GLOBAL LEDGER

Trata de personas y delitos relacionados con las criptomonedas

Global Ledger & Aguirre Schwarz

Trafico humano y Crypto

Las criptomonedas se han convertido en una herramienta financiera fundamental en las operaciones de tráfico de personas en toda **América Latina**.

Su accesibilidad transfronteriza, su seudonimato y su facilidad de conversión las hacen ideales para facilitar los pagos, blanquear ganancias y eludir la supervisión financiera tradicional.

Trafico humano y Crypto

Los principales activos de liquidación en el espacio criptográfico siguen siendo **Bitcoin** y **Monero**.

Es probable que Bitcoin mantenga su posición debido a su temprana adopción, su amplio reconocimiento y su infraestructura fácil de usar, en particular su simplicidad, sin depender de contratos inteligentes y con un riesgo reducido de errores operativos (por ejemplo, enviar por error ERC-20 USDT a una dirección TRON, lo que puede provocar una pérdida irreversible).

Monero, por el contrario, es preferido por las sólidas garantías de anonimato que ofrece.

Tipos de trata de personas y evidencia

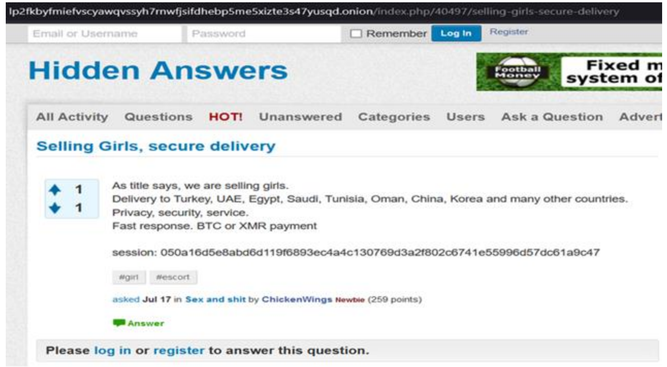
- **Trata con fines sexuales**
  Obligar o coaccionar a personas para que se dediquen a la explotación sexual comercial.
- **Trata con fines laborales**
  Explotar a personas para que trabajen mediante el uso de la fuerza, el fraude o la coacción en sectores como la agricultura, la construcción o el servicio doméstico.
- **Trata de órganos**
  Extracción y venta ilegal de órganos de víctimas vulnerables, a menudo mediante engaño o coacción..
- **Trata y explotación de niños**
  Traslado o explotación de menores con fines sexuales, laborales, de adopción ilegal o mendicidad forzada.
- **Contrabando que se convierte en trata**
  Migrantes que son objeto de contrabando y luego se ven obligados a trabajar en condiciones de explotación para saldar deudas

Human trafficking types and evidence

Una de las formas más extendidas de trata de personas es la **trata con fines sexuales**.

El siguiente intercambio encubierto con un **vendedor de la deep web** que afirma traficar con niños ilustra la naturaleza profundamente arraigada de la trata de personas en México (un país ampliamente considerado como el hogar de los cárteles más poderosos de América Latina desde el declive de la red de Escobar en Colombia).

La disposición del vendedor a ofrecer descuentos a personas que cree que están afiliadas a los cárteles pone de relieve lo estrechamente interrelacionadas que están estas empresas criminales. La captura de pantalla adjunta muestra un anuncio publicado en una **popular plataforma de preguntas y respuestas basada en Tor**.



