UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

ciie
Centro de Investigación
e Innovación Educativa

Minería de Bitcoin

5.2 Evolución del hardware de minería

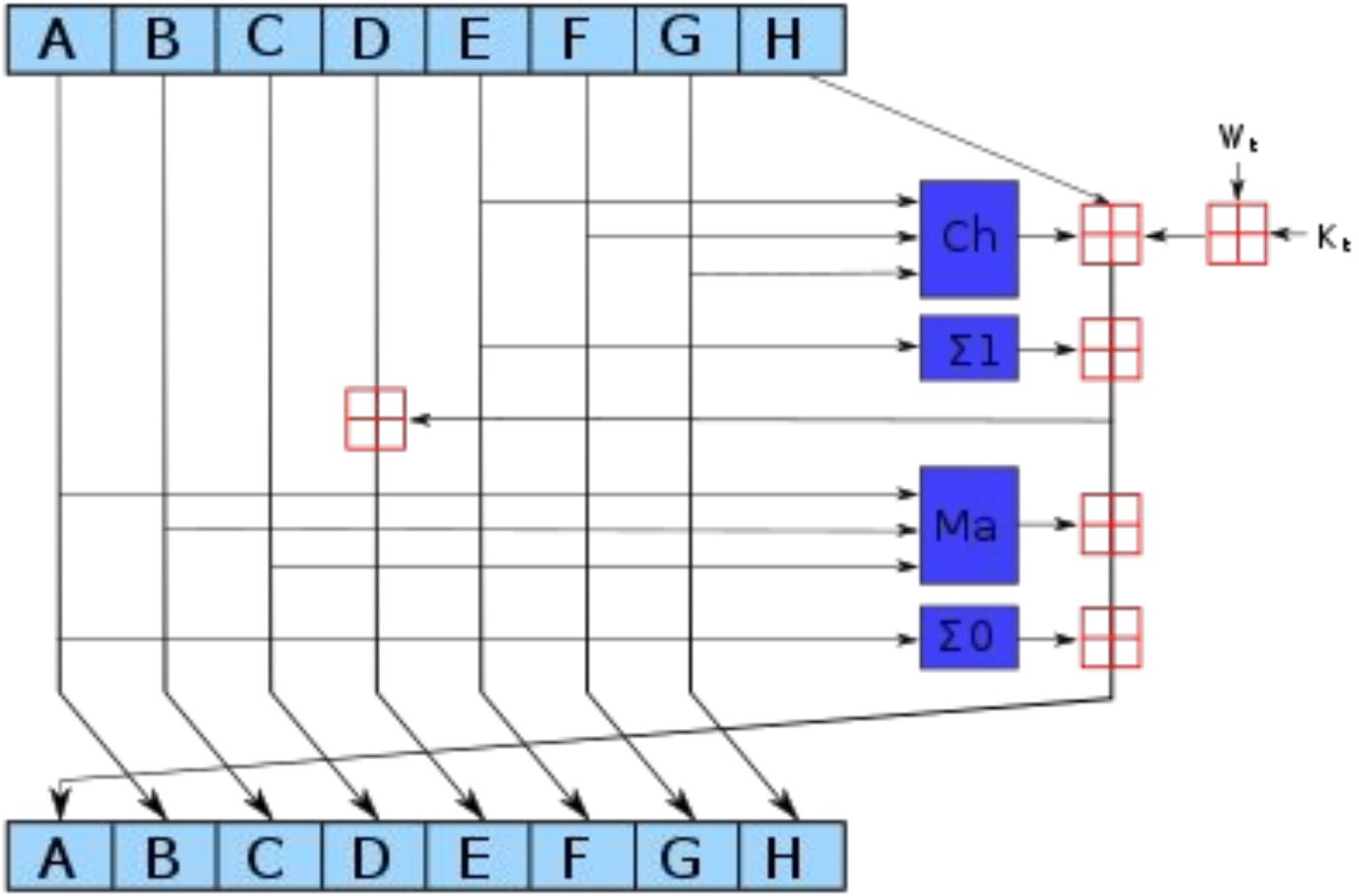
Función hash SHA-256

La familia de funciones hash, es una familia de funciones de uso general. Se agrupan como SHA-1; SHA-2; SHA-3

- Fueron creadas por la NSA (National Security Agency)
- SHA-2 fue publicada en el 2001.
- Hasta el día de la fecha se mantienen seguras criptográficamente
  - Se conoce que existen colisiones.
- Bitcoin es un software en desarrollo y entonces puede ser actualizado y modificado en el caso de encontrar vulnerabilidades.

