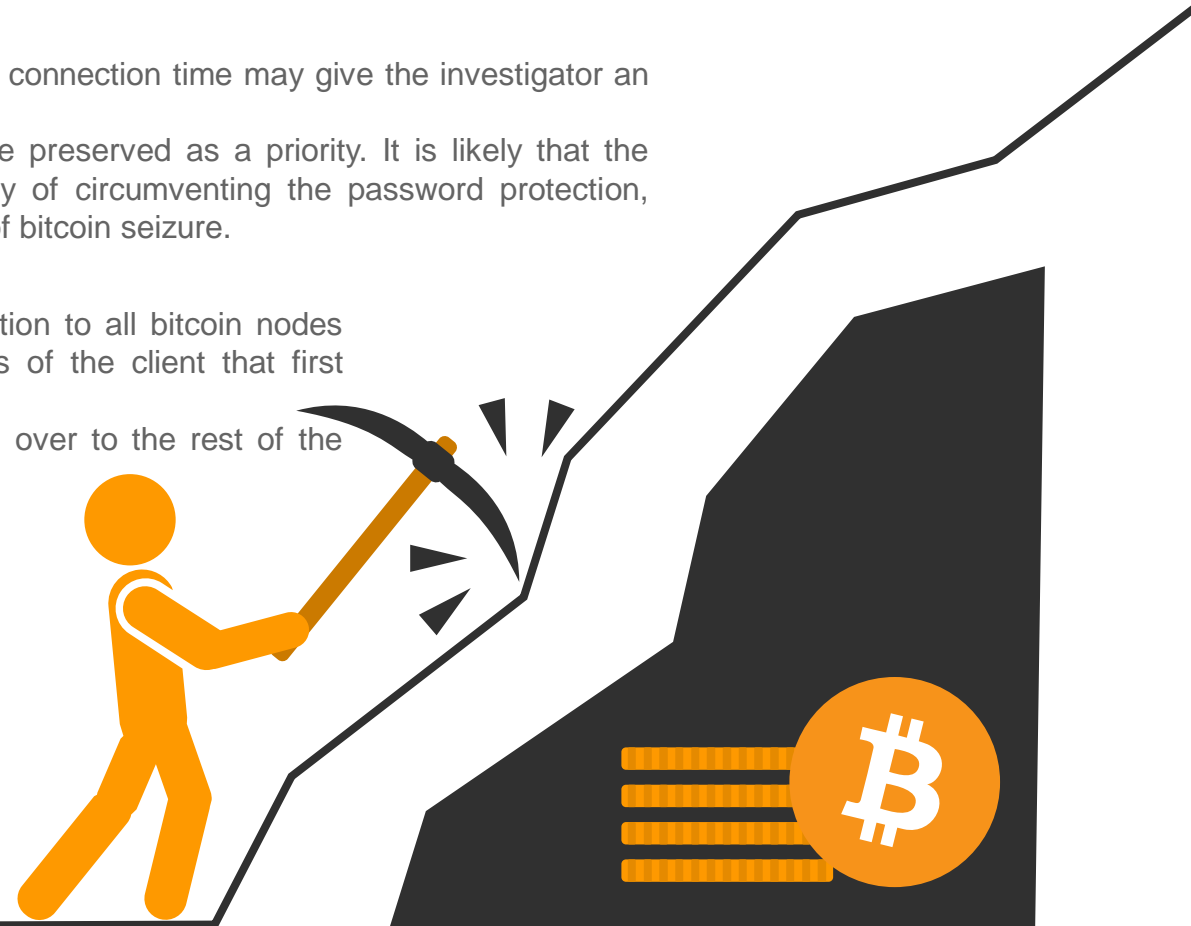
03

To conduct deanonymisation, it would be necessary to open a connection to all bitcoin nodes active in the network and for each transaction to find the IP address of the client that first broadcast the transaction to the network.

Based on how bitcoin works, the first person who sends a transaction over to the rest of the bitcoin network should be the payer.

04

It is recommended that LE does not spend investigation resources on trying to monitor the bitcoin network in order to discover the payer's IP address. Instead, LE should keep in touch with partners in the specialised private sector and academia who may invest in running their own nodes in the bitcoin network.





