



Introducción a los activos virtuales

Panorámica general

- **Formato nativo digital** – Igual que el dinero transferido a través de los métodos de pago tradicionales, por ejemplo, SWIFT.
- **Entre pares (P2P)** – Red sustentada por los participantes, no por un tercero centralizador*.
- **Cadena de bloques o blockchain** – extracto/registro de todas las transacciones
- **Direcciones** – Se utilizan para realizar transacciones; similares a los números de cuenta.
- **Carteras o monederos** – Software controlado por el usuario que genera y almacena las direcciones.
- **Identificadores de transacciones** – Cada transacción tiene un identificador único
- **Entradas y salidas** – Las entradas son los activos que se gastan y las salidas son las que se crean a partir de las entradas.
- **Minería/Consenso** – Es el medio para acuñar moneda y añadir nuevas transacciones a la cadena de bloques.
- **Transparente** – Muchas cadenas de bloques son fácilmente auditables, por lo que es posible asignar la actividad transaccional a una dirección.
- **Una o varias direcciones** – Algunas criptomonedas utilizan una sola dirección para todas las transacciones; otras utilizan varias.

Consenso

- Para los sistemas distribuidos basados en Blockchain:
 - permite un acuerdo unificado
 - alinea los incentivos económicos o de otro tipo
 - asegura la equidad
 - diseño tolerante a fallos
 - asegura la sincronización global
- Prueba de Trabajo (PoW); Gasto de recursos costosos
- Prueba de participación (PoS); Compromiso de valor
- Consorcio: Número establecido de verificadores reconocidos/validados
- Este es un aspecto que está en constante evolución, así que no conviene preocuparse mucho al respecto

Jerga: ¡Hay mucha!

criptoactivo

**criptomoneda
criptodivisa**

token

**criptomoneda
estable
(*stablecoin*)**

**custodia/sin
custodia**

**VC: moneda
virtual**

**NFT: token no
fungible**

VA: activo virtual

**VASP: proveedor
de servicios de
activos virtuales**

**CBDC: monedas
digitales emitidas
por bancos
centrales**

**DEX: intercambio
descentralizado**

**DeFi: finanzas
descentralizadas**

**DAO:
organización
autónoma
descentralizada**

**Dapp: aplicación
descentralizada**

Ejemplos de uso

- Dinero digital
- Almacén de valor
- Mercados financieros
- Música
- Propiedad digital
- Comunicación
- Identidad
- Gobernanza/legal
- Juegos de azar
- Almacenamiento
- Cadenas de suministro
- Hostelería
- Energía
- Salud

Cartera

Instale Bluewallet desde Google Play o la App Store de Apple

Frase mnemotécnica

Haga clic en «Añadir cartera» y seleccione «Bitcoin». Aparecerá la frase mnemotécnica que representa la «clave privada». Es preciso apuntarla en un papel. Una vez hecho esto haga clic en «Ok, ya lo he anotado»

Recepción

Haga clic en la casilla azul denominada «Cartera» que muestra «0 BTC». Seleccione «Recibir» y haga clic en «Sí, lo he hecho».

Dirección

El código QR es una representación de la dirección (número de cuenta) y debajo aparece la dirección (de carácter alfanumérico y que empieza por «bc1q»).

Cartera HD

Haga clic en la opción atrás y luego seleccione el menú de opciones/configuración de la cartera. Haga clic en «Mostrar dirección» y examine las opciones «Recibir» y «Cambio».

Explore las opciones de la aplicación. Pruebe a activar el «Modo avanzado» (salga a la pantalla principal y haga clic «Ajustes» y luego en «General»). Cree una nueva cartera y seleccione «Segwit». ¿Qué tiene de diferente la dirección?

Preguntas

Analice este proceso y debata en sus grupos de trabajo qué cuestiones plantea. Elija la más sugerente para compartirla con el resto de los participantes.

Ejercicio 1

Summary

USD BTC

This transaction was first broadcast to the Bitcoin network on April 24, 2021 at 11:01 AM GMT+1. The transaction currently has 1 confirmations on the network. At the time of this transaction, 0.08187360 BTC was sent with a value of \$4,058.54. The current value of this transaction is now \$4,032.36. Learn more about [how transactions work](#).

