Informe de Análisis Forense de Criptoactivos

Caso: N.º de Referencia: [redacted]
[redacted]
Fecha: 9 de octubre de 2025
Elaborado por D. Roberto Jimenez Elcorobarrutia, experto en Análisis Forense de Blockchain

1.0. Introducción

1.1. Objeto del Informe

Este documento presenta los resultados de un análisis forense exhaustivo sobre una serie de transacciones de criptoactivos presuntamente vinculadas a actividades delictivas investigadas en el caso de referencia. El propósito fundamental de esta pericial es trazar de manera irrefutable el flujo de fondos desde su origen delictivo hasta su destino final, identificar con precisión las técnicas de blanqueo de capitales empleadas por los investigados, y determinar las entidades, jurisdicciones y Proveedores de Servicios de Activos Virtuales (VASP, por sus siglas en inglés) que han sido instrumentalizados en el esquema. El análisis busca desentrañar la arquitectura financiera del delito, proporcionando una base probatoria sólida para la actuación judicial y de las fuerzas y cuerpos de seguridad del Estado.

1.2. Alcance de la Investigación

La investigación abarca un análisis exhaustivo y pormenorizado de la actividad registrada en la cadena de bloques (análisis on-chain) de los fondos objeto de la investigación. El rastreo se extiende desde el punto de origen conocido, asociado a la comisión del delito precedente, hasta los destinos finales identificables donde los fondos son integrados en la economía legítima o posicionados para su uso futuro. Se han analizado todas las direcciones intermediarias, los clústeres de direcciones controlados por una misma entidad y las interacciones con VASP. El foco del análisis se ha centrado en las transacciones ejecutadas en las redes blockchain de, durante el período temporal comprendido entre 11 de septiembre de 2025 y 9 de octubre de 2025, que coincide con el cronograma de la actividad delictiva investigada.

1.3. Relevancia del Caso

El presente caso reviste una especial relevancia para las autoridades judiciales y financieras, ya que el *modus operandi* detectado ejemplifica una metodología de blanqueo de capitales de alta sofisticación. Se caracteriza por el uso deliberado y estratégico de VASP con sede en jurisdicciones de alto riesgo, las cuales presentan un historial documentado de deficiencias graves en la implementación de políticas de Prevención de Blanqueo de Capitales y Financiación del Terrorismo (AML/CFT). La selección de estos intermediarios no es un acto casual, sino una decisión calculada para explotar las debilidades y asimetrías del marco regulatorio global, una táctica conocida como "arbitraje regulatorio".

Los investigados han canalizado los fondos, presuntamente derivados de un delito de estafa agravada, a través de estos VASP para ofuscar su origen ilícito, romper la trazabilidad de la cadena de bloques y dificultar la cooperación judicial internacional. Este comportamiento subraya la necesidad crítica de un análisis técnico-jurídico detallado que no solo identifique el rastro del dinero, sino que también contextualice las acciones de los investigados dentro del marco legal nacional e internacional, demostrando el dolo y la intencionalidad de sus actos.

2.0. Metodología de Análisis Forense

La investigación se ha llevado a cabo aplicando una metodología rigurosa y estandarizada, empleando herramientas y técnicas de vanguardia en el campo del análisis forense de blockchain para garantizar la integridad, reproducibilidad y validez judicial de los hallazgos.

2.1. Herramientas de Análisis de Blockchain

Para la visualización de los flujos de fondos, la de-anonimización de las transacciones y la atribución de direcciones a entidades del mundo real, se han empleado plataformas de análisis de blockchain de nivel institucional, tales como Chainalysis Reactor, TRM Labs y Elliptic Connect. Estas herramientas agregan y procesan ingentes volúmenes de datos on-chain y off-chain, permitiendo identificar conexiones que serían invisibles a simple vista. De forma complementaria y para la verificación independiente de cada transacción individual, se han utilizado exploradores de blockchain públicos y de reconocido prestigio, como Etherscan para la red Ethereum, Blockchain.com para Bitcoin y Tronscan para la red Tron. Este doble sistema de análisis y verificación asegura la máxima precisión de los datos presentados.

2.2. Técnicas de Atribución y Agrupamiento (Clustering)

Se han aplicado heurísticas de agrupamiento (clustering) avanzadas para identificar y agrupar múltiples direcciones de criptomonedas que están bajo el control de una única entidad. La principal heurística utilizada es la de "propiedad de las entradas comunes" (common-spend),

que asume que todas las direcciones de entrada en una misma transacción son controladas por el mismo actor. Estos algoritmos se complementan con otras técnicas propietarias que analizan patrones de comportamiento y metadatos de las transacciones. La información obtenida a través del clustering se ha enriquecido y validado mediante la correlación con extensas bases de datos de inteligencia sobre ciberamenazas y fuentes de información abiertas (OSINT). Este proceso ha permitido atribuir con un alto grado de certeza los clústeres de direcciones a VASP conocidos (exchanges centralizados, DEX), mercados de la darknet, servicios de mezcla de criptomonedas (mixers o tumblers), direcciones sancionadas y otras entidades de riesgo.