# Bitcoin wallets and seizure



Identify the suspect and seize bitcoins that were stolen or used to facilitate criminal activities.

Bitcoins are not actually stored 'on' a device; instead, the device stores a wallet that contains the private key that allows the bitcoins to be spent.



## **The private key will be controlled:**

1. by a wallet installed on the suspect's computer, phone or external storage device including a HW wallet or USB disk;
2. by a paper wallet or being written on a piece of paper;
3. by the third party who manages bitcoins for someone else — usually — or the virtual currency exchanger or online wallet provider. In these cases, the third party may be in control of the private key.

# Bitcoin wallets and seizure



## Software wallets

These wallets provide a graphic user interface (GUI) that allows the users to conveniently check the balance on their bitcoin addresses and the list of recent transactions and to send/receive bitcoins. Some of the most popular software wallets are Bitcoin Core and Electrum. A key difference between the original client Bitcoin Core (previously also known as Bitcoin-Qt) and many other software wallets is that the former requires download of the full blockchain

Most of the other wallets are so-called lightweight wallets that only download the portion of the blockchain that is relevant for the user rather than the full blockchain. Software wallets store wallet.dat file on a local drive. access to the suspect's computer is all that is required to access the bitcoins and transfer them to an LE-controlled wallet

*The light wallets* are particularly popular on mobile devices and smartphones that are short on disk space, computing resources and battery. As the blockchain gradually increases in size, we can expect increasing number of users to move from full to lightweight clients or online or mobile wallets such as Coinbase, Blockchain.info, Xapo or Circle. Since these wallets do not store blockchain locally, they are dependent on third party online services to parse the blockchain and return relevant results to the user's wallet. When a wallet requests specific data, it reveals the bitcoin addresses it stores, which creates a privacy risk and provides an interesting opportunity for a bitcoin investigator.

# Bitcoin wallets and seizure



## Mobile devices

Access to the private keys for mobile wallets requires:

- (a) unlocking the phone;
- (b) opening the wallet application, which may be locked by a PIN/fingerprint verification.

users who own large amount of bitcoins store the majority of bitcoins in paper, hardware or a software wallet and would only use the mobile wallet to store smaller amounts of bitcoin for day-to-day transactions

## Web wallets

Access to web wallets requires knowledge of the username or wallet ID, password and possibly twofactor authentication codes. The best-known web wallet is the one operated by the most popular blockchain explorer [blockchain.info](https://blockchain.info)

## Paper wallets

Paper wallets store private keys completely offline. All that is required for access to bitcoins is the private key that can be printed and stored exclusively on paper. The private key is often accompanied by a public key and corresponding QR codes. Afterwards, the keys are saved to a piece of paper and any files created on the computer can be deleted. . Most wallets allow import of private keys and this option can be commonly seen in File -> Import menu.

## Deterministic wallets

So-called deterministic wallets, which can be either software, online wallets or paper or hardware wallets, derive private keys from a seed, quite commonly in form of 10 to 15 words that may or may not form a sentence. The key advantage of the deterministic wallet for a typical user is the ease of backup and recovery. If the user remembers or writes down the seed to a deterministic wallet, he or she no longer has to worry about unrecoverable wallet files or corrupted hard drive. Instead, he or she may recreate a new wallet from the seed. This would reliably recover all private and public keys from the wallet so the seed can essentially be thought of as the master password. That also means that if an attacker or investigator discovers the seed he or she will gain an immediate access to all bitcoin addresses in the deterministic wallet.

# Bitcoin wallets and seizure



## Hardware wallets

A hardware wallet is a special type of bitcoin wallet which stores the user's private keys in a secure hardware device. This wallet securely stores the private keys so that it cannot be transferred out of the device in plaintext.

How hardware wallets sign transactions:

1. Hardware wallets often receive a transaction from a computer typically via USB.
2. The hardware wallet signs the transaction.
3. The signed transaction is then transferred back to the computer and broadcast to the network.

This process does not reveal a private key. Therefore, this process does not expose the private keys to an accessible internet connection. Access to the private keys stored on a hardware wallet requires physical access to the device.

