

maldita.es

Supuestos grupos de inversión en criptomonedas en Telegram y su modus operandi: qué hay detrás y por qué tenemos que desconfiar

Maldita.es

14-17 minutos

Telegram es un nido para los inversores en criptomonedas. En esta plataforma, muchos entusiastas del mundo cripto se dedican a crear grupos masivos en los que puede que alguna vez hayas terminado sin comerlo ni beberlo, en los que se nos presentan supuestas ofertas para invertir en criptoactivos a cambio de grandes ganancias. Pero cuidado, pueden ser estafas. Os contamos cómo algunos de estos grupos usan supuestas plataformas de inversión que suplantán a empresas reales, enlaces con invitaciones para darnos de alta que recuerdan a estafas piramidales y transacciones que hacen saltar el dinero de un lado a otro hasta perder el rastro.

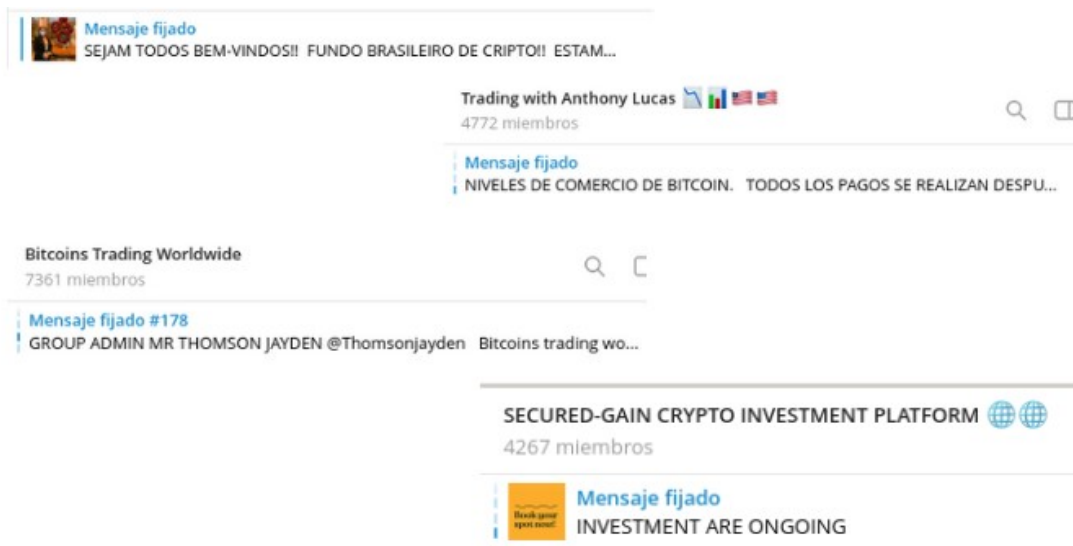
En *Maldita.es* nos hemos adentrado en ellos para conocer mejor qué hay detrás de algunas de estas campañas. Es

común en esta red de mensajería recibir mensajes privados procedentes de desconocidos que nos proponen invertir en criptomonedas “muy rentables” y que nos incluyen sin nuestro permiso en grupos con miles de personas donde nos animan a participar, dejar nuestro dinero y presumir de las ganancias. Sin embargo, en ocasiones se trata de estafadores que prometen “ganancias rápidas” a través de las criptomonedas para quedarse con nuestro dinero.

