GUÍA DE ACTUACIÓN

CRIPTOACTIVOS

PERSECUCIÓN PATRIMONIAL

MINISTERIO PÚBLICO FEDERAL

GUÍA DE ACTUACIÓN

CRIPTOACTIVOS

PERSECUCIÓN PATRIMONIAL

MINISTERIO PÚBLICO FEDERAL

MINISTERIO PÚBLICO FEDERAL
2ªCÁMARA DE COORDINACIÓN Y REVISIÓN

GUÍA DE ACTUACIÓN
CRIPTOACTIVOS
PERSECUCIÓN PATRIMONIAL

Brasilia - MPF 2023

Disponible en:
<http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes>

Cámara Criminal
Miembros titulares
Carlos Frederico Santos
Coordinador
Fiscal General Adjunto de la República

Luiza Cristina Fonseca Frischeisen
Fiscal General Adjunta de la República

Francisco de Assis Vieira Sanseverino
Fiscal General Adjunto de la República

Miembros suplentes
Paulo de Souza Queiroz
Fiscal General Adjunto de la República

Adriana de Farias Pereira
Fiscal Regional de la República

José Robalinho Cavalcanti
Fiscal Regional de la República

Coordinación y Organización
Grupo de Trabajo Criptoactivos
2ª CÁMARA DE COORDINACIÓN Y REVISIÓN

Alexandre Senra
Fiscal de la República en Espírito Santo

Anamara Osório Silva
Fiscal Regional de la República
Secretaria Adjunta de Cooperación Internacional/PGR

Eduardo El Hage
Fiscal de la República en Rio de Janeiro

Marisa Varotto Ferrari
Fiscal de la República en Rio de Janeiro

Thiago Augusto Bueno
Fiscal de la República en Amazonas

Tiago Misael de Jesus Martins
Fiscal de la República en Minas Gerais

Fiscalía General de la República
2ª Cámara de Coordinación y Revisión
SAF Sur, Quadra 4, Conjunto C
Teléfono (61) 3105-5100
70050-900 - Brasilia - DF
www.mpf.mp.br

ÍNDICE

INTRODUCCIÓN

Esta es la primera versión de la guía para la acción del Ministerio Público Federal sobre criptoactivos. El objetivo principal es que el miembro comprenda las discusiones, calificándolo para adoptar o no las propuestas de acción.

La guía está organizada en tres partes. La primera reúne información necesaria para comprender las discusiones y las orientaciones funcionales propuestas. La segunda presenta las discusiones y las orientaciones propiamente dichas. La última cuenta con modelos que pueden ser utilizados por los miembros del MPF en casos prácticos.

La comprensión de esta guía de acción prescinde de conocimiento previo sobre criptoactivos, siendo, en este sentido, una guía desde cero. Sin embargo, es una guía de acción, no un curso sobre criptoactivos o blockchain. Representa, por lo tanto, un recorte de lo que importa a la acción del MPF en esta materia. El mar de conocimiento con un palmo de profundidad, aquí, nada valdría. En cambio, la guía se adentra en lugares estratégicos, en la profundidad necesaria.

A lo largo del texto, especialmente en la primera parte, la guía utiliza definiciones operacionales útiles para las discusiones propuestas, sin pretensión de rigor científico. No encontramos forma más objetiva para cumplir la finalidad de esta guía.

Un ejemplo: criptoactivo fue definido como activo digital que no puede ser copiados. No se trata de ignorar la importancia de elementos como la criptografía y la tecnología Blockchain, sino de demostrar que no son necesarios para comprender el término "criptoactivo" en el contexto utilizado en esta guía.

La guía no es completa ni tiene la pretensión de serlo. Incluso dentro del primer recorte (lo que interesa a la acción del MPF), el tema es potencialmente inagotable. Se realizaron otros dos recortes posteriores: esta primera versión se limitó al subtema de la persecución patrimonial, que nos pareció el más urgente; y el enfoque es el Bitcoin, aunque gran parte de lo que se dice aquí es aplicable a muchos otros criptoactivos.

CRIPTOACTIVOS

Los criptoactivos son activos digitales que no pueden ser copiados. También son el designativo de un género.

A continuación, se examina cada una de estas proposiciones.

CRIPTOACTIVOS COMO ACTIVOS DIGITALES QUE NO PUEDEN SER COPIADOS

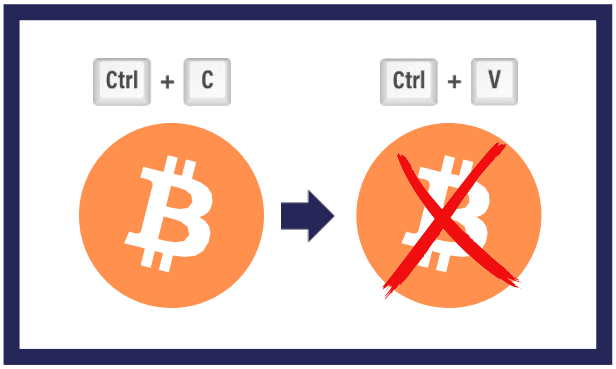
El 25 de mayo de 2022, desde mi computadora en Vitória/ES, envío el PDF de esta guía, aún en elaboración, a un colega del MPF. De esta simple acción surgen al menos tres copias más del PDF. El documento, que antes existía solo en mi computadora, ahora también existe en la carpeta "elementos enviados" de mi correo electrónico, en la carpeta "elementos recibidos" del correo electrónico de mi colega y en su computadora, una vez que descarga el archivo.

El mismo día y lugar, envío 0,1 bitcoin de mi cartera a otra cartera. Poco después, mi cartera tiene 0,1 bitcoin menos y la cartera de destino pasa a tener 0,1 bitcoin más.

Aunque utilicé el verbo "enviar" en ambas situaciones, las consecuencias del "envío" fueron completamente diferentes.

La primera situación involucró un objeto digital copiable, mientras que la segunda involucró un objeto digital que no puede ser copiado, es decir, un objeto digital escaso.

¿Y si en lugar de un documento en formato .pdf, hubiera enviado una fotografía o una película? Nos encontraríamos ante el mismo problema, consistente en la ausencia de escasez de estos medios, que, como bienes digitales, pueden ser copiados a un costo muy cercano a cero.



Es, por lo tanto, el atributo de la escasez el que particulariza a los criptoactivos y no el hecho de ser activos digitales. Juegos y programas de computadora, por ejemplo, también son activos digitales, pero pueden ser técnicamente copiados, como la piratería bien demuestra.

CRIPTOACTIVOS COMO EL DESIGNATIVO DE UN GÉNERO

Criptoactivo es sinónimo de token en sentido amplio y designa un género, compuesto por especies que pueden ser clasificadas a través de diversos criterios.

Veamos algunos de ellos.

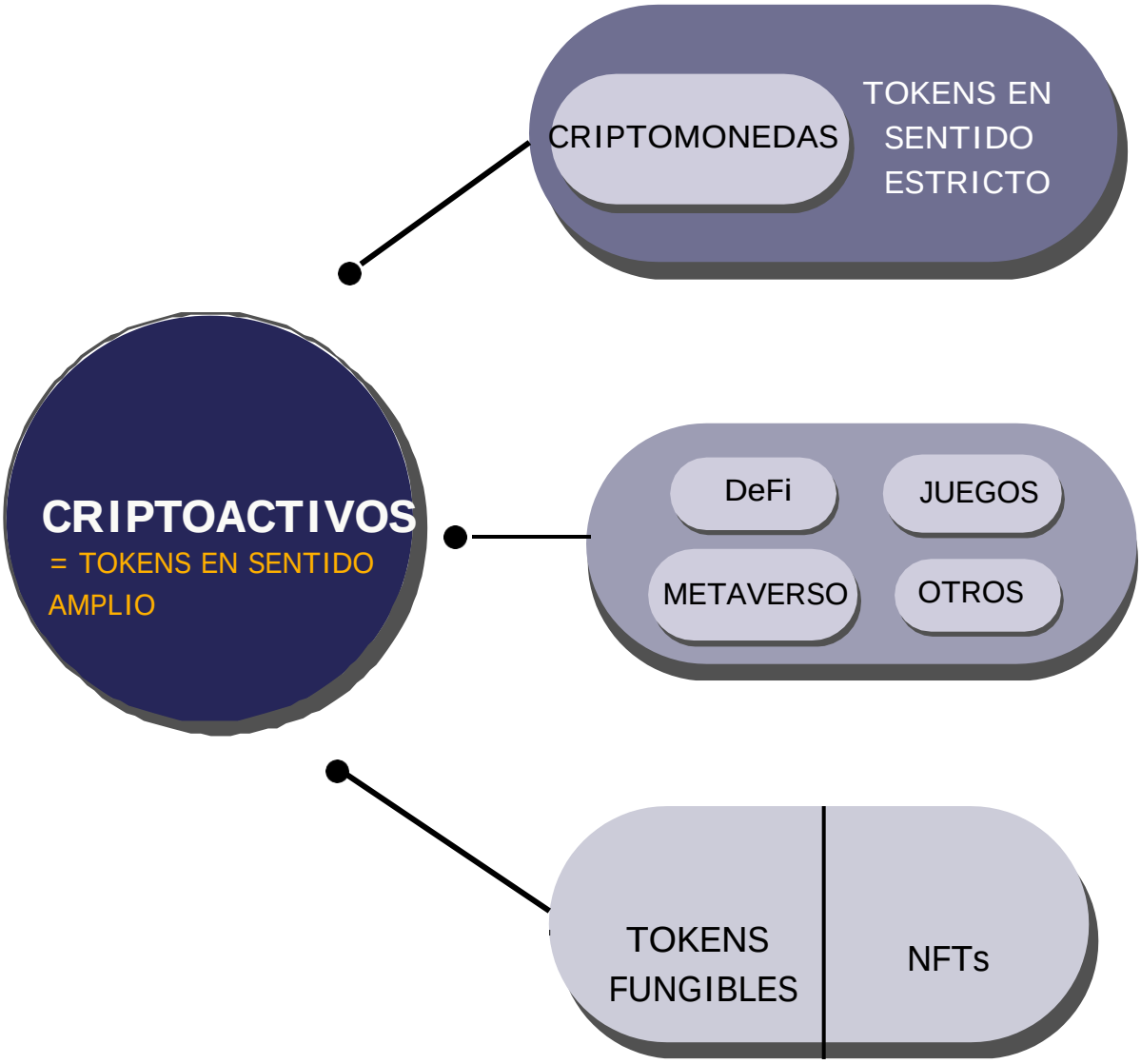
(a) Según sirvan o no para el pago de las tasas de uso de una Blockchain: criptomonedas y otros tokens.

(b) Según la finalidad de la aplicación a la que se vinculan: tokens de DeFi, de juegos, de metaversos, etc.

(c) De acuerdo con la fungibilidad: tokens fungibles y NFTs.

Evidentemente, algunas correlaciones pueden trazarse entre estas clasificaciones. Por ejemplo: todas las criptomonedas son tokens fungibles; los metaversos se estructuran generalmente sobre tokens fungibles y sobre NFTs. Pero hacerlo en este momento causaría una confusión innecesaria.

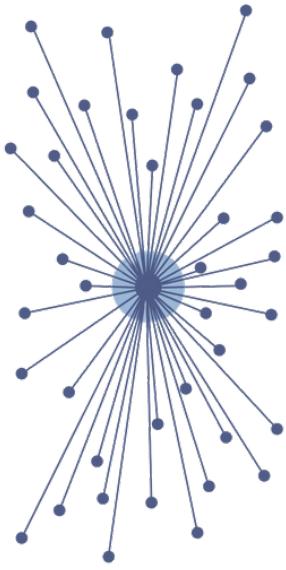
Las especies que interesan a esta guía serán tratadas adecuadamente más adelante.



BLOCKCHAIN

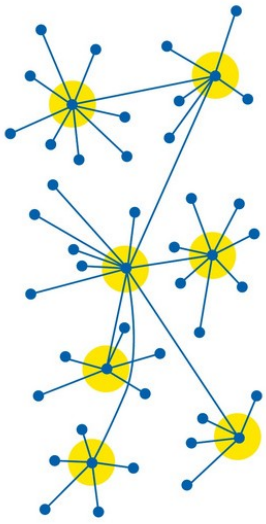
Blockchain es la principal especie del género "tecnologías de registro distribuido”.

La información puede registrarse de forma centralizada en un solo punto de la red, también llamado proveedor, en oposición a los demás puntos de esa red, llamados usuarios. O bien, puede registrarse de manera descentralizada entre varios puntos de la red, que ahora pasan a ser llamados nodos.



Proveedor

Usuario



Nodos

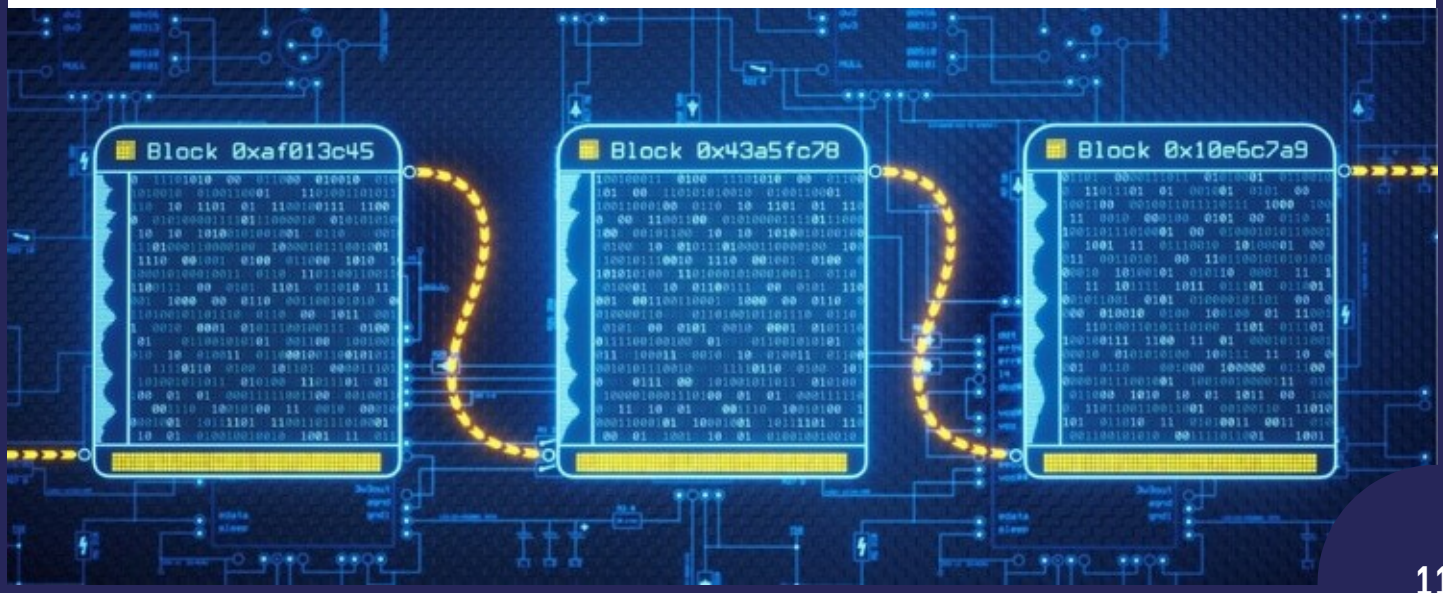
Cada manera de hacerlo presenta sus ventajas y desventajas.

Los registros centralizados son extremadamente baratos y rápidos, pero dependen de la confianza en la autoridad responsable de ese registro. Los registros descentralizados o distribuidos, a su vez, son comparativamente más caros y lentos de realizar, pero no requieren la exigencia de confianza en cualquier autoridad.

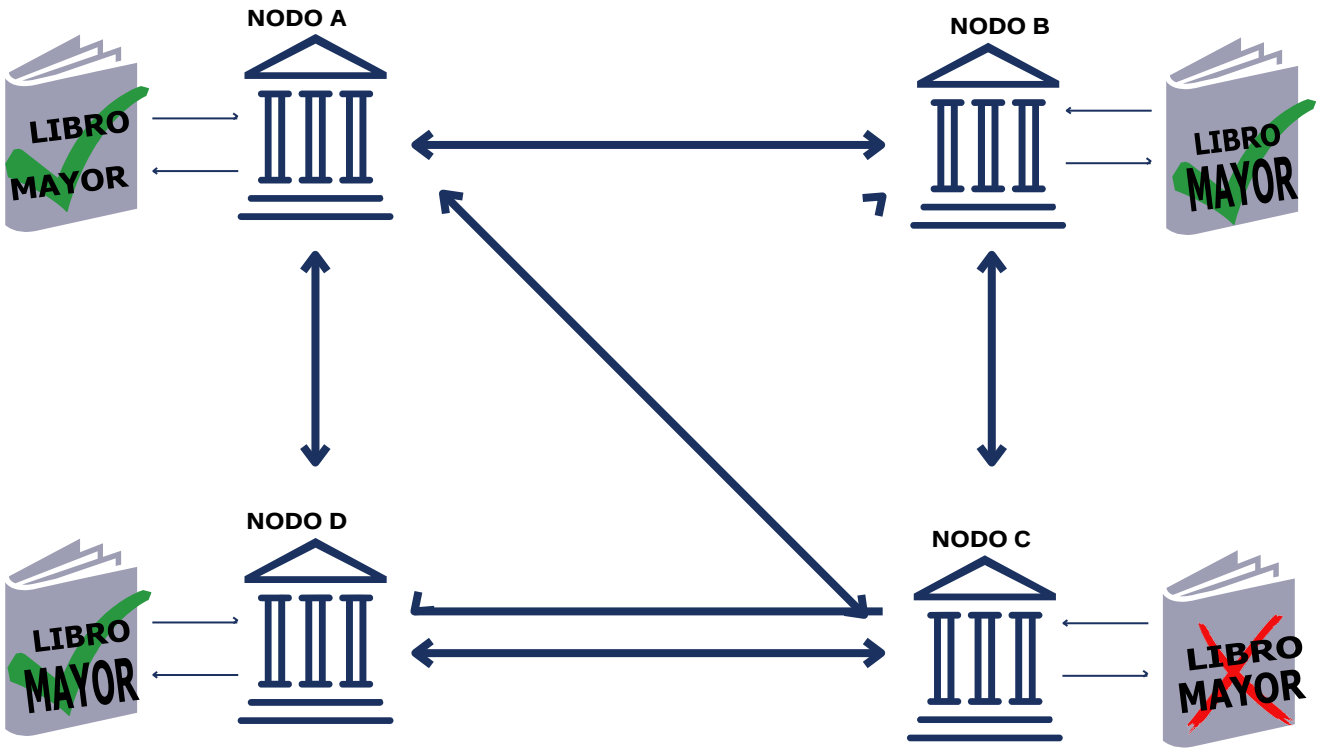
Un ejemplo: las transacciones entre cuentas de una misma exchange de criptoactivos son rápidas y baratas, pero su veracidad requiere que confiemos en esa exchange, responsable del registro centralizado de la información. Las transacciones realizadas entre direcciones de Bitcoin son más caras y lentas, pero no requieren que confiemos en ninguna autoridad, ya que no existe una autoridad responsable del registro, que se mantiene de forma distribuida entre los diversos nodos de la red.

Solo una de las repercusiones prácticas de esta diferencia: un registro centralizado puede ser adulterado por la autoridad responsable del mismo; un registro distribuido no puede ser adulterado por nadie.

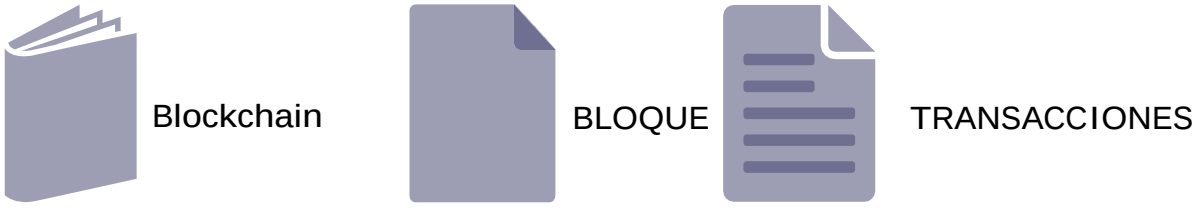
Blockchain es un tipo de registro distribuido, compuesto por bloques de datos ordenados cronológicamente, donde cada bloque se conecta inmediatamente al anterior y confirma, a través de pruebas matemáticas, las transacciones contenidas en todos los bloques anteriores.



Imagínese el Blockchain como un libro mayor (ledger) presente en diversas ubicaciones alrededor del mundo. No son copias hechas a partir de un mismo original, sino ubicaciones de igual importancia y originalidad, sincronizadas entre sí, donde cualquier alteración indebida realizada en una de estas ubicaciones es fácilmente detectada y rápidamente rechazada por las demás.



Continuando con la metáfora del libro mayor distribuido, imagine que este libro va recibiendo nuevas hojas a lo largo del tiempo y que en cada hoja puede haber muchas o pocas líneas escritas. Las hojas corresponden a los bloques del Blockchain. Las frases corresponden a las transacciones de cada bloque.



En el caso de Bitcoin, desde que se extrajo su primer bloque (Bloque Cero) a las 16:15 (UTC-3) del 03/01/2009, se añade una nueva hoja cada diez minutos aproximadamente. En este momento, a las 15:00 del 06/10/2022, este libro ya cuenta con 757.395 hojas.[1]

1- El Bloque número 757,394 corresponde a la 757.395 hoja de nuestro libro porque el Bloque Cero corresponde a la primera hoja.

BITCOIN

El Bitcoin fue concebido para ser un sistema de pagos sin intermediarios.[2] Pero para comprender el tema, es más relevante saber que "Bitcoin" es una palabra ambigua.

Tres de sus significados, a pesar de estar íntimamente relacionados, deben ser discernidos: Bitcoin-hardware, Bitcoin-software y Bitcoin-criptoactivo.

Bitcoin-hardware es el nombre dado al conjunto de dispositivos físicos alrededor del mundo, responsables de la seguridad del Blockchain contra cualquier intento de fraude. Es la red de Bitcoin.

