



OAS | More rights
for more people

Secretariat for Multidimensional Security

**XLVII MEETING OF THE GROUP OF EXPERTS
FOR THE CONTROL OF MONEY LAUNDERING
September 23 to 25, 2019.
Bogota – Colombia**

**OEA/Ser.L/XLV.4.47
DDOT/LAVEX/doc.11/19
September 24, 2019
Original: Spanish**

**VIRTUAL CURRENCY: AN FIU
PERSPECTIVE**

2019



Cripto-Moneda: Una Perspectiva del UIF

GELAVEX Coordination, Septiembre 2019

Sean Evans y Veyra Cottie

FinCEN Inteligencia, Cibernética y Tecnología



Agenda

- Regulación y Recolección
- Revisión General de Conceptos
- Uso Ilícito
- Análisis de *Blockchain*
- Prácticas



El ALD es sólo una parte de la Arquitectura General de la Regulación Financiera





El Cambio de Moneda Virtual es una Actividad Regulada debido a Cómo se Define la “Transmisión de Dinero”

2011 – Definición de “Servicios de Transmisión de Dinero”

- “La aceptación de moneda, fondos, u otro valor que substituya a la moneda de una persona y la transmisión de moneda, fondos, u otro valor que substituya a la moneda a otro lugar o persona por cualquier medio.”– 31 CFR § 1010.100(ff)(5)(i)(A)

2013 – Guía (FIN-2013-G001)

- **Usuario:** “una persona que obtiene moneda virtual para comprar bienes o servicios” para su propio uso.
- **Cambista:** “una persona que se dedica al negocio del cambio de moneda virtual por moneda real, fondos, u otra moneda virtual.”
- **Administrador:** “una persona que se dedica al negocio de emitir (poner en circulación) una moneda virtual, y quien tiene la autoridad de disponer (sacar de circulación) dicha moneda virtual.”

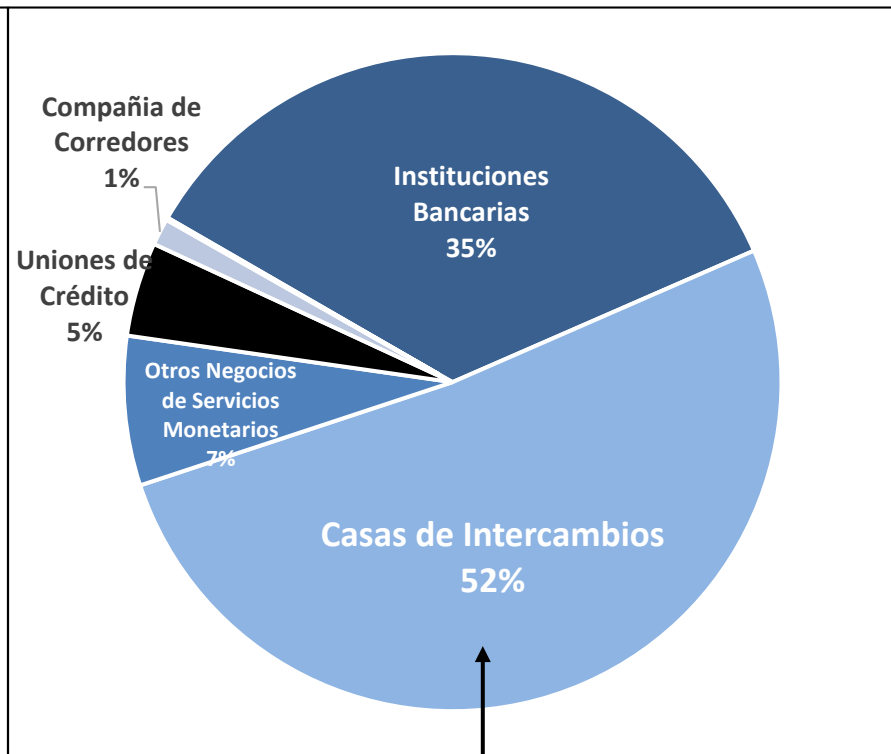
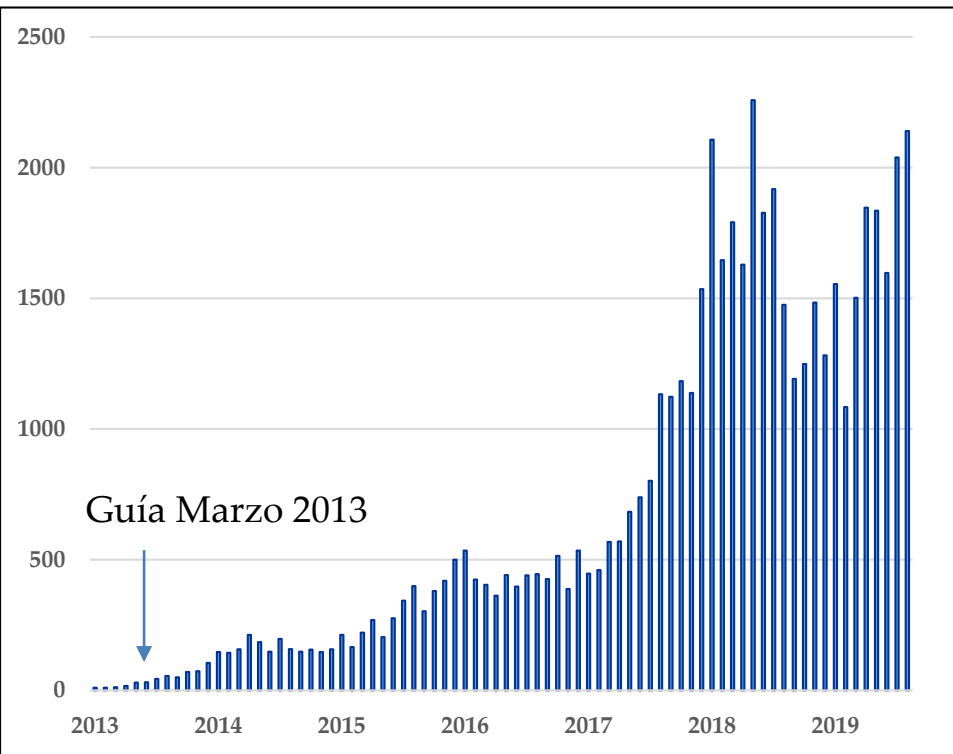


Guía Pública, Advertencias, Examinaciones, y Acciones de Aplicación que Impactan el Cobro & el Cumplimiento

- Guía sobre Moneda Virtual: Marzo 2013
- 7 Reglas Administrativas :2014-2015
- Examinaciones de IRS: 2014-2015
- Penalización a Ripple: Mayo 2015
- BTC-e, Penalización y Cierre: Julio 2017
- Guía sobre Moneda Virtual y Consulta:
Mayo 2019



