UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

ciie
Centro de Investigación
e Innovación Educativa

Minería de Bitcoin

5.1 ¿Qué hacen los mineros de Bitcoin?

Recapitulemos lo que ya sabemos de los mineros

En Bitcoin dependemos de los mineros para:

- Almacenen la base de datos de Bitcoin (blockchain) completa y que además puedan transmitir su data.
- Validen las transacciones en conjunto con los Nodos Completos (Full Node)
- Propongan nuevos bloques candidatos de acuerdo a las reglas del consenso proporcionalmente a su poder de cómputo (hash power)

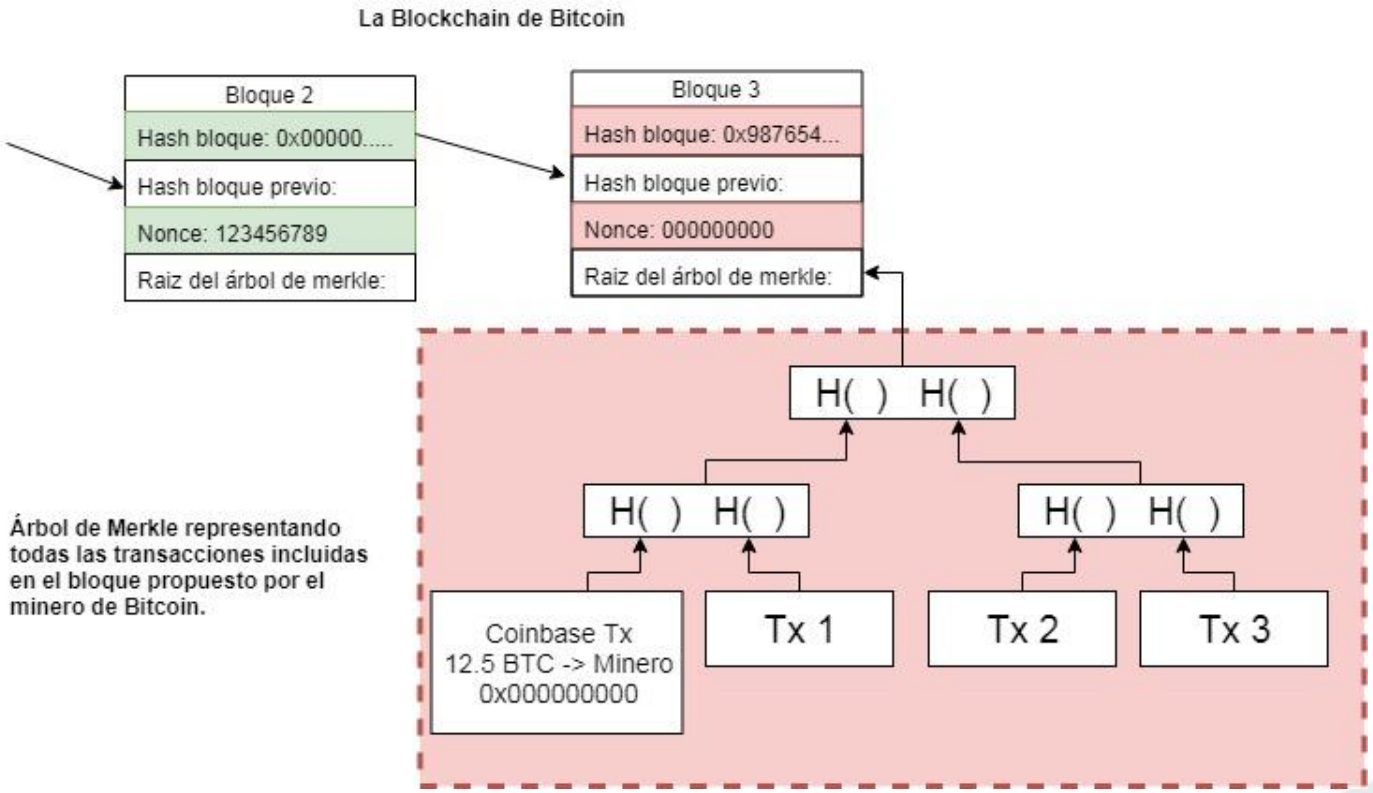
Lo más importante: ¿Quienes son los mineros?

