

PRACTICAS-BLOCKCHAIN

Alejandro Ramírez y David Seijas

February 2022

1 Practica 1

Adjuntamos capturas en los ejercicios en los que se sugiere utilizarlas.

1.1 BITCOIN

1.1.1 Ejercicio 1

Somos el grupo 9, por lo que hemos buscado la información del bloque 722109. En las capturas señalamos los datos que se piden:

[Explorador](#) > [Bitcoin Explorer](#) > [Bluecoin](#)
USD <
 Buscar tu transacción, una dirección o un bloque

Bloque 722109 ⓘ

Este bloque se minó el día febrero 06, 2022 a las 11:09 PM GMT +01:00 por [Unknown](#). En la actualidad tiene 507 confirmaciones en la cadena Bitcoin.

El minador/los minadores de este bloque ganaron una recompensa total de 6.25000000 BTC (281.650,75 US\$). La recompensa consistía en una recompensa base de 6.25000000 BTC (281.650,75 US\$) con una recompensa de 0.12733180 BTC (5738,09 US\$) pagada en calidad de 1756 transacciones que estaban incluidas en el bloque. La recompensa Bitcoin, también llamada recompensa Coinbase, se enviaron a esta dirección:

Un total de 33.914.8004989 BTC (1.528.340.619,22 US\$) se enviaron en el bloque, siendo la transacción media 19.3136455 BTC (870.353,43 US\$). Aprende más sobre cómo funcionan los bloques.

Hash	000000000000000000000000f8f6967ae01c056f0ec649e77bbaf039e3012f64a48385 ⓘ
Confirmaciones	507
Sello de tiempo	2022-02-06 23:09 ⓘ
Altura	722109 ⓘ

Número de transacciones	1756
Complejidad	26.690.525.287.405,50 ⓘ
Raíz de merkle	0811905004bdcc3f45f1ce0fb70f2870ebfc3f247ef1ff753ea9429f7af64036
Versión	0x20004004
Bits	386.567092
Peso	3.992.899 WU
Tamaño	1.425.520 bytes
Único	737.565.754
Volumen de transacciones	33914.800498989 BTC
Recompensa de bloque	6.25000000 BTC
Recompensa de tasa	0.12733180 BTC ⓘ

El número de 0's iniciales del hash está directamente relacionado con la dificultad de minado del bloque. El minero obtiene una recompensa de 6.25 bitcoins por el minado del bloque, además de las tasas de cada transacción que se incluye en el propio bloque. Las tasas de la transacción es la moneda que

surge de la diferencia entre las monedas resultado y las monedas origen. En total, el minero ha obtenido $0.127 + 6.25 = 6.337$ bitcoins

1.1.2 Ejercicio 2

La dificultad se debe modificar periódicamente para que de media se tarden aproximadamente 10-15 minutos en minar un nuevo bloque. El bloque 123456 presenta una complejidad menor. Además se aprecia que el número de 0's iniciales del hash también es menor.

Bloque 123456	
Este bloque se minó el día mayo 12, 2011 a las 1:48 PM GMT +02:00 por Unknown . En la actualidad tiene 596.163 confirmaciones en la cadena Bitcoin.	
El minero/las mineras de este bloque ganaron una recompensa total de 50.00000000 BTC (2.242.200,00 USD). La recompensa consistió en una recompensa base de 50.00000000 BTC (2.242.200,00 USD) con una recompensa adicional de 0.00000000 BTC (22,62,20 USD) pagada en calidad de 13 transacciones que estaban incluidas en el bloque. Las recompensas Block, también llamadas recompensas Coinbase, se enviaron a esta dirección .	
Un total de 165.50889992 BTC (7.422.081,11 USD) se enviaron en el bloque, siendo la transacción media 12.71345384 BTC (570.929,32 USD). Aprende más sobre cómo funcionan los bloques.	
Hash	f0c0d0e00000000002917cd0805cc6174aacdfdc4f63cf480aaef682ff6cdc83cc3ca
Confirmaciones	596.163
Sello de tiempo	2011-05-12 13:46
Altura	123456
Minador	Unknown
Número de transacciones	13
Complejidad	107.4316,4m

1.1.3 Ejercicio 3

Ya hemos visto anteriormente que el minero del bloque 722109 ha ganado 6.37 bitcoins. La transacción asociada a esta ganancia es la siguiente

