CRIPTOMONEDAS Y CIBERDELITO: PERSPECTIVA DE POLICÍA NACIONAL

Working Paper 1/2025

Andrés Román Izquierdo
Isidro Almendros
Iván Moreno
Policía Nacional

Resumen: El artículo examina el creciente uso de criptomonedas por parte de ciberdelincuentes, destacando su papel en actividades delictivas como el blanqueo de dinero y estafas de inversión. Las criptomonedas, también conocidas como criptoactivos, son descritas como activos digitales que emplean tecnología blockchain para registrar transacciones, lo que las hace atractivas por su descentralización, seguridad criptográfica y pseudoanonimato. Sin embargo, estas mismas características las convierten en herramientas útiles para los cibercriminales. Se aborda el concepto de cibercrimen como servicio y las estafas de inversión, donde las criptomonedas se utilizan como gancho para defraudar a personas. Además, se menciona cómo el ecosistema digital y la falta de regulación facilitan la rápida movilización de fondos ilícitos.

Palabras clave: criptomonedas; ciberdelincuencia; blockchain; blanqueo de dinero; estafa de inversión; criptoactivos; cibercrimen como servicio.

Códigos JEL: K42; G28; D18; O33.

La mejor protección es la prevención. Las tecnologías tan disruptivas que estamos viendo han llegado para ofrecernos oportunidades de trabajo especialmente a los jóvenes que van a desarrollar su carrera profesional en un mundo financiero digital, pero sobre todo ofrecen oportunidades al ciberdelincuente. Así que este trabajo se centrará en hablar del mal, no del bien.

Al enemigo, al que nos quiere atacar y que nos está atacando continuamente hay que conocerlo y vamos a abordar una de las maneras en que nos atacan o se aprovechan que es con las criptomonedas, que no son criptomonedas, son criptoactivos. Los criptoactivos son una tecnología, pero es una tecnología que es aprovechada y va a ser utilizada para infinidad de cosas.

En un primer bloque se va a definir conceptualmente qué es una criptomoneda y en un segundo bloque se aborda qué representa y por qué son tan beneficiosas y utilizadas por la ciberdelincuencia. Se hará un recorrido por una novedad que hay en el mundo cibercriminal, que es la democratización o el cibercrimen como servicio. Y, por último, se tratarán determinadas casuísticas delictivas en las que las criptomonedas se utilicen como gancho o como medio para blanquear dinero.

¿Qué son las criptomonedas? Se pueden definir como activos digitales que emplean un cifrado criptográfico para garantizar la integridad de las transacciones, lo que se puede decir que es como si tuviéramos efectivo, pero de manera digital sin depender de entidades como pueden ser los bancos.

¿Cómo se pueden adquirir este tipo de criptomonedas? Básicamente hay dos grandes bloques que sería a través de los mineros o validadores. Al principio de las criptomonedas se introdujo el concepto de minero que consiste en una serie de ordenadores que hacían cálculos matemáticos para descifrar un acertijo y gracias a eso se daba estabilidad a la red y a cambio de esos ordenadores que estaban realizando ese esfuerzo computacional la red le ofrecía una recompensa y esa recompensa se la da en la criptomoneda o criptoactivo que se esté minando, en este caso si hablamos del Bitcoin, podemos encontrarnos con una serie de ordenadores que se encuentran continuamente realizando esas operaciones matemáticas y una vez que descifran lo que es un bloque reciben una recompensa.

Esto energéticamente no era sostenible, por lo tanto, se ha introducido lo que son los validadores, que son otros tipos de criptomonedas que lo que hacen es en lugar de tener ordenadores continuamente realizando operaciones, son personas que tienen una cantidad determinada de criptoactivos en un determinado contrato y son los que validan las transacciones que esto energéticamente pues es mucho más eficiente y por eso se introdujo este nuevo sistema.

Además del papel de los mineros y validadores, la otra forma para adquirir criptomonedas es a través de la compraventa, ya sea entre usuarios o en plataformas digitales como son los *exchange*.

Todas las transacciones que se realizan en criptomonedas se anotan en la *blockchain*. La *blockchain* podemos asimilarlo como un libro grande de contabilidad donde todos los usuarios de la red tienen una copia de ese libro, por lo tanto, es inmutable, es decir, no se puede modificar. Una vez que se anota una transacción eso queda registrado ahí para el resto de la vida, por lo tanto, eso les da una seguridad a esas transacciones y también una trazabilidad o sea cualquier persona puede confirmar si se ha hecho un determinado pago o no.

