#CRYPTOANALISIS AML:

- ¿Dónde está el riesgo real en la utilización de la tecnología crypto en materia de prevención de lavado de activos?
- Avances (o no) en la regulación y supervisión en la región.
- El impacto en las recomendaciones del GAFI.
- Misceláneas.

RETROSPECTIVA

- Las monedas virtuales son representaciones de valor emitidas por desarrolladores privados, pueden comprarse, negociarse y redimirse por vía electrónica y abarcan desde millas aéreas hasta el Bitcoin (El cual está encriptado y es “cuasi” anónimo).

- El dinero electrónico es la expresión binaria de una moneda de curso legal

Aspectos regulatorios:

- El dinero electrónico puede regularse (De hecho, lo está).

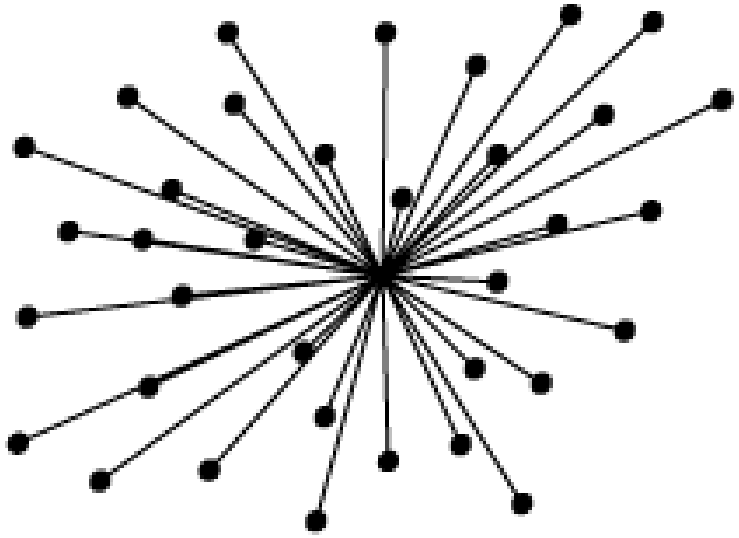
- Las monedas virtuales...
- …Representan un peculiar desafío al conformar redes globales extremadamente sofisticadas, mientras que las regulaciones han sido tradicionalmente desarrolladas a nivel local.

