Introducción

Con la mayoría de las criptomonedas que no están basadas en la prueba de estaca, hay un proceso llamado minería. Este proceso es la base de una cadena de bloques para crecer y asegurar las transacciones dentro de la red. ATMcash no es diferente, excepto que usa hashes precalculados para encontrar valores que pueden usarse para forjar un bloque. Para comprender completamente este documento, debe leer el documento denominado información técnica para crear archivos de trazado. Este documento pretende ser una descripción general de los procesos. Es información técnica, pero no lo suficientemente profunda como para ser utilizada como referencia para un programador ya que falta información sobre temas como AT, suscripciones y activos.

Algoritmos y acrónimos

- **Shabal / Sha256 / Curve25519**

Shabal, Sha256 y Curve25519 son funciones hash criptográficas utilizadas en este texto. Shabal es el principal usado por ATMcash. Shabal es una función hash criptográfica bastante pesada y lenta en relación con muchas otras como SHA256. Debido a esto, lo convierte en una buena criptografía para monedas con capacidad de prueba como ATMcash. Esto se debe a que almacenamos hashes precalculados, y aún es lo suficientemente rápido como para hacer verificaciones en vivo más pequeñas. ATMcash usa la versión de 256 bits de Shabal también conocida como Shabal256.

- **Hash / Digest**

Un hash, o resumen en este contexto, es un resultado al computar datos a través de una función hash criptográfica. Si no se dice lo contrario, la longitud de un hash es de 32 bits (256 bits).

- **Trazar los archivos**

Al extraer, lee los hashes precalculados de los archivos almacenados en un dispositivo de almacenamiento. Estos archivos se llaman archivos de trazado.

- **Nonce**

Dentro de un archivo de trazado, hay uno o más grupos de datos llamados nonces. Un nonce contiene 8192 hashes, y debido a eso, los nonces son 256KiB de gran tamaño. Cada nota tiene su propio número individual. Este número de 64 bits puede oscilar entre 0-18446744073709551615 (2^{64}).

- **Scoop**

Cada fuente se clasifica en 4096 lugares de datos diferentes. Estos lugares se llaman números primarios. Cada primicia contiene 2 hashes. Cada uno de estos hashes se xored con un hash final.

- **ID de cuenta**

Cuando crea su archivo de trazado, se lo vinculará a una cuenta específica de CashCash. Debido a esto, todos los mineros tienen diferentes archivos de trama.

- **Fecha límite**

Cuando extrae y procesa los archivos de su trazado, terminará con los valores resultantes denominados plazos. Los valores representan el número de segundos que deben transcurrir desde que se forjó el último bloque antes de poder forjar un bloque. Si nadie más ha forjado un bloque dentro de este tiempo, puedes forjar un bloque y reclamar una recompensa en bloque.

- **Bloquee la recompensa**

Si tiene la suerte de forjar un bloque, obtendrá ATMcash como recompensa. Esto se llama recompensa de bloque. La recompensa del bloque disminuye un 5% cada 10800 bloques. Esto es aproximadamente cada 30 días ya que se supone que cada bloque se forja cada 4 minutos (360 bloques por día).

- **Objetivo base El objetivo**

base se calcula a partir de los últimos 24 bloques. Este valor ajusta la dificultad para los mineros. Cuanto menor sea el objetivo base, más difícil es para un minero encontrar una fecha límite baja. Se ajusta de manera tal que ATMcash puede tener un promedio de 4 minutos por cada bloque.

- **Dificultad de la red La dificultad de la**

red, o NetDiff en resumen, es un valor que puede leerse como un cálculo aproximado de la cantidad total de espacio en terabytes dedicado al cajero automático de la mina. Dado que este es un valor que cambia con cada bloque en relación con el objetivo base, se debe tomar en un promedio de al menos 360 valores antes de que se considere algo preciso.

- **Altura del**

bloque Cada bloque forjado obtiene un número individual. Cada nuevo bloque forjado obtiene el número del bloque anterior + 1. Este número se llama altura del bloque y se puede usar para identificar un bloque específico.

