Introducción a los activos virtuales

Ejercicio 1

- Discutan en sus grupos lo que entienden por activos virtuales y detallen dos preguntas sobre algo que no sepan y sobre lo que les gustaría recibir información. Traten de identificar lo que creen que saben como grupo y utilícenlo como base para las preguntas que les gustaría plantear.

  Al final se les pedirán las dos preguntas en un papel que yo recogeré.

Introducción

- Activos de origen digital que tiene un valor asociado a ellos por dos motivos:
  - Aplicación
  - Oferta y demanda
- Muchos tipos de activos distintos, en cierto modo el mercado de valores puede verse como un paralelo.
- Existe un infinito número de ideas de negocio que pueden conducir a la formación de una empresa. Si procede, una empresa legítimamente constituida que se dedique a casi cualquier tipo de negocios puede tratar de ser admitida a cotización en el mercado de valores.
- Por consiguiente, el mercado de valores contiene entidades que se dedican a actividades empresariales conocidas, las que prestan servicios a empresas altamente especializadas, y todo lo demás que se encuentre entre ambos extremos.
- Los mercados de criptomonedas son similares. Muchas ideas y modelos de negocio distintos se reflejan en un activo digital. Algunos compiten con otros por las cuotas de mercado y otros presentan una oferta única.

Introducción (continuación)

- Las métricas clave que imponen el uso de criptomonedas son la liquidez y el valor.
- Seguridad: para mantener un valor considerable a largo plazo, un activo debe estar respaldado por una seguridad suficiente a fin de evitar el doble gasto o la manipulación de la oferta.
- Liquidez: un activo debe ser fácil de comprar y vender. Esto significa que muchos mercados precisan ofertarlo como un par de divisas.
- Bitcoin es actualmente la criptomoneda imperante en lo que se refiere a estas características.

Redes

Dos tipos de criptomonedas: centralizadas (entidad reconocida ejerce el control) y descentralizadas (ninguna entidad ejerce el control).

Los activos descentralizados presentan dos partes conceptuales:

1) Una red entre pares (P2P): las redes P2P funcionan principalmente a través de Internet. Utilizan un software diseñado para transmitir mensajes específicos a través de una red de participantes. No suelen estar reguladas, por lo que cualquiera puede conectarse a la red. Esto dificulta su censura.

2) Aplicaciones que utilizan la infraestructura de esta red. Suelen ser de código abierto y, por tanto, gratuitas.

Resumiendo, las aplicaciones generan datos necesarios para realizar operaciones, mientras que las redes organizan y garantizan el flujo de información.

Redes (continuación)

Las criptomonedas centralizadas tienen participantes regulados en la red que organizan el flujo de información. Éstos pueden supervisar e imponer las condiciones de tráfico en la red que se consideran aceptables.

Suelen ser un fiel reflejo del actual sistema financiero. Las monedas digitales emitidas por los bancos centrales son un ejemplo de red centralizada.

Existen varios grados de centralización, lo cual es motivo de continuos debates en la esfera de las criptomonedas.

Jerga: ¡Hay para dar y tomar!

Criptoactivo	Criptomoneda/ Criptomonedas	Token	Criptomoneda estable
Custodia/No custodia	VC: moneda virtual	NFT: token no fungible	VA: activo virtual
VASP: proveedores de servicios de activos virtuales	CBDC: moneda digital de banco central	DEX: Intercambio descentralizado	DeFi: Finanzas descentralizadas
	DAO: organización autónoma descentralizada	Dapp: aplicación descentralizada	

Hay que conocer la terminología

Blockchain: base de datos que contiene identificadores únicos que asocian una nueva entrada a la anterior. En el sistema de Bitcoin, actúa como un registro de finanzas (piense en la llevanza de la contabilidad).

Identificador de Transacción (TXID): referencia de una operación única en la blockchain.

Hora de la red: la blockchain de Bitcoin opera solo con el tiempo universal coordinado (UTC).

Monederos de criptomonedas; un software que se puede considerar como un banco en el que residen sus activos.

Direcciones: números de cuenta generados por el software del monedero de criptomonedas.

Entradas y salidas: las entradas son los activos que se gastan y las salidas son los que se generan a partir de las entradas.

Minería

Proceso informático intensivo para validar operaciones, incluirlas en el libro de contabilidad, acuñar nuevos activos y proteger la red.