Some bitcoin wallets have a convenient interface for signing and verifying messages. Bitcoin Core offers these functions right under File in the main menu. Despite the prominent placement, these functions are often not understood or actively used by the majority of bitcoin users.



**Seizing the illegal  
BITCOIN in order to  
compensate the  
victims of THB**

# Seizing the illegal BITCOIN



**To seize the bitcoins at the suspect's premises, investigators have to locate:**

1. the bitcoin wallet on the suspect's hard drive — in which case a password is needed to manipulate the bitcoins as the vast majority of wallets nowadays are encrypted;
2. the suspect's private key — in which case there is a need to import it into a wallet;
3. the suspect's recovery seed (usually 12-24 random words).

To seize bitcoins it is not sufficient to simply copy the wallet.dat file, import the private key or enter the recovery seed into the LE-controlled software. The investigator has to transfer these into a bitcoin address controlled by law enforcement.

Alternatively, the bitcoin address can also be provided to LE by a bitcoin exchanger. This is particularly useful if LE seek to immediately convert seized bitcoins to fiat currency (a traditional currency such as € or \$)

## How to investigate bitcoin transactions

Unknown creator Satoshi Nakamoto: 'The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.' As mentioned earlier in this guide, all bitcoin transactions can be viewed and inspected without a need to send subpoenas or MLATs .



**Google it!**



**Use a  
blockchain  
explorer**

Before trying anything else, one should simply run the BTC address through the search engine. The successful hits often lead to online forums such as [bitcointalk.org](http://bitcointalk.org), where the bitcoin addresses feature in the messages, signatures or profiles of the discussants. Many forums display public information on the person who created the post including nickname, contact details and lists of all posts along with associated timestamps. Furthermore, IP logs, activity summaries, personal/private messages and additional contact details may be provided by the administrators on request.

All bitcoin transactions dating back to the very beginning of 2009 are recorded in bitcoin blockchain, a large public database storing all data in an unencrypted state. The blockchain is not stored centrally — it is stored by thousands of individuals and companies around the world running bitcoin clients. Anyone can download the blockchain files and try to dissect the data, import it to a database and query it.

# Seizing the illegal BITCOIN



**Tracing bitcoin transactions using miners!**



**Commercial tracing and attribution tools for investigators**

Every single participant may see a slightly different list of transactions. This is due to many factors including the distributed nature of the network, network latency, different implementation of bitcoin clients and malicious actors trying to spend the same input twice or otherwise abuse the network. Therefore it is common that some nodes in the network know about a particular transaction while some others do not. And so there is a need to establish which set of transaction is the 'correct' one.

There are commercial tools available on the market that are customised to cater for an investigator's needs. These are often superior to a combination of the open source tools as they may offer:

- improved clustering of addresses;
- a higher number of identified entities;
- an improved user interface;
- the possibility to import/export data;
- references to bitcoin addresses and transactions harvested from both the clear web and darknet;
- further functionality, such as searching for the shortest path to an entity that can identify the suspect;
- assistance with specific investigation-related queries.