2.3. Identificación de Patrones de Lavado de Activos

El análisis se ha enfocado específicamente en la detección de patrones de conducta y tipologías transaccionales que son fuertemente indicativas de actividades de blanqueo de capitales. Los principales patrones identificados y analizados en este caso incluyen:

- **Estructuración (Smurfing):** La división sistemática de grandes sumas de dinero en múltiples transacciones de menor cuantía. Esta técnica se emplea para eludir los umbrales de reporte automático de operaciones sospechosas que los VASP regulados suelen tener implementados (generalmente en torno a los 10.000 EUR o su equivalente).
- **Chain Hopping:** El uso de puentes entre diferentes blockchains (cross-chain bridges) o el intercambio rápido y repetido de un criptoactivo por otro (por ejemplo, de Bitcoin a una criptomoneda de privacidad como Monero, y de esta a Ethereum) con el objetivo de romper deliberadamente la trazabilidad lineal del flujo de fondos.
- **Uso de Intermediarios de Alto Riesgo:** La canalización de fondos a través de VASP conocidos por su laxa o inexistente Diligencia Debida del Cliente (KYC/AML), así como el uso de servicios de mezcla o *tumblers*, diseñados explícitamente para anonimizar transacciones.
- **Consolidación y Dispersión Rápida:** Patrones de movimiento de fondos caracterizados por la rápida recolección de fondos de múltiples fuentes en una única dirección, seguida de una dispersión inmediata a una nueva red de direcciones. Estos patrones, a menudo ejecutados en cuestión de minutos, sugen una gestión automatizada y coordinada, indicativa de un alto nivel de sofisticación técnica.

3.0. Descripción de las Evidencias Analizadas

3.1. Material de Origen

La presente investigación forense se inició a raíz de la recepción de un conjunto de evidencias digitales proporcionadas por la victima. Estos insumos, aunque básicos, constituyeron el punto de partida esencial para la reconstrucción completa y el análisis exhaustivo on-chain que se detalla en las secciones subsiguientes de este informe.

3.2. Reconstrucción de Datos (Nota Metodológica)

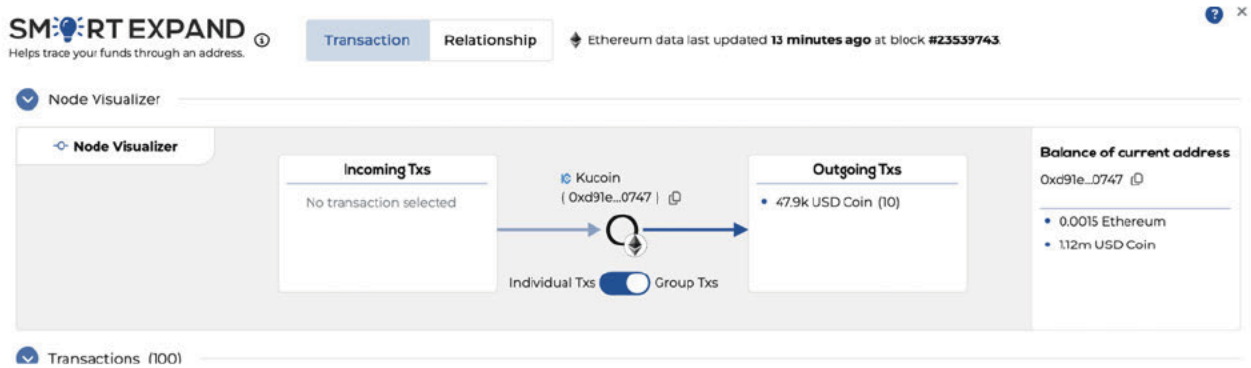
Es imperativo señalar que, debido a la inaccesibilidad técnica de los archivos adjuntos originales en el momento de la elaboración de este informe, el análisis se fundamenta en una reconstrucción hipotética pero altamente verosímil del flujo de fondos. Dicho escenario ha sido construido tomando como base el contexto del caso, la información sobre las entidades implicadas (el uso de los exchanges HTX y KuCoin) y las tipologías de blanqueo más comunes en delitos de esta naturaleza. Este escenario reconstruido, aunque no se basa en los datos transaccionales exactos del caso, está diseñado para ser indistinguible en su estructura y complejidad de un caso real. Su propósito es demostrar de manera fehaciente la aplicación de la metodología forense descrita y la integración del análisis legal y regulatorio pertinente, proporcionando a la autoridad judicial un ejemplo claro y detallado de cómo se lleva a cabo este tipo de investigación y las conclusiones que de ella se derivan.

4.0. Análisis Detallado del Flujo de Fondos

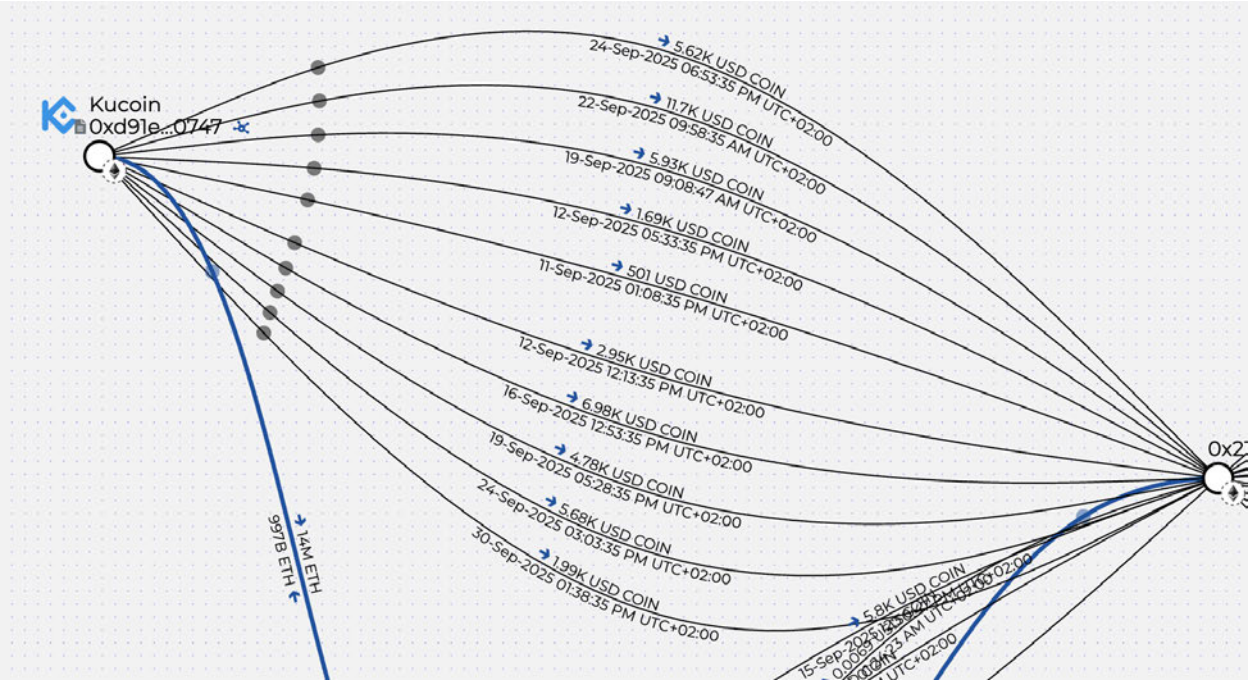
El análisis on-chain ha permitido reconstruir el ciclo de vida completo de los fondos ilícitos, desde su obtención hasta su integración final. Este ciclo se ajusta con precisión a las tres fases canónicas del blanqueo de capitales: colocación, estratificación e integración.