La función SHA-256 en detalle

Una iteración en una función de compresión de la familia SHA-2



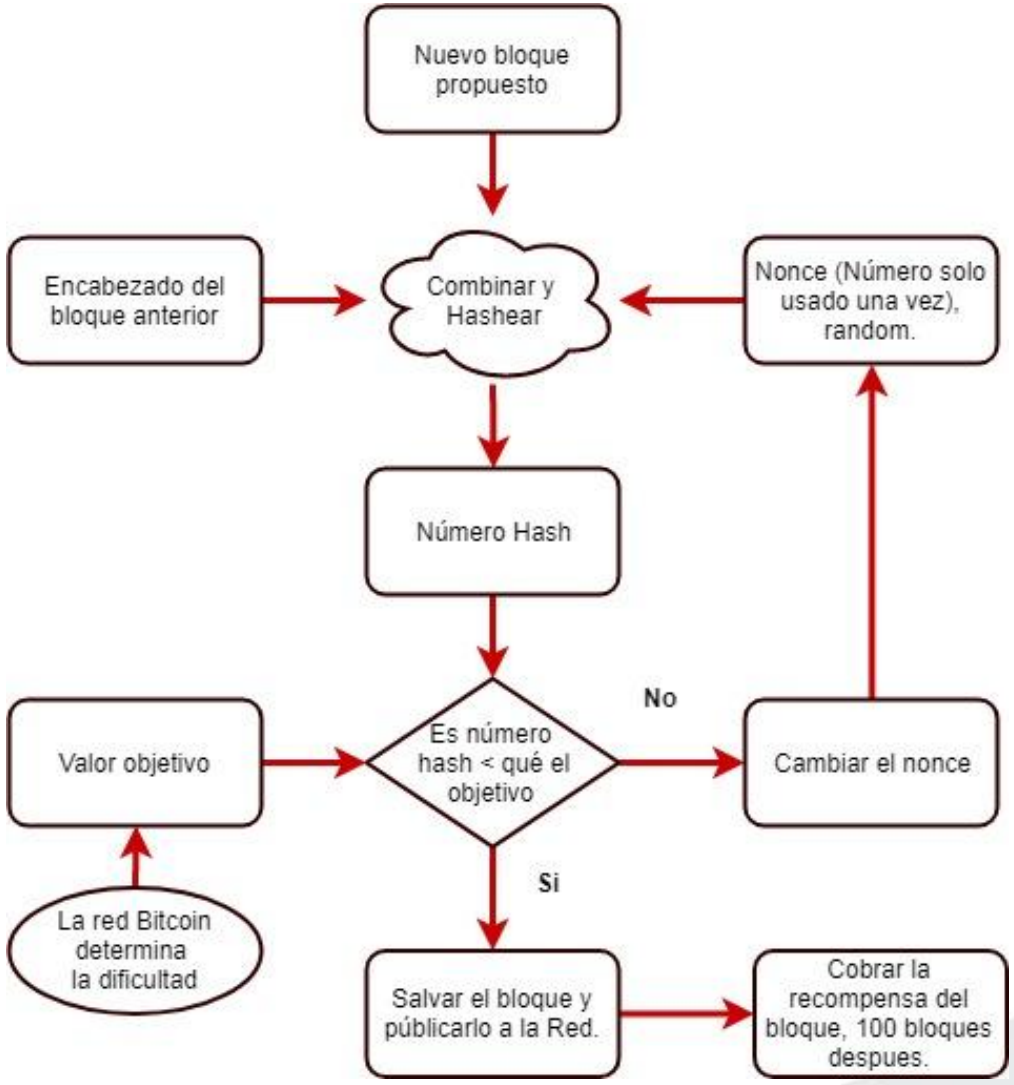
Pseudo Código de Minería

La primera generación de minería se realizó en computadoras de propósito general, es decir, unidades centrales de procesamiento general (CPU).

```
TARGET = (65535 << 208) / DIFFICULTY;
coinbase_nonce = 0;
while (1) {
  header = makeBlockHeader(transactions, coinbase_nonce);
  for (header_nonce = 0; header_nonce < (1 << 32); header_nonce++){
    if (SHA256(SHA256(makeBlock(header, header_nonce))) <
    TARGET)
        break; //block found!
    }
    coinbase_nonce++;
}
```

