



OECD International Academy for Tax Crime Investigation

*Anti-Money Laundering: Current Trends, Prosecutions,
and the Challenges around Cryptocurrencies*

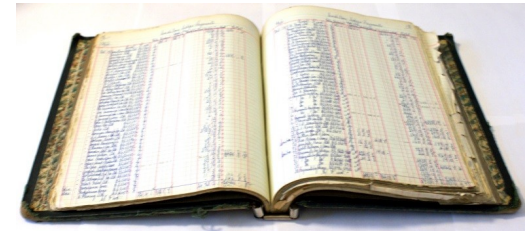


Exploradores de la blockchain de Bitcoin

EXPLORADORES DE LA BLOCKCHAIN DE BITCOIN: CONCEPTOS BÁSICOS

Exploradores de la blockchain de Bitcoin

- La blockchain de Bitcoin es un libro mayor digital público que registra cada transacción de Bitcoin que se ha realizado.
- Los exploradores de blockchain permiten visualizar información como:
 - Direcciones emisoras y receptoras
 - Fechas y horarios
 - Montos
 - Y mucho más...
- También permiten buscar por:
 - Números de bloque
 - Direcciones
 - Hashes de transacciones



<https://www.blockchain.com/charts/n-transactions-per-block>

<https://www.blockchain.com/charts/avg-block-size>

Exploradores de la blockchain de Bitcoin

- Muchos exploradores de blockchain permiten visualizar datos de diferentes blockchains.
- Toman los datos en bruto de las redes y los presentan en un formato legible para humanos.
- Distintos exploradores pueden presentar la información de forma más o menos útil, según su diseño.

Exploradores de la blockchain de Bitcoin


- No identifican billeteras
- No identifican propietarios
- No identifican direcciones de cambio
- Proporcionan datos de transacciones más detallados que las herramientas de rastreo como Chainalysis
- Permiten un mayor acceso a los datos contenidos en los mensajes de transacción
- Permiten corroborar las conclusiones obtenidas con herramientas de rastreo
- A menudo ofrecen soporte en múltiples idiomas

Soporte de idiomas



| |
|-------------------------|
| English |
| Español |
| Português |
| Русский |
| Türkçe |
| Italiano |
| Español (Latinoamérica) |
| Français |
| Deutsch |

| | |
|---|-----|
|  BLOCKCHAIR | |
| English | ENG |
| Español | SPA |
| Français | FRA |
| Italiano | ITA |
| Nederlands | DUT |
| Português | POR |
| Русский | RUS |
| 中文 | CHI |
| فارسی | PER |
| Bahasa Indonesia | IND |
| Türkçe | TUR |
| 日本語 | JPN |
| 한국어 | KOR |
| Deutsch | DEU |

| | |
|--|-------------|
|  mempool .space | |
| العربية | Nederlands |
| Català | 日本語 |
| Čeština | Norsk |
| Deutsch | Polski |
| English | Português |
| Español | Română |
| فارسی | Русский |
| Français | Slovenščina |
| 한국어 | Suomi |
| हिन्दी | Svenska |
| Italiano | ไทย |
| עברית | Türkçe |
| ქართული | Українська |
| Magyar | Tiếng Việt |
| Македонски | 中文 |

Marcas de tiempo en la blockchain

https://en.bitcoin.it/wiki/Block_timestamp

- Bitcoin utiliza la hora UTC.
- Las marcas de tiempo de los bloques son precisas solo **dentro de un margen de dos horas.**

Una marca de tiempo se acepta como válida si es mayor que la mediana de las marcas de tiempo de los 11 bloques anteriores y menor que la hora de red ajustada + **2 horas**.

La “hora de red ajustada” es la mediana de las marcas de tiempo devueltas por todos los nodos conectados a usted.

Como resultado, las marcas de tiempo de los bloques **no son exactamente precisas**, y no es necesario que lo sean para que el sistema funcione correctamente.