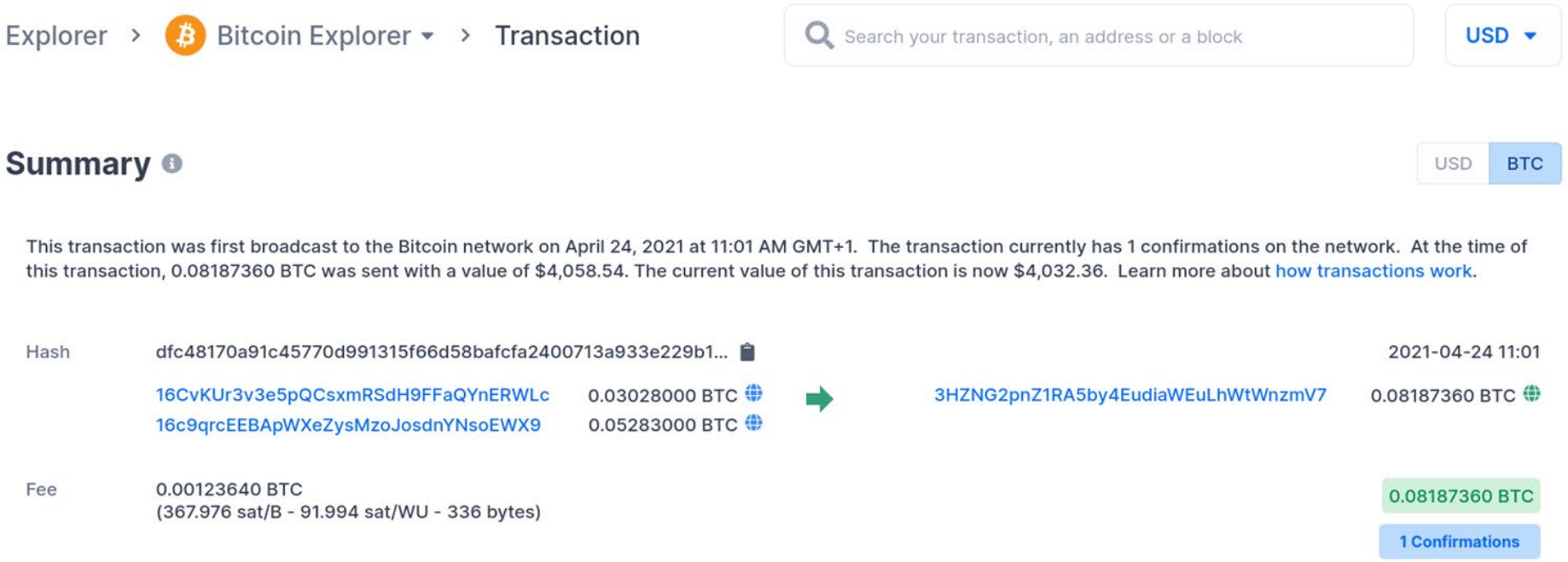
Incentivos financieros para completar esta tarea. Los mineros son retribuidos con comisiones y una nueva emisión de activos. Si actúan con honestidad y protegen la red, el activo podrá revalorizarse. Esto generará otros beneficios a los mineros y una inversión continua en el mantenimiento de la red.

Dado que la red está descentralizada, ninguna entidad central puede imponer quién mina o quién es retribuido por ello. Para atenuar esta situación, el protocolo de Bitcoin convierte la minería en un mercado libre, entorno competitivo. Cualquiera puede competir y quienes sean más eficientes obtendrán las mayores retribuciones.

«La minería se podría describir como un gran juego competitivo de sudoku que se vuelve a poner a cero cada vez que alguien encuentra la solución y cuya dificultad se ajusta automáticamente, por lo que se tarda aproximadamente 10 minutos en dar con la solución. Imagínese un gran rompecabezas de sudoku de varios miles de filas y columnas. Si le muestro el rompecabezas completado, usted podrá verificarlo con mucha rapidez. Pero si el rompecabezas tiene varias casillas completas y las demás están vacías, ¡cuesta mucho trabajo resolverlo!

Si bien la dificultad del sudoku se puede ajustar cambiando su tamaño (más o menos filas y columnas), se puede seguir comprobando con bastante rapidez por muy grande que sea. El «rompecabezas» utilizado en bitcoin se basa en un hash criptográfico y presenta características similares: es difícil de resolver por su falta de simetría, aunque fácil de comprobar, y puede ajustarse su dificultad».