Grupos con miles de miembros que presumen de las “ganancias obtenidas” a través del método del grupo

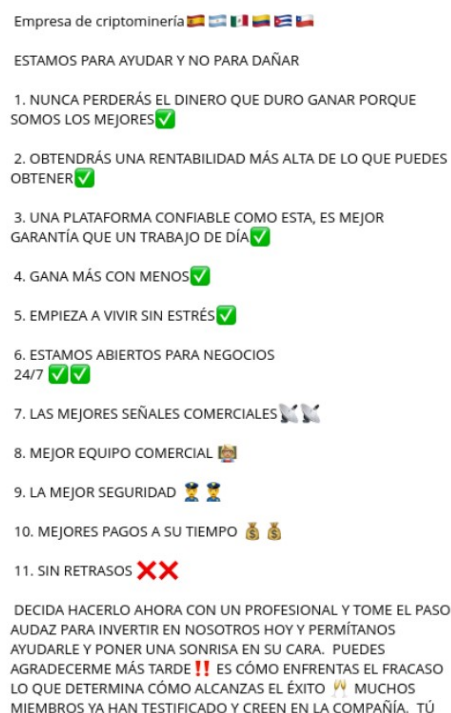
La dinámica es la misma en todos los que hemos observado: suelen ser grupos internacionales con una clara llamada en su título a las inversiones en criptomonedas. Lo normal es que la batuta la lleve el administrador del grupo. Entre una y dos veces al día, envía instrucciones sobre cómo proceder en las inversiones, y también es el que, supuestamente, nos ingresa las ganancias. A veces, requiere que nos demos de alta en una plataforma de criptomonedas, como Coinbase o Binance, y nos guía por el proceso de registro y verificación, hasta llegar al de inversión. En otras ocasiones, nos pide datos personales como el teléfono o el correo electrónico para darnos de alta en su sistema y así, en teoría, empezar a invertir.