La regulación de las Entidades de Moneda Virtual y sus Instituciones Patrocinadoras proporciona Visibilidad



160 Prestadores únicos de MV

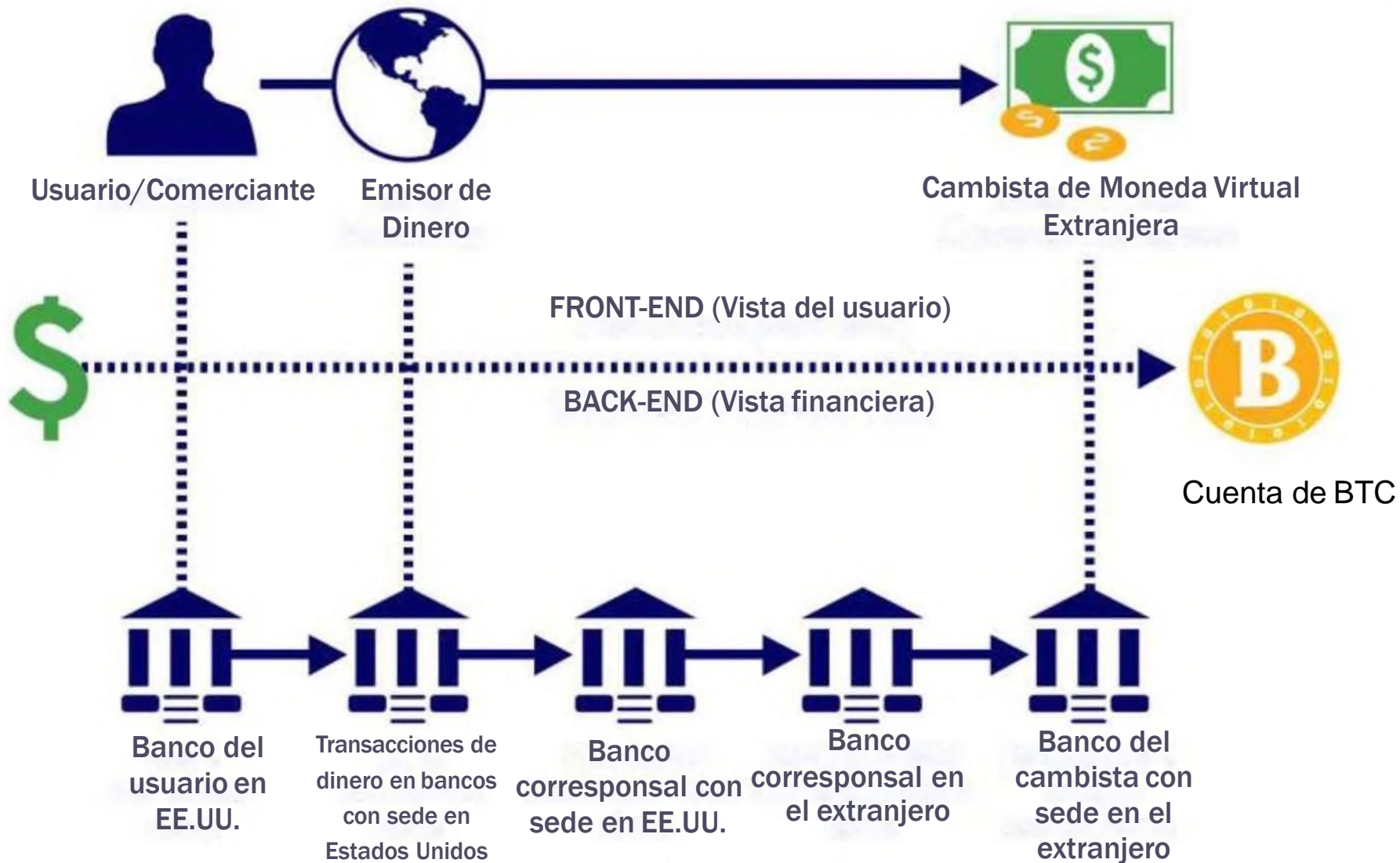


El Cumplimiento del sector Cripto-Monedas Conduce a una Mayor Inteligencia Financiera, Generación de Clientes Potenciales y Análisis de Tendencias

<i>Observación</i>	Banco	Banco Corresponsal	MSB	Cambios Bitcoin
Usuarios	X	X	X	
Cambistas P2P	X		X	X
Casinos Online	X			X
Malware	X			X
Fondos Agregados a Cambistas VC (MV)		X		
Personas Extranjeras		X	X	
Adquirientes de Cuentas			X	X
Fraude	X			X
Servicios Online Ilícitos				X
Mercados en la Darknet				X
Accesos Tor				X



Varias instituciones tienen una ventana única a los flujos de transacciones ilícitas dependiendo de su posición en los esquemas generales





Bitcoin permite el intercambio sin una autoridad central - un banco sin empleados



Usuarios atraídos por el potencial de:

- Velocidad de las transferencias
- Alcance global
- Costes de transacción bajos o nulos
- Privacidad/anonimato
- Programabilidad

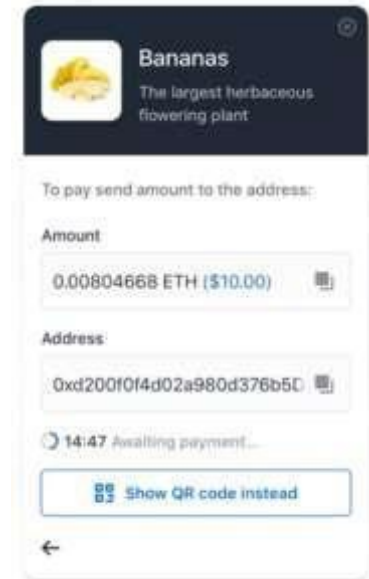
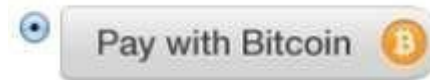
Con limitaciones:

- Valor volátil
- Aceptación limitada (pero en aumento)
- Desafíos con el Software

Aceptado por decenas de miles de comerciantes, incluyendo:



Ejemplos de Pagos de Bitcoin





Implicaciones sobre cómo se mantienen y analizan los registros y cómo se llevan a cabo las investigaciones

