Universidad de Cantabria - Universidad Internacional Menéndez Pelayo

Master en Ciencia de Datos

Asignatura: Nuevos Desarrollos 2021/2022

Resumen del articulo: *Bitcoin: A Peer-to-Peer Electronic Cash System*

- Pablo Calatayud Pelayo
- Mohamed Charif El Yacoubi Benabbou

El 31 de octubre de 2008 se publicó el Bitcoin White Paper con el nombre de *Bitcoin: A Peer-to-Peer Electronic Cash System* firmado por Sathosi Nakamoto. Como curiosidad, Sathorsi Nakamoto es un seudónimo y se cree que esta tecnología fue desarrollada por un grupo multidisciplinar de investigadores con conocimientos tanto criptográficos como de teoría monetaria. Un bitcoin se divide en cien millonésimas partes y esta mínima unidad recibe el nombre de satoshi en honor al desarrollador.

1 Introducción

Las entidades financieras pueden mediar en disputas de reversión de pagos y servicios, pero esto incrementa el coste de la transacción, añadiendo comisiones a los intercambios. En el artículo se propone un sistema de pagos no reversible, aceptando que un cierto porcentaje de transacciones pudiera derivar en fraude. El objetivo es crear un sistema de pagos descentralizado, sin la necesidad de que haya un tercero conocido por ambas partes, a través de un canal de comunicación de confianza.

2 Transacciones y Servidor de Marcas de Tiempo

Bitcoin es una moneda digital que funciona por medio de cadenas de firmas digitales. Las transacciones se realizan por medio de criptografía asimétrica usando el sistema de clave pública y clave privada. Las transacciones han de contener una o varias direcciones con fondos, una o varias direcciones a las que enviar dichos fondos, la cantidad de Bitcoin enviada y la cantidad de Bitcoin recibida. Esta diferencia entre cantidad enviada y cantidad recibida se conoce como comisión y cuanto más alta sea esta comisión, más prioridad dará la red a dicha transacción.

La cadena de bloques de bitcoin puede entenderse como un libro contable. Donde cada bloque es una página y cada línea de la página está compuesta por el hash de la página anterior, una marca de tiempo, y las transacciones relativas. Las transacciones son públicas, de forma que los mineros pueden verificar por medio de la cadena de bloques que la dirección tiene fondos. Todo esto garantiza que no haya transacciones de doble gasto y que una dirección sin fondos no pueda enviar bitcoins.

3 Prueba de Trabajo y Red

Cuando la red selecciona un bloque, se dice que el bloque ha sido minado y a los nodos que proponen bloques se les llama mineros. La prueba de trabajo es el sistema de consenso para decidir que bloque es minado. El bloque ha

de contener los requisitos mencionados anteriormente más una línea de cogido libre que se llama *nonce*. Esta línea de código libre contiene un número aleatorio que es alterado voluntariamente por los mineros con el único objetivo de que el output de la función Hash *SHA-256* aplicada al contenido del bloque varíe. El output ha de ir cambiando hasta que su valor cumpla una condición. Según la potencia de hash de la red se establece un número de ceros al principio del output de la función hash como condición imprescindible para aceptar dicho bloque. La cantidad de ceros exigida varía en función del poder de hash de la red, intentando que cada solución sea encontrada cada 10 minutos aproximadamente, manteniendo un ritmo de creación de bloques constante.

El nodo que encuentra la solución la comparte con el resto de nodos de la red y estos verifican el contenido del bloque, es decir, que el bloque contiene el hash del bloque anterior, el sello de tiempo, las transacciones, el *nonce* y que el output del hash de dicho bloque cumple la condición de dificultad exigida por la red. Una vez la solución es aceptada, esta se añade a la cadena de bloques. En caso de disputa, porque que se presenten dos soluciones a la vez, sé hace un fork y se siguen minando ambas ramas. El empate se rompe en los siguientes bloques, cuando se van encontrando distintas soluciones y una cadena se vuelve más larga que la otra. La cadena larga prevalece y la otra rama se descarta. La cadena de bloques es compartida por todos los nodos y estos pueden acceder a dicha información en todo momento, permitiendo que nodos se unan y abandonen la red.

4 Incentivo

La primera transacción del bloque es un número concreto de nuevas monedas que son adquiridas por el minero del bloque como recompensa. Además, también hay incentivos por comisión en cada transacción. Esta comisión es elegida por quién efectúa la transacción al establecer una diferencia entre la cantidad enviada y la cantidad recibida.

El número de unidades de bitcoin es limitado y la cantidad de nueva moneda creada por bloque disminuirá con el tiempo hasta que dicha recompensa sea nula. En ese punto, el incentivo será únicamente la comisión por las transacciones y como resultado se creará un activo libre de inflación.

Si un nodo intenta romper el sistema, este requerirá de una capacidad de cómputo enorme y debería encontrar mayor recompensa en mantener el sistema minando nuevos bloques y obteniendo sus bonificaciones.

5 Reclamando Espacio en Disco y Verificación de Pagos Simplificada

Se emplea la tecnología de los árboles de Merkle. Esto permite agregar todas las transacciones de un bloque en un árbol de hashses, desde las hojas del árbol que son las transacciones, hasta el nodo padre, obteniendo un único hash de hashes. De esta forma se consigue la inmutabilidad de cada transacción y no es necesario que todos los nodos almacenen todas las transacciones, pudiendo almacenar en memoria solamente el hash padre. Habrá bloques donde todas las direcciones de envío hayan gastado sus bitcoins y dichos bloques pueden quedar cerrados por sus hashses. Las instituciones que empleen este sistema de pagos también estarán interesadas en aportar nodos fiables que se dediquen exclusivamente a verificar que las soluciones propuestas son fiables. Este proceso requiere mucha menos capacidad de cómputo que el minado al tener como objetivo la verificación de la solución y no el cálculo esta.

