UNIVERSIDAD AUTONOMA DE MADRID

ESCUELA POLITECNICA SUPERIOR

Doble Grado en Ingeniería Informática y Matemáticas

TRABAJO FIN DE GRADO

ANÁLISIS Y TRAZABILIDAD DE OPERACIONES EN CRIPTOMONEDAS

Pablo Zapata Rodríguez
Tutor: Álvaro Ortigosa Juárez

JUNIO 2019

ANÁLISIS Y TRAZABILIDAD DE OPERACIONES EN CRIPTOMONEDAS

AUTOR: Pablo Zapata Rodríguez
TUTOR: Álvaro Ortigosa Juárez

Dpto. Ingeniería Informática
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Junio de 2019

Resumen

Las criptomonedas son una alternativa digital a las divisas tradicionales. Se utilizan como bien de intercambio y usan la criptografía tanto como para crear nuevas unidades como para asegurar las transacciones y garantizar su seguridad e integridad. No requieren una institución central que lo gestione, sino que se basan en un sistema totalmente distribuido y descentralizado, y todas las transacciones e información se almacena en una gran estructura de datos conocida como *blockchain*.

Esta cadena de bloques es un registro público que conocen todos los usuarios de la red. En ella se almacenan los datos de todas las transacciones en conjuntos conocidos como bloques, con la peculiaridad de que cada bloque contiene información del bloque anterior, por lo que quedan enlazados formando una gran cadena. Esto implica que para modificar un bloque habría que modificar también todos los siguientes, lo que convierte a esta cadena en un sistema de almacenamiento muy seguro e inmutable. Si además añadimos los beneficios de la criptografía asimétrica y las funciones hash, la tecnología *blockchain* garantiza la seguridad de las operaciones con criptomonedas.

Para añadir un nuevo bloque a esta cadena, tarea conocida como minar un bloque, los usuarios tienen que resolver un complicado problema conocido como Prueba de Trabajo. Consiste en encontrar un número que al *hashearlo* junto con el resto del encabezado del bloque cumpla una condición determinada. Este proceso requiere mucha capacidad de computación, pero a cambio el minero obtiene una recompensa monetaria, por lo que son muchos los que quieren ganar esta competición.

Al minar un bloque se publican nuevas transacciones en la cadena, haciendolas públicas para todos los nodos de la red, de manera que todos pueden comprobar que son transacciones válidas, y no se comete ninguna irregularidad como un doble gasto de la misma cantidad de dinero. Además estas transacciones se publican sin información de la persona física que las realiza o las recibe, únicamente se conoce la dirección pública de los monederos emisor y receptor. Este pseudoanonimato convierte a las criptomonedas en un atractivo medio de pago para los delincuentes, y dificulta a las Fuerzas y Cuerpos de Seguridad las tareas de seguimiento.

Por tanto, en este Trabajo se va a desarrollar un sistema que nos permita obtener cierta claridad a la hora de seguir los movimientos de algunas carteras sospechosas, observar las transacciones en las que se involucran u obtener la información que se encuentra en la cadena de bloques.

Palabras clave

Bitcoin, Bloque, Cadena de Bloques, Criptomoneda, Minería, Transacción

Abstract

Cryptocurrencies are a digital alternative to traditional currencies. They are used as exchange and they use cryptography as much to create new units as to secure transactions and guarantee their security and integrity. They do not require a central institution to manage it, but rather they are based on a fully distributed and decentralized system, and all transactions and information are stored in a large data structure known as blockchain.

This blockchain is a public ledger that is known by all users of the network. It stores the data of all transactions in sets known as blocks, with the peculiarity that each block contains information from the previous block, so they are linked together forming a large chain. This implies that in order to modify a block, all the following ones must also be modified, which makes this chain a very secure and immutable storage system. If we add the benefits of asymmetric cryptography and hash functions, the blockchain technology guarantees the security of operations with cryptocurrencies.

