CiberData. Núm. 1, 2025, pp. 19-23

CRIPTOMONEDAS Y FRAUDE: ESTAFAS DE INVERSIÓN

Dra. Patricia Saldaña-Taboada
Universidad de Málaga - España
Orcid: 0000-0002-9989-7457

Resumen. Las criptomonedas han pasado de ser una innovación en el comercio electrónico a una herramienta para la comisión de delitos. En los últimos años han atraído a criminales que las utilizan para favorecer el desarrollo de estafas de inversión. Estas estafas no dependen solo de la tecnología, sino de estrategias de captación altamente persuasivas, ingeniería social y, más recientemente, el uso de Inteligencia Artificial para crear contenido falso. La prevención debe centrarse en disuadir estos mecanismos de manipulación más que en la prohibición del uso de los criptoactivos.
Palabras clave.Estafas de inversión, Criptomonedas, Ingeniería social, Esquema piramidal

Abstract.Cryptocurrencies have evolved from being an innovation in e-commerce to a tool for committing crimes. In recent years, they have attracted criminals who use them to facilitate investment scams. These scams rely not only on technology, but also on highly persuasive recruitment strategies, social engineering and, more recently, the use of artificial intelligence to create fake content. Prevention efforts should focus on deterring these manipulation mechanisms rather than prohibiting the use of crypto assets.
Keywords. Investment scams, Cryptocurrencies, Social engineering, Pyramid schemes

Cómo citar: Saldaña-Taboada, Patricia (2025). "Criptomonedas y fraude: estafas de inversión". En CiberData, núm. 1, 2025, pp. 19-23. Disponible en:

1. Las criptomonedas como herramienta para la comisión de ciberdelitos

Las criptomonedas, creadas en 2008 a partir del Bitcoin fueron concebidas como una alternativa descentralizada al sistema bancario tradicional (Nakamoto, 2008). Son monedas virtuales protegidas mediante criptografía, que permiten realizar transacciones entre pares (peer-to-peer) sin intermediarios financieros. Sin embargo, esta descentralización y su anonimato relativo atrajeron la atención de aquellos con motivaciones delictivas.

El punto de inflexión en la vinculación entre criptomonedas y delitos lo marcó la introducción del Bitcoin como forma de pago en el mercado clandestino “Silk Road” (Christin,

2013). Desde entonces, su uso se ha expandido a todo tipo de actividades delictivas: crimen organizado, financiación del terrorismo, y por supuesto, cibercrimen.

2. Estafas cometidas con criptomonedas

En España, preocupa especialmente el uso de criptomonedas en delitos contra el patrimonio como el blanqueo de capitales y, con especial intensidad, las estafas.

Como ocurre en cualquier estafa tipificada en el Código Penal (art.248CP), el núcleo del delito sigue siendo el mismo: engaño con ánimo de lucro para inducir a error a la víctima, que realiza un acto de disposición patrimonial en perjuicio propio o ajeno. Lo que cambia en este caso es el medio: las criptomonedas se convierten en el vehículo idóneo para dar verosimilitud al engaño y dificultar el rastreo posterior de los fondos.

Las tipologías de estafas vinculadas al uso de criptomonedas son variadas y en constante evolución. Uno de los ejemplos son las Rug pull (tirón de alfombra), para la que los estafadores crean tokens, NFT o supuestos proyectos de criptomonedas que prometen elevadas rentabilidades. Atraen capital mediante campañas agresivas, y una vez tienen suficientes fondos, desaparecen sin dejar rastro. Un ejemplo reciente es el caso de la criptomoneda "$Libra", promocionada por el presidente argentino Javier Milei (Salvador, 2025). Relacionado con esto se encuentran también los Exit scams o "estafas de salida" en los que el fraude se produce cuando plataformas aparentemente legítimas de compraventa de criptomonedas cesan sus operaciones de forma repentina y desaparecen con los fondos de los usuarios. El caso más paradigmático ha sido el de "Mt.Gox 2" (Ibarra, 2021).

No obstante, las estafas menos sofisticadas y más comunes son las de phishing y suplantación de plataformas legitimas, en las que los atacantes crean páginas web que imitan servicios reales -billeteras digitales, exchanges o incluso bancos- y atraen a las víctimas con pretextos como premios, alertas de seguridad o supuestas actualizaciones (Ministerio Público Fiscal, 2024). Una vez el usuario introduce sus credenciales, los estafadores acceden a sus fondos y los transfieren a monederos imposibles de rastrear.