Bitcoin-software es el término utilizado para referirse al programa que se ejecuta en estos dispositivos físicos, que consta, en un recorte simplificado: del Blockchain, un generador aleatorio de pares de claves y un conjunto de reglas.

En una analogía, el bitcoin-hardware es como su computadora portátil, mientras que el bitcoin-software es como Windows o Linux que se ejecuta en ella. Del mismo modo que la computadora portátil y Windows no se confunden, el bitcoin-hardware y el bitcoin-software no deben ser confundidos.

2- http://bitcoin.org/files/bitcoin-paper/bitcoin_pt_br.pdf

Del Blockchain ya hablamos. El generador de pares de claves lo abordaremos más adelante. Hablaremos ahora de algunas de las reglas del protocolo Bitcoin, comenzando por la definición de lo que es el bitcoin-criptoactivo.

El Bitcoin-criptoactivo (BTC) es un activo digital escaso cuya primera finalidad es servir como pago que el software hace al hardware para funcionar y cuya segunda finalidad es servir como moneda para el pago de tarifas por quien quiera hacer uso de la red bitcoin.

Examinemos, brevemente, cada una de esas finalidades.

Primera finalidad: Nuevos bloques son agregados al Blockchain a través de un proceso comúnmente llamado "minería", que implica un elevado gasto de energía eléctrica y de potencia computacional. Se trata de una disputa, librada entre mineros, buscando una recompensa, consistente en los nuevos BTC emitidos y atribuidos, a cada nuevo bloque, a un minero ganador.

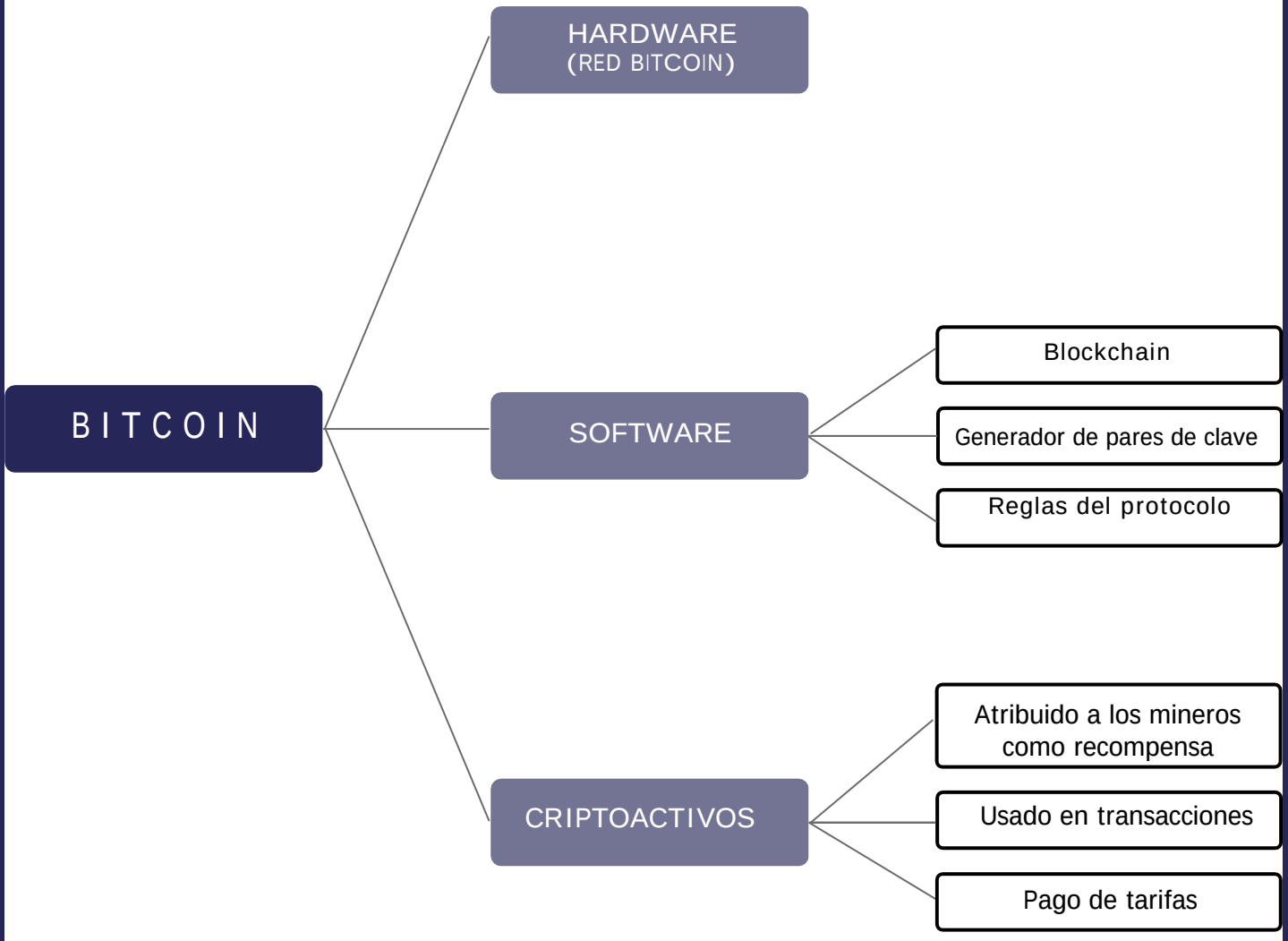
Segunda finalidad: Para enviar BTC a través de la red Bitcoin no es necesario ser un minero ni es necesario tener consigo una copia del Blockchain. Sin embargo, se debe pagar una pequeña tarifa de transacción, necesariamente en BTC.[3] Por eso, el BTC es una criptomoneda, porque desempeña, en este contexto, la función de una moneda.

Su emisión sigue algunas reglas del protocolo:

- está limitada a 21 millones;
- ocurre cada nuevo bloque minado;
- inicialmente era de 50 BTC por bloque y actualmente es de 6.25 BTC por bloque, teniendo en cuenta que se reduce a la mitad cada 210.000 nuevos bloques, en un proceso llamado halving.

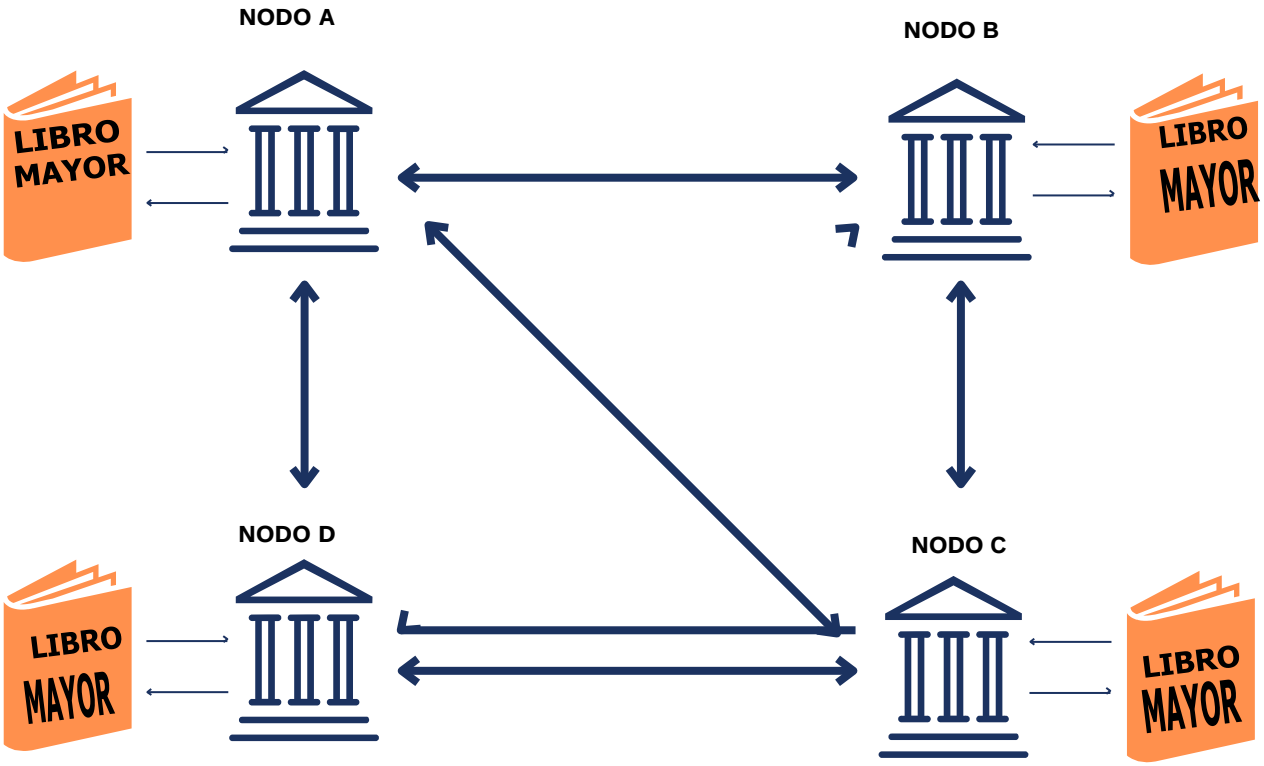
3- El valor de la tarifa de transacción no depende del valor de la transacción y sí de otros dos factores: del espacio que la transacción ocupa en el Blockchain y de la demanda por el uso de la red Bitcoin. Cuanto mayor sea el espacio ocupado por la transacción y cuanto mayor sea la demanda por el uso de la red, mayor será la tarifa a pagar.

1


BITCOIN
HARDWARE
(RED BITCOIN)
SOFTWARE
Blockchain
Generador de pares de clave
Reglas del protocolo
CRIPTOACTIVOS
Atribuido a los mineros como recompensa
Usado en transacciones
Pago de tarifas

¿DÓNDE SE ALMACENAN LOS CRIPTOACTIVOS?

Siendo bienes digitales, los criptoactivos no existen en el mundo físico. Desde la perspectiva del usuario, los criptoactivos pueden estar con él o con terceros. Desde la perspectiva técnica, los criptoactivos no están con nadie. Son registros en un libro mayor público y distribuido llamado Blockchain. O bien están en este libro o simplemente no existen.



Es importante no confundir los criptoactivos con los saldos en criptoactivos. Los criptoactivos están registrados en el Blockchain, mientras que los saldos en criptoactivos están registrados en una base de datos privada y centralizada, perteneciente, por ejemplo, a una exchange.

Un término comúnmente utilizado para hacer esta distinción es el de transacciones on-chain y transacciones off-chain. En el primer caso, no es necesario confiar en nadie más que en el proceso de seguridad del Blockchain. En el segundo caso, es necesario confiar en la persona responsable del registro centralizado.

Esto se debe a que, cuando un cliente abre una cuenta en una casa de cambio, las claves privadas de esa cuenta quedan en poder de la exchange, que se encarga de realizar las operaciones en nombre del cliente, en lugar de que el cliente tenga el control sobre ellas.

Para recibir depósitos en criptoactivos, la exchange asigna a cada cliente una dirección en el Blockchain. Después de que el criptoactivo es recibido en esa dirección de depósito individual del cliente, la exchange lo transfiere a direcciones más seguras de su propiedad (cold wallets).

En cuanto a los retiros en criptoactivos, la casa de cambio suele agrupar las solicitudes de retiro de varios clientes en una única transacción, que tiene como origen direcciones de la exchange similares a cuentas bancarias de giro, y como destino las direcciones proporcionadas por cada cliente en su solicitud.

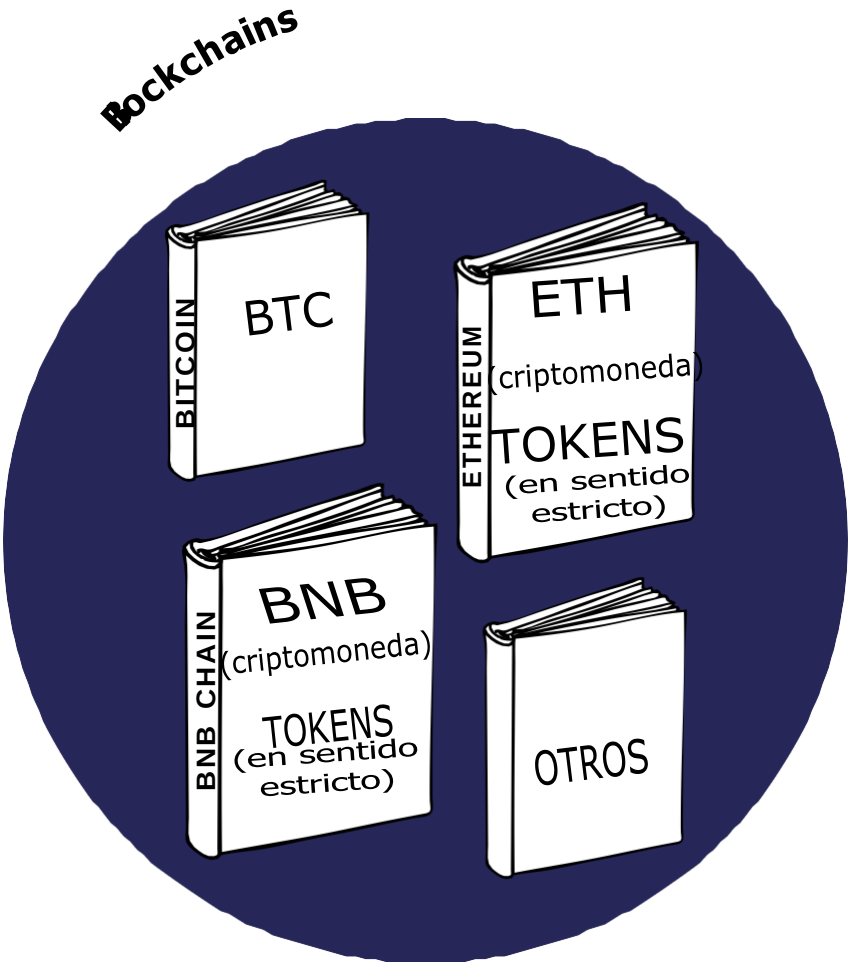
Las direcciones de retiro de la exchange deben tener suficientes criptoactivos para hacer viables los retiros solicitados por los clientes y no deben confundirse con las direcciones de depósito. Las direcciones de depósito son individuales para cada cliente, mientras que las direcciones de retiro son comunes.

Allí radica la razón por la cual, para identificar qué transacciones fueron realizadas por la exchange en nombre de un cliente específico, no es suficiente mirar el Blockchain. Es necesario también acceder a los datos y documentos de transacciones internos de la exchange, una especie de "libro mayor" de la empresa. Para este acceso, se recomienda el modelo de levantamiento de secreto de transacciones específicas que consta en el anexo a esta Guía (Esbozo de Levantamiento de Secreto Telemático de Operaciones con Criptoactivos en SIMBA).

Más allá de Bitcoin: Blockchains públicos y seudónimos

En un principio solo existía Bitcoin, un Blockchain con una única criptomoneda, el BTC, utilizada como medio de pago en la red. Hoy en día existen numerosos Blockchains mantenidos por diferentes redes.

Hay Blockchains que cuentan con múltiples criptomonedas transigibles, es decir, que pueden ser enviadas y recibidas. Sin embargo, en cada uno de ellos, se puede identificar su criptomoneda, es decir, el criptoactivo en el que se deben pagar las tarifas de la red.



		[4]	

Una excepción que vale la pena mencionar es el Blockchain de Monero, cuyo contenido no es accesible públicamente. Monero (XMR) es la criptomoneda de este Blockchain y el principal ejemplo de las llamadas "monedas de privacidad".[5]

Volviendo al examen de los Blockchains en general, a pesar de ser públicos, son seudónimos. Esto significa que, en general, con la simple visualización del libro no es posible saber quiénes son las personas involucradas en las transacciones de criptoactivos allí registradas.

La identificación que figura en el libro es a través de una dirección pública (algo similar a un número de cuenta), y no por nombre. En otras palabras, podemos consultar fácilmente todas las transacciones realizadas por ciertas cuentas, pero no podremos saber, solo por la lectura del libro, quiénes están detrás de ellas:

4 - Los criptoactivos homónimos pueden existir en más de un Blockchain. Por ejemplo, existe el USDT en el Blockchain de Ethereum y el USDT en BNB Chain.

5- Las monedas de privacidad no serán tratadas en detalle en esta primera versión de la guía.

Address

USD BTC

This address has transacted 2 times on the Bitcoin blockchain. It has received a total of 3.02625922 BTC ($58,013.78) and has sent a total of 3.02625922 BTC ($58,013.78). The current value of this address is 0.00000000 BTC ($0.00).

Address	bc1q84m06cqjj8xm77a9j72pz6245r6zzp35nu9dya
Format	BECH32 (P2WPKH)
Transactions	2
Total Received	3.02625922 BTC
Total Sent	3.02625922 BTC
Final Balance	0.00000000 BTC

Transactions

Fee 0.00037180 BTC
(165.982 sat/B - 65.343 sat/WU - 224 bytes)
(260.000 sat/vByte - 143 virtual bytes)

-3.02625922 BTC

1 Confirmations

Hash ec6fc328520989802fa264bba0f30cced23ca03ac3faf0...

2022-10-11 13:43

bc1q84m06cqjj8xm77a9j72pz6245r... 3.02625922 BTC

3KeDmvaCJeV64QCC3ynfXkzCMpS... 0.00201913 BTC
358JVUtKdhaTdfKRY8RaHXm4saA... 0.02386829 BTC

Fee 0.00036660 BTC
(165.135 sat/B - 65.348 sat/WU - 222 bytes)
(260.000 sat/vByte - 141 virtual bytes)

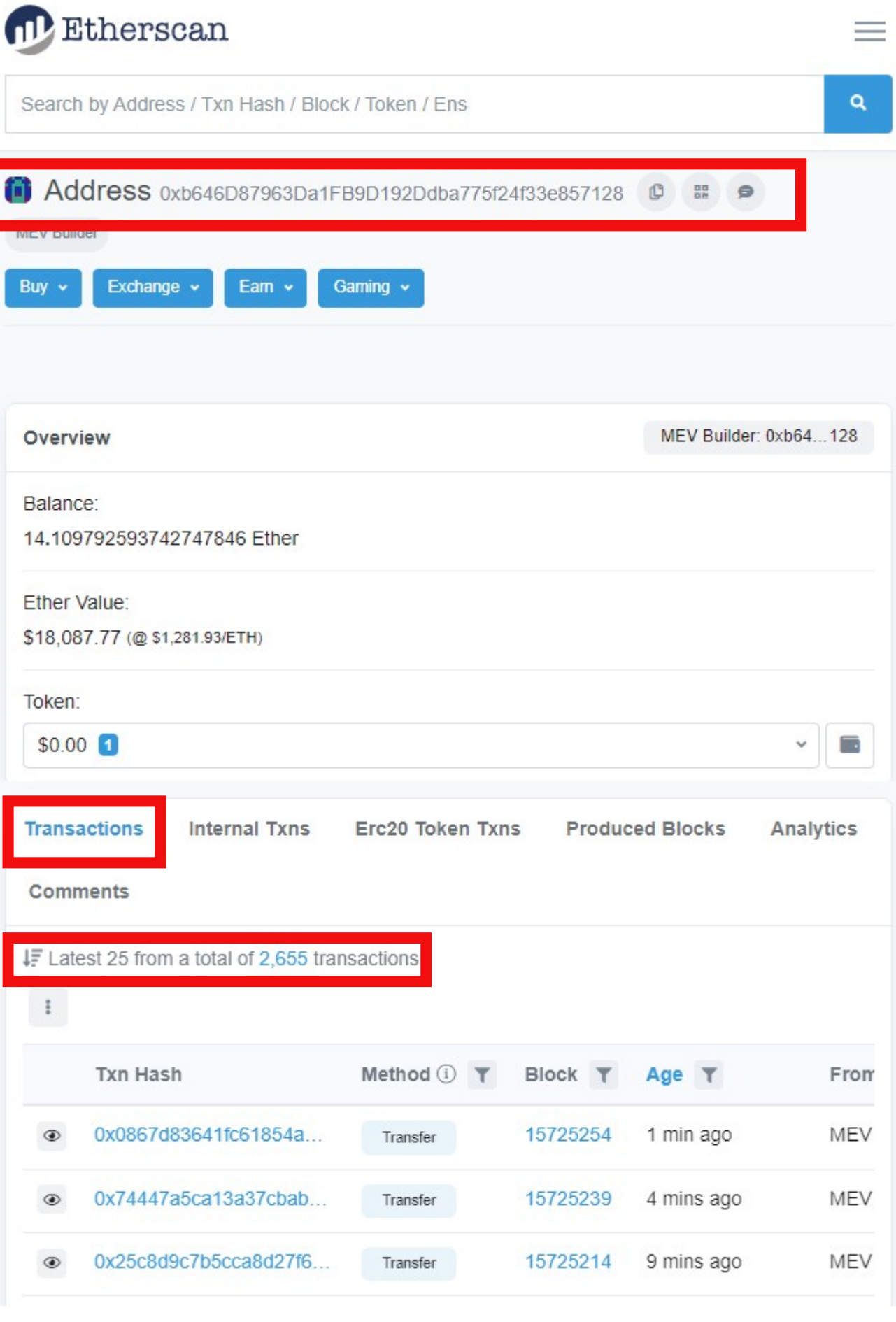
+3.02625922 BTC

Hash a045730dbc010368444ebb4df2aef11d063ee9035ffa3...