To add a new block to this chain, as known as mining a block, users have to solve a difficult problem known as Proof of Work. It consists on finding a number that hashed with the rest of the block header meets certains conditions. This process requires a lot of computing capacity, but in return the miner obtains a monetary reward, so there are many users who want to win this competition.

When a block is mined, new transactions are published in the blockchain, making them public for all the nodes of the network, so all of them can verify that every transaction is valid, and no irregularity is committed as a double spend of the same amount of money. In addition, these transactions are published without information from the person who makes or receives them, only the public address of the sending or receiving wallet is known. This pseudo-anonymity turns cryptocurrencies into an attractive way of payment for criminals, and makes really difficult the follow-up tasks for the Security Forces.

Therefore, in this Bachelor Thesis I will develop a system that allows us to obtain certain clarity when following the movements of some suspicious wallets, looking at the transactions in which they are involved or obtaining the information found in the chain of blocks .

Keywords

Bitcoin, Block, Blockchain, Cryptocurrency, Mining, Transaction

Agradecimientos

A mis padres y a mi hermana Irene, a mis amigos, y a mi novia Adriana, por apoyarme siempre incondicionalmente.

Gracias por aconsejarme siempre que lo he necesitado y aguantarme y soportarme cuando ni yo mismo lo he hecho.

A todos los profesores que he tenido en mi etapa de estudiante, desde los del colegio hasta los de la universidad, por transmitirme sus conocimientos y formarme hasta ser lo que soy ahora.

Todos han pasado por mi vida y dejado su huella y entre todos me han ayudado a conseguir este logro.

Muchas gracias.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. Introducción

1.1. Motivación

Las criptomonedas son un medio digital de intercambio, una alternativa a las divisas tradicionales. Lo que las hace especiales es que usan la criptografía tanto como para crear nuevas unidades como para asegurar las transacciones y garantizar su seguridad e integridad. Además, a diferencia del dinero tradicional, que necesita de una entidad central que lo gestione, normalmente un banco o un gobierno, las criptomonedas son un sistema totalmente distribuido y descentralizado. Las transacciones se realizan entre dos usuarios (*peer to peer*), y se almacenan en un gran registro de cuentas que es la cadena de bloques o *blockchain*. Las monedas se generan en un proceso llamado minado, que puede realizarlo cualquier usuario con la suficiente capacidad de computación.

Por tanto, la aparición de este dinero criptográfico, seguro, global, descentralizado y anónimo, supone un cambio de paradigma respecto a lo que estábamos acostumbrados. No hay duda de que estas nuevas divisas nos proporcionan beneficios tanto a los usuarios individuales, como a las instituciones financieras, o incluso a gobiernos e instituciones públicas ya que facilitan el acceso a los productos financieros, ayudan al crecimiento económico y reducen los riesgos de corrupción y fraude. Pero uno de los riesgos más significativos que aparecen con las criptomonedas es la capacidad de los criminales y terroristas para usar estas nuevas tecnologías para sus propios beneficios [1].

Las razones por las que los criminales se están beneficiando de estas tecnologías son bastante variadas. El anonimato que estas redes proporcionan es posiblemente la más importante de ellas, puesto que aunque toda operación y transacción queda grabada en la cadena de bloques, no se encuentra en ella nada relacionado con el nombre, dirección física o cualquier tipo de identificación ni del pagador ni del receptor, únicamente las direcciones donde se guardan las monedas (monederos). Esto supone una gran ventaja a la hora de delinquir, hacer compras y realizar gastos de dudosa moralidad o legalidad, puesto que para las Fuerzas y Cuerpos de Seguridad del Estado resulta muy complicado identificar a los propietarios de los monederos o carteras que contienen esas direcciones.

Gracias a un estudio realizado en 2015 por Europol [2], se sabe que más de un 40% de las transacciones ilícitas llevadas a cabo en la Unión Europea se han realizado con Bitcoin (BTC), y este porcentaje ha podido incrementarse en la actualidad debido a los beneficios de confianza, credibilidad y seguridad que estas monedas proporcionan.