Human trafficking types and evidence

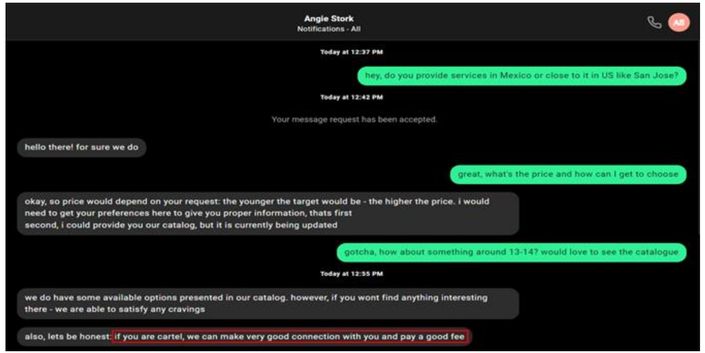
- **Bitcoin (BTC)** y **Monero (XMR)** son métodos de pago aceptados.
- Session Messenger ID es propuesto como medios de comunicación
- Hay una amplia gama de países disponibles.:
  - Turquia
  - Los Emiratos Arabes Unidos
  - Egipto
  - Saudi Arabia
  - Tunisia
  - Oman
  - China
  - Korea y muchos otros paises

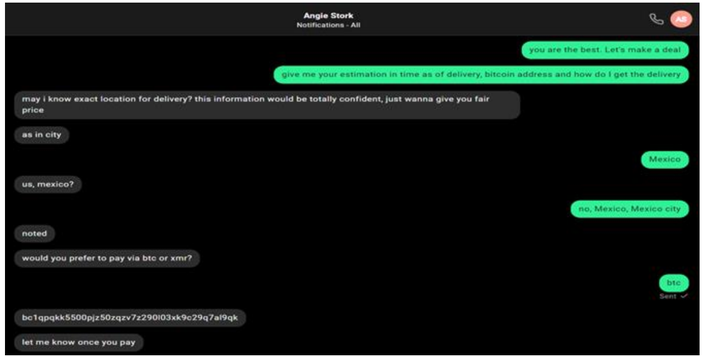
Fuimos extremadamente cautelosos con este distribuidor, ya que sabemos que este tipo de servicios suelen ser una tapadera para suplantaciones de identidad y estafas.

Human trafficking types and evidence

Cuando nos pusimos en contacto con este vendedor con el fin de obtener su **cartera BTC** y rastrear su actividad en la cadena, recibimos una propuesta de cooperación (lo que implica vínculos con la red del cártel) en los primeros minutos de la conversación.

No obstante, la oferta no solicitada por sí sola constituye un indicio revelador de la **conexión entre la trata de personas y las operaciones de los cárteles** en una región muy afectada por este tipo de actividad delictiva.





Tipologías de delitos relacionados con las criptomonedas

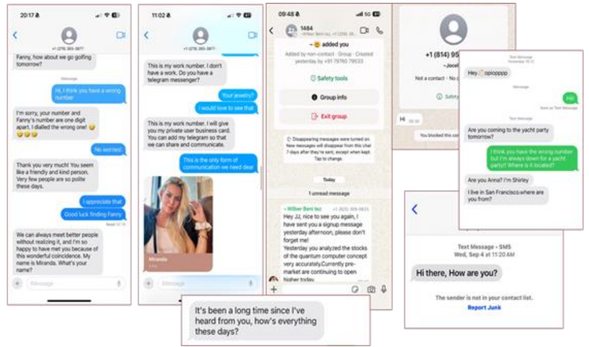
What is crypto fraud?

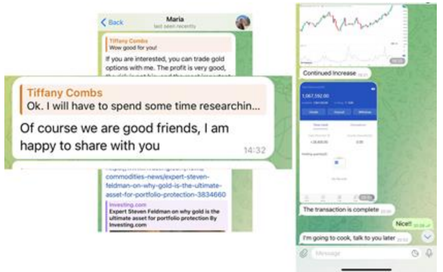
Un esquema fraudulento que utiliza criptomonedas o activos digitales para engañar a personas o empresas con el fin de obtener beneficios económicos. Estos esquemas suelen implicar:

