Análisis de sentimientos multimodal

Sara Olías Zapico

12 de enero de 2022

Índice

1. Fundamentos teóricos

1.1. Bitcoin

1.1.1. Concepto de criptomoneda

Una criptomoneda es una moneda digital que utiliza la criptografía como medio de seguridad, impidiendo así que se falsifiquen o se produzca el doble gasto de estas. Estas monedas tienen una administración descentralizada (peer-to-peer) y se basan en el Blockchain, un histórico de todas las transacciones del sistema o anlálogamente, un libro contable público y distribuido. Esta forma de organización descentralizada característica de las criptomonedas permite que estas no sean generadas por ninguna autoridad central, lo que las hace teóricamente inmunes a la interferencia o manipulación del gobierno [1].

El origen de las criptomonedas se remonta a 1982, cuando David Chaum publicó el artículo "*Blind Signatures for Untraceable Payments*"[2] en el que presenta un sistema formal para cifrar matemáticamente los pagos. Este sistema supuso un gran avance para la seguridad digital ya que anonimizaba los pagos, lo que impedía a los bancos y el gobierno rastrear al pagador en una transacción. Sin embargo, es diferente de la tecnología blockchain porque requiere que los bancos actúen como terceros confiables para todas las transacciones electrónicas.

No fué hasta 1998 cuando Wei Dan publicó el concepto de criptomoneda en su artículo "*b-money, an anonymous, distributed electronic each system*". En el artículo, Dai describió el b-money como "un plan para que un grupo de seudónimos digitales imposibles de rastrear se paguen entre sí con dinero y hagan cumplir los contratos entre ellos sin ayuda externa".

1.1.2. Bitcoin

Es en noviembre de 2008 cuando nace el Bitcoin. Aparece tras la publicación en un foro del artículo "*Bitcoin: A Peer-to-Peer Electronic Cash System* "[3] bajo el pseudónimo de Satoshi Nakamoto; sin embargo, hasta el momento no se sabe si este pseudónimo engloba a una única persona o un grupo de personas.

En Enero de 2009 entró en funcionamiento esta moneda, lo que supuso la creación de la primera criptomoneda descantralizada. Nakamoto inventó un sistema de seguridad, el Blockchain, que marca la diferencia con todas las criptomonedas anteriores. Otra de sus características es el anonimato exitente entre las transacciones, haciendo prácticamente imposible el rastrearlas.

1.1.3. Blockchain

Un blockchain o cadena de bloques es un histórico con todas las transacciones del sistema. La estructura de datos de la cadena de bloques es una lista ordenada y vinculada de bloques de transacciones. Cada uno de ellos está vinculado a su bloque anterior y a menudo, se visualizan como una pila vertical, por lo que podemos utilizar el término "altura"para referirnos a la distancia entre el primer y último bloque.

Cada uno de estos bloques tiene como identificador un código hash, que es generado mediante el algoritmo criptográfico SHA-256 [4]. Para hacer referencia a su bloque anterior, en cada uno de ellos se añade también el hash de su bloque antecesor. La secuencia de hashes que uno cada bloque con el anterior es la que crea la cadena hasta el primer bloque existente, llamado bloque génesis.

El campo "hash del bloque anterior " está dentro del encabezado del bloque y, por lo tanto, afecta al hash del bloque actual . Si el bloque padre se modfica, el hash de este cambia, haciendo que el bloque posterior a el tenga que cambiar también. De esta forma, se genera un efecto cascada implicando que si un bloque tiene muchas generaciones posteriores, al realizar un cambio, este fuerza un nuevo cálculo para todos los bloques que lo suceden. Debido a que este cambio requeriría un enorme cálculo para toda la cadena, la existencia de una larga cadena de bloques hace que la historia profunda de la cadena de bloques sea inmutable, que es una característica clave de la seguridad de bitcoin.

Veamos con detalle las componentes del encabezado de un bloque:

Tamaño(bytes)	**Campo**	**Descripción**
4 bytes	Versión	Un número de versión para realizar un seguimiento de las actualizaciones de software
32 bytes	hashPrevBlock	Una referencia al hash del bloque anterior en la cadena
32 bytes	hashMerkleRoot	Un hash de la raíz del árbol merkle [5] de las transacciones de este bloque.
4 bytes	Timestamp	El tiempo de creación aproximado de este bloque en UNIX
4 bytes	Bits	El objetivo de dificultad del algoritmo de prueba de trabajo para este bloque
4 bytes	Nonce	Número aleatorio utilizado para generar el hash del bloque

Cuadro 1: Cabezal de un bloque de blockchain de Bitcoin

El blockchain está distrubuido en una red peer-to-peer, esta consiste en una red de ordenadores (o nodos) donde cada uno de ellos tiene una copia local de toda la cadena de blockchain, consiguiendo así que la cadena sea verificada de forma independiente y descentralizada. Cuando se añade una nueva transacción a la cadena, esta es registrada por cada nodo y tras esto se transmite al resto de la red. Para cada nuevo bloque recibido, cada nodo ejecuta un protocolo ya establecido, ya sea para rechazar este bloqu o aceptarlo en la cadena, cuando es aceptado en mas del 50 de los nodos, el bloque se agrega a la cadena. Estas verificaciones se realizan cada diez minutos aproximadamente, esto quiere decir, que cada diez minutos un nuevo conjunto de transacciones es aceptada por la red y se incluye como un nuevo bloque de la cadena, sin la necesidad de una entidad supervisora.