El hecho de que las criptomonedas tengan herramientas que impiden el doble gasto del dinero, hace que no se puedan duplicar gastos y operaciones, por lo que también los criminales se sienten seguros frente a otros delincuentes que pudieran estafarles a ellos.

A raíz de este más que posible uso delictivo de las criptomonedas surje el interés de las Fuerzas y Cuerpos de Seguridad del Estado, y más concretamente de la Guardia Civil de desarrollar un sistema que ayude a monotorizar movimientos extraños o sospechosos, y es en ese contexto donde surge la idea de desarrollar este trabajo.

1.2. Objetivos

El objetivo por tanto de este Trabajo de Fin de Grado es llevar a cabo un estudio de la cadena de bloques, comprender cómo se minan, conseguir obtener de ellos la información que contienen, y ser capaces de tratar esta información, de manera que podamos diseñar un sistema que, a partir del análisis de la cadena de bloques de una criptomoneda en particular, Bitcoin, sea capaz de seguir el rastro a determinadas operaciones, o mostrar la información más relevante de un bloque, una transacción o una dirección pública (monedero).

El hecho de que la *blockchain*, que guarda un registro de todas las operaciones y transacciones que se realizan en la red, sea de acceso público hace que cualquier persona con unos mínimos conocimientos informáticos sea capaz de seguir el rastro de una serie de direcciones que sean consideradas sospechosas.

Sin embargo, la existencia en la red de "*mixers*" o "*tumblers*" hace que este proceso sea exponencialmente más complejo. Estos servicios son utilizados por los delincuentes para "lavar" el dinero, ya que se dedican a mezclar las monedas de diversos usuarios, haciendo imposible seguir el rastro. El procedimiento es el siguiente, un usuario envía su dinero a un servicio anónimo que le responderá enviándole la misma cantidad pero en criptomonedas que pertenecían a otros usuarios [3].

1.3. Organización de la memoria

La memoria se divide en cinco capítulos, además de los apartados de Referencias y Glosario, y un breve resumen, en castellano y en inglés al principio del trabajo. A continuación, se describe el contenido de cada uno de ellos.

El primer capítulo se trata de una introdución al trabajo. En ella se plantea de manera general el problema que tenemos, lo que ha motivado a realizar este trabajo y se describen los objetivos del mismo.

Esto deriva al segundo capítulo, donde abordamos el qué se debe hacer. Este capítulo contiene una descripción detallada de la criptomoneda utilizada en particular en mi investigación, Bitcoin, así como de la tecnología de bloques en la que se basan esta y todas las demás criptomonedas existentes en la actualidad.

En el tercer capítulo se describirá el diseño del sistema web que he desarrollado, así como la información que somos capaces de obtener de cada una de las entidades que componen esta tecnología.

En el cuarto capítulo se detalla sobre la implementación del sistema, además de explicar las bibliotecas que se han utilizado, y se verán algunas pruebas de su funcionamiento y los resultados y datos que este sistema es capaz de proporcionarnos.

Por último, en el quinto y último apartado se presentan las conclusiones, y se proponen líneas que quedan abiertas para el trabajo futuro.

Finalmente se incluye un apartado con las referencias utilizadas durante todo el proceso de estudio y que son citadas durante el trabajo, y un glosario con alguna definición básica aclaratoria.

2. Requisitos

2.1. Estado del arte

En este trabajo, para poder realizar el estudio y análisis de la trazabilidad, he decidido utilizar como criptomoneda el Bitcoin (BTC). Me decanté por ella debido a que, además de ser la primera en nacer y la más popular, es la que más valor tiene y su uso está más extendido.

El 31 de octubre de 2008 se publicó un artículo de divulgación cientifica titulado "*Bitcoin: A peer-to-Peer Electronic Cash System*" [4]. El autor de esta publicación fue Satoshi Nakamoto, que todavía a día de hoy no se sabe si se trata de una persona real, una persona bajo un pseudónimo o una organización o grupo de personas que prefieren mantener el anonimato. Hay multitud de teorías sobre este hecho, pero ninguna está confirmada. Lo que si está claro es que Satoshi Nakamoto, sea quien sea, es el creador del protocolo Bitcoin (además de su cliente de referencia, *Bitcoin Core*) y que sentó las bases de toda la tecnología *blockchain* que conocemos.