- **Ingenieria social**
  Manipular a las personas para que revelen información confidencial o realicen acciones perjudiciales.
- **Suplantación de identidad**
  Fingir ser una persona u organización de confianza para ganarse la confianza de las victimas
- **Falsas promesas**
  Ofrecer rendimientos o garantías poco realistas para atraer víctimas.
- **Plataformas falsas**
  Crear sitios web o aplicaciones fraudulentas que imitan servicios legítimos.
- **Pequeñas ganancias**
  Ofrecer ganancias iniciales menores para generar confianza antes de robar sumas más grandes.
- **Urgencia y presión**
  Presionar a las víctimas para que tomen decisiones creando una sensación de urgencia.
- **Anonimato e irreversibilidad**
  Aprovechar la naturaleza anónima e irreversible de las transacciones criptográficas para evitar detección

Pig-Butchering Scam

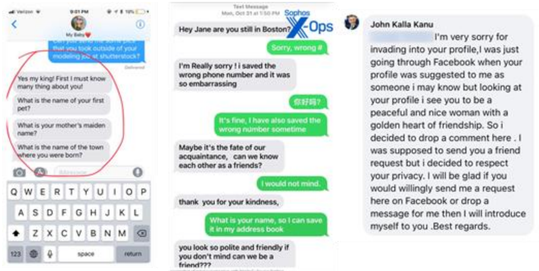
- Tipo de fraude muy manipulador y elaborado.
- Inicio a través de redes sociales, aplicaciones de citas o plataformas de mensajería.
- Los estafadores establecen relaciones duraderas con las víctimas.
- Siempre ofrecen oportunidades de inversión falsas a través de criptomonedas, minería, staking u oro.
- Ilusión de ganancias simuladas a través de plataformas falsas.
- El despojo (final del juego).

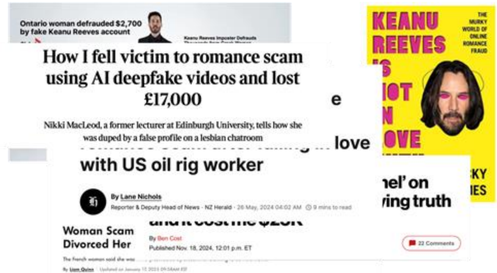




Romance Scams

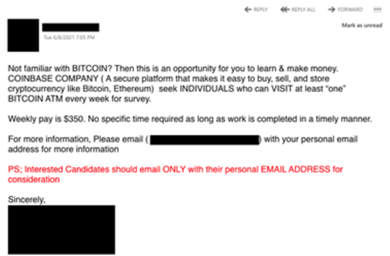
- Perfiles falsos en sitios web de citas, aplicaciones o plataformas de redes sociales.
- Crear conexiones y generar confianza en la pareja.
- Introducir una crisis (por ejemplo, el perro del estafador se enfermó y necesita dinero para medicinas).
- Explotación de la víctima y agotamiento de sus fondos.
- Se puede combinar con la estafa del «pig butchering».
- Uso de criptomonedas como la forma más rápida y conveniente de transferir dinero.





Phishing Scams

- Los estafadores envían correos electrónicos, mensajes o mensajes directos falsos.
- Estos mensajes suelen imitar sitios web o plataformas legítimas (incluidas plataformas relacionadas con las criptomonedas).
- Las víctimas son engañadas para que introduzcan sus datos de inicio de sesión, claves privadas o descarguen software malicioso.
- Los ataques se distribuyen masivamente, con el objetivo de afectar al mayor número de personas posible.
- Se utilizan con frecuencia como paso inicial antes de intentar suplantar la identidad o hacerse con el control de una cuenta.


[redacted]

Not familiar with BITCOIN? Then this is an opportunity for you to learn & make money. COINBASE COMPANY (A secure platform that makes it easy to buy, sell, and store cryptocurrency like Bitcoin, Ethereum) seek INDIVIDUALS who can VISIT at least "one" BITCOIN ATM every week for survey.

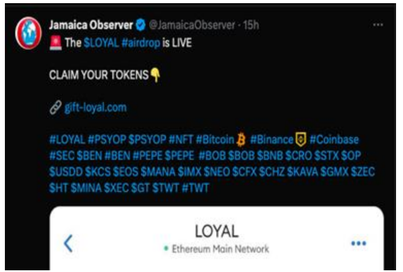
Weekly pay is $350. No specific time required as long as work is completed in a timely manner.