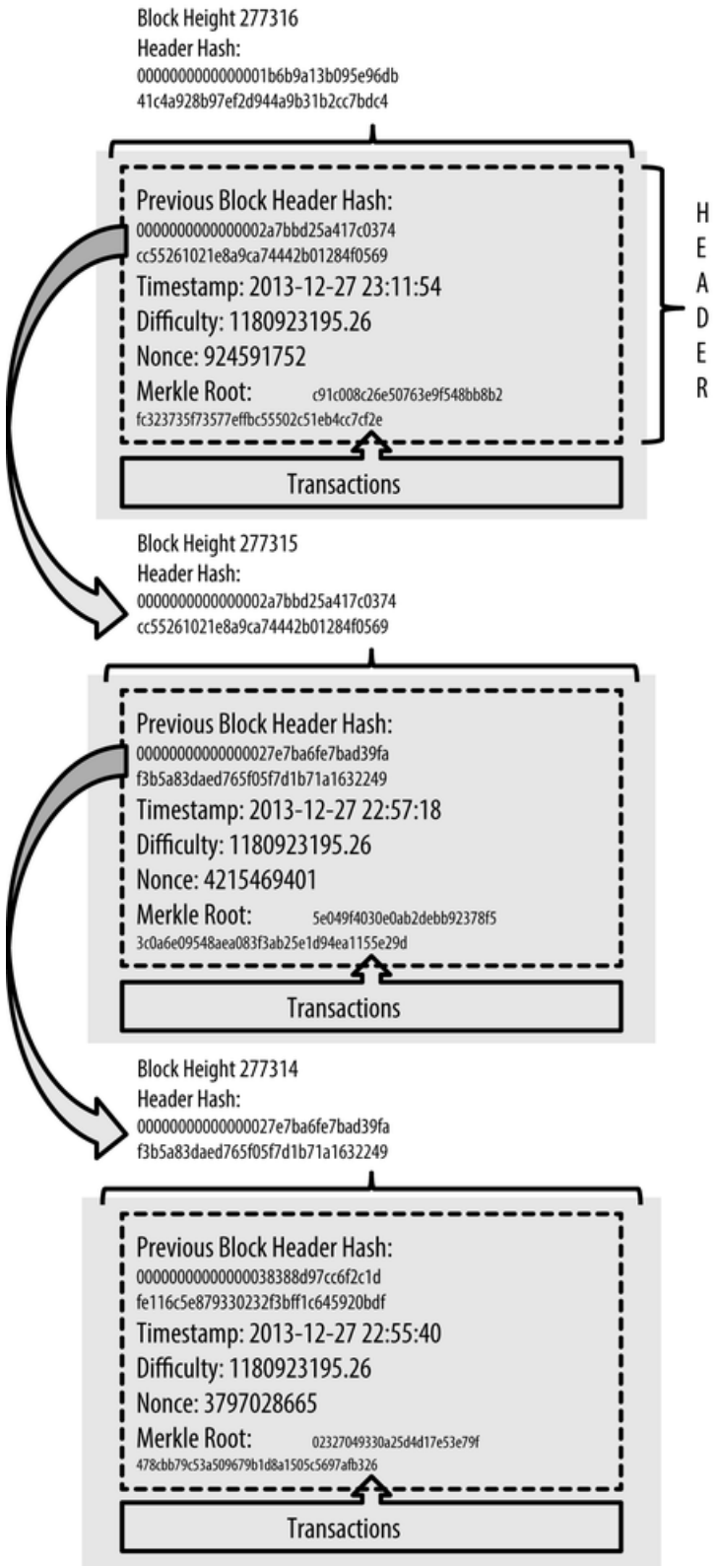

Figura 1: Ejemplo de tres bloques de la cadena de Bitcoin

1.1.4. Transacciones

En el concepto básico, una transacción es un envío o transferencia de valor entre dos partes. En Bitcoin, estas transacciones pueden entenderse como el envío de Bitcoins entre varias personas que utilizan la red. Pero en realidad, todas estas transacciones no son más que registros guardados en la cadena de bloques de Bitcoin. Es decir, el flujo de información. Por tanto las transacciones de Bitcoin son mensajes que contienen información, mensajes que pueden programarse y firmarse digitalmente con encriptación y enviarse a toda la red para su verificación. Por eso dicen que Bitcoin es dinero programable. Además, dado que las transacciones en la red Bitcoin son públicas, es fácil encontrarlas en su cadena de bloques. En ellos se puede verificar cada transacción desde el nacimiento del primer Bitcoin.