En dicho artículo, se describe por completo el protocolo Bitcoin y su funcionamiento. Se detalla el problema existente, y se propone una serie de soluciones que llevadas a cabo solucionarían este inconveniente. El problema viene ocasionado por el incremento de las compras y del comercio a través de Internet. Esto ha provocado que haya que confiar en instituciones financieras ajenas a la operación que se desea tramitar, para que se encarguen de procesar estos pagos electrónicos. El coste de esta mediación incrementa el coste de las transacciones, aunque bien es cierto que aporta una seguridad y confianza tanto para el emisor como el receptor, ya que esta institución confiable evita que se produzcan situaciones de fraude.

Por tanto, para solucionar esto, la propuesta de Satoshi Nakamoto fue una versión puramente entre pares, *peer-to-peer,* de pago electrónico en la que se permite a un usuario enviar directamente hacia otro una serie de pagos de manera online y prácticamente inmediata. El mecanismo de firma digital solucionaba parte del problema, pero seguía siendo necesaria una tercera parte intermediaria que previniera sobre el doble gasto. El doble gasto es un problema potencial del dinero digital, por el que una misma unidad puede gastarse en más de una ocasión. Esto se produce cuando el archivo digital que contiene a las monedas puede duplicarse o falsificarse. Para evitar que esto ocurra, la solución propuesta por Nakamoto utiliza un protocolo criptográfico basado en pruebas de trabajo que evita la necesidad de una tercera parte confiable que valide las transacciones.

Estas transacciones se almacenan *hasheadas* en la cadena de bloques (*blockchain*) que no es otra cosa que un gran libro de contabilidad que lleva un registro de todas las transacciones realizadas en la historia de esta criptomoneda. Estos registros no se pueden alterar sin volver a superar la prueba de trabajo, por lo que alterar una transacción ya almacenada se trata de una tarea prácticamente imposible, y que se hace más difícil todavía a medida que sigue creciendo la cadena de bloques.

Una moneda electrónica se define en el ensayo de Satoshi Nakamoto como una cadena de firmas digitales. Un usuario que posee una cantidad de criptomonedas y que quiere transferírselas a otro, lo hace firmando digitalmente un *hash* de la transacción previa y la clave pública del receptor, y añadiendo esto al final de la moneda. El receptor puede verificar las firmas con su clave privada para comprobar la cadena de pertenencias y obtener acceso a su dinero y ser capaz de gastarlo.

Un *hash* es un algoritmo matemático determinista que, dada una entrada, la cifra y devuelve una salida de longitud fija, independientemente del tamaño que tuviera la entrada. Este algoritmo tiene que ser muy sencillo y rápido de calcular, ya que se pueden necesitar miles de *hashes* por minuto; sin embargo debe ser no reversible, es decir, dado un *hash* debe ser muy difícil obtener la entrada que lo generó. Hay multitud de ejemplos de funciones *hash*, pero la que nos interesa es la que Satoshi decidió que iba a usar Bitcoin, que fue SHA256. Su decisión fue muy acertada, ya que ese mismo *hash* ha sido usado en la mayoría de las criptomonedas existentes con resultados muy positivos.