Hash	dfc48170a91c45770d991315f66d58bafcfa2400713a933e229b1... 	2021-04-24 11:01
	16CvKUr3v3e5pQCxmRSdH9FFaQYnERWLc 0.03028000 BTC 	
	16c9qrcEEBApWXeZysMzoJosdnYNsoEWX9 0.05283000 BTC 	
	➡	3HZNG2pnZ1RA5by4EudiaWEuLhWtWnzmV7 0.08187360 BTC 
Fee	0.00123640 BTC (367.976 sat/B - 91.994 sat/WU - 336 bytes)	0.08187360 BTC

1 Confirmations

Anatomía de una transacción de Bitcoin

Cryptocurrency Prices by Market Cap

USD ▾ Filter Portfolio Explore All Coins Recently Added Categories										
#	Coin	Price	1h	24h	7d	24h Volume	Mkt Cap	Last 7 Days		
☆ 1	 Bitcoin BTC	\$49,643.86	-0.0%	-2.3%	-17.6%	\$40,994,473,986	\$928,031,806,988			
☆ 2	 Ethereum ETH	\$2,294.40	-0.2%	0.6%	-2.0%	\$33,245,743,168	\$265,699,125,886			
☆ 3	 Binance Coin BNB	\$501.91	-0.5%	-1.3%	-2.9%	\$3,206,163,902	\$77,593,462,608			
☆ 5	 Tether USDT	\$0.997877	0.1%	-0.1%	-0.2%	\$87,435,549,732	\$50,000,878,543			
☆ 4	 XRP XRP	\$1.09	-0.2%	-0.5%	-29.7%	\$6,603,376,362	\$50,029,479,116			
☆ 6	 Cardano ADA	\$1.11	-0.4%	-1.8%	-18.9%	\$2,065,409,903	\$35,744,184,429			
☆ 7	 Dogecoin DOGE	\$0.253554	0.9%	-8.6%	-11.1%	\$6,254,492,048	\$33,146,619,777			
☆ 8	 Solana SOL	\$20.72	0.8%	1.3%	20.8%	\$1,351,125,571	\$20,422,224,222			

¿Y las demás?

Ethereum: Aspectos clave

1. Ethereum utiliza «cuentas» en lugar del modelo UTXO. Lo que significa que se puede utilizar una dirección para realizar todas las transacciones. No hay una dirección de cambio separada ni es necesario crear una nueva dirección para cada recepción.

2. Los tokens creados en el protocolo Ethereum no son almacenados por los titulares en tipos de dirección independientes. Se depositan en una dirección de Ethereum.

3. Las comisiones por transacción se calculan mediante un elemento llamado "Gas". El activo nativo de Ethereum (ETH) se utiliza para pagar las comisiones

4. Es posible servirse del carácter transparente de muchos contratos inteligentes para seguir la ruta de un activo.

5. Cuanto más compleja sea la ejecución de la transacción, en más gas incurrirá. Esto supone que habrán de pagarse comisiones más altas.

6. La ETH por sí misma no se considera un activo muy utilizado por los delincuentes.

7. Sin embargo, es la principal plataforma de criptomonedas estables (*stablecoins*), ampliamente utilizadas en el lavado de activos. En particular, destaca el uso del activo Tether (USDT).

8. La capacidad de utilizar las criptomonedas como herramienta de lavado de activos se ve reforzada por el valor estable de la USDT (vinculado al dólar). Esto permite cerrar acuerdos y realizar pagos a través de otros canales (transferencias bancarias, etc.) sin que la volatilidad afecte a los términos del acuerdo.