2022-10-11 13:06

bc1q5xutv5gr72t7f9cpjwea8rspx45... 3.10129645 BTC

bc1qxy08jgn8lm3kdpe2lh4zj9qgjs2... 0.07467063 BTC
bc1q84m06cqjj8xm77a9j72pz6245r... 0.02625922 BTC

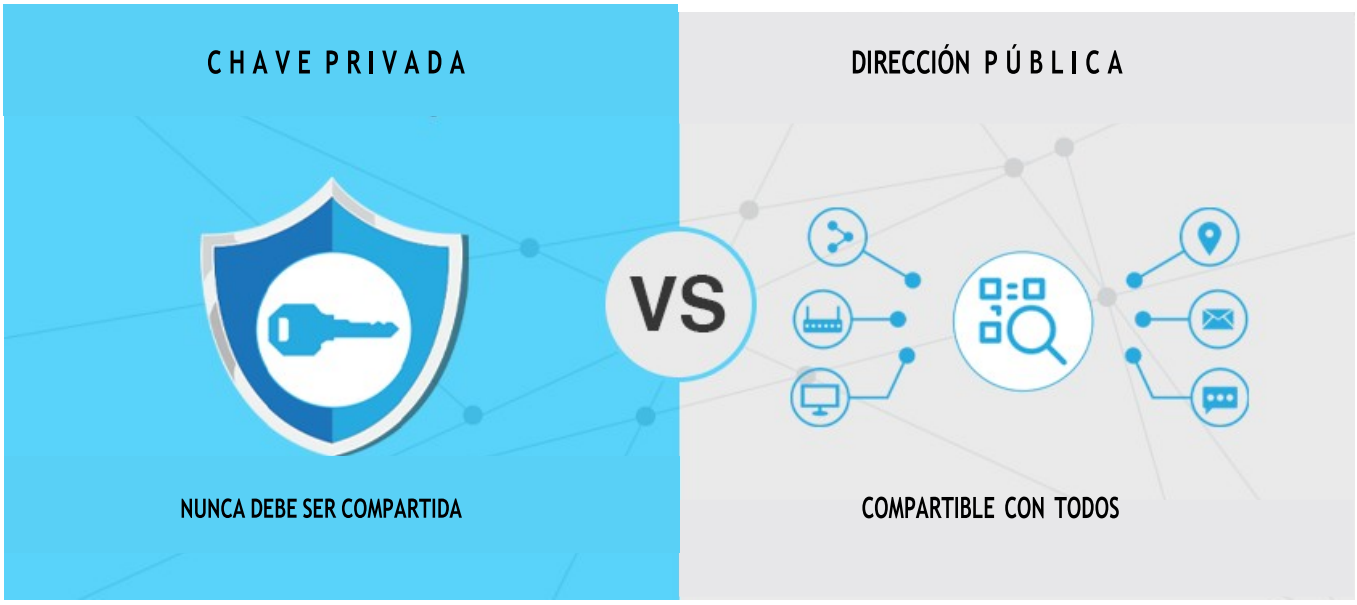

Etherscan
Search by Address / Txn Hash / Block / Token / Ens
Address 0xb646D87963Da1FB9D192Ddba775f24f33e857128
Buy
Exchange
Earn
Gaming
Overview
MEV Builder: 0xb64...128
Balance:
14.109792593742747846 Ether
Ether Value:
$18,087.77 (@ $1,281.93/ETH)
Token:
$0.00 1
Transactions
Internal Txns
Erc20 Token Txns
Produced Blocks
Analytics
Comments
Latest 25 from a total of 2,655 transactions
Txn Hash
Method
Block
Age
From
0x0867d83641fc61854a...
Transfer
15725254
1 min ago
MEV
0x74447a5ca13a37cbab...
Transfer
15725239
4 mins ago
MEV
0x25c8d9c7b5cca8d27f6...
Transfer
15725214
9 mins ago
MEV

ALMACENAMIENTO DE CRIPTOACTIVOS

El almacenamiento de criptoactivos implica poseer la clave privada que permite su movimiento.

Para continuar, hay dos términos que deben ser entendidos: clave privada y dirección pública, que forman un par, también llamado cuenta. Una cuenta de criptoactivos no es más que ese par.

La clave privada y la dirección pública mantienen una relación de correspondencia biunívoca. Es decir, para cada clave privada existe una única dirección pública y para cada dirección pública existe una única clave privada.



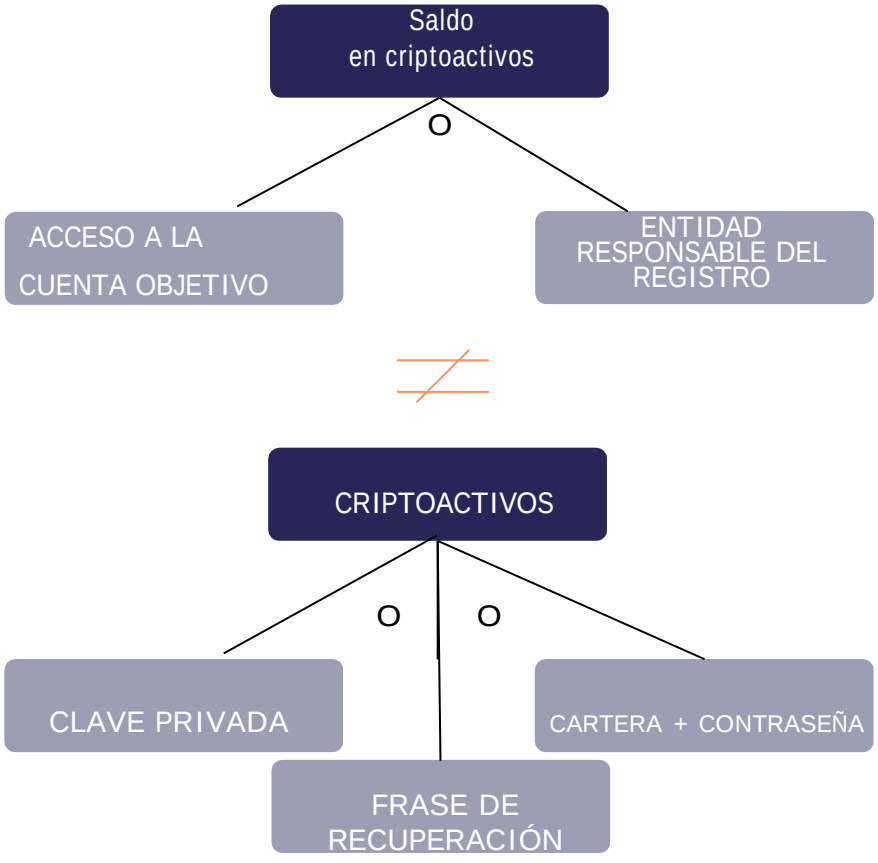
Piense en la clave privada como la llave de su casa y en la dirección pública como su dirección residencial. Considere también que esta clave privada tiene dos características particulares: solo ella abre una puerta que no puede ser forzada y es una llave que viene con su dirección escrita en ella.

De esto se derivan algunas consecuencias. Destaquemos dos de ellas. Compartir su dirección pública no presenta ningún riesgo de pérdida de criptoactivos, ya que la puerta no puede ser forzada (primera). Pero compartir su clave privada permitiría que cualquier persona entrara en su casa y tomaría todo lo que tenga valor allí, ya que con la clave se tiene acceso a la dirección (segunda).

MOVIMIENTO DE CRIPTOACTIVOS

Los saldos en criptoactivos, al igual que las constancias en registros privados centralizados, pueden ser movidos y bloqueados por cualquier persona que tenga acceso a la cuenta objetivo (login + contraseña + posibles factores de autenticación múltiple) o, más fácilmente, por la propia exchange o empresa responsable del registro.

Los criptoactivos, por otro lado, pueden ser movidos por quien tenga acceso a la clave privada de la cuenta correspondiente, la frase de recuperación de una cartera o la propia cartera más la contraseña de acceso a la misma.



Ya hemos hablado sobre la clave privada en el tema anterior. Ahora pasaremos a los conceptos de cartera, contraseña de acceso y frase de recuperación.

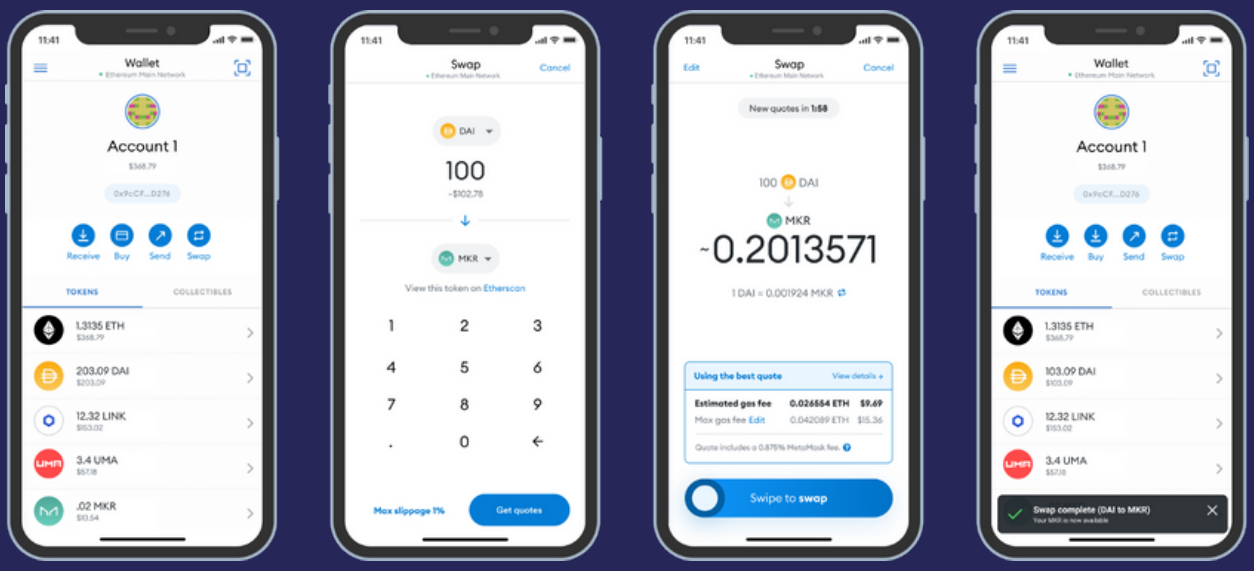
CARTERAS

Las carteras de criptoactivos no son como las carteras de dinero. Las carteras de dinero almacenan dinero. Las carteras de criptoactivos no almacenan criptoactivos, sino las claves privadas que permiten su movimiento.

Cartera, en este contexto, también es un término ambiguo y tres significados nos importarán:

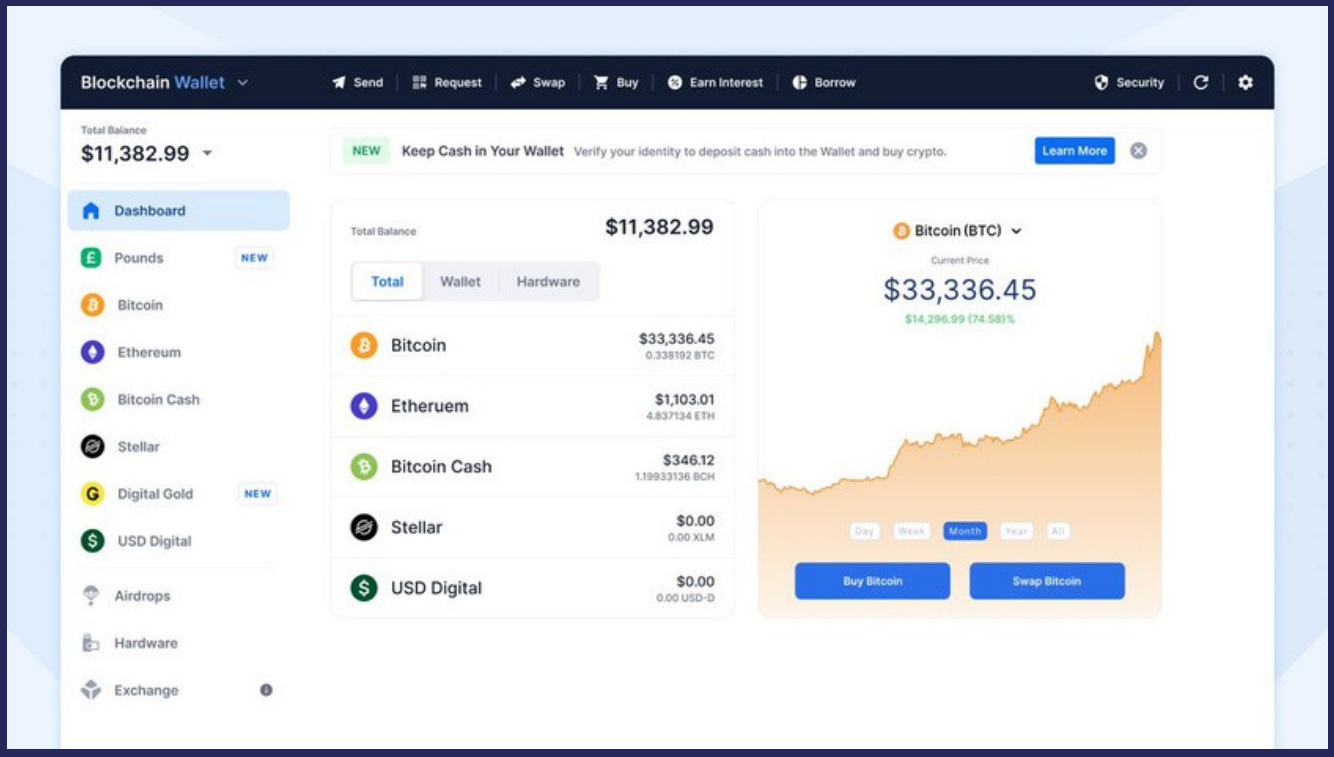
- Cartera como el nombre dado a un pedazo de papel (paper wallet), donde se encuentran anotados los datos de una cuenta (clave privada y dirección pública);
- Cartera como el designativo de un dispositivo físico específicamente creado para la custodia de claves privadas (hardware wallet); y
- Cartera como el nombre dado a un software que ayuda al usuario en la protección de sus claves privadas y que puede ser ejecutado en línea (webwallet), estar instalado en la computadora (desktop wallet) o en el celular (mobile wallet).

HARDWARE WALLET (TREZOR Y LEDGER)

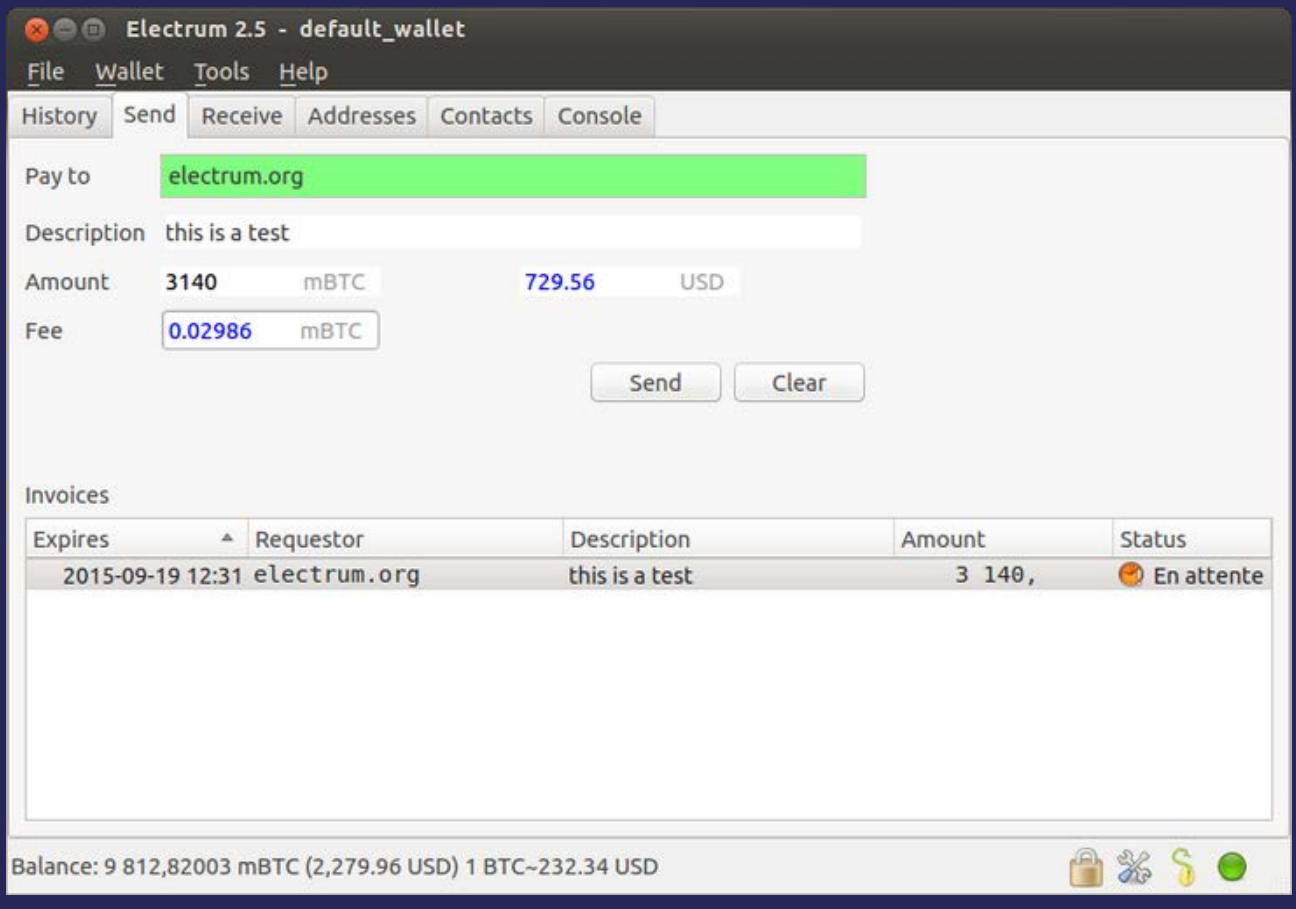


MOBILE WALLET

PAPER WALLET



WEB WALLET



DESKTOP WALLET

Las carteras de papel y las webwallets tienen contraindicaciones importantes. Las primeras porque solo serán seguras si son creadas y manejadas por alguien con conocimiento técnico profundo en el tema. Las segundas porque almacenan las claves privadas en la nube, aumentando el riesgo de acceso no autorizado a ellas.

Las demás carteras se diferencian básicamente por el lugar donde se almacenan las claves privadas. En la hardware wallet las claves privadas están en un dispositivo físico específico[6]. En la desktop wallet, en la computadora. Y en la mobile wallet, en el celular.

Contraseña de acceso (PIN)

Si su cartera de dinero fuera robada, seguramente perdería el dinero que allí estuviera guardado. Sin embargo, si su cartera de criptoactivos o el dispositivo donde está instalada fuera robado, no perdería sus criptoactivos, a menos que el criminal supiera su contraseña o pudiera violarla.

Esto ocurre porque, para evitar accesos no autorizados, las carteras de criptoactivos almacenan las claves privadas de forma cifrada. Lo que permite que sean descifradas es la contraseña creada por el usuario, también conocida como PIN (número de identificación personal).

En términos prácticos, para la movilización de los criptoactivos de una cuenta:

- Quien tiene la clave privada descifrada, no necesita la contraseña;

6- En uso y funcionamiento adecuados, las carteras de hardware son el tipo más seguro de cartera por dos razones. En primer lugar, porque no permiten que las claves almacenadas toquen cualquier entorno en línea. En segundo lugar, porque exigen el accionamiento físico de un botón cada vez que el usuario pretende realizar una transacción.

- quien tiene la clave privada encriptada, necesita la contraseña;

- quien tiene solo la contraseña, no tiene nada.

Frase de recuperación (seed phrase)

Normalmente, una sola cartera comprende varias cuentas (tres, ocho, veinte ...) [7] y cada vez que el usuario utiliza una nueva cuenta, se vuelve más complejo hacer una copia de seguridad de sus respectivas claves privadas.

Para superar esta dificultad, las carteras utilizan la "frase de recuperación" (seed phrase), que se presenta como una secuencia aleatoria de 12, 18 o 24 palabras, de entre dos mil y cuarenta y ocho palabras del idioma inglés.

Si la clave privada es como la llave de su casa, piense en la frase de recuperación como un llavero con todas sus llaves (la de la casa, la del auto, la del armario, etc.). En otras palabras, la frase de recuperación equivale a todas sus claves, permitiendo a quien la posea ingresar en todos esos entornos y retirar todo lo que encuentre de valor. Técnicamente, la frase de recuperación representa una clave privada maestra (*private master key / extended private key*) de la cual todas las demás se derivan.

7- La posibilidad de crear nuevas cuentas en una sola cartera es prácticamente ilimitada.

