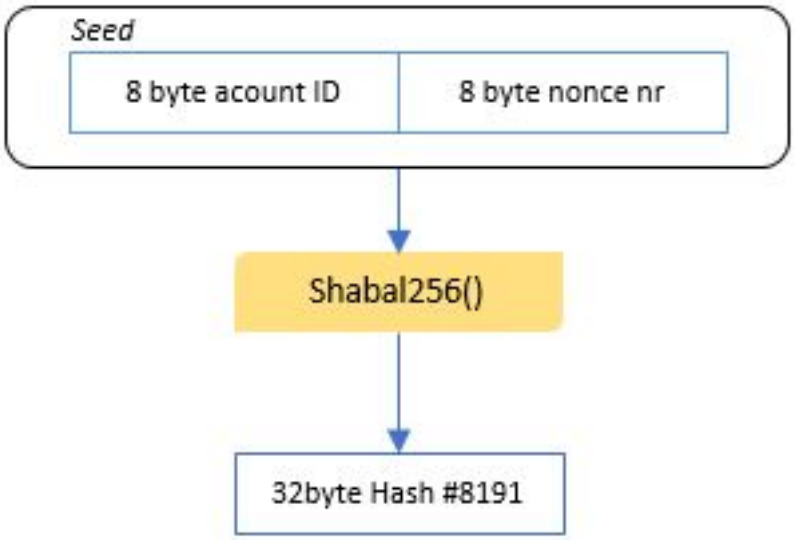
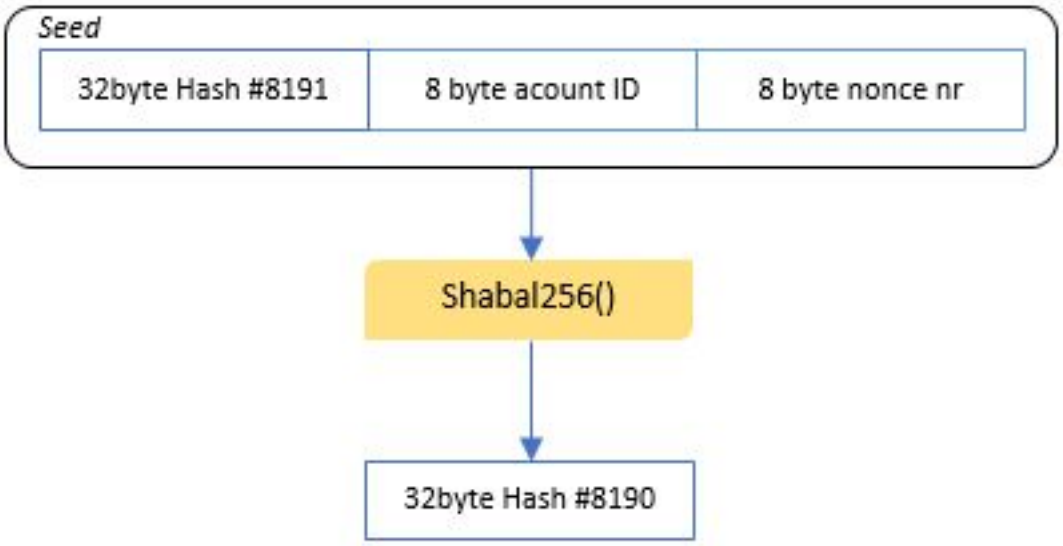
Generando un nonce

