

CRIPTO · SERIE 1 · PARTE 04 / 04

LA PRUEBA DE TRABAJO

Minar como búsqueda de preimágenes parciales. La distribución de los intentos, la relación entre objetivo, dificultad y ceros, el espacio de búsqueda del minero y el análisis de Nakamoto de la probabilidad de reescribir la historia.

Complemento técnico de la guía «Así se mina un bloque»
<https://amstech.dev/guias/bitcoin-s1/04-asi-se-mina-un-bloque/>

@ams_tech

ÍNDICE

1 Resumen

2 El problema

3 La distribución de los intentos

4 Objetivo, dificultad y ceros

5 El espacio de búsqueda del minero

6 ¿Se puede reescribir la historia? El análisis de Nakamoto

7 Respuesta a la pregunta de la serie

8 Lo que el vídeo simplifica

9 Referencias

1. RESUMEN

La **prueba de trabajo** convierte la creación de cada bloque en un problema que solo se resuelve probando: encontrar una cabecera cuya doble SHA-256, leída como número, quede por debajo de un **objetivo**. Como SHA-256 se comporta como una función aleatoria (dossier 2), cada intento es una lotería independiente y el número de intentos sigue una distribución **geométrica**.

Este dossier:

- formaliza el problema y su distribución, y comprueba con un minero de juguete que obtener 4 ceros en 85.200 intentos (frente a una media de 65.536) es un resultado normal: ocurre el 27 % de las veces (§2-§3);
- relaciona objetivo, dificultad y ceros, y muestra que hoy hacen falta unos $6 \cdot 10^{23}$ intentos por bloque (§4);
- describe el espacio de búsqueda real de un minero (§5);
- reproduce el análisis de la sección 11 del whitepaper sobre la probabilidad de que un atacante reescriba la historia (§6). Es la respuesta a la pregunta que abría la serie.

2. EL PROBLEMA

Sea T el objetivo vigente. Un minero busca una cabecera B (dossier 3) tal que

$$\text{SHA256d}(B) < T, \tag{1}$$

interpretando la huella como un entero de 256 bits. Es una **preimagen parcial**: no se busca una huella concreta, sino una cualquiera de las T que están por debajo del objetivo. Si las huellas se comportan como valores uniformes e independientes en $[0, 2^{256})$, la probabilidad de acierto de cada intento es

$$p = \frac{T}{2^{256}}. \tag{2}$$

No se conoce ningún método para elegir cabeceras con más probabilidad de acierto que otras: el efecto avalancha (dossier 2) hace que la huella no dé ninguna pista. **Probar es la única estrategia**, y por eso el trabajo realizado se puede medir por el número de intentos.

3. LA DISTRIBUCIÓN DE LOS INTENTOS

El número de intentos N hasta el primer acierto sigue una distribución geométrica:

$$P(N > n) = (1 - p)^n \approx e^{-np}, \quad E[N] = \frac{1}{p}, \quad \text{mediana}(N) \approx \frac{\ln 2}{p}. \quad (3)$$

Dos consecuencias poco intuitivas:

- **No hay memoria.** Haber probado un millón de valores sin éxito no acerca el siguiente acierto: $P(N > n + m \mid N > n) = P(N > m)$.
- **La mediana es menor que la media.** La mitad de las veces se acierta antes del 69 % de la media; a cambio, a veces hacen falta muchos más intentos.

3.1 EL MINERO DE JUGUETE

El minero del vídeo busca "hola" + nonce con SHA256 simple cuya huella empiece por cuatro ceros hexadecimales, así que $p = 16^{-4} = 1/65.536$:

```
hola85199 → 0000755d0fcdda53afe92ecf435286b802fe63872fd881f086aba589783df83b
85.200 intentos
```

MEDIDA	VALOR
Media teórica $1/p$	65.536
Mediana teórica $\ln 2/p$	≈ 45.426
Observado	85.200
$P(N > 85.200) = (1 - 1/65.536)^{85.200}$	$\approx 0,27$

Necesitar más de 85.200 intentos ocurre aproximadamente **1 de cada 4 veces**: el resultado es compatible con el modelo. Los primeros aciertos con 1, 2 y 3 ceros llegaron en los nonces 12, 192 y 563, también dentro de lo esperable para medias de 16, 256 y 4.096.