NEGOCIACIÓN DE CRIPTOACTIVOS

Las dos principales formas de negociación de criptoactivos son las siguientes:

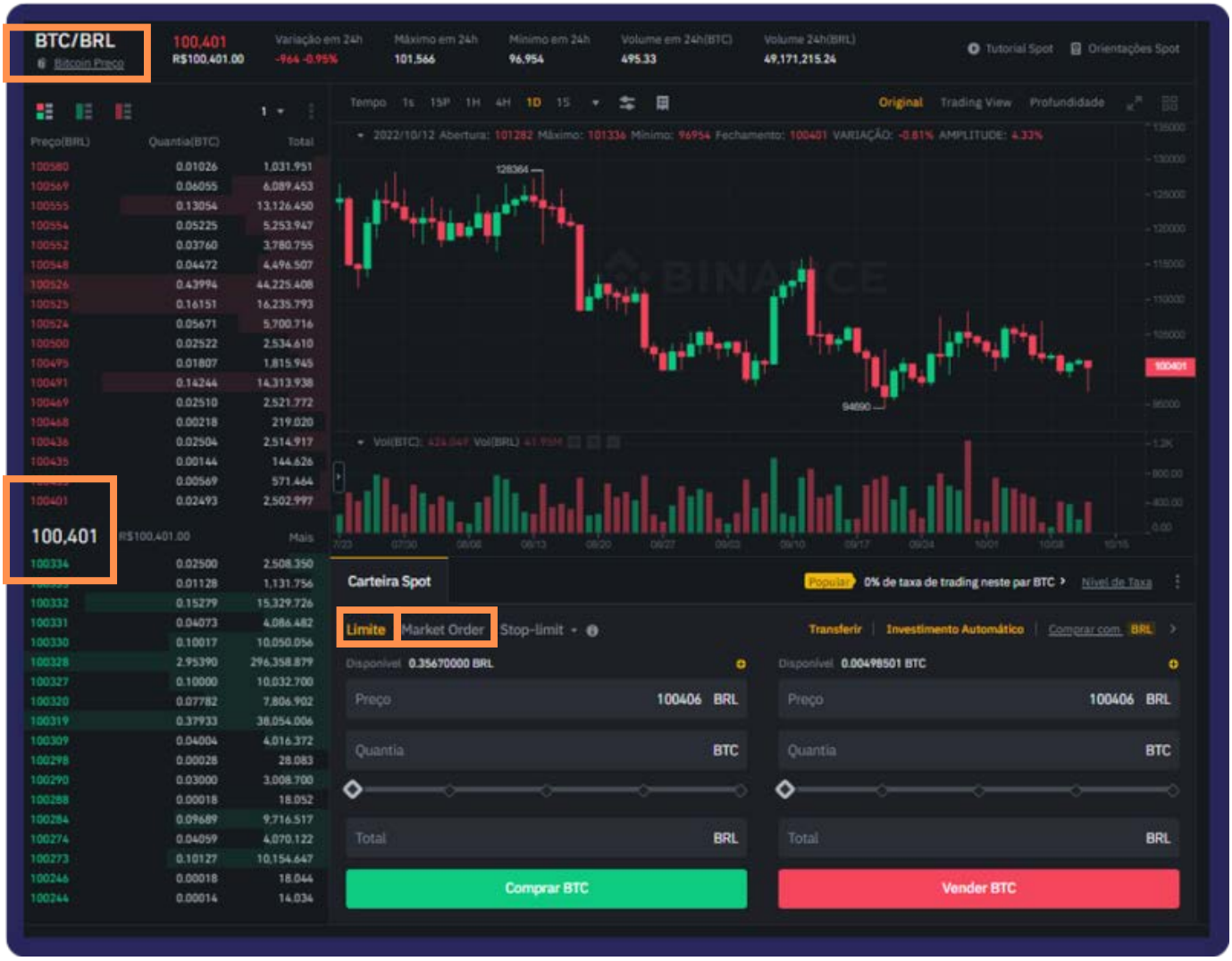
- Peer to peer (P2P): negociaciones no intermediadas, realizadas directamente entre dos carteras;

- En exchanges: negociaciones intermediadas, realizadas a través de libros de ofertas disponibles en una plataforma centralizada.

Las primeras transacciones quedan registradas en el Blockchain, por lo que se llaman onchain. Por otro lado, las segundas se registran en el registro privado de la entidad responsable de la plataforma, y se pueden llamar offchain.

Un libro de ofertas (book) es un instrumento para facilitar el encuentro de personas con intereses contrapuestos, es decir, quienes quieren comprar con quienes quieren vender un activo determinado. O, técnicamente, para quienes desean intercambiar A por B con quienes desean intercambiar B por A, en cualquier cantidad.

A continuación, reproducimos la imagen de un libro de ofertas para luego destacar algunos elementos de ese libro.



1) **Par de negociación:** un libro de órdenes siempre se refiere a dos activos. En este caso, BTC y BRL, con el fin de facilitar el encuentro entre aquellos que desean intercambiar bitcoins por reales, es decir, vender, con aquellos que desean comprar bitcoins.

2) **Orden:** es la formalización de una intención.

Tipos de órdenes:

- Orden de compra u orden de venta;

- Orden de mercado (market order) y orden límite.

Por ejemplo: Si quiero comprar bitcoins, debo formalizar esta intención a través de una orden de compra. Si estoy dispuesto a pagar lo que el mejor vendedor está pidiendo,

independientemente del precio, mi orden será a mercado; en cambio, si establezco un precio máximo por encima del cual no quiero comprar, mi orden será limitada.

Las órdenes a mercado se ejecutan de inmediato, independientemente del precio de mercado. Por otro lado, las órdenes limitadas se envían al libro de ofertas (órdenes de venta en rojo y de compra en verde), donde esperan a que el precio de mercado alcance el límite establecido.

3) **Spread:** es la diferencia entre la mejor orden de venta y la mejor orden de compra (100.401 - 100.334 = 67,00).

4) **Operación:** es el nombre dado al encuentro de dos órdenes opuestas.

5) **Precio de mercado de un activo:** es el precio correspondiente al de la última operación (R$100.401,00).

LEY DE CRIPTOACTIVOS BRASILEÑA

Activos Virtuales

A finales de 2022 se promulgó en Brasil la primera ley sobre el mercado de criptoactivos. La Ley n. 14.478/22 establece directrices que deben ser obedecidas en la prestación de servicios de activos virtuales, nombre adoptado por la legislación para los criptoactivos, y en la regulación de los prestadores de tales servicios.

La nueva ley brasileña considera activo virtual como "la representación digital de valor que puede ser negociada o transferida por medios electrónicos y utilizada para realizar pagos o con fines de inversión" (art. 3). [8]

8- La definición de activos virtuales dada por el art. 3 de la Ley n. 14.478/22 no es la misma adoptada por la CVM (Comissão de Valores Mobiliários) en el Parecer de Orientación n. 40/22. Allí, la CVM adoptó el siguiente concepto de criptoactivos: activos representados digitalmente, protegidos por criptografía, que pueden ser objeto de transacciones ejecutadas y almacenadas por medio de tecnologías de registro distribuido (distributed ledger technologies, DLTs). Usualmente, los criptoactivos (o su propiedad) son representados por tokens, que son títulos digitales intangibles. Los criptoactivos suelen ser designados como tokens y pueden desempeñar diversas funciones. La CVM adopta un enfoque funcional para la clasificación de los tokens en una taxonomía que servirá para indicar su tratamiento jurídico: Token de Pago (cryptocurrency o payment token): busca replicar las funciones de moneda, especialmente de unidad de cuenta, medio de intercambio y reserva de valor; Token de Utilidad (utility token): utilizado para adquirir o acceder a determinados productos o servicios; y Token referenciado a Activo (asset-backed token): representa uno o más activos, tangibles o intangibles. Son ejemplos los security tokens, las stablecoins, los non-fungible tokens (NFTs) y los demás activos objeto de operaciones de tokenización. De esta clasificación adoptada por la CVM, solo los ítems i y iii pueden desempeñar "la representación digital de valor que puede ser negociada o transferida por medios electrónicos y utilizada para realizar pagos o con fines de inversión" (art. 3, Ley n. 14.478/22). Estos son aquellos tokens que pueden, según la nueva ley, considerarse activos virtuales.

La misma disposición establece que no son activos virtuales:

- **La moneda nacional** (el Real, art. 1º, Ley nº 9.069/95[9]) y las demás monedas extranjeras, como el euro, el dólar, etc.;

- **La moneda electrónica**, definida en la Ley nº 12.865/13 como recursos almacenados en un dispositivo o sistema electrónico que permiten al usuario final realizar transacciones de pago (art. 6º, inciso VI), como operaciones con tarjetas de crédito y débito, tarjetas prepagas y transacciones vía teléfono celular, etc. Estas transacciones son intermediadas por instituciones de pago, integrantes del Sistema de Pagos Brasileño y del mercado de crédito del Sistema Financiero Nacional, supervisadas por el BACEN (Banco Central do Brasil) y reguladas por el Consejo Monetario Nacional;

- Instrumentos que brinden a su titular acceso a productos o servicios específicos o a beneficios provenientes de esos productos o servicios, como **puntos y recompensas de programas de fidelidad;**

- Representaciones de activos cuya emisión, escrituración, negociación o liquidación estén previstas en ley o reglamento, como **valores mobiliarios y activos financieros**[10]. Esta norma es complementada por el párrafo único del art. 1º de la Ley nº 14.478/22, que excluye de la nueva ley de criptoactivos los activos representativos de valores mobiliarios (Ley nº 6.385/76), sin alterar la competencia de la CVM.

9- Es interesante señalar que la configuración que el Banco Central de Brasil ha dado al **Real Digital**, una especie de moneda digital de banco central (*Central Bank Digital Currency*, CBDC) que tiene el mismo respaldo que la moneda fiduciaria, también la excluiría del concepto de activo virtual tratado aquí. Más información en https://www.bcb.gov.br/estabilidadefinanceira/real_digital.

10- Los activos financieros son bienes o derechos que una empresa o persona posee y que pueden generar ingresos, como acciones, dinero, bonos del gobierno, fondos de inversión, certificados de depósito bancario, etc.

Prestadoras de Servicios de Activos Virtuales

Las **Prestadoras de Servicios de Activos Virtuales (PSAVs)** son personas jurídicas que ejecutan, en nombre de terceros, al menos uno de los servicios de activos virtuales (art. 5º). Son las empresas actualmente designadas como **corredores** o **exchanges**.

Los **servicios de activos virtuales** definidos en la nueva legislación son:

- El intercambio entre activos virtuales y moneda nacional o extranjera;
- El intercambio entre uno o más activos virtuales;
- La transferencia de activos virtuales;
- La custodia o administración de activos virtuales o de instrumentos que permitan el control de activos virtuales, como las claves privadas de los clientes; o
- La participación en servicios financieros y prestación de servicios relacionados a la oferta por un emisor o venta de activos virtuales.

Una entidad de la Administración Pública federal, designada en un acto posterior del Poder Ejecutivo, podrá autorizar la realización de **otros servicios** que estén directa o indirectamente relacionados con la actividad de las prestadoras de servicios de activos virtuales.

La Ley n. 14.478/22 somete a las PSAVs a importantes leyes nacionales al establecer que su actividad debe observar las siguientes directrices, especificadas en un acto del órgano federal (art. 4º):

- La libre iniciativa y libre competencia;
- Buenas prácticas de gobernanza, transparencia en las operaciones y un enfoque basado en riesgos. Este último abre espacio para la tendencia internacional de regulación defendida por FATF/GAFI;

- Seguridad de la información y protección de datos personales, en referencia a las normas de la Ley General de Protección de Datos (Ley n. 13.709/2018);

- Protección y defensa de los consumidores y usuarios. La norma se complementa con el artículo 13 de la nueva ley, al establecer expresamente que las operaciones realizadas en el mercado de activos virtuales estarán sujetas, en lo que corresponda, al Código de Defensa del Consumidor (Ley n. 8.078/90);

- Protección del ahorro popular;

- Solidez y eficiencia de las operaciones; y

- Prevención del lavado de dinero (Ley n. 9.613/98) y del financiamiento del terrorismo (Ley n. 13.260/16) y la proliferación de armas de destrucción masiva, en línea con los estándares internacionales.

Regulación Federal

Será responsabilidad de un órgano o entidad de la Administración Pública Federal, definido en un futuro acto del Poder Ejecutivo, establecer qué activos financieros serán regulados para los fines de la Ley n. 14.478/22. Este mismo órgano tendrá el poder de autorizar previamente el funcionamiento de PSAVs en Brasil, además de establecer los casos en que la autorización podrá ser otorgada mediante un procedimiento simplificado. El artículo 6 prevé que un acto del Poder Ejecutivo asignará a uno o más órganos o entidades de la Administración Pública Federal la disciplina del funcionamiento y la supervisión de las PSAVs.

El Art. 8 prevé que las instituciones autorizadas a funcionar por el BACEN podrán ofrecer exclusivamente el servicio de activos virtuales o acumularlo con otras actividades, según lo dispuesto en la regulación a ser emitida por un órgano o entidad de la Administración Pública Federal indicada en un acto del Poder Ejecutivo Federal.

Además, corresponde al organismo o entidad reguladora indicada en un acto del Poder Ejecutivo Federal (art. 7):

- Autorizar el funcionamiento, transferencia de control, fusión, escisión e incorporación de PSAV;
- Establecer condiciones para el ejercicio de cargos en órganos estatutarios y contractuales en PSAV y autorizar la posesión y el ejercicio de personas para cargos de administración;
- Supervisar a las PSAV y aplicar las disposiciones de la Ley nº 13.506/2017 (que trata sobre el proceso administrativo sancionador del BACEN y de la CVM), en caso de incumplimiento de la Ley n. 14.478/22 o de su regulación;
- Cancelar, de oficio o a pedido, las autorizaciones de las PSAV; y;
- Disponer sobre las hipótesis en que los servicios de activos virtuales del art. 5 serán incluidos en el mercado de cambio o en que deberán someterse a la regulación de capitales brasileños en el exterior y capitales extranjeros en el país.

Después de su entrada en vigor, la Ley n. 14.478/22 prevé aún un subsiguiente plazo para que las PSAV se ajusten a la regulación. Este plazo será definido por el órgano federal a designar, pero no será inferior a seis meses (art. 9º).

Disposiciones penales y normas complementarias

El art. 10 de la Ley n. 14.478/22 introduce en el Código Penal el art. 171-A, nueva forma de estafa: "**Fraude con la utilización de activos virtuales, valores mobiliarios o activos financieros".**

Art. 171-A. Organizar, gestionar, ofrecer o distribuir carteras o intermediar operaciones que involucren ***activos virtuales, valores mobiliarios o cualquier activo financiero*** *con el fin de obtener una ventaja ilícita, en perjuicio de terceros, induciendo o manteniendo a alguien en error, mediante artificio, engaño o cualquier otro medio fraudulento.*

Pena - reclusión, de 4 (cuatro) a 8 (ocho) años, y multa.

La Ley n.º 14.478/22 también modifica el párrafo único del Art. 1 de la Ley n.º 7.492/86 para que conste lo siguiente:

Artículo 1.º Se considera institución financiera, para efectos de esta ley, a la persona jurídica de derecho público o privado, que tenga como actividad principal o accesorio, acumulativa o no, la captación, intermediación o aplicación de recursos financieros (vetado) de terceros, en moneda nacional o extranjera, o la custodia, emisión, distribución, negociación, intermediación o administración de valores mobiliarios.

Párrafo único. Se equipara a la institución financiera:

I - la persona jurídica que capte o administre seguros, cambio, consorcio, capitalización o cualquier tipo de ahorro, o recursos de terceros;

I-A - la persona jurídica que ofrezca servicios referentes a operaciones con activos virtuales, incluyendo intermediación, negociación o custodia;

II - la persona natural que ejerza cualquiera de las actividades referidas en este artículo, incluso de forma eventual.

Con esto, las PSAV pasan a ser instituciones financieras por equiparación y se someten a todos los delitos contra el SFN (Sistema Financiero Nacional) de la Ley nº 7.492/86.

Las normas antilavado de dinero traídas por la nueva legislación serán analizadas en el siguiente tema.

Por último, la Ley n. 14.478/22 modificó la Ley Antilavado para incluir en ella el artículo 12-A, que dispone sobre la creación del Registro Nacional de Personas Expuestas Políticamente (RNPEP), disponible en el Portal de la Transparencia.

A partir de su entrada en vigencia, los organismos y entidades de cualquier poder de la Unión, los Estados, el Distrito Federal y los Municipios deberán enviar al gestor del CNPEP, de acuerdo con la forma y la periodicidad definidas en el reglamento, información actualizada sobre sus miembros o ex-miembros clasificados como personas expuestas políticamente (PEPs) en la legislación y regulación vigentes. El gestor del CNPEP indicará en la transparencia activa, por internet, los organismos y entidades que no cumplan con la obligación.

Las personas obligadas por el Sistema Antilavado incluirán la consulta al CNPEP entre sus procedimientos para el cumplimiento de las obligaciones previstas en los artículos 10 y 11 de la Ley Antilavado, sin perjuicio de otras diligencias exigidas conforme a la legislación. § 3º

INVESTIGACIÓN FINANCIERA DE DELITOS QUE INVOLUCRAN CRIPTOACTIVOS

El uso del sistema financiero por parte de los delincuentes para transferir, guardar o disimular las ganancias del delito desafía a las agencias de investigación estatales a recopilar, analizar y presentar pruebas de las transacciones financieras utilizadas con ese fin, con el fin de fortalecer y posibilitar la persecución penal ante el Poder Judicial y la recuperación de los activos involucrados.

Como método de investigación, la Investigación Financiera se enfoca en los asuntos financieros relacionados con la conducta ilícita, buscando identificar y documentar, con fines probatorios, el movimiento de dinero durante el curso de la actividad criminal[11]. Dicho de otra manera, la Investigación Financiera es un método que busca conectar personas, lugares y eventos a través de hechos financieros[12]. Este tipo de investigación gira en torno al concepto de datos financieros, que representa la información relacionada con el dinero, los activos, los gastos y las finanzas, presente en casi todos los aspectos de la vida de una persona.

Estos datos financieros se han desmaterializado desde principios de la década de 2010, en el contexto de la crisis financiera global de 2008, a partir de la migración de las relaciones financieras tradicionales a medios digitales y del advenimiento de un **criptomercado** paralelo a los sistemas financieros nacionales.

11-FATF, Operational Issues Financial Investigations Guidance (Guía sobre Cuestiones Operativas en Investigaciones Financieras), 2012, p. 03.

12- SLOT, Brigitte; SWART, Linette de; DELEANU, Ioana; MERKUS, Erik; LEVI, Michael; KLEEMANS, Edward. Evaluación de necesidades sobre herramientas y métodos de investigación financiera en la Unión Europea: Informe final. Rotterdam: ECORYS, 2015, p. 09-17.

Los criptoactivos representan la faceta más importante de este dinero inmaterial, compuesto en última instancia por bits en el sistema informático de alguien, acercando la investigación financiera a una investigación informática y exigiendo importantes interacciones entre el secreto financiero y el secreto que cubre algunas huellas digitales.

Como un activo patrimonial, la investigación financiera de delitos que involucran criptoactivos se desarrolla a través de la **misma metodología de investigación patrimonial** utilizada por el Ministerio Público Federal para el rastreo de otros activos, como se explica en la Guía de Persecución Patrimonial y Administración de Bienes elaborada por el grupo de trabajo instituido por las 2ª y 5ª Cámaras de Coordinación y Revisión.[13]

Si bien la metodología de investigación es la misma, las herramientas tecnológicas utilizadas para el rastreo patrimonial (búsqueda remota y búsqueda presencial) y las particularidades involucradas en la incautación y administración de este tipo de bienes requieren la elaboración de una guía de actuación específicamente enfocada en los criptoactivos.

METODOLOGÍA DE RASTREO PATRIMONIAL

Se utiliza el término Investigación Financiera para el complejo de actividades de recolección, análisis y uso de información financiera por los organismos de aplicación de la ley. Aunque este documento presenta una sugerencia metodológica para la realización de la investigación financiera, parece cierto que las medidas adecuadas para cada caso deben ser determinadas por el propio caso. Solo él exige las medidas necesarias para su propio éxito, y esto quizás represente la regla de oro de cualquier resumen investigativo.[14]

13- BRASIL. Ministerio Público Federal. 2ª Cámara de Coordinación y Revisión. Guía de Actuación - Persecución Patrimonial y Administración de Bienes, 2017. Disponible en: https://portal.mpf.mp.br/novaintra/areas-tematicas/camaras/criminal/publicacoes/roteiros-de-atuacao-restrito/roteiro_atuacao_persecucao_patrimonial

14- MARTINS. Tiago Misael de Jesus. Persecución Patrimonial por Medio de Investigación Financiera, en BRASIL. Ministerio Público Federal. 2ª Cámara de Coordinación y Revisión. Temas Procesales, Prueba y Persecución Patrimonial, 2019. Disponible en: https://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea-de-artigos-temas-processuais-prova-e-persecucao-patrimonial/at_download/file

En cualquier caso, los investigadores financieros deben tener en cuenta que deben pacientemente “seguir el dinero” (follow the money); en los delitos tratados aquí, si no se sigue el dinero, el delito vale la pena.[15]

A pesar de las dificultades derivadas del flujo globalizado e instantáneo de activos en la contemporaneidad, siempre se debe tener en cuenta que el patrimonio es el objetivo del delito cometido. Por lo tanto, los delincuentes prefieren mantener cierto grado de control sobre sus activos y, como resultado, generalmente hay una "huella de papel" (paper trail) que puede conducir la investigación de regreso al infractor. Esta huella de papel también se puede seguir para identificar infractores adicionales y la ubicación de pruebas e instrumentos utilizados para cometer delitos.[16]

Los investigadores financieros desarrollan hipótesis basadas en la información disponible. La hipótesis imaginada determina la extensión y el tipo de información requerida para probar su mérito. Identificar el tipo de información necesaria permite al investigador determinar dónde se guardan esas informaciones (si en fuentes abiertas o cerradas, por ejemplo). Una vez que el investigador ha determinado qué información es necesaria y dónde se almacena, puede prever los métodos y desafíos para obtener la información (por ejemplo, acceso directo a bases de datos públicas, acceso mediante solicitud directa, desbloqueo de secreto bancario mediante una orden judicial, etc.). Por lo tanto, implementa un plan de recopilación de datos que conduce a la obtención exitosa de la información necesaria para probar la hipótesis.[17]

Este razonamiento se puede presentar mediante el siguiente gráfico[18]

15- UNODC. Inteligencia Criminal: Manual para Analistas. Viena: UNODC, 2011, p. 35-36.

16- FATF, ibídem, p. 07.

17- FATF, ibídem, p. 17.

18- MARTINS, ibídem.


Plan de recolección de Datos
1
Desarrollar la hipótesis a partir de las pruebas disponibles;
2
Identificar el tipo de información (prueba) a recolectar;
3
Identificar el repositorio de esta información (fuentes abiertas o cerradas);
4
Identificación del método de recolección;
5
Realizar la recolección de datos.

La metodología para la recopilación de información financiera se basa en una fase secreta, iniciada para permitir la adopción de medidas de recopilación de información sin el conocimiento del objetivo, especialmente debido a la posibilidad real de rápida disipación patrimonial y destrucción de pruebas por medios tecnológicos modernos; y en una fase ostensible, en la cual esta precaución ya no es necesaria, por ejemplo, porque no se encontró ningún activo en la fase secreta o porque se prevé que los bienes descubiertos por medidas adoptadas en la fase ostensible compensen el descarte de la sorpresa de las medidas de restricción cautelares.

Al comienzo de la fase secreta, gran parte de los datos se encuentran en fuentes abiertas de información. Toda investigación comienza lentamente y toma impulso a medida que se acumulan información y datos[19]. Para recopilar esta información, el investigador primero utiliza las llamadas fuentes abiertas (open sources), consistentes en toda la información públicamente disponible a través de Internet, medios sociales, medios impresos y electrónicos, así como los registros mantenidos por organismos públicos o por organismos privados, pero de acceso al público[20].

