Blockchain

Estructura de Blockchain

Miguel González

2 de octubre de 2025

Estructura del bloque

Tamaño	Campo	Descripción
4 bytes	Tamaño del bloque	El tamaño del bloque, en bytes, después de este campo
80 bytes	Encabezado del bloque	Varios campos que forman el encabezado del bloque
1–9 bytes (VarInt)	Contador de transacciones	Cantidad de transacciones que siguen
Variable	Transacciones	Las transacciones registradas en este bloque

Cabecera del bloque

Tamaño	Campo	Descripción
4 bytes	Versión	Número de versión para rastrear actualizaciones del software/protocolo
32 bytes	Hash del bloque previo	Referencia al hash del bloque anterior (padre) en la cadena
32 bytes	Raíz de Merkle	Hash de la raíz del árbol de Merkle de las transacciones de este bloque
4 bytes	Marca de tiempo	Momento aproximado de creación del bloque (segundos desde la época Unix)
4 bytes	Objetivo de dificultad	Objetivo de dificultad del algoritmo Proof-of-Work para este bloque
4 bytes	Nonce	Contador usado por el algoritmo Proof-of-Work

Ejemplos de bloques

Portales:

- Blockchain.com
- BlockExplorer

Línea de comandos

Uso:

- `bitcoin-cli getblock <block>`
- `bitcoind -daemon -server=1`

Instalación:

- `brew install bitcoin`
- `brew install --cask bitcoin-core`

Bloque génesis

```
GEN=$(bitcoin-cli getblockhash 0)

bitcoin-cli getblock "$GEN" 2 | head -n 60

bitcoin-cli getblock "$GEN" 2 \
  | jq -r '.tx[0].vin[0].coinbase' \
  | xxd -r -p
```

Tipos de transacciones

Existen fundamentalmente dos tipos de transacciones en blockchain:

- Transacción *Coinbase*:
  - Primera transacción en cada bloque
  - No tiene un output previo
- Transacción estándar:
  - Tiene inputs normales referenciando UTXOs anteriores
  - Se mueven importes entre direcciones
  - No tiene privilegios especiales

Ejemplos

- Ejemplo de transacción
- Transacción especial

Estructura de transacción

Tamaño	Campo	Descripción
32 bytes	Hash de transacción	Puntero al **hash** de la transacción que contiene el UTXO a gastar
4 bytes	Índice de salida	Número de índice del UTXO a gastar (el primero es 0)
1–9 bytes (VarInt)	Tamaño del script de desbloqueo	Longitud en bytes del script de desbloqueo, que sigue a continuación
Variable	Script de desbloqueo	Script que satisface las condiciones del script de bloqueo del UTXO
4 bytes	Número de secuencia	Función de reemplazo de transacción (Tx-replacement), actualmente deshabilitada; suele fijarse en 0xFFFFFFFF

Transacción coinbase

Tamaño	Campo	Descripción
32 bytes	Hash de transacción	Todos los bits en cero → **no es** una referencia a un hash de transacción
4 bytes	Índice de salida	Todos los bits en uno → 0xFFFFFFFF
1–9 bytes (VarInt)	Tamaño de datos coinbase	Longitud de los datos coinbase (entre 2 y 100 bytes)
Variable	Datos coinbase	Datos arbitrarios, usados para **extra nonce** y etiquetas de minería. En bloques versión 2 o superior debe comenzar con la altura del bloque
4	Número	Fijado en 0xFFFFFFFF