Entre las características principales que tienen las criptomonedas se podría destacar que no están controladas por ningún gobierno o institución si bien en los últimos años se está intentando regular lo que es el uso de las criptomonedas, el control no es de los gobiernos, por lo tanto, el usuario no necesita tener sus criptoactivos en un tercero como puede ser una entidad bancaria.

Las transacciones son descentralizadas lo que quiere decir que son *peer to peer*, es decir, entre pares por lo que no se depende de ninguna entidad para hacer un pago. Normalmente en las transacciones normales cuando vamos a comprar a una tienda pagamos con nuestro móvil y el dinero está depositado en una entidad bancaria, que en este caso entonces tenemos una entidad que es centralizada. En el caso de las criptomonedas, son descentralizadas y las transacciones se hacen entre pares.

El valor que tiene la criptomoneda depende de la confianza que el público le otorgue, cuanta más demanda de una criptomoneda determinada, su precio sube y viceversa. Por tanto, no hay ningún precio que esté estipulado ni lo marca ningún organismo internacional.

Otra de las características principales de las criptomonedas tiene que ver con la criptografía. Por un lado, está la clave pública, es decir, la dirección donde el usuario va a recibir o desde la que va a emitir los pagos y luego tenemos la clave privada que sería la que nos vale para operar con dicha cartera o dirección.

Son de código abierto, eso quiere decir que cualquier usuario que tenga conocimiento puede examinar perfectamente el código de esa criptomoneda para ver que no se producen tipos de estafa o engaños.

Otra característica es que el registro es descentralizado y distribuido, eso quiere decir que la *blockchain* no se encuentra en un solo ordenador, sino que está distribuido por todos los ordenadores que están en ese momento mirando o validando las transacciones.

Una de las características también que destaca de las criptomonedas es la alta volatilidad que tienen. En cuanto al almacenamiento de los criptoactivos, aunque podemos tenerlos en entidades centralizadas, lo normal es que se tenga en carteras propias particulares.

¿Cuántas criptomonedas existen en la actualidad? No se podría decir un número porque dentro de cada *blockchain* a su vez existe lo que son los llamados *token* que son otras criptomonedas que dependen de esa *blockchain,* por lo tanto, podemos hablar de cientos de miles de criptomonedas diferentes.

El término *wallet* lo que llamamos cartera, billetera o monedero virtual que es la que gestiona nuestros activos, es donde están nuestros criptoactivos con los cuales vamos a operar. Dentro de estas *wallet* encontramos dos tipos básicamente: las carteras calientes y las carteras frías. Las carteras calientes son aquellas que están conectadas directamente (no la cartera sino el dispositivo) directamente a internet y las frías son aquellas que no están conectadas a la red, por lo tanto, suelen ser bastante seguras.

Dentro de las carteras calientes, están las que son servicios *online* que son plataformas como Binance, Coinbase, etc., son plataformas en las que realmente el usuario no tiene el control de la clave privada, por lo tanto, lo que tenemos ahí es una cuenta de usuario. Ahí sí dependería de un organismo principal que sería centralizado, la ventaja es que es muy cómodo a la hora de utilizarse, pero la seguridad es baja porque cualquiera con acceso al teléfono móvil vinculado o el robo de la contraseña pueden hacer que los criptoactivos ahí depositados sean movidos de un sitio a otro sin que el usuario se dé cuenta.

Otro tipo de carteras dentro de las calientes serían las aplicaciones móviles, cuya ventaja es la comodidad, pero la seguridad, al igual que en el caso anterior, sigue siendo baja, porque cualquiera en un momento particular puede acceder a nuestro teléfono ya sea de manera física o en remoto y movernos esos criptoactivos a otra dirección. Como ejemplo de carteras de este tipo podríamos poner el caso de Metamask, que es muy conocida para la red Ethereum, o Coinbase *wallet*.

Las aplicaciones de escritorio son aplicaciones que al igual que tenemos apps en los teléfonos móviles, pues tenemos instaladas aplicaciones en nuestros ordenadores, en este caso de carteras comunes podríamos citar Electrum o Exodus. La comodidad de este tipo de aplicaciones es media, ya que no es como nuestro teléfono que lo llevamos siempre encima, por lo tanto, deberíamos siempre desplazarnos a un sitio donde tuviéramos la cartera y la seguridad igualmente es media porque al igual que con nuestro teléfono pueden acceder a nuestro ordenador en cualquier momento ya sea a través de malware o algún tipo de fuga de base de datos en la que se filtre nuestro usuario y contraseña por distintos métodos.

