Enigmail

Miguel Santiago Cervilla

Firmado digitalmente por Miguel Santiago Cervilla
Fecha: 2019.01.23 19:06:17 +01'00'

Alumno: Miguel Santiago Cervilla

Profesor: Justo Peralta López

Teoría de Códigos y Criptografía

Indicar para qué objetivos se usa la función hash en bitcoin y su sintaxis en java

Este tipo de funciones se caracterizan por cumplir propiedades que las hacen idóneas para su uso en sistemas que confían en la criptografía para dotarse de seguridad.
Un algoritmo de Hash convierte una cantidad arbitrariamente grande de datos en un Hash de longitud fija.
Para generar el Hash de las claves públicas y privadas de Bitcoin se utiliza el algoritmo de **encriptación ECDSA**. Con el algoritmo ECDSA es posible generar la clave pública y la dirección pública a partir de la clave privada, pero no al revés. Esto es fundamental porque la clave privada es la que da acceso a gastar los Bitcoins que uno tiene en su monedero o wallet.

Bitcoin utiliza el algoritmo **SHA-256** para generar de manera verificable "al azar" la secuencia de números del Hash que se requieren para definir una cantidad previsible de esfuerzo CPU.

```
public Sha256Hash(String s) {

Objects.requireNonNull(s);

if (s.length() != HASH_LENGTH * 2 || !s.matches("[0-9a-fA-F]*"))

throw new IllegalArgumentException("Invalid hash string");

hash = new byte[HASH_LENGTH];

for (int i = 0; i < hash.length; i++)

hash[hash.length - 1 - i] = (byte)Integer.parseInt(s.substring(i * 2, (i + 1) * 2),
16);

}


public int hashCode() {

return (hash[0] & 0xFF) | (hash[1] & 0xFF) << 8 | (hash[2] & 0xFF) << 16 | hash[3] <<
24;

}
```

¿La identidad que tenemos en bitcoin está conectada con nuestra identidad en el mundo real?

Como cualquier tecnología que usamos como usuario, estamos conectados y puede ser rastreada. Para ello debemos tener en cuenta 3 premisas:

- Los datos no caducan.
- Las máquinas trabajan muy rápido y no se cansan.
- Los humanos cometemos fallos y dejamos información a diario.

Aunque se trata de un sistema seguro, se puede observar la transacción que se está realizando, pero sin que haya información alguna vinculada a nadie en la transacción.

¿Cuál es la estructura de una moneda?

Como si de una moneda tradicional se tratase, con la diferencia de que ésta no existe de manera física. Cada bitcoin es único (o cada porción de él) , cada transacción se registra públicamente.

¿Que cambia en una moneda cuando cambia de dueño?

Se añade la clave pública del nuevo propietario en la transacción.

¿En qué consiste el consenso distribuido?

Se puede replicar la base de datos en varios servidores. De esta forma, si un servidor falla, la información aún estaría accesible en alguna de las réplicas. Sin embargo, como la transmisión de datos no es inmediata, y las fallas pueden ocurrir en cualquier momento, es posible que en ciertas ocasiones exista **más de una versión** de la base de datos.

¿Cuál es el tiempo que se tarda en validar e insertar un bloque?

Existen dos factores principales, que son:

- Cargar en la red de Bitcoin
- Tarifa de transacción asociada a una transferencia de BTC

Cuanto mayor es el número de transacciones, mayor es el tiempo que le tomara para procesar todas ellas.

Hay un limitado número de transacciones pueden ser procesados en un bloque de tamaño de 1 MB en Bitcoin.

Haga una lista de mayor o menor con los nombres de sus compañeros de grupo atendiendo al esfuerzo realizado y aportaciones a su grupo de trabajo. No puedes insertar tu nombre en la lista.

Dentro del grupo de trabajo, cabe destacar que ambos integrantes hemos realizado el trabajo juntos y por tanto hemos aportado el mismo esfuerzo al mismo. Aun así la lista sería:

1º Jesús Sánchez Sánchez

2º Jorge Titos Payán