- **Generador de bloques**

Cuando se falsifica un bloque, una cuenta ha encontrado un nonce y una fecha límite. El generador de bloques es la cuenta utilizada cuando se forja un bloque. Esta es la cuenta desde la cual se ha encontrado una fecha límite al forjar un bloque. Esta es siempre la cuenta real, incluso si se ha establecido una asignación de recompensa.

- **La firma Generation Signature**

Generation está basada en la firma de generación de bloque anterior y el generador de bloques. Este valor es utilizado por los mineros para forjar un nuevo bloque. La firma de generación tiene 32 bytes de longitud.

- **Firma del**

bloque Cada bloque está firmado por el generador que forja un bloque. Esto se hace tomando la mayor parte del bloque y firmándolo con la clave privada del generador de bloques usando Sha256 y Curve25519. El resultado es un hash de 64 bytes de longitud.

- **Asignación de**

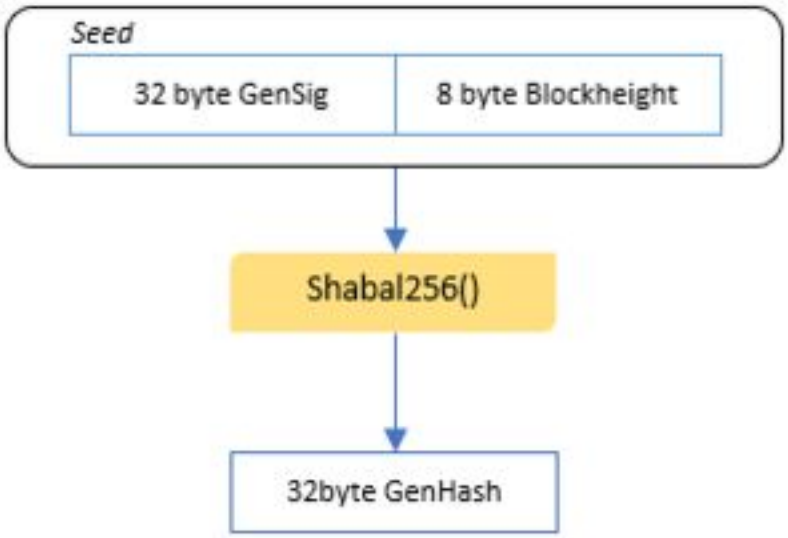
recompensas La asignación de recompensas se usa con frecuencia cuando se minería en grupo. Al cambiar su asignación de recompensa, le dice a la red que otra cuenta (la cuenta del grupo) está actuando en su lugar para 2 funciones específicas. La primera característica es que todas las recompensas en bloque que se deben otorgar a su cuenta ahora se otorgarán a la cuenta del grupo. En segundo lugar, para que el grupo pueda utilizar los plazos encontrados en los archivos de su trazado, también se le concede la acción para firmar los bloques recién forjados con la cuenta que pertenece al conjunto.

Proceso de minería

Todas las referencias a monedero en este texto también pueden ser un grupo dependiendo del escenario.

