



UTN.BA

UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES



ciie

Centro de Investigación
e Innovación Educativa

¿Cómo funciona Bitcoin?

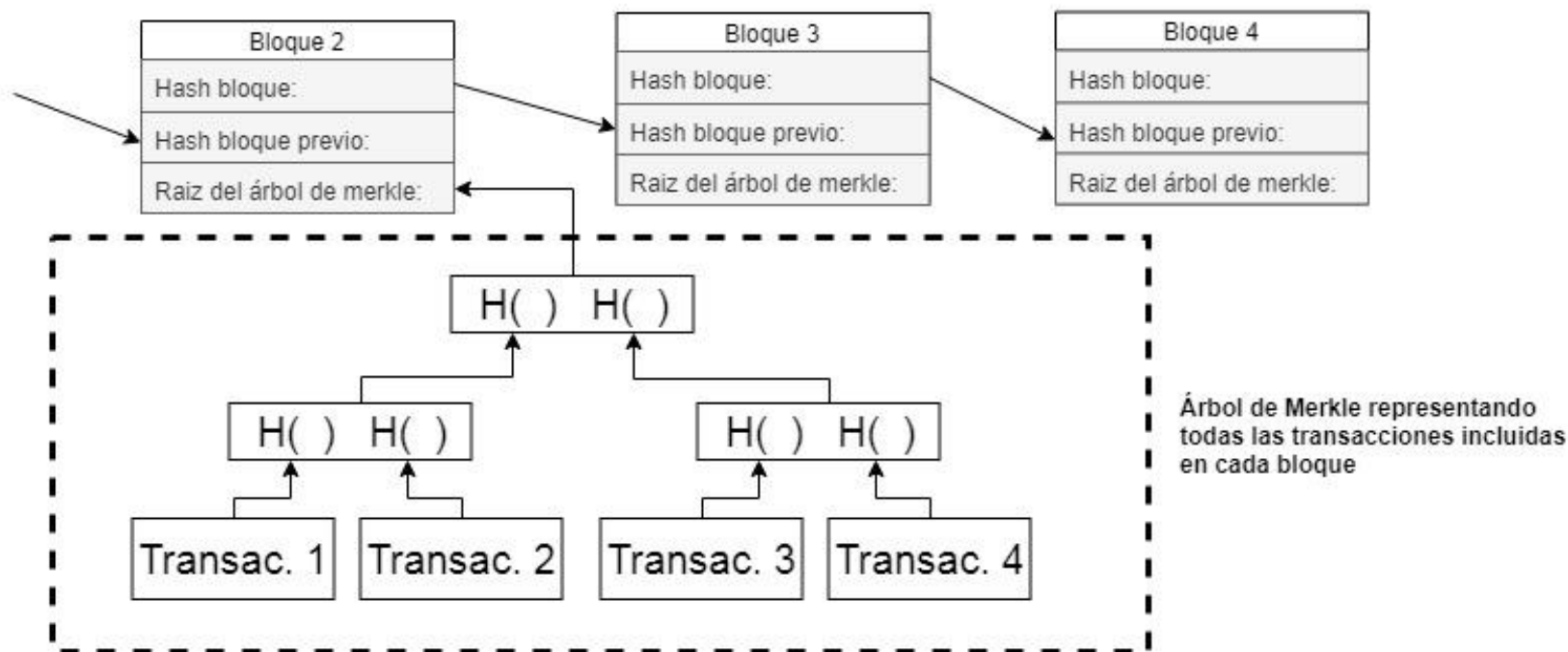
3.3 Bloques Bitcoin

La razón para agrupar “tx” en bloques

Por qué agrupar las transacciones?

- Se transforman en una sola unidad de trabajo para los mineros
- Limita la longitud de la cadena de hashes de los bloques

La Blockchain de Bitcoin



Encabezado del Bloque

Tamaño del campo	Descripción	Tipo de datos	Comentarios
4	versión	int32_t	Bloquear información de versión (nota, esto está firmado)
32	bloque anterior	char [32]	El valor hash del bloque anterior a este bloque particular hace referencia
32	merkle_root	char [32]	La referencia a una colección de árbol Merkle que es un hash de todas las transacciones relacionadas con este bloque
4	marca de tiempo	uint32_t	Una marca de fecha y hora cuando se creó este bloque (se desbordará en 2106 ^[2])
4	nBits	uint32_t	El objetivo de dificultad calculado que se está utilizando para este bloque.
4	nonce	uint32_t	El nonce utilizado para generar este bloque ... para permitir variaciones del encabezado y calcular diferentes hashes
1	txn_count	var_int	Número de entradas de transacciones, este valor es siempre 0

Encabezado del Bloque: Construcción del puzzle

Campo	Propósito	Actualizado cuando ...	Tamaño (Bytes)
Versión	Número de versión del bloque	Actualizas el software y especifica una nueva versión.	4
hashPrevBlock	Hash de 256 bits del encabezado de bloque anterior	Entra un nuevo bloque	32
hashMerkleRoot	Hash de 256 bits basado en todas las transacciones en el bloque	Se acepta una transaccion	32
Hora	Marca de tiempo actual como segundos desde 1970-01-01T00: 00 UTC	Cada pocos segundos	4
Bits	Objetivo actual en formato compacto.	Se ajusta la dificultad.	4
nonce	Número de 32 bits (comienza en 0)	Se prueba un hash (incrementos)	4