# Seizing the illegal BITCOIN



Tracing  
bitcoin  
transactions

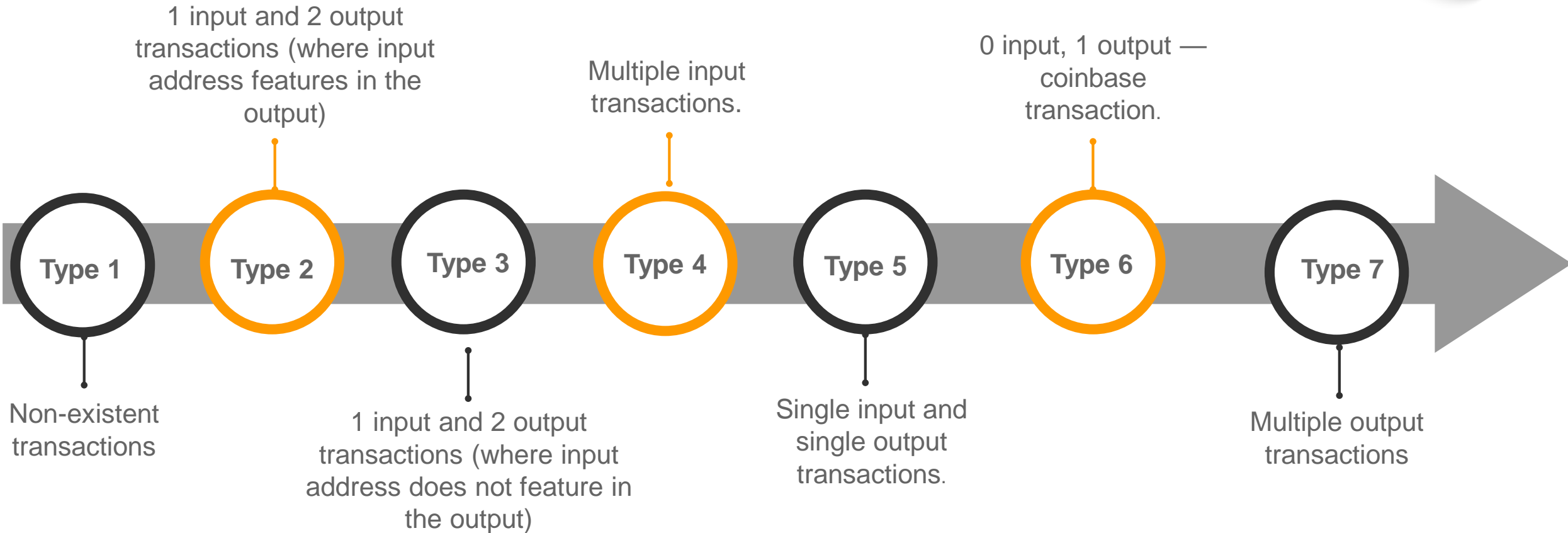
## It is necessary to understand the following basic rules for the transactions:

1. One person can have multiple wallets and one wallet can hold multiple bitcoin addresses.
2. A non-zero number of bitcoins must be transferred from one address to another.
3. Each transaction has an input and output side. Input shows where bitcoins are coming from and output shows where the bitcoins are going to.
4. The addresses on the input side must have a sufficient amount of bitcoins available for the transaction. It is not possible to send more bitcoins than one already has in one's possession.
5. All addresses on the input side will be fully spent.
6. The majority of transactions in the blockchain and practically all recent transactions have to include a fee; otherwise miners may not put the transaction into the blockchain.
7. The amount of all inputs must be equal to amount of all outputs plus the fee for the transaction (Sum of inputs = sum of outputs + fee). Bitcoin transactions follow the zero sum logic so what goes in must come out.

A transfer from one bitcoin address to another does not necessarily represent a movement of funds from one person to another and it may not even represent a movement between two different wallets. One address may send bitcoins to another address and but these two addresses may still reside in the same wallet. What is 100 % certain is that the flow of bitcoins from one bitcoin address to another and everything else is a mere hypothesis.



# Types of transactions



# Recommendations for the investigators



**We highly recommend that, due to very technical method, the transaction analysis must be done by a digital police officer and an analyst officer, under the supervision of the main Investigator**

# Seizing procedure



The bitcoin does not 'physically exist', meaning potential investigative and legal challenges arise for law enforcement and the Courts.

**The United Nations Office on Drugs and Crime ('UNODC')** published a 'Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies' (hereinafter 'Manual') providing a guide as to how the Bitcoin can be located and seized.

According to the Manual, the way in which Bitcoin can be located and seized is by locating and taking control of the Bitcoin wallet. This is because the bitcoin wallet contains the intrinsic information of the private keys. It can either be seized by the authorities by taking away the instrument (e.g. the hard drive) or by transferring the balance to the Bitcoin wallet that is in the control of the State.

## **Jurisdictional Issue**

The advantage of locating and seizing the Bitcoin wallet is that the potential complex jurisdictional issues that the use of virtual currencies creates, (as it operates in the online environment that blurs the national borders) can be avoided. The physical location of the instrument containing the Bitcoin wallet will in most cases be considered as the rightful jurisdiction for the purposes of freezing, seizure and confiscation.