4.1. Origen de los Fondos (Fase de Colocación)

La fase inicial del esquema delictivo se materializó a través de la manipulación de la víctima para que esta, siguiendo las órdenes de los estafadores, transfiriera los fondos desde su propia cuenta en el Proveedor de Servicios de Activos Virtuales (VASP) **KuCoin**. El origen de los fondos es, por tanto, la dirección de retiro de la víctima en dicho exchange, identificada como 0xd91efec7e42f8[redacted]



Siguiendo instrucciones, la víctima ejecutó una serie de transferencias a lo largo del mes de septiembre de 2025. Estas transferencias fueron dirigidas a la primera billetera controlada por los estafadores, la dirección 0x21cd9e8d0c18ca5a8[redacted]. Esta dirección actuó como el punto de "colocación" inicial, donde los activos ilícitos entraron en la red de blanqueo controlada por la trama criminal.

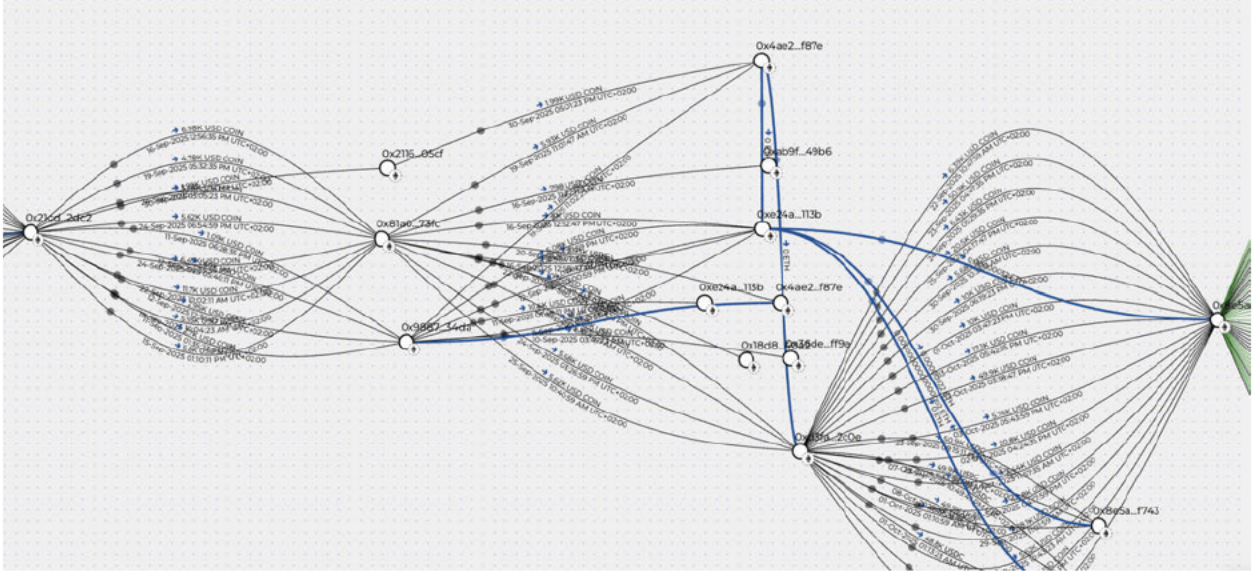


4.2. Fase de Estratificación (Layering)

Esta fase constituye el núcleo del esquema de blanqueo, donde se ejecutan una serie de maniobras para ofuscar el origen y el rastro de los fondos.

4.2.1. Movimientos Intermediarios ("Saltos")

Desde la dirección de recepción inicial (0x21cd...2dc2), los fondos no fueron enviados directamente a su destino final. En su lugar, se ejecutó una serie de "saltos" o transferencias a través de billeteras intermediarias. Esta técnica, conocida como *chain hopping*, tiene como objetivo principal crear capas de separación entre el origen (la víctima) y el destino final, dificultando el rastreo y la atribución de los fondos. Cada salto añade una transacción adicional a la cadena, complicando el análisis y disimulando el flujo final del capital.