Algunos exploradores de la blockchain de Bitcoin

- **Bitinfocharts:** <https://bitinfocharts.com/>
- **Blockchain.com:** <https://www.blockchain.com/>
- **Blockstream:** <https://blockstream.info/>
- **Blockchair:** <https://blockchair.com/>
- **Mempool:** <https://Mempool.Space/>
- **CoinMarketCap:** <https://blockchain.coinmarketcap.com/>
 - Guía del explorador de bloques de CoinMarketCap: <https://coinmarketcap.com/guides/blockexplorer#guide-main>

DIRECCIONES

Direcciones

- Puede buscar direcciones en un explorador, y este le proporcionará una lista de todas las transacciones de envío y recepción en las que ha participado esa dirección.
- Es posible que pueda identificar otras direcciones que forman parte de la misma billetera observando sus patrones de gasto.
 - Las direcciones que gastan en conjunto en una misma transacción suelen estar controladas desde la misma billetera.

<https://blockstream.info/>

Address ⓘ

USD BTC

This address has transacted 2 times on the Bitcoin blockchain. It has received a total of 60.87000000 BTC (\$1,177,094.93) and has sent a total of 60.87000000 BTC (\$1,177,094.93). The current value of this address is 0.00000000 BTC (\$0.00).



| | |
|----------------|------------------------------------|
| Address | 1Bb4mQ6G6wqdnRuCqA7YZSMsGnB59DS9cU |
| Format | BASE58 (P2PKH) |
| Transactions | 2 |
| Total Received | 60.87000000 BTC |
| Total Sent | 60.87000000 BTC |
| Final Balance | 0.00000000 BTC |

Blockstream Explorer
Bitcoin
Liquid

Dashboard
Blocks
Transactions

Address

1Bb4mQ6G6wqdnRuCqA7YZSMsGnB59DS9cU

| | |
|--------------------|----------------------|
| CONFIRMED TX COUNT | 2 |
| CONFIRMED RECEIVED | 1 output (60.87 BTC) |
| CONFIRMED SPENT | 1 output (60.87 BTC) |
| CONFIRMED UNSPENT | No outputs |

<https://blockstream.info/>

<https://blockchair.com/>

<https://bitinfocharts.com/bitcoin/>

Ejercicio: Dirección de ransomware de WannaCry

- Utilice **Blockchair.com** y **Blockstream.info** para examinar la siguiente dirección:

115p7UMMngoJ1pMvKpHjCrdFjNXj6LrLn

1. ¿Cuántos bitcoins ha recibido en total?
2. ¿Cuál fue la fecha y hora de la primera transferencia?
3. ¿Cuál fue la fecha y hora de la última transferencia?
4. ¿Aparece la misma fecha y hora en ambos exploradores de blockchain?
5. Examine la línea de tiempo de la dirección en Bitinfocharts
 - ¿Ofrece Bitinfocharts una visión más clara de la actividad de la dirección?

Wannacry - Blockchair



Address

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Balance

0.46702392 BTC · 9,042.63 USD

Total received

14.87769994 BTC · 30,258.40 USD

Total spent

14.41067602 BTC · 39,250.36 USD



Wallet statement



Wallet statement



BLOCKCHAIR

info@blockchair.com

https://blockchair.com

12/05/2017 - 10/10/2022 (Part 1/1)

WALLET STATEMENT

BITCOIN

WALLET ADDRESS: 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

STATEMENT PERIOD: 12/05/2017 - 10/10/2022


BTC BALANCE SUMMARY:

| | | |
|-------------------------------|-----------------|---------------|
| STARTING BALANCE (12/05/2017) | 0.00000000 BTC | 0.00 USD |
| TOTAL RECEIVED | 14.87769994 BTC | 30,259.36 USD |
| TOTAL SENT | 14.41067602 BTC | 39,250.36 USD |
| ENDING BALANCE (10/10/2022) | 0.46702392 BTC | 9,042.63 USD |

HISTORY OF TRANSACTIONS: 12/05/2017 - 10/10/2022

| # | TIME | | AMOUNT (BTC) | AMOUNT (USD) | TRANSACTION HASH |
|---|------------------------|----------|--------------|--------------|---|
| 1 | 2017-05-12 13:34:58 | Received | 0.15000000 | 273.87 | 01b9e19b74335b6ab5f56abee48a861de31d997a64d4d624748ae65921c8e86 |

