Criptomonedas

Criptomonedas y estafas: Un análisis de los fraudes más comunes

Sara Abreu Hernández

Especialista en IA y Análisis de datos

INTRODUCCIÓN

Las criptomonedas han revolucionado el mundo financiero, ofreciendo nuevas oportunidades de inversión, descentralización y anonimato. Sin embargo, este mismo ecosistema ha dado lugar a un aumento significativo de fraudes y estafas. La falta de regulación en muchos países y el desconocimiento de los usuarios han permitido que los ciberdelincuentes desarrollen estrategias cada vez más sofisticadas para engañar a inversores y entusiastas del sector.

Este informe tiene como objetivo identificar patrones comunes en las estafas de criptomonedas, analizando los métodos más utilizados por los estafadores, los términos empleados para atraer víctimas y las plataformas más afectadas. A través de la recopilación y análisis de datos, se busca detectar tendencias geográficas y temporales, así como explorar posibles modelos predictivos que ayuden a prevenir futuros fraudes.

Para ello, se utilizarán fuentes de datos como Crypto Scam DB, Blockchain Explorer y conjuntos de datos disponibles en Kaggle. Mediante herramientas de análisis de datos y visualización, se examinarán las características principales de estas estafas y su impacto en la comunidad cripto. Finalmente, se presentarán conclusiones y recomendaciones para mitigar los riesgos y mejorar la seguridad en el ecosistema de las criptomonedas.

HIPÓTESIS

Los fraudes relacionados con criptomonedas, particularmente las estafas en plataformas como Twitter, Telegram y sitios de phishing, son más frecuentes en determinadas categorías y subcategorías (como el "trust trading" en la categoría "scamming" o los fraudes de "fake ICO"). Además, las direcciones asociadas a estas estafas están generalmente vinculadas a plataformas específicas que utilizan para recibir fondos de las víctimas.

MATERIAL

1. Dataset: Utilicé el "Cryptocurrency Scam Dataset" disponible en Kaggle (https://www.kaggle.com/datasets/zongaobian/cryptocurrency-scam-dataset), que incluye información sobre URLs de estafas, descripciones de los fraudes, las plataformas implicadas y direcciones de billeteras de criptomonedas.
2. Herramientas de análisis:
    a. **Lenguaje de programación**: Python
    b. **Librerías utilizadas**: Pandas, Matplotlib, Seaborn, NetworkX, Numpy, y

urllib para el procesamiento y análisis de datos.

c. **Plataforma**: Kaggle para la realización del análisis y la creación de visualizaciones.

PROCEDIMIENTO

1. Definir el objetivo del proyecto
2. **Cargar y explorar los datos**: Se cargaron los archivos `urls.csv` y `uris.csv` desde el dataset y se inspeccionaron las columnas y tipos de datos.
3. **Limpieza de datos**: Se realizaron varias operaciones de limpieza, eliminando filas nulas, transformando las direcciones de Ethereum y normalizando las descripciones.
4. **Análisis de URLs de estafas**: Se extrajeron las plataformas más usadas (por ejemplo, dominios populares en estafas) y se visualizaron las distribuciones de las URLs fraudulentas.
5. **Análisis de categorías y subcategorías**: Se analizaron las categorías de estafas, como "scamming", "phishing" y "fake ICO", y se exploraron las subcategorías asociadas.
6. **Análisis de plataformas y reporteros**: Se evaluaron las plataformas que más contribuyen a las estafas y los reporteros que identifican las estafas.
7. **Análisis de redes de conexiones entre estafadores**: Se creó una red de conexiones entre plataformas, reporteros y sitios de estafas usando NetworkX.
8. **Visualización**: Se generaron gráficos de barras, histogramas y redes para presentar los resultados.

DATOS

Nombre	Descripción
URLs de estafas:	Incluyen dominios asociados con fraudes en criptomonedas
Categorías y subcategorías:	Los datos contienen etiquetas de categorías como "Phishing", "Scamming", "Fake ICO", entre otras

Descripciones:	Se incluyen descripciones detalladas de las estafas reportadas, lo que permitió identificar patrones en el lenguaje utilizado.
Direcciones de criptomonedas:	Algunas filas contienen direcciones de Ethereum y otras criptomonedas que los estafadores usaron para recibir fondos.
Plataformas y reporteros:	Las plataformas involucradas en las estafas y las entidades que reportan estas estafas.

RESULTADOS

Las plataformas más comunes para las estafas fueron **Twitter**, **Telegram** y sitios con dominios como **medium.com**.

1. Las categorías de estafa más comunes fueron **Scamming**, **Phishing** y **Fake ICO**, con subcategorías como **Trust Trading** en "scamming" y **MyEtherWallet** en "phishing".
2. **CryptoScamDB** fue la fuente de información más citada en el reporte de estafas.
3. No se encontraron direcciones válidas de Ethereum asociadas a las estafas dentro del dataset.
4. El análisis de las redes de conexiones mostró que **CryptoScamDB** y **Twitter** están fuertemente conectados, con Twitter siendo un canal popular para la difusión de estafas.

CONCLUSION

El análisis mostró que las estafas de criptomonedas son prevalentes en plataformas como Twitter y Telegram, con algunas categorías y subcategorías dominando el panorama, como "scamming" y "phishing".

Aunque se intentó analizar las direcciones de criptomonedas asociadas a las estafas, no se encontró información válida en el dataset. Sin embargo, la investigación proporcionó una visión sobre la prevalencia de estas estafas en diferentes plataformas y categorías.

Es esencial seguir monitoreando las plataformas y las tácticas de los estafadores para mejorar la seguridad en el ecosistema de criptomonedas.

REFERENCIAS

1. **Dataset**: "Cryptocurrency Scam Dataset" de Zongao Bian, disponible en Kaggle (https://www.kaggle.com/datasets/zongaobian/cryptocurrency-scam-dataset).
2. **Herramientas**: Pandas (https://pandas.pydata.org/), Matplotlib (https://matplotlib.org/), Seaborn (https://seaborn.pydata.org/), NetworkX (https://networkx.github.io/).
3. **Investigación adicional**: Artículos y estudios sobre fraudes de criptomonedas, como los informes de CryptoScamDB.