No es la intención de este trabajo sobre criptoactivos, que solo recuerda conceptos metodológicos sobre investigación patrimonial, describir las fuentes de investigación abiertas, sino solo presentar su existencia y utilidad en el contexto de la Investigación Financiera. Para consultar las fuentes abiertas en Brasil y en el extranjero, se recomienda consultar la Guía de Persecución Patrimonial y Administración de Bienes, capítulo III, puntos 4 y 5.

Con la recopilación de información contenida en la fuente abierta, se puede buscar acceso a fuentes cerradas, entendidas como aquellas a las que el investigador no tiene acceso, a través de investigación directa o solicitud, sin necesidad de intervención judicial. Las fuentes cerradas normalmente se identifican como sujetas a secreto legal, como los datos bancarios, fiscales, telefónicos, telemáticos, etc.

19- UNODC, ibídem, p. 41.
20- FATF, ibídem, p. 18.

En el MPF, los modelos adoptados para el acceso a datos financieros y fiscales se encuentran en los borradores del Sistema de Investigación de Movimientos Bancarios - **SIMBA**[21] y de la Sistemática de Investigación Fiscal - **SIFISCO**[22], mientras que la recepción de datos telefónicos, si interesan a la investigación, pueden ser recibidos en el Sistema de Investigación de Registros Telefónicos - **SITTEL**[23]. A su vez, los modelos de solicitudes de levantamiento del secreto de las comunicaciones telemáticas se encuentran compilados en el portal e-Evidence, mantenido por el Grupo de Apoyo a la Criminalidad Cibernética.[24]

La secuencia presentada para la recolección de datos en fuentes abiertas y luego en fuentes cerradas fue adoptada solo con fines didácticos. Lo que ocurre en la práctica es una retroalimentación de las fuentes. Esto se debe a que la información vuelve a ser recolectada en medios abiertos a medida que nuevas informaciones son obtenidas de fuentes cerradas y viceversa.

Con la recolección de estas fuentes de prueba, puede ser conveniente realizar una fase ostensiva con interrogatorios de los objetivos, de sus familiares, asociados formales o informales, allanamiento de sus hogares (art. 240, § 1º, b y h, CPP), de sus empresas, oficinas, incautación de computadoras para peritaje, incautación de libros contables para auditoría, etc.

HERRAMIENTAS PARA EL RASTREO PATRIMONIAL DE CRIPTOACTIVOS

De acuerdo con la metodología presentada en la Guía de Persecución Patrimonial del MPF, el rastreo de criptoactivos comienza generalmente con la consulta de fuentes abiertas de registro de transacciones, que son de gran importancia en el contexto de criptoactivos que adoptan un libro mayor público.

21- Disponible en https://portal.mpf.mp.br/simba/php/Simba.php.

22- Disponible en https://portal.mpf.mp.br/portaldedados/.

23- Disponible en https://portal.mpf.mp.br/sittel/.

24- Disponible en https://portal.mpf.mp.br/eevidence/.

- **Fuentes Abiertas**[25]

Evidentemente, las fuentes abiertas indicadas en la Guía de Persecución Patrimonial del MPF siguen siendo importantes para el rastreo patrimonial de investigados que operan con criptoactivos. Mediante la búsqueda en fuentes abiertas, como redes sociales, se pueden obtener datos importantes que, junto con los demás elementos de prueba obtenidos de otras fuentes abiertas (generales o específicas para criptoactivos) o fuentes de prueba cerradas, resultan útiles para la investigación.

Con el objeto delimitado del presente documento, se describe a continuación las herramientas de búsqueda específicas para criptoactivos.

- **Fuentes Abiertas Disponibles en la Web**

En primer lugar, es importante que el investigador tenga conocimiento sobre el **modelo de negocio del criptoactivo** investigado, cuyas características técnicas y limitaciones prácticas son de suma importancia en la investigación. Para cada criptoactivo, normalmente hay un sitio web específico con la descripción general de su funcionamiento y acceso al libro mayor público. Ejemplo: Ethereum (ethereum.org/pt-br/), Monero (monero.inf.br/), etc. Para una visión amplia de las criptomonedas existentes y continuamente creadas, se puede consultar, por ejemplo, el sitio web mantenido por la empresa CoinMarketCap (http://www.coinmarketcap.com).

Una de las principales herramientas de fuentes abiertas utilizadas para las investigaciones son aquellas que exploran la tecnología de Blockchain pública subyacente a la mayoría de los criptoactivos. De hecho, **el análisis de Blockchain** permite a los investigadores identificar relaciones y flujos financieros entre carteras, con el objetivo de investigar direcciones, valores de transacciones, carteras emisoras y receptoras, y otros detalles relacionados con una transacción. Este análisis no está asociado con el nombre de una persona física, pero indica

25- Contribuyó a la prueba de herramientas de fuentes abiertas sobre criptoactivos la servidora Adriana Shimabukuro, miembro del GT de Criptoactivos instituido por la SPPEA/PGR.

un gran nivel de detalle sobre la cartera y sus movimientos y, a veces, analizar las transacciones puede respaldar hipótesis de que las carteras recurrentes pertenecen al mismo investigado.[26] El análisis de Blockchain, combinado con otras fuentes abiertas y cerradas, representan, casi siempre, el primer paso en una investigación con criptoactivos.[27]

Sitios como **Blockchain** (*www.Blockchain.com/explorer*) permiten buscar el número de una cartera de Bitcoin, Ethereum y Bitcoin Cash[28], mostrando el número de transacciones vinculadas a ella, el total de activos recibidos, saldo final y un historial completo de transacciones, permitiendo rastrear cada entrada o salida de activos de la cartera. Para herramientas con otras opciones de criptos, hay **Blockchair** (https://blockchair.com/pt), **Coin Market** (https://Blockchain.coinmarketcap.com/), **OXT** (https://oxt.me/), **Trade Block** (https://tradeblock.com/home), entre otros.

Además de las transacciones en sí, puede ser importante para una investigación identificar quién fue el minero del bloque de Blockchain. Actualmente, los mineros son empresas con gran capacidad computacional, que a veces representan el conjunto de varios mineros individuales (pool de minería).[29] Como los participantes reciben su parte de la recompensa del pool y el bloque minado puede ser identificado, las empresas de minería pueden cooperar con eventuales investigaciones indicando, por ejemplo,

26- El análisis de Blockchain puede verse dificultado por el investigado al utilizar técnicas de mezclado (tumbler, fogger o blender), que pueden ser contratadas como servicios de un tercero o simplemente a través de un software. Estas técnicas combinan entradas y salidas de muchos usuarios diferentes en una misma cartera o conjunto de carteras, con el objetivo de dificultar el rastreo de las transacciones. Cuando son contratados a una empresa, se cobran tarifas y normalmente no se mantienen registros de los usuarios contratantes. En este enlace se describen algunos de los servicios de mezclado de criptoactivos más famosos: https://beincrypto.com/learn/best-bitcoin-mixers/. Algunos criptoactivos fueron diseñados para contar ya con mezcladores integrados, como Dash y Monero (https://monero.inf.br/tecnologia-de-privacidade-do-monero/)

27- Dado que no posee información completamente intuitiva, el investigador necesita tener conocimientos del modelo de negocio del criptoactivo que está rastreando, ya que de lo contrario podría interpretar los resultados del rastreo de la Blockchain de manera errónea y perder detalles importantes relacionados con un caso.

28- Además de las operaciones con NFTs: https://www.Blockchain.com/pt/nfts.

29- En el contexto de la minería de criptomonedas, un pool de minería es la agrupación de recursos por parte de los mineros individuales, quienes comparten su poder de procesamiento en una red para dividir la recompensa de manera equitativa y de acuerdo con la cantidad de trabajo que cada uno contribuyó a la resolución de bloques de transacciones.

cuál integrante del pool fue remunerado por la minería de un bloque en particular. En la mayoría de las transacciones, es fácil identificar al minero del bloque ya que sus nombres (o los nombres de los pools o empresas) a menudo están "etiquetados" en los bloques y ya figuran en las herramientas descritas anteriormente para el análisis de las carteras.

Para el monitoreo de carteras con la recepción de alertas por correo electrónico, existen servicios prestados por **Cryptocurrency Alerting** (*https://cryptocurrencyalerting.com/*), gratuito hasta tres alertas, y **Blockonomics** (*https://www.blockonomics.co/*).

La herramienta Wallet Explorer (www.walletexplorer.com) proporciona información histórica sobre otras direcciones poseídas por una sola cartera virtual, vincula direcciones de Bitcoin a entidades conocidas, incluyendo exchanges, “pools” de minería, páginas de juegos, carteras o darknet.[30] Descontinuada en 2016, su metodología fue incorporada a la herramienta comercial de la empresa Chainalysis, descrita a continuación.

Wallet Explorer sigue siendo una herramienta poderosa hasta el día de hoy, especialmente para aquellos organismos de investigación que no tienen acceso a una alternativa comercial más sofisticada, especialmente si a través de los datos presentados por la plataforma se identifica una relación con algún exchange u otra entidad que pueda identificar, aunque sea con datos históricos, el propietario de la cartera.

Con un producto similar y gratuito, pero limitado a treinta consultas, está la solución de la empresa **Crystal Explorer** (*https://explorer.crystalBlockchain.com*).

30- Wallet Explorer agrupa direcciones en carteras, reuniendo principalmente direcciones de entrada de múltiples transacciones y de cambio. Después de que se identifican grupos de determinada dimensión, es necesario que al menos una de sus direcciones sea identificada a través de un reconocimiento pasivo o activo. Una dirección identificada en el grupo sería suficiente, en principio, para identificar todas las demás direcciones restantes como pertenecientes a ese grupo.

El sitio **Bitcoin Who's Who** (*www.bitcoinwhoswho.com*) proporciona más información sobre alguna cartera sospechosa, como si ha estado involucrada en delitos virtuales a partir de información pública. Se puede identificar la dirección IP de la transacción, aunque generalmente está encubierta por alguna VPN. La herramienta **Bitcoin Abuse** (*www.bitcoinabuse.com*) informa al usuario si otros han reportado alguna cartera como asociada con actividades ilegales (ransomware, spam, fraude, etc.). El resultado informa el tipo de delito y a veces el correo electrónico asociado con dicha actividad. Con una propuesta similar, existe el servicio **Check Bitcoin Address** (*https://checkbitcoinaddress.com/*).

Algunas herramientas permiten la representación gráfica de operaciones con criptoactivos, como **Maltego** (*https://www.maltego.com/blog/cryptocurrency-investigations-with-maltego/*).

Si hay información proveniente de otros elementos de prueba, el miembro del MPF puede solicitar a las exchanges de criptoactivos en operación en el país que informen los **datos de registro de la persona responsable por determinada cartera**, utilizando para ello los diversos dispositivos legales que permiten esta solicitud[31].

La salvedad se da en aquellos casos en que la exchange acepta interacciones a distancia, permitiendo que un cliente haga una cuenta con la carga de documentos de identificación y, a veces, fotografía. En estas situaciones, es posible que el cliente emplee identificación fraudulenta o fotos manipuladas en el proceso de registro junto a la exchange.

31- En este sentido, por ejemplo, el art. 15 de la Ley 12.850/13, el art. 17-B de la Ley 9.613/98 y el art. 10, § 3º, de la Ley n.12.965/14.

- **Herramientas Comerciales de Investigación**

Los delincuentes que operan con criptoactivos dependen intensamente de software especializado y técnicas evasivas para garantizar el anonimato y oscurecer la titularidad de la cartera de criptoactivos. Por lo tanto, es absolutamente fundamental que los organismos de investigación empleen software que pueda penetrar las contramedidas adoptadas por los investigados.

La descripción de las posibilidades de las herramientas de fuentes abiertas mencionadas anteriormente indica que su uso aislado no cumple el objetivo final de la investigación, que es definir la autoría del hecho delictivo. En la gran mayoría de los casos, se tendrá seguridad sobre el flujo de los recursos, pero no sobre la identidad de quien los titula, ya que las personas físicas que mueven las carteras permanecen, casi siempre, ocultas.

Las fuentes abiertas disponibles en la web permiten el acceso a registros de transacciones de la mayoría de los criptoactivos, pero fallan, por lo general, en determinar la identidad de las personas detrás de una cartera determinada. Vincular a una persona con una dirección o cartera es el mayor desafío de la investigación con criptoactivos. A excepción de los casos en los que, como resultado de otros elementos de prueba, el investigador puede exigir a las exchanges de criptoactivos en operación en el país que proporcionen los datos de registro de la persona responsable de una determinada cartera, la investigación puede llegar a un callejón sin salida debido a la indeterminación de la autoría, es decir, por el desconocimiento de quién opera una determinada cartera.

Observando esta deficiencia en las investigaciones sobre criptoactivos, diversas empresas comenzaron a ofrecer herramientas tecnológicas pagas en el mercado que pueden determinar, en base a una base de datos de la empresa, quién es el responsable (persona o exchange) de la cartera investigada.[32]

32- Por lo general, los proveedores de software son muy abiertos, cercanos y rápidos cuando se trata de la posibilidad de probar sus productos antes de que alguien o alguna entidad se comprometa a comprarlos.

En general, las herramientas comerciales de investigación son superiores, ya que proporcionan más información de manera más detallada y rápida que las herramientas disponibles en fuentes abiertas. Las herramientas comerciales de investigación suelen permitir obtener el siguiente conjunto de información y realizar varias acciones importantes para el análisis de datos financieros de una sola vez: a) importar y exportar datos; b) identificar un mayor número de entidades; c) realizar agrupaciones de forma más rápida y con una mejor interpretación; d) tener una interfaz más simplificada; e) tener referencias a direcciones de la dark web y de la web abierta (open web); f) permitir consultas específicas para obtener asistencia técnica; g) tener varias funcionalidades adicionales para alcanzar información de manera más rápida. [33]

Hay varias soluciones disponibles en el mercado, como **Reactor** de la empresa Chainalysis (*https://www.chainalysis.com/chainalysis-reactor/*), **Inspector** de la empresa Cellebrite-Ciphertrace (https://ciphertrace.com/ y https://ciphertrace.com/financial-investigations-and-blockchain-forensics/), **Coinbase Analytics** de Coinbase (https://www.coinbase.com/pt/analytics); **Blockchain Analytics** de Elliptic (https://www.elliptic.co/solutions/crypto-investigations); y **Crystal Blockchain Analytic** de la empresa Crystal Blockchain (https://crystalBlockchain.com/).[34]

33- Otra funcionalidad presentada en algunas herramientas comerciales es la posibilidad de vincular direcciones de Bitcoin a una cartera específica basada en las direcciones solicitadas por el cliente light, y el registro de direcciones IP que pueden usarse para identificar a un sospechoso.

34- Con la alerta del GAFI, el uso de herramientas de análisis de criptoactivos, aunque útil, también puede representar un desafío para las investigaciones. Como cada herramienta de rastreo contiene datos de código abierto diferentes y utiliza diferentes algoritmos para buscar en el Blockchain, estos servicios pueden proporcionar diferentes resultados a los investigadores. Conocer las herramientas y sus resultados es esencial para el uso adecuado de estas tecnologías para fines investigativos. En algunos casos, los países que utilizan estas herramientas descubrieron que diferentes exchanges y/o plataformas de criptoactivos son menos visibles que otras, lo que aumenta la dificultad de seguir los flujos de activos. Además, las herramientas de análisis actualmente disponibles en el mercado son compatibles solo con un número limitado de activos virtuales (FATF, Orientación sobre Investigaciones Financieras Involucrando Activos Virtuales. Enfrentando Desafíos con Investigaciones y Confiscaciones, mayo de 2019, p. 39).

Una preocupación en el uso de herramientas comerciales está relacionada con la capacidad de la agencia de investigación de explicar sus descubrimientos y procedimientos investigativos al Poder Judicial. Es decir, la herramienta debe presentar información clara sobre cómo se llegó a determinado investigado, por ejemplo, para que la agencia de investigación pueda evaluar la prueba y su pertinencia en juicio. Algunas herramientas proporcionan expertos en la herramienta para testificar sobre cómo se llevó a cabo el análisis de Blockchain.[35]

Algunas herramientas utilizadas para la extracción de datos de medios incautados (por ejemplo, teléfonos inteligentes y computadoras) se pueden utilizar para identificar, entre los archivos extraídos, programas relacionados con criptoactivos[36]. El MPF tiene acceso al **Cellebrite Physical Analyzer**, que revela la existencia de programas de criptoactivos. Para la extracción de estos archivos, se debe enviar el medio al sector de peritaje de la SPPEA[37], a partir de la apertura de una solicitud de peritaje en el Sistema Pericial.

- ## Informes de Inteligencia Financiera

La información sobre operaciones con criptoactivos se puede obtener del Consejo de Control de Actividades Financieras - COAF a través de informes de inteligencia financiera solicitados directamente (**informes de intercambio**) [38] en el Sistema de Control de Actividades Financieras - SisCOAF.[39]

35- FATF, Ibídem, p. 41/42.

36- En este sentido: https://cellebrite.com/en/walkthrough-of-parsing-cryptocurrency-applications-in-cellebrite-physical-analyzer/.

37- Instrucción de Servicio SPPEA/PGR n. 41/2021 sobre manejo de huellas digitales con soporte físico visible.

38- Los RIFs de intercambio son aquellos elaborados para atender solicitudes de información por parte de autoridades nacionales o Unidades de Inteligencia Financiera. Por otro lado, los RIFs espontáneos (de oficio) son elaborados por iniciativa del COAF a partir del análisis de comunicaciones y denuncias.

39- Disponible en: https://www.gov.br/coaf/pt-br/sistemas/siscoaf-2-1.

Antes de la entrada en vigor de la Ley n. 14.478/2022, los exchanges nacionales no estaban incluidos como "personas obligadas" según el artículo 9 de la Ley 9.613/1998 - Ley de Lavado de Dinero. A través de un modelo de autorregulación, algunos exchanges nacionales comenzaron a informar voluntariamente al COAF sobre operaciones sospechosas relacionadas con el lavado de dinero y el financiamiento del terrorismo[40].

Con la llegada de la Ley del Mercado de Criptoactivos, los exchanges - ahora denominados prestadoras de servicios de activos virtuales, PSAVs (art. 5) - pasaron a formar parte del Sistema Antilavado de Capitales brasileño ([41]). El artículo 9 de la Ley 9.613/1998 fue modificado para someter a las PSAVs a las obligaciones previstas en los artículos 10 y 11 de la misma ley.

Las obligaciones impuestas por el art. 10 están relacionadas principalmente con la obligación de conocer a sus clientes (KYC) y las transacciones financieras que realizan (KYT):

> Identificar a sus clientes y mantener un registro actualizado, de acuerdo con las instrucciones emitidas por las autoridades competentes. En el caso de que el cliente sea una persona jurídica, la identificación deberá abarcar a las personas físicas autorizadas a representarla, así como a sus propietarios (§ 1) - la idea es evitar el uso del velo corporativo de la empresa para ocultar al beneficiario final (12). Los datos deben ser conservados por un mínimo de cinco años a partir del cierre de la cuenta o de la conclusión de la transacción (§ 2º).
>
> Mantener registro de todas las transacciones en moneda nacional o extranjera, títulos y valores mobiliarios, títulos de crédito,

40- En este sentido, el Código de Conducta y Autorregulación de las empresas vinculadas a ABCripto: https://www.abcripto.com.br/_files/ugd/55dd41_206786481fc84485817e8d906b54b241.pdf.

41- Dos disposiciones ya presentes en la Ley Antilavado que no fueron modificadas por la Ley n. 14.478/22 son de interés para las investigaciones financieras que involucren criptoactivos, especialmente en el momento del dilema de la conversión de criptoactivos en moneda fiduciaria. En primer lugar, el artículo 10-A que crea el Registro de Clientes del SFN - CCS, a través del cual el BACEN mantiene un registro centralizado del registro general de titulares y clientes de instituciones financieras, así como de sus apoderados. En segundo lugar, el artículo 11-A establece que las transferencias internacionales y los retiros en efectivo deben ser comunicados previamente a la institución financiera, en los términos, límites, plazos y condiciones establecidos por el Banco Central del Brasil.

metales, activos virtuales (agregado por la Ley n. 14.478/22), o cualquier activo susceptible de ser convertido en dinero, que exceda el límite fijado por la autoridad competente, deben ser registrados. Los datos deben ser conservados durante al menos cinco años a partir del cierre de la cuenta o la conclusión de la transacción (§ 2º). Además, el registro de las transacciones se efectuará también cuando la persona física o jurídica, sus entes ligados, hayan realizado, en un mismo mes calendario, operaciones con una misma persona, conglomerado o grupo que, en su conjunto, superen el límite fijado por la autoridad competente (§ 3º);

Adoptar políticas, procedimientos y controles internos compatibles con su tamaño y volumen de operaciones, de acuerdo con las normas de los organismos competentes;

Registrarse y mantener su registro actualizado en el organismo regulador o fiscalizador y, en su defecto, en el Consejo de Control de Actividades Financieras (COAF), en la forma y condiciones establecidas por ellos;

Responder a las solicitudes del COAF en la periodicidad, forma y condiciones establecidas por él, y preservar, en los términos de la ley, la confidencialidad de la información proporcionada.

Las obligaciones previstas en el artículo 11 están relacionadas con el deber de comunicar operaciones financieras sospechosas al Consejo de Control de Actividades Financieras (COAF):

Prestar especial atención a las operaciones que, de acuerdo con las instrucciones de las autoridades competentes, puedan constituir graves indicios de lavado de dinero. Las autoridades competentes elaborarán una lista de operaciones que, por sus características, en cuanto a las partes involucradas, valores, forma de realización, instrumentos utilizados o por la falta de fundamentos económicos o legales, puedan configurar la hipótesis prevista en él (§ 1º).

Comunicar al COAF, sin informar a ninguna persona, incluyendo aquella a la que se refiera la información, dentro de las 24 horas, la propuesta o realización de todas las transacciones mencionadas en el inciso II del artículo 10, acompañadas de la identificación a la que se refiere el inciso I del mismo artículo; y de las operaciones mencionadas en el inciso I del artículo 11;

Comunicar al regulador o fiscalizador de su actividad o, en su defecto, al COAF, en la periodicidad, forma y condiciones establecidas por ellos, la no ocurrencia de propuestas, transacciones u operaciones susceptibles de ser comunicadas.