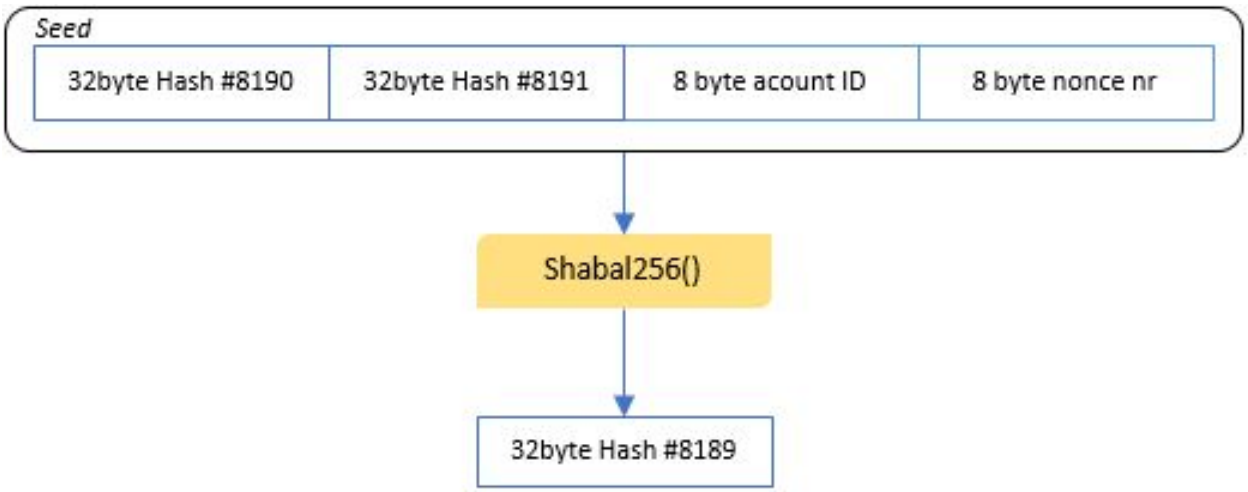
El primer paso para crear un nonce es hacer el primer seed. La semilla es un valor de 16 bytes que contiene la identificación de la cuenta para la que generaremos un nonce y el número de nonce. Cuando esto se hace, comenzamos a alimentar la función Shabal256 para obtener nuestro primer hash.



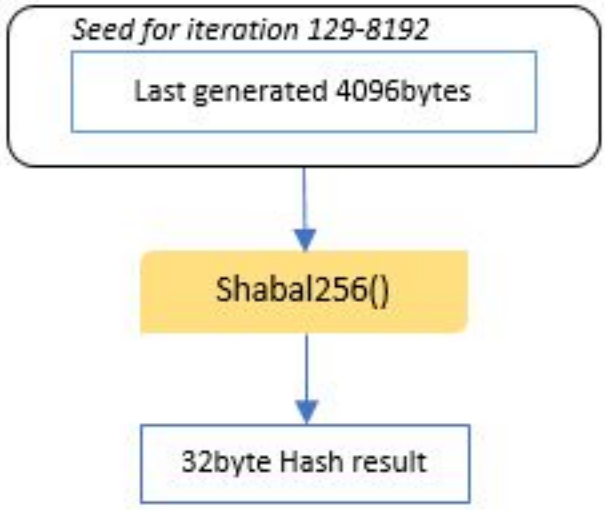
Hemos producido el primer hash. Este es el último hash en el nonce. Hash # 8191. Ahora tomamos este hash producido (# 8191) y lo agregamos previamente a la semilla inicial. El resultado será ahora nuestra nueva semilla para la próxima ronda de cómputo Shabal256.



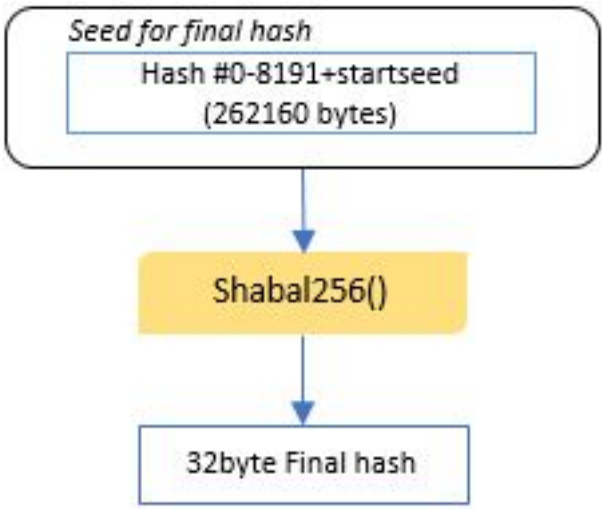
Ahora hemos producido dos hashes. Hash # 8191 y Hash # 8190. Esta vez preadjudicamos Hash 8190 a la última semilla que utilizamos. El resultado ahora será una nueva semilla para alimentar a Shabal256.