- ***(Mastering Bitcoin: https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch02.asciidoc)***



Anatomía de una transacción bitcoin

Details

Hash	dfc48170a91c45770d991315f66d58bafcfa2400713a933e229b108bd73c4de3
Status	Confirmed
Received Time	2021-04-24 11:01
Size	336 bytes
Weight	1,344
Included in Block	680400
Confirmations	1
Total Input	0.08311000 BTC
Total Output	0.08187360 BTC
Fees	0.00123640 BTC
Fee per byte	367.976 sat/B
Fee per weight unit	91.994 sat/WU
Value when transacted	$4,058.54

Inputs

HEX ASM

Index	0	Details	Output
Address	16CvKUr3v3e5pQCsxmRSdH9FFaQYnERWLc	Value	0.03028000 BTC
Pkscript	OP_DUP OP_HASH160 3919b66fc78f9e0a739fb630ad79c9d3bf097bbc OP_EQUALVERIFY OP_CHECKSIG		
Sigscript	3044022067c429d37093682c5990e4588a0680ab0c5907ee790e51e2951b649a8b7ebf3402202ef2320480bb03e6e53b9f40fc48bcaa092d544e72c2081745194032f26c210b01 02f63d2d95ec336499a6bbc1b8109fcd6086a6f8d7e78fb1862e976b12ae5e487b		
Witness			

Index	1	Details	Output
Address	16c9qrcEEBApWXeZysMzoJosdnYNsoEWX9	Value	0.05283000 BTC
Pkscript	OP_DUP OP_HASH160 3d7e919c2aec4ae3a1bb3fde39c7e03457ff14b0 OP_EQUALVERIFY OP_CHECKSIG		
Sigscript	304402203d02ceec5ccb1d3d89c4cd73bff286def94a109cffbd0a3c26b301089104e33c02207ee257d4e4cf4e80791853d57bd4bda6c469bf14ebf9dd8e320d4f31f26ce6ba01 0293590a3fb3d03afebe1d5cdffc4f0f07cc9c83dabc934ee025cc0b7a9beb22c8		
Witness			

Outputs

Index	0	Details	Unspent
Address	3HZNG2pnZ1RA5by4EudiaWEuLhWtWnzmV7	Value	0.08187360 BTC
Pkscript	OP_HASH160 ae0fa915f65c6fe4ebaa19d29237368fb43a66af OP_EQUAL		

Ethereum: Cuestiones principales

1. Ethereum utiliza «cuentas» en lugar de un modelo de transacción de salida no gastada o modelo UTXO. Esto significa que se puede utilizar una dirección para completar todas las transacciones. No existen cambios de dirección separados o la necesidad de crear una nueva dirección para cada recibo.

2. Los tokens creados en el protocolo Ethereum no son almacenados por los titulares en tipos de dirección separados. Son ingresados en una dirección de Ethereum.

3. Las comisiones por transacción realizada se calculan utilizando un elemento denominado «Gas». El valor del activo digital de Ethereum (ETH) se utiliza para pagar las comisiones.

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

5. Cuanto más compleja sea la ejecución de la operación, más Gas consume. Esto equivale al pago de mayores comisiones.

6. El ETH por sí solo no se considera un activo importante utilizado por delincuentes.

7. No obstante, es la principal plataforma de criptomonedas estables, que ha sido ampliamente utilizada para el lavado de activos. En particular, el activo Tether (USDT) ha ocupado un lugar destacado.

8. La posibilidad de utilizar criptomonedas como herramienta de lavado de activos se refuerza gracias al valor estable del USDT (vinculado a un 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

Buy Exchange Earn Gaming

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 0x7a250d5630b4cf539739df2c5dacb4c659f2488d (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

Demostración

https://www.chainabuse.com/report/82855fa1-3851-4739-9fd8-f0af8b05ed6d?context=browse-chain&chain=ETH

- Caso sobre información procedente de fuentes de dominio público Visualizador de gráficos OXT / https://www.ethtective.com / mistrack.io
- TRM Forensics

Ejercicio 2

- Navegar a www.chainabuse.com/reports
- Pinchar en Bitcoin
- Buscar una dirección detallada en un informe y copiarla
- Pegue esto en los siguientes exploradores de bloques y revise las transacciones asociadas:
  - https://oxt.me
  - https://mempool.space/
  - www.blockchain.com

- Ahora haga lo mismo para Ethereum, vuelva a Chainabuse y pinche en Ethereum.
- Revise las transacciones vinculadas a una dirección en los siguientes exploradores de bloques:
  - https://debank.com/
  - https://etherscan.io/
  - https://eigenphi.io/

- Elija una transacción Bitcoin y Etherum para mostrarla al grupo [destaque el Identificador de transacción (TXID), la hora/fecha, las entradas/salidas, la comisión pagada y cualquier otro detalle que considere relevante].