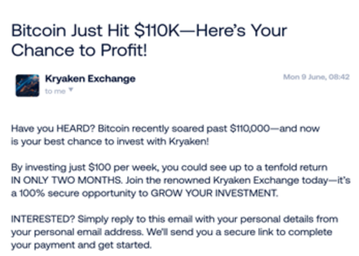
For more information, Please email ([redacted]) with your personal email address for more information

PS; Interested Candidates should email ONLY with their personal EMAIL ADDRESS for consideration

Sincerely,

[redacted]




Bitcoin Just Hit $110K—Here's Your Chance to Profit!

Kryaken Exchange
to me

Mon 9 June, 08:42

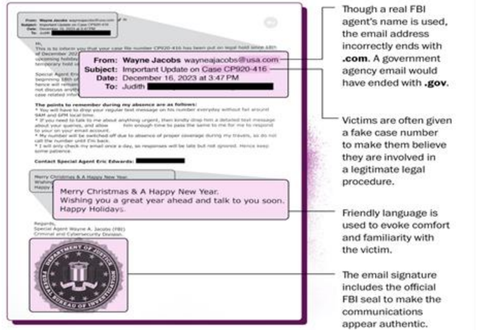
Have you HEARD? Bitcoin recently soared past $110,000—and now is your best chance to invest with Kryaken!

By investing just $100 per week, you could see up to a tenfold return IN ONLY TWO MONTHS. Join the renowned Kryaken Exchange today—it's a 100% secure opportunity to GROW YOUR INVESTMENT.

INTERESTED? Simply reply to this email with your personal details from your personal email address. We'll send you a secure link to complete your payment and get started.

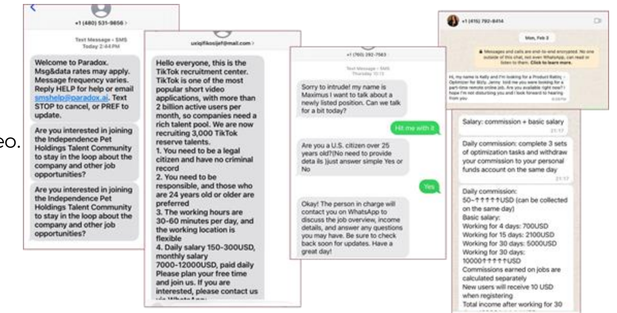
Impersonation Scams

- El estafador se hace pasar por una figura de confianza
  - Policia
  - Bancos
  - Agencia gubernamental
  - Familiares
- A menudo utiliza identificadores de llamadas falsos, correos electrónicos falsos o perfiles de redes sociales falsos
- Crea una sensación de urgencia o miedo:
  - «Estás siendo investigado» o «Tu cuenta está comprometida»



Employment Scams

- Anuncios de empleo falsos.
- Mensajes y correos electrónicos no solicitados.
- Llamadas telefónicas sobre oportunidades de empleo.
- Solicitan pagos por adelantado para equipo o capacitación.
- Envían cheques falsos y luego solicitan que se les devuelva una parte.
- Solicitan información personal confidencial.
  - SSN o bank account



Investment Scams

- Promesas de rendimientos elevados o garantizados con poco o ningún riesgo.
- Presión para actuar rápidamente u ofertas «por tiempo limitado».
- Falta de transparencia sobre la inversión o las personas que están detrás de ella.
- Solicitudes de pagos por adelantado o información personal.
- Uso de credenciales, testimonios o documentos de aspecto oficial falsos.
- Dificultades para retirar fondos o excusas por retrasos.
- Plataformas no registradas o falta de licencias adecuadas.
- Seguimiento agresivo y solicitudes repetidas.
- La comunicación puede ser impersonal, a través de correo electrónico, teléfono o aplicaciones de mensajería.

Resumen de cómo estas tipologías pueden ayudar en la denuncia de actividades sospechosas y en las investigaciones.

