Análisis de la cadena de bloques

Heurística

- **La «agrupación o *clustering* de direcciones» se refiere al proceso de asignar numerosas direcciones a la misma cartera/entidad de control mediante el uso de heurísticas conductuales en transacciones.**

- Hay una serie de factores que intervienen en estas heurísticas. En la siguiente diapositiva abordaremos algunos de los más conocidos. Sin embargo, es importante señalar que ninguna de las heurísticas es concluyente. Sus resultados pueden ser erróneos y los investigadores siempre han de corroborarlos.

- Las criptomonedas centradas en los principios de la autosoberanía consideran el análisis de la cadena de bloques como un ataque a la red. **Pequeñas minorías dentro de estas comunidades están trabajando para quebrar las heurísticas utilizadas y minimizar la capacidad de socavar la privacidad en el protocolo**.

- El punto clave aquí es que es probable que los métodos que se utilizan para proporcionar herramientas de análisis de la cadena de bloques (Blockchain Forensic Tools) evolucionen en consonancia con los esfuerzos para quebrar las heurísticas. Podría llegar a ser más difícil identificar cómo se están obteniendo los resultados, de ahí la importancia de mantenerse informado sobre el tema.

Heurística 1 - Propiedad de entrada común

Supuesto: Todas las entradas de una transacción pertenecen a la misma entidad, ya que residen en la misma cartera.

- La gran mayoría de las transacciones en Bitcoins son de carácter simple. Hay muy pocas transacciones colaborativas.

- En consecuencia, una cartera controlada por una entidad habrá proporcionado todas las entradas de la transacción para enviar los fondos.

Heurística 2 - Detección de la dirección del cambio:

- Los importes del cambio están vinculados a direcciones nunca vistas anteriormente en la cadena de bloques.
- Si la dirección de salida es la misma que la de entrada, se trata del cambio.
- La huella digital de la cartera puede utilizarse para detectar las salidas del cambio porque una salida de cambio refleja la misma huella digital que la cartera.
- Los números redondos como salida son pagos, no cambio.
- Si los valores de las entradas son mayores que una de las salidas pero menores que otra, la de menor cuantía es el cambio (heurística de la entrada innecesaria), ejemplo.

Inputs	Outputs	Assumption
1BTC	3.5BTC →	Payment
2BTC	0.5BTC →	Change
1BTC		

Supuestos:

- **Si una dirección de salida ha sido reutilizada es muy probable que sea una salida de pago**, no de cambio. Esto se debe a que el software de cartera crea las direcciones de cambio de forma automática, mientras que las direcciones de pago se envían de forma manual entre personas.

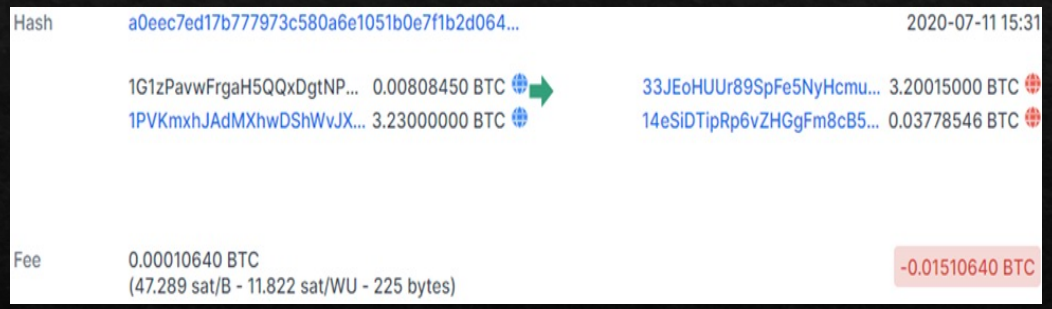
- Las entidades utilizan los valores predeterminados de las carteras para la selección de monedas y el pago de comisiones.

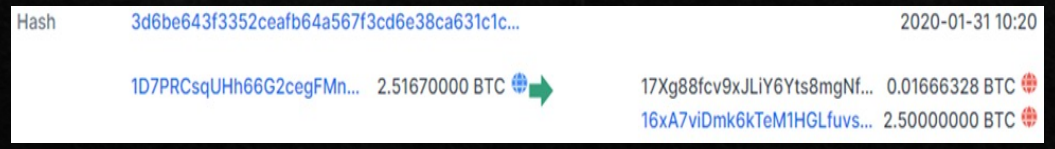
- **Muchos importes de pago son números redondos**, por ejemplo 1 BTC o 0,1 BTC. El importe del cambio sobrante sería entonces un número no redondo (por ejemplo, 1,78213974 BTC). Esto puede ser útil para encontrar la dirección del cambio. El importe puede ser un número redondo en otra moneda. La cantidad 2,24159873 BTC no es un número redondo en Bitcoins, pero al convertirla a USD quizás se acerque a un valor exacto en esa moneda.