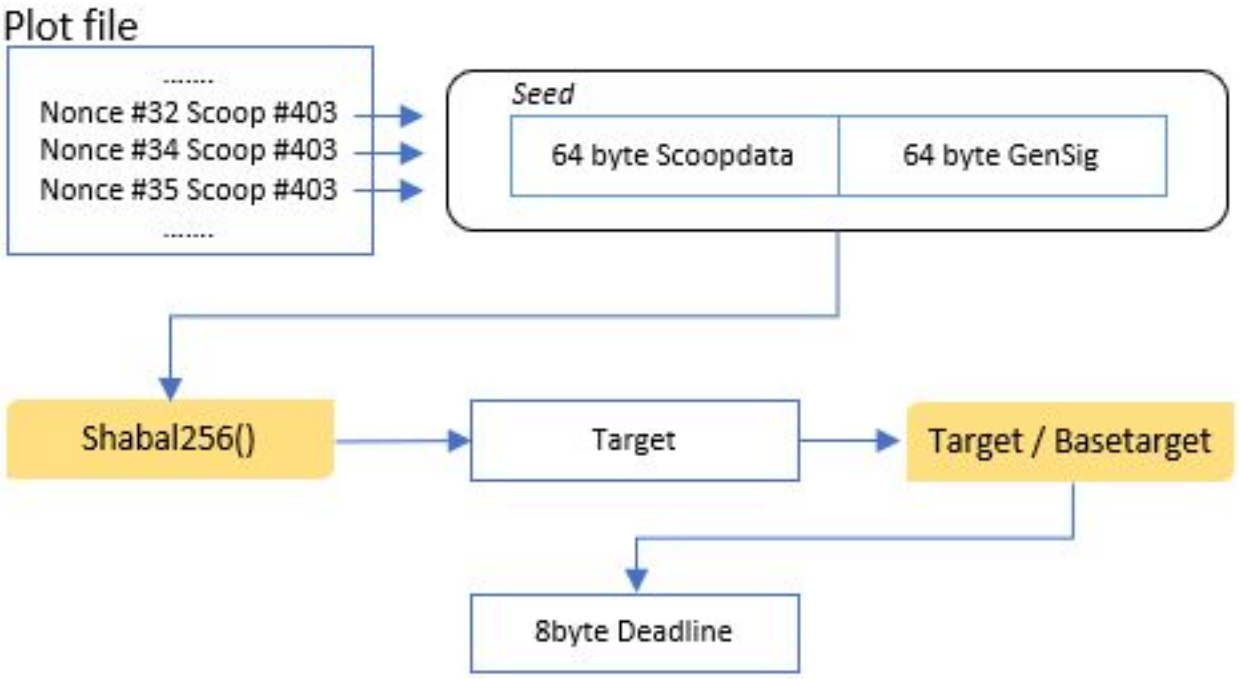
Todas las referencias a Miner en este texto es un software capaz de hacer una operación minera para ATMcash.

Lo primero que sucede cuando comienzas a extraer, es que el minero habla con la billetera y solicita información sobre la extracción. Esta información contiene una firma de nueva generación, un objetivo base y la siguiente altura de bloque. Antes de que la billetera envíe esta información, crea la firma de generación tomando la firma de la generación anterior junto con el generador de bloques anterior y ejecuta esto a través de shabal256 para obtener el nuevo hash. El minero tomará ahora la nueva firma de generación de 32 bytes y la altura del bloque de 8 bytes y los juntará como una semilla para Shabal256. El resultado será un valor hash llamado generación hash.



Ahora, el minero realizará una pequeña operación matemática en este hash para averiguar qué número de primicia usar al procesar los archivos de la parcela. Esto se hace tomando el módulo hash de generación 4096, ya que solo hay muchas primicias.

El siguiente paso para el minero es leer todas las primicias de 64 bytes de todos los nonces en todos los archivos de trazado. Los procesará individualmente a través de shabal256 junto con la firma de nueva generación para obtener un nuevo hash llamado target. Este objetivo ahora se divide con el objetivo base y los primeros 8 bytes del resultado es la fecha límite de valor.



Para evitar el llamado "correo basura nonce" en la billetera, el minero generalmente verifica si la fecha límite actual encontrada es menor que la más baja que haya encontrado hasta ahora. Por lo general, también hay un valor máximo que se puede establecer, ya que los plazos ridículamente grandes no sirven para nadie. Después de estos controles, el minero envía información a la billetera. Esta información contiene la identificación numérica de la cuenta vinculada al archivo de trazado y el número de nonce que contiene los datos primarios utilizados para generar la fecha límite. Si está trabajando en solitario, el minero también envía la frase de contraseña para la identificación de cuenta utilizada en los archivos de trazado. Si la contraseña no se envía al minería

individual, la billetera no podrá forzar bloques para esa cuenta. Cuando se extrae la agrupación, se utiliza la frase de contraseña para la identificación de la cuenta del grupo.