Transacciones de bloque ①			
Cuota	0.00000000 BTC (0.000 sat/Byte - 0.000 sat/WU - 206 bytes) (0.000 sat/Byte - 179 virtual bytes)		6.37733160 BTC
Hash	b64d2a7590af010f4a6f0e225fa3984a2c9250ca9424b6707872e...		2022-06-08 23:09
	CONBASE (Monedas Generadas Últimamente)	➡	bcd3appanhefcldm48bzuzqpf8fd6dcspu0h9qj2 OP_RETURN
			6.37733160 BTC 0.00000000 BTC
Cuota	0.00076400 BTC (341.071 sat/Byte - 65.268 sat/WU - 224 bytes)		1.44332889 BTC
Hash	bea93993850f7b4de4744612a7568a6f1cda30135cdca83427e...		2022-06-08 23:01
	190ca0c196cf7d91cd963e92679c47202	➡	382d307f7hw92q3773y9uYwVkgbjiu5oIcN OP_RETURN
			0.00129201 BTC 1.44332889 BTC

1.1.4 Ejercicio 4

El bloque 300000 se minó con una recompensa (25 BTC) que cuadruplica la del 722109. En números de bloques esto tiene sentido, pues cada 210.000 bloques se divide a la mitad la ganancia.

Bloque 300000

USD

BTC

Este bloque se minó el día mayo 10, 2014 a las 8:32 AM GMT +02:00 por [GHash.IO](#). En la actualidad tiene 422,618 confirmaciones en la cadena Bitcoin.

El minador/los minadores de este bloque ganaron una recompensa total de 25,000,000,000 BTC (123,141.50 US\$). La recompensa consistía en una recompensa base de 25,000,000,000 BTC (123,141.50 US\$) con una recompensa de 0.04028360 BTC (1809.77 US\$) pagada en calidad de 237 transacciones que estaban incluidas en el bloque. Las recompensas Block, también llamadas recompensas Coinbase, se enviaron a esta [dirección](#).

Un total de 2,055,014,082,45 BTC (92,322,863.96 US\$) se enviaron en el bloque, siendo la transacción media 8.67094550 BTC (389,547.95 US\$). Aprende más sobre [cómo funcionan los bloques](#).

Hash	0000000000000000082c0cf8f1557c5d40b21edab618d2d691c0f87118bac7254
Confirmaciones	422,618
Sello de tiempo	2014-05-10 08:32
Altura	300000
Minador	GHash.IO
Número de transacciones	237
Complejidad	8,000,872,135.97
Raíz de merkle	915c887a2d9ec3f56da648bedcf4ed30d0988e22268cfe43ab5b0c0f863899d3
Versión	0x2
Bits	419,465,580
Peso	515,240 WU
Tamaño	128,810 bytes
Único	222,771,801
Volumen de transacciones	2055,014,082,45 BTC
Recompensa de bloque	25,000,000,000 BTC
Recompensa de tasa	0.04028360 BTC

1.1.5 Ejercicio 5

El bloque 722612 fue minado a las 11:48. Son las 13:13 y ya se han minado otros 5 bloques nuevos, por lo que podemos asumir que el bloque ya es definitivo. El bloque 722617 (que lo confirmaba por 6^a vez) se minó a las 13:04, así que han pasado 76 minutos para que sea definitivo.

En el bloque 722612, el campo de confirmaciones indica que hay 6. Hemos seguido esta marca, aunque difiere en un bloque con el concepto de confirmaciones del enunciado. Si siguiéramos el enunciado, deberíamos esperar al minado del bloque 722618 para obtener las 6 confirmaciones.

Bloque 722612

USD

BTC

Este bloque se minó el día febrero 10, 2022 a las 11:48 AM GMT +01:00 por [Unknown](#). En la actualidad tiene 6 confirmaciones en la cadena Bitcoin.

El minador/los minadores de este bloque ganaron una recompensa total de 6,250,000,000 BTC (281,208.44 US\$). La recompensa consistía en una recompensa base de 6,250,000,000 BTC (281,208.44 US\$) con una recompensa de 0.11299728 BTC (5084.13 US\$) pagada en calidad de 2943 transacciones que estaban incluidas en el bloque. Las recompensas Block, también llamadas recompensas Coinbase, se enviaron a esta [dirección](#).

Un total de 33,470,608,529,71 BTC (1,505,954,804.29 US\$) se enviaron en el bloque, siendo la transacción media 11.37295567 BTC (511,707.37 US\$). Aprende más sobre [cómo funcionan los bloques](#).

Hash	0000000000000000000000001e3a3a8f31a6c69cad378b12e253c968da9f0f68f79ac
Confirmaciones	6
Sello de tiempo	2022-02-10 11:48
Altura	722612

Bloque 722617

USD

BTC

Este bloque se minó el día febrero 10, 2022 a las 1:04 PM GMT +01:00 por [AntPool](#). En la actualidad tiene 1 confirmaciones en la cadena Bitcoin.