4. OBJETIVO, DIFICULTAD Y CEROS

El objetivo se codifica en el campo `bits` (dossier 3). Con el objetivo máximo $T_{\max} = 0xffff \cdot 2^{208}$ y la dificultad $D = T_{\max}/T$, el número medio de intentos por bloque es

$$E[N] = \frac{2^{256}}{T} = \frac{2^{256}}{T_{\max}} D = \frac{2^{48}}{0xffff} D \approx 2^{32} D. \quad (4)$$

Los ceros hexadecimales iniciales exigidos son, aproximadamente, $\log_{16}(2^{256}/T) = (32 + \log_2 D)/4$:

MOMENTO	DIFICULTAD D	CEROS	INTENTOS MEDIOS POR BLOQUE
2009	1	8,00	$\approx 4,3 \cdot 10^9$
16/10/2026	$1,4058 \cdot 10^{14}$	19,75	$\approx 6,04 \cdot 10^{23}$

Hoy, por tanto, la huella necesita 19 ceros y «tres cuartos» del siguiente. Cada cero hexadecimal adicional multiplica el trabajo por 16, y cada bit, por 2.

5. EL ESPACIO DE BÚSQUEDA DEL MINERO

El nonce tiene 32 bits: $2^{32} \approx 4.300$ millones de valores. Una máquina de minar actual (un **ASIC**, un chip diseñado solo para calcular SHA-256) los recorre en mucho menos de un segundo. Cuando se agotan, el minero cambia otro campo para obtener cabeceras nuevas:

1. **extraNonce** : un contador dentro de la transacción coinbase. Cambiarlo cambia la raíz de Merkle, y con ella toda la cabecera. Recalcular la raíz solo exige actualizar el camino de la coinbase: $\lceil \log_2 n \rceil$ huellas.
2. **time** : dentro de las reglas de validez (dossier 3), puede avanzarse segundo a segundo.
3. **version** : algunos bits pueden usarse como espacio adicional (la técnica conocida como *version rolling*, BIP 320).

Además, como explica el dossier 2, la cabecera ocupa dos bloques de SHA-256 y el primero no depende del nonce. Los mineros calculan su estado intermedio (**midstate**) una vez y evalúan solo dos compresiones por intento.

Los mineros rara vez trabajan solos. En un **pool**, cada participante busca soluciones a un objetivo mucho más fácil (*shares*) que demuestran su trabajo, y el premio de los bloques reales se reparte en proporción. La varianza de cada minero baja enormemente; la esperanza no cambia.

6. ¿SE PUEDE REESCRIBIR LA HISTORIA? EL ANÁLISIS DE NAKAMOTO

6.1 EL MODELO

La sección 11 del whitepaper [1] modela una carrera entre la red honesta, con una fracción p de la potencia de cálculo, y un atacante, con $q = 1 - p$. El atacante quiere sustituir un bloque que ya tiene z bloques encima: necesita rehacerlo, rehacer los z siguientes y adelantar a la red, que sigue añadiendo bloques.

Si el atacante va k bloques por detrás, la probabilidad de que llegue a alcanzar a la red es la de un **paseo aleatorio** con deriva en su contra (el problema de la ruina del jugador):

$$q_k = \begin{cases} 1 & \text{si } p \leq q \\ (q/p)^k & \text{si } p > q \end{cases} \quad (5)$$

Mientras la red produce sus z bloques, el progreso del atacante sigue aproximadamente una distribución de Poisson de media $\lambda = z q/p$. Combinando ambas:

$$P(\text{éxito}) = 1 - \sum_{k=0}^z \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - \left(\frac{q}{p} \right)^{z-k} \right). \quad (6)$$