Wannacry - Blockstream

 Blockstream Explorer


BitcoinLiquid

DashboardBlocksTransactions

Search for block height, hash, transaction, or address

Address

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn




| | |
|--------------------|-------------------------------|
| CONFIRMED TX COUNT | 124 |
| CONFIRMED RECEIVED | 122 outputs (14.87769994 BTC) |
| CONFIRMED SPENT | 112 outputs (14.41067602 BTC) |
| CONFIRMED UNSPENT | 10 outputs (0.46702392 BTC) |






Transaction



01b9e19b74335b6ab5f56abee48a861ede31d997a64d4d624748ae65921c8e86






Blockstream Explorer

 Bitcoin
 Liquid


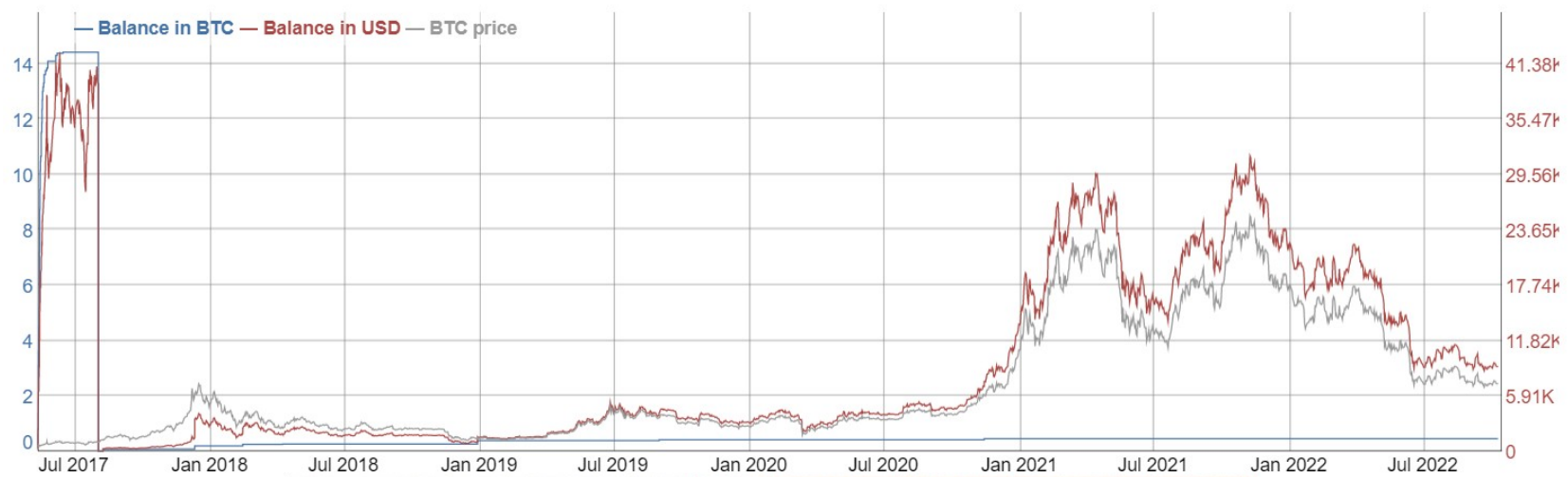
Dashboard
Blocks
Transactions

Search for block height, hash, transaction, or address



 Transaction

14449446275da0bf11825d14733fcc28f7264f8a2c3a506752f92fddb8e1aa16


| | |
|-------------------|--|
| STATUS | 101179 Confirmations |
| INCLUDED IN BLOCK | 0000000000000000000000008746b94257e056b29166411f64681e4aaa86fea57869 |
| BLOCK HEIGHT | 656858 |
| BLOCK TIMESTAMP | 2020-11-14 02:08:23 GMT -5 |
| TRANSACTION FEES | 0.0011388 BTC (129.4 sat/vB) |
| SIZE | 880 B |
| VIRTUAL SIZE | 880 vB |
| WEIGHT UNITS | 3520 WU |
| VERSION | 1 |
| LOCK TIME | 0 |