BITCOIN

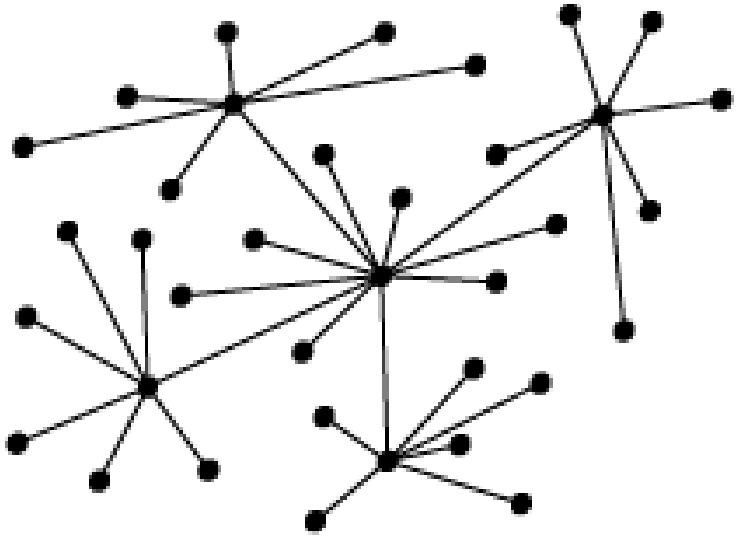
=

MONEDA VIRTUAL

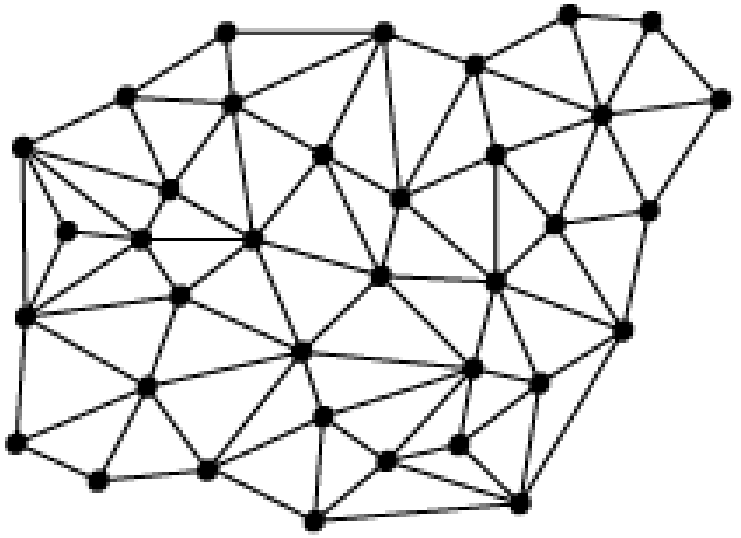
MONEDA VIRTUAL
≠
DINERO ELECTRÓNICO



centralised



decentralised

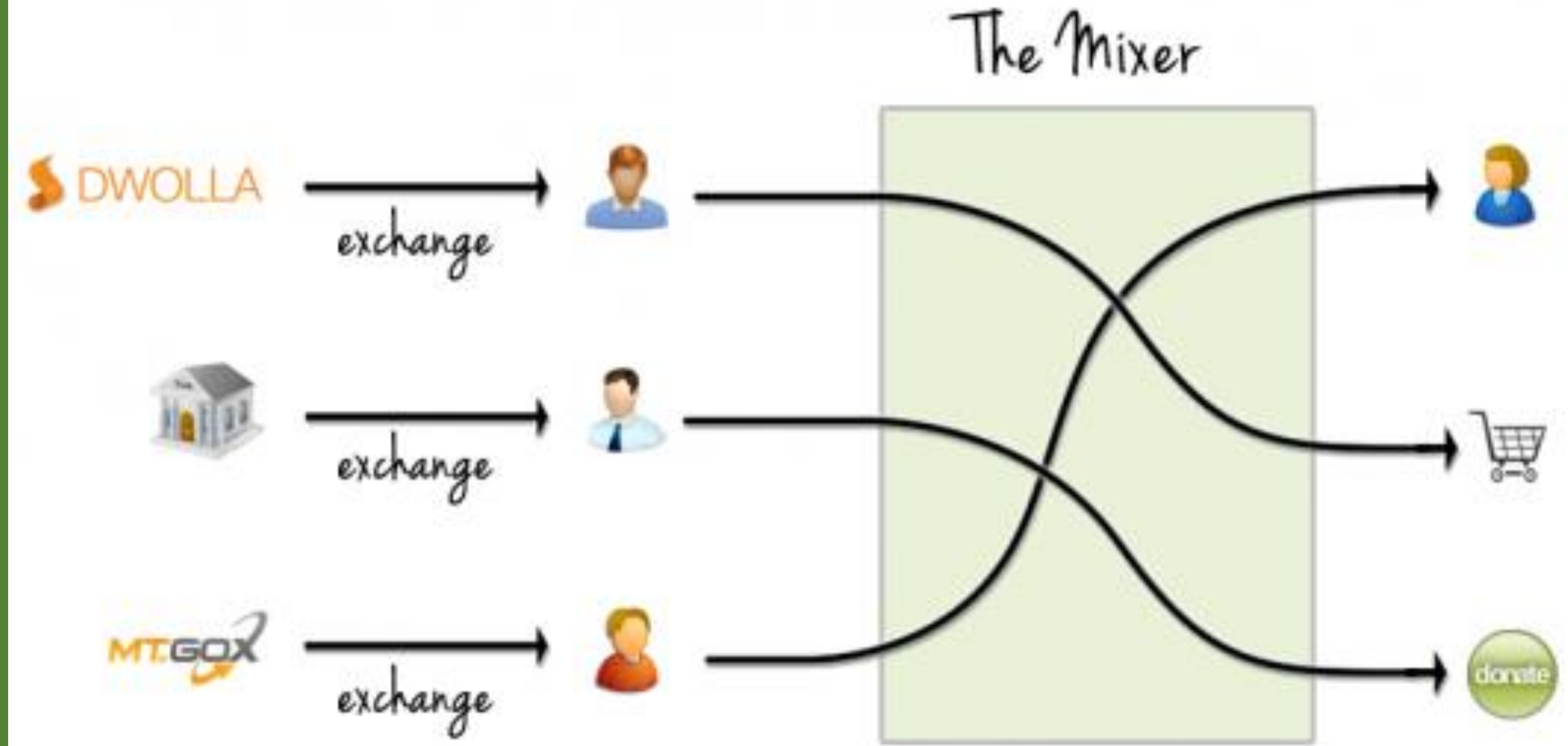


distributed

- Cada transacción Bitcoin es registrada públicamente. **Con suficientes recursos destinados al análisis**, es posible llegar a reconocer que un grupo de transacciones han sido realizadas desde una misma cartera, e incluso dar con la identidad del dueño de dicha cartera, si alguna vez hubiera revelado información personal asociada a una dirección pública.