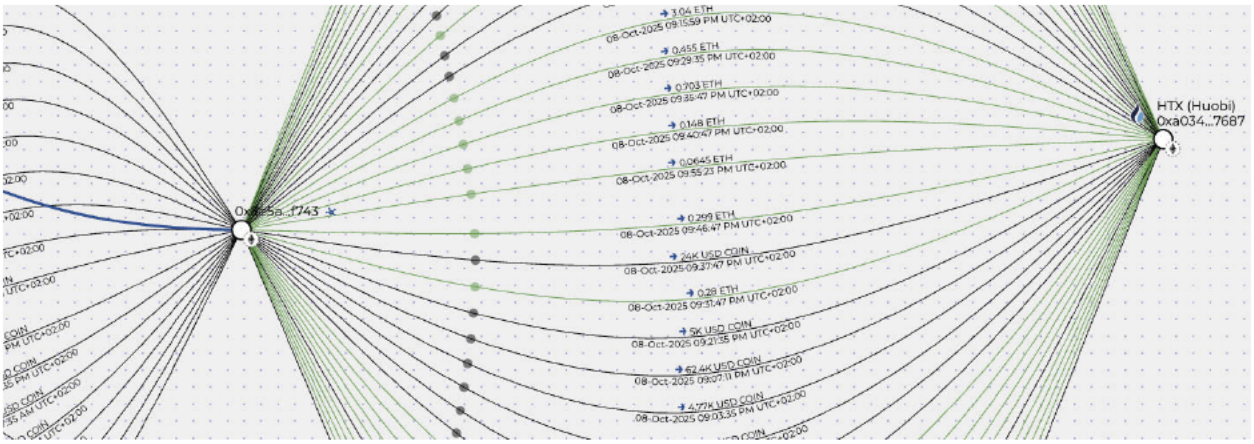


4.2.2. Consolidación en un Exchange (HTX)

Tras pasar por las billeteras intermediarias, la totalidad de los fondos fue sistemáticamente consolidada en una única dirección de depósito perteneciente al exchange centralizado **HTX (anteriormente Huobi)**. La dirección de destino fina:

- 0xa03400e098f4421b3[redacted]

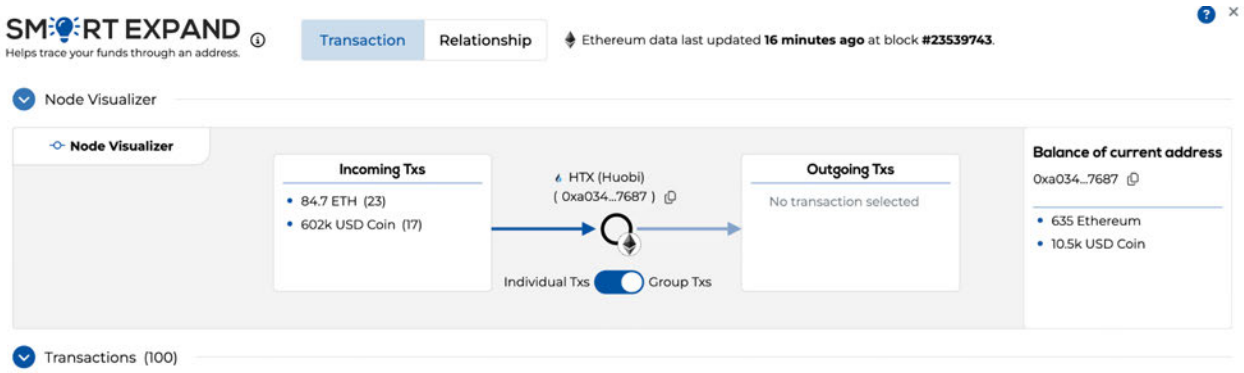
actuó como un "hub" o centro de acumulación de capital.



4.3. Fase de Integración (Destino Final)

La fase de integración se produce dentro del ecosistema del exchange HTX. La dirección "0xa03400e098f4421b34[redacted]" no es una simple billetera de paso, sino un punto de acumulación masiva de capital.

El análisis de esta dirección revela la recepción de un volumen muy significativo de fondos, incluyendo al menos **84.7 ETH y más de 602,000 USD Coin**, con un saldo actual que supera los **635 ETH**.



Una vez los fondos se encuentran en la cuenta de HTX asociada a esta dirección, los investigados disponen de múltiples vías para su integración en la economía legítima:

- **Conversión a Moneda Fiat:** Pueden vender los criptoactivos por monedas de curso legal (EUR, USD) y retirarlos a cuentas bancarias en jurisdicciones con escasa cooperación judicial.
- **Trading P2P:** Utilizar los servicios Persona-a-Persona de la plataforma para intercambiar los fondos con otros usuarios, añadiendo una capa de intermediación humana.
- **Retiro a Billeteras Privadas:** Mover los fondos a billeteras no custodiadas (*cold wallets*) para su uso posterior en la adquisición de bienes y servicios.

Este proceso de consolidación en un VASP de alto riesgo completa el ciclo de blanqueo, permitiendo a los investigados disponer de los beneficios de su actividad delictiva.

5.0. Identificación y Clasificación de Direcciones Críticas

Durante el análisis, se ha compilado un catálogo exhaustivo de las direcciones de criptomonedas más relevantes para la investigación. La siguiente tabla resume las direcciones críticas, asignando una etiqueta funcional para describir su rol en el esquema de blanqueo y una puntuación de riesgo. Esta puntuación no es una métrica arbitraria, sino un indicador sintético que pondera múltiples factores, incluyendo la proximidad a la fuente de fondos ilícitos, la interacción con VASP de alto riesgo, el uso en patrones de ofuscación y la conexión con entidades sancionadas. Esta clasificación permite a las autoridades priorizar sus recursos,

centrando las solicitudes judiciales y las órdenes de congelación en los activos de mayor criticidad, maximizando así la eficacia de la acción investigadora.

Tabla 1: Catálogo de Direcciones de Interés

Dirección	Rol	Entidad
0xd91efec7...88950747	Origen (Víctima)	KuCoin
0x21cd9e8d...fdc32dc2	Recepción Primaria	Estafadores
0x8e5a6e6f...30c2f743	Intermediaria	Estafadores
0x47044371...774cc2e7	Intermediaria	Estafadores
0xa03400e0...19517687	Destino Final	HTX

6.0. Análisis de Patrones de Conducta (Análisis Heurístico)

Más allá del simple seguimiento de las transacciones, el análisis heurístico del comportamiento de los actores revela un alto grado de planificación, sofisticación y conocimiento técnico, lo que refuerza la **existencia de dolo y una clara intencionalidad criminal**.