Dentro de las carteras frías nos encontramos con dos tipos principalmente: una que sería *hardware*, es decir, dispositivos físicos similares a un pendrive donde guardamos nuestros criptoactivos. Esto al

estar en un dispositivo físico externo a la red nos da un control total sobre nuestros criptoactivos y la seguridad también es máxima, ya que solamente lo conectaremos en el momento que queramos realizar una transacción. En este caso podemos poner como ejemplo los Ledger o los Trezor.

Por otro lado, están las carteras de papel. Esto es un documento impreso donde se apunta la clave pública que es la que nosotros vamos a dar a la otra persona para emitir los pagos o dónde vamos a recibir y si queremos operar tenemos que operar con la clave privada que es la que aparece en el papel. Por supuesto la clave privada siempre debería estar oculta porque en el momento que un usuario tenga acceso a ella podría robarnos todos nuestros activos. La comodidad es bastante baja por no decir casi nula porque es bastante difícil operar con carteras de papel, pero la seguridad al igual que los dispositivos físicos es bastante alta.

¿Son anónimas las criptomonedas? Es cierto que las criptomonedas en sí son anónimas, pero al final cuando la persona quiere disponer de esos criptoactivos en dinero fiduciario tiene que sacar ese dinero por algún tipo de entidad ya sea un *Exchange,* un procesador de pago o un cajero, por lo tanto, digamos que las criptomonedas no son anónimas sino que son pseudo anónimas porque a través de la trazabilidad ya que la *blockchain* es pública podemos hacer un seguimiento a esas direcciones de criptomonedas y poder llegar a ese tipo de casa de cambio o procesador de pagos en el que nos va a facilitar a la policía información acerca de la persona que ha retirado ese efectivo o aportado la documentación a la hora de hacerse su cuenta de usuario.

¿Qué es lo que suponen las criptomonedas? Las nuevas generaciones se van a desenvolver en una economía global, pero además muy importante lo que se denomina DeFi, o economías descentralizadas, es decir, que no va a depender de los bancos eso tiene una parte buena y una parte mala y la parte mala es que los delincuentes se van a desenvolver en un paraíso donde no va a haber control más que la posesión de una clave para mover a placer el dinero producto de delitos.

En los últimos años se ha agilizado un proceso histórico de digitalización de la sociedad, las sucursales bancarias han ido cerrado, se han abierto aplicaciones *online*, es decir, se está digitalizando todo y se está descentralizando en gran medida. Lógicamente hay neobancos que operan fuera del ámbito de la Unión Europea y no están regulados, no se puede poner límites a una tecnología. El *blockchain* y las criptomonedas son una tecnología, se podrá regular los que tengan sede jurídica en Europa y en España, pero como estamos una comunidad global, como tradicionalmente se dice «no se le puede poner puertas al campo» eso es una valoración que nosotros hacemos y lo estamos viendo día a día porque los delincuentes se aprovechan de eso para mover el dinero fácilmente y blanquear lo que de otra manera era muy complicado o dejaba rastro.

En esta economía digital existe un concepto que es las *fintech* que es la tecnología financiera conformada por todas esas miríadas de aplicaciones incluidas Bizum, Remitly, plataformas de trading, los *exchange* que no son más que casas de compraventa de criptomonedas, es el banco digital que transforma el euro en cripto y el cripto en euro en dólar o incluso en petróleo porque son verdaderos *broker online* y que no tienen por qué tener residencia en la Unión Europea.

Esta economía digital tiene una serie de características policiales y delincuenciales y esto es lo que queremos poner en relevancia y se va a poder entender el rol y el papel que representan las criptomonedas en esta nueva economía digital en gran parte descentralizada.

En primer lugar, nunca antes en la historia del crimen había sido tan fácil y rápido, inmediato disponer de los beneficios del delito. Hace 10 años el que robaba y estafaba tenía que hacer un ingreso, las

transferencias tenían cierto retraso mientras que hoy en día las transferencias son inmediatas incluso las internacionales.

Por ejemplo, con Bizum hay que tomar ciertas precauciones porque no solamente es un medio de pago, sino que es un medio para requerir el pago y con esto que se llama «pago mocho» hay muchas estafas.

Bizum es un medio de pago que se enmarca dentro de estas ventajas que tiene la tecnología financiera, es decir, las criptomonedas ¿por qué? Porque son un medio de pago y un medio de pago tan rápido como la velocidad de la luz en la que enviamos un pago inmediato a otra parte del mundo, un mundo etéreo que no está en ningún lado. Nosotros por nuestra experiencia, ahora mismo tenemos carteras localizadas que no están en ningún país y tienen 3 millones de euros y sabemos que son de delincuentes, incluso delincuentes que detenemos y tienen millones de euros y nos lo dicen. Una de las características que tiene el *blockchain* y las criptomonedas es que son públicas, todo el mundo puede consultar la cartera, que es un código QR, y sabemos que hay 3 millones de euros, pero no nos da la clave privada.

