LISA Institute

Memoria Trabajo Fin de Máster

Estrategias de Prevención y Detección de Criptofraudes:

El Caso CoinBlack-Wendimine

Autora: Aitana González Mejía

Tutora: Icíar Iriondo

Máster de Analista Criminal y Criminología Aplicada

Madrid, Julio 2025

Índice

1. Introducción

Este trabajo aborda el fenómeno del criptofraude desde una perspectiva aplicada, tomando como referencia el caso *CoinBlack-Wendimine*, una operación fraudulenta de alcance transnacional que combinó el uso de tecnologías emergentes con estrategias de manipulación digital. A través del análisis de este caso, se pretende identificar los factores que facilitaron su ejecución, examinar las debilidades normativas e institucionales que lo permitieron y proponer medidas concretas para su detección y prevención en contextos reales de auditoría, análisis financiero y regulación.

El informe técnico resultante está dirigido a la firma *Ernst & Young* (EY), con especial atención a sus áreas de riesgos emergentes, cumplimiento normativo y prevención del blanqueo de capitales. En él se formulan recomendaciones operativas orientadas a fortalecer la capacidad de respuesta de la organización frente a esquemas delictivos complejos vinculados al uso de criptoactivos. Este enfoque aplicado responde a la necesidad de adaptar las metodologías tradicionales de control a un entorno financiero cada vez más digitalizado y dinámico.

La presente memoria complementa dicho informe desde un enfoque académico y metodológico. Su función es documentar el proceso de investigación, justificar las decisiones adoptadas y ofrecer una base teórica y analítica que sustente las propuestas formuladas. De este modo, se establece una relación clara entre ambos documentos: mientras el informe constituye el producto final orientado a la práctica profesional, la memoria proporciona el marco conceptual y técnico que lo respalda.

2. Planteamiento del Problema

La expansión de los criptoactivos ha favorecido la aparición de nuevas formas de fraude financiero. Entre ellas, el criptofraude destaca por su carácter trasnacional su sofisticación tecnológica y su capacidad de eludir regulaciones convencionales. El caso *CoinBlack-Wendimine* representa un ejemplo de cómo estos fraudes operan, utilizando IA, *blockchain* y estrategias de marketing engañoso basadas en la manipulación emocional y en los *deepfakes*.

La problemática principal radica en desentrañar cómo estas estructuras criminales logran operar con relativa impunidad y qué herramientas están disponibles – o deberían desarrollarse – para prevenirlas y combatirlas.

2.1 Necesidades del nuevo conocimiento

Ante este escenario, se detectan las siguientes necesidades de conocimiento:

1. Comprender el modus operandi del criptofraude.
2. Detectar debilidades normativas y tecnológicas que lo faciliten.
3. Evaluar herramientas de detección temprana y análisis forense.
4. Proponer medidas aplicables en auditorías internas y procesos de *compliance*.

3. Estrategias de investigación

La investigación parte de una estrategia de análisis de caso, combinada con apoyo bibliográfico especializado y aplicación de técnicas de investigación cualitativa y cuantitativa.

3.1 Hipótesis

El estudio del caso *CoinBlack-Wendimine* permite identificar elementos clave para mejorar la prevención y detección de criptofraudes en entornos financieros digitales.

4. Obtención de información

4.1 Tipos de Fuentes Utilizadas

La recopilación de datos se basó tanto en fuentes primarias como secundarias:

- Primarias: Informes policiales (Europol, Guardia Civil, Policía Nacional), sentencias judiciales, datos extraídos de *blockchain* y plataformas de intercambio.
- Secundarias: Literatura académica (artículos de criminología, derecho financiero), manuales FATF/GAFI, reportes de empresas de ciberseguridad.

4.2 Fiabilidad

Las fuentes utilizadas fueron contrastadas y verificadas con criterios de actualidad, relevancia y procedencia institucional (organismos oficiales, publicaciones indexadas).

5. Tratamiento de la Información

5.1 Técnicas y Herramientas

Para el tratamiento de la información se aplicaron herramientas complementarias:

- Criminología analítica. Identificación de patrones delictivos y modus operandi.
- OSINT (*Open Source Intelligence*). Recopilación de información pública en redes y foros especializados.

- Herramientas de trazabilidad *blockchain*. Uso de *Chainalysis* y *Etherscan* para el rastreo de fondos.
- Estudio de caso. Análisis profundo del caso *CoinBlack-Wendimine* como metodología principal.

6. Métodos y Técnicas de Análisis

Se utilizó una combinación de análisis cuantitativo y cualitativo:

- Análisis cualitativo: Examen detallado de las estrategias utilizadas por los perpetradores para ocultar la estructura del fraude y manipular a las víctimas.
- Análisis cuantitativo: Revisión de transacciones en la *blockchain*, flujos financieros y redes de direcciones asociadas.
- Estudio comparado: Se contrastó el caso *CoinBlack-Wendimine* con otros fraudes similares (Bitconnect, OneCoin) para identificar patrones recurrentes.
- Triangulación de datos: Validación cruzada de información para confirmar hipótesis y aumentar la fiabilidad de los hallazgos.

El análisis evidenció que el uso combinado de anonimato, inteligencia artificial y falta de regulación efectiva fue clave para el éxito del fraude.

7. Difusión de los resultados

7.1 Tipología y Formato del Informe

- Tipo de documento: Informe académico-aplicado con orientación profesional.
- Formato: Documento en formato PDF, acompañado de anexos técnicos, gráficos de red de transacciones y cronología del fraude.
- Resumen ejecutivo: Incluye un resumen enfocado en *stakeholders* de cumplimiento normativo y prevención del delito financiero.

8. Conclusiones y Recomendaciones

8.1 Conclusiones

1. El ecosistema de criptoactivos presenta una serie de características técnicas que, sin un marco regulatorio adecuado, facilitan la comisión de fraudes financieros a gran escala.

2. Las herramientas de análisis *blockchain* y criminología digital pueden ser clave para la detección temprana, pero requieren integración institucional y capacitación especializada.
3. La cooperación internacional sigue siendo insuficiente para actuar de manera eficaz ante fraudes de carácter transnacional y altamente tecnificado.

Aunque centrado en el caso *CoinBlack- Wendemine*, el análisis y las recomendaciones poseen una aplicabilidad general para otras operaciones similares que emplean tecnologías disruptivas con fines delictivos.

8.2 Recomendaciones para EY

- Inversión en herramientas *OSINT* y trazabilidad *blockchain* para análisis forense financiero.
- Formación continua del personal de *compliance* en materia de criptoactivos e inteligencia artificial.
- Desarrollo de alertas tempranas basadas en patrones detectados en fraudes previos.
- Fomento de alianzas interinstitucionales con organismos internacionales y empresas de ciberseguridad.

9. Retroalimentación y aprendizajes del proceso

9.1 Aciertos

- Integración eficaz de herramientas digitales y fuentes abiertas para análisis criminológico.
- Enfoque multidisciplinario que permitió abordar el fenómeno desde el derecho, la economía y la tecnología.

9.2 Dificultades

- Subestimación inicial del papel de la inteligencia artificial como herramienta de persuasión delictiva.
- Limitado acceso a ciertas bases de datos judiciales internacionales por barreras idiomáticas o legales.
- Este estudio reconoce ciertas limitaciones, como la disponibilidad parcial de datos judiciales internacionales y la rápida evolución de los entornos tecnológicos, lo cual obliga a una revisión constante de los métodos de análisis y detección.