Una vez más, hemos creado un nuevo hash. Este procedimiento de hashes resultantes preanexados a una nueva semilla continuará para todos los 8192 hash que creamos para un nonce. Después de la iteración 128, hemos alcanzado más de 4096 bytes en la semilla. Para todas las iteraciones restantes solo leeremos los últimos 4096 bytes generados.

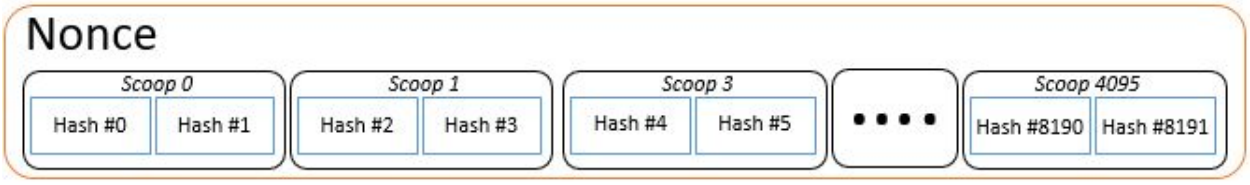


Una vez que hemos creado 8192 hashes, vamos a hacer un hash final. Esto se hace usando los 8192 hashes y los primeros 16bytes como seed.



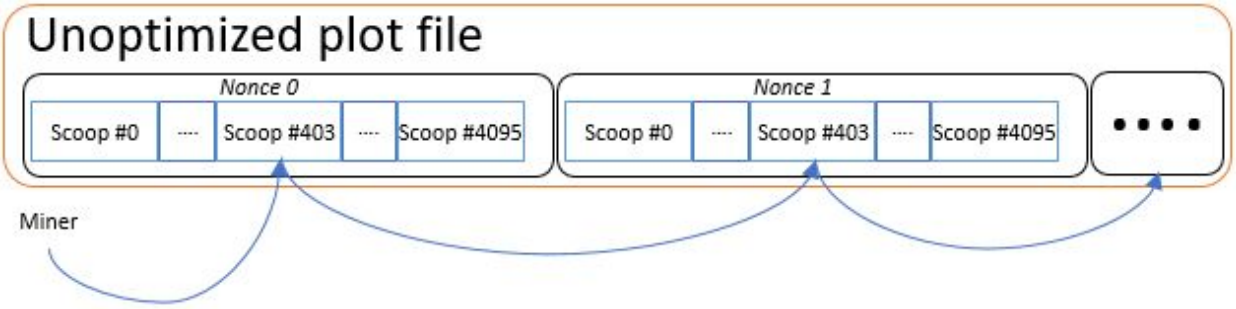
El hash final ahora se usará para xor todos los demás hash de forma individual.

Ahora hemos creado nuestro nonce y podemos almacenarlo en un archivo de trazado antes de continuar con el próximo evento.



Estructura del diagrama

Cuando estamos extrayendo leemos de uno o más archivos de trazado. El software del minero abrirá un archivo de trazado y buscará las ubicaciones de la pala para leer los datos de las cucharas. Si el archivo de trazado no está optimizado, las ubicaciones de las cucharas estarán en más de un lugar. En el siguiente ejemplo, el minero buscará y leerá la primicia # 403.



Esta no es la forma más efectiva ya que el minero pasará mucho tiempo buscando nuevas ubicaciones en el dispositivo de almacenamiento para poder leer las primicias. Para evitar esto, podemos optimizar trazados o usar un software de trazador que crea trazados optimizados desde el

principio. La optimización se realiza reordenando los datos en el archivo de trazado y agrupando todos los datos del mismo número de primicia.