

CRIPTO · SERIE 2 · PARTE 01 / 04

HASHRATE, DIFICULTAD Y ENERGÍA

Cómo se mide la potencia de la red, el algoritmo de ajuste de dificultad y sus límites, por qué los bloques llegan como un proceso de Poisson y qué dicen las cifras de consumo eléctrico, con su incertidumbre.

ÍNDICE

1	Resumen
2	El hashrate y cómo se estima
3	El algoritmo de ajuste
4	Los bloques llegan al azar
5	Consumo eléctrico
6	Lo que el vídeo simplifica
7	Referencias

1. RESUMEN

Bitcoin produce un bloque cada 10 minutos de media aunque la potencia de cálculo de la red se haya multiplicado por más de 10^{14} desde 2009. Lo consigue con un **ajuste de dificultad** cada 2.016 bloques que corrige el objetivo según el tiempo real empleado.

Este dossier:

- define el hashrate y muestra cómo se **estima**, ya que nadie lo mide directamente (§2);
- describe el algoritmo de ajuste y sus límites (§3);
- explica por qué los intervalos entre bloques siguen una distribución exponencial (§4);
- analiza el consumo eléctrico. Con unos 190 TWh/año y un hashrate de unos 1.025 EH/s, la eficiencia media implícita del parque de máquinas es de unos 21 J por billón de hashes (§5).

Con los datos del 16/10/2026, el tiempo medio por bloque que predicen la dificultad y el hash-rate es de 589 s, coherente con el objetivo de 600 s.

2. EL HASHRATE Y CÓMO SE ESTIMA

El **hashrate** es el número de evaluaciones de la doble SHA-256 por segundo que realiza el conjunto de los mineros. Se expresa con prefijos del Sistema Internacional:

PREFIJO	FACTOR	EJEMPLO
kH/s	10^3	
TH/s	10^{12}	una máquina de minar (ASIC) actual: del orden de cientos de TH/s
EH/s	10^{18}	la red: ≈ 1.025 EH/s (16/10/2026)

Nadie ve el hashrate de los demás: se **infiera** de los bloques. Si cada bloque requiere de media $2^{32}D$ intentos (dossier 4) y en un periodo de duración Δt se han encontrado n bloques,

$$\widehat{H} = \frac{n \cdot 2^{32} D}{\Delta t}. \quad (1)$$

Como n es una variable aleatoria (§4), la estimación tiene un error relativo de aproximadamente $1/\sqrt{n}$: con un día de datos ($n \approx 144$) ronda el 8 %, y por eso las cifras de hashrate «diario» fluctúan tanto. Con los datos del 16/10/2026 se puede comprobar la coherencia de (1):

$$\bar{t} = \frac{2^{32} D}{H} = \frac{4,295 \cdot 10^9 \times 1,4058 \cdot 10^{14}}{1,025 \cdot 10^{21}} \approx 589 \text{ s} \approx 9,8 \text{ min.} \quad (2)$$

2.1 LA COMPARACIÓN DEL VÍDEO

Mi minero de juguete hace unos $5 \cdot 10^5$ hashes/s. La red es $\approx 2,05 \cdot 10^{15}$ veces más rápida, y mi minero tardaría de media

$$\frac{6,04 \cdot 10^{23}}{5 \cdot 10^5 \text{ s}^{-1}} \approx 1,21 \cdot 10^{18} \text{ s} \approx 3,8 \cdot 10^{10} \text{ años,} \quad (3)$$

casi tres veces la edad del universo (unos $1,38 \cdot 10^{10}$ años). En sentido inverso: con la potencia actual y la dificultad de 2009 ($D = 1$), la red encontraría unos $2,4 \cdot 10^{11}$ bloques por segundo.

3. EL ALGORITMO DE AJUSTE

Cada 2.016 bloques, todos los nodos recalculan el objetivo con la misma regla [1][2]:

$$T_{\text{nuevo}} = T_{\text{viejo}} \cdot \frac{t_{\text{real}}}{2016 \times 600 \text{ s}}, \quad \frac{1}{4} \leq \frac{t_{\text{real}}}{1.209.600 \text{ s}} \leq 4, \quad (4)$$

donde t_{real} es el tiempo que separa las marcas de hora del primer y del último bloque del periodo. Como la dificultad es inversa al objetivo, $D_{\text{nuevo}} = D_{\text{viejo}} \cdot 1.209.600 / t_{\text{real}}$.

2.016 BLOQUES EN...	FACTOR DEL OBJETIVO	FACTOR DE LA DIFICULTAD
12 días	×0,857	×1,167
14 días	×1	×1
16 días	×1,143	×0,875
2 días	×0,25 (límite)	×4
70 días	×4 (límite)	×0,25

Detalles relevantes:

- **Es un control con retardo.** El ajuste corrige el periodo **anterior**. Si el hashrate sube de forma sostenida, los bloques salen durante un tiempo algo por debajo de 10 minutos.
- **Hay un error de uno.** El código original mide el tiempo entre el primer y el último bloque del periodo, es decir, 2.015 intervalos y no 2.016. El error es diminuto ($\approx 0,05\%$), pero está relacionado con el llamado ataque de **deformación temporal** (*time warp*), que manipula las marcas de hora en los límites de los periodos y que se ha estudiado en las propuestas de limpieza del consenso.