- Lo que se registra en el blockchain, queda allí para la eternidad.

Sí… Pero no…


The Mixer
DWOLLA
exchange
exchange
MT.GOX
exchange
donate

El problema de esto es…

La asequibilidad de la opacidad y el anonimato

Al disminuir enormemente el costo de la privacidad y al mismo tiempo aumentar exponencialmente el costo de la violación de la privacidad, Bitcoin ha cambiado las reglas del juego.


MOSSACK FONSECA

- El problema era la opacidad de las estructuras corporativas.

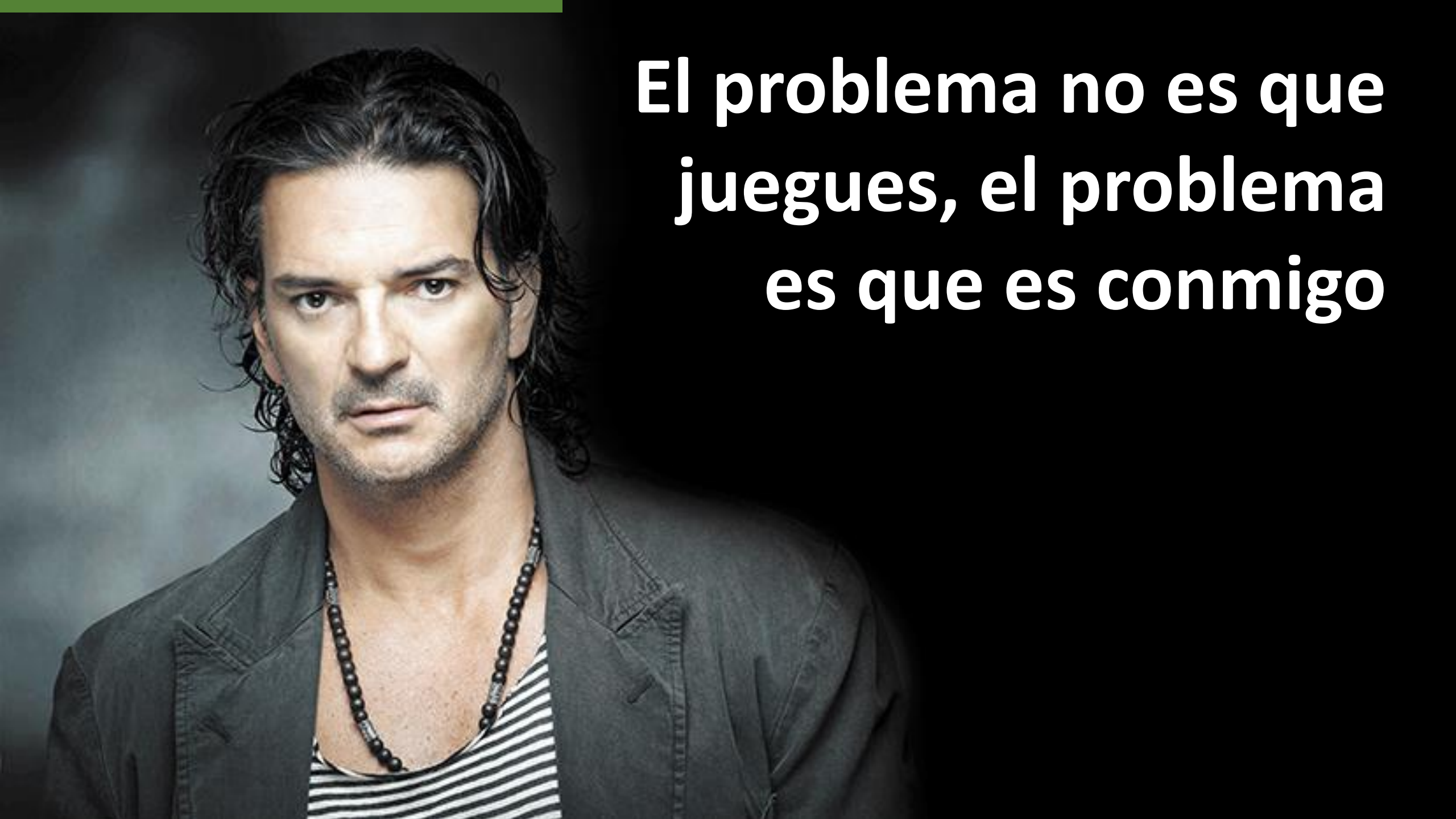
- Allí, lo opaco es básicamente el B.O. de la sociedad que aparece como protagonista de la transacción. La transacción no es opaca puesto que es realizada mediante el sistema bancario, mecanismo controlado si los hay.