Transaction Details

Overview

Internal Txns

Logs (5)

State

Comments

Transaction Hash:	0x042b7053bab1e80e5761adab3b223c3c576ff4e2a93c392d46cc5715308acefd
Status:	Success
Block:	12290049 4 Block Confirmations
Timestamp:	53 secs ago (Apr-22-2021 12:38:28 PM +UTC) Confirmed within 12 secs
From:	0xd7f8157fc629584c2b3c6f7291de1a373b045676
To:	Contract 0x7a250d5630b4cf539739df2c5dadb4c659f2488d (Uniswap V2: Router 2) TRANSFER 0.11 Ether From Uniswap V2: Rout... To → Wrapped Et...
Transaction Action:	Swap 0.11 Ether For 189,675,405.387924102848950964 SHIB On Uniswap
Tokens Transferred: 2	From Uniswap V2: Rout... To Uniswap V2: SHIB 4 For 0.11 (\$284.71) Wrapped Ethe... (WETH) From Uniswap V2: SHIB 4 To 0xd7f8157fc62958... For 189,675,405.387924102848950964 (\$286.41) SHIBA INU (SHIB)
Value:	0.11 Ether (\$284.20)
Transaction Fee:	0.0099856944 Ether (\$25.80)
Gas Price:	0.0000001089 Ether (108.9 Gwei)
Click to see More	
Private Note:	To access the Private Note feature, you must be Logged In

Lavado de activos

- Los facilitadores/controladores/redes profesionales de lavado de activos recurren cada vez más al uso de criptomonedas.
- Utilizan cualquier protocolo de criptomoneda/activo virtual que se adapte a su propósito. Un ejemplo es la transición a protocolos con comisiones más bajas (de ETH a TRON).
- Las monedas estables resultan especialmente atractivas para estas redes. Eliminan el aspecto de la volatilidad de los activos flotantes al tiempo que permiten realizar pagos internacionales rápidos que no pasan por las redes financieras tradicionales. Esto hace que las negociaciones y las conversiones a valores en efectivo sean mucho más fáciles de llevar a cabo.
- Es importante destacar que las criptomonedas no constituyen el activo deseado como producto final. El efectivo limpio o las transferencias bancarias siguen siendo los mecanismos financieros más ansiados. Así, las criptomonedas se han convertido en un instrumento más para el lavado de activos.

Lavado de activos cont.

- Una táctica particular identificada en varios casos ha sido la creación de empresas de pagos digitales. Estas se constituyen como un vehículo para facilitar las cuentas OTC con las principales plataformas de negociación de criptomonedas de alta liquidez. El lavado de activos se oculta entonces como actividad comercial mediante la participación de facilitadores profesionales que ayudan a falsificar los controles de lavado de activos y conocimiento del cliente.
- También se ha hecho muy evidente que los grupos de delincuencia organizada (OCG) están buscando entidades que puedan facilitar el lavado de activos con criptomonedas. Como resultado, las redes profesionales están prestando servicio a múltiples OCG en el ámbito de una o más jurisdicciones. En los casos de corrupción internacional también se observa que estas redes son aspectos clave del proceso de lavado de activos.
- Se siguen utilizando las mismas tácticas, por ejemplo, IVTS, uso de mulas de dinero voluntarias o involuntarias a escala internacional, múltiples tipos de cuentas en muchos servicios financieros, alto volumen de transacciones intermedias, paso de una moneda a otra, uso de empresas ficticias/interpuestas, y la combinación de múltiples tipos de delitos, por ejemplo, el fraude MTIC con tipos de delitos tradicionales con el lavado de activos como servicio.

Lavado de activos cont.

Los protocolos/redes de criptomonedas ofrecen ciertas ventajas únicas para el lavado de activos:

Tokens no fungibles (NFT) – Estos *tokens* constituyen una prueba criptográfica de propiedad de artículos del mundo real o digital. Funcionan de forma similar a los bonos al portador; el control de la clave privada es una prueba de propiedad de facto. Actualmente los NFT se centran en mercado del arte y artículos de juegos virtuales. En recientes ventas en casas de subastas como Sotheby's se han visto NFT por valor de millones de dólares. Más allá del enfoque actual, existe un movimiento encaminado a fomentar la adopción de los NFT en una amplia gama de sectores económicos, por ejemplo, servir como entradas para festivales, prueba de identidad, acceso a plataformas, etc. Con un mercado líquido para este tipo de artículos y muchas herramientas para facilitar esta actividad, parece que es solo cuestión de tiempo que su explotación delictiva se convierta en un problema. Un ejemplo son las entidades de lavado de activos que organizan una serie de ventas y compras consecutivas para un NFT. Se trata de una práctica que también puede utilizarse para manipular el precio de los NFT.