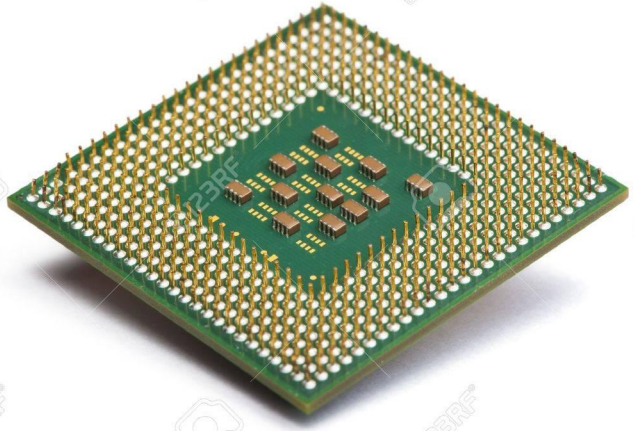
Pseudo Código de Minería - Flowchart

Es una representación usando diagramas de bloques del código anterior.



Minería 1era. Generación - CPU

- Todas las computadoras tienen una CPU.
- Fueron utilizadas para la primera minería de Bitcoin en 2009.
- Si se intenta minar en una PC genérica hoy, la minería de CPU ya no es rentable con la dificultad actual. Eso quiere decir que se gasta más energía que lo que se puede obtener de redito.



Minería 2da. Generación - GPU

La segunda generación comenzó cuando la gente comenzó se dio cuenta de la lentitud de la CPU para hacer minería y, en su lugar, usó su tarjeta gráfica o unidad de procesamiento de gráficos (GPU).

Minería 2da. Generación - GPU

- Las GPUs fueron diseñadas para rendimientos altos en el procesamiento de gráficos.
  - Cómputos en paralelo
  - Alto rendimiento
- Fueron utilizadas por primera vez en el año 2010
- Se encuentran disponibles en stock y son fáciles de armar.
- Se pueden controlar todo el rig de minería desde 1 CPU
- Se pueden overclockear.

Minería 2da. Generación - GPU

- Pobre utilización del Hardware.
- Pobre ventilación.
- Alto consumo eléctrico.
- Se necesitan racks diseñados para mejorar la ventilación.

Minería 3era. Generación - FPGA

Algunos mineros comenzaron a cambiar de GPU a FPGA (Field Programable Gate Array) o Matriz de compuertas programables. La razón general detrás de los FPGA es tratar de acercarse lo más posible al rendimiento del hardware personalizado y, al mismo tiempo, permitir que el propietario de la tarjeta la personalice o la reconfigure "en funcionamiento".

Minería 3era. Generación - FPGA

- Tienen más performance que las GPUs
- Fueron utilizadas por primera vez en el año 2011
- Tienen mejores sistemas de refrigeración.
- Se pueden customizar sus operaciones.
- Se pueden optimizar.

Minería 3era. Generación - FPGA

- Consumen más electricidad que las GPUs.
- Se necesita una expertise para setearlas.
- Más costosas que las GPUs.
- Tienen una ganancia marginal por sobre encima de las GPUs.

Minería 4ta. Generación - ASICs

En la actualidad, la minería está dominada por los ASIC (Application Specific Integrated Circuit) de Bitcoin o circuitos integrados para aplicaciones específicas. Estos son chips que fueron diseñados, construidos y optimizados para el único propósito de minar Bitcoin.

Minería 4ta. Generación - ASICs

- Son solamente diseñados para minar Bitcoin.
  - Ya estamos en los límites de diseño de microchips.
  - Solamente se van a poder mejorar (con suerte) un x10 veces
- Diseñadas para funcionar 24x7x365
- Requiere una especialización para su utilización.
- Son los chips más rápidos diseñados con un propósito.

Minería 4ta. Generación - ASICs

- La mayoría de los ASICs se vuelven obsoletos después de 6 meses - Esto se debe a que no pueden competir en eficiencia con el nuevo hardware
- Como hay pocos fabricantes de ASICs, hay demoras en los envíos y eso hace que los clientes no puedan planificar.
- La mayoría de las compañías tienen un pro-order, pero utilizan ellos mismos el hardware las primeras semanas.

Comparación de Bitcoin Vs Oro

Podemos ver un claro paralelo entre la evolución de la minería de Bitcoin y la evolución de la minería de oro. Ambos fueron inicialmente llevados a cabo por personas y con el tiempo se convirtieron en operaciones masivas controladas por grandes compañías.

CPU (2009-2010)

GPU (2010-2011)

FGPA (2011-2013)

ASIC (2013-2019)

Bateo (≈1850)

Esclusa de oro(≈1880)

Mezcla de oro(≈1900)

Minería a cielo abierto(≈1950)

Xinjiang – China

- Aproximadamente 200 Mwatts de consumo energético

Quebec - Canadá

- Aproximadamente 150 Mwatts de consumo energético