No es infrecuente que los investigados operen en exchanges con sede en países que tienen controles débiles contra el lavado de dinero y el financiamiento del terrorismo, o incluso en países que sistemáticamente se niegan a cooperar, a pesar de la existencia formal de herramientas de cooperación jurídica internacional.

Además de los proveedores de servicios virtuales previstos en la Ley n. 14.478/2022, las operaciones con criptoactivos pueden ser comunicadas al COAF por entidades pertenecientes a otros sectores obligados por ley, como instituciones financieras bancarias y corredores y distribuidores de valores mobiliarios. De hecho, las entidades tradicionales de los sectores legalmente obligados pueden notificar dos tipos de operaciones financieras sospechosas: a) operaciones ocurridas en sus productos financieros por personas físicas o jurídicas investigadas; y b) operaciones sospechosas realizadas por las propias exchanges.

Esto sucede porque, aunque operen con criptoactivos, los investigados siempre encuentran el dilema del retiro (o dilema de conversión), es decir, necesitan convertir el criptoactivo en moneda fiduciaria. fiduciária[42]. Cuando esta conversión ocurre en instituciones financieras nacionales, es posible que estas operaciones hayan sido comunicadas al COAF.

Eventuales informes de inteligencia financiera pueden ser analizados a través de la herramienta RIF Análisis, a partir de archivos del tipo .CSV enviados por el COAF adjuntos a los informes.[43]

Debido a la transnacionalidad inherente a las operaciones con criptoactivos, a menudo es necesario buscar datos de unidades de inteligencia financiera en el extranjero. Para ello, el COAF intermedia las solicitudes al **Grupo Egmont**. Las orientaciones adicionales se encuentran en el siguiente video producido por el COAF, Inteligencia Financiera: Aspectos Prácticos del Intercambio Internacional a través de la *Red Egmont: https://youtu.be/i5N_LqLmewI*.[44]

42- Como el propósito de una investigación es acumular evidencia para probar que un delito que involucra criptoactivos ha ocurrido, los investigadores pueden intentar seguir el dinero hasta que identifiquen a un conocido proveedor de servicios con criptoactivos, como un exchange o un procesador de pago. El punto focal crítico en una investigación relacionada con criptoactivos generalmente es la identificación del punto en el que el criptoactivo se cambia por moneda fiduciaria o por otro tipo de criptoactivo (FATF, Orientación sobre Investigaciones Financieras Involucrando Activos Virtuales. Enfrentando Desafíos con Investigaciones y Confiscaciones, mayo de 2019, p. 48).

43- El manual de implementación del RIF Análisis (Información 022/2020-SPPEA/PGR, PGR-00197821/2020) se puede solicitar a la SPPEA a través del correo electrónico pgr-atendimento-sppea@mpf.mp.br.

44- El COAF indica que para el intercambio de información que requiere información a través de la Red Egmont, además de la información y documentos ingresados para el intercambio nacional, se deben incluir en el campo "Detalles" del Sistema Electrónico de Información (SEI-C) los siguientes requisitos obligatorios: 1- Descripción de los objetivos con los respectivos elementos identificadores. En el caso de la investigación de una persona física o jurídica extranjera, la identificación puede hacerse en el propio texto, no siendo necesario listar el nombre en "Principales Relacionados". En este caso, incluir toda la información disponible, como nacionalidad y fecha de nacimiento para PF y dirección y número de registro para PJ. 2- Relación de los objetivos/hechos investigados con el país requerido. Es importante demostrar la relación existente entre el objetivo o el hecho investigado con el país que está siendo consultado. Las solicitudes genéricas, sin tal vinculación, no serán enviadas. 3- Resumen de los hechos/personas investigadas. El resumen debe contemplar al menos información sobre el delito investigado y el modus operandi. Si hay más de un objetivo listado, es importante describir la sospecha sobre cada uno de ellos (incluso si es solo una relación de parentesco). 4- Descripción de la información que se pretende obtener en el país requerido. Registrar específicamente lo que se espera del intercambio (por ejemplo, información sobre posibles movimientos sospechosos, información comercial, datos sobre el beneficiario final de una empresa, etc.). Si la solicitud se dirige a más de un país, describir separadamente lo que se desea de cada uno de ellos. Si la solicitud se refiere a transacciones financieras sospechosas específicas, favor incluir también la información disponible sobre la institución financiera extranjera, como el nombre del banco, el número de cuenta y el de la agencia.

Fuentes cerradas

Las fuentes cerradas se refieren, brevemente, a aquellas para las cuales el acceso necesita ser precedido de una autorización judicial (reserva de jurisdicción). En este campo se incluyen los datos financieros, fiscales, telemáticos, etc.

En el criptomercado, los datos resultantes de la eliminación del secreto telemático (gran fuente de prueba), asociados con las solicitudes de eliminación del secreto fiscal de la RFB y las operaciones de las exchanges (modelos de borrador del SIMBA) pueden ser de interés para la investigación.

- **Levantamiento del Secreto Financiero y Fiscal de Operaciones con Criptoactivos a través del SIMBA**

Actualmente, en el SIMBA existe la posibilidad de acceder a datos financieros de todos los mercados financieros (crédito, cambio, valores mobiliarios, seguros y previsión privada, y previsión cerrada), nuevos medios de pago (como PIX y los iniciadores de pago), sistemas informáticos de especial interés para la investigación financiera, datos fiscales y telemáticos con estrecha intersección con las transacciones financieras, y operaciones con criptoactivos.[45]

Específicamente en relación a las transacciones que involucran criptoactivos de investigados identificados civilmente (nombre, número de identificación tributaria o de personería jurídica – CPF y CNPJ, respectivamente en Brasil -, por ejemplo), pueden ser alcanzadas mediante la solicitud de los datos transmitidos por las exchanges a la Receita Federal do Brasil o, en caso de que el MPF conozca la exchange involucrada en la transacción, mediante la obtención de datos de transacciones intermediadas por estas plataformas electrónicas (exchanges) y en sus sistemas internos.[46]

45- Disponible en https://portal.mpf.mp.br/simba/php/Simba.php.

46- Como se explicó anteriormente, las exchanges poseen los datos y documentos de transacción en una especie de "libro mayor" de la empresa.

En el primer escenario, se trata de una solicitud de levantamiento del secreto fiscal de un investigado, dirigida a la Receita Federal do Brasil. Las exchanges de criptoactivos con domicilio tributario en Brasil están obligadas a informar a la RFB, mensualmente, las operaciones realizadas por sus clientes dentro de la plataforma, independientemente del valor operado (IN RFB 1888/2019, art. 6º)[4].[7]

Por su parte, el contribuyente (persona física o jurídica) domiciliado en Brasil tiene tres obligaciones fiscales relacionadas con criptoactivos: a) informar las operaciones a la RFB cuando, en el mes anterior, el total de operaciones realizadas fuera de las exchanges nacionales haya superado los R$ 30.000,00 (IN RFB 1888/2019, art. 6º, §1º); b) pagar impuestos sobre las ganancias de capital cuando, en el mes anterior, haya obtenido ganancias y el total de ventas de criptoactivos haya superado los R$ 35.000,00 (IN SRF 599/2005, art. 1º, II y Ley 8.981/95, art. 21); y c) completar la Declaración de Impuesto a la Renta. En el caso del IRPF, los criptoactivos deben ser registrados en la ficha de bienes y derechos (cód. 81, 82 y 89), y los ingresos por criptoactivos deben ser registrados como "ingresos no gravables" o "ingresos sujetos a tributación exclusiva".

Al final de esta Guía de Actuación se incluye un modelo para la solicitud de levantamiento del secreto fiscal de operaciones con criptoactivos en el SIMBA.

Por otro lado, si el MPF conoce la *exchange* involucrada en la transacción[48], puede solicitar el levantamiento del secreto telemático de las operaciones intermediadas por estas plataformas electrónicas (*exchanges*) y en sus sistemas internos. Esta relación entre los investigados y las *exchanges* puede surgir de otros elementos probatorios, como la identificación de las carteras en el análisis de los datos telemáticos obtenidos judicialmente.

47- Para la RFB, se considera criptoactivo "la representación digital de valor denominada en su propia unidad de cuenta, cuyo precio puede expresarse en moneda soberana local o extranjera, transaccionado electrónicamente con el uso de criptografía y de tecnologías de registros distribuidos, que puede utilizarse como forma de inversión, instrumento de transferencia de valores o acceso a servicios, y que no constituye moneda de curso legal" (artículo 5). De igual manera, la RFB considera exchange de criptoactivo "a la persona jurídica, aún no financiera, que ofrece servicios referentes a operaciones realizadas con criptoactivos, incluyendo intermediación, negociación o custodia, y que puede aceptar cualquier medio de pago, incluyendo otros criptoactivos". Se incluyen en el concepto de intermediación de operaciones realizadas con criptoactivos, la puesta a disposición de ambientes para la realización de operaciones de compra y venta de criptoactivo realizadas entre los propios usuarios de sus servicios.

48- La SPPEA tiene la lista compilada de los corredores de criptoactivos que operan en Brasil.

Al final de esta Guía de Actuación se incluye una modelo para el levantamiento del secreto bancario telemático de operaciones con criptoactivos utilizando el SIMBA y destinado a una exchange específica.

A partir del Parecer de Orientación n. 40/2022, la Comisión de Valores Mobiliarios consolidó la comprensión de que algunas operaciones con criptoactivos pueden configurarse como valores mobiliarios. Por lo tanto, aunque los criptoactivos no estén expresamente incluidos entre los valores mobiliarios citados en los incisos del art. 2º de la Ley nº 6.385/76, los agentes de mercado deben analizar las características de cada criptoactivo con el objetivo de determinar si es un valor mobiliario, lo que ocurre cuando: es la representación digital de alguno de los valores mobiliarios previstos taxativamente en los incisos I a VIII del art. 2º de la Ley nº 6.385/76 y/o previstos en la Ley nº 14.430/2022 (es decir, certificados por cobrar en general); o se encuadra en el concepto abierto de valor mobiliario del inciso IX del art. 2º de la Ley nº 6.385/76, en la medida en que sea un contrato de inversión colectiva.

Para estos casos, tanto el borrador simplificado como el completo del SIMBA[49] cubren este producto financiero, al solicitar acceso a los datos de las transacciones de títulos y valores mobiliarios realizados a través de sociedades intermediarias de títulos y valores mobiliarios (CTVM) y sociedades distribuidoras de títulos y valores mobiliarios (DTVM) integrantes del CCS.

Con las normas de la Ley n. 14.478/22, corresponderá a un órgano o entidad de la Administración Pública federal, definido en un acto del Poder Ejecutivo, establecer cuáles serán los activos financieros regulados, siendo posible que la futura regulación establezca nuevas posibilidades de acceso a datos financieros confidenciales de operaciones con criptoactivos.

49- Para las orientaciones sobre el uso del SIMBA, consulte la guía disponible en: https://portal.mpf.mp.br/novaintra/informa/2022/documentos/SIMBACartilhaparaMembros.pdf.

Dado que las operaciones con criptoactivos son operaciones financieras realizadas en plataformas electrónicas, parece natural que algunos de los datos telemáticos asociados puedan ser solicitados judicialmente, en particular la dirección de protocolo de internet (dirección IP) de acceso al proveedor de la aplicación del corredor de criptoactivos y los registros de acceso a la aplicación de internet mantenida por el corredor.[50]

En caso de incumplimiento injustificado de la orden judicial de entrega de los datos de las operaciones o de sospecha sobre la integridad de las operaciones de la exchange, se abre la posibilidad de realizar un allanamiento e incautación del personal de la exchange para realizar análisis forenses capaces de recuperar los datos necesarios para la investigación o documentar si los datos son efectivamente irreparables o si fueron borrados. Esta estrategia, naturalmente, no se puede aplicar a servicios instalados en la darknet, donde la ubicación de la infraestructura es desconocida o en países que tienen un historial de negarse a la cooperación judicial internacional.

Hay un problema adicional cuando se trata de exchanges descentralizadas. Aún hoy, la mayoría de las exchanges son centralizadas y almacenan información de los usuarios en un servidor centralizado. Sin embargo, desde 2012, la comunidad de criptoactivos ha estado desarrollando modelos de exchanges descentralizadas en las que la negociación puede ocurrir sin que los usuarios tengan que enviar sus criptoactivos a una entidad centralizada y todas las transacciones se vuelven transacciones P2P, es decir, entre particulares.

50- La migración de las transacciones financieras a soportes digitales significó que varios datos telemáticos se asociaron a información financiera. Estos datos telemáticos, recopilados por las instituciones financieras, pueden ser de interés para la investigación financiera y están sujetos al acceso por autorización judicial. A modo de ejemplo, los datos telemáticos que pueden ser accesibles por orden judicial son: a) la dirección del protocolo de internet (IP) de acceso al proveedor de aplicación de la institución financiera; b) los registros de acceso a la aplicación de internet mantenida por la institución financiera, que comprenden la información sobre la fecha y hora de uso de la aplicación de internet de la institución financiera desde las direcciones IP relacionadas con el investigado y mencionadas en el elemento anterior; c) el correo electrónico registrado por el usuario para acceder al servicio financiero digital; d) el terminal registrado (teléfono móvil, computadora, etc.); e) el tipo y versión de la aplicación utilizada; f) los datos de la tarjeta de crédito asociada al servicio financiero digital (nombre del titular, número de identificación fiscal, número de teléfono, dirección, número de la tarjeta, ingresos declarados y perfil de gastos); g) fotografías y filmaciones del momento de las operaciones indicadas, en caso de que se hayan realizado en cajeros automáticos (ATM). Es importante que el MPF especifique las transacciones para las que se busca la entrega de los datos telemáticos asociados, para agilizar la respuesta de la institución financiera. El modelo de la orden judicial para estas operaciones se encuentra en el SIMBA.

La Resolución RFB 1888/2019 ofrece una definición sobre este tipo de entidad en el artículo 5, párrafo único, al determinar que se incluyen en el concepto de intermediación de operaciones realizadas con criptoactivos la disponibilidad de ambientes para la realización de operaciones de compra y venta de criptoactivos realizadas entre los propios usuarios de sus servicios. La Ley 14.478/22 también considera prestador de servicio de activos virtuales a aquella persona jurídica que ejecuta, en nombre de terceros, entre otros, la participación en servicios financieros y prestación de servicios relacionados con la oferta por un emisor o venta de activos virtuales (artículo 5, inciso V).

Se puede imaginar que las exchanges descentralizadas, con infraestructura distribuida en muchas jurisdicciones alrededor del mundo y ningún órgano central que supervise transacciones, dificultará, por ejemplo, la obtención de información específica sobre transacciones.[51]

- **Levantamiento del Secreto Telemático**

En una investigación sobre criptoactivos, puede haber necesidad de formular pedidos de preservación de datos telemáticos y apartamiento de secretos de datos telemáticos diversos de aquellos asociados a transacciones financieras ya constantes de la minuta del SIMBA. Para ello, las orientaciones están compiladas en el portal e-Evidence, mantenido por el Grupo de Apoyo a la Criminalidad Cibernética, en rutas objetivas: *HTTPS://PORTAL.MPF.MP.BR/EEVIDENCE*

- **Precauciones con Seeds y Claves Privadas Encontradas**

Conforme visto anteriormente, el acceso a seeds y claves privadas da acceso a la movilización de los criptoactivos. A diferencia de la investigación tradicional, donde los valores están custodiados en instituciones financieras centralizadas, aquí cualquier persona que tenga acceso a esta información podrá movilizar el activo.

51- FATF, Guía para Investigaciones Financieras Involucrando Activos Virtuales. Abordando Desafíos en Investigaciones y Confiscaciones, mayo de 2019.

Durante la investigación criminal, a partir de las medidas de levantamiento de secreto mencionadas anteriormente, es posible encontrarse con seeds, passphrases, claves privadas y contraseñas (claves de acceso) antes incluso del despliegue de una medida ostensiva. Es común que los investigados almacenen esta información en la nube, por lo que es accesible mediante la simple violación de la privacidad telemática.

Si se encuentran claves de acceso durante la fase encubierta de la investigación, es importante considerar la necesidad de incautar los criptoactivos inmediatamente, en comparación con la posibilidad de esperar un momento más apropiado para el despliegue de la operación policial.

En estas situaciones, nos parece ser la postura más adecuada registrar todo lo que se encuentre de manera detallada y llevarlo inmediatamente al conocimiento del juez competente, para que se pueda hacer una evaluación de conveniencia y oportunidad, clasificando el documento con el máximo grado de confidencialidad.

De hecho, este análisis es fundamental, ya que las diligencias pueden estar en curso y la inmediata incautación de los activos puede alertar a los objetivos de la existencia de cautelares, frustrando otras medidas.

ALLANAMIENTO E INCAUTACIÓN DE CRIPTOACTIVOS

Las claves de acceso a criptoactivos pueden estar almacenadas en diversos dispositivos físicos electrónicos, como hardwallets, computadoras y teléfonos celulares, o incluso impresas o anotadas en papel. Por lo tanto, la diligencia de allanamiento e incautación puede dar resultados muy fructíferos en investigaciones que involucren criptoactivos.

Sin embargo, para el éxito de la diligencia, es imprescindible una fase previa de preparación y la adopción de algunos cuidados durante las búsquedas, de manera que los criptoactivos encontrados puedan ser efectivamente incautados por el Estado.

PREPARACIÓN PARA EL ALLANAMIENTO PRESENCIAL

En el caso de investigaciones en las que exista la sospecha de utilización de criptoactivos, es esencial que el representante del Ministerio Público Federal y la Policía Federal proporcionen la creación de una cartera controlada por el Estado para que los criptoactivos encontrados en el momento de la búsqueda presencial puedan ser inmediatamente transferidos a la custodia estatal.

Es imposible precisar qué tipos de criptoactivos se encontrarán en las búsquedas, pero a través de las diligencias remotas tratadas en el tema anterior, es posible prever las especies de criptoactivos utilizadas habitualmente por el investigado.

De cualquier manera, se sugiere que se creen previamente direcciones de al menos Bitcoin y Ethereum.

Estas direcciones pueden ser abiertas en forma de una cuenta en una bolsa de valores nacional, previa autorización judicial, o pueden ser direcciones de carteras propias, preferiblemente hardwallets, cuyas claves privadas/frase de recuperación estén bajo la custodia de agentes públicos.[52]

En este último caso, es fundamental que los involucrados en el cumplimiento de la medida de allanamiento e incautación conozcan el riesgo de un eventual filtrado o compartición indebido de las claves privadas o de la frase de recuperación de las carteras bajo la responsabilidad del Estado, ya que cualquier persona con acceso a estas claves podrá mover libremente los criptoactivos incautados a cualquier otra dirección. Peor aún: protegido por el seudónimo del Blockchain.

Una vez establecido un mecanismo para la custodia de los criptoactivos eventualmente incautados, es imprescindible designar una persona o equipo (punto focal) para estar en alerta remota durante las diligencias, con acceso a una computadora, internet, dirección de la cartera estatal y algún software que permita la recuperación remota de carteras de criptoactivos, como por ejemplo, el Coinomi[53]. Esta persona o equipo será responsable de realizar la inmediata transferencia de los criptoactivos encontrados con los investigados a la cartera estatal.

Esta medida es esencial para el éxito de las diligencias, teniendo en cuenta la posibilidad de movimiento remoto de los criptoactivos por cualquier otra persona que tenga una copia de las claves privadas, que no son más que un código.

52- Aunque hay discusión en el Consejo de Justicia Federal (CJF) sobre la incautación de activos virtuales, aún no hay regulación que regule su custodia. En el proyecto de regulación del CJF, se prevé que los tribunales acrediten a las exchanges, "que serán responsables de crear, por orden judicial, una cartera (wallet) para almacenar temporalmente los activos virtuales en procesos e investigaciones". Técnicamente, esta es una de las soluciones posibles, siendo la otra que algún agente público o (grupo de agentes públicos) asuma la custodia de estos activos, como se indicó en el párrafo anterior. Lo que parece claro es que su custodia no debe ser responsabilidad del MPF, que no tiene el deber de ser depositario judicial.

53- https://www.coinomi.com/downloads/

EJECUCIÓN DE ALLANAMIENTO PRESENCIAL

Durante las diligencias de allanamiento e incautación es imprescindible que los equipos estén atentos a las anotaciones, impresas o manuscritas, que puedan configurar frases de recuperación (seed phrases), conjuntos de 12 a 24 palabras, o combinaciones de direcciones y claves privadas de criptoactivos, además de dispositivos físicos (hardwallets) que almacenan las claves privadas.

Como se destacó en la parte inicial de este guion de actuación, la mera incautación de dispositivos electrónicos de almacenamiento de claves privadas (hardwallets) no garantiza la incautación de los criptoactivos. Para que esto ocurra, es necesario que se llegue a las claves privadas y/o a la seed phrase.

Así, incluso si se encuentra una seed en la casa de un objetivo, que ha sido arrestado en una operación, un cómplice que no ha sido afectado por la medida cautelar puede mover libremente los activos, si tiene en su posesión las mismas palabras claves. Se recomienda un cuidado especial con las seed phrases y claves privadas, que no deben ser compartidas, pues, como ya se ha advertido, cualquier persona que tenga esta información puede mover los criptoactivos.

Ejemplo: Orden de allanamiento e incautación realizada a las 6h con la incautación de claves de acceso. En circunstancias ideales, a las 6:30 a. m. estos recursos ya deben haber sido transferidos a claves públicas en poder de las autoridades. Es decir, antes de que la medida cautelar haya sido publicada para los cómplices del objetivo o en la prensa. Si esto no se hace, un cómplice puede, desde cualquier lugar del mundo, recuperar los activos y transferirlos a direcciones que no pueden ser objeto de bloqueo.

De esta forma, es fundamental que después de la recuperación de las claves de acceso se siga la transferencia de los fondos a una cartera en posesión de las autoridades

o a la cuenta de alguna exchange nacional, de acuerdo con lo que haya sido autorizado por la Justicia.

