

Práctica 1. Blockchain.info

1. Objetivo

Afianzar los conceptos del blockchain de Bitcoin monitoreando la cadena de bloques con la herramienta blockchain.info

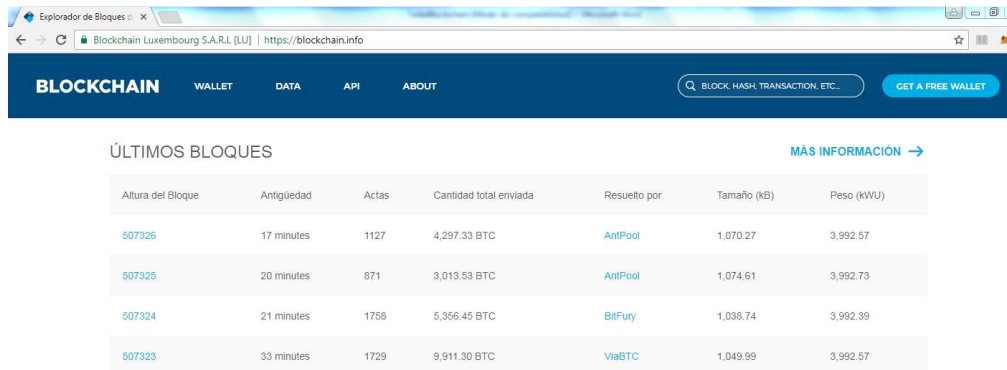
2. Introducción

Blockchain.info (<https://blockchain.info/>) es un proveedor de monederos para Bitcoin. También es una de las herramientas de exploración de la cadena de bloques de Bitcoin más populares.

3. Desarrollo

3.1. Página principal

Entremos a la página principal:



The screenshot shows the Blockchain.info website interface. At the top, there is a navigation bar with links for WALLET, DATA, API, and ABOUT. Below this, a table titled 'ÚLTIMOS BLOQUES' (Latest Blocks) displays the most recent blocks in the Bitcoin chain. The table has seven columns: 'Altura del Bloque' (Block Height), 'Antigüedad' (Age), 'Actas' (Transactions), 'Cantidad total enviada' (Total amount sent), 'Resuelto por' (Solved by), 'Tamaño (kB)' (Size in kB), and 'Peso (kVU)' (Weight in kVU). The first four rows of the table are visible, showing blocks 507326, 507325, 507324, and 507323. The 'Resuelto por' column shows the mining pool for each block: AntPool, AntPool, BitFury, and ViaBTC.

Altura del Bloque	Antigüedad	Actas	Cantidad total enviada	Resuelto por	Tamaño (kB)	Peso (kVU)
507326	17 minutes	1127	4,297.33 BTC	AntPool	1,070.27	3,992.57
507325	20 minutes	871	3,013.53 BTC	AntPool	1,074.61	3,992.73
507324	21 minutes	1758	5,356.45 BTC	BitFury	1,038.74	3,992.39
507323	33 minutes	1729	9,911.30 BTC	ViaBTC	1,049.99	3,992.57

Figura 1. Página principal de blockchain.info

Encontramos la siguiente información:

- **Altura.** La posición del bloque en la cadena

Con base en la información obtenida, ¿aproximadamente hace cuánto que está activa la cadena? Recuerde que un bloque se agrega aproximadamente cada 10 minutos

- **Antigüedad.** El tiempo transcurrido entre un bloque y otro

¿Hace cuánto tiempo se minó? En promedio, deberían verse saltos de alrededor de 10 minutos

- **Actas.** Es el número de transacciones que tiene el bloque

- ### 3.2. Información de un bloque

Bloques #507343

Figura 2. Información de un bloque

¿Qué bloque minó, cuántas transacciones tenía, cuál fue el promedio de comisión por transacción (en dólares)?

Recompensa. Sabemos que la recompensa que se recibe por minar un bloque se reduce a la mitad cada 210,000 bloques.

¿Qué recompensa recibieron los bloques 209,999; 210,000; 409,999 y 420,000? (Puede colocar el número de bloque en el campo de búsqueda en la esquina superior derecha)

Al barrer hacia abajo la página, aparece información sobre las transacciones como se muestra en la figura 3.

