Minería

- El minado es una validación de las transacciones.
- Por este esfuerzo, los mineros obtienen dinero como recompensa.
- Esta recompensa disminuye las tarifas, creando un incentivo complementario para contribuir al poder de procesamiento de la red.

Progreso de la minería

- Creación máquinas especializadas como FPGAs y ASICs.
- Carrera por construir máquinas más baratas y eficientes
- Incremento en el número de mineros aumenta complejidad de la generación de hashes
- Mineros invierten grandes cantidades de dinero en máquinas especializadas.

Recompensas

- El sistema se sostiene gracias a recompensas. Las transacciones y los bloques dan recompensas.
- Los mineros dedican potencia de ordenadores a crear bloques a cambio de la posibilidad de ganar dinero
- Para este minado se necesita cada vez más potencia de computación

El reto

El sistema de Bitcoin intenta crear bloques de forma regular cada diez minutos aproximadamente. Para ello, se establece un reto de dificultad que debe ser resuelto mediante criptografía. Esta criptografía consiste en generar un código hash específico mediante información del bloque actual y del bloque anterior.

Esta tarea es relativamente fácil en sí misma, y para **aumentar la dificultad** se requiere que el hash cumpla con una condición previamente establecida. Esto se consigue aumentando el número de pruebas necesarias hasta encontrar un hash válido. Para adaptar la dificultad según el aumento de la potencia de los ordenadores, se ajusta la condición del hash a una más exigente. El parámetro que hay que variar para conseguir el hash válido se conoce como nonce.

Crear el hash

- Este hash se genera a partir de información del bloque actual, y del anterior
- Cada hash identifica un bloque, y se calcula con el hash del bloque anterior.
- Crear un código hash requiere muy poco tiempo
- Para complicar la tarea, se pone una condición que el hash debe cumplir
- Se tienen que hacer muchas pruebas hasta hallar un hash válido
- Este cálculo es más rápido a medida que la potencia de los ordenadores aumenta
- Por ello, la dificultad se va ajustando poniendo una condición más estricta
- El **nonce** es el parámetro que hay que variar hasta conseguir un hash válido.

Videos interesantes

- http://www.youtube.com/watch?v=44D9nVxqGIE
- http://www.youtube.com/watch?v=YBNr69vrscw