6 Combinando y Dividiendo Valor

Para que se combine y se divida valor se permiten múltiples direcciones tanto al enviar como al recibir bitcoins.

7 Privacidad

Es un sistema seudo-anónimo donde se conoce la clave pública, pero esta no tiene por qué estar relacionada con una persona. Como medida extra de seguridad, se genera un par de claves nuevo para cada transacción.

8 Cálculos

La red será atacada cuando un agresor intente generar una rama de la cadena con intenciones espurias. Los nodos honestos nunca aceptarían un bloque que cree dinero fuera del protocolo o donde el atacante tome más fondos de los disponibles en su dirección. El único ataque posible es que intente rehacer alguna de sus transacciones engañando a un cobrador. El atacante envía la transacción honrada a la red y trabaja en crear una cadena de bloques paralela con la transacción modificada. Se asume que la probabilidad de que un nodo honesto mine un bloque es mayor a la probabilidad de que lo haga uno deshonesto. La probabilidad de que un nodo deshonesto resuelva Z bloques antes de que un nodo honesto note el cambio y no haya una solución alternativa baja exponencialmente con el número de bloques.

9 Conclusión

Se propone un sistema de intercambio electrónico usuario a usuario que utiliza una cadena de bloques para registrar una historia de transacciones y una prueba de trabajo para verificar las nuevas transacciones. Los nodos pueden trabajar al mismo tiempo. Un nodo solo necesita aceptar la cadena de bloques de consenso para unirse a la red y puede abandonarla cuando considere. Los nodos aportan confianza a la red en función de su potencia de cómputo.

10 Opinión

10.1 Opinión sobre la tecnología de Bitcoin

Desde un punto de vista tecnológico queremos destacar que todas las tecnologías empleadas en bitcoin ya existían anteriormente a su creación. Es decir, el merecido reconocimiento a Satoshi Nakamoto no viene por un descubrimiento científico, sino por articular un conjunto de desarrollos ya existentes para crear un sistema de pagos descentralizado.

10.2 Opinión sobre la posible aplicación de Bitcoin

Se piensa que la motivación de Bitcoin se genera a raíz de la crisis financiera de 2007-2008 y la necesidad de crear un sistema de pagos independiente de las instituciones financieras que habían sido las responsables de la crisis.

Desde un punto de vista social, el lenguaje, el derecho y la moneda son los tres conceptos que históricamente han sido controlados por poderes centrales. Se ha desarrollado a través del consenso, el derecho internacional y el inglés como fórmulas universales. Respecto a la moneda, el dólar dejó de ser una divisa respaldada al abandonar el patrón oro en 1971 y creemos que bitcoin no ha de verse como un activo especulativo, sino como una oportunidad para la posible instauración de una divisa global que permita crear un sistema financiero internacional descentralizado. Entendiendo por sistema financiero como el método que permite el intercambio de bienes y servicios entre dos partes. Bitcoin puede convertirse en el actor principal de una nueva teoría monetaria que tenga como principales características la descentralización y la no inflación monetaria como consecuencia de que solo habrá 21 millones de unidades.

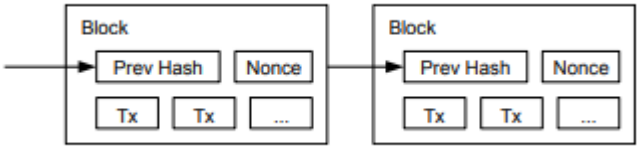
A Apéndice

A.1 Función Hash y Hash

Una función hash es una función criptográfica que recibe como input cualquier tipo de información finita y lo transforma unidireccionalmente en una serie de bits de longitud finita. Concretamente, la función hash *SHA-256* transforma cualquier cadena de información finita en una serie de 256 bits. Con unidireccional se refiere a que sin saber nada de la información del input es imposible por medio del output y la función empleada conocer el input. Coloquialmente, se conoce como hash o valor del hash al output de la función hash.

A.2 Cadena de Bloques

Se entiendo por cadena de bloques al conjunto de bloques minados. Desde el primero hasta el último. Estos bloques están unidos por una cadena de hashes. De forma que el bloque *j* contiene en su cuerpo el hash del bloque *j-1* y así sucesivamente.



A.3 Prueba de Trabajo

El concepto de prueba de trabajo fue creado por Adam Back. El coste inexistente de enviar un email favorece las prácticas de spam masivo por correo. Lo que A. Back propone en la referencia *[6]* es a través de hashes exigir un pequeño coste computacional al envío de un email, de forma que el envío masivo de correos sea ineficiente.

A.4 Árboles Merkle

El árbol es un hash de hashes que se construye de la siguiente forma. Todas las transacciones son los nodos terminales, conocidos como hojas. Estas hojas se van agrupando en nodos superiores, de forma que el nodo padre inmediatamente superior a las hojas recibe como input la información de las transferencias correspondientes y como output genera un hash. Después estos nodos padres se agrupan en otros nodos superiores que reciben como input los hashes de sus hijos y como output el único hash generado. De esta forma se sigue ascendiendo hasta alcanzar un único nodo padre. Todo el árbol queda condicionado al hash del nodo padre.