Riesgos y estafas en el mundo *crypto*

31 de marzo de 2023

Autor: Arnie Zareei Bogoya
Miembro del equipo de trabajo del Proyecto Edufinet

Las criptomonedas y la tecnología *blockchain* están ganando popularidad, pero como cualquier otra industria, también existen riesgos y estafas asociadas a ellas. A continuación, se presentan algunos de los riesgos y estafas más comunes en el mundo de las criptomonedas:

Fraude ICO

La ICO (del inglés *Initial Coin Offering* y en castellano Oferta Inicial de Moneda) es el medio común por el que las empresas recaudan fondos para sus proyectos criptográficos. Los estafadores utilizan una ICO como una forma de atraer inversores incautos con la promesa de una alta rentabilidad de inversión en un proyecto criptográfico.

En estos casos, los estafadores pueden crear un sitio web falso, una documentación engañosa y una promoción exagerada para convencer a los inversores de que inviertan en su proyecto. Una vez que los inversores envían sus criptomonedas al estafador, este desaparece con los fondos, dejando a los inversores sin nada a cambio.

El fraude ICO es una preocupación común en la industria de las criptomonedas, por lo que es importante investigar a fondo cualquier proyecto antes de invertir en él. Los inversores deben verificar la autenticidad del proyecto y su equipo, así como revisar la documentación, el código fuente y cualquier otra información relevante para determinar si la inversión es legítima y segura.

Uno de los ejemplos más sonados de este tipo de fraude fue "El juego del calamar crypto", una estafa en línea que ha sido reportada en las redes sociales y medios de comunicación de distintos países.

Se presenta como un juego en línea que, supuestamente, permite a los usuarios ganar dinero a través de la compra y venta de criptomonedas. Los participantes deben pagar una tarifa de entrada para participar en el juego, y se les promete grandes beneficios si reclutan a otros usuarios.

Sin embargo, era una estafa y los participantes nunca vieron el retorno de su inversión. Este fraude funcionó como una estafa piramidal clásica, el esquema Ponzi, donde los participantes más tempranos reciben el dinero de los nuevos miembros, y cuando no hay más personas que se unan al esquema, los fundadores desaparecen con el dinero y los participantes se quedan sin nada, que es lo que sucedió (recaudaron 3,32 millones de dólares)[1]:

> Streamer watches his life savings go to zero after Squid Game Token rug pulls and drops -99.99%. pic.twitter.com/6hoDGBJeZO
>
> — Mr. Whale (@WhaleWire) November 1, 2021

Estafas de phishing

Las estafas de phishing son comunes y pueden ser muy peligrosas para los inversores. El phishing es una técnica que utilizan los ciberdelincuentes para obtener información confidencial, como contraseñas y datos financieros, haciéndose pasar por una entidad legítima. En el caso de las criptomonedas, los estafadores pueden utilizar el phishing para robar los datos de acceso a las billeteras de criptomonedas de las víctimas.

Los estafadores de phishing pueden crear sitios web falsos que se parezcan mucho a los sitios web de intercambios de criptomonedas legítimos o billeteras de criptomonedas. Estos sitios web falsos pueden incluir formularios de inicio de sesión y solicitar a los usuarios que ingresen información de su cuenta,

incluyendo sus contraseñas y frases de recuperación. Los estafadores también pueden enviar correos electrónicos de phishing a los usuarios, solicitando que hagan clic en un enlace que parece legítimo, pero en realidad dirige al usuario a un sitio web falso.

Es importante que los usuarios de criptomonedas se protejan de las estafas de phishing. Algunas formas de hacerlo son:

- Verificar la URL del sitio web antes de ingresar cualquier información de inicio de sesión o financiera, por ejemplo, con la información que nos proporciona el candado.
- No hacer clic en enlaces en correos electrónicos sospechosos o no solicitados.
- Habilitar la autenticación de dos factores en todas las cuentas de criptomonedas para aumentar la seguridad de la cuenta, como el uso de una aplicación externa que nos proporcione el doble factor (*Google Authenticator*).
- Utilizar una billetera de hardware, que es menos susceptible al phishing que una billetera de software.

Pump and Dump

Se basa en la manipulación del precio de una criptomoneda mediante tres pasos que incluyen, la compra masiva de un valor («*pump*«), su promoción masiva y engañosa (*"shilling"*), seguida de una venta rápida para obtener ganancias antes de que el precio caiga ("dump").

Veamos cómo funciona esta estafa: un grupo de personas se unen y compran grandes cantidades de una criptomoneda específica para aumentar artificialmente su precio (esto es conocido como «*pump*«). Luego, comienzan a promocionar en línea y en redes sociales la criptomoneda (por ejemplo, grupos de Telegram), utilizando tácticas engañosas o exageradas para atraer a más inversores y hacer que el precio suba aún más. A esta elevación artificial del precio de una criptomoneda se la denomina s*hilling*.

Una vez que el precio ha alcanzado una cotización que proporcione grandes beneficios a los compradores que se han unido para elevar artificialmente su precio, éste vende rápidamente sus acciones o criptomonedas, obteniendo una ganancia significativa (esto es conocido como «*dump*«). Como consecuencia, el precio caiga rápidamente, dejando a los inversores que compraron más tarde con grandes pérdidas.

Por ejemplo, alguien que posee una gran cantidad de una criptomoneda específica podría publicar en línea información falsa o exagerada sobre el proyecto o la moneda para intentar que más personas inviertan en ella y, por lo tanto, aumentar su valor.

CIBERESTAFAS

Un popular streamer estafa 500.000 dólares en criptomonedas a sus fans y se compra un Tesla

• Ice Poseidon ha reconocido parcialmente las acusaciones, pero ha descartado devolver el dinero

Fuente: La Vanguardia.

Estafas de *exchanges*

Las estafas de *exchanges* se refiere a una forma de fraude en la que una plataforma de intercambio de

criptomonedas toma el dinero de sus clientes sin ofrecer ningún servicio a cambio, o realiza operaciones fraudulentas en su contra. Estas estafas pueden tomar varias formas, incluyendo:

- Cierre súbito: puede cerrar repentinamente y desaparecer con los fondos de sus clientes sin previo aviso.
- Operaciones fraudulentas: puede realizar operaciones fraudulentas que benefician a los propietarios o administradores del *exchange*, en lugar de los clientes.
- Robo: puede sufrir un robo por parte de un hacker, lo que resulta en la pérdida de los fondos de los clientes.
- Trading falso: puede anunciar que realiza operaciones de trading en nombre de sus clientes, pero en realidad no realiza ninguna operación y simplemente roba los fondos de los clientes.

Para evitar las estafas de exchanges, es importante investigar a fondo cualquier plataforma de intercambio de criptomonedas antes de depositar fondos. Los inversores deben verificar que el *exchange* tenga una reputación sólida en la comunidad de criptomonedas, revisar los términos y condiciones de la plataforma y leer las reseñas de los usuarios. También es importante utilizar billeteras de criptomonedas fuera del *exchange* para almacenar sus fondos, lo que reduce el riesgo de pérdida de fondos en caso de que el exchange sea víctima de una estafa.

Es importante ser cauteloso y tomar medidas de seguridad adecuadas al invertir en criptomonedas. Realizar investigaciones exhaustivas y tener una estrategia de inversión clara son las mejores formas de evitar caer en estafas y minimizar los riesgos asociados.

Atribución: Imagen de vectorjuice en Freepik

---

[1]
https://www.xataka.com/criptomonedas/criptomoneda-juego-calamar-ha-resultado-ser-timo-se-derrumba-a-cero-sus-creadores-desaparecen-llevandose-millones-dolares