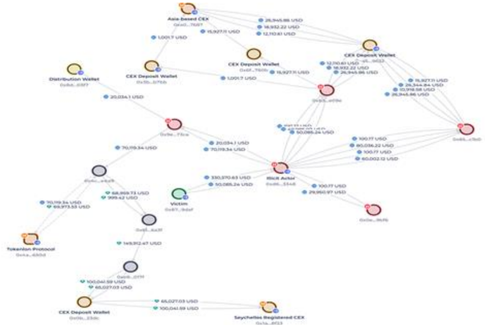
Case Analysis - Investment Scam

- La víctima denunció una pérdida de **380 000 USDC** el 3 de enero de 2025.
- Según el relato de la víctima, **inicialmente confió en la oportunidad de inversión** tras haber recibido anteriormente rendimientos del mismo actor ilícito. Sin embargo, cuando envió una cantidad mayor de fondos, toda comunicación cesó. Solo más tarde se dio cuenta de que **había sido víctima de una estafa de pig butchering**.
- Poco después del incidente, el actor ilícito depositó una parte de los fondos robados en intercambios centralizados, mientras que el resto se consolidó en múltiples carteras autohospedadas **(SHW).**
- Se observó que el actor ilícito utilizó protocolos de intercambio descentralizado **(DEX)** en un intento de ocultar el rastro de la transacción.

Case Analysis - Investment Scam

Durante la investigación hemos identificado::

- **~155 049 USDC** fueron depositados en CEX, con sede en Asia, el mismo día del incidente.
- **~70 000 USDC** fueron depositados en un CEX, **registrado en Seychelles.**



Img. 1 Initial tracing of stolen funds with destinations to Centralised Exchanges and Wallets controlled by an Illicit Actor

- **1** representa «depósitos» directos desde la billetera de la víctima directamente a la billetera del actor ilícito.
- **2, 3, 4 y 5** muestran cómo un actor ilícito ha dividido **380 000 USDC** de fondos robados en porciones más pequeñas entre otras billeteras.

Img. 2 "Deposit" and break down of stolen funds by an Illicit Actor

Case Analysis - Investment Scam

- **1** representa «depósitos» directos desde la billetera de la víctima directamente a la billetera del actor ilícito.
- **2, 3, 4 y 5** muestran cómo un actor ilícito ha dividido **380 000 USDC** de fondos robados en porciones más pequeñas entre otras billeteras.

Img. 2 "Deposit" and break down of stolen funds by an Illicit Actor

Lo que finalmente ocurre en el 99 % de los casos es que, **tarde o temprano, los fondos se depositan en una o varias bolsas centralizadas (CEX).**

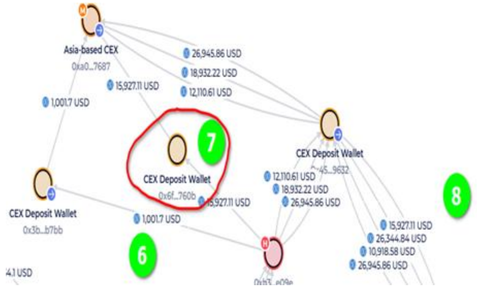
En los puntos **6, 7 y 8** vemos cómo un actor ilícito deposita sus fondos en carteras de depósito de CEX.

Img. 3 Actual Deposits to CEX Wallets

Case Analysis - Investment Scam

La cartera de depósito de intercambio centralizada podría identificarse con las siguientes características::

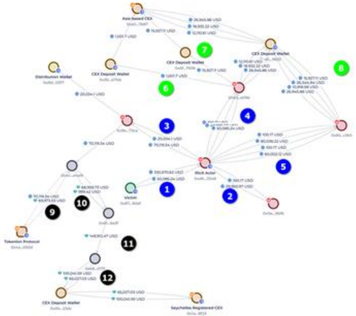
- Transacciones entrantes y salientes consecutivas
- Breve intervalo de tiempo entre transacciones
- Importe exacto incluido en las transacciones entrantes y salientes
- Transacciones salientes repetitivas a la cartera caliente



Img. 4 Deposit Wallets Pattern

Con un **9** podemos ver la interacción del protocolo TokenIon que se ejecutó como un intercambio de **USDT a USDC.**

En los números **10, 11 y 12** podemos ver el destino posterior de estos fondos, que se depositaron en otra cartera de depósito CEX (registrada en Seychelles).