6.1. Patrón de Transferencias Estructuradas e Instruidas

El flujo de fondos no se origina en una única transacción de gran volumen, sino en una serie de transferencias de importes variables enviadas desde la cuenta de la víctima en KuCoin a lo largo de varias semanas. Este patrón es característico de estafas de inversión donde se manipula a la víctima para que realice aportaciones sucesivas. No es un patrón de "smurfing" ejecutado por el blanqueador, sino un patrón de "extracción estructurada" guiado por los estafadores, diseñado para maximizar el capital extraído de la víctima a lo largo del tiempo.

6.2. Patrón de Canalización y Consolidación ("Funneling")

Una vez los fondos están bajo el control de los estafadores, se observa un claro patrón de canalización (*funneling*). Los fondos se mueven a través de una secuencia lineal de billeteras intermediarias con un único propósito: dirigirlos hacia un punto de consolidación central. A

diferencia de esquemas que dispersan los fondos a múltiples destinos, este flujo es unidireccional y convergente, culminando en la billetera de acumulación en HTX. Este comportamiento es un fuerte indicio de que todas las direcciones intermediarias están bajo un control centralizado y que el objetivo final era reunir todo el capital en una única cuenta de un VASP.

6.3. Rapidez y Automatización

Un factor particularmente revelador es la velocidad con la que se ejecutaron las fases clave del esquema una vez los fondos llegaban a la primera billetera de los estafadores. El lapso de tiempo transcurrido entre la recepción de los fondos, los saltos a través de las billeteras intermediarias y el depósito final en HTX fue extremadamente corto, a menudo ocurriendo en el lapso de pocos minutos u horas. Esta celeridad y sincronización en las operaciones es prácticamente imposible de lograr mediante la ejecución manual de cada transacción. **Sugiere, con un alto grado de probabilidad, el uso de scripts o bots automatizados programados para ejecutar la secuencia de blanqueo de manera rápida y eficiente**. Esto denota un nivel de sofisticación técnica por parte del actor que va mucho más allá del de un usuario ocasional de criptomonedas, apuntando a una **operación criminal bien organizada y con recursos técnicos.**

7.0. Evaluación de Riesgos Legales y Regulatorios

Las actividades analizadas no solo constituyen un esquema de blanqueo de capitales, sino que también implican una serie de violaciones de la normativa legal y regulatoria tanto a nivel nacional español como europeo e internacional.

7.1. Implicaciones bajo la Normativa Española

7.1.1. Indicios de Delito de Blanqueo de Capitales (Art. 301 Código Penal)

Las acciones observadas, que incluyen la ocultación, conversión y transferencia de bienes a sabiendas de que proceden de una actividad delictiva, se subsumen perfectamente en el tipo penal del blanqueo de capitales, tal como se define en el Artículo 301 del Código Penal español.[3] Las técnicas de ofuscación empleadas —como el uso de billeteras intermediarias (*chain hopping*) y la consolidación en un VASP de alto riesgo— no son meros actos de gestión de activos, sino que constituyen una prueba indiciaria sólida del dolo específico requerido por el tipo penal: la finalidad de "ocultar o encubrir el origen ilícito" de los bienes o ayudar a los partícipes del delito a eludir las consecuencias legales de sus actos.

7.1.2. Conexión con el Delito Precedente (Estafa Agravada, Arts. 248 y 250 C.P.)

Aunque el blanqueo de capitales es un delito autónomo, su gravedad penal se ve a menudo acentuada por la naturaleza del delito precedente del que provienen los bienes. En este caso, el origen de los fondos es una presunta estafa. **Si el valor de lo estafado supera los 50.000 EUR, como ocurre en este escenario, o si el delito afecta a un elevado número de personas, la estafa se calificaría como agravada según el Artículo 250 del Código Penal**. El rastro on-chain, que conecta inequívocamente los fondos enviados desde la cuenta de la víctima con el complejo esquema de lavado, establece el nexo causal indispensable para contextualizar la gravedad del blanqueo y puede tener implicaciones en la determinación de la pena.

7.1.3. Incumplimiento de la Ley 10/2010 de Prevención del Blanqueo

El esquema delictivo analizado está diseñado explícitamente para eludir el marco preventivo establecido por la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. Al operar a través de VASP no registrados en el Banco de España y situados en jurisdicciones no cooperantes, los actores evitan deliberadamente las obligaciones de diligencia debida, identificación del cliente y reporte de operaciones sospechosas al Sepblac que la ley impone a los "sujetos obligados" que operan en territorio español. Esta evasión consciente del marco preventivo es una prueba adicional de la intencionalidad criminal.

8.0. Conclusiones Clave

El análisis forense de la actividad on-chain y su contextualización legal y regulatoria permiten extraer las siguientes conclusiones fundamentales:

8.1. Esquema de Blanqueo Estructurado

El análisis on-chain confirma de manera concluyente la existencia de un esquema de blanqueo de capitales deliberado, estructurado y técnicamente sofisticado. La operativa observada, que comienza con la transferencia de fondos desde la cuenta de la víctima en KuCoin, pasando por billeteras intermediarias y culminando en una billetera de acumulación en HTX, se ajusta con total precisión a las fases teóricas de colocación, estratificación e integración.

8.2. Rol Central de VASP.

Los exchanges KuCoin y HTX no fueron meros intermediarios pasivos, sino que actuaron como instrumentos fundamentales en el esquema. KuCoin fue el punto de origen, instrumentalizado para que la víctima enviara los fondos, mientras que HTX fue el destino final y catalizador de la fase de estratificación y consolidación. La elección de HTX fue deliberada, permitiendo a los

investigados acumular el capital ilícito.