Capturas de pantalla de los nombres de los diversos grupos de inversión a los que fuimos añadidos. Fuente: *Maldita.es*

Mientras, en los grupos no paran de sucederse mensajes con capturas de pantalla en las que se ven supuestos pagos al administrador y pidiéndole que confirme su recepción para empezar a operar. Otros miembros responden alabando todas las ganancias que han conseguido desde que están “invirtiendo” en la plataforma y animan a los demás a hacer lo mismo.





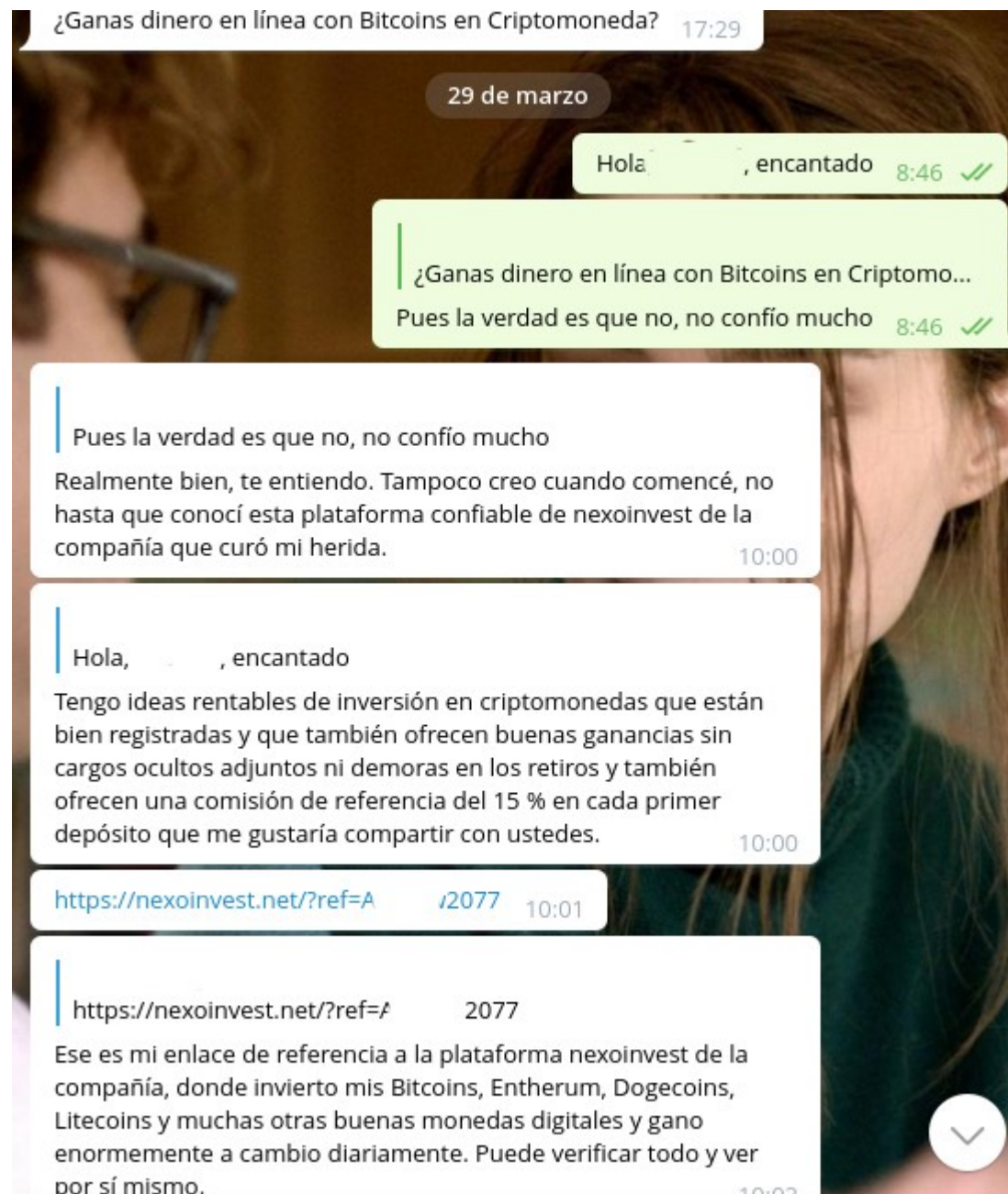
A la izquierda, mensaje de información del administrador de uno de los grupos. A la derecha, usuarios respondiendo al comprobante de una transacción animando al resto a invertir. Fuente: *Maldita.es*