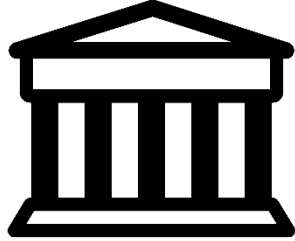
- Cambio en el mantenimiento de
 - Desintermediación entre entidades y propietarios/beneficiarios
 - No hay una ubicación central para los registros
- Cambio en el análisis
 - Diferentes técnicas de investigación
 - Nuevas herramientas de análisis
- Nuevos tipos de delitos/Financiación ilícita
 - Educación
 - Nuevas tipologías



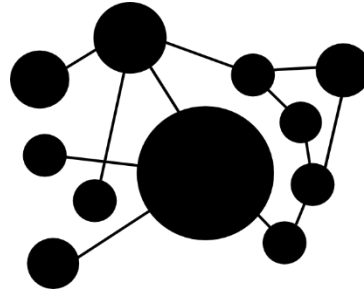
Investigaciones Tradicional vs. Cyberneticas



Suspect



Subpoena
Bank



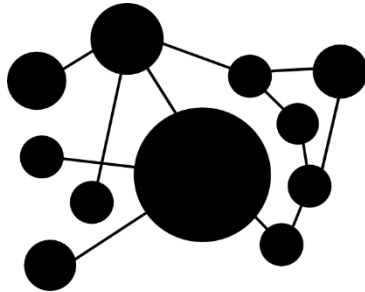
Financial
Analysis



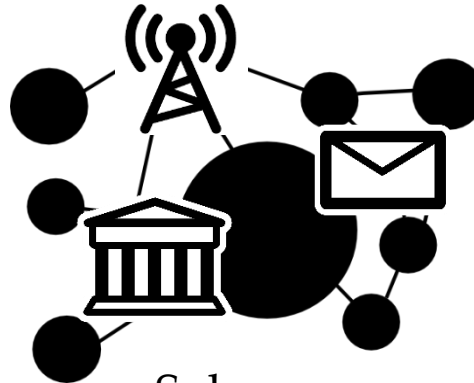
Arrest



No
Suspect



Network &
Financial
Analysis



Subpoena
Record Holders



Arrest



La innovación es posible gracias a una nueva tecnología de contabilidad llamada Blockchain

Banco Tradicional	Bitcoin
Número de cuenta bancaria	Dirección Bitcoin
Ejemplo de cuenta: 012345678	Ejemplo de dirección Bitcoin: 1BUo3pVrFtfMqEz9Uy5UUXoDAYYL46fj2h
Acceso con contraseña/PIN	Accedido con clave privada
Ejemplo de PIN: 1234	Ejemplo de clave privada: 5JtQrdBfgDx4btMBmiTZcrSQqBourYH8p1o PFvbWyU79EvATiJF
Libro de cuentas bancarias = Centralizado	Blockchain=Decentralizado
Libro de cuentas bancarias = Privado	Blockchain=Público
Liquidación=Administrador de confianza	Liquidación = Consenso



Las direcciones pueden ser creadas sin necesidad de Incorporación ...

- Bitaddress.org; <https://www.offlineaddress.com/>; <http://cryptolife.net/upwg/>



Open Source JavaScript Client-Side Bitcoin Wallet Generator

Generating Bitcoin Address...

MOVE your mouse around to add some extra randomness... 318

OR type some random characters into this textbox

```
9f8be774967a59a2be49b983d19d1b35168c0bf850c16efabce9c5f0f5b6c987
b71e9d0b2fbb7844168e96c1a14b667af9a698df56c607027adfd99f51cd1778
69ddd93d2c58bb9e52021bfd0c920784e805894c32d510c38305478a0e30e8e4
3253584a90074209e0ee35fb8edc1b14f21a928b7bc0152b9a195909e78efe38
c2de4b3a8903db35c4d12d18adac7acb154e610d6582474c6636b6b633034c3e
73573ba92eced266cecb75204072285a064098bd6ebc4dab13a9a8b44e6b3768
b36fbc5ba7eadc4359a3b9419c0a6360e14106b839ee0130247faa5a2bb2ecf
bca2371871c73e73b05e673f7fde0dc7d2003b88ca93a9d0e1c86f1bcb266ad6
```



Cada clave privada tiene una clave pública correspondiente



Open Source JavaScript Client-Side Bitcoin Wallet Generator

Single Wallet

Paper Wallet

Bulk Wallet

Brain Wallet

Vanity Wallet

Split Wallet

Wallet Details

Generate New Address

Print

Bitcoin Address

Private Key (Wallet Import Format)



SHARE

SECRET



1BUo3pVrFtFMqEz9Uy5UUXoDAYYL46fj2h

5KQiTLEyCs3DP8xLgAG4X1U293ttvSzbPGgLtycwMR27BHmkEa



La innovación es posible gracias a una nueva tecnología de contabilidad llamada Blockchain

Banco Tradicional	Bitcoin
Número de cuenta bancaria	Dirección Bitcoin
Ejemplo de cuenta: 012345678	Ejemplo de dirección Bitcoin: 1BUo3pVrFtfMqEz9Uy5UUXoDAYYL46fj2h
Acceso con contraseña/PIN	Accedido con clave privada
Ejemplo de PIN: 1234	Ejemplo de clave privada: 5JtQrdBfgDx4btMBmiTZcrSQqBourYH8p1o PFvbWyU79EvATiJF
Libro de cuentas bancarias = Centralizado	Blockchain=Decentralizado
Libro de cuentas bancarias = Privado	Blockchain=Público
Liquidación=Administrador de confianza	Liquidación = Consenso



Las transacciones y los saldos se pueden consultar con Block Explorers

B BLOCKCHAIN info [Home](#) [Charts](#) [Stats](#) [Markets](#) [API](#) [Wallet](#)

Home Welcome to Blockchain

Height Age Transactions Total Sent Relayed By Size (kB)

 **Litecoin Block Explorer**

Search by address, block number or hash, transaction or public key hash, or chain name:

Search

Address or hash search requires at least the first 6 characters.