TRANSACCIONES

“Coinbase Transaction”

(La recompensa que se pagó al minero)

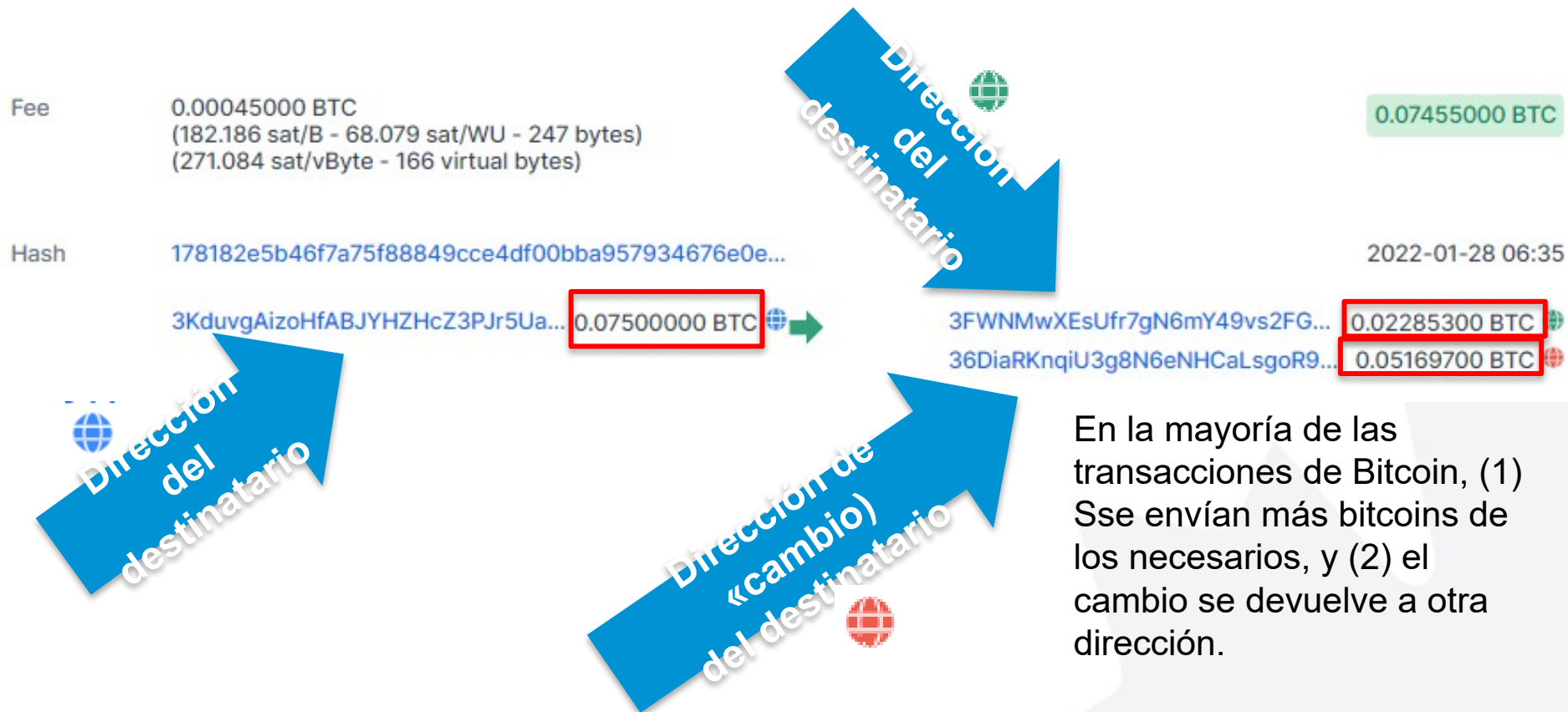
| | |
|--------------|----------------|
| Block Reward | 6.25000000 BTC |
|--------------|----------------|

| | |
|------------|----------------|
| Fee Reward | 0.04385193 BTC |
|------------|----------------|