# A 4-step process to seizing a suspect's Bitcoin



Once it is discovered that criminal activity may involve bitcoin, there is often limited time to access the suspect's wallet. At this step, law enforcement should determine if it is possible to access the wallet by obtaining necessary passcodes or keys. Access should be restricted to all devices that may contain bitcoin.

Law enforcement must have its own bitcoin wallet to store seized bitcoins. If the bitcoin wallet is not encrypted, law enforcement has complete access (provided proper warrants have been obtained for the seizure of the device). If the bitcoin wallet is encrypted, getting the suspect to volunteer the encryption code is the easiest method of access. If the suspect does not offer the encryption code, an admission that the suspect knows the encryption code is helpful in obtaining an order compelling the suspect to unlock the wallet. If immediate access to the suspect's wallet is not possible, the device should be switched to airplane mode or placed in a faraday bag to prevent tampering. Once decrypted, law enforcement can transfer the seized bitcoin to their wallet. Note there are different ways of transferring the bitcoin depending on how it was stored by the suspect.



Law enforcement must ensure that their bitcoin wallet is secure. For example, a web-based wallet should only operate on a secure server. Establishing a bitcoin vault (if possible) also provides additional security because transfers out of the wallet are subject to approval by multiple parties.

Bitcoin is often used on the dark web, which is a part of the Internet that requires special software access. The dark web provides a layer of anonymity for illicit transactions using bitcoin. However, it is still possible to trace seized bitcoins back to these dealings. This is done by accessing a 'blockchain' ledger that stores information which is similar to a full history of banking transactions.



# A short review of detecting illegal cryptocurrencies. Few ideas

1

## Open source

Often, the OCG`s members expose their goods in online: Facebook, Twitter. etc. Luckily, some of the assets must be registered(cars, terrains, houses), If these are not present in the suspect`s financial balance, a cryptocurrency investigation can be launched

2

## HumInt

One of the most common gathering information police method. Human sources could lead to the discovery of goods, bank accounts, secret meeting and plans, new victims etc. Not always these information can use as judicial evidence, because of the risk of identity deconspiration.

3

## Victim interview

The best source of intelligence and evidences.

4

## Suspects statement

Sometimes some of the suspects can give important details in order to take advantage of an agreement with the prosecutor or the judge.

5

## JIT`s /LoR`s benefits

Ask the support of the foreign agencies.It also might have better IT techniques.

6

## IT private companies

There are commercial tools available on the market that are customised to cater for an investigator`s needs. It may offer:

- improved clustering of addresses;
- a higher number of identified entities;
- an improved user interface;
- the possibility to import/export data;
- references to bitcoin addresses and transactions harvested from both the clear web and darknet;
- further functionality, such as searching for the shortest path to an entity that can identify the suspect;
- assistance with specific investigation-related queries.

7

## Devices DataExtract

When do house searches, be always accompanied by a digital police investigator. Also look after handnotes, QR codes, passwords etc.

8

## Look for Hardware wallets like TREVOR or BITLOX

A hardware wallet is a special type of bitcoin wallet which stores the user`s private keys in a secure hardware device. This wallet securely stores the private keys so that it cannot be transferred out of the device in plaintext.









9

## RED FLAG SYSTEM

Compare all the data`s that you collect with others authorities(foreign police force) databases, that they have from other investigations  
Asset tracing Implementing `red flag` indicator systems to notify relevant authorities about certain wallets