Estructura del bloque

```
"hash": "0000000000000048b0c039662062210c361d65e61ff647675f8c1996c81df62ec2",
"confirmations": 2,
"strippedsize": 19707,
"size": 32114,
"weight": 91235,
"height": 1448370,
"version": 536870912,
"versionHex": "20000000",
"merkleroot": "950f320d615072892cf917e0b25761129d69e75d77e74c47dbae46bcb056a0d7",
"tx": [
  "eca5f7d704e42d5b105a1ee25f114f1b4dd66710144715b1db40c50f667e308e",
  "366423fd81eac9d987ebc2f7076bfd213deea0ac1fd6962e1e0ed1a959b60961",
  "622f4293fefa2434148783ecc9ea7d3db90660d95ef40f2f908fd4ef12951d4e",
  "95d10b1dc494c9325afb3c44572b804793105c2c5de2129461e4a37f662ada92",

  "531b714e86647fc8045c58f0fde6fbb700b11f05e5012153b19e7f8d57695ce8",
  "fe10d0bfc6018cf1302b8924320d60c43a55934508e3247c5397bff6b3f69bf2"
],
"time": 1545157786,
"mediantime": 1545154063,
"nonce": 1230191700,
"bits": "1d00ffff",
"difficulty": 1,
"chainwork": "0000000000000000000000000000000000000000000000000000000000000000dd49671ab2d837840d",
"previousblockhash": "000000000000000819c7d67c99da4e286558ab6fc86319b8e0bccf849769e861e",
"nextblockhash": "000000000000eb5ebd547659ab3adf743e9eca6ed38aca24c03e9438b771a2d12"
```

Transacción de base monetaria “Coinbase”

La información del parámetro coinbase es arbitraria



```
"ver":1,
"inputs":[
  {
    "sequence":4294967295,
    "witness":"0120000000000000000000000000000000000000000000000000000000000000",
    "script":"0390fd08000411494c5d0412862e0e08da60b25c390f4100092f426974667572792f"
  }
],
"weight":692,
"block_height":589200,
"relayed_by":"0.0.0.0",
"out":[
  {
    "spent":false,
    "tx_index":477911042,
    "type":0,
    "addr":"3KF9nXowQ4asSGxRRzeiTpOjMuuM2nypAN",
    "value":1303919997,
    "n":0,
    "script":"a914c08e030911ba85f4a3c324ec6aa6d6722250be7487"
  },
  {
    "spent":false,
    "tx_index":477911042,
    "type":0,
    "value":0,
    "n":1,
    "script":"6a24aa21a9ed29322dec713dc3fbd3160e80bb5ed7356f0622b8b76790f74553bade3627d3e"
  }
],
"lock_time":0,
"size":200,
"double_spend":false,
"block_index":1777529,
"time":1565280539,
"tx_index":477911042,
"vin_sz":1,
"hash":"5b5ad9d6ef5c3d42b260f3fb55c0df3908eaae12f767fc1287143d195c834843",
"vout_sz":2
```

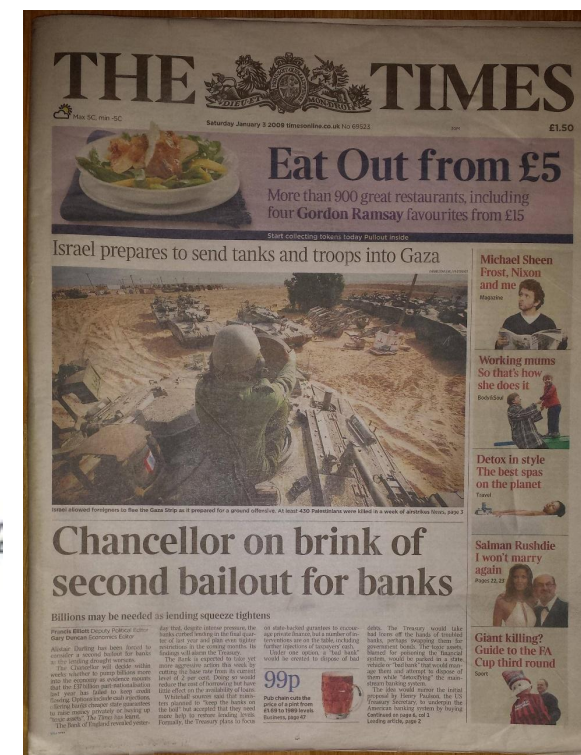
Parámetro coinbase del bloque Génesis

El 3 de enero del año 2009 se minó el primer bloque de la red Bitcoin.
La transacción coinbase del bloque 0:

- Tx Id: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

CoinBase

04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f77
(decoded)   EThe Times 03/Jan/2009 Chancellor on brink of second bailout for banks



Exploradores de bloques

Estas son las webs de algunos exploradores de bloques:

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



BLOCKCHAIN

2. <https://blockexplorer.com/>



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




BLOCKCHAIR

Blockchain.info últimos bloques

BLOCKCHAIN**WALLET****DATA****API****ABOUT**

Q BLOCK, HASH, TRANSACTION, ETC...