Block Transactions ⓘ

| | | |
|------------------------------------|---|------------------|
| Fee | 0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 351 bytes) (0.000 sat/vByte - 324 virtual bytes) | 6.29385193 BTC |
| Hash | d6eedf232a48df9d911c35f14c4911abdd1111660ec778... | 2022-01-28 06:37 |
| COINBASE (Newly Generated Coins) → | | |
| | 12dRugNcdxK39288NjcDV4GX7rM... | 6.29385193 BTC |
| | OP_RETURN | 0.00000000 BTC |
| | OP_RETURN | 0.00000000 BTC |
| | OP_RETURN | 0.00000000 BTC |

Transacciones simples



Transacción simple



En ocasiones, se utilizan varias direcciones para reunir el monto necesario antes de enviarlo al destinatario.




Transacciones de servicio

| | | |
|---|--------------|--|
| 1J2xbjqkxzNfjrqrUgUm7L9eYde8xphQc | \$192,560.49 | |
| <div> <div>Dirección del remitente</div> <div>Direcciones del destinatario</div> </div> | | |
| 124oMvN4q8GGFh1zZgTEzsbYnUL6XiA9Ps | \$351.40 | |
| 1EJUphJj1PqnBmEw2vYSVTNfAatPkqwQ4e | \$865.31 | |
| 1BCABWjMq5HBBqFqiT7WgHNGBMaDPFaHrN | \$668.01 | |
| 1E945s1VTLiSy7URwPUSGpRLbX6SRtRAQX | \$11.75 | |
| 1PoWYLUirvaDEYeSHNzeouM2XKA8kqMFn | \$252.63 | |
| 14RFHy9hNcsW1AMJyTP1WiTsnS58CtCaX3 | \$371.32 | |
| 1LWd9hH5HHdUgbNDJf7htjtSyW8ebiMXzd | \$222.05 | |
| 151Cs7YhQ44S3y5YqyvE2Vdb6vC96TuSx | \$223.27 | |
| 1Gi53u341Xfcvtj2W46qgADAEyxBp6VAzn | \$457.01 | |
| 115Fi5utSi6SXdEyDpVJHKXwwarPiQ8yCG | \$169.90 | |
| 1BhkGCZedHwL3xaX43hRkmFV1jFWGmTkPv | \$26.93 | |
| 17xVubHQE7gzd54HgaqgCoXKwzWrxQL3N5 | \$67.20 | |
| 1MBwAAxHUF3np5bkR4o8RsTHr1qJjdJYGj | \$886.09 | |
| 1Ag5gaX5aqkXwhXsWXYZ6yWQZcFJyEUzZk | \$1,483.25 | |
| 1AxtqqdBxBnZHAqh1EqCrky8eHvY9gAa1 | \$381.64 | |
| 1K6apAqNJGp2r6WERFLaTuWshvh4pSkXGo | \$559.57 | |
| 1ApdfmXckRQKvxarc9roJ7iPqF54bg7VQL | \$446.54 | |
| 36GTTCi5TDA978tZHy4D3MdktpPjhdFNdG | \$180.11 | |
| 12N5epQZtWQoYDLh9iYeW9deqZrDjwL66i | \$731.03 | |
| 1G78LBDJ5ezHHvpt8gvJ8cMdSsnKdEK376 | \$8,907.76 | |
| Load more outputs... (49 remaining) | | |

Las transacciones de servicio se agrupan para ahorrar en comisiones.

Seguimiento de transacciones

- Puede trazarse el recorrido de las transacciones, hacia adelante o hacia atrás, examinando las direcciones implicadas para ver el flujo de los bitcoins.
- Este seguimiento puede conducir a plataformas de intercambio u otros proveedores de servicios financieros, donde es posible emitir órdenes de producción y/o obtener información KYC.

| | | |
|------|--|---|
| Fee | 0.00045000 BTC (182.186 sat/B - 68.079 sat/WU - 247 bytes) (271.084 sat/vByte - 166 virtual bytes) | 0.07455000 BTC |
| Hash | 178182e5b46f7a75f88849cce4df00bba957934676e0e... | 2022-01-28 06:35 |
| | 3KduvgAizoHfABJYHZHcZ3PJr5Ua... 0.07500000 BTC  | 3FWNMwXEsUfr7gN6mY49vs2FG... 0.02285300 BTC  |
| | | 36DiaRKnqiU3g8N6eNHCaLsgoR9... 0.05169700 BTC  |