Entidades ficticias/interpuestas específicas de criptomonedas - Los proyectos DeFi han utilizado modelos de financiación alternativos para eludir las controvertidas estructuras de las ICO de 2017 (por ejemplo, las entidades deben prestar un servicio al proyecto como recompensa por los *tokens*). Esto ha permitido, hasta la fecha, que estos proyectos eludan la normativa y los mecanismos de control. Se sospecha que sofisticados delincuentes han utilizado la DeFi para poner en marcha proyectos mediante los que han amañado la emisión de *tokens* haciéndose así con importantes cantidades de dinero por medios delictivos.

Estos medios para el lavado de activos ofrecen varias ventajas, por ejemplo, las entidades que están detrás del proyecto pueden funcionar bajo alias/seudónimos, ya que el proyecto carece de identidad comercial registrada. Esto se debe a que utilizan un contrato inteligente para controlar la plataforma y el término «descentralizado» para señalar que no está dirigido por ninguna entidad, sino por la comunidad que posee *tokens* de «gobernanza».

Aportación del sector privado

«El delito predominante en relación con las criptomonedas es el fraude»: Falsas plataformas de inversión, fraudes románticos, cuentas comprometidas, estafas de salida, corrupción.

La vulneración de los contratos inteligentes de DeFi constituye el factor que más contribuye a las pérdidas financieras. El posterior lavado de activos conlleva el movimiento entre diferentes activos a través de los DEX y el intento de intercambio en cadena cuando es posible. Por ello, distintos informes sobre el tema han destacado que cada vez se mueve más dinero de origen ilícito a través de los protocolos DEX.

La transparencia de la mayoría de las plataformas y la centralización de muchos proyectos ha dificultado seriamente a los delincuentes el blanqueo de fondos. ¡Incluso se han dado casos en los que el delincuente ha devuelto todos los fondos tras negociar una «comisión de intermediación»!

Las entidades de investigación empresarial también están informando del creciente número de casos que implican activos de criptomonedas.

La financiación del terrorismo sigue basándose en gran medida en los sistemas financieros tradicionales. Sin embargo, cada vez son más los casos en los que destaca el uso de criptomonedas:

«Además de Bitcoin y Ethereum, la orden de incautación demuestra que Hamás también recibió donaciones en Tether, TRON, Cardano, XRP y DOGE, lo que indica sus intentos de liberarse de la dependencia del Bitcoin después de que el Departamento de Justicia de EE.UU. anunciara la incautación de 2 millones de dólares en criptomonedas a destacados grupos terroristas».

Malware específico para criptomonedas

Type	Description	Example
Info stealers	Collect saved credentials, files, autocomplete history, and cryptocurrency wallets from compromised computers.	Redline
Clippers	Can insert new text into the victim's clipboard, replacing text the user has copied. Hackers can use clippers to replace cryptocurrency addresses copied into the clipboard with their own, allowing them to reroute planned transactions to their own wallets.	HackBoss
Cryptojackers	Makes unauthorized use of victim device's computing power to mine cryptocurrency.	Glupteba
Trojans	Virus that looks like a legitimate program but infiltrates victim's computer to disrupt operations, steal, or cause other types of harm.	Mekotio banking trojan

Dificultades

- El desafío que han de afrontar las fuerzas del orden es que los delincuentes explotarán de forma dinámica las distintas posibilidades de uso de este tipo de activos.
- Un ejemplo paradigmático es el sector energético. El creciente interés por la energía verde y el reciclaje ha abierto numerosas vías para el lavado de activos.
- Los investigadores que trabajan en este campo tienen mucho que tratar en relación con este tema.
- Es necesario aplicar estrategias eficaces en todos los ámbitos de la Agencia de Lucha contra el Blanqueo de Capitales correspondiente (LEA). Estos organismos han de tener en cuenta los recursos, la formación, la observación del panorama y las competencias.
- Para lograrlo, es vital conseguir la adhesión de los altos cargos de la Administración.

¡Fin!
¿Alguna pregunta?