- Esta nueva ola de ~~criptomonedas~~ criptoactivos genera opacidad tanto en la identificación del protagonista (B.O.) como en la trazabilidad real de la transacción.

El problema empieza cuando tienen contacto estos dos mundos: el regulado y el desregulado.

Y quienes deben resolverlo son siempre los mismos: los del mundo regulado.

problem?


El problema no es que juegues, el problema es que es conmigo

Criptoactivos

Bitcoin, Crimen Organizado, Corrupción, Lavado de Dinero y Terrorismo

¿Qué está pasando?

Criptoactivos… Cripto… Crypt…


TALES
FROM THE
CRYPT

Bitcoin sigue siendo la herramienta preferida de lavado de dinero en América Latina

NOTICIAS DEL DÍA Escrito por Juan Camilo Jaramillo - MAYO 7, 2019

Brasil | Colombia | Lavado de dinero

SHARE

Despite having lost most of its value since December 2017, bitcoin remains a tool of choice for laundering the proceeds of

El aumento en el uso de criptomonedas por parte de organizaciones criminales para limpiar el dinero proveniente de actividades ilícitas, es un llamado a las principales autoridades

ARTÍCULOS RELACIONADOS

Principales casos e investigaciones sobre corrupción en Odebrecht en 2019

Pandilla en México ofrece 'menú de drogas' por WhatsApp cifrado

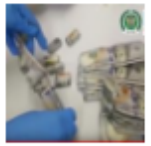
El pasado 23 de abril, agentes del Departamento de Investigaciones sobre Narcóticos (DENARC), lograron la captura de un hombre que manejaba un laboratorio clandestino de minería de criptomonedas en la ciudad de Porto Alegre, Brasil. El hallazgo, tomó por sorpresa a las autoridades, quienes estaban detrás de una investigación vinculada al tráfico de drogas en esta zona.

"Todo indica que puede ser una actividad de minería de bitcoin. Pueden hacer el cambio y el pago para los distribuidores de drogas. También hay posibilidad de estar usando el dinero del tráfico para comprar bitcoins", declaró un delegado de la Policía en el caso.

En el sitio de la captura, las autoridades se encontraron con 25 máquinas de minería de criptomonedas, que operaban las 24 horas del día. Esta maquinaria de avanzada tecnología, tenía un valor estimado de US$65.000 y de acuerdo a la policía, su origen estaba relacionado con mercancía de contrabando procedente de China.

VEA TAMBIÉN: Cobertura sobre lavado de dinero

La minería de criptomonedas, es una modalidad que permite la validación de las transacciones hechas con bitcoins por medio de una red de computadores que demandan un gran gasto de energía. Es de gran atractivo para los criminales emplear la minería de estas