El minador/los minadores de este bloque ganaron una recompensa total de 6,250,000,000 BTC (281,178.56 US\$). La recompensa consistía en una recompensa base de 6,250,000,000 BTC (281,178.56 US\$) con una recompensa de 0.14764864 BTC (6642.50 US\$) pagada en calidad de 3315 transacciones que estaban incluidas en el bloque. Las recompensas Block, también llamadas recompensas Coinbase, se enviaron a esta [dirección](#).

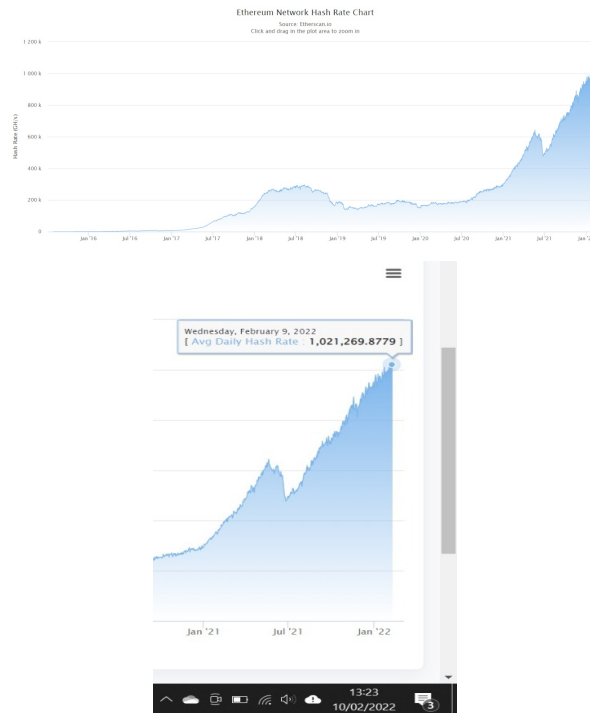
Un total de 102,868,751,641,0 BTC (4,628,816,902.18 US\$) se enviaron en el bloque, siendo la transacción media 31.03732476 BTC (1,396,324.86 US\$). Aprende más sobre [cómo funcionan los bloques](#).

Hash	00000000000000000000000a4e1270dbe42e22ca6ec6ae4c4269f0ce4454707d57
Confirmaciones	1
Sello de tiempo	2022-02-10 13:04
Altura	722617
Minador	AntPool

1.2 Ethereum

1.2.1 Ejercicio 6

La gráfica de hashrate viene dada en gigaHashes/segundo. Ayer, Miércoles 9 de Febrero, el ratio marcaba 1.021.269,8779, lo que significa 1×10^{15} hashes/segundo aproximadamente.



1.2.2 Ejercicio 7

En Ethereum el ratio de transacciones/segundo es de 14.5



1.2.3 Ejercicio 8

El bloque 14178311 tiene un uncle block (en este caso coincide con el anterior, es decir, 14178310). El minero del uncle block obtuvo una recompensa de 1.75

ethers, mientras que el minero del bloque analizado ganó 2.14 ethers. Se observa que no existe gran diferencia entre ambas ganancias. Además, explorando la web nos hemos dado cuenta de que la mayoría de bloques no tienen un uncle block.

Block #14178311	
Flashbots Unconventional Ordering	
Overview Comments	
Block Height:	14178311
Timestamp:	6 mins ago (Feb-10-2022 12:20:16 PM +UTC)
Transactions:	236 transactions and 250 contract internal transactions in this block
Mined by:	0x7f101fe45e040a0fb8f3f8b43ed03d3532b00c (Flexpool.io) in 7 secs
Reward:	2.147671803763910438 Ether (2 + 1.545670610232833612 + 0.0625 - 1.460498806468823174)
Uncles Reward:	1.75 Ether (1 uncle at Position 0)
Difficulty:	12,931,492,535,736,926
Total Difficulty:	41,129,797,726,484,335,145,100
Uncle #0x2b2433815a4cef61cf249b06648f9a59a50eef10443281a82bac562a2b2598fe	
Overview	
Uncle Height:	14178310
Uncle Position:	0
Block Height:	14178311
Hash:	0x2b2433815a4cef61cf249b06648f9a59a50eef10443281a82bac562a2b2598fe
Parent Hash:	0x6714857e120fb73022f836a8526dc6eb6d7a1274f36088681e423d4acbaa7b
Sha3Uncles:	0x1dcd4de8dec75d7aab85b567b6cc041ad312451b048a7413f0a142f640d49347
Mined by:	0x829bd824b016326a401d083b33d09229333a830 (F2Pool Old) in 0 secs
Difficulty:	12,925,177,119,129,431

