BACSIRT
Vamos Buenos Aires | Centro de Ciberseguridad
LA AGENCIA DE SISTEMAS
www.ba-csirt.gob.ar
BOLETÍN N°34
FECHA DE PUBLICACIÓN
23 02 18


# CRIPTOMONEDAS II: CÓMO SE ALMACENA Y SE UTILIZA EL DINERO VIRTUAL

**Las criptomonedas, dada su naturaleza, son de carácter anónimo, descentralizado y no censurable, lo cual ofrece grandes ventajas. Sin embargo, no es correcto pensar que las operaciones con las mismas no dejan huellas ni pueden ser rastreadas. En caso de ser necesario, los especialistas pueden analizar las transacciones como el objetivo de relacionar las cuentas con los usuarios físicos.**

A lo largo del boletín N° 32 nos hemos dedicado a explicar, en términos generales, qué son las criptomonedas, de dónde salen y para qué se usan. La idea del boletín de esta semana, es profundizar un poco más en algunas de las características más relevantes de las mismas y explicar de forma sencilla cómo se almacenan y de qué manera se utilizan para realizar operaciones.

Respecto del primer punto, Sebastián Stranieri –CEO de la empresa VU Security- nos dice: "***una característica muy importante de las criptomonedas es que no requieren que uno demuestre y revele su identidad.*** *Para verificar la propiedad de un bitcoin y acceder a él, se emplea una contraseña creada con técnicas derivadas de la criptografía*". Y **otro de los rasgos fundamentales del dinero virtual, es el hecho de que no está regulado por ninguna entidad central**, sino que es la propia naturaleza de la red y los usuarios en ella son quienes hacen que el sistema funcione equilibradamente.

La contraseña de la que habla Sebastián, es lo que se conoce como "clave o llave privada" y bitcoin.org[1] define de la siguiente manera: **una clave privada es una pieza secreta de datos que acredita su derecho a gastar Bitcoins de un monedero Bitcoin por medio de una firma criptográfica**. Las claves privadas se almacenan en la computadora, si se utiliza un monedero de escritorio; mientras que, si se utiliza un monedero web, serán almacenadas en servidores remotos del proveedor. Las claves privadas nunca deben ser compartidas ya que les permiten a los usuarios gastar bitcoins desde su monedero correspondiente.

**Cada una de las claves privadas está asociada a una dirección**

**Bitcoin; esta última podría ser comparada con un número de cuenta bancaria**. Toda vez que queramos recibir bitcoins, usaremos esa dirección como referencia para pasarle a los demás usuarios. A la vez que, si nosotros quisiésemos enviar bitcoins, lo haremos a través de nuestra cuenta (a la que accedemos con la clave privada) y los usuarios receptores, verán como referencia nuestra dirección Bitcoin. La persona que disponga de la clave privada de una cuenta Bitcoin será la dueña de la misma.

**El principal legado que, sin dudas, dejarán las cripto-monedas es la tecnología Blockchain o "cadena de bloques", la cual se está implementando cada vez más en diversos servicios.**

Ahora bien, **para realizar todas las operaciones entre cuentas o direcciones Bitcoins, es necesario contar con un "monedero" o "billetera virtual"**. De acuerdo con las definiciones de bitcoin.org [2], "*un monedero Bitcoin es aproximadamente equivalente a un monedero físico en la red Bitcoin. El monedero realmente contiene su clave privada [o más de una, si es que el usuario posee varias cuentas] que le permite gastar los bitcoins asignados a la clave en la cadena de bloques. Cada monedero Bitcoin puede mostrarle la cantidad de bitcoins que contiene y le permite pagar una cantidad específica a una persona específica, como un monedero de verdad.*"


Si bien Bitcoin es la criptomoneda de mayor uso y difusión, existen muchas más en el mercado.

Tal como explicamos en el boletín anterior, **Blockchain o cadena de bloques, es el registro público de las transacciones Bitcoin en orden cronológico que se comparte entre todos los usuarios de la red**. Es decir, que la cadena de bloques funciona como un libro de contabilidad que asocia saldos con las distintas direcciones Bitcoin y es lo que garantiza la seguridad y transparencia de las operaciones, dado que para su funcionamiento utiliza técnicas criptográficas.

Entonces, recapitulando... **para poder comenzar a operar con bitcoins (u otra criptomoneda), se necesita contar con una cuenta (y su correspondiente clave privada) y un monedero virtual**, en el cual podremos administrar dichas claves y, por ende, las operaciones derivadas de ellas. En cuanto a las billeteras virtuales, existen las que se llaman "calientes" porque funcionan conectadas a Internet -lo que implican que almacenan la información en servidores de la red- y las llamadas "frías" o "de hardware"; es decir: que funcionan sin conexión a Internet, utilizando la memoria de algún dispositivo electrónico, lo cual las hace más seguras.

Según Stranieri, "*las criptomonedas son la disrupción en un espacio donde no existe una regulación, donde los usuarios ven sus grandes ventajas y le dan uso de forma cotidiana. Podríamos hablar de casos clásicos como Uber, AirBnb, Netflix, Skype, o WhatsApps, por ejemplo. Ahora, si me preguntan si bitcoin será la moneda líder dentro de 5 años, no lo sé,*


Tal como ocurre con las monedas tradicionales -e incluso, tal vez , más aún a causa de la naturaleza de las monedas virtuales-, el valor de las criptomonedas es volátil y se encuentra en constante cambio, influido por múltiples factores.

*pero seguramente el concepto y la implementación de "blockchain", que es la autopista por la que viaja bitcoin, va a prevalecer como una de las tecnologías más disruptivas de la historia. Existirán las privadas, las públicas, las gubernamentales, pero lo importante será la forma en que esa tecnología impacte en la vida de un ciudadano."*

Dado que si bien no podemos asegurar que efectivamente las criptomonedas se convertirán en el dinero del futuro pero sí sabemos que su uso se está masificando cada vez más, es fundamental entender, al menos básicamente, el funcionamiento de las mismas y de qué forma utilizarlas a los fines de evitar los riesgos derivados de su uso. En tal sentido, Stranieri explica:

*"Las criptomonedas no son 100% seguras en su uso. Eso significa que debamos estar pendientes, así como con las tarjetas de débito o crédito, de a quién le estamos enviando nuestros fondos. Al igual que las transacciones realizadas con estos medios de pago, las transacciones con criptomonedas tienen detalle de movimientos, saldos y balance.*

*Como las transacciones no son reversibles, es recomendable utilizar algún agente de scrow, los cuales garantizan las operaciones, funcionando como un intermediario que comprueba que se cumplen las condiciones estipuladas (que el producto llegue a su destino o que un servicio se realice correctamente).*

*También se sugiere habilitar el segundo factor de autenticación, tanto para el acceso web como para mobile, con un sistema de recuperación que también sea seguro, asociándolo por ejemplo a un celular o un sistema de reconocimiento facial o documental.*

*Respecto al almacenamiento de las monedas, es importante conocer el monto que uno desea atesorar en una billetera offline, además de tener las semillas o identificador único de la misma guardado en una caja fuerte o lugar seguro. De la misma forma que uno guardaría un ahorro en billetes, acciones de la bolsa o una escritura de un hogar. Es importante generar las palabras claves para poder recuperar la billetera en caso de pérdida o cualquier tipo de inconveniente.*

*Dada la volatilidad del precio de las criptomonedas, es importante recalcar que como en toda inversión de riesgo, uno debería destinar sólo determinado capital a dicho tipo de inversiones."* ▪

[1] https://bitcoin.org/es/vocabulario

[2] Ib.