6.2 RESULTADOS

Evaluando (6) con un script propio se reproducen exactamente las tablas del whitepaper:

z	0	1	2	3	4	5	6	10
$q = 0,10$	1	0,2046	0,0510	0,0132	0,0035	0,00091	0,00024	0,0000012
$q = 0,30$	1	0,6277	0,4457	0,3246	0,2391	0,1774	0,1321	0,0417

Confirmaciones necesarias para que la probabilidad de éxito baje del 0,1 %:

Q	0,10	0,15	0,20	0,25	0,30	0,35	0,40	0,45
z	5	8	11	15	24	41	89	340

La probabilidad **cae exponencialmente** con z mientras el atacante tenga menos de la mitad de la potencia, y crece sin límite al acercarse q a 0,5. Con $q \geq 0,5$ la ecuación (5) da $q_k = 1$: el atacante acaba alcanzando a la red tarde o temprano. Es el **ataque del 51 %**. De aquí sale la práctica de esperar **6 confirmaciones** (≈ 1 hora) en pagos importantes.

6.3 MATICES POSTERIORES

El modelo de Poisson de (6) es una aproximación. Rosenfeld [2] y Grunspan y Pérez-Marco [3] calcularon la probabilidad exacta con una distribución binomial negativa y obtuvieron valores algo mayores que los de Nakamoto para z pequeño. La conclusión cualitativa se mantiene: decrecimiento exponencial con z si $q < 1/2$.

7. RESPUESTA A LA PREGUNTA DE LA SERIE

¿Qué impide falsificar la cadena si recalcular huellas es facilísimo (dossier 1)? Que los nodos no aceptan cualquier cadena bien enlazada, sino **la válida con más trabajo acumulado**. Cada bloque cuesta hoy unos $6 \cdot 10^{23}$ intentos de media, y la red produce uno cada 10 minu-

tos. Reescribir un bloque con z confirmaciones exige rehacer $z + 1$ bloques de ese coste **más deprisa que todo el resto de la red**: con menos de la mitad de la potencia, la probabilidad de lograrlo es (6) y decrece exponencialmente.

8. LO QUE EL VÍDEO SIMPLIFICA

EN EL VÍDEO	CON PRECISIÓN
«Probar números hasta dar con uno que sirva»	Variar nonce, <code>extraNonce</code> , hora y bits de versión (§5)
«Cada cero lo hace 16 veces más difícil»	Exacto para ceros hexadecimales; la dificultad real varía de forma continua (§4)
«Hoy pide 19 ceros»	19,75 de media (16/10/2026): 19 ceros y algo más
«Más rápido que toda la red»	Con más del 50 % de la potencia; con menos, la probabilidad viene dada por (6)
Minero de juguete	SHA-256 simple sobre texto; Bitcoin usa SHA256d sobre la cabecera binaria

9. REFERENCIAS

- [1] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*, secciones 4 y 11. 2008. <https://bitcoin.org/bitcoin.pdf>
- [2] M. Rosenfeld. «Analysis of Hashrate-Based Double Spending». arXiv:1402.2009, 2014.
- [3] C. Grunspan, R. Pérez-Marco. «Double Spend Races». *International Journal of Theoretical and Applied Finance*, 21(8), 2018. arXiv:1702.02867.
- [4] Bitcoin Project. *Bitcoin Developer Reference: Block Chain (target, nBits, difficulty)*. https://developer.bitcoin.org/reference/block_chain.html
- [5] BIP 320. *nVersion bits for general purpose use*. <https://github.com/bitcoin/bips/blob/master/bip-0320.mediawiki>
- [6] A. Narayanan et al. *Bitcoin and Cryptocurrency Technologies*, cap. 5. Princeton University Press, 2016.
- [7] Dificultad del 16/10/2026: pickaxe.io y coinotag (ver la guía web).

El minero, las probabilidades de §3, los ceros de §4 y las tablas de §6 se han calculado con scripts propios. Las tablas de §6 coinciden con las del whitepaper.