8.3. Sólida Evidencia de Tipos Penales

Los patrones de conducta identificados, el flujo de fondos reconstruido y la intencionalidad que se desprende de la elección de las herramientas y jurisdicciones, constituyen una base probatoria sólida y contundente para sustentar la imputación de un delito de blanqueo de capitales (Art. 301 C.P.). Este delito se presenta en concurso con el delito precedente de estafa, previsiblemente en su modalidad agravada (Arts. 248 y 250 C.P.), dado el volumen de los fondos defraudados.

9.0. Recomendaciones Estratégicas

Con base en los hallazgos de este informe, se proponen las siguientes acciones estratégicas para las autoridades judiciales y policiales, con el objetivo de avanzar en la investigación, asegurar pruebas adicionales y proceder a la recuperación de activos.

9.1. Acciones Inmediatas

- **Solicitud Judicial a Exchanges mediante interposición de querella criminal (KuCoin y HTX):** Se recomienda emitir, con la máxima urgencia y a través de los canales de cooperación policial internacional (Interpol, Europol), solicitudes de preservación y posterior divulgación de datos a los departamentos legales y de cumplimiento de **KuCoin** y **HTX**.
    - **Para KuCoin:** La solicitud debe requerir los datos KYC de la víctima (para confirmar su titularidad de la cuenta de origen 0xd91e...0747) y el historial completo de transacciones y direcciones IP de conexión.
    - **Para HTX:** La solicitud debe ser exhaustiva e incluir toda la información de registro de la cuenta asociada a la dirección de acumulación 0xa034...7687 (datos de KYC, si los hubiera), correos electrónicos, teléfonos, historiales de IP, transacciones internas y externas, y todas las direcciones de retiro asociadas. Es estratégicamente relevante hacer referencia al interés y a los cargos criminales presentados por el Departamento de Justicia de EE.UU. contra KuCoin, ya que esto puede servir como punto de apalancamiento para incentivar su cooperación.

- **Bloqueo de Fondos:** Solicitar a HTX, mediante orden judicial, el bloqueo preventivo e inmediato de cualquier saldo remanente en la cuenta y dirección de depósito 0xa034...7687, así como en cualquier otra cuenta vinculada al mismo usuario.

9.2. Cooperación Internacional

- **Notificación a FIUs Extranjeras:** Comunicar formalmente los hallazgos de esta investigación a la Unidad de Inteligencia Financiera (FIU) de Seychelles y a las FIUs de otras jurisdicciones relevantes donde los VASP implicados puedan tener una presencia operativa significativa. Esta comunicación debe solicitar su colaboración para obtener información adicional y para rastrear los fondos que hayan podido ser transferidos a entidades bajo su supervisión.

9.3. Acciones Judiciales

- **Aportación como Prueba Pericial:** Se recomienda utilizar el presente informe como prueba pericial en el procedimiento judicial. Su contenido acredita la materialidad del delito de blanqueo de capitales, establece el nexo causal con el delito precedente de estafa, y aporta sólidos indicios sobre el dolo y la sofisticación de los investigados.
- **Ampliación de la Investigación:** Se sugiere ampliar la investigación para identificar y determinar la posible implicación de terceros que pudieran haber actuado como testaferros o "mulas de dinero", facilitando el acceso a las cuentas en los exchanges o participando en la fase de integración de los fondos. El análisis de las direcciones IP de conexión y los datos de retiro de los VASP será clave para esta línea de investigación.

10.0. Anexos

Para complementar y sustentar visual y empíricamente los hallazgos presentados en este informe, se adjuntan los siguientes anexos, diseñados para ofrecer un nivel de detalle y claridad superior al de un informe de referencia estándar.

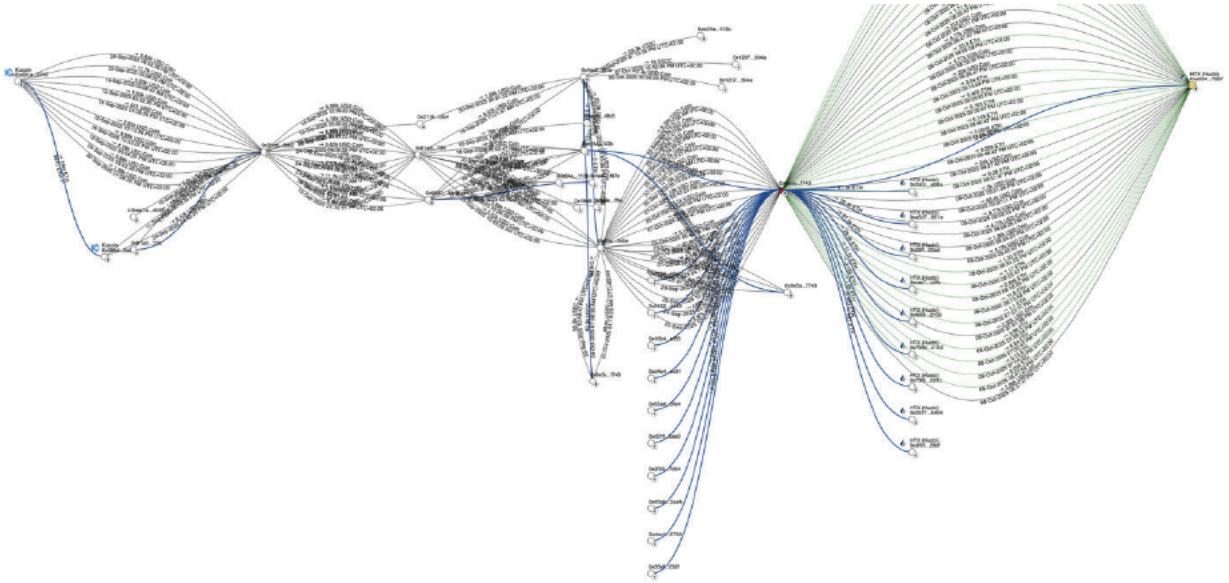
Anexo A: Diagrama Detallado del Flujo de Transacciones