En los mismos términos que con la incautación de activos tradicionales, la medida debe ser llevada a cabo por la Policía Federal, de manera documentada, para preservar la cadena de custodia de las pruebas y el rastreo de los activos. Es importante también detallar en el informe de la diligencia todo lo que se realizó en el lugar y las personas presentes.

Otro punto a considerar con mucha atención es la compartimentación de la información sobre las claves de acceso. Como el acceso a estos datos permite el control de los activos, es fundamental que el menor número posible de personas (tanto en el ámbito del Ministerio Público, la Policía y el Poder Judicial) tenga acceso a dicha información.

Por último, considerando que las claves privadas de los criptoactivos pueden estar almacenadas en computadoras y teléfonos móviles, se recomienda solicitar prioridad al departamento de pericias de la Policía Federal para la extracción y copia de los elementos electrónicos incautados, de manera que sea posible el análisis del material en busca de posibles contraseñas y claves privadas.

SECUESTRO E INHIBICIÓN DE CRIPTOACTIVOS

Los casos de secuestros e inhibiciones, civiles y penales, de activos y las respectivas hipótesis en que corresponden fueron delineados en la Guía de Persecución Patrimonial y Administración de Bienes, específicamente en los capítulos V y VI, elaborado por el grupo de trabajo instituido por las 2ª y 5ª Cámaras de Coordinación y Revisión[54]. Estas medidas de coacción se constituyen en poderosas herramientas de combate a la delincuencia económica, con eficacia a veces superior a las tradicionales penas privativas de libertad.

El caso concreto determinará qué tipo de medida restrictiva patrimonial es aplicable y su respectiva fundamentación jurídica. También se debe prestar atención a las hipótesis de enajenación anticipada y a las buenas prácticas para la administración de bienes, tratadas, en lo que se refiere a criptoactivos, en el presente manual.

De acuerdo con el tipo de secuestro e inhibición adoptado, el miembro del MPF debe solicitar en el juicio la restricción de los bienes de los demandados, emitiendo una orden de restricción de **criptoactivos**, **monedas electrónicas** u **otros valores custodiados por cualquier título,** incluyendo **la congelación de eventuales órdenes de retiro en moneda corriente o criptoactivos**, hasta el valor determinado, eventualmente existente en las *exchanges* nombradas.

54- BRASIL. Ministerio Público Federal. 2ª Cámara de Coordinación y Revisión. Guía de Actuación – Persecución Patrimonial y Administración de Bienes, 2017. Disponible en: https://portal.mpf.mp.br/novaintra/areas-tematicas/camaras/criminal/publicacoes/roteiros-de-atuacao-restrito/roteiro_atuacao_persecucao_patrimonial.

Asimismo, es importante solicitar al juez que adopte algunas medidas para la efectividad de la orden judicial. En primer lugar, que la orden de secuestro indique que el MPF y la Policía Federal podrán llevar a cabo el cumplimiento de las órdenes de secuestro directamente en contacto con los corredores o, en caso de que no sean atendidos, inspeccionar la propia sede de las empresas en busca de activos. La medida se justifica para agilizar el cumplimiento de la orden en caso de que el Poder Judicial tenga dificultades para llevarla a cabo. En segundo lugar, que los corredores destinatarios de la orden realicen la transferencia de los valores a la cartera previamente creada y bajo el control del Estado, según se aborda en un tema anterior de este manual.

Finalmente, se debe tener en cuenta que el secuestro no siempre tiene que recaer solo en los criptoactivos del demandado, e incluso es prudente para la efectividad de la restricción, la acumulación de solicitudes tradicionales de secuestro de activos[55] con las solicitudes especiales de secuestro de criptoactivos mencionados anteriormente.

55- Tales como el embargo en línea, previsto en el artículo 854 del Código Procesal Civil e instrumentado por el Sistema de Búsqueda de Activos del Poder Judicial - SISBAJUD; el bloqueo vía RENAJUD de todos los vehículos registrados a nombre de los demandados; el bloqueo de embarcaciones y aeronaves eventualmente registradas a nombre de los requeridos, con la expedición de oficio a la Capitanía de los Puertos y a la ANAC (Agência Nacional de Aviação Civil) para efectuar la medida; el bloqueo de bienes inmuebles registrados a nombre de los demandados, insertando la orden de restricción en la CNIB - Central Nacional de Inhibición de Bienes.

ENAJENACIÓN DE CRIPTOACTIVOS

Una vez realizada la incautación y transferencia de los criptoactivos, surgen preguntas sobre el momento de su venta, particularmente si debe realizarse una venta anticipada o esperar el resultado del proceso penal para convertir los criptoactivos en moneda fiduciaria.

Los efectos prácticos de esta discusión se refieren a la gran volatilidad del precio de los criptoactivos. En un corto período de tiempo, a veces incluso en cuestión de segundos, el precio de un determinado criptoactivo puede sufrir severas oscilaciones. A modo de ejemplo, véase la variación de los valores de Bitcoin en el período del 01/01/2021 al 31/12/2022[56] (los valores en la columna de la izquierda están en dólares):

56- https://coinmarketcap.com/currencies/bitcoin/?period=7d

De acuerdo con el gráfico anterior, extraído del sitio web Coinmarketcap.com, el valor más bajo de la cotización de Bitcoin en 2021 ocurrió el 20 de julio, cuando se negoció a $29,807.35[57], y el valor máximo se alcanzó el 8 de noviembre a $67,566.83. Por lo tanto, hubo una apreciación del 226.67% del valor más bajo al más alto de la cotización en 2021, en un lapso de menos de 4 meses. Sin embargo, los últimos 45 días del año mostraron una fuerte caída en la cotización de Bitcoin, que cerró el año en $46,306.45.

La gran volatilidad de Bitcoin, que se muestra aún más acentuada en otros criptoactivos, es uno de los indicativos de su uso masivo con fines especulativos. Este panorama puede producir, en la práctica, grandes diferencias de valores al comparar la fecha de adquisición y la fecha de conversión efectiva en moneda soberana, lo que puede implicar una apreciación o no.

Cabe destacar la existencia de las stable coins, una modalidad de criptoactivos que, en teoría, no están sujetos a la volatilidad. Las stable coins son criptoactivos que vinculan su valor a una moneda soberana emitida por el Estado, normalmente el dólar. Ejemplos son Tether (USDT), Gemini Dollar (GUSD), Dai (DAI), USD Coin (USDC), Binance USD (BUSD) y True USD (TUSD), criptoactivos que igualan su valor al dólar, de modo que una unidad de cada uno de estos criptoactivos vale 1 dólar. Para alcanzar esta paridad existen diferentes técnicas, como la emisión de criptoactivos vinculados al depósito de moneda soberana, la programación de smart contracts y algoritmos que controlan la compra y venta de los activos.[58]

Las stable coins han recibido especial atención por parte de las autoridades, especialmente de los organismos estatales de regulación del mercado financiero. En los Estados Unidos, Tether fue multado con $42.5 millones por la Commodity Future Tradings Commission (CTFC), un organismo administrativo nacional, debido a fraudes relacionados con las garantías de su emisión.[59]

57- Todos los valores están fijados en dólares estadounidenses.

58- Puede encontrarse más información en https://www.gemini.com/cryptopedia/what- arestablecoins-how-do-they-work

59- https://www.cftc.gov/PressRoom/PressReleases/8450-21

Como se indicó antes, en cuanto al momento de la enajenación, se debe definir entre mantener los criptoactivos custodiados durante el proceso o realizar su enajenación anticipada. En la primera situación, solo al final del proceso penal, con la confirmación definitiva de la sentencia penal condenatoria, se determinaría su enajenación judicial, con la consecuente conversión a moneda soberana, según la cotización de la respectiva fecha. Por otro lado, con la enajenación anticipada, habría una conversión a moneda fiat aún durante el proceso, de acuerdo con el artículo 144-A del Código Procesal Penal.

En búsqueda de una solución para la definición del momento de la enajenación, el Código de Proceso Penal, en su artículo 144-A, primer párrafo, parte final, en la forma de la redacción dada por la Ley n.° 12.694/2012, autoriza la enajenación anticipada siempre que haya dificultad para el mantenimiento de los bienes incautados:

> *“"Art. 144-A: El juez determinará la enajenación anticipada para preservación del valor de los bienes siempre que estén sujetos a cualquier grado de deterioro o depreciación, o cuando haya dificultad para su mantenimiento" – subrayado nuestro.*

Como se vio en el propio tema, la incautación y custodia de criptoactivos exigen preparación y cuidados específicos para evitar la frustración de las diligencias. Dado el carácter digital, transfronterizo, descentralizado e irreversible de las operaciones que involucran criptoactivos, son imprescindibles medidas especiales para garantizar el efectivo control de los valores que representan.

Ya sea que los criptoactivos estén bajo custodia de una exchange nacional o en una cartera propia del Estado, existirán riesgos en su mantenimiento que no se limitan al riesgo de mercado, es decir, a la volatilidad del precio. La realidad es pródiga en ejemplos, tanto de problemas relacionados con grandes exchanges[60] como de problemas relacionados con la custodia propia de usuarios experimentados[61].

60- https://www.seudinheiro.com/2021/bitcoin/bitcoin-africa-do-sul-desaparece-24-06/ https://canaltech.com.br/criptomoedas/quadriga-conspiracy-a-suposta-morte-do-ceo-e-o-misterio-de-us-190- milhoes-132453/

61- https://www.correiobraziliense.com.br/mundo/2021/07/4937888-bitcoins-bilionario-que-morreu-afogadodeixa-no-limbo-fortuna-de-rs-11-bilhoes-em-criptomoeda.html https://www.istoedinheiro.com.br/investidor-esquece-senha-de-conta-com-us-240-milhoes-em-bitcoin/

De esta manera, ya sea debido a la alta volatilidad de los precios o a las especificidades técnicas relacionadas con la seguridad de la custodia de los criptoactivos, sus características propias demuestran que son bienes de difícil mantenimiento, lo que autoriza, de acuerdo con el artículo 144-A del CPP, la venta anticipada.

Al igual que otros países, entre ellos Suiza y Alemania[62], Brasil tampoco cuenta con una legislación específica sobre la venta de criptoactivos incautados.

A pesar de ello, hay fundamentos técnicos y jurídicos para que la venta anticipada se realice en base al artículo 144-A del CPP, como se vio en el apartado anterior.

En términos prácticos, a diferencia de lo que ocurre con monedas extranjeras, títulos de crédito negociados en bolsa, títulos de la deuda pública, acciones y otros valores mobiliarios, no existe una institución equivalente a Caixa Econômica Federal para recibir los criptoactivos y realizar el cambio a una cotización oficial[63].

Técnicamente, consideramos que las dos alternativas más viables son: la venta en subasta, en la forma del artículo 879 y siguientes del CPC; y la venta a través de exchanges nacionales. En la práctica, sin embargo, entendemos que es preferible que la venta se realice de la segunda forma, es decir, a través de exchanges nacionales[64], sobre todo cuando se tiene en cuenta el principio de eficiencia (CPC, artículo 8). Esto se debe a que, además de que la tarifa cobrada por las exchanges es menor que la del subastador, la posibilidad de obtener un precio de venta más alto es inmensamente mayor en los libros de ofertas que en las subastas [65].

62- Esto también ocurre en otros países, que no tienen, al igual que Brasil, una regulación propia sobre la restricción patrimonial de criptoactivos. Suiza y Alemania, por ejemplo, utilizan sus normas procesales penales sobre incautación y secuestro, según un cuestionario enviado por el GT Criptoactivos a esos respectivos países, disponible de forma restringida en la Secretaría de Cooperación Internacional/PGR. En este primer país, surgió el debate sobre la enajenación en la alza de los criptoactivos, lo que sería problemático en Brasil por falta de regulación legal, sin entrar en el debate sobre si esta práctica permitiría, en caso de grandes incautaciones y enajenaciones, que la exchange encargada acabara compitiendo para la fluctuación de los valores y aún si, de alguna manera, el Estado no estaría asociado a una práctica especulativa e incompatible con la adoptada con otros activos volátiles, como valores mobiliarios y monedas extranjeras (FIAT). Consulte la Decisión 1B_59/2021 del 18 de octubre de 2021, del Tribunal Supremo Suizo en https://archipel.law/en/insights/the-early-liquidation-of-crypto-assets-and-the-need-for-crypto-expertise//

63- Resolución nº 428/2005 del CJF, art. 1, inciso VI.

64- Práctica también adoptada en Estados Unidos:: https://www.cnbc.com/2021/07/28/us-marshalsservice-hires-custodian- to-hold-crypto-seized-in-criminal-activity.html

65- No se desconoce la existencia de países que ya han realizado la enajenación de criptoactivos vía subastas conducidas por casas especializadas. Cf.: https://www.irishnews.com/business/2019/10/01/news/wilson-auctionsoff-500-000-of-bitcoin-seized-from-uk-criminal-1726231/

No existe un procedimiento previsto para la elección del exchange a través del cual se realizará la enajenación. Ante esta situación, se sugiere el uso de criterios objetivos en la elección de los exchanges, como la tasa cobrada, el volumen de negociación, etc., y la presentación de la elección al juez.

Por último, es deseable adoptar estrategias que, en colaboración con la exchange, permitan obtener el mejor precio medio. A continuación, se presenta el ejemplo de la estrategia homologada judicialmente el 14/07/2021 para la enajenación de casi 30 bitcoins, incautados en el proceso nº 5004543-34.2019.4.02.5001, tramitado en la Justicia Federal de Espírito Santo. En ese caso, se establecieron los siguientes parámetros para la venta:

1. Los BTC se enajenarán de manera fraccionada (10 lotes, siendo los primeros 9 de 3 BTC y el último por el valor remanente);

2. La venta de cada lote se realizará mediante la presentación de una única orden de venta en el libro de ofertas, por el valor total del lote en BTC, con un precio límite no inferior al 2% del precio de mercado, entendido como el precio correspondiente a la última operación realizada a través del libro de ofertas;

3. Si la orden de venta con precio límite no se completa completamente en hasta treinta minutos, se puede lanzar una nueva orden de venta por el valor restante del lote, siguiendo la misma directriz anterior (ítem 2);

4. Una vez finalizada la venta de un lote, se puede lanzar la orden correspondiente al siguiente lote sin la necesidad de respetar un intervalo mínimo, pero siempre cumpliendo con los mismos parámetros definidos en el ítem 2.

El objetivo fue no afectar negativamente el precio del bitcoin en el libro de ofertas del exchange, lo que ocurriría si se realizara la enajenación de todos los bitcoins de una sola vez o en un intervalo de tiempo muy corto.

DEFI Y SUS PARTICULARIDADES

DeFi es el acrónimo de Decentralized Finances (Finanzas Descentralizadas) y denomina una especial categoría de aplicaciones ejecutadas[66] en ambientes descentralizados, los llamados DApps (decentralized applications), cuyo objetivo es facilitar servicios financieros, como préstamos, seguros y provisión de liquidez.

Para comprender lo que son DApps, retomemos la comparación que hicimos entre, por un lado, el bitcoin-hardware/bitcoin-software y, por el otro, el notebook/su sistema operativo (Windows o Linux). En esta comparación, el bitcoin-software es como un sistema operativo que presenta funcionalidades, pero que no fue diseñado para acomodar la instalación de programas.

A partir de Ethereum, el primer Blockchain programable que surgió, este escenario cambia drásticamente, y el Windows de nuestra comparación pasa a ser un sistema operativo pensado y concebido para alojar la instalación de programas que se ejecutan sobre él.

En este nuevo escenario comparativo, el Ethereum-hardware se asemeja al Notebook, el Ethereum-software a Windows y los DApps a cualquier programa que se ejecute en Windows, como Word, Google Chrome y Zoom.

Al igual que los programas de nuestro ejemplo (Apps) pueden clasificarse en diversas categorías, basadas en el servicio que proporcionan,

66- Programas, aplicaciones y aplicativos son palabras sinónimas en este contexto.

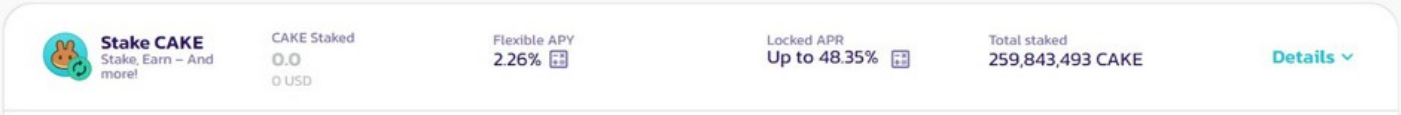
(edición de textos, la navegación web, la videoconferencia, etc.). Los DApps también pueden ser clasificados. Una de las especies resultantes del uso de este criterio clasificatorio son los DApps de DeFi.

Los programas que se ejecutan localmente en su notebook, como Word y Chrome, dependen de una instalación local. Por otro lado, los programas que se ejecutan de forma descentralizada dependen de la instalación en el Blockchain. Instalar un programa en la máquina virtual de Ethereum (EVM: Ethereum Virtual Machine) en la computadora mundial descentralizada es exactamente lo mismo que implementar un contrato inteligente en el Blockchain de Ethereum.

Sin embargo, se debe hacer una aclaración adicional: los contratos inteligentes son programas que se ejecutan en los Blockchains y no son contratos ni son inteligentes en el sentido común del término. Son simplemente programas que ejecutan aquello para lo que fueron programados para hacer (autoejecutables).

En un “contrato inteligente”, cada vez que se cumple la condición A, se produce el resultado B. Son programas escritos en la forma de una condición SI → ENTONCES (IF → THEN).

El siguiente ejemplo ilustrará por qué es importante comprender este tema.



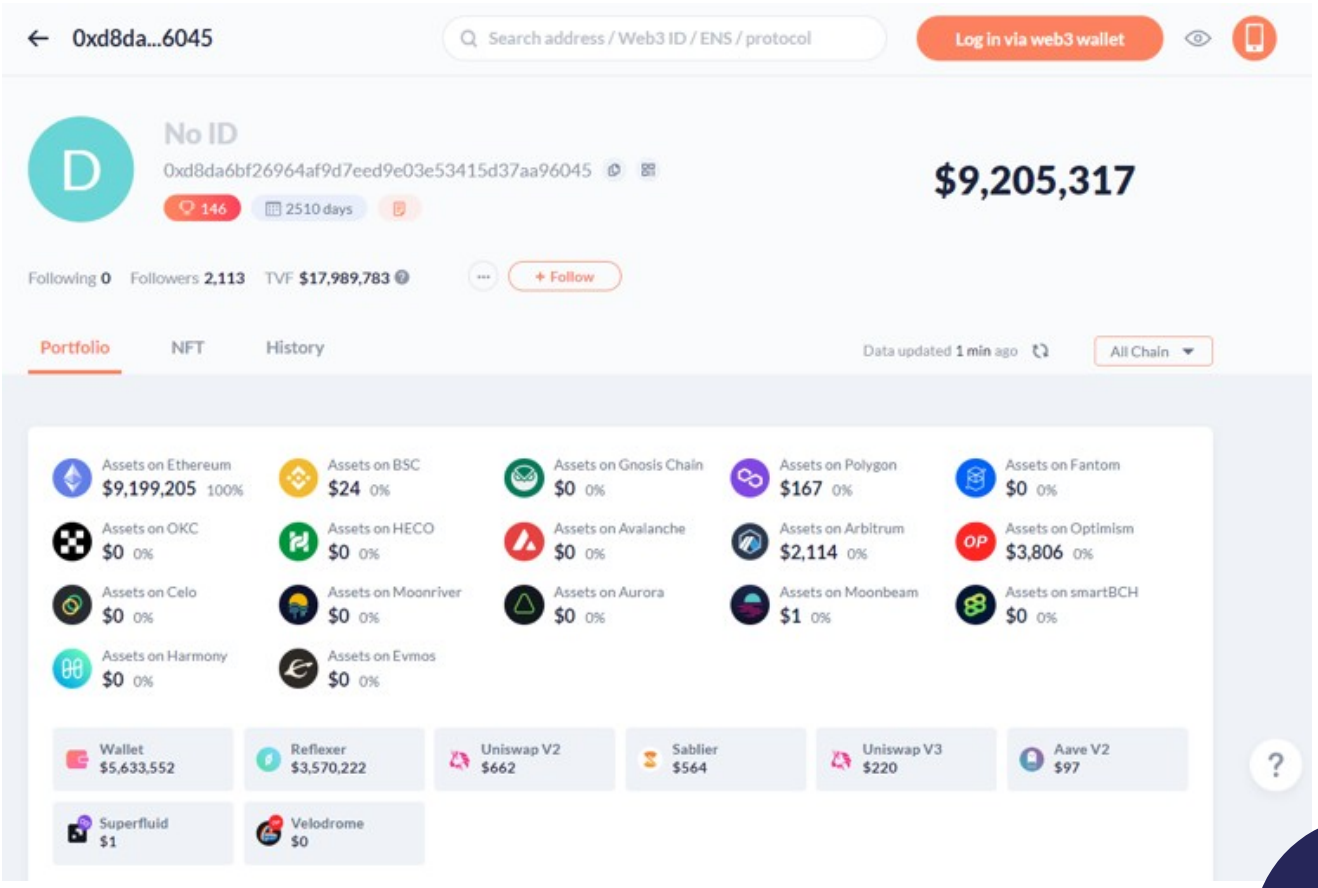
La imagen reproduce una aplicación de DeFi que, para aquellos que bloqueen (stake) tokens CAKE (SI), otorga rendimientos (yield) anualizados de hasta el 48.35%, en tokens CAKE (→ ENTONCES).

Por "stake" se entiende el envío de tokens CAKE desde su cuenta a la cuenta del contrato inteligente que le remunerará.

La consecuencia práctica es que, a partir de ese envío, los tokens ya no estarán en su dirección sino en la dirección del contrato inteligente. Su clave privada permitirá, entonces, no el envío inmediato de esos tokens a otra dirección, sino la recuperación de esos tokens, algo similar a un rescate de los tokens invertidos.

Imaginemos, entonces, que esta sea la situación del objetivo de una investigación patrimonial. Incluso si su dirección pública es conocida, los tokens "invertidos" no se encontrarán allí, porque estarán en las direcciones de contratos inteligentes de DApps de DeFi.