Desconocidos que nos hablan por mensaje privado para proponernos “grandes ganancias”

El modus operandi en algunos casos consiste en enviar mensajes privados a usuarios para proponer una idea de inversión o, directamente, para preguntarnos si “ganamos dinero en línea con criptomonedas”. En un caso específico, al solicitar información nos envían un enlace a una plataforma (NexoInvest) que garantiza “buenas ganancias sin cargos ocultos adjuntos ni demoras en los retiros”, además de comisiones “de hasta el 15%” por traer a nuevos inversores. “Siempre suelen prometer un porcentaje de ganancias bastante inverosímil, y dejan un enlace a uno de esos grupos para captar nuevos usuarios”, comenta a Maldita.es José Antonio Bravo, experto en fiscalidad de criptomonedas. Este modus operandi recuerda a estafas piramidales como la de organizaciones como [IM Mastery Academy, de la que ya os hemos hablado en Maldita.es](#): se ofrecen ganancias extras muy altas si se consigue a más gente.

Estas cuentas, además de meternos en grupos, nos escriben por privado con imágenes que, en teoría,

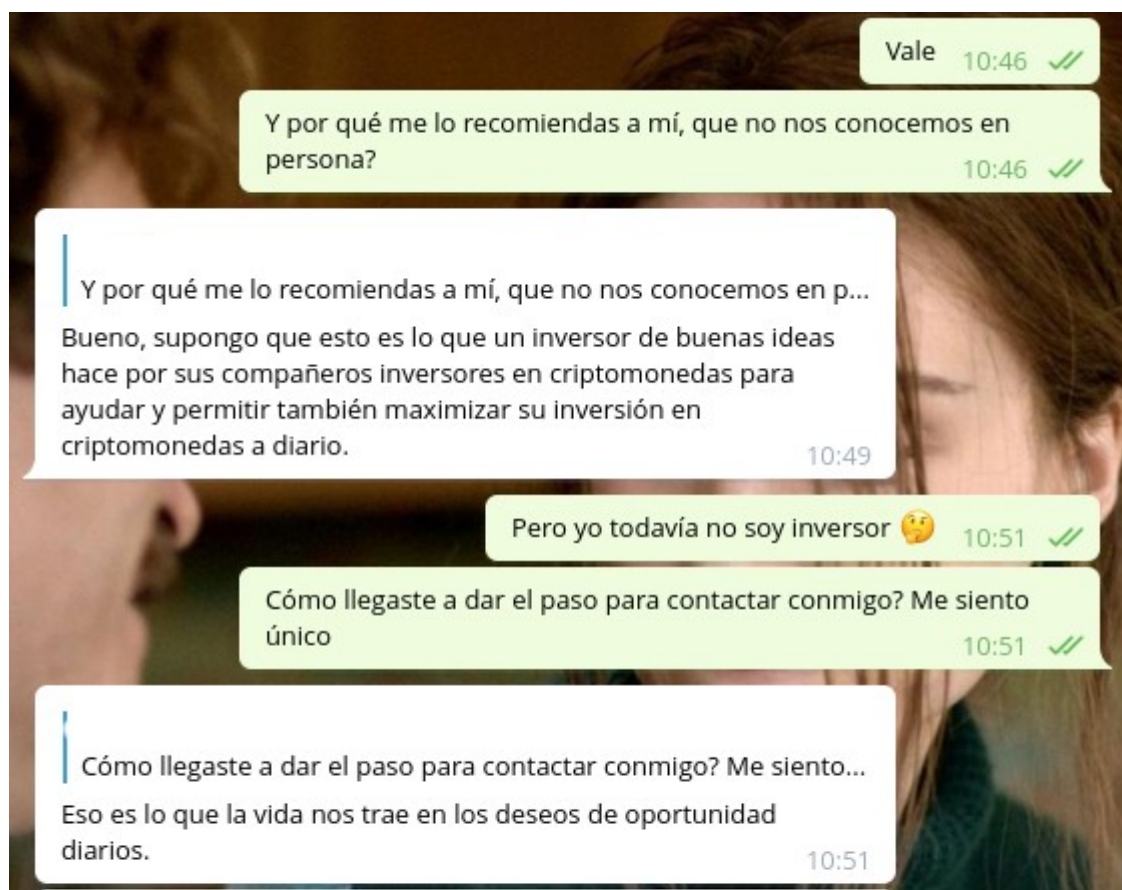
demuestran las cantidades que han ganado con la inversión y de la supuesta rentabilidad que han obtenido. Lo hacen con capturas de pantalla de correos electrónicos en los que aparece la transacción que ha realizado la empresa con la que ha invertido.

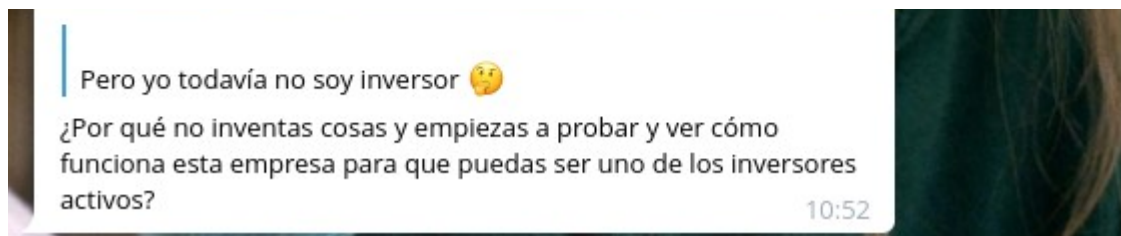


Captura de pantalla de la conversación en Telegram de un usuario desconocido que nos escribió para ofrecernos inversiones en criptomonedas a través de una plataforma. Imagen: *Maldita.es*

Todos los que nos han escrito lo han hecho en español, pero con un lenguaje poco fluido, con claros fallos gramaticales y repitiendo varias veces los mismos párrafos de forma literal, lo que nos puede llevar a pensar que se tratan de cuentas automatizadas. “Lo habitual es que estas cuentas, presumiblemente falsas, nos hablen en un castellano bastante tosco, producto seguramente de un traductor instantáneo como el de Google”, señala Bravo.

