Laboratorio BlockChain – Información Seguridad y Privacidad

Santiago Rodriguez – 202011182 ; Diego Rodriguez – 201923986
Universidad de los Andes, 2023
MINE 4204

Link Repositorio Git Hub : https://github.com/SantiagoRodriguezBernal/Tarea-4-Blockchain.git

1. **¿Qué algoritmo usa el programa para manejo de códigos criptográficos de hash?**

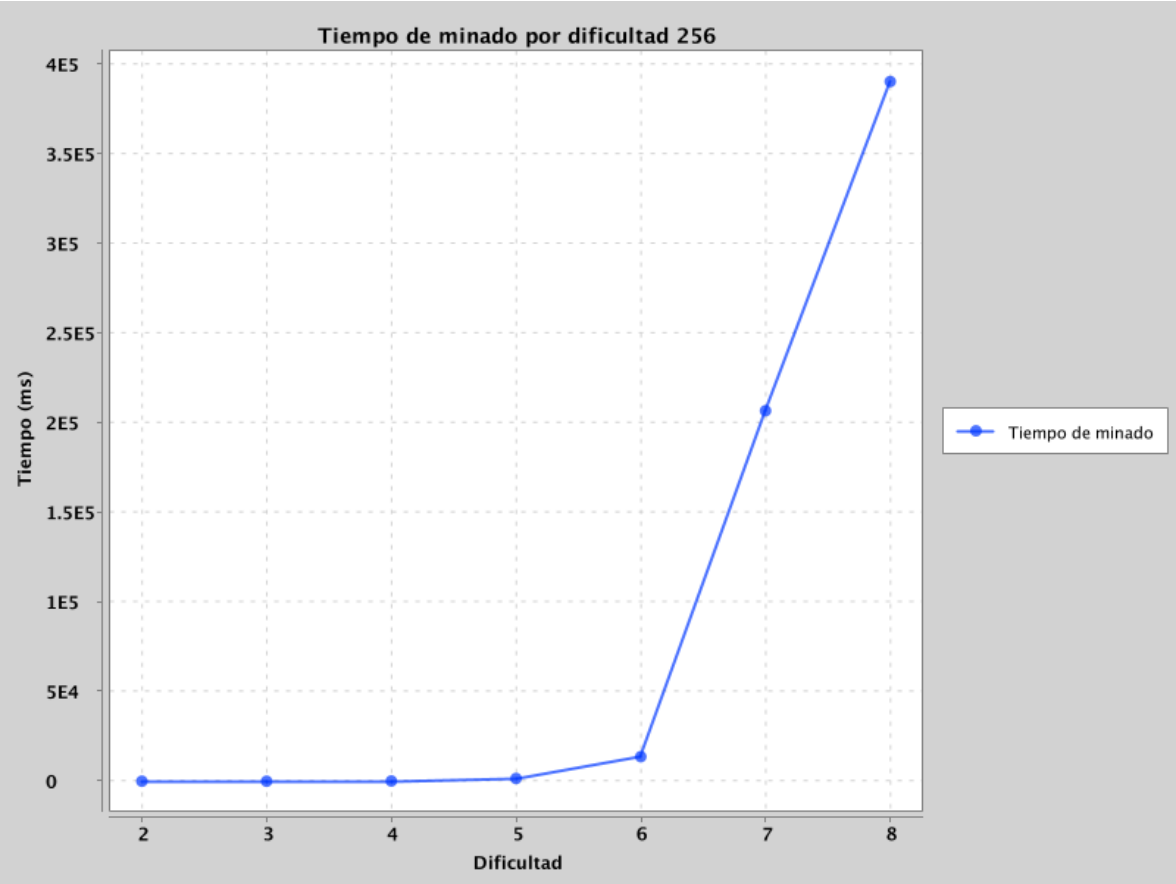
   El algoritmo de hash usado es SHA 256 (Secure Hash Algorithm 256 bits).

2. **¿Qué representa la variable dificultad?**

   La variable `dificultad` se utiliza para controlar el nivel de dificultad con el que se están minando los bloques en la cadena. En concreto se utiliza en el método `minarBloque` de la clase Bloque para ajustar la dificultad de minado. Este valor controla cuántos ceros se deben encontrar al principio del hash para que un bloque se considere minado, entre más ceros al inicio existan mayor será el tiempo que tome minar un bloque, pues, requerirá mayor potencia al tener una mayor dificultad.