Sin embargo, esta dificultad se puede superar. Los tokens pertenecientes al objetivo, temporalmente ubicados en alguna de las principales direcciones de contratos inteligentes de DeFi, pueden ser fácilmente encontrados mediante el uso de herramientas en línea gratuitas como https://debank.com/ y https://apeboard.finance/.



En otras palabras, el objetivo no solo posee criptoactivos que se encuentren en sus direcciones públicas, sino también aquellos vinculados a sus direcciones públicas que, temporalmente, se encuentren en contratos inteligentes DeFi.

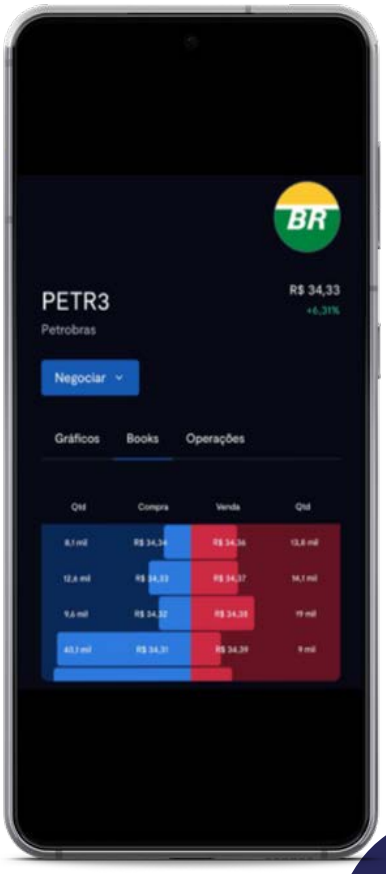
Ante esto, cualquier medida de investigación o restricción patrimonial que recaiga sobre criptoactivos custodiados por el objetivo debe considerar la posibilidad de que una parte considerable de ellos se encuentre temporalmente en otras direcciones públicas.

NFTS Y SUS PARTICULARIDADES

NFT es la sigla de non-fungible tokens. En traducción literal, son tokens no fungibles. Si los tokens son activos digitales que no pueden ser copiados, los tokens no fungibles son activos digitales que, además de no poder ser copiados, son únicos, irreemplazables.

Las criptomonedas y los tokens fungibles en general se pueden negociar en los libros de órdenes de las exchanges, de la misma manera que las acciones se negocian a través de los libros de órdenes en la B3. Por otro lado, los NFTs no pueden - al igual que los bienes inmuebles y las obras de arte - ser negociados a través de un libro de órdenes, aunque la legislación lo permita.

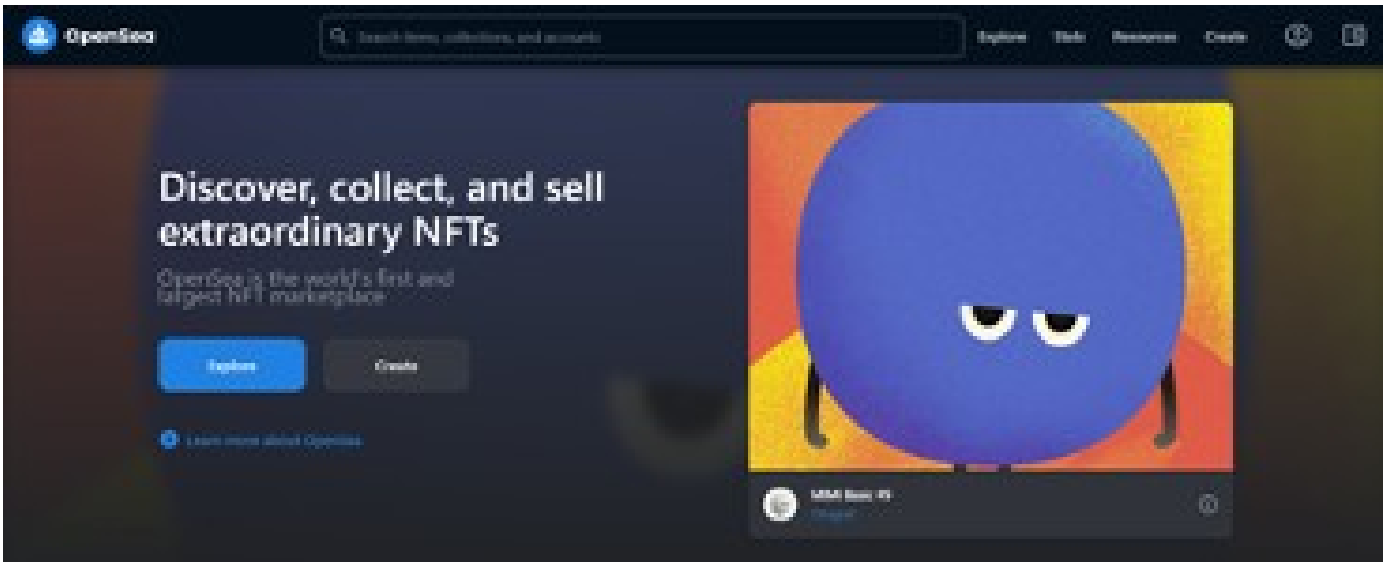
Esto se debe a que los bienes inmuebles y las obras de arte son bienes únicos, es decir, no fungibles. Y el libro de órdenes es un instrumento para reunir intereses contrapuestos relativos a un par de cosas fungibles. Veamos el siguiente ejemplo.



En la imagen adjunta vemos el libro de órdenes (book) del par de negociación BRL (real) y PETR3 (acciones ordinarias de Petrobrás). Recurren a él las personas que quieren intercambiar reales por acciones o acciones por reales, ambos bienes fungibles, no únicos. Un real equivale a otro real. Una acción equivale a otra acción.

Los bienes inmuebles y las obras de arte pueden ser puestos en venta directamente por sus propietarios o pueden recurrir a un intermediario, como una inmobiliaria o una galería de arte. De manera similar, los NFTs pueden ser puestos en venta directamente por sus propietarios. Sin embargo, lo más común es que se pongan a la venta a través de un intermediario, una plataforma que, sin hacer la custodia de estos NFTs, les brinde mayor visibilidad y, sobre todo, seguridad en la negociación.

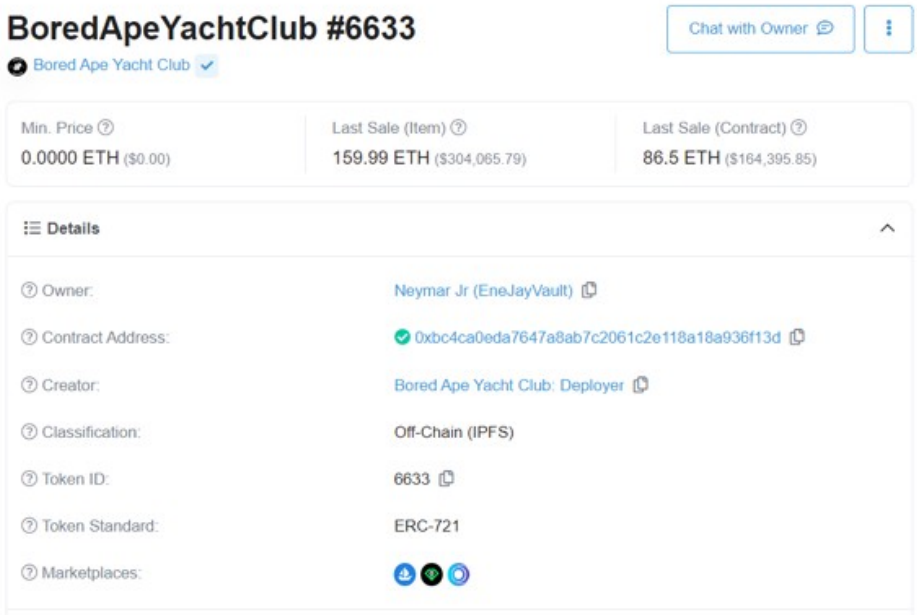
A estas plataformas se les llama marketplaces y la principal de ellas, con amplia ventaja, es Opensea (https://opensea.io/).



No hay nada que particularice la custodia de los NFTs. La diferencia práctica entre los tokens fungibles y los NFTs que nos interesa consiste en la forma de enajenación, siendo que los primeros tienen como lugar más propicio de enajenación los libros de órdenes de las exchanges y los segundos pueden ser enajenados a través de mercados.

Los NFTs no son figuritas. Son, en cambio, un objeto digital único. Y este objeto digital único no es el medio que pueda estar asociado a él, sino un identificador único en la cadena de bloques (Blockchain).

La imagen de arriba no es un NFT. Es el medio asociado al NFT BAYC #6633, que forma parte de la colección Bored Ape Yacht Club y actualmente pertenece al jugador de fútbol Neymar. Técnicamente, la imagen reproducida arriba puede ser copiada libremente por terceros y no tiene nada de no fungible.



La captura de pantalla anterior, por otro lado, expone los datos del NFT mencionado. Un token con identificación única (6633), vinculado a un contrato inteligente (0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d), implementado en un Blockchain (Ethereum).[67]

Los NFT son la no fungibilidad del mundo real llevada al mundo digital. Al igual que los documentos originales, las propiedades y las obras de arte son fundamentalmente diferentes entre sí, a pesar de ser todos bienes no fungibles, los NFT también pueden serlo.

Algunos de estos NFT pueden no tener ningún valor de mercado (por ejemplo, documentos), mientras que otros pueden tener un valor inmenso (por ejemplo, propiedades virtuales y artículos de colecciones famosas).

En cuanto a lo que nos interesa, la manera más efectiva de enajenar los NFT que se encuentran en las carteras de los objetivos es a través de marketplaces, debido a su no fungibilidad, y no se debe recurrir a intercambios en este caso.

67- Curiosamente, esta imagen del mono ni siquiera está en la cadena de bloques. Está en un servicio de almacenamiento distribuido llamado IPFS, y lo que hace el NFT en verdad es señalar la ubicación (off-chain).

MODELOS

LEVANTAMIENTO DEL SECRETO FISCAL DE OPERACIONES CON CRIPTOACTIVOS EN EL SIMBA

De esta forma, el Ministerio Público Federal solicita, en virtud del artículo 198 del Código Tributario Nacional, la orden de levantamiento del secreto fiscal de las personas físicas y jurídicas enumeradas en la siguiente lista, durante el período especificado:

(lista generada por el SIMBA con nombre, CPF/CNPJ y período)

Con respecto a estos investigados, la Receita Federal do Brasil debe suministrar, en un plazo de 30 (treinta) días a partir de la recepción de la orden judicial, toda la información disponible relacionada con criptoactivos, como: a) declaraciones de operaciones con criptoactivos (informadas por el contribuyente o por intercambios nacionales); b) documentos relacionados con el pago de impuestos sobre las ganancias de capital devenidas de la venta de criptoactivos, y c) declaraciones de impuestos a las ganancias con información sobre criptoactivos.

Para la ejecución de la orden judicial, se requiere:

I – Que la orden judicial establezca la obligación de que la Receita Federal do Brasil envíe los datos y documentación complementaria en formato .txt, .cvs, .xlsx o, si no es posible, en formato .pdf, a través del SIMBA, haciendo referencia al caso Simba 001-MPF-00XXXX-XX, utilizando el programa "VALIDADOR BANCÁRIO SIMBA" en la opción "TRANSMISIÓN DE DOCUMENTOS", cuyas instrucciones se encuentran en la dirección electrónica https://asspaweb.pgr.mpf.mp.br;

II – Que la orden judicial establezca que, en caso de dudas por parte de las instituciones destinatarias, la dirección electrónica para contactar a la Secretaría de Pericias, Investigación y Análisis - SPPEA/PGR es pgr-simba@mpf.mp.br.

LEVANTAMIENTO DEL SECRETO TELEMÁTICO DE LAS OPERACIONES CON CRIPTOACTIVOS EN EL SIMBA (EXCHANGES)

De esta manera, el Ministerio Público Federal solicita, con base en la Ley N° 12.965/14 (Marco Civil de Internet), la orden de levantamiento del secreto telemático de las personas físicas y jurídicas enumeradas en la lista a continuación, por el período indicado:

(lista generada por el SIMBA con nombre, CPF/CNPJ y período)

I. Con respecto a estos investigados, el corredor de criptoactivos (...), deberá enviar en un plazo de 30 (treinta) días desde la recepción de la orden judicial:

a) todos los datos y documentos de registro propios y de apoderados habilitados para el uso de sus cuentas;

b) información sobre todas las operaciones realizadas por ellos (ya sea en criptoactivos o en moneda fiduciaria), en una planilla que contenga un campo con el valor en REAL correspondiente a cada operación con criptoactivos en el momento de su realización;

c) sobre cada operación, también se debe informar el valor correspondiente en dólares estadounidenses en el momento de la transacción y el saldo restante después de la transacción, así como:

- Fecha y hora;
- Identificación del activo y cantidad;
- Identificación del remitente y destinatario (incluyendo cuenta bancaria o dirección cripto);
- Identificación del remitente y destinatario (incluyendo cuenta bancaria o dirección cripto);
- Valor correspondiente en REAL (en la fecha y hora de la transacción);
- Red (cripto) y Banco (corresponsal bancario), según el caso (involucramiento de criptoactivos y/o moneda fiduciaria en la operación);
- ID de hash de la transacción.

d) información sobre el saldo actual de cada uno de los investigados, discriminado por moneda fiduciaria o especie de criptoactivo, en este último caso con valor actual referenciado en REAL.

II. Para la ejecución de la orden judicial, se requiere que:

a) Se incluya en la orden judicial la obligación del corredor de criptoactivos de enviar los datos y documentación complementaria, en formato .txt, .cvs, .xlsx o, en caso de imposibilidad, en .pdf, a través del SIMBA, en referencia al caso Simba 001-MPF-00XXXX-XX, utilizando el programa "VALIDADOR BANCÁRIO SIMBA", en la opción "TRANSMISIÓN DE DOCUMENTOS", cuyas orientaciones se encuentran en la dirección electrónica https://asspaweb.pgr.mpf.mp.br;

b) Se incluya en la orden judicial la obligación de los corredores de criptoactivos de mantener el secreto de la decisión judicial de ruptura, absteniéndose de dar conocimiento del proceso o de la diligencia a sus clientes, bajo pena de la ley;

c) Se incluya en la orden judicial que, en caso de dudas por parte de las instituciones destinatarias, la dirección electrónica para contactar a la Secretaría de Pericia, Investigación y Análisis - SPPEA/PGR es pgr-simba@mpf.mp.br.

ALLANAMIENTO E INCAUTACIÓN

El MINISTERIO PÚBLICO FEDERAL solicita, en virtud del artículo 240, §1, letras "b", "c", "e", "f" y "h" del Código Procesal Penal, la emisión de órdenes de allanamiento e incautación penal con el objetivo de incautar cualquier documento, medio de comunicación y demás pruebas encontradas relacionadas con los delitos (...), en particular, pero no taxativamente:

a) registros y libros contables, formales o informales, comprobantes de pago/recibo, rendición de cuentas, órdenes de pago, agendas, cartas, actas de reuniones, contratos, copias de opiniones y cualquier otro documento relacionado con los ilícitos descritos en esta manifestación;

b) discos rígidos, notebooks, smartphones, unidades flash, medios electrónicos de cualquier tipo, archivos electrónicos de cualquier tipo, agendas manuscritas o electrónicas, de los investigados o de sus empresas, cuando haya sospecha de que contienen pruebas relevantes, como se especifica arriba;

c) archivos electrónicos de los sistemas y direcciones electrónicas utilizadas por los representados, así como los registros de las cámaras de seguridad de los lugares donde se lleven a cabo las medidas;

d) valores en especie en moneda extranjera o en reales con un valor igual o superior a R$ 20.000,00 o US$ 5.000,00 y siempre que no se presente prueba documental contundente de su origen legal; y;

e) dispositivos físicos de almacenamiento de claves de criptoactivos (coldwallets, hardwallets o carteras frías).

El MPF solicita además que los teléfonos celulares y tablets incautados sean enviados inmediatamente a Pericia de la Policía Federal después de la operación policial para que sus datos sean extraídos y agregados al expediente, y que se presenten en un plazo razonable los análisis de los demás dispositivos.

Asimismo, se solicita que este juzgado determine que los datos se extraigan mediante "extracción por sistemas de archivos", en la medida de lo posible, ya que permite recopilar un mayor número de información del dispositivo.

Se requiere, además, en relación a todos los equipos, medios electrónicos y dispositivos físicos de almacenamiento de claves de criptoactivos (coldwallets, hardwallets o carteras frías) incautados, la autorización para acceder a su contenido, y especialmente en lo que respecta a los smartphones, el acceso a todos los datos almacenados en la nube relacionados con los servicios vinculados a los celulares incautados.

En cuanto a los dispositivos físicos de almacenamiento de claves de criptoactivos (coldwallets, hardwallets o carteras frías), se solicita que conste expresamente en la orden de allanamiento e incautación la autorización para acceder a su contenido, y que la autoridad policial se esfuerce por transferir inmediatamente los activos encontrados a la cartera (...) bajo custodia estatal.

MEDIDA CAUTELAR PATRIMONIAL

En ese sentido, el MINISTERIO PÚBLICO FEDERAL solicita se ordene el SECUESTRO de los bienes de los demandados, solidariamente, hasta el valor de (...).

Para la ejecución de la medida de secuestro, el MPF solicita:

a) la comunicación de la decisión de secuestro a las instituciones financieras, a través de la técnica de embargo en línea, prevista en el art. 854 del nuevo Código Procesal Civil e implementada por el Sistema de Búsqueda de Activos del Poder Judicial - SISBAJUD, con respecto a todas las cuentas corrientes y aplicaciones financieras de titularidad de los demandados[68], a fin de asegurar que no sean rescatadas o transferidas de ninguna manera. En caso de no implementación de la medida, se solicita la reiteración automática de órdenes de bloqueo;

b) de manera acumulativa, se solicita la emisión de una orden de incautación de los criptoactivos eventualmente existentes bajo custodia de los siguientes corredores (...). Para la ejecución de la orden de secuestro, también se solicita que:

1. conste en la orden que el MPF y la Policía Federal podrán cumplir las órdenes de secuestro directamente en contacto con los corredores o, en caso de que no sean atendidos, inspeccionar la propia sede de las empresas en búsqueda de activos;

2. el MPF y la Policía Federal podrán tener acceso a dispositivos electrónicos o de almacenamiento, correos electrónicos o teléfonos vinculados para fines de doble factor de autenticación, para realizar la transferencia de los valores a la cartera descrita en el anexo bajo control del Estado, con fines de custodia provisional de estos criptoactivos; y

68- Incluyendo activos móviles, como títulos de renta fija y acciones, custodia de acciones, títulos privados, títulos públicos y derivados, aplicaciones en fondos de inversión, VGBL, PGBL, aplicaciones en LCA y LCI, aplicaciones en CDBs, RDBs, COE, oro y similares, previsión privada y cartas de consorcio.

3. el MPF y la Policía Federal pueden realizar la transferencia de valores custodiados, adoptando las medidas de ejecución operacional para el cumplimiento de la orden judicial, incluso la creación de cartera de custodia de criptoactivos, la liquidación por el valor de mercado del día del criptoactivo y la transferencia del resultado a cuenta judicial ligada a los autos, mediante orden judicial;

4. el MPF y la Policía Federal pueden transferir a la cartera virtual descrita en el documento adjunto los valores en criptoactivos eventualmente incautados en las órdenes de allanamiento e incautación expedidas en el proceso n. (...), protocolado en esa misma fecha.

c) se solicita el bloqueo vía RENAJUD de todos los vehículos registrados a nombre de los demandados hasta el valor de (...), cuyo año de fabricación sea superior a 2010, con el objetivo de evitar bloqueos de vehículos antiguos sin valor de mercado. Se solicita que se inserte una nota en RENAJUD, especificando la restricción como "transferencia del vehículo, su licenciamiento anual y circulación en la vía pública";

d) se solicita el bloqueo de embarcaciones y aeronaves eventualmente registradas a nombre de los requeridos, con la expedición de oficio a la Capitanía de Puertos y a ANAC para ejecutar la medida;

e) se solicita el bloqueo de bienes inmuebles registrados a nombre de los demandados hasta el valor de R$, insertando la orden de restricción en la CNIB - Central Nacional de Inhibición de Bienes[69], instituida en forma de Decisión de la Corregidora General de Justicia mediante la Resolución n. 39/2014;

f) se solicita la expedición de una orden a la Junta Comercial de los Estados Federales en que se sitúan las empresas demandadas, comunicándole la inhibición de todas las cuotas integradas del capital social de las personas jurídicas indicadas en la tabla anterior;

69- https://www.indisponibilidade.org.br/autenticacao/

g) inclusión de los bienes en el Sistema Nacional de Bienes Incautados - SBNA del Consejo Nacional de Justicia, según lo establecido en la Resolución n. 63, de 16 de diciembre de 2008;

h) la evaluación judicial de los bienes inmuebles y automotores eventualmente incautados, notificando al MPF y al propietario de su resultado, y su homologación judicial;

i) la enajenación anticipada de los inmuebles y automotores eventualmente incautados, de acuerdo con el artículo 144-A del Código Procesal Penal y la Resolución n. 92/09 del Consejo de Justicia Federal, para preservar su valor, dado que se trata de un bien sujeto a un grado significativo de deterioro y depreciación, así como por implicar dificultades y costos para el Estado en su mantenimiento;

j) el depósito del producto de la venta en una cuenta vinculada al juez hasta la decisión final condenatoria de la acción penal principal, procediendo a su conversión en ingresos para la Unión (artículo 91, inciso I, CP);

l) autorización para la transmisión de la decisión a las autoridades extranjeras en solicitudes de cooperación judicial internacional, con el objetivo de bloquear y repatriar eventuales bienes identificados en el extranjero.

m) autorización para el secuestro de bienes considerados de alto valor, como obras de arte, vehículos y joyas encontrados en posesión/propiedad de los demandados, por el valor especificado anteriormente, en el momento del cumplimiento de las órdenes de allanamiento e incautación solicitadas en el proceso iniciado en esta fecha.

MPF

Ministério Público Federal