Currency

Litecoin

blockr
block reader

CoinDD

0.9753%

Bitcoin

Price

\$ 382.90

Bitstamp

Litecoin

Price

₿ 0.01009000

BTC-e

Digitalcoin

Price

₿ 0.00031900

Vircolex

Quark

Price

₿ 0.000019

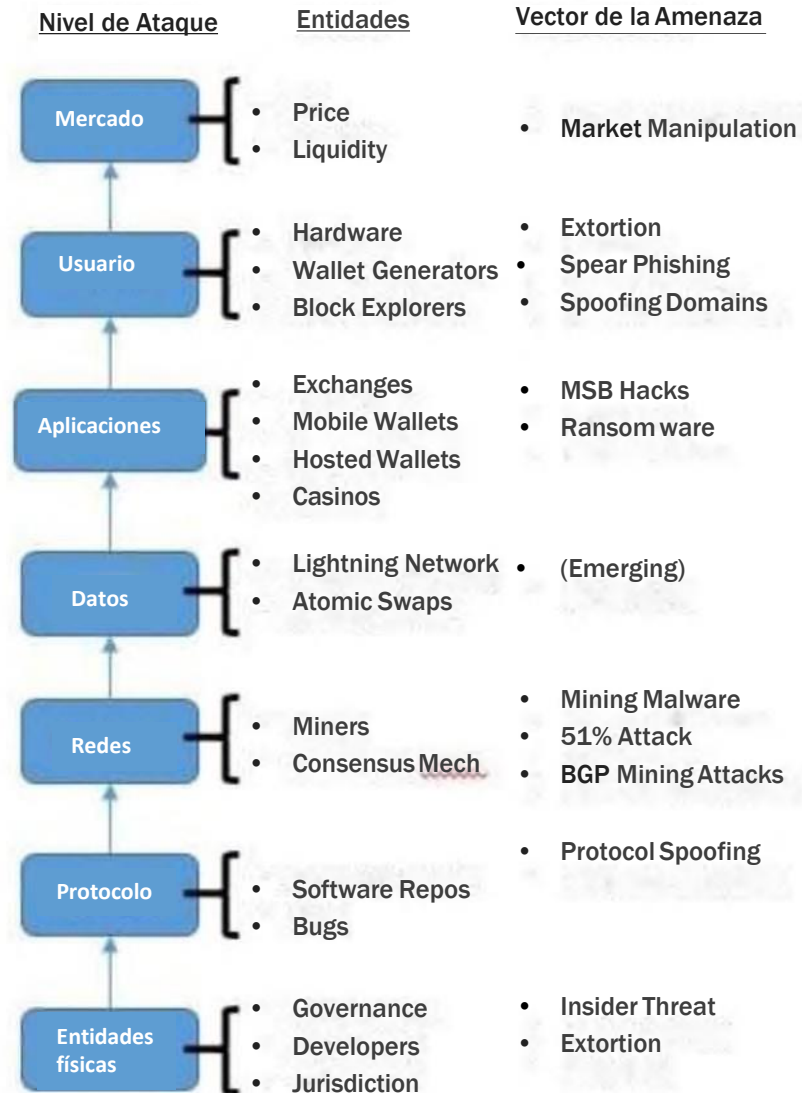


El libro abierto permite el estudio de las transacciones de una dirección conocida.

- Capacidad de determinar:
 - Cantidad almacenada en una dirección en particular
 - Direcciones Bitcoin asociadas
 - Fechas y horas de operaciones específicas
 - Conexiones a carteras sospechosas



Los participantes de la amenaza han intentado beneficiarse de atacar cada parte del ecosistema de las criptomonedas





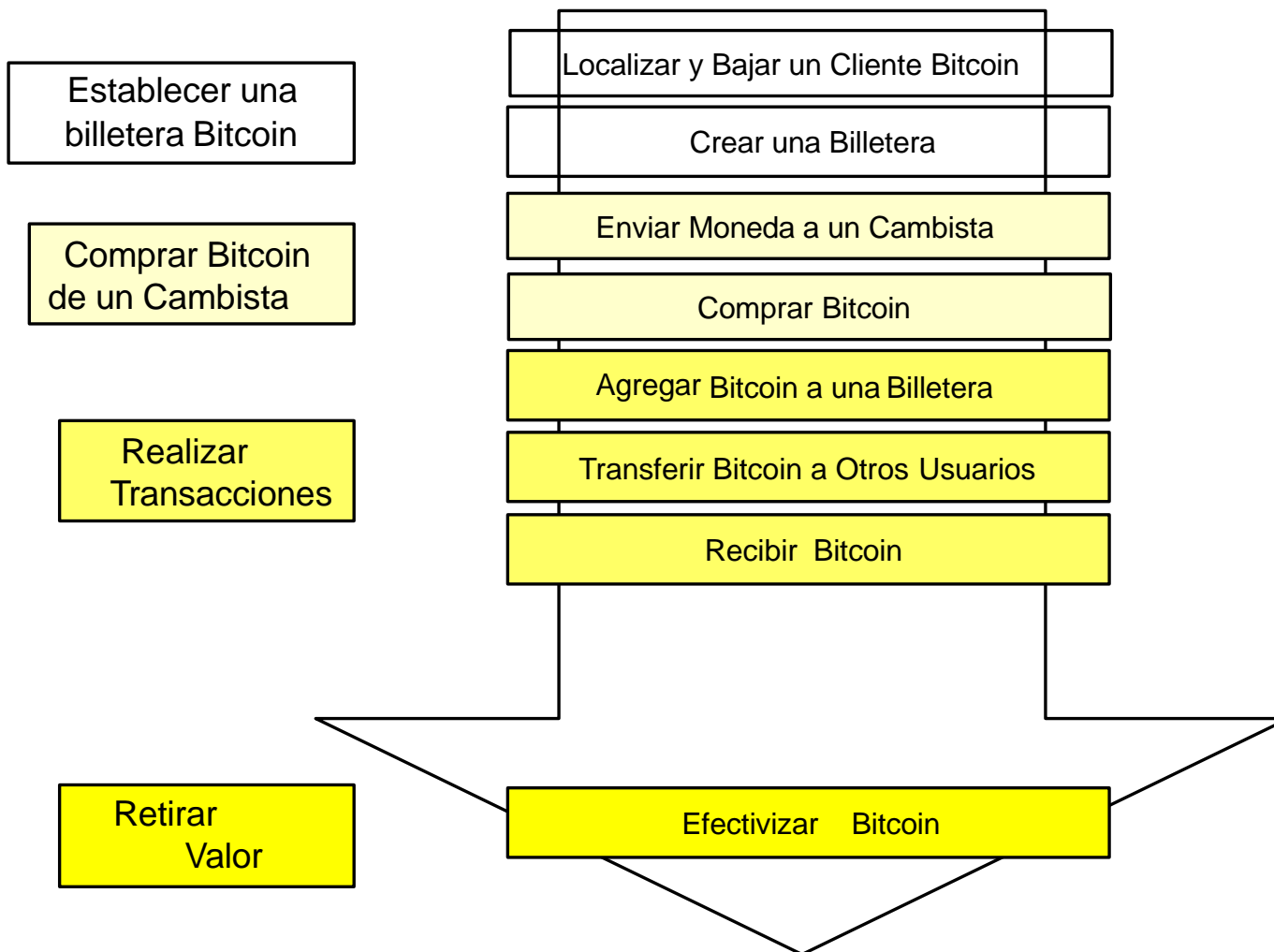
Entre las miles de Criptomonedas hay múltiples tipos con diferentes utilidades y tecnología

Tipos de criptomonedas

- Tradicional: Bitcoin, Litecoin, Dogecoin
- Monedas Pivot: Ripple, Stellar
- Con Anonimato Mejorado: Monero, Zcash
- Tokens DDNS: Namecoin, Emercoin
- Criptos DDNM: Syscoin, Cloakcoin
- Plataformas Blockchain: NXT, Ethereum, NEM
 - Dapps: 0x, DAO, Airlock
 - Tokens de Equidad/Seguridad:
 - Token Utilitario/AppCoin: Steemit, Storj, Filecoin
 - Stablecoins: Tether, DAI, Basecoin, Haven, Goldmint
- CBDCs? DBMs?