Mulas en Colombia ahora ingieren dinero sucio

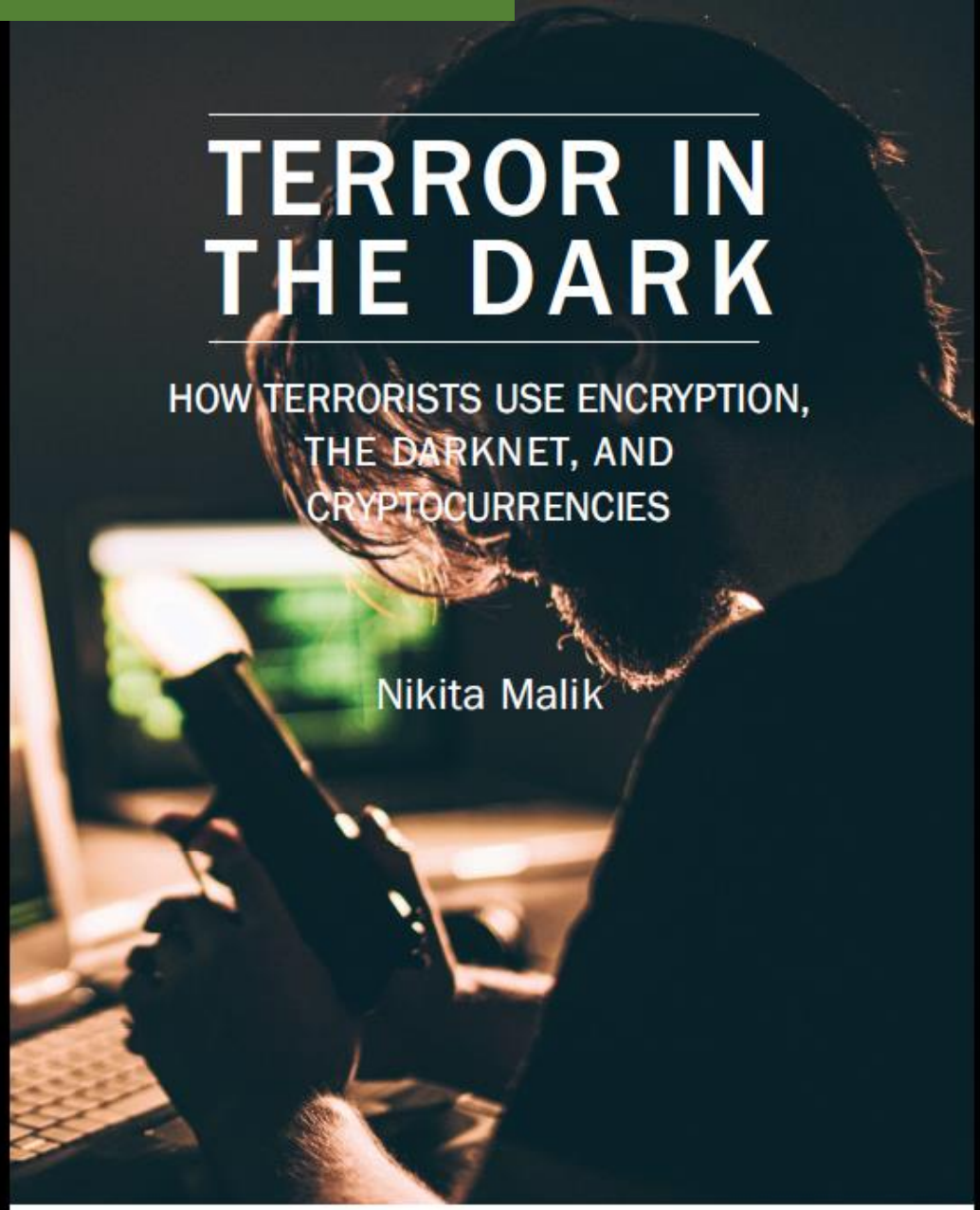
Persiste impunidad en casos de periodistas asesinados en Latinoamérica

La minería de criptomonedas, es una modalidad que permite la validación de las transacciones hechas con bitcoins por medio de una red de computadores que demandan un gran gasto de energía. Es de gran atractivo para los criminales emplear la minería de estas divisas, ya que les permite realizar transacciones internacionales para blanquear el dinero sucio sin ningún tipo de control financiero estatal.

No es el primer caso en el que se involucra el uso de criptomonedas y lavado de activos en América Latina, en abril de 2018 la Guardia Civil española, desarticuló una estructura criminal que se encargaba de comprar Bitcoins con dinero procedente de negocios ilícitos, cuyo destino eran cuentas en Colombia donde se "legalizaba" el dinero. En total, la banda uso 174 cuentas corrientes para lavar US$9,3 millones.

Análisis de InSight Crime

La limitada legislación existente en Latinoamérica que previene este tipo de delitos y el escaso control financiero que se puede ejercer sobre las criptomonedas, se convirtieron en motivos de suficiente peso para que las estructuras criminales limpien sus dineros turbios por medio de este sistema,



CRT Centre for the Response to Radicalisation and Terrorism

THE HENRY JACKSON SOCIETY

http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf

Executive Summary

Following the five terror incidents on British soil in 2017, the Government has devoted greater attention to the presence of online extremism, recognising that it has a role to play in the fostering of "homegrown" terrorism within the UK. However, this report makes a strong case for greater attention to be placed on the "Darknet" – portions of the internet that are not easily accessible by the public at large, without dedicated expertise. This report demonstrates how terrorists and extremists have utilised the Darknet to mask their communication and propaganda efforts, to recruit and radicalise, and to gain material benefits such as illicit goods: including, but not limited to, weapons and fraudulent documents. In addition, this report notes the growing tendency of these individuals to utilise cryptocurrencies for transactions and fundraising, enabling them to evade detection by law enforcement entities.