Img. 5 Tokenion Protocol interaction and another deposit

Case Analysis - Investment Scam

Con un **13** podemos ver que se enviaron **20 000 USDC** desde una de las carteras que ha recibido parte de los fondos robados a la cartera de distribución.

En la siguiente diapositiva exploramos la distribución en detalle.

Img. 6 Distribution Wallet funds

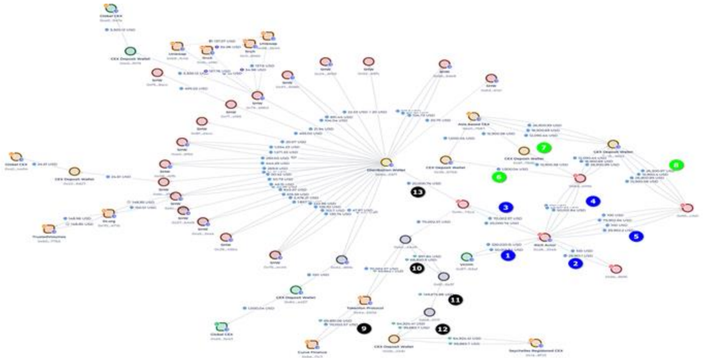
- Se transfirieron aproximadamente **20 000 USDC** a una cartera de distribución que ha repartido los fondos robados entre **17 carteras autohospedadas (SHW**), donde aún permanecen.
- Se identificó que se depositaron aproximadamente **3429 USDC** en tres CEX.

Img. 7 ~20,000 USDC distribution illicit funds tracing

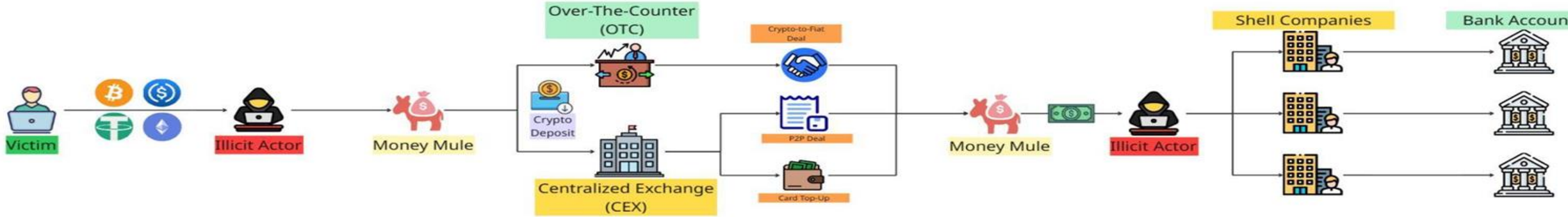
Case Analysis - Investment Scam

Incluso cuando los actores ilícitos intentan ocultar el destino final de los fondos, la transparencia de la cadena de bloques y las **técnicas de atribución de Global Ledger** pueden ayudar a rastrear el flujo.

Si los fondos llegan a una cartera de depósito de un intercambio centralizado **(CEX)** específico, esto permite presentar un informe de actividad sospechosa (**SAR**) o configurar alertas con el **conjunto de herramientas de Global Ledger** para carteras autohospedadas con el fin de monitorear cualquier movimiento posterior.



Img. 8 Whole case tracing landscape


Victim
Illicit Actor
Money Mule
Over-The-Counter (OTC)
Crypto Deposit
Centralized Exchange (CEX)
Crypto-to-Fiat Deal
P2P Deal
Card Top-Up
Money Mule
Illicit Actor
Shell Companies
Bank Accounts

Muchisimas gracias por su tiempo y atención.

Paul Densley

Head of Sales

paul.d@globalledger.io