Ejemplos de heurísticas

Heurística de la entrada común

Heurística del cambio: Las salidas son diferentes tipos de *scripts*.





Heurística del cambio: La dirección 16xA7 estaba activa antes de esta transacción. La dirección 17Xg88 se activó por primera vez para esta transacción. Pago en número redondo realizado a la dirección 16xA7

Información de inteligencia del sector privado

Además de estas heurísticas, las herramientas de análisis de la cadena de bloques **utilizarán información sectorial y tácticas de vigilancia encubierta para asignar entidades a las direcciones y formar clústers.** Esto implica que, a menudo, el proceso de identificación o el modo en que se ha desarrollado un clúster es opaco.

Es posible tratar de encontrar conexiones. Se puede comprobar manualmente la heurística y llevar a cabo una investigación de código abierto. No obstante, esto puede resultar poco práctico (si se trata de un gran volumen de datos) o no ser concluyente. En estos casos también vale la pena registrar los esfuerzos realizados y el resultado negativo. Esto demostrará al menos que se han realizado esfuerzos para comprender la información y cuantificar su origen.

Ejemplos prácticos

1

Cualquiera puede utilizar la licencia, basta con cerrar la sesión y las credenciales pueden ser utilizadas por otro usuario. Lo mejor es ponerse manos a la obra, así que no dude en intentarlo.

2

Lleve un registro de auditoría utilizando hojas de cálculo o cualquier otro mecanismo que prefiera.

3

Piense en cómo trataría de hacer progresar sus averiguaciones y hágalo constar en la estrategia.

Ejercicio 1

- Cargue el archivo .grf en Chainalysis
- Identifique la transacción de robo para cada clúster.
- Trace las entradas que aportaron fondos a la cartera de la víctima
- Destaque los servicios que aportaron fondos a la cartera de la víctima (proporcione una breve visión general de en qué consiste el servicio/su localización).

Ejercicio 1

- Marque las carteras utilizadas por los delincuentes
- Al observar la cartera 17vDMhe1Ym9XQMyaa6ahW4fvU5ibCniBi, ¿puede discernir por qué su historial de transacciones no parece encajar con la información?
- Identifique cualquier oportunidad de agrupar las direcciones y fusionarlas en un solo clúster.
- Ultime una estrategia en la que se describan los parámetros utilizados en la investigación y las posibilidades de perseguir a los delincuentes o el producto del delito.

Ejercicio 2 – Hackeo de Kucoin

- 1NRsEQRg5EjmJHbPUX7YADVPcPzCQBkyU7
  12FACbewf5Fy9nmeaLQtm6Ugo5WS8g2Hay
  1TYyommJW3uhjhcnHhUSuTQFqSBAxBDPV
- Busque en blockchair.com utilizando las direcciones anteriores. ¿Qué información obtiene sobre los activos? ¿Qué resulta interesante en relación con esto?
- Busque estas direcciones en sitios web de código abierto. ¿Puede encontrar información para asignar estas direcciones?

Ejercicio 2 – Hackeo de Kucoin

- 0xeb31973e0febf3e3d7058234a5ebbae1ab4b8c23
- Busque esta dirección en https://etherscan.io. ¿Qué puede encontrar en este sitio web?
- TB3j1gUXaLXXq2bstiSMfjQ9R7Yh9DdDgK
- Busque esta dirección en Tronscan.io y https://trx.tokenview.com/en. ¿Qué puede encontrar en este sitio web?
- Elabore un breve informe sobre sus hallazgos

Ejercicio 2 – Hackeo de Kucoin

- Abra Chainalysis y rastree las tres direcciones BTC
- Observe los fondos que entran en la cartera sospechosa. ¿Se le ocurre alguna línea de investigación en relación con esto?
- Observe los fondos que salen de la cartera sospechosa. ¿Qué líneas de investigación podrían seguirse al respecto?
- Ultime una estrategia en la que se describan los parámetros utilizados en la investigación y las posibilidades de perseguir a los delincuentes o el producto del delito.