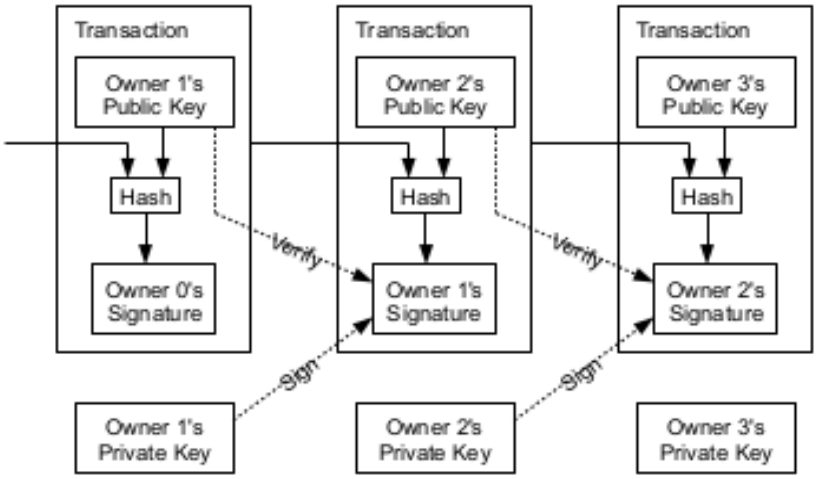

Figura 1: Cadena de firmas digitales

Cada transacción contiene uno o más *inputs*, que son débitos contra una cuenta de Bitcoins, y uno o más *outputs*, que son créditos añadidos a una cuenta de Bitcoins. Estas entradas y salidas no necesariamente tienen que sumar el mismo valor. De hecho, lo habitual es que la suma de los *outputs* sea ligeramente inferior a la suma de los *inputs*, ya que esta diferencia, conocida como propina de la transacción, es la cantidad de Bitcoin que serán pagados al minero que incluya esta transacción en la *blockchain*.

Estas transacciones son pseudoanónimas, ya que no incluyen ningún dato de la persona física que las realiza, ni de su dirección física o ubicación, tan solo una dirección de su monedero. Esta dirección es pública, y se asemeja al número de cuenta bancaria, es el lugar al que se deben enviar los fondos para realizar un pago. Esta dirección se genera a través de la clave pública y la clave privada, que son claves criptográficas usadas para firmar electrónicamente y poder gastar los fondos asociados a dicha dirección. Las direcciones se pueden generar muy fácilmente, y de manera prácticamente instantánea. Es

gratuito y se puede hacer tantas veces como se quiera, por lo que es común que sean usadas para un sólo uso y luego ser desechadas o no volver a usarse nunca más. El número total de direcciones diferentes que pueden existir en la red de Bitcoin es de $2^{160.}$, y según [5], para quedarnos sin direcciones, cada humano que actualmente vive en la tierra (más de 7,5 miles de millones) debería generar 500 millones de direcciones cada nanosegundo(10^{-9}) durante la totalidad de la edad del universo (15 mil millones de años), por lo que se podría considerar que son infinitas.

Una de las propiedades más curiosas que tiene el protocolo Bitcoin es que el número de monedas que existirán en la red es finito y fue definido por Satoshi Nakamoto. Esto convierte al Bitcoin en una moneda deflacionaria, al igual que ocurre en el caso del oro. La cifra máxima de Bitcoins que podrá haber será de 21 millones, y la pregunta natural que surge es que pasará en el momento que se alcance esa cantidad.

En cada bloque que se mina y se añade a la cadena, se recogen una serie de transacciones entre pares, pero también hay una transacción especial en cada uno de ellos, que se conoce como *Coinbase transaction.* Esta transacción recoge todas las propinas de las transacciones añadidas en ese bloque, y además genera unas monedas nuevas que se añaden junto a las propinas a la cartera del minero. Es la única transacción del bloque sin origen y sirve como recompensa o premio al minero por haber sido quien ha validado el bloque. Cada 210000 bloques generados en la cadena el valor de la recompensa se reduce a la mitad. La recompensa comenzó en 50 BTC en 2009, y actualmente está en 12,5 BTC. La próxima bajada lo colocará en 6,25 BTC y hay quien dice que debido al alto valor de dificultad y el coste de minado puede que ya no sea rentable invertir en ello.

En la actualidad, ya se han minado más de 17,5 millones de BTC, por lo que puede parecer que el fin está cerca, pero como la dificultad del minado se va ajustando, los expertos estiman que no será hasta 2140 cuando se llegue al 100% de monedas minadas.