Ejercicio 2 continuación

- Inicie sesión en TRM Forensics
- Inicie el explorador de bloques y busque los detalles pertinentes
- Navegar a https://www.chainabuse.com/report/a36786da-b8d5-46df-b4a9-8f804fc63779?context=browse-chain&chain=BTC
- Desglose el informe y busque identificadores de Bitcoin pertinentes en el visualizador de gráficos. Corrobore la información facilitada por la víctima.
- Una vez completado, esbozar una estrategia de investigación para avanzar el asunto. Incluya cualquier cosa que considere relevante al respecto.
- Que otra persona presente un resumen sobre lo ocurrido, cómo se ha corroborado la información y cuál es la estrategia de investigación posterior.

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	

¿Y qué hay del resto?

Monero: Características principales

Ring CT:
Oculta el monto de la operación.

Ring Signatures:
Protegen al remitente al complicar cuál fue la salida que se gastó.

Dandalion++:
Oculta el origen de emisión de la operación.

Direcciones ocultas:
Garantizan que la dirección del remitente no quede registrada en la blockchain.

Estas características hacen que Monero sea muy complejo. Existen algunas opciones aún disponibles. Se trata de debilitar el anonimato, participar en servicios de criptomoneda y analizar el tiempo.

Es posible intercambiar Monero por Bitcoin y es probable que este sea el modus operandi adoptado por muchos delincuentes para lavar el producto de sus actividades.

Monero se está convirtiendo en un activo importante en los ataques de ransomware. Al margen de estos ataques, todavía está muy por detrás de Bitcoin. Esto se debe a la disponibilidad de un fondo de liquidez menor para el proceso de lavado de activos.

Si bien no es un proceso fácil, el análisis de sincronización puede revelar los puntos en los que se produce la conversión. Gracias a ello, es mucho más fácil rastrear los activos de Bitcoin a medida que circulan a través del sistema financiero.

Difficulty	Height	Hashrate	Emission
287773042775	2344885	2398.1 Mh/s	17892727

Transaction 3a7359d3e589ce71888b5152b6392261c94a7ef4f3d22f07b188020c508d2625

Confirmations	1
From Block	2344884
Output total	confidential
Fee	0.018856790000 XMR
Size	1456 bytes
Mixin	10
Unlock	0

Confidential Transaction — amounts are not disclosed.

Inputs (1)

Amount	Key Image
0.000000000000	26511d04d1fea4f6b132ff13047a5d6f53bd0f9de6e9c483f9ac07d433940eab

From Block	Public Key
2314316	bc171b412410732963e6623a8bd4de3491b6ec53ddfe3912cf0c7d9653d32bcb
2335113	45d1e748be84b5efefb101f1a40aaef59ef4e2a3cae58884323ae4bcc96c5ac3
2342631	613df1c762e3f9536bf8b4904bc4bad97710fc5ab0ca992eaca4c31f3617a480
2343112	4ef5172d333c1ec9a66abf7ff702566b49c9d6aee98ca737b8cf22862139b007
2343768	4055765e2d47eb886d92234e1c16090ba359d996c9e99a17030326b60037d388
2343950	807e60cee001db3a8b161e797e2a79daefec8d02ae6a33d3cbacc3ad62c03278
2344013	e2f2eca59917bc1e1986dbea736bb32d55abc0b5666e60b2b02448279f2b4736
2344241	0f49ecf93702ab680e84343c7cca380bd3787e975dc50e97bbf4f83f4f9d5437
2344447	2b851f462b71ec7bf0c4100a1d07e4936693b42a9e76fa72706125499c339bda
2344779	4487223ba0353b60794df84b5cbf6ed6bc8dd7b3031f86542a735b4b62a73ee7
2344809	6810ed6d3ccb06e68e7aed34bfe3c325dd51bab4cd39947b68fc1b96ad40448f

Outputs (2)

Amount	Public Key
0.000000000000	8932b6720f4b202b435982cec94e55d07f0df4315ad02a633e7d8647bb14f305
0.000000000000	171cfb05313556873a73424bcf4636ba2f62f9c4994a229192fd26f3ee33824e

Ejercicio 3

- Vuelva a la situación de fraude de inversión y aplique el siguiente aspecto de su estrategia de investigación. Si tiene que elegir un nuevo informe de Chainabuse o desea hacerlo, asegúrese de que está relacionado con BTC. Deténgase en el punto que considere adecuado y conforme a la estrategia diseñada.

- Cree un registro de auditoría de sus acciones y de cualquier prueba pertinente utilizando el sistema de gestión de casos.

- Tome nota de cualquier cosa que no entienda y sobre lo que quiera recibir más información.

- Prepare un resumen sobre sus conclusiones. Alguien que no haya expuesto hasta ahora ante el grupo lo hará al final del tiempo asignado.

¡Fin!
¿Alguna pregunta?