Los elementos que conforman una transaccion son:

- **Entradas o inputs:** cada entrada debe hacer referencia a una salida sin gastar de otra transferencia o a una generación, es decir, la primera transferencia de un bloque.
- **Salida o outputs:** contienen la dirección a la cual se realiza la transferencia y la cantidad enviada-
- **Identificador(TXid):** las transacciones estan asociadas a un hash para poder identificar cada una de ellas de forma única.
- **Tarifa de comision(fee):** La fee es un pequeño pago que reciben los mineros por procesar una transacción.

Veamos un ejemplo de una transacción extraida de la web *bit2me*:

Figura 2: Ejemplo de transacción en Bitcoin

- **Transacciones pendientes de gasto UTXO**

Una transacción UTX(Unspent Transaction Output), o transacción pendiente de gasto, es una salida que un usuario recibe para poner gastar en el futuro como una entrada para alguien más [6]. El balance de la cartera de un usuario esta formado por diferentes UTXOs con distintas cantidades cada una.

Supongamos que tienes 100 $ en Bitcoin divididos en diferentes UTXOs (20 $, 20 $,10 $,7.5 $,13 $,2.5 $,11 $16 $) y quieres pagar 45 $; al realizar el pago se envían 3 UTXOs: 20 $, 20 $ y 7.5 $, por lo que se devolvería una UTXO de 2.5 $. Sin embargo, debemos contar con que hay que incluir una comisión para quienes mantienen la red (imaginemos 0.5 $), por lo que la UTXO devuelta sería de 2 $.

Es importante tener en cuenta que, más que de monedas, toda la blockchain es una red de UTXO que esperan a ser desbloqueadas y enviadas a alguien más como una nueva UTXO.

Problema del doble gasto

Otro problema existente en las transacciones es el problema del doble gasto. Esta consiste en la incidencia que se produce cuando un individuo gasta el mismo saldo más de una vez, creando una disparidad entre el registro de gastos y la cantidad disponible.

El blockchain tiene un mecanismo eficaz para detectar el doble gasto. Imagina que tienes 1 BTC e intentas gastarlo dos veces en dos transacciones separadas. Puede intentar hacer esto enviando el mismo BTC a dos direcciones de billetera de bitcoin separadas. Ambas transacciones pasarán al conjunto de transacciones no confirmadas. La primera transacción se aprobaría a través del mecanismo de confirmación y luego se verificaría en el bloque posterior. Sin embargo, la segunda transacción sería reconocida como inválida por el proceso de confirmación y no sería verificada. Si ambas transacciones se extraen del grupo para su confirmación simultáneamente, la transacción con el mayor número de confirmaciones se incluirá en la cadena de bloques, mientras que la otra se descartará.

Imagina que tienes 1 BTC e intentas gastarlo dos veces en dos transacciones separadas. Puede intentar hacer esto enviando el mismo BTC a dos direcciones de billetera de bitcoin separadas. Ambas transacciones pasarán al conjunto de transacciones no confirmadas. La primera transacción se aprobaría a través del mecanismo de confirmación y luego se verificaría en el bloque posterior. Sin embargo, la segunda transacción sería reconocida como inválida por el proceso de confirmación y no sería verificada. Si ambas transacciones se extraen del grupo para su confirmación simultáneamente, la transacción con el mayor número de confirmaciones se incluirá en la cadena de bloques, mientras que la otra se descartará.

Quedan otras vulnerabilidades en este sistema que podrían permitir que se lleven a cabo ataques de doble gasto. Por ejemplo, si un atacante de alguna manera es capaz de controlar al menos el 51 del poder de la red , puede cometer el doble de gasto. Si un atacante de alguna manera pudiera obtener el control de esta gran potencia computacional, podría revertir las transacciones y crear una cadena de bloques privada separada. Sin embargo, el rápido crecimiento de bitcoin prácticamente ha asegurado que este tipo de ataque sea imposible.

Bibliografía

[1] "*Cyptocurrency*", mayo 2020. Frankenfield,J. Disponible: *https://www.investopedia.com/terms/c/cryptocurrency.asp*

[2] "*Blind Signatures for Untraceable Payments*", 1982. David Chaum. Disponible: *https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF*

[3] "*Bitcoin: A Peer-to-Peer Electronic Cash System* ",2008, Satoshi Nakamoto. Disponible: *https://bitcoin.org/bitcoin.pdf*

[4] "*Security Analysis of SHA-256 and Sisters*",2003, Henri GilbertHelena Handschuh.

[5] "*A digital signature based on a conventional encryption function*", 1987, pags. 369-378, Ralph C Merkle.

[6] "*Blockchain: bloques, transacciones, firmas digitales y hashes*", 2015, Isabel Pérez. Disponible: "*https://www.criptonoticias.com/criptopedia/blockchain-bloques-transacciones-firmas-digitales-hashes/*"