De hecho, nos contactaron dos perfiles que aparentaban ser dos personas diferentes: compartían el nombre, pero los apellidos y la foto de perfil variaban. Al preguntar a uno de ellos si conocía al otro, las respuestas fueron ambiguas: en un primer momento comentó que era otra cuenta “de la empresa”, para posteriormente decir que era de “su tío” y después hacer coincidir las fotos de perfil.





Captura de pantalla de una conversación en Telegram con un usuario que nos habló para invertir en la que responde a nuestras preguntas sobre por qué contactar con otros usuarios desconocidos. Imagen: *Maldita.es*

En *Maldita.es* ya os hemos hablado de lo que debemos tener en cuenta [si queremos invertir en este mercado de las criptomonedas](#) y también [os hemos advertido de los timos y las estafas que suelen rodear este mundo](#). En base a ello, hay algunas prácticas que pueden hacernos sospechar y plantearnos la legitimidad de estos grupos de Telegram y de los desconocidos que nos hablan con la promesa de sacar “rentabilidad”.

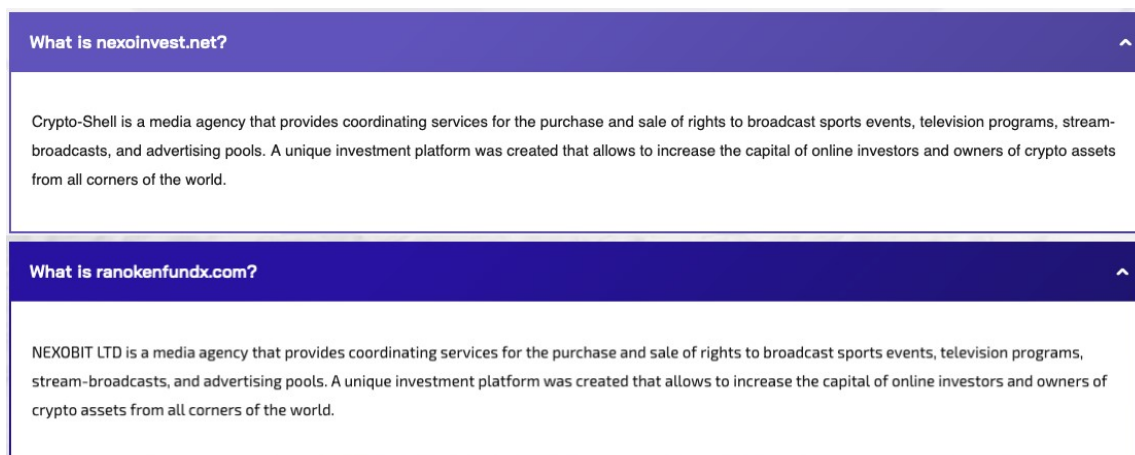
Páginas web clonadas unas de otras y con texto sin conexión con las criptomonedas

Si ponemos aun más la lupa sobre estos grupos, empezamos a ver incongruencias y pistas que nos hacen sospechar de la legitimidad de lo que hay detrás. Por ejemplo, las páginas web que nos envían para registrarnos son prácticamente calcadas, a pesar de que pertenecen, supuestamente, a empresas diferentes. Con una búsqueda en Google de un extracto de un texto de una de ellas, hemos encontrado al menos una decena con el mismo contenido y diseño, pero con diferente

nombre. Por ejemplo, nos encontramos con una copia exacta del mismo apartado de preguntas frecuentes que habla sobre “qué es” el sitio web que visitamos.