Esto es muy peligroso porque las criptomonedas no tienen titular, depende de quien tenga la clave privada y además son descentralizada dependen de todos los nodos que están participando en el sistema y, por tanto, no dependen de ningún Banco Central, de ninguna organización a la que podamos recurrir o los jueces y bloquearla. Es un medio de pago rápido e inmediato, pero sobre todo es un medio para blanquear dinero.

Se caracterizan además porque se pueden enmascarar, por tanto, es la situación idónea para el delincuente. Por ejemplo, plataformas *online* de envío de dinero, TPV virtuales, transferencias bancarias internacionales con comisiones que no tienen retrocesión, Bizum y tarjetas prepago. Dentro de estos medios de pago digitales cobran especial relevancia las criptomonedas y no solamente las criptomonedas *per se* con estas aplicaciones que las custodian que son las apps, carteras calientes o el que quiere tener plena seguridad pues la tiene en su casa o una placa metálica por si se quema o de dispositivos que parecen *pen drives* y pasan desapercibidos.

¿Por qué son importantes para el cibercrimen? En primer lugar, son pseudo anónimas, es decir, que no tienen un titular. Por ejemplo, tenemos una cartera de papel, que es un QR y a través de una investigación hemos llegado a la conclusión de que tiene 3 millones de euros, pero ¿dónde está? ¿a quién pertenece? ¿a quién acudimos para intervenir los 3 millones producto de un delito? No se puede. Por tanto, este es el primer ingrediente ideal para el que quiere que no le quiten el dinero, que es el ciber delincuente. ¿A quién recurrimos? Lleva ahí 2 años y no podemos acudir a nadie porque es una tecnología que es una anotación en un libro con de contabilidad virtual infalsificable y permanente que se llama *blockchain*, que es una tecnología que no solamente se utiliza como medio de pago sino para muchas otras cosas como, por ejemplo, para garantizar las transacciones, para garantizar la identidad, para hacer contratos inteligentes en los que las partes ya no median porque el contrato queda sellado bajo un protocolo de un algoritmo que es inmutable que lo hace cumplirse, porque el mismo programa va a retener las cantidades y va a ejecutar lo que diga la letra. En definitiva, es una tecnología y parte de esa tecnología tiene un componente de activo financiero.

Son pseudo anónimas por lo que la cartera en la que están depositadas las criptomonedas no sabemos a quién pertenece, pero tiene una ventaja y es que como queda el registro en ese libro contable podemos hacerle una trazabilidad para cuando ese dinero pase del mundo virtual al mundo físico se pueda saber quién está detrás de la extracción del dinero.

La descentralización, que es una de las características de esta tecnología, se extrapola a muchos sistemas de préstamo, de *crowfunding* y demás que suponen una amenaza directa para las entidades financieras. No hay peor enemigo para un estado y para un sistema que es algo que no es controlado por al menos alguien que quiere hacer el bien.

Es infalsificable, es decir, el dinero en criptomonedas no se puede falsificar ni robar, solo se podrá robar siempre que se tenga la clave privada.

¿Cómo se blanquea? ¿Qué es lo que hace el delincuente? Alguien comete un ciberdelito y tiene una transferencia, es decir, la víctima hace una transferencia. ¿Dónde va el dinero? Pues a esas casas de compraventa que se llaman *exchange,* transforman el dinero estafado en bitcoin, la criptomoneda más conocida, y a continuación la almacena, puede ser en una cartera fría, en una cartera de papel, en un dispositivo o en una aplicación. A continuación, empiezan a traspasar el dinero y lo blanquean, o bien acuerdan una transacción con alguien por medio de la cual le van a vender las criptomonedas con descuento. Otra opción es a través de los criptocajeros, donde se puede extraer en efectivo de los cajeros el dinero que se tenga almacenado en criptomonedas.

También existe la opción de la tecnología financiera que no exigen poner la cara, ni piden documentación y aunque pidan documentación se puede falsificar y cripto monedas confidenciales a las que no se les puede hacer trazabilidad.

Tenemos, por tanto, un ecosistema criminal basado en esta tecnología. Un «empresario», que es el ciberdelincuente, tenemos unos proveedores de servicio, el crimen como servicio ya que el que comete un delito puede ser cualquiera porque existen proveedores de servicios y los servicios son los ataques. Los clientes son las víctimas.

Por otro lado, tenemos los medios de pago a través de las «mulas financieras» y los medios de pago a través de las criptomonedas, luego el blanqueo y se cierra círculo.