La tarea de los Mineros de Bitcoin

1. Unirse a la red para recibir y propagar nuevas transacciones.
   - Validar cada una de las transacciones con las reglas del consenso
2. Recibir y propagar nuevos bloques, y mantener una copia fiel de la blockchain
   - Validar los nuevos bloques con las reglas del consenso
3. Construir un nuevo bloque candidato.
   -Eso quiere decir que todas las Tx incluidas deben ser válidas
4. Encontrar el Nonce (número usado una sola vez) que hace que el bloque sea válido.
5. Propagar el bloque en la red y esperar que los demás nodos lo acepten como válido.
6. 100 Bloques después, tomar ganancia de los Bitcoins creados.

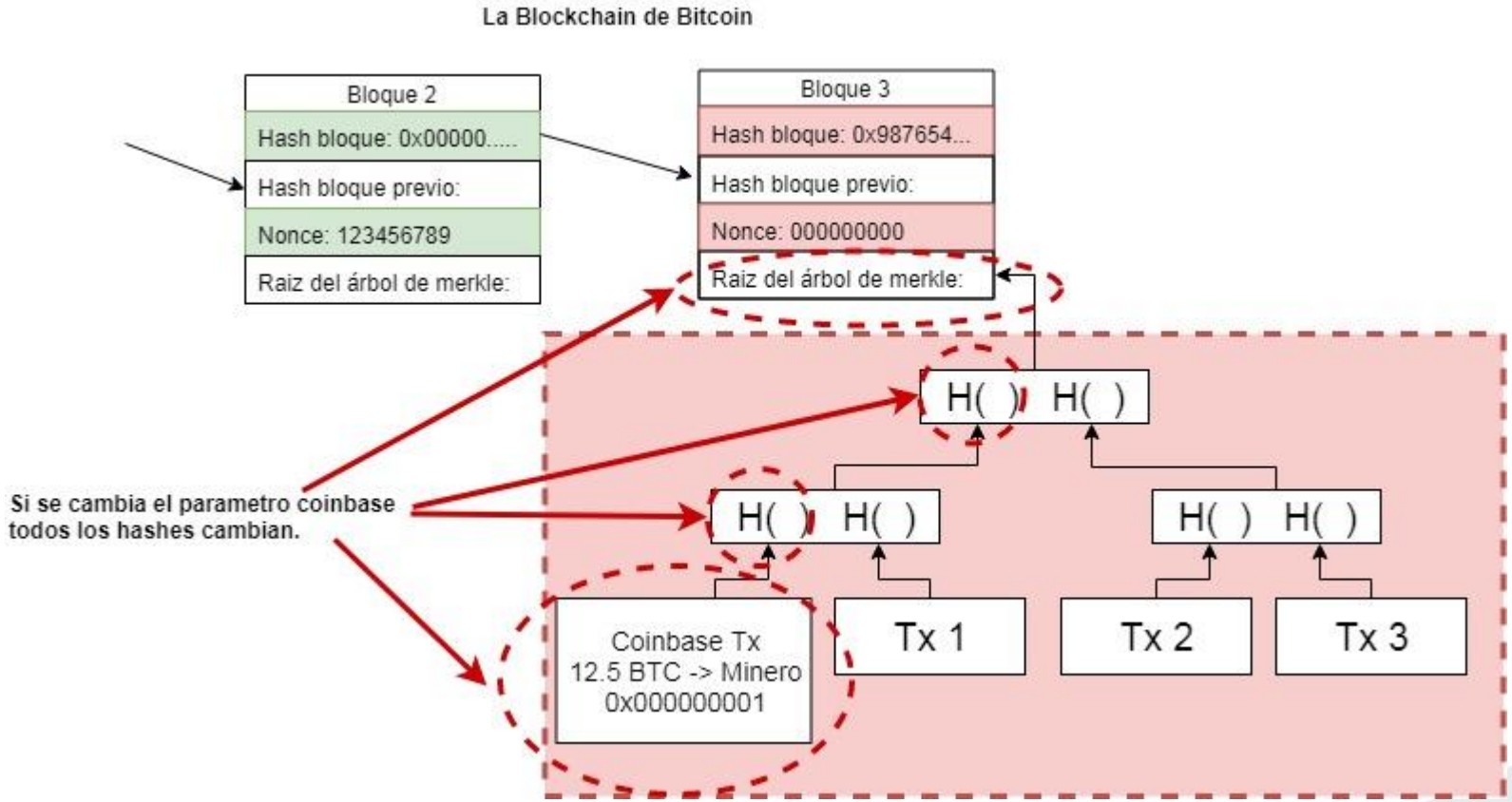
¿Cómo encontrar un bloque válido?