While the first decade of the century was defined by the battle against jihadist "safe havens" – physically located in Afghanistan, North West Pakistan, Yemen, Islamic State, and so on – this report draws attention to the possible rise of "virtual safe havens": encrypted communication channels, hidden portions of the internet, cryptocurrency accounts that are not registered with any banks, and more. In doing so, it highlights the following trends:

- **Terrorists using encryption to hide:** Better monitoring of the surface web by social media companies and security officials has resulted in a faster rate of removal of extremist content from social media platforms.[1] Correlated to this is an increased use by extremist networks of the Darknet as a "jihadist safe haven" for planning attacks. Evidence suggests that recruiters use the Darknet to plan and launch terrorist attacks, because detection by law enforcement is less likely.[2] While initial contact can be made on surface web platforms, further instructions are often given on end-to-end encryption apps such as Telegram on how to access jihadist websites on the Darknet.

- **Terrorists using the Darknet for recruitment purposes:** Given the largely inaccessible nature of encrypted channels like Telegram and areas of the Darknet, it is perhaps unsurprising that mass recruitment rarely takes place on these channels. Instead, IS aims to draw interested sympathisers from the surface web and social media into the more secure recesses of the Darknet for further interaction and indoctrination.

- **Terrorists using the Darknet as a reservoir of propaganda:** The removal of extremist and terrorist content from the surface web and deep web – particularly in the case of artificial intelligence programs that may do "bulk" removals – increases the risk that evidence needed to prosecute individuals disseminating content or providing material support to terrorist organisations may be lost. Much of this material later resurfaces on the Darknet. Technology companies should work with law enforcement to ensure that this material is archived effectively to understand patterns of behaviour.

- **Terrorists using cryptocurrency to evade detection and to fundraise:** Terrorists, like other criminals, use cryptocurrency because it provides the same form of anonymity in the financial setting as encryption does for communication systems. By fundraising and making financial transactions online with bitcoin, terrorists and other criminals can avoid interference from financial regulators or other third parties who might otherwise take steps to prevent their operations. According to a 2015 Europol

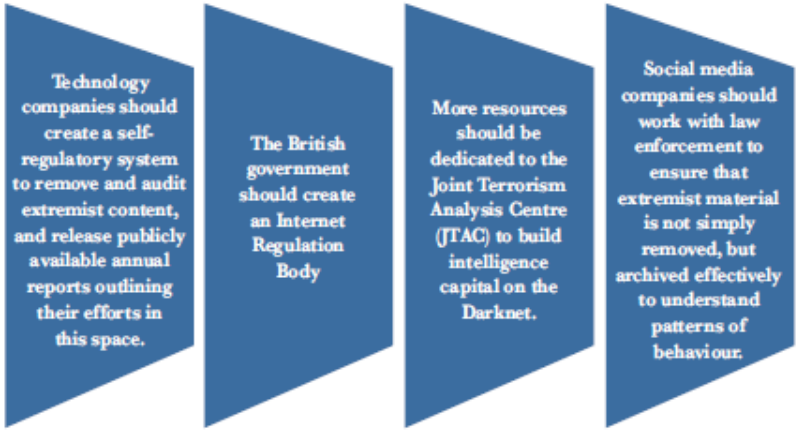
[1] See, for example: The YouTube Team, 'An update on our commitment to fight terror content online', *YouTube Official Blog*, 1 August 2017, available at: http://youtube.googleblog.com/2017/08/an-update-on-our-commitment-to-fight.html, last visited: 17 March 2018; Hutchinson, T., 'How Tech Giants Team Up to Fight Terrorism', *Fortune*, 26 June 2017, available at: http://fortune.com/2017/06/26/twitter-facebook-youtube-microsoft-eighth-forum-terrorism/, last visited: 14 March 2018.

[2] Dearden, L., 'ISIS urged radicalised BBC reporter to launch terror attacks in London Bridge and Westminster', *Independent*, 4 September 2017, available at: http://www.independent.co.uk/news/uk/home-news/isis-radicalised-bbc-reporter-london-bridge-terror-attack-westminster-borough-market-police-a7929546.html, last visited: 14 March 2018.

http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf

report, bitcoin featured in high-profile investigations involving payments between criminals, and was used in more than 40% of these transactions in the European Union (EU).[1]

The report includes the following policy recommendations:



[1] 'The Internet Organised Crime Threat Assessment (IOCTA) 2015', *Europol*, available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015, last visited: 14 March 2018, p. 11.

http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf

Chapter 1: Surface Web, Deep Web, and Darknet

The following chapter differentiates between the surface web, used by all internet users, the deep web, areas of internet sites only accessible by certain users, and the Darknet, hidden sites that can only be accessed with specialist expertise. This chapter also provides an assessment of the Darknet browser The Onion Router (Tor).

What is the Surface Web? How Does it Differ from the Deep Web?

The surface web, the part of the internet most familiar to everyday users, contains information and websites that are accessed by using standard search engines such as Yahoo, Google, or Bing.[1] Information obtained from these sites is visible to those who want to see it, without any restrictions.