- El límite **x4** impide cambios bruscos de dificultad, por ejemplo por marcas de hora manipuladas.

4. LOS BLOQUES LLEGAN AL AZAR

Cada intento de cada minero es una prueba independiente con probabilidad diminuta p , y se hacen del orden de 10^{21} por segundo. En ese régimen (muchísimas pruebas, probabilidad ínfima), el número de bloques en un intervalo sigue una distribución de **Poisson** y el tiempo entre bloques, una **exponencial** de media $\mu = 10$ min:

$$P(\text{espera} > t) = e^{-t/\mu}. \quad (5)$$

ESPERA MAYOR QUE...	1 MIN	10 MIN	20 MIN	30 MIN	60 MIN
Probabilidad	90,5 %	36,8 %	13,5 %	5,0 %	0,25 %

Con unos 144 bloques al día, una espera de más de una hora ocurre aproximadamente una vez cada 3 días. Por la misma razón, el tiempo hasta 6 confirmaciones sigue una distribución de Erlang de media 60 minutos, y conseguir las 6 en menos de 30 minutos ocurre en torno al 8 % de las veces.

La propiedad de **falta de memoria** de la exponencial tiene una consecuencia curiosa (la *paradoja del tiempo de espera*): si llegas en un momento al azar, la espera media hasta el siguiente bloque sigue siendo de 10 minutos, aunque el último haya salido hace 9.

5. CONSUMO ELÉCTRICO

5.1 LAS CIFRAS

	ENERGÍA ANUAL	POTENCIA MEDIA
Bitcoin (estimación de Cambridge, dic. 2025) [3]	≈ 190 TWh	≈ 21,7 GW
España, demanda eléctrica 2025 (REE) [4]	256 TWh	≈ 29,2 GW

El cociente es $190/256 \approx 0,74$: unas tres cuartas partes de la demanda eléctrica española. Repartida entre unos 52.600 bloques al año, la energía por bloque es de unos **3,6 GWh**.

5.2 CÓMO SE ESTIMA

El consumo tampoco se mide: se **modela**. La potencia de la red es el hashrate por la eficiencia media de las máquinas:

$$P = H \cdot \varepsilon \implies \varepsilon = \frac{P}{H} \approx \frac{2,17 \cdot 10^{10} \text{ W}}{1,025 \cdot 10^9 \text{ TH/s}} \approx 21 \text{ J/TH.} \quad (6)$$

Una eficiencia media de unos 21 julios por billón de hashes es plausible para un parque que mezcla máquinas de varias generaciones (las más recientes están por debajo de esa cifra). El índice de Cambridge [3] da una **horquilla**: una cota inferior, en la que todos los mineros usarían las máquinas más eficientes, y una superior, con las menos eficientes que aún resultan rentables. El valor central es una estimación dentro de ella. Por eso las cifras de consumo hay que leerlas con su fecha y su margen.

5.3 EL DEBATE

Que la prueba de trabajo gaste energía no es un efecto secundario: es el mecanismo. El coste de reescribir la historia (dossier 4 de la serie 1) es precisamente el coste de igualar esa potencia. La discusión real es si ese nivel de seguridad compensa su coste ambiental, que depende de qué fuentes alimentan la minería. El dossier siguiente presenta la alternativa que eligió Ethereum.

6. LO QUE EL VÍDEO SIMPLIFICA

EN EL VÍDEO	CON PRECISIÓN
«Más de 30.000 millones de años»	$\approx 3,8 \cdot 10^{10}$ años con la dificultad del 16/10/2026
«Más de mil trillones»	$\approx 1,025 \cdot 10^{21}$ hashes/s, estimados a partir de los bloques
«Lo ajusta cada 2.016 bloques»	Con la regla (4), limitada a un factor 4 y con un retardo de un periodo
«Un bloque cada 10 minutos de media»	Intervalos exponenciales: hay esperas de más de una hora cada pocos días
«Tres cuartas partes de España»	Cociente de 0,74 sobre una estimación con horquilla

7. REFERENCIAS

- [1] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*, sección 4. 2008. <https://bitcoin.org/bitcoin.pdf>
- [2] Bitcoin Project. *Bitcoin Developer Guide: Proof of Work y ajuste de dificultad*. https://developer.bitcoin.org/devguide/block_chain.html
- [3] Cambridge Centre for Alternative Finance. *Cambridge Bitcoin Electricity Consumption Index*. <https://ccaf.io/cbnsi/cbeci> (dato de dic. 2025 citado por CoinTurk).
- [4] Red Eléctrica de España. *Datos de cierre del sistema eléctrico 2025*. <https://www.ree.es>
- [5] Hashrate y dificultad del 16/10/2026: pickaxe.io, [coinotag](https://coinotag.com) y [millionminer](https://millionminer.com) (ver la guía web).

[6] A. M. Antonopoulos, D. A. Harding. *Mastering Bitcoin*, 3.ª ed., cap. 12. O'Reilly, 2023.

Las cifras derivadas (tiempo medio, años, probabilidades, potencia y eficiencia) se han calculado con un script propio.