# Main cryptocurrencies used in criminal activities



Coin	Bitcoin	Ethereum	Ripple	Litecoin	Dash	Monero	Doge	Zcash
Ticker	BTC	ETH	XRP	LTC	DASH	XMR	DOGE	ZCE
Logo								
Total value	\$37.7B	\$15.8B	\$13,2B	\$1.5B	\$980M	\$598M	\$401M	\$337M
Price	\$2308	\$176	\$0.34	\$29.3	\$134	\$42	\$0.004	\$243
Started	Jan 2009	Jul 2015	2012	Oct 2011	Jan 2014	April 2014	Dec 2013	Oct 2016
Unique selling point	Leader	Smart contracts	Relations with banks	Early follower	Privacy Instant Tx	Privacy	Marketing	Privacy
Address starts with	1, 3	0x	r	L	X	4	D	t1, t3, z1, z3
Address length	26-35	42 hex	34	34	34	95	34	35 or 96
Private key starts with	5, L, K	random	s, p	6, T	7, X	random	K, L, 6	K, L
Private key length	51/52	64 hex	51/52	51/52	51/52	64 hex	51/52	51/52
Largest Exchanges (>5% share)	Poloniex Bitfinex Kraken GDAX Bitstamp	Poloniex Kraken Bitfinex GDAX xBTCe	Poloniex Kraken Ripple BTC38	Poloniex OKCoin Huobi BTC38 Bitfinex	Poloniex YoBit HitBTC Bitfinex	Poloniex HitBTC Bitfinex	Poloniex BTC38 Jubi Yuanbao	Poloniex HitBTC Bitfinex Yunbi Kraken



# AML D 5 EFFECT

# Anti money laundering Directive 5



**DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU**

“A digital representation of value that can be digitally transferred, stored or traded and is accepted by natural or legal persons as a medium of exchange.”

**Information Sharing.** In order to enhance and simplify access to information on the identity of holders of bank and payment accounts, the 5AMLD requires EU Member States to put centralized automated mechanisms in place at the national level to identify payment accounts and bank accounts held by a credit institution, thereby developing a central source to identify all bank accounts for an individual person.

**Enhanced Due Diligence.** The 5AMLD will require Member States to apply a specific list of enhanced due diligence (EDD) measures for transactions involving entities on a list of high-risk third countries defined by the European Commission. This proposal outlines the minimum EDD measures obliged entities must apply, which will provide for a formalized approach and alignment of such EDD measures with the list of actions drawn up by the FATF. This will ultimately lessen differences in regulatory requirements between States, minimizing cases where a select number of EU countries commercially benefit relative to others adopting more stringent EDD requirements. Critically, this aims to reduce the ability of terrorists to exploit weaknesses in these measures.

The 5AMLD also brings Virtual Currency Exchange Platforms ( ), Digital Asset Platforms and Custodian Wallet Providers (CWPs) under the scope of the framework and includes them within the definition of ‘obliged entities’, conferring them the same responsibilities as financial institutions, requiring them to apply KYC and EDD controls and conduct ongoing transactions monitoring with the requirement to immediately report suspicious activity to government entities.