¿Cuál es el valor de los criptoactivos? ¿Lo que alguien esté dispuesto a pagar? Las criptomonedas nunca van a bajar de valor porque van a ser utilizadas como el «dólar» del cibercrimen.

A continuación, vamos a hablar de un tipo de delito que se llama *broker scam,* que son los chiringuitos financieros basados en ofrecer como gancho ganancias espectaculares con criptomonedas.

Nuestras emociones y nuestra conducta se rigen por una norma fundamental que es maximizar los beneficios y minimizar los costes. Esto lo conocen los estafadores para estafarnos.

A continuación, se va a explicar brevemente cómo funciona una estafa de inversión. En primer lugar, tenemos a un inversor, una persona, que quiere que su dinero crezca y le va a entregar su dinero a una compañía de solvencia y le va a entregar pingües beneficios. Pero esto no es así, lo que realmente pasa es una estafa donde hay una víctima que da su dinero a un criminal y todo esto sucede por un engaño.

Esto no es nuevo, no es algo del siglo XXI ya que esto viene sucediendo desde que existe el dinero. En el siglo XXI estamos bombardeados todos los días de información, grandes cantidades de información, y para ilustrarlo, he buscado en Google «inversión criptomonedas» y estos son los titulares de noticias que he obtenido: medio de noticias generalistas «Mejor que el oro, esta es la

inversión que va a estallar próximamente según un gigante financiero». Xataka «la industria cripto está produciendo muchos millonarios, así que Ferrari permitirá comprar sus coches con bitcoin». Medio de comunicación especializado en noticias de economía «ahorro e inversión: cómo invertir en criptomonedas de manera segura, guía completa para principiantes».

Esto es lo que nos transmiten los medios de comunicación y las redes sociales a diario y esto no solo lo transmiten las redes sociales, también lo hacen los estafadores y aprovechan este nuevo oro del siglo XXI, que son las criptomonedas, para embaucar a la gente.

El esquema básico de una estafa de inversión en criptomonedas es muy similar al esquema básico de la estafa: tenemos un inversor que quiere ganar mucho dinero con poco esfuerzo y tenemos en el otro lado a una persona de solvencia, de reputación, de ganancia, en definitiva, una persona en quien podemos confiar perfectamente nuestro dinero y que a través de las criptomonedas nos va a dar pingües beneficios. Pero esto como antes se apuntó, es totalmente falso ya que lo que tenemos es una víctima que da dinero a un criminal y finalmente el producto es que no hay criptomoneda y tampoco hay beneficio, lo ha engañado totalmente.

En la ciudad de Málaga al cabo del mes entran ocho denuncias de este tipo. Y si calculamos la acumulación de todo el dinero defraudado, el total asciende el año pasado a 2 millones de euros defraudados en estafas de inversión en criptomonedas. El perfil de la víctima es de una persona de nivel cultural medio y de clase media acomodada. La carencia que tienen estas víctimas es sus bajos conocimientos en el manejo de las tecnologías que es por ahí por donde atacan los criminales.

Las tipologías de estafas de inversión en criptomonedas son básicamente cuatro: por un lado, tenemos el *broker* estafador que es una persona que se nos presenta como un gestor experto en criptomonedas que va a hacer que nuestro dinero crezca y esta gente accede a las víctimas a través de internet, esencialmente a través de los canales de Telegram especializados en la inversión en criptomonedas, ahí es donde abordan a sus víctimas.

Al principio a la víctima le engañan primero con una pequeña cantidad de dinero, por ejemplo, 50 euros y este dinero lo multiplican por dos, luego hacen otro segundo intento donde les dan 200 y les dicen que no es que ha duplicado, sino que aún más ha conseguido un beneficio increíble pero que tienen que tener premura porque estamos en el momento es el momento ahora de invertir y si invierte una cantidad mucho más alta, por ejemplo, 10.000 euros la víctima se puede hacer millonaria y claro, finalmente esto no ocurre.

¿Cuál es el modus operandi? Se hacen con el poder del teléfono de la víctima a través de aplicaciones de escritorio remoto como Anydesk o Teamviewer, para ello utilizan portales de *exchange* y ahí el dinero lo convierten en criptomonedas y las criptomonedas que están en el *wallet* de la víctima pasan automáticamente al *wallet* del criminal y desaparecen.

También hay aplicaciones móviles que ofrecen servicios de minería. Servicios que, por una pequeña inversión, por ejemplo, 200 euros afirman que van a dar un beneficio del 30%. Eso no es verdad, ya que el minado de datos es muy costoso y requiere mucha energía.