Proceso de falsificación de bloques

Gestión de plazos

La billetera ahora recibió la información presentada por el minero y ahora creará la cuenta para poder encontrar y verificar la fecha límite por sí misma. Una vez hecho esto, la billetera ahora comprobará y verá si ha pasado una cantidad igual o más segundos, según lo definido en la fecha límite. De lo contrario, la billetera esperará hasta que lo haga. Si se anuncia un bloque forjado válido de otra billetera en la red antes de que venza el plazo, la billetera descartará la información de minería enviada porque ya no es válida. Si el minero envía nueva información, el monedero creará ese nonce y comprobará si el valor del plazo es más bajo que el valor anterior. Si la nueva fecha límite es menor, la billetera usará ese valor en su lugar. Cuando la fecha límite sea válida, la billetera comenzará a forjar un bloque.

Forjar

Hay dos límites para un bloque. Primero, un bloque puede contener max. 255 transacciones. El segundo es que una carga útil de bloque puede tener un máximo. 44880bytes (43KiB). La billetera comenzará recibiendo todas las transacciones no confirmadas que haya recibido de los usuarios o de la red. Tratará de ajustar la mayor cantidad posible de estas transacciones hasta que alcance uno de los límites, o hasta que se procesen todas las transacciones. Para cada transacción que lee el monedero, hará los cheques. Por ejemplo, si la transacción tiene una firma válida, si tiene una marca de tiempo correcta, etc. La billetera también sumará todas las cantidades y tarifas de transacciones agregadas. El bloque solo contendrá la identificación de transacción de cada transacción y un hash Sha256 de todas las transacciones incluidas. Las transacciones completas se almacenan por separado. Además de esto, un bloque contiene muchos conjuntos diferentes de valores.

Contenido del

- **bloque Número de versión del bloquenúmero de**

Elversión básicamente le dice a la billetera qué puede contener un bloque y cómo está contenido. Este número cambia cada vez que un bloque obtiene un nuevo formato.

- **Lista de ID de transacción**

Una lista de todos los ID de transacción que se incluyen en este bloque.

- **Hash de carga útil**

Este es el hash Sha256 de todos los datos en la carga útil de ladel bloque

- **marca deTimestamp**

tiempoA que describirá cuándo se falsificó el bloque; derivado del nacimiento de la cadena de bloques. Fecha de nacimiento: 11 de agosto de 2014, Hora: 02:00:00

- **Cantidad total de monedas**

Esta es la suma de todas las transacciones en el bloque.

- **Cantidad total de tarifas.**

Esta es la cantidad de tarifas que se le dará al falsificador de bloques para generar este bloque.

- **La longitud de la carga útil**

Este es un número en bytes que representa la longitud de la carga útil.

- **Clave pública**

Esta es una clave pública para la cuenta que forja el bloque.

- **Firma de**

generación La firma de generación de 32 bytes que se usó para forjar el bloque.

- **Hash de bloque anteriorhash**

UnSha256 de los contenidos del bloque anterior.

- **ID de bloque anterior**

Estos son los primeros 8 bytes en el hash de bloque anterior convertido a un número.

- **Dificultad acumulativa**

Se usa para evitar problemas con Nothing at Stake durante potenciales tenedores. Calculado: Dificultad acumulativa previa + (18446744073709551616 / objetivo base)

- **Objetivo**

base El objetivo base utilizado al forjar este bloque

- **Altura**

Valor de altura de este

- **bloque ID del bloque**

Estos son los primeros 8 bytes en el hash del bloque convertido a un número

- **Nonce**

El número nonce utilizado para forjar este bloquear.

- **AT**

Si se agrega un AT a este bloque, estos son los bytes de carga para ese AT.

- **Block Signature**

Este es un hash de 64 bytes generado con la clave privada del falsificador y el contenido del bloque. Cuando se hace esto, se anunciará a la red. La billetera se conectará con todos los pares y les enviará el bloque. El par recibirá el bloque y verificará que toda la información no sea falsificada.