1.2.4 Ejercicio 9

Un contrato es un código fuente asociado a una address de la blockchain. También almacena su estado (valor de sus variables). A parte de la captura del contrato, incluimos otras que muestran información de las transacciones que se han realizado a este contrato y el código fuente

Contract 0xAc17f9a002e025220d09e5e07c130c1f40	
Sponsored: Nexo - Earn up to 20% on your Stablecoins, paid out daily! Start Earning	
Contract Overview	
Balance:	1 wei
Ether Value:	Less Than \$0.01 (0 \$1.04 (2467%))
Token:	+ \$768,781.89
Advertise your brand here! Start Today	
More Info	
My Name Tag:	Not Available, login to update
Contract Creator:	0x3902800bc1ebd7e8... at bn 0x211d52b44f77e842a...
Token Tracker:	Solter USD (USDt) (0\$0.0995)
Transactions Internal Txns Erc20 Token Txns Erc721 Token Txns Contract Events Analytics Info Comments	
If Lateral 20 from a total of 15,330,708 transactions	
(> More than 25 Pending Txns)	

Transactions	Internal Txns	ERC20 Token Txns	ERC721 Token Txns	Contract	Events	Analytics	Info	Comments
17 Latest 25 from a total of 125,193,078 transactions (> More than 25 Pending Txns)								
Txn Hash	Method	Block	Age	From	To	Value	Txn Fee	
0x9b7860d6d3b4c45a...	transfer	(pending)	1 sec ago	Crypto.com 2	Tether: USDT Stablecoin	0 Ether	(pending)	
0xa6d0f6a413181444b...	transfer	(pending)	1 sec ago	0xa3043ba059478856...	Tether: USDT Stablecoin	0 Ether	(pending)	
0x245d4d881e118d888...	transfer	(pending)	1 sec ago	Coinbase 5	Tether: USDT Stablecoin	0 Ether	(pending)	
0x3e6c38d8a3a0c4997...	transfer	(pending)	1 sec ago	0x3355b671855d4d19...	Tether: USDT Stablecoin	0 Ether	(pending)	
0x95d32229c18a088...	transfer	(pending)	1 sec ago	0x40a4361e45791d5e...	Tether: USDT Stablecoin	0 Ether	(pending)	
0x9c38433c95d3250c...	transfer	(pending)	1 sec ago	0xa23a95ea153e892cd...	Tether: USDT Stablecoin	0 Ether	(pending)	
0xeca4e7822c6b727...	transfer	(pending)	5 secs ago	Binance 18	Tether: USDT Stablecoin	0 Ether	(pending)	
0x34a6d46216d4302...	transfer	(pending)	10 secs ago	Coinbase 5	Tether: USDT Stablecoin	0 Ether	(pending)	

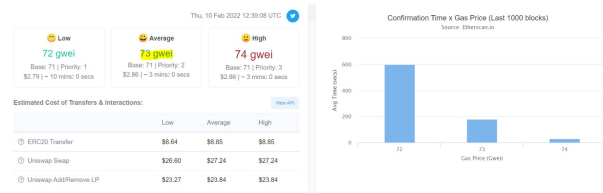
Contract Source Code (Solidity) [Audit Report](#)

```

1 * /**
2  *Submitted for verification at Etherscan.io on 2017-11-28
3  */
4
5  pragma solidity ^0.4.17;
6
7  /**
8   * @title SafeMath
9   * @dev Math operations with safety checks that throw on error
10  */
11  library SafeMath {
12    function mul(uint256 a, uint256 b) internal pure returns (uint256) {
13      if (a == 0) {
14        return 0;
15      }
16      uint256 c = a * b;
17      assert(c / a == b);
18      return c;
19    }
20
21    function div(uint256 a, uint256 b) internal pure returns (uint256) {
22      // assert(b > 0); // Solidity automatically throws when dividing by 0
23      uint256 c = a / b;
24      // assert(a == b * c + a % b); // There is no case in which this doesn't hold
25      return c;
  
```

1.2.5 Ejercicio 10

El gas promedio de las últimas transacciones es de 73 gwei, que son 73000000000 wei o 0,000000073 ethers. Una transferencia que requiere de 21000 unidades de gas cuesta $21000 * 0,000000073 = 0,001533$ ethers, que son 4.77558627 dólares (1 ether = 3115.19\$).




ETHER PRICE
\$3,115.19 @ 0.0711 BTC