3. Estafas de inversión con criptomonedas

Las estafas de inversión merecen una atención especial por su impacto económico y social. El desconocimiento generalizado sobre el funcionamiento de las criptomonedas, sumado a las promesas irreales de rentabilidad, han permitido a los delincuentes construir entramados sofisticados para atraer y engañar a sus víctimas.

De forma general, las estafas de inversión con criptomonedas comienzan con el estafador diseñando una estructura de captación que le permite aproximarse a potenciales víctimas. Una vez establecida la conexión frecuentemente a través de redes sociales, correos electrónicos o incluso conocidos , utiliza un discurso persuasivo sobre las supuestas ventajas de invertir en criptomonedas, atrayendo a la víctima con la promesa de altos rendimientos a medio o largo plazo. Una vez la víctima accede, el delincuente facilita los mecanismos de inversión, bien mediante transferencia de dinero fiduciario, bien directamente en criptomonedas. En muchos casos, se simulan rendimientos falsos a través de plataformas diseñadas para mostrar beneficios inexistentes, lo que incentiva nuevas aportaciones económicas. Cuando la víctima solicita retirar sus fondos o los beneficios prometidos, se le imponen condiciones adicionales (pagos, comisiones, contratación de servicios), o directamente se bloquea el acceso. Finalmente, cuando el estafador percibe que no obtendrá más dinero,

desaparece con el capital recaudado.

En ciertas ocasiones, el fraude evoluciona hacia un esquema piramidal: la víctima, para recuperar su inversión o acceder a beneficios, debe captar a nuevos participantes. Las ganancias aparentes de los primeros miembros se nutren de los fondos de los últimos, en un ciclo que se sostiene hasta el colapso del sistema. Aunque se trata de una metodología clásica, la irrupción de las criptomonedas ha facilitado su expansión global. Un ejemplo paradigmático de este delito en España es el de la macroestafa "Arbistar" investigada por la Fiscalía de la Audiencia Nacional, que habría recaudado para los estafadores más de 6000 bitcoins (valorados en cerca de 600 millones de euros), afectando a miles de víctimas (Agencia EFE, 2025).

3.1. Mecanismos de captación: del falso bróker al romance virtual

El éxito de este tipo de fraude depende, en gran medida, de los métodos empleados para atraer y convencer a la víctima. La fase de captación es esencial, ya que si no se establece el vínculo de confianza la inversión no llegaría a producirse.

Los delincuentes suelen adoptar roles persuasivos como brókeres expertos, asesores financieros o incluso se valen de conocidos de su entorno. Es común el uso de redes sociales, aplicaciones de mensajería o plataformas de citas para iniciar el contacto. En este sentido, ha aparecido el termino Pig butchering ("engorde del cerdo"), que consiste en que, tras una fase de contacto prolongado y aparentemente desinteresado, el estafador establece una relación de confianza con la víctima y una vez se ha generado ese vínculo, se introduce la propuesta de inversión (Acharya & Holz, 2024). Esta modalidad se vincula con las llamadas estafas románticas, que a través de una supuesta relación romántica, aprovechan la intimidad emocional para manipular la voluntad de la víctima (Cross, 2023).

Especialmente frecuente es la figura del falso bróker, que asegura una alta cualificación técnica y experiencia en inversiones con criptomonedas. A través de este perfil profesional, persuade a la víctima para invertir bajo su intermediación (Agencia EFE, 2023).

3.2. Uso de tecnologías emergentes y manipulación digital

El avance tecnológico ha elevado el nivel de sofisticación de estas estafas. Los delincuentes emplean técnicas de marketing digital para construir una narrativa de éxito e inducir a la inversión. Para ello, crean perfiles falsos en redes sociales, páginas web clonadas y generan material gráfico, desde capturas de pantallas manipuladas hasta vídeos y anuncios falsos. Todo ello para mostrar a las potenciales víctimas los beneficios esperados de una inversión con criptoactivos.

En muchos casos se está observando, fruto de la sofisticación y adaptación de los criminales a las nuevas tecnologías, que se utilizan sistemas de Inteligencia Artificial (IA) para crear contenido falso protagonizado por celebridades nacionales que supuestamente avalan la inversión (Ministerio del Interior, 2025). Se reproducen imágenes, voces y testimonios digitales que inducen a error. Las víctimas, al ver rostros conocidos "recomendando" los criptoactivos, creen estar ante una oportunidad legítima y segura (Ministerio del Interior, 2025).