El minero intenta un número, en este caso todos 0s. No produce una salida de hash válida, por lo que el minero procederá a probar un número diferente.



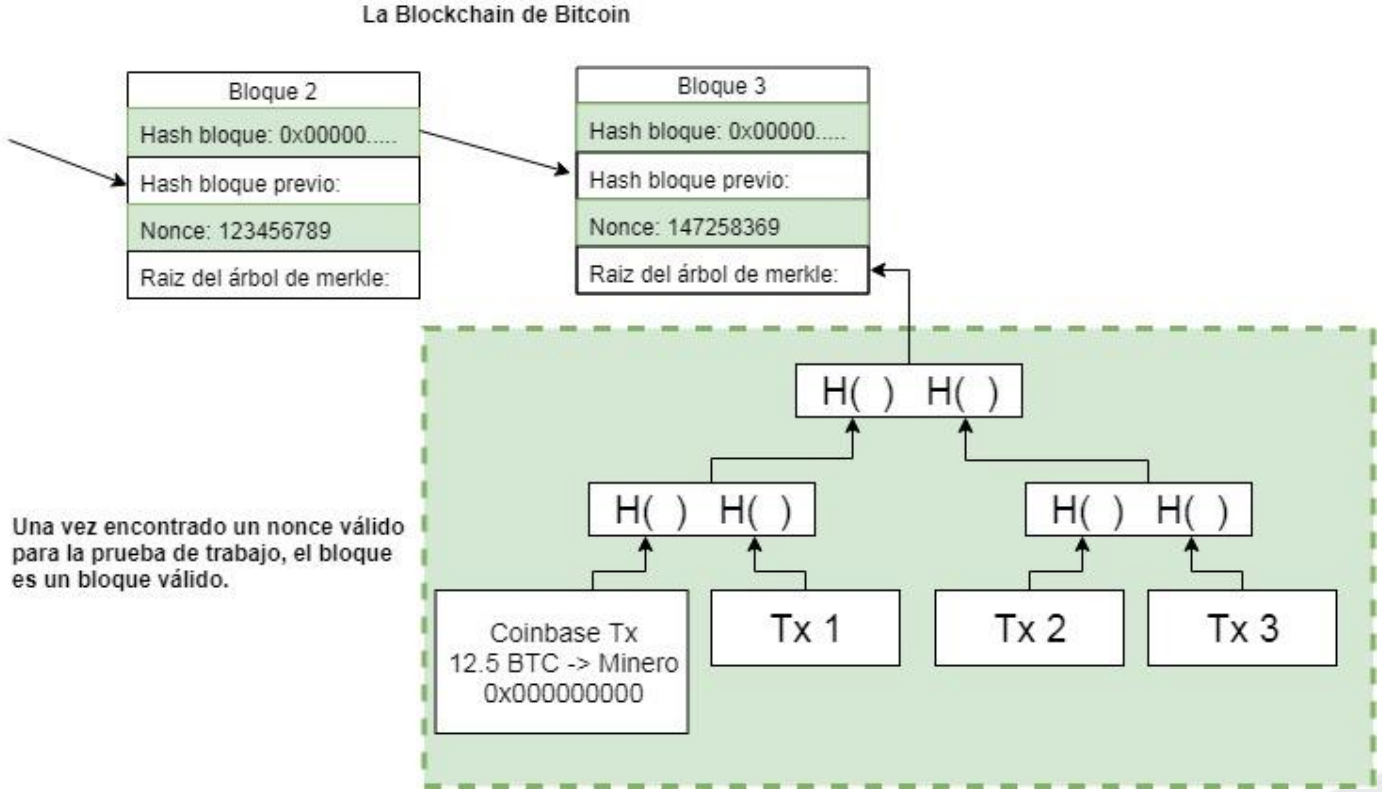
¿Cómo encontrar un bloque válido?

Cambiar un número en la transacción de coinbase se propaga hasta la raíz del árbol de Merkle.



¿Cómo encontrar un bloque válido?

Una vez encontrado el número que hace que el bloque sea uno válido satisfaciendo la condición de prueba de trabajo, el hash identificador del bloque empieza con una cantidad significante de 0s.



Dificultad, nBits y el objetivo (target)

¿Qué tan difícil es encontrar un nuevo bloque válido?

- Dificultad

La dificultad es una medida de lo difícil que es encontrar un hash por debajo de un objetivo determinado. La red de Bitcoin tiene una dificultad de bloque global.