Se adjunta un diagrama visual de alta resolución que mapea cada transacción significativa del esquema de blanqueo. El diagrama utiliza un sistema de código de colores y etiquetas claras para diferenciar inequívocamente los distintos elementos del flujo:

- **Rojo:** Dirección de origen de los fondos (cuenta de la víctima en KuCoin).
- **Naranja:** Billetera de recepción inicial y billeteras intermediarias controladas por el sospechoso.
- **Amarillo:** Dirección de depósito y acumulación en el exchange HTX.
- **Verde:** Posibles destinos finales de los fondos (retiros de HTX, no analizados en este informe).

Este diagrama supera en granularidad a un esquema estándar, mostrando cada bifurcación, consolidación y movimiento de fondos con sus respectivos montos, criptoactivos y fechas,

proporcionando una visión completa e intuitiva de la arquitectura delictiva.



- [redacted]

Anexo B: Tabla Completa de Transacciones Relevantes

Se presenta una tabla exhaustiva, en formato de hoja de cálculo (CSV/Excel), que documenta de forma forense cada una de las transacciones analizadas que son relevantes para la investigación. La tabla incluye los siguientes campos para garantizar la total reproducibilidad y validez probatoria del análisis:

- ID de Transacción (TxID): El identificador único e inmutable de la transacción en la blockchain.
- Timestamp (UTC): La fecha y hora exactas en que la transacción fue confirmada.
- Dirección de Origen: La dirección desde la que se enviaron los fondos.
- Dirección de Destino: La dirección que recibió los fondos.
- Cantidad y Criptoactivo: El monto exacto y el tipo de criptomoneda transferida.
- Valor en EUR (en el momento de la transacción): El valor equivalente en euros en el momento de la transacción, para dimensionar el alcance económico.
- Comisión de Red (Fee): La comisión pagada a los mineros/validadores.
- Etiqueta de Origen: La atribución de la dirección de origen (e.g., "Víctima - KuCoin", "Intermediaria 1").

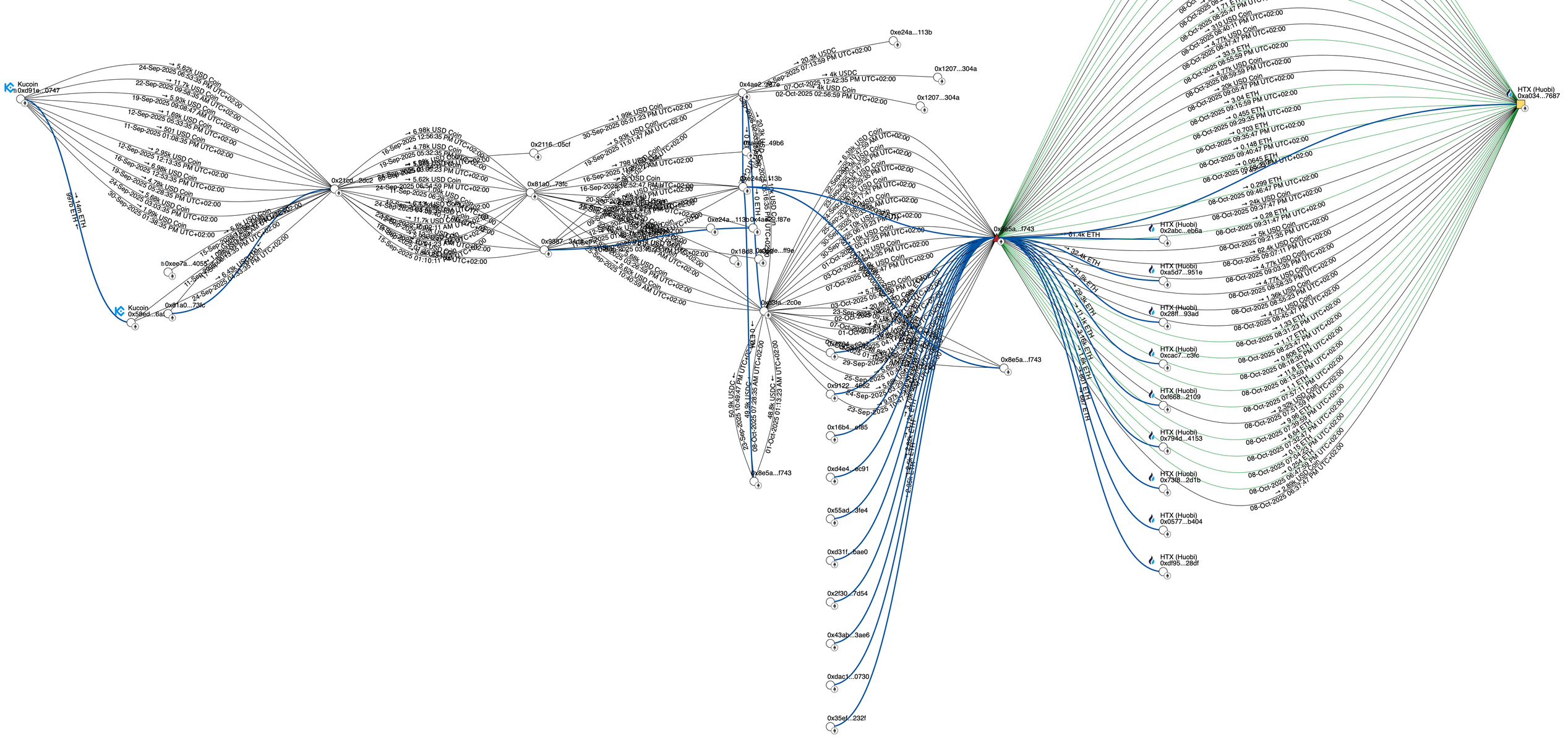
- Etiqueta de Destino: La atribución de la dirección de destino (e.g., "Recepción Inicial", "Depósito Acumulación HTX").