Actas

0dca90e0482fc9510c68791dc77e0ae79dd5aabbf456cbe7b0d3e94af309e3		(Tamaño: 243 bytes) 2018-02-02 23:57:33
No hay entradas (monedas recién generadas)	➔ 1C1mCxRukix1KfegAY5zQJv7samAcIzpv - (No gastado) No se puede decodificar la dirección de salida - (No gastado)	\$ 120,377.97 \$ 0.00
		\$ 120,377.97
67d980f5be90077f6838a9c3be4964ecceada9adec99a08265c4e8df0261765		(Cuota: \$ 1.06 - 13.44 sat/WU - 53.76 sat/B - Tamaño: 226 bytes) 2018-02-02 22:24:06
13b2Fg52YuzrW3KSEEKSPDttXyeQa2ic (\$ 563,557.97 - Salida)	➔ 121IS21CPj5Szqfa6gESE8ymcJ6nCRJnz - (No gastado) 1PIMp3V2LUCJ7yMTuG2KQGFH5f6B4Gu8A - (Gastado)	\$ 126,575.91 \$ 436,981.00
		\$ 563,556.91
feb0416bd37176c2a709211f07dc1b8926d76e48d67e3d18586cb550750ec8d		(Cuota: \$ 52.44 - 666.67 sat/WU - 2,666 sat/B - Tamaño: 225 bytes) 2018-02-02 23:56:08
1H6ZZpRmMnW8yepv3BYwMjYYnEKWDqVP (\$ 196,054.29 - Salida)	➔ 19Fyyr1vA7WFKKp2w6Ae9uGKUX6ArFBIG5 - (Gastado) 1H6ZZpRmMnW8yepv3BYwMjYYnEKWDqVP - (No gastado)	\$ 3,928.46 \$ 192,073.39
		\$ 196,001.85
03fe390a28090a022f9e03e0dadab38d3180a4b07280a57adce5dc18643ba		(Cuota: \$ 37.14 - 284.85 sat/WU - 1,139 sat/B - Tamaño: 373 bytes) 2018-02-02 23:54:45

Figura 3. Transacciones

El hash en los renglones sombreados identifica a esa transacción. En el renglón también aparece la hora en que llegó esa transacción.

En el renglón de abajo aparecen las carteras de salida (a la izquierda) y de entrada (a la derecha). Puede haber más de una cartera de salida para poder juntar el monto total a enviar, desde distintos fondos. *Esto puede afectar la comisión a pagar.*

El botón verde muestra el total de la transacción en BTC. Si damos clic en él, todos los valores de criptomoneda se convierten a dólares americanos, como se muestra en la figura 3.

3.3. Transacción

Si damos clic al hash de la transacción, aparecerá una pantalla como la de la figura 4.

Transacción Ver información de una transacción de Bitcoin

53e2b20328846144553ce6e8922384c3c1723e5f07e65965d3f038a4bac14

37qLMAmEZxw5mFhRdMjrfmCPZhrCc2e (0.0071445 BTC - Salida)

➔

3LTSLSW8NpDw144Umn7UCEKzTyTbcFFYpgh - (No gastado)

1Lraaic2rb6FC6g53WzxbgBKkCXouYjgr - (No gastado)

0.0000916 BTC

0.0065 BTC

15 Confirmaciones

0.0065916 BTC

Resumen

tamaño

249 (Bytes)

Peso

669

Hora de Recepción

2018-02-02 23:53:48

Incluidas en el Bloque

507342 (2018-02-02 23:54:03 + 0 minutos)

Confirmaciones

15 Confirmaciones

Visualizar

Ver Gráfico de Árbol

Entradas y Salidas

Entrada total

0.0071445 BTC

Salida Total

0.0065916 BTC

Comisiones

0.0005529 BTC

Tarifa por byte

222.048 sat/B

Tarifa por unidad de peso

82.646 sat/WU

Estimado de BTCs transaccionados

0.0000916 BTC

Scripts

Ocultar scripts y Coinbase

Scripts de Entrada

ScriptSig: PUSHDATA[22]([0014f1e5c32b4bc45564405ed96cf59227a2d9002669])
Witness: 0247304402207df3d1eaf790a25950d5f2de37f95626bdf259e0b6544ff625908b4a6c37310022017e47f45e6a917de8771bd3ca75de5664265e6e00d75093991b648b0e5dae2a012103

Scripts de Salida

HASH160 PUSHDATA[20]([cd8f208596ad18aa7f3f034fc8a01d3b0c0157f] EQUAL
DUP HASH160 PUSHDATA[20]([d9cace6e622fc2749e4ec8f320b76c0c5ffe7dd] EQUALVERIFY CHECKSIG

Figura 4. Una transacción

En el resumen encontramos detalles de la transacción, como su tamaño y el costo en watts (peso), nuevamente la hora de recepción y el bloque en que fue registrada. A la derecha se muestran el total de salida, de entrada y las comisiones pagadas.