A través de enlaces disponibles en estos contenidos, se redirige al usuario a páginas web falsas, diseñadas para simular medios de comunicación o casas de cambio reales. En estas páginas se ofrece un vídeo explicativo y se proporcionan contactos para iniciar la inversión (Europa Press, 2024). Además, algunos grupos delictivos llegan a instalar software de control remoto en los dispositivos

de las víctimas, con el que acceden directamente a sus cuentas bancarias o wallets, ampliando el alcance y el daño de la estafa (20minutos, 2023).

4. Conclusiones y recomendaciones

Las estafas de inversión con criptomonedas han crecido de forma significativa, generando pérdidas millonarias y afectando a miles de víctimas, que, en muchos casos, no encuentran mecanismos efectivos de restitución. Las características propias de los criptoactivos dificultan la recuperación de los fondos y la persecución de los responsables, planteando desafíos para los sistemas de justicia penal y los legisladores.

Más allá del componente tecnológico, el éxito de estas estafas se basa en: estrategias de captación altamente persuasivas, utilización de identidades falsas o manipuladas, explotación emocional de las víctimas y sobre todo, el desconocimiento de los riesgos reales asociados a las inversiones con criptoactivos. A menudo las criptomonedas no son el medio real de inversión, sino un simple gancho para atraer a la víctima. Por tanto, el foco de la prevención no debe estar únicamente en la regulación de las criptomonedas, sino en disuadir el éxito de los mecanismos de ingeniería social que permiten el fraude, especialmente en aquellos casos sofisticados que utilizan sistemas de Inteligencia Artificial.

5. Referencias

20minutos. (2023, noviembre 14). Recuperan más de 10.000 euros estafados con inversiones en criptomonedas. 20 minutos. https://www.20minutos.es/noticia/5190092/0/recuperan-mas-10000-euros-estafados-con-inversiones-criptomonedas/

Acharya, B., & Holz, T. (2024). An Explorative Study of Pig Butchering Scams (Versión 1). arXiv. https://doi.org/10.48550/ARXIV.2412.15423

Agencia EFE. (2023, julio 6). Detenido por estafar 2,5 millones simulando ser bróker de inversión en criptomonedas. 20minutos. https://www.20minutos.es/noticia/5145017/0/detenido-por-estafar-2-5-millones-simulando-ser-broker-inversion-criptomonedas/

Agencia EFE. (2025, mayo 28). La Fiscalía asegura que la estafa con criptomonedas de Arbistar ganó cerca de 600 millones de euros en bitcoins desaparecidos. 20minutos. https://www.20minutos.es/noticia/5716602/0/criptomonedas-estafa-fiscalia-asegura-arbistar-gano-600-millones-bitcoins-desaparecidos/

Christin, N. (2013). Traveling the silk road: A measurement analysis of a large anonymous online marketplace. Proceedings of the 22nd International Conference on World Wide Web, 213-224. https://doi.org/10.1145/2488388.2488408

Cross, C. (2023). Romance baiting, cryptorom and 'pig butchering': An evolutionary step in romance fraud. Current Issues in Criminal Justice, 0(0), 1-13. https://doi.org/10.1080/10345329.2023.2248670

Europa Press. (2024, marzo 18). Aumentan las estafas de criptomonedas con imágenes de famosos españoles como Broncano y Pedroche para robar dinero. Europa Press PortalTIC. https://www.europapress.es/portaltic/ciberseguridad/noticia-aumentan-estafas-criptomonedas-imagenes-famosos-espanoles-broncano-pedroche-robar-dinero-20240318153142.html

Ibarra, J. (2021, julio 3). 7 mayores robos de bitcoin de la historia. CriptoNoticias. https://www.criptonoticias.com/seguridad-bitcoin/7-mayores-robos-bitcoin-historia/

Ministerio del Interior. (2025, abril 7).

Detenidas seis personas por estafar más de 19 millones de euros usando inteligencia artificial. http://platon:10100/opencms/es/detalle/articulo/Detenidas-seis-personas-por-estafar-mas-de-19-millones-de-euros-usando-inteligencia-artificial/

Ministerio Público Fiscal. (2024, septiembre 25). Dieron de baja y alertan sobre un sitio falso sospechado de captar credenciales de cuentas de la plataforma Binance. https://www.fiscales.gob.ar/ciberdelincuencia/dieron-de-baja-y-alertan-sobre-un-sitio-falso-sospechado-de-captar-credenciales-de-cuentas-de-la-plataforma-binance/

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org

Salvador, R. (2025, febrero 22). Qué es el «rug pull», y cómo arruinó en 6 horas a 40.000 inversores en la criptomoneda de Milei. La Vanguardia. https://www.lavanguardia.com/internacional/20250222/10411634/que-es-rug-pull-arruino-inversores-libra-criptomoneda-milei.html