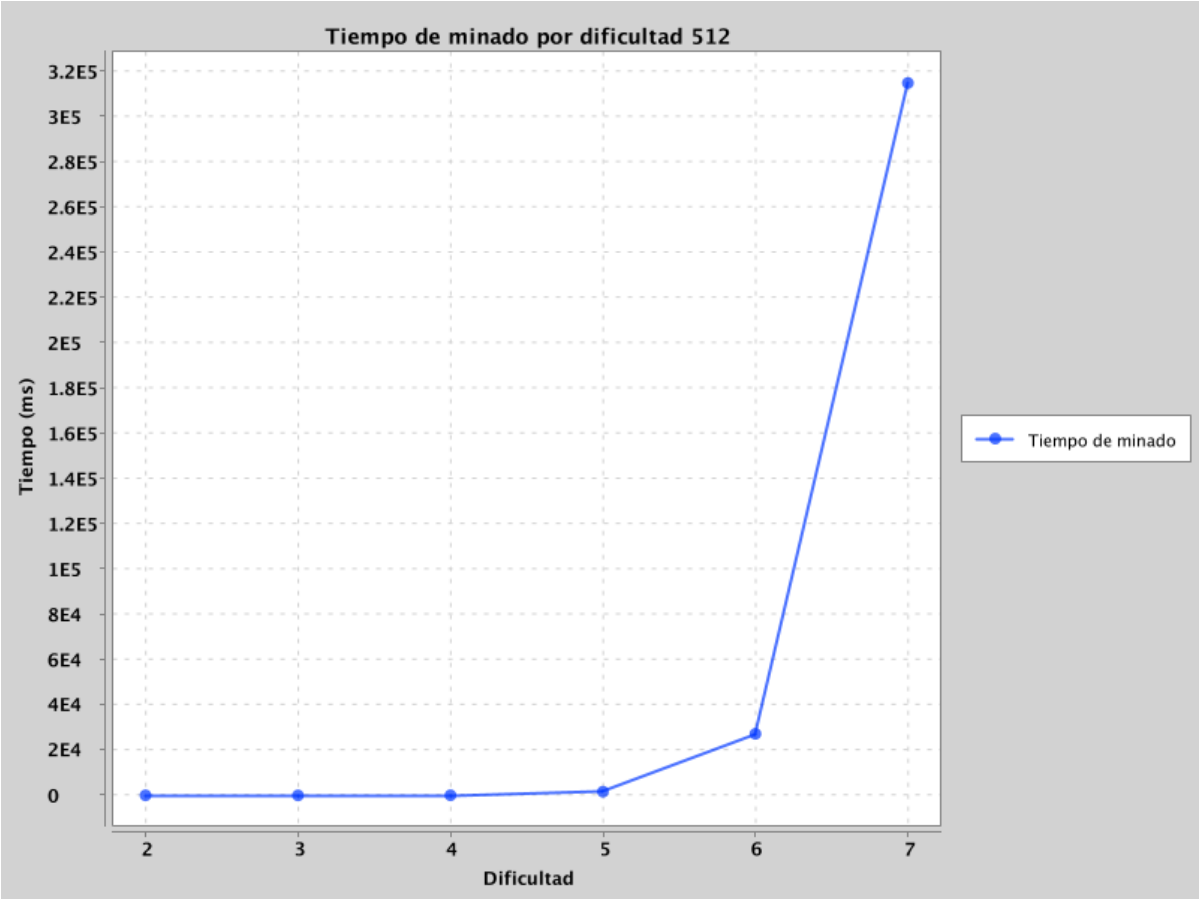
3. **Cree una tabla que muestre el cambio en el tiempo necesario para minar usando las siguientes dificultades: 2, 3, 4, 5, 6, 7, 8. Cree una gráfica que ilustre el incremento.**

Dificultad	Tiempo Promedio (ms)	Tiempo Promedio (s)
2	**31**	**0.031**
3	**18**	**0.018**
4	**142**	**0.142**
5	**1547**	**1.547**
6	**13722**	**13.722**
7	**206756**	**206.756**
8	**390475**	**390.475**



4. **Cambie el algoritmo de generación de códigos de hash por "SHA-512" y cree una tabla que muestre el cambio en el tiempo necesario para minar usando las siguientes dificultades: 2, 3, 4, 5, 6, 7, 8. Cree una gráfica que ilustre el incremento.**

Dificultad	Tiempo Promedio (ms)	Tiempo Promedio (s)
2	**42**	**0.042**
3	**13**	**0.013**
4	**64**	**0.064**
5	**1642**	**1.642**
6	**27229**	**27.229**
7	**314939**	**314.939**



5. ¿Qué representa este incremento, para las garantías de seguridad que ofrece la tecnología blockchain?

Los tiempos tienen cambios significantes al variar dos parámetros. Uno la dificultad, y el segundo el algoritmo de cifrado, estos incrementos son fundamentales para la seguridad del sistema. En cuanto al aumento en la dificultad esto implica que los mineros deben aportar más trabajo computacional a la red para encontrar un hash válido que cumpla con los requisitos de dificultad establecidos y así valide un bloque. Esto fortalece la seguridad de la red, ya que vuelve más costoso y difícil para un atacante generar bloques falsos o realizar modificaciones no autorizadas en la cadena. Por otro lado, el cambio de SHA-256 a SHA-512 implica un incremento en la longitud del hash lo que a su vez implica más operaciones y tiempo para calcular cada hash debido a que SHA 512 presenta 512 bits en lugar de 256 bits, lo que también implica un requerimiento de más recursos computacionales. Debido a esto la única manera de que un atacante pueda atacar la red y realizar modificaciones en ella seria que tuviera mas del 50% de todo el poder computacional, lo cual es absurdo, pues actualmente en redes como Bitcoin que ya son bastantes extensas, estos procesos de minería se hacen a través de grupos mineros en todo el mundo.