The deep web is approximately 400 to 500 times larger than the surface web.[2] As a result, it holds 400 times more content: 7,500 terabytes of information compared to 19 terabytes on the surface web.[3] In terms of documents, there are approximately 550 billion documents on the deep web (made up of social media pages, email domains, and online banking data), compared to one billion documents available on the surface web.[4] In short, the deep web is the depth of the sea, compared to the surface (see Figure 1).

Figure 1: Surface web, deep web, Darknet

Source: Reproduced and modified with permission from Brandpowder

Unlike the surface web, the deep web has certain user restrictions when it comes to access. Though internet users use the deep web regularly, its data is generally only accessible through application programming interfaces (APIs) in which the user is granted access to the required database.[5] Internet sites

[1] Chertoff, M., 'A public policy perspective of the Dark Web', *Journal of Cyber Policy* Vol. 2 (1), (2017): pp. 26-38, last visited: 3 October 2017, p. 26.
[2] Bergman, M. K., 'White Paper: The Deep Web: Surfacing Hidden Value', *Journal of Electronic Publishing* 7.1 (2001), last visited: 24 October 2017.
[3] Ibid.
[4] Ibid.
[5] Chertoff, M., op. cit., p. 27, last visited: 14 March 2018.

http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf

in Latakia province, Syria.[87] On 30 November 2017, a donation of BTC0.075 (US$685 at the time) was sent by an unknown individual to the organisation's advertised bitcoin address. The following day, the funds (which had risen in value to US$803 overnight) were forwarded to another address.[88] When the group's Telegram account was taken down by administrators, it shifted its fundraising activities to an alternative Telegram account, and by late December 2017 it was still sharing Islamist propaganda and imploring supporters to donate securely with bitcoin.[89] In March 2018, the group was still active on Twitter.

Figure 5: Screenshot of *Al-Sadaqah* campaigning for bitcoin funding on Twitter

How Anonymous is Bitcoin?

Terrorists and criminals use bitcoin because of its anonymity. However, bitcoin is not as anonymous as commonly perceived, as it uses a blockchain system which serves as a virtual record of all transactions on the network. The blockchain is publicly accessible, meaning that someone with a sufficient level of computer literacy can trace the digital footprints of anonymous traders.[90] Because of this, bitcoin is often used on the Darknet with the anonymising software Tor for increased security and anonymity. In this context, criminals use cryptocurrency because it provides the same form of anonymity in the financial setting as encryption does for communication systems.[91]

Both systems hamper efforts by law enforcement to unravel complicated encrypted messaging sites and blockchain payments on the internet. The dangers of cryptocurrency have been highlighted by Europol,

[87] Tsantis, Y. J., 'Terrorist Networks Eye Bitcoin as Cryptocurrency's Price Rises', *The Cipher Brief*, 21 December 2017, available at: [illegible], last visited: 16 March 2018.
[88] Tsantis, Y. J., 'The New Frontier in Terror Fundraising: Bitcoin', *Foundation for Defense of Democracies*, 26 August 2016, available at: [illegible], last visited: 16 March 2018.
[89] Ibid.
[90] Solomon, S., op. cit., pp. 1-2.
[91] 'The Internet Organised Crime Threat Assessment' (IOCTA) 2017', op. cit. p. 40.

¿Qué dice OFAC?

NEWS

Press Releases

Statements & Remarks

Readouts

Testimonies

Featured Stories

Press Contacts

PRESS RELEASES

Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses

LATEST NEWS

May 23, 2019

Treasury Sanctions Argentina-based Goldpharma

May 17, 2019

Treasury May 17 Response to Chairman Neal Regarding Tax Return Request

Treasury Works with Government of Mexico Against Perpetrators of Corruption and their Networks

May 16, 2019

WASHINGTON – The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) took action today against two Iran-based individuals, **Ali Khorashadizadeh** and **Mohammad Ghorbaniyan**, who helped exchange digital currency (bitcoin) ransom payments into Iranian rial on behalf of Iranian malicious cyber actors involved with the SamSam ransomware scheme that targeted over 200 known victims. Also today, OFAC identified two digital currency addresses associated with these two financial facilitators. Over 7,000 transactions in bitcoin, worth millions of U.S. dollars, have processed through these two addresses - some of which involved SamSam ransomware derived bitcoin. In a related action, the U.S. Department of Justice today indicted two Iranian criminal actors for infecting numerous data networks with SamSam ransomware in the United States, United Kingdom, and Canada since 2015.

