Computación Distribuida
Tarea 10

González Montiel Luis Fernando

13 de noviembre de 2019

1. ¿Cuál es el problema del doble gasto? ¿Cómo Bitcoin soluciona este problema?

   Respuesta: El doble gasto es un defecto potencial del dinero digital, en el que una misma moneda puede gastarse más de una vez. El problema de un sistema de pagos descentralizado es que, para representar una unidad monetaria de un euro de la misma forma que para los ficheros audiovisuales (música, videos, etc) solamente se necesitan bits y, hasta la llegada de Bitcoin, no existía ninguna forma de asegurar esos bits en un sistema descentralizado para que no pudieran ser replicados y gastados de nuevo. A este problema para los pagos en sistemas descentralizados se le denomina el problema del doble gasto. Este problema se soluciona con el protocolo Bitcoin.

2. ¿Cómo funciona el cifrado con llave pública y privada?

   Respuesta: Las direcciones de tu monedero (la que se da para que te envíen Bitcoin) son tus claves públicas. Puede conocerlas cualquiera pues solo sirven para recibir, no para usar el Bitcoin. Esa clave pública o dirección se ha creado a partir de una clave privada bastante más compleja. La clave privada del transmisor se utiliza para firmar la transacción. La clave privada del receptor asegura que esa dirección (clave pública) le pertenece y por tanto podrá usar ese Bitcoin. Afortunadamente todo este proceso se realiza de una forma sencilla e intuitiva sin tener que pensar mucho en cómo se hace ya que se encarga de ello ese software especial que llamamos wallet o monedero. En general, el usuario solo tiene que ocuparse de poner la dirección Bitcoin (clave pública) a donde quiere mandar ese dinero, poner la cantidad y pulsar el botón "Enviar".

3. ¿Cómo funciona el cifrado hash y para qué se usa?

   Respuesta: Una función hash es un procedimiento criptográfico donde se emplea un algoritmo específico para transformar una información determinada (por ejemplo, un texto) en una una secuencia alfanumérica única de longitud fija, denominada hash. Las funciones hash se emplean en acciones como la validación y autenticación de usuarios, la firma de documentos, y también en las criptomonedas como método para evitar la falsificación de transacciones y prevenir acciones maliciosas.

4. ¿Cómo funciona el protocolo Bitcoin?

   Respuesta: Bitcoin tiene un libro contable descentralizado, distribuido a través de un programa que se descargan los ordenadores de la red Bitcoin, llamada blockchain (cadena de bloques en español) donde se anotan todas las transacciones hechas con bitcoins para evitar el doble gasto de los mismos. Esta blockchain es pública y puede ser consultado por cualquier persona para comprobar todas las transacciones que se han hecho. Las transacciones que se anotan en la blockchain se anotan por los mineros de Bitcoin

5. ¿Qué es la prueba de trabajo?

Respuesta: Una prueba de trabajo (en inglés Proof of work o PoW) es un mecanismo de control aplicado a un sistema que, con el propósito de afianzar, así como de eludir ataques y conductas fraudulentas, requiere la realización de alguna clase de trabajo por parte de los usuarios que conlleva una significativa inversión de tiempo y, por lo general, también, un coste elevado, ya sea en equipamiento, por consumo eléctrico o en ambas facetas. La implantación de la prueba de trabajo en el protocolo de Bitcoin obedecía a dos motivos principales. Por un lado proteger la moneda electrónica de fraudes y manipulación de datos, blindarla contra toda clase de ataques informáticos. Por el otro, certificar la validez de las transacciones de un modo público, descentralizado, mediante consenso entre los mismos usuarios, de tal forma que no se dependiera de ciertas instituciones (bancos, entidades financieras).

6. ¿Qué es un fork? ¿Cómo se solucionan los forks?

   Respuesta: En las redes blockchain, las bifurcaciones son usadas tanto para crear nuevos proyectos partiendo de uno anterior, como para actualizar un proyecto en cuestión. Las redes blockchain se rigen bajo unas reglas codificadas en el protocolo que permiten a los nodos validar bloques de transacciones de la misma forma y mantenerse en consenso. Estas reglas verifican que la estructura del bloque y las transacciones incluidas en él, como el tamaño del bloque (cantidad de espacio disponible) sean correctas.

7. ¿Por qué la prueba de trabajo no es exactamente un algoritmo de consenso?

   Respuesta: La prueba de trabajo es un método para establecer un consenso entre un número de personas interesadas, ninguna de las cuales está subordinada a otra, y existen incentivos considerables para resistirse a dicho consenso.

8. ¿Qué es un contrato inteligente?

   Respuesta: Son programas informáticos. No están escritos en lenguaje natural, sino en código virtual. Su cumplimiento, por tanto, no está sujeto a la interpretación de ninguna de las partes: si el evento A sucede, entonces la consecuencia B se pondrá en marcha de forma automática. Asegurará sin dudas el cumplimiento de las condiciones. Por tanto, se reducen tiempo y costes significativos.

9. ¿Cómo se ejecuta un contrato inteligente?

   Respuesta: La definición más simple al respecto es que se tratan de contratos que tienen la capacidad de cumplirse de forma automática una vez que las partes han acordado los términos.

10. ¿Qué es lo que más te pareció importante o interesante del seminario?¿Por qué?

    Respuesta: Me gustó bastante el seminario ya que es un tema que es muy innovador en estos tiempos y yo le veo demasiado futuro a la economía para dejar a un lado bancos y organizaciones, aunque por desgracia como dicen, los países comienzan a controlarlo un poco el mercado para tener un control más adecuado, ya sea para bien o para mal. Y un dato interesante que aún hasta la fecha sigo sorprendido de cómo puede valor tanto un bitcoin que equivale a 8,760 dólares por unidad.