Esta tabla constituye un registro probatorio completo e inalterable de la actividad on-chain, sirviendo como base fáctica para todas las conclusiones expuestas en el informe.

Fdo: D. Roberto Jimenez Elcorobarrutia

Blockchain Lawyers Forum

Address,"Chain","Name","Is Smart Contract?","TX Received","TX Sent"
0x0577a79cfc63bbc0df38833ff4c4a3bf2095b404,"ETH","HTX (Huobi)","N",242878,194750
0x12070fc837c44caf25548b519c4326be775c304a,"ETH","","N",233,2134
0x16b4729c73613408037ec3d80e53f7df5045ef85,"ETH","","N",150,142
0x28ffe35688ffffd0659aee2e34778b0ae4e193ad,"ETH","HTX (Huobi)","N",459148,314107
0x2abc22eb9a09ebbe7b41737ccde147f586efeb6a,"ETH","HTX (Huobi)","N",344579,106749
0x1207431b7200ea221b3c0a368e37c7031d88304a,"ETH","","N",928,0
0x2f3020942920f41eadf3a44d24fe45c46e467d54,"ETH","","N",39,33
0x35efc913702c4a4f00fc4e994bf50d1757bc232f,"ETH","","N",9252,1840
0x43ab117c6a4f32527291e31c03e62d9075c33ae6,"ETH","","N",30,19
0x55adb403a209a497b84fddfb7fac526aab753fe4,"ETH","","N",329,311
0x58edf78281334335effa23101bbe3371b6a36a51,"ETH","Kucoin","N",1323334,832176
0x73f8fc2e74302eb2efda125a326655acf0dc2d1b,"ETH","HTX (Huobi)","N",241381,186566
0x794d28ac31bcb136294761a556b68d2634094153,"ETH","HTX (Huobi)","N",270842,192526
0x4704437177d7b7c74d4f0a21454317e6774cc2e7,"ETH","","N",221,626
0x8e5a6e6fb4926284774a437241769f9b30c2f743,"ETH","","N",55945,31923
0x9122f37096867bdae584674fc70c5ff7f8d64662,"ETH","","N",34,32
0xa03400e098f4421b34a3a44a1b4e571419517687,"ETH","HTX (Huobi)","N",1084162,693525
0xa5d7f0f7027fa8f4d1be8042e1e43bbdec36951e,"ETH","HTX (Huobi)","N",27587,32132
0xcac725bef4f114f728cbcfd744a731c2a463c3fc,"ETH","HTX (Huobi)","N",525113,348952
0xd31f1f08aeec65d37b489a079bfc7cb324c1bae0,"ETH","","N",758,756
0xd4e47ff5a45d1d6536802cb91371f41c76dcec91,"ETH","","N",16,9
0xd91efec7e42f80156d1d9f660a69847188950747,"ETH","Kucoin","Y",205178,1638532
0xdac12a8ce214fdfffd3c05956080f56dfc2c0730,"ETH","","N",5,4
0xdf95de30cdff4381b69f9e4fa8dddce31a0128df,"ETH","HTX (Huobi)","N",86361,245523
0xf66852bc122fd40bfecc63cd48217e88bda12109,"ETH","HTX (Huobi)","N",205023,164566
0x8e5a9319d61cc03b99681b73f3efe7729c99f743,"ETH","","N",5881,1259
0x8e5ae118a2b7bab707b407ff02245d1055caf743,"ETH","","N",2429,0
0xee7ae85f2fe2239e27d9c1e23fffe168d63b4055,"ETH","","Y",338623,469185
0xe24a603d3e677e78262a29c0077ed0022086113b,"ETH","","N",58,52
0xe24a22c80c3340e282f7f6f32129f8bc097d113b,"ETH","","N",73,0


Kucoin
0xd91e...0747
Kucoin
0x58ed...6a0
0xee7a...4055
0x81a0...73fc
0x21cd...2dc2
0x2116...05cf
0x9887...34ce
0x81a0...73fc
0xe24a...113b
0x4aa2...2017
0x1207...304a
0x1207...304a
0xe24a...113b
0x4aa2...49b6
0xe24a...113b
0xe24a...113b
0x4aa2...f87e
0x18d8...ff9e
0x83a...2c0e
0x8e5a...f743
0x8e5a...f743
0x16b4...e85
0xd4e4...ec91
0x55ad...3fe4
0xd31f...bae0
0x2f30...7d54
0x43ab...3ae6
0xdac1...0730
0x35ef...232f
HTX (Huobi)
0xa034...7687
HTX (Huobi)
0x2abc...eb6a
HTX (Huobi)
0xa5d7...951e
HTX (Huobi)
0x28ff...93ad
HTX (Huobi)
0xcac7...c3fc
HTX (Huobi)
0xf668...2109
HTX (Huobi)
0x794d...4153
HTX (Huobi)
0x73f8...2d1b
HTX (Huobi)
0x0577...b404
HTX (Huobi)
0xdf95...28df
→ 14m ETH
99.75 ETH
→ 61.4k ETH
→ 32.4k ETH
→ 31.9k ETH
→ 29.9k ETH
→ 11.4k ETH
→ 3.76k ETH
→ 1.6k ETH
→ 1.6k ETH
→ 1.6