Ejercicio: Dirección de ransomware de WannaCry

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

1. Encuentre una transacción que haya enviado bitcoins a la dirección de WannaCry
2. ¿La transacción envió bitcoins a más de dos direcciones al mismo tiempo?
 - ¿Cuántas?
3. ¿Qué podría sugerir el hecho de que haya dos direcciones receptoras?
4. ¿Qué podría sugerir el hecho de que haya más de dos direcciones receptoras?

<https://www.blockchain.com/explorer>

Ejercicio: Transacción de ransomware de WannaCry

8def6458a46234ab0e040602e7852ff5cf58650f3f1102803b1d4bca4cc293a1

- Busque esta transacción de envío desde la dirección de WannaCry
 1. ¿Se enviaron bitcoins a más de dos direcciones al mismo tiempo?
 2. ¿Qué sugiere eso sobre la dirección de WannaCry?
¿La transacción envió bitcoins a más de dos direcciones al mismo tiempo?

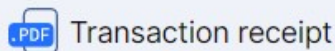
<https://www.blockchain.com/explorer>

Ejercicio de transacción

<https://blockchair.com/>
<https://blockchair.com/>

91aae9ca97764b101a1238a0134db12e64b15596b5e8bcfd7a3eae24c9944482

- Utilice Blockchain.com y Blockchair para examinar la transacción.
- 1. ¿Son iguales los montos de la transacción en BTC?
- 2. ¿Son iguales los montos de la transacción en USD?
- 3. ¿Las marcas de tiempo coinciden?
- Para exportar la información de la transacción desde Blockchair, haga clic en “*Transaction Receipt*”.



IDENTIFICACIÓN DE DIRECCIONES MULTIFIRMA

Scripts de transacciones en la blockchain

- Las transacciones en la blockchain son scripts complejos, y estos scripts se almacenan en la propia blockchain.
- El análisis de scripts permite a los exploradores de blockchain extraer una gran cantidad de información sobre una transacción:
 - Datos de multifirma
 - Datos de *replace-by-fee*
 - Datos de *segregated witness*
 - Datos de *coinbase*
 - Datos OP_RETURN

Cómo identificar si una transacción es multifirma

- Para verificar si una dirección requería múltiples firmas para gastar durante una transacción:
 1. Busque la transacción en Mempool.Space (<https://Mempool.Space/>)
 2. Examine las «entradas y salidas» en busca de una burbuja amarilla que indique si la dirección emisora era multifirma (y cuántas firmas se utilizaron).
 3. Haga clic en “Details” para ver el script.
 - El primer OP_PUSHNUM_# indica el número de claves utilizadas.
 - El segundo OP_PUSHNUM_# indica el número total de claves posibles para la dirección multifirma.

MENSAJES EN LA BLOCKCHAIN

Se pueden insertar mensajes o datos en la blockchain de Bitcoin

- Los mensajes pueden crearse usando direcciones personalizadas (***vanity addresses***).
- Los mineros pueden agregar mensajes en las ***coinbase transactions*** (transacciones de recompensa).
- Los usuarios pueden insertar mensajes de hasta 80 bytes durante una transacción, utilizando la función **OP_RETURN**.

Ejercicio: Mensajes en la Blockchain de Bitcoin

1. ¿Cuál fue el mensaje insertado en la primera transacción de Bitcoin? (**Consulte los “Technical Details” – Coinbase Data.**)
 - <https://blockchair.com/bitcoin/block/0>
2. ¿Cuál fue el mensaje de WikiLeaks del 20 de noviembre de 2016, creado mediante direcciones de Bitcoin en una transacción? (**Mire los primeros caracteres de las direcciones receptoras.**)
 - <https://www.blockchain.com/btc/tx/fc722ce39094500690a4d4676fe475520d6a0af590336b73202010ca260bbd20>