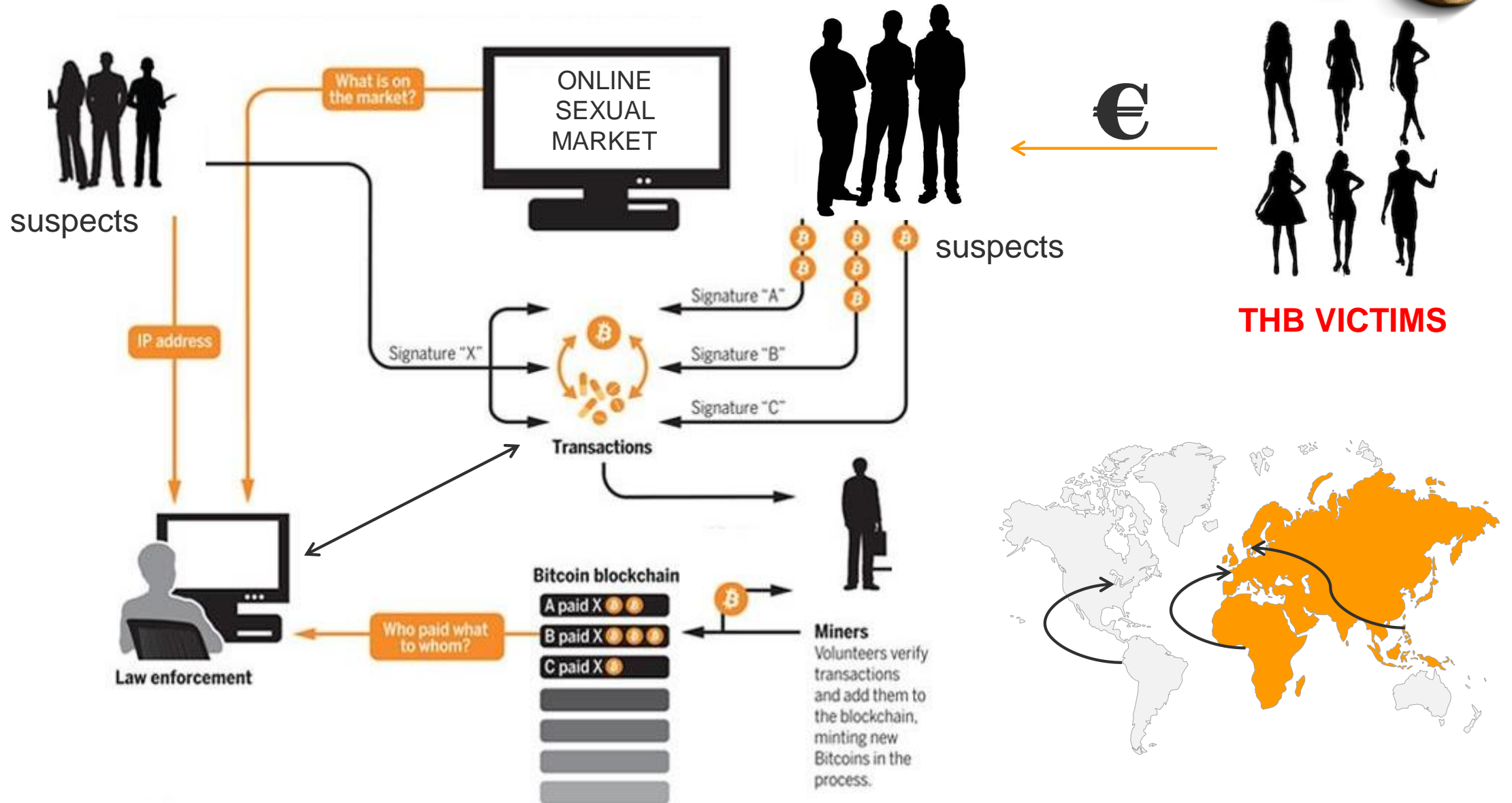
The anonymity of crypto and virtual currencies facilitates the potential misuse for criminal purposes, in order to combat the 5 AMLD proposes that EU Financial Intelligence Units (FIUs) should be able to obtain authoritative identity information allowing them to associate addresses to its owner.

AMLD5 would enter into force by the end of 2019.





# CRIMINAL DRAW





# Conclusions

Bitcoin is far from completely anonymous. Yes, it is true that bitcoin blockchain itself does not reveal any information that could lead to identification of a payer and a recipient.

On the other hand, a combination of open source research, commercial tools and information provided by private sector can lead to identification of suspects and their financial activities. Bitcoin was not created with the objective of being completely anonymous. Instead, it combines an interesting mix of transparency and privacy for its users, which is referred to as pseudonymity. This concept is best explained by its to-this-day-unknown creator Satoshi Nakamoto: *'The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.'*

More and more criminals accept cryptocurrencies payments in their illegal activity. They are preferred by migrant smugglers, like the following scheme: the migrants are paying the services of the final guide in a FIAT currency, and after that he is exchanging the money into BITCOIN for paying the other members of the OCG. Also, lately some of the legal brothels or escorts agencies accept BITCOIN payments(for example VIP Passion, Bubble Escorts or Bunny Ranch). Police force should be very preventive because might be a risk that the traffickers, hiding behind legal companies, could create organised crime groups for sexual exploitation of the girl/minors, so that illegal incomes might be hard to trace.



**Pitești Brigade of Countering  
Organized Criminality  
Unit of Combating Human  
Trafficking**

# Thank you!

Deputy superintendent

Alexandru VIZIRU

[alexandru.viziru@ag.politiaromana.ro](mailto:alexandru.viziru@ag.politiaromana.ro)