La dificultad en mayo 2019 es: 6,702,169,884,349.17

- Objetivo (target)

El objetivo es un número de 256 bits que todos los clientes de Bitcoin comparten. El hash SHA-256 del encabezado de un bloque debe ser inferior o igual al objetivo actual para que la red acepte el bloque. Cuanto menor sea el objetivo, más difícil será generar un bloque.

- Bits

Cada bloque almacena una representación empaquetada (llamado "Bits") para su objetivo hexadecimal real. El objetivo se puede derivar de él a través de una fórmula predefinida.

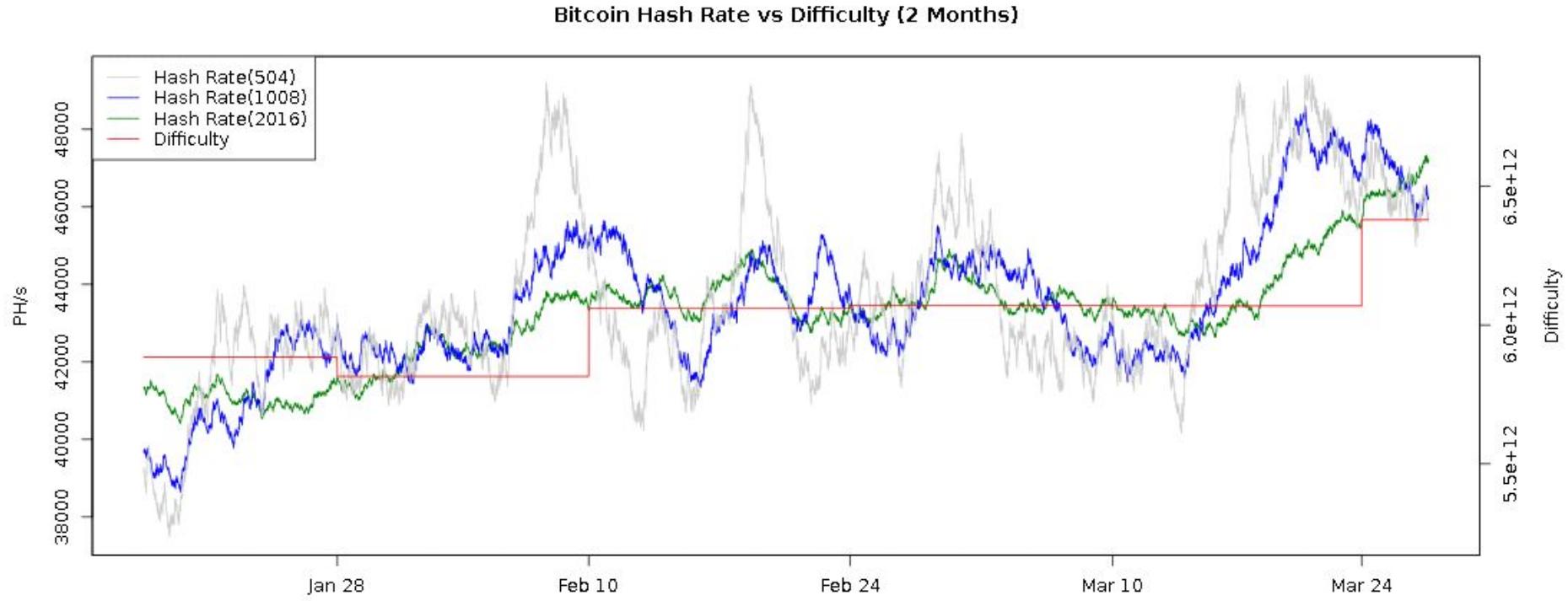
Actualización de la dificultad

Cada 2016 bloques (aproximadamente 2 semanas) la dificultad se ajusta de forma que el tiempo de los bloques se mantenga constante (10 min)

$$Prox\_dificultad = (Prev\_dificultad)*(2016*10min)/(tiempo\ de\ los\ últimos\ 2016\ bloques)$$

Dificultad de Bitcoin ajustada en el tiempo

En la web https://bitcoinwisdom.com/bitcoin/difficulty , nos muestra un gráfico del Hash Rate (poder de computo) vs La dificultad de la red.



Tiempo de emisión de bloques Bitcoin

En la web https://bitcoinwisdom.com/bitcoin/difficulty , nos muestra un gráfico del tiempo de emisión de un bloque en el tiempo.