Podemos gráficamente la secuencia de los BTC utilizados dando clic en *Ver Gráfico de Árbol*. Conviene que seleccione una transacción que tenga salidas gastadas. Al dar clic en los círculos naranja, que representan las salidas gastadas, va creciendo el grafo mostrando cómo fueron siendo intercambiados los BTC. Ver figura 5.

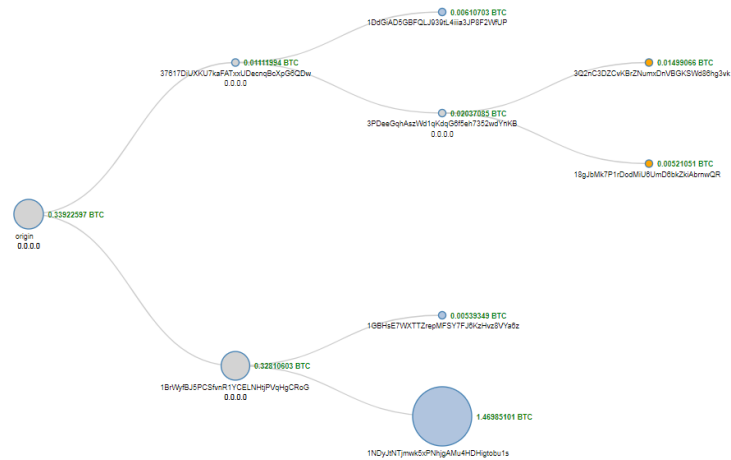


Figura 5. Gráfica de árbol de intercambios de BTC

Encuentre una transacción donde se vean al menos cuatro niveles en la gráfica de árbol. Indique el bloque en donde está la transacción y el hash de la transacción (primeros 4 y últimos 4 dígitos)

3.4. Una cartera

Regresemos a la vista de la figura 4. En la parte superior podemos ver las carteras que fueron utilizadas en esta transacción. Al seleccionar una de ellas, se obtendrá información sobre esa cartera, como su dirección y el hash de la dirección (figura 6).

A la derecha se observa un resumen de las transacciones y los fondos que aún quedan disponibles. Las transacciones que ha realizado se muestran cronológicamente en la parte inferior.

Dirección de Bitcoin Las direcciones son identificadores que se utilizan para enviar Bitcoins a otra persona.

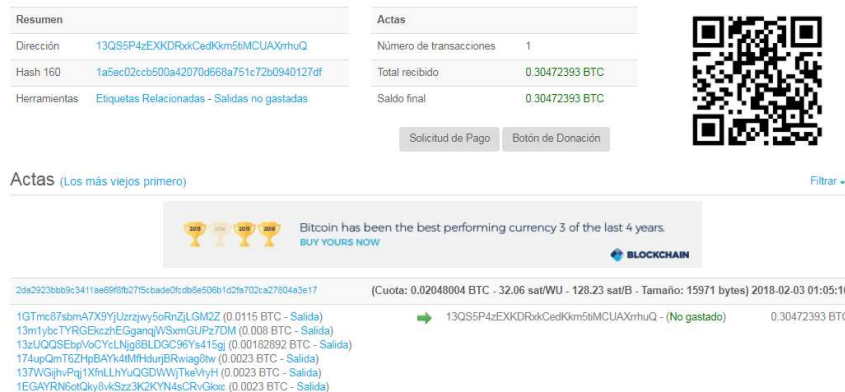


Figura 6. Información de una cartera

Busque el bloque 27218. ¿Cuántas transacciones tiene? ¿Cuánto se le pagó de recompensa? ¿Qué significará esto?

3.5. Estadísticas

Para terminar, veamos algunas estadísticas que ofrece este sitio. De clic en la opción Data/Charts del menú principal.



Figura 7. Estadísticas de los bloques

Podrá encontrar estadísticas de los bitcoins, como su fluctuación en el mercado, su capitalización y la evolución de las monedas en circulación. También podrá encontrar estadísticas de los bloques (figura 7), de los mineros y del sistema en su conjunto.

Para terminar con esta práctica, siéntase en libertad de navegar por esta sección. Reporte un par de estadísticas que le hayan parecido interesantes.