El texto común, en este caso, es el siguiente:

“[Empresa] es una agencia de medios que provee servicios coordinados para la venta de derechos de retransmisión de eventos deportivos, programas de televisión y lugares para anuncios. Una única plataforma de inversión fue creada para permitir incrementar el capital de inversores online y de propietarios de activos en criptomonedas de todo el mundo”.



Captura de pantalla de dos páginas webs de diferentes plataformas de inversión en criptomonedas que comparten el mismo texto. Imagen: *Maldita.es*

Como vemos, sólo cambia el nombre de la supuesta agencia de medios. La segunda frase no parece tener conexión con la primera. También hemos detectado otra página que utiliza ese mismo párrafo, aunque esta vez sí que menciona un “sistema de inversiones de Reino Unido”: “[Empresa] es un sistema de inversión profesional de Reino Unido líder en el mundo, que provee de

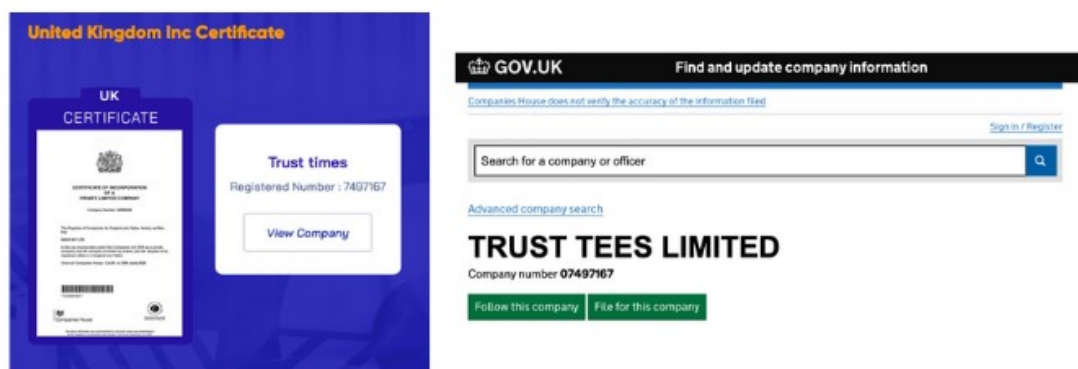
servicios de inversión avanzada en criptomonedas a inversores globales basados en el uso efectivo de la interpretación de datos”. Salvo ese detalle, el texto es el mismo que el resto de webs mencionadas.



Captura de pantalla de dos páginas webs de diferentes plataformas de inversión que nos han recomendado en la que aparece el mismo texto. Imagen: *Maldita.es*

Estas webs utilizan certificados falsificados para dar más credibilidad

Estas páginas aportan documentos supuestamente expedidos por el [Registro Mercantil de Reino Unido](#) en los que, presuntamente, aseguran la identidad y la integridad de quién está detrás. ¿Por qué decimos presuntamente? Porque si buscamos en la base de datos del Registro Mercantil, los nombres de las empresas de las webs no aparecen y el número del registro corresponde a otra empresa, ya sea una que cesó su actividad u otra que, a pesar de seguir en activo, se dedica a un ámbito diferente.



Captura de pantalla de la página web de la plataforma de inversión en la que muestran su supuesto número de registro, suplantando a un bufete de abogados.

Por ejemplo, en el caso de una de las webs, [Bitcash](#), se usa un certificado falsificado a nombre de Bitcomet (que no es el nombre de la página) y utilizan [el registro de una empresa dedicada a instalaciones eléctricas e informáticas](#), llamada Fieldco. Esta, según el registro británico, no realiza ninguna actividad relacionada con las criptomonedas. [Trust Times](#), otra de las plataformas, falsifica el certificado de [otra compañía](#) (en este caso, un bufete de abogados, Trust Tees) y coloca su nombre manteniendo el número de registro de la original. Utiliza también [la dirección física de una de las oficinas del bufete](#).