GET A FREE WALLET

 WE'RE PACKING OUR BAGS AND PREPARING TO MOVE...DOMAINS!

LATEST BLOCKS

[SEE MORE →](#)

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)	Weight (kWU)
529083	11 minutes	381	965.23 BTC	ViaBTC	218.37	786.89
529082	14 minutes	1458	5,694.74 BTC	Unknown	711.42	2,363.91
529081	27 minutes	1044	8,003.67 BTC	SlushPool	493.15	1,691.97
529080	36 minutes	485	1,378.10 BTC	BTC.com	190.6	635.75



Blockchain.info transacciones dentro del bloque

BLOCKCHAIN			
WALLET	DATA	API	ABOUT
<input type="text" value="BLOCK, HASH, TRANSACTION, ETC..."/>			GET A FREE WALLET
Transactions			
<div>8008d111b749174373da3b58c24a3cb7b5f681357a7933f142d0173e4199b8dd (Size: 290 bytes) 2018-09-26 21:08:29</div>			
No Inputs (Newly Generated Coins)	➔	bc1qjl8uwezzlech723lpryuza0h2cdkvvxh54v3dn - (Spent) Unable to decode output address - (Unspent) Unable to decode output address - (Unspent)	12.57896091 BTC 0 BTC 0 BTC <div>12.57896091 BTC</div>
<div>aca8b6e69c83c1bf9cf0934503f458e6df9794eb2a13ceaba3dbd97f63803a6 (Fee: 0.0025 BTC - 168.46 sat/WU - 673.85 sat/B - Size: 371 bytes) 2018-09-26 21:06:31</div>			
18ePfs2bLsUwUWT6gtfDUDMDB4tv4fhFk (0.0508261 BTC - Output) 1Lcncvgzht93cQoeGuiMXwLXtca1UYXa (1.0165 BTC - Output)	➔	3MYKzo57rTo6j6a6jFhsxEg3UM8DmtFtqH - (Unspent) 123Vkoob88D9aV6sqNjDc1sFLSpUqSC3kY - (Unspent)	1.064 BTC 0.0008261 BTC <div>1.0648261 BTC</div>
<div>1418a96b847a38e3d04a2d5c2454e016f39977fe3a5f64cc741b569b36aca51e (Fee: 0.00078733 BTC - 87.48 sat/WU - 349.92 sat/B - Size: 225 bytes) 2018-09-26 21:07:41</div>			
18UyRSR4LhJ2KnYBErhmqBZHLnLvgNiSGu (0.06210959 BTC - Output)	➔	16L8RL4rzBWgZqsRvR6KCpaNHlynENQ1BT - (Spent) 1AeWrpchzctn9B1MWLJ8AyiVF7QpBJjuXk - (Spent)	0.05075926 BTC 0.010563 BTC <div>0.06132226 BTC</div>
<div>6751057ac7c0a54ec965e0157593e2888838b95b23c6b531b4382ef2133c5171 (Fee: 0.0005 BTC - 74.74 sat/WU - 200.8 sat/B - Size: 249 bytes) 2018-09-26 21:05:05</div>			
3PmppghYYCT2PgBeh2pfxMZY2okR7xWPsG (0.78463281 BTC - Output)	➔	1Nzf8B1bfdDSyeamjqJp5dBQqmUp3yqRRk - (Spent) 35oWmhkJJEeZXkDN7ScN1ybiErz322UNX2 - (Spent)	0.0130186 BTC 0.77111421 BTC <div>0.78413281 BTC</div>

Blockchain.info transacción

BLOCKCHAIN

WALLET

DATA

API

ABOUT

Q BLOCK, HASH, TRANSACTION, ETC...

GET A FREE WALLET

Transaction View information about a bitcoin transaction

1418a96b847a38e3d04a2d5c2454e016f39977fe3a5f64cc741b569b36aca51e

18UyRSR4LhJ2KnYBErhmqBZHLnLvGniSGu



16L8RL4rzBWgZqsRvR6KCpaNHiynENQ1BT
1AeWrpchzctn9B1MWLJ8AyiVF7QpBJjuXk

0.05075926 BTC
0.010563 BTC

0.06132226 BTC

Summary

Size	225 (bytes)
Weight	900
Received Time	2018-09-26 21:07:41
Lock Time	Block: 543209
Included In Blocks	543210 (2018-09-26 21:08:29 + 1 minutes)
Confirmations	15897
Visualize	View Tree Chart

Inputs and Outputs

Total Input	0.06210959 BTC
Total Output	0.06132226 BTC
Fees	0.00078733 BTC
Fee per byte	349.924 sat/B
Fee per weight unit	87.481 sat/WU
Estimated BTC Transacted	0.010563 BTC
Scripts	Show scripts & coinbase