Múltiples pasos relacionados con el uso de Criptomoneda, con opciones en cada paso





Sólo se necesita una billetera para recibir Criptomoneda; viene en una variedad de formatos

Tipo de Billetera	Seguridad	Ubicación del Valor
Celular	Baja	Celular o Servidor
Navegador	Baja	PC
Cambios	Baja	Servidor
Software	Media	PC
Físico	Alta	En cualquier parte (papel)
Cerebro	Alta	Memoria





Hay muchas fuentes de Criptomonedas, cada una con su propio Proceso

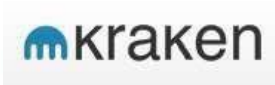
- Cambio Nacional



- Cajero Automático de Bitcoin



- Cambio Intenacional



- Financiero Intermediario



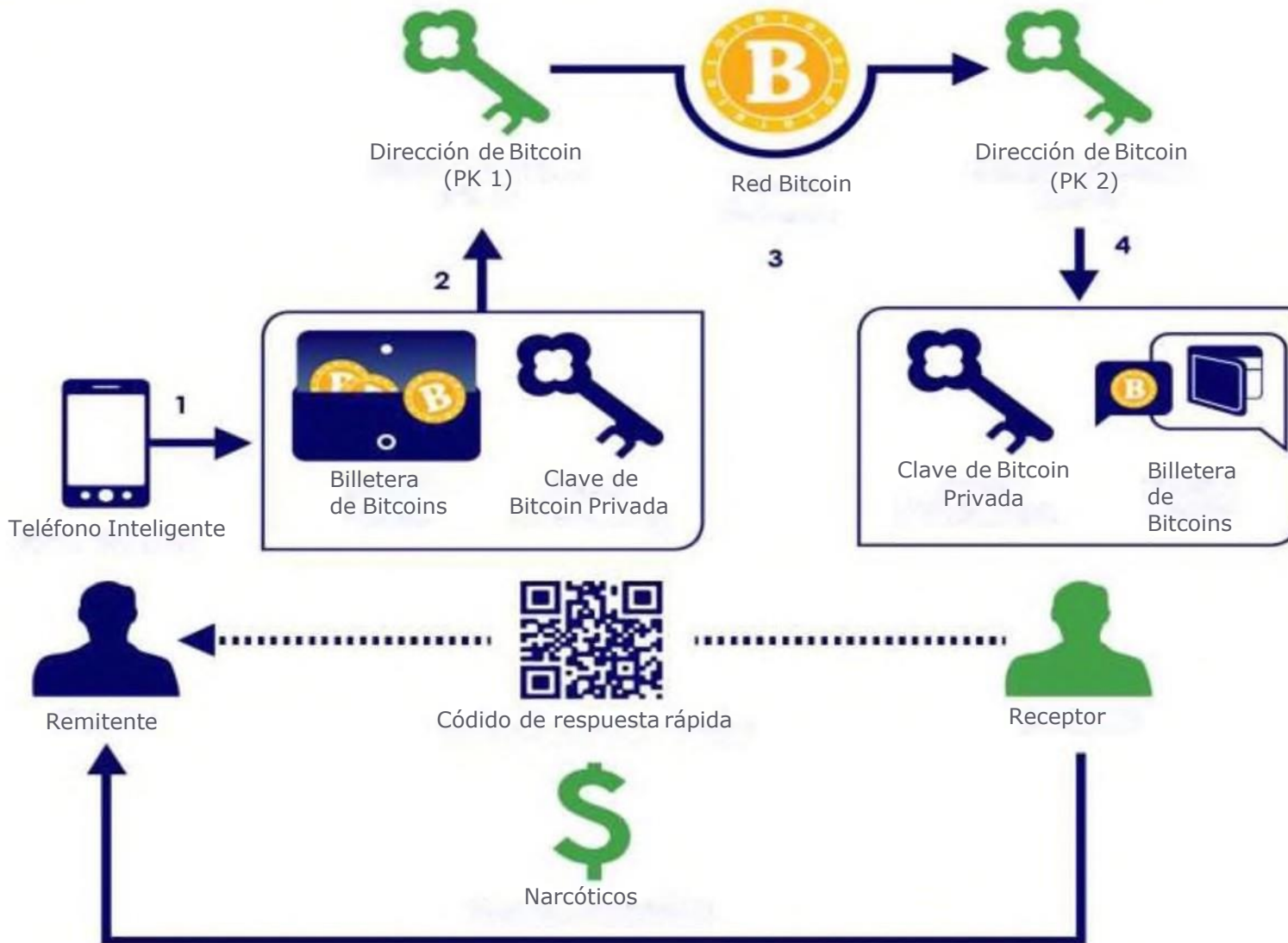
- Cambio P2P



- Mining (*minería*)



El P2P es un proceso simple, que necesita tan pocas cosas como una dirección y un teléfono.





El Anonimato No Está Garantizado, Depende de los Métodos y Entidades que Utilizan los Delincuentes.

- Uso de MSBs No Reguladas
 - Cambios P2P / Cajeros Automáticos
 - El intercambio físico rompe el rastro digital
 - Casinos en línea de propiedad opaca
- Uso de Mixers
- Capas de Cripto-Moneda
- Jurisdicción de Arbitraje
- Cripto-moneda de Anonimato Mejorado



Criptomoneda Forense

Indicadores de que un sujeto es usuario de Criptomoneda



Los Indicadores Forenses de Criptomoneda Pueden Ser Abiertos o Identificados a través de otra Inteligencia

- ¿Naturaleza del delito?
- Billeteras: Ordenador/Teléfono móvil/Otro
- Equipo de Mining
- OSINT: Foros/Medios Sociales/Donaciones
- Historial Web/E-mail/Chat
- Registros Bancarios



Análisis de Blockchain

Rastreo de Transacciones Dentro de las Criptomonedas



Fuentes, registros y documentación existentes para entidades de moneda virtual

- Cambistas, bancos y MSBs
 - Registros KYC
 - ROS
- Blockchain
 - Historial de transacciones
- Direcciones Bitcoin, IP logins, emails, claves PGP