Otras no aportan este número de registro mercantil, sino una dirección física para intentar dar más credibilidad. El caso es que el lugar al que se refieren se trata de “oficinas virtuales”. ¿Qué es una oficina virtual? Son

locales vacíos que la empresa propietaria “alquila” a otras empresas para que estas puedan usar la dirección del local sin la necesidad de usar el recinto como lugar de trabajo, sino solo como dirección de contacto y dirección postal. Por ejemplo, la dirección publicitada en [la web de Koinpaxful](#) corresponde a las [London Virtual Office](#), una empresa que se dedica a ello. Hemos tratado de ponernos en contacto con la empresa que gestiona estas oficinas virtuales, pero no hemos obtenido respuesta.

Otra de las webs a la que nos invitaron a invertir, [Heritage Capital](#), aparece listada por la [Comisión Nacional de Mercado de Valores](#) (y su homóloga inglesa [Financial Conduct Authority](#)) como “clon fraudulento” de una empresa lícita del mismo nombre y advierte de posibles “fraudes”. Es más, si nos fijamos en la dirección del clon de Heritage Capital que lista la FCA, podemos comprobar que coincide con la que también tiene en su web una de las supuestas empresas de inversión citadas Nexoinvest.



Heritage Capital (clone of FCA authorised firm)

Address: 1 Canada Square, Canary Wharf, UNITED KINGDOM, E14 5AB

Arriba, la dirección de una de las plataformas que nos recomendaban para invertir. Abajo, la dirección de un clon de una empresa legítima que coincide con la anterior.

Imagen: Financial Conduct Authority

Las transacciones se producen pero el dinero rebota de una cartera a otra en cuestión de segundos

Hasta ahora hemos visto que las páginas webs a las que se refieren para hacer las inversiones son clonadas unas de otras, que los certificados que utilizan para demostrar su integridad son falsificados o suplantados y que utilizan direcciones de otras empresas o que aparecen listadas como fraude en las autoridades competentes. Pero, ¿qué pasa con las transacciones? ¿Son reales?

En Maldita.es hemos verificado algunas de las transacciones que nos han enviado como prueba del “retorno de la inversión”, ya sea por los grupos o por mensaje privado. También lo hemos consultado en los registros públicos de las [blockchains](#) utilizadas, principalmente la de Bitcoin y la de Ethereum.

En ambos casos, las transacciones existen (como [esta que nos mandó un usuario como comprobante](#) o [esta otra](#), ambas registradas en la blockchain de Bitcoin). Sin embargo, poco después (normalmente, entre 1 y 10 minutos) [el dinero ingresado en esas carteras](#) sale hacia otra cartera, y así va rebotando de una a otra, hasta que

se divide la cantidad y se bifurca en otras.

Transacciones ⓘ

Cuota	0.00000560 BTC (2.932 sat/B - 1.281 sat/WU - 191 bytes) (5.091 sat/vByte - 110 virtual bytes)	-0.02459142 BTC
Hash	9fc11171b08779be271403ffcaf263186ec40fcb7565099eff5add71b2ecd1c	2022-03-25 07:32
	bc1qt7zgjm2f9tytv8clvgu9fwmwfkpfgetm30eq74m 0.02459142 BTC ➡ bc1qmw976zm8h5np6agtyt7q8qsz304s47vr7ap074 0.02458582 BTC ⬅	
Cuota	0.00000560 BTC (2.917 sat/B - 1.279 sat/WU - 192 bytes) (5.091 sat/vByte - 110 virtual bytes)	+0.02459142 BTC
Hash	ddfa76d6f8786c8daed309da8c28b2f6f7fd69f31d16110899e2d83bd42458f4	2022-03-25 07:31
	bc1q8rnqhfwdz5z3c3dams9x6khg32u3hikz16qz4 0.02459702 BTC ➡ bc1qt7zgjm2f9tytv8clvgu9fwmwfkpfgetm30eq74m 0.02459142 BTC ⬅	

Registros de transacciones comprobadas por Maldita.es.