"Treasury is targeting digital currency exchangers who have enabled Iranian cyber actors to profit from extorting digital ransom payments from their victims. As Iran becomes increasingly isolated and desperate for access to U.S. dollars, it is vital that virtual currency exchanges, peer-to-peer exchangers, and other providers of digital currency services harden their networks against these illicit schemes," said Treasury Under Secretary for Terrorism and Financial Intelligence Sigal Mandelker. "We are publishing digital currency addresses to identify illicit actors operating in the digital currency space. Treasury will aggressively pursue Iran and other rogue regimes attempting to exploit digital currencies and weaknesses in cyber and AML/CFT safeguards to further their nefarious objectives."

Today's action focuses on a ransomware scheme known as "SamSam" that has victimized numerous corporations, hospitals, universities, and government agencies and held over 200 known victims' data hostage for financial gain. To execute the SamSam ransomware attack, cyber actors exploit computer network vulnerabilities to gain access and copy the SamSam ransomware into the network. Once in the

in the Sergei Magnitsky Case and Gross Violations of Human Rights in Russia

May 15, 2019

Statement of Secretary Steven T. Mnuchin Bef the U.S. Senate Appropriations Subcommitte on Financial Services and General Governmen

¿Qué dice el GAFI?

FATF: Draft, Interpretive Note to Recommendation 15 (New Technologies).

1. For the purposes of applying the FATF Recommendations, countries should consider virtual assets as “property,” “proceeds,” “funds”, “funds or other assets,” or other “corresponding value”. Countries should apply the relevant measures under the FATF Recommendations to virtual assets and virtual asset service providers (VASPs).

2. In accordance with Recommendation 1, countries should identify, assess, and understand the money laundering and terrorist financing risks emerging from virtual asset activities and the activities or operations of VASPs. Based on that assessment, countries should apply a risk-based approach.

3. VASPs should be required to be licensed or registered.

4. A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions

5. Countries should ensure that VASPs are subject to adequate regulation and supervision or monitoring for AML/CFT and are effectively implementing the relevant FATF Recommendations.

6. Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative.

7. With respect to preventive measures, the requirements set out in Recommendations 10 to 21 apply to VASPs, subject to the following qualifications:

(a) R.10 - The occasional transactions designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000.

(b) R.16 – Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information2 on virtual asset transfers, submit the above information to beneficiary VASPs and counterparts (if any), and make it available on request to appropriate authorities.

8. Countries should rapidly, constructively, and effectively provide the widest possible range of international cooperation in relation to money laundering, predicate offences, and terrorist financing relating to virtual assets

https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html

Y ya que estamos: Economías colaborativas y *Fintech*

Coordinando a los descoordinados


NYC Subway
Uber
KAYAK
Airbnb
TripCase
Hotel Tonight


SHARING
ECONOMY
OFFERING
SHARE
FINANCE
CONTRIBUTION
EXPERTISE
PROJECT
SUPPORT
NON-PROFITS
PEER-TO-PEER
MARKET
ORGANIZATION
REDISTRIBUTION
UNION
SOLIDARY
PEOPLE
SOLUTIONS
SOCIAL
LENDING
CONTRIBUTION
MONEY
PARTICIPATIVE
TRADING
FUNDING
SYSTEM
COLLABORATIVE
SOCIAL
NETWORK
Airbnb
VISION
MARKETPLACES
PEER
STRATEGY
CORPORATIONS
COMMUNITY
SHARING
FAIR
TRADING
SOCIAL
COOPERATIVE
DISTRIBUTION
TRADE
CONSUMPTION
TripCase


JURASS
K PARK


JURASSIC PARK
™


JURASSIC BANK

Reflexiones finales

- Regulación para *Fintech* y *Cryptoassets*: ¿Analgesia y anestesia?
- Las monedas virtuales y *cryptoassets* no son malos *per se*. Sus problemas son:
  - Su funcionalidad para el LA/FT.
  - Que se mueven en un ecosistema que, por definición, es oscuro, opaco.
- Son preocupantes los casos detectados…
  - … Pero son aún más preocupantes los casos que no fueron detectados.
- Fintech y Economías colaborativas: Coordinando a los descoordinados:
  - ¿Se controla al coordinador?
  - ¿Cómo controlar a los descoordinados?


TITANIC

Derecho Bancario

Cumplimiento ALD y CFT

Derecho Corporativo y Societario

GUILLERMO OMAR GARCÍA ORUÉ

A B O G A D O

guillermo@garciaorue.com

www.garciaorue.com

https://www.linkedin.com/in/guillermogarciaorue/

Tel.: +595 981 550900