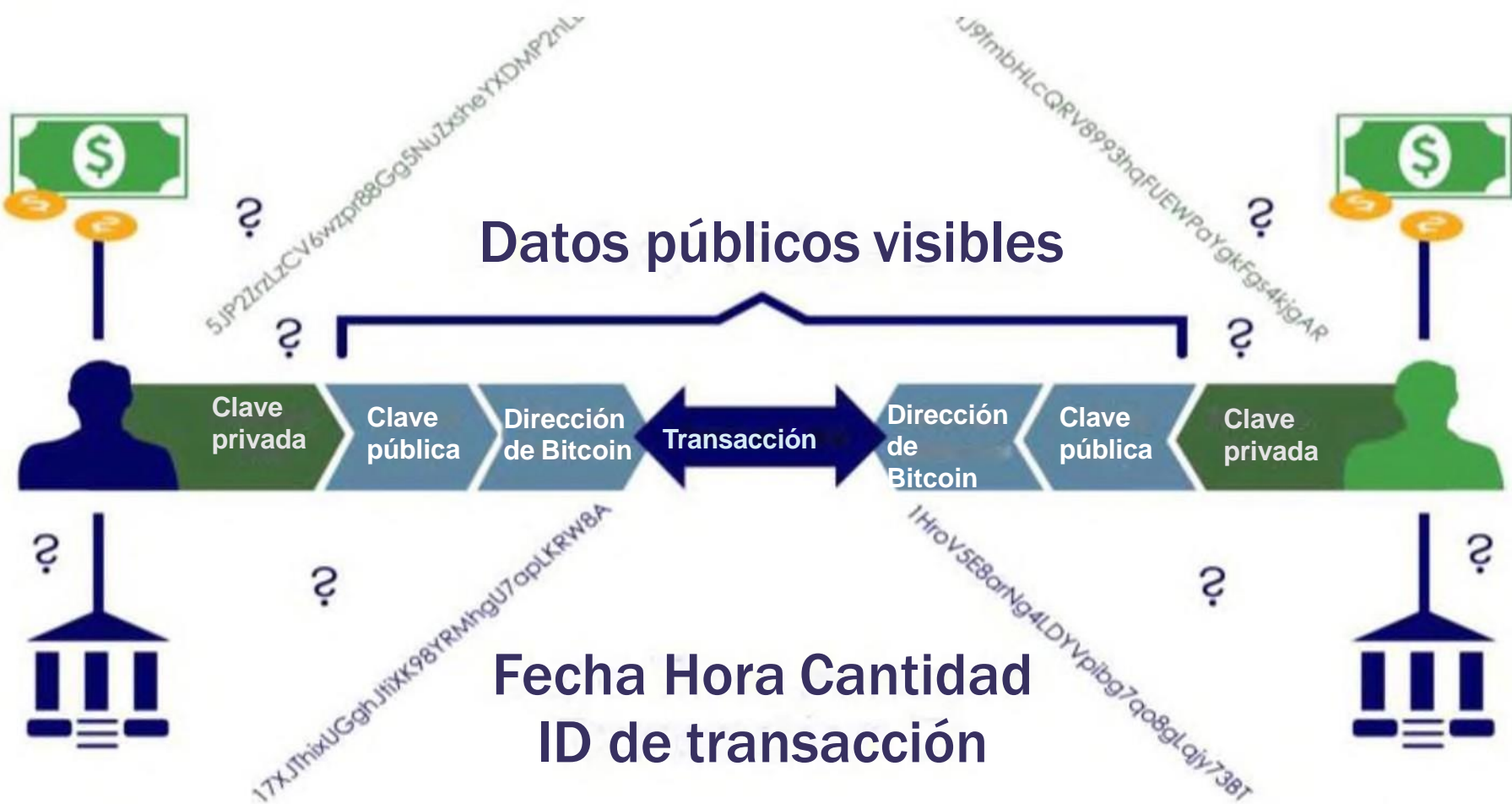


El libro abierto permite el estudio de las transacciones de una dirección conocida

- Permite Determinar:
 - Cantidad almacenada en una dirección en particular
 - Direcciones Bitcoin asociadas
 - Fechas y horas de operaciones específicas
 - Conexiones a billeteras conocidas



Este libro distribuido comparte el historial de transacciones con todos y utiliza el consenso para determinar la validez de las transacciones.





Una Variedad de Fuentes Abiertas y Comerciales Disponibles para Acceder y Analizar los Registros de Blockchains

- Navegadores Blockchain
 - WalletExplorer.com
 - Blockchain.info
- APIs
 - Blockcypher
- Utilidades Gráficas
 - ABE
- Servicios Comerciales Tercerizados
 - Chainalysis
 - Elliptic
 - Blockchain Intelligence Group
 - Bitfury Crystal
 - Neutrino



Estudio de Casos

Casos Prácticos de Análisis de Blockchain



El sitio web del Foro Público revela supuestas direcciones relacionadas con sitios web de extremistas

The screenshot shows a Reddit post on the r/bitcoin subreddit. The post title is "Active Bitcoin addresses for ISIS" and it was submitted 20 days ago by a user named "captained". The post content describes how the author discovered Bitcoin donation addresses on the website of ISIS (http://khilafah.is) and scraped them. The author mentions finding 700 unique Bitcoin addresses, but only 3 had seen any transactions. These addresses are redacted with blue boxes. The author also mentions that they posted this from a fresh alt account because of ISIS. The post includes an edit where the author clarifies that they are not trying to discredit Bitcoin and that they are a huge supporter of it. The post has 10 comments and 8 points (59% upvoted). The top comment is also redacted with a blue box. The comment text says "amazing that one bored programmer can do the work of financial investigation that would take a team of 12 federal agents and half a million dollars. Can we get some love for the blockchain?" and is marked as a permalink.

Active Bitcoin addresses for ISIS (self.Bitcoin)
submitted 20 days ago by captained

Browsing through <http://khilafah.is> (now defunct), the website of ISIS, I noticed that they accepted Bitcoin donations. Thinking that they had a finite pool of addresses, I decided to scrape their site and see if I could exhaust their pool.

The bitcoin donations page was located on a subdomain: <http://fisabilillah.khilafah.is/>. It contained minimal HTML, so scraping it was easy.

So I wrote a simple scraper and left it running for a few hours until I had drained their pool.

In total, I found 700 unique bitcoin addresses. But only 3 of them had seen any transactions. They are

[Redacted]

Figured someone here might be bothered to look into the blockchain and follow the transactions.

Posted this from a fresh alt because ISIS.

EDIT: Apparently I have to say this, but I am not trying to discredit Bitcoin by connecting it with ISIS. Bitcoin is an awesome technology, which I have actively followed since almost from the beginning. I am a huge supporter of Bitcoin, I run a business which accepts Bitcoin and I think Bitcoin is nothing but good news. Of course, some "bad people" might use the technology, which cannot be avoided (nor should it be, it should be available for everyone). The blockchain makes all transactions public and I thought that somebody might be interested in hunting coins connected to ISIS.

10 comments share

[Redacted]

amazing that one bored programmer can do the work of financial investigation that would take a team of 12 federal agents and half a million dollars. Can we get some love for the blockchain?

permalink

Search

This post was submitted on 14 Oct 2014
8 points (59% upvoted)
url: <http://redd.it/2j8ndg>

username password
remember me reset password login

Use Gyft to shop with Bitcoin at 200+ retailers. SHOP NOW

Submit a new link
Submit a new text post

Bitcoin

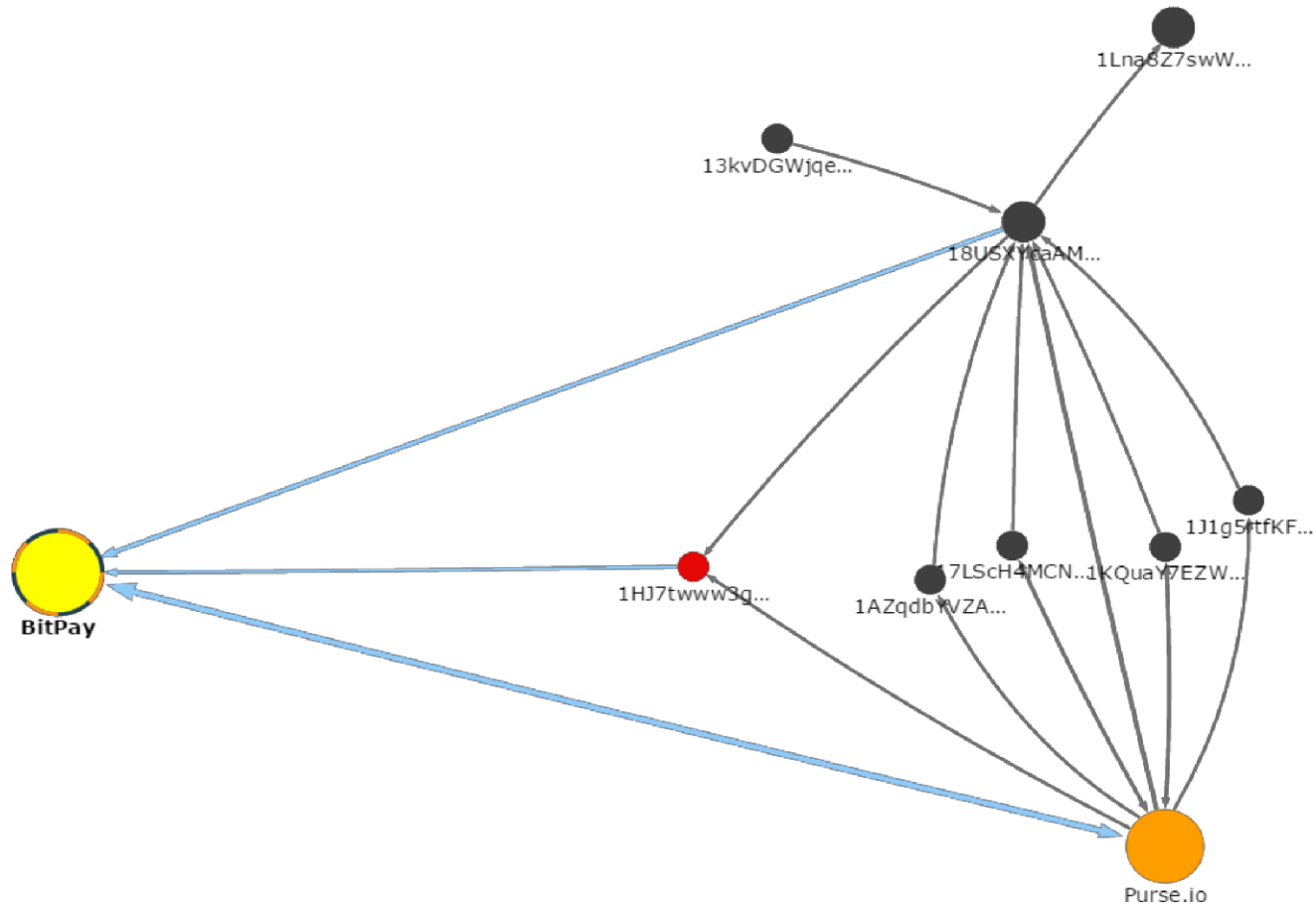
139,530 readers
688 users here now

Bitcoin is the currency of the Internet: a distributed, worldwide, decentralized digital money. Unlike traditional currencies such as dollars, bitcoins are issued and managed without any central authority whatsoever: there is no government, company, or bank in charge of Bitcoin. As such, it is more resistant to wild inflation and corrupt banks. With Bitcoin, you can be your own bank.



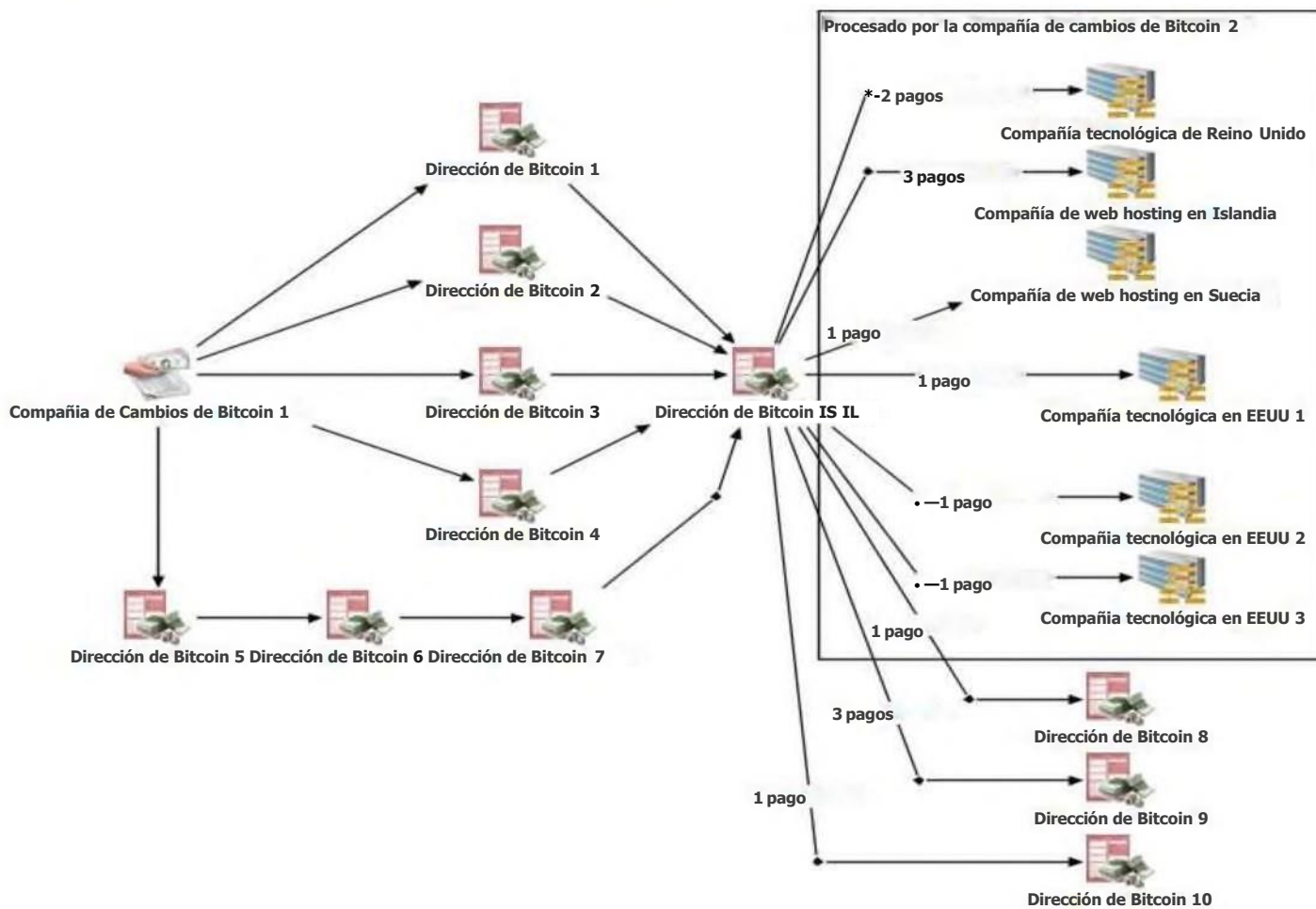
Análisis de la cadena Blockchain de presuntos extremistas - Direcciones asociadas

Rastrear los Intercambios Regulados Practicando la debida diligencia



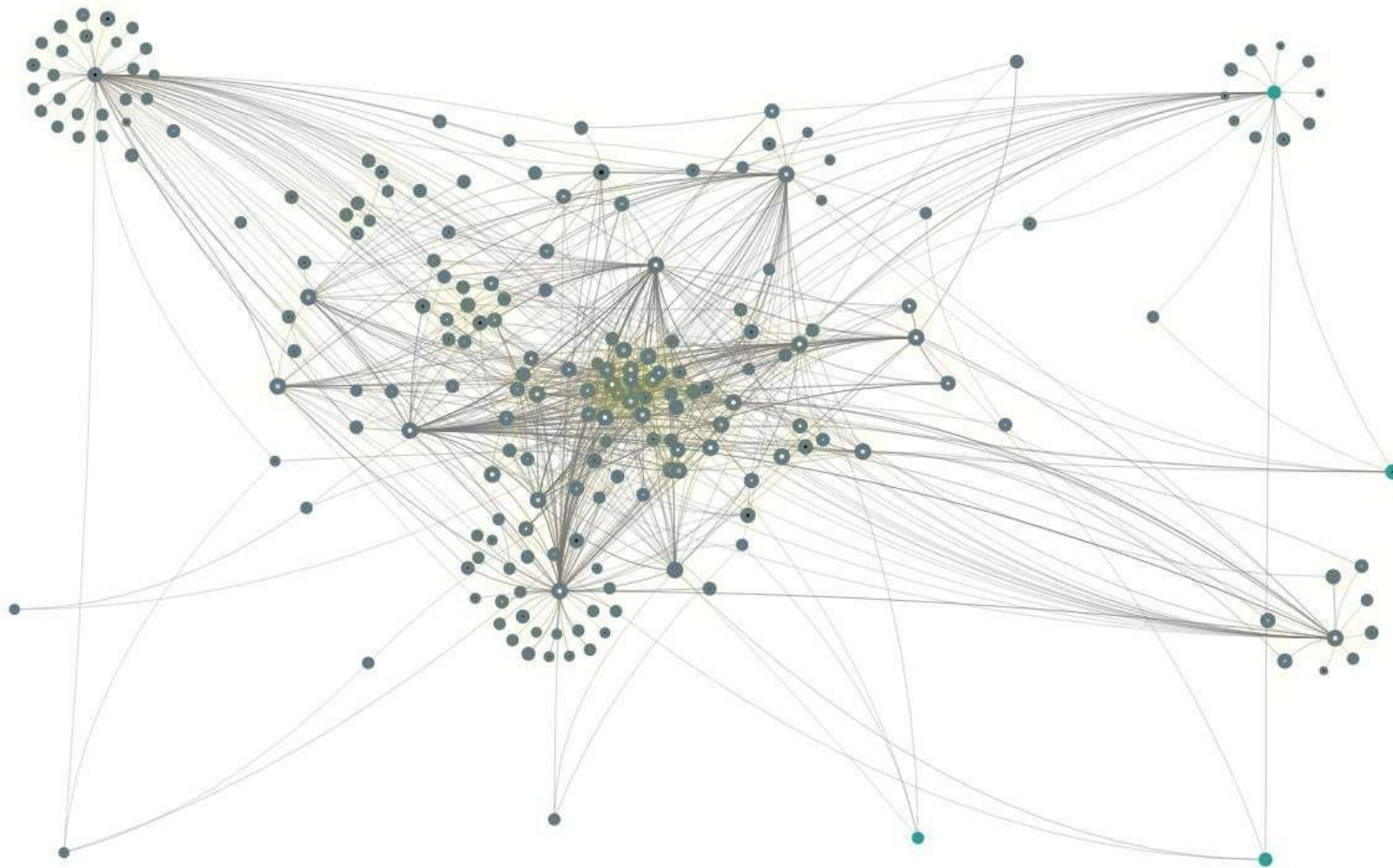


La entidad regulada también observó esta actividad en los informes abiertos y la vincula a su institución





Las herramientas pueden ser utilizadas para el análisis estratégico: ID realiza análisis de direcciones asociadas con Ransomware





¿Preguntas?

Sean Evans

FinCEN Inteligencia, Tecnología Cibernética y Emergente

Sean.evans@fincen.gov