Iñaki Úcar, doctor en telemática e investigador de la Universidad Carlos III, explica a Maldita.es que es “el modo de actuar habitual que utilizan en cualquier actividad ilegal”: “La transacción se recibe en una cuenta y de ahí la van diluyendo en pequeñas transacciones a través de una red de carteras finales para luego volver a juntarlo en una o varias carteras finales que será desde donde lo conviertan a dinero”, añade.

“Tenemos que tener en cuenta que las direcciones de las carteras, sobre todo las de Bitcoin, son seudónimas, variables y muchas veces de un solo uso”, añade José Antonio Bravo. En la misma línea que Úcar, Bravo agrega que, “una vez mostradas las transacciones, al poco tiempo, son retiradas por los mismos que las han efectuado”.

Nuevos reclamos, mismos métodos

José Antonio Bravo señala que “todas estas plataformas son, sin duda, fraudulentas” y que operan “con el objetivo

de captar fondos de usuarios que conocen muy poco acerca del funcionamiento de las criptomonedas”. “Estos actores se aprovechan de personas que, movidas por la necesidad o por la codicia, quieren obtener altos resultados en sus inversiones que les permitan ser millonarios en breve tiempo”, apunta el experto en fiscalidad de criptomonedas.

Úcar recuerda que estas prácticas se asemejan a “las mismas estafas de siempre pero con la pátina de lo ‘crypto’, que suena más sofisticado y moderno, pero es el mismo modus operandi con nuevo nombre, algo así como [la estafa de Fórum Filatélico](#) pero con bitcoins”.

Eso sí, tal y como advierte Bravo y [como os hemos recomendado en Maldita.es](#), “es importante no invertir en algo que no se conoce, y sobre todo en las criptomonedas, hasta que no se posee un nivel lo suficientemente alto de conocimiento acerca de cómo funcionan, no es conveniente realizar ninguna operativa”.

Si hemos caído en un timo relacionado con las criptomonedas, [lo primero es denunciar a los Cuerpos y Fuerzas de Seguridad del Estado, como nos explicó Ayelén Anzola](#), abogada especializada en materia de blanqueo de capitales relacionado con las operaciones con activos virtuales. Recuperar el dinero es muy complicado por el propio carácter anónimo, descentralizado y sin intermediarios del mundo de las criptomonedas.

“Una vez la transacción está confirmada ya no puede

revocarse, a excepción de algún caso excepcional, con lo que no se podría recuperar el pago, aunque este pertenezca a una transacción hecha en el contexto de una estafa”, indica Cristina Pérez Solà, profesora de la Universitat Oberta de Catalunya (UOC) especializada en criptodivisas y protocolos seguros de blockchain.

Qué hacer para evitar recibir estos mensajes y que no nos añadan a grupos de inversión

¿Qué hacemos si queremos dejar de recibir estos mensajes? Si no queremos que desconocidos nos metan en grupos, Telegram nos ofrece la opción de restringir quién puede añadirnos a uno de estos grupos. En los Ajustes, en la pestaña de Privacidad y Seguridad, podemos elegir que sólo nuestros contactos puedan añadirnos a un grupo. De esta forma, podemos evitar los canales no deseados, aunque no hay forma de evitar recibir mensajes privados de cuentas personales. En estos casos, la mejor opción que tenemos es reportar por spam y bloquear al usuario que nos ha hablado.



Ajustes de Telegram para evitar que personas que no estén en nuestros contactos nos puedan añadir a grupos.

Hemos consultado a Telegram acerca de la presencia de estos grupos en la red de mensajería y las políticas de la empresa contra las posibles estafas que se puedan estar produciendo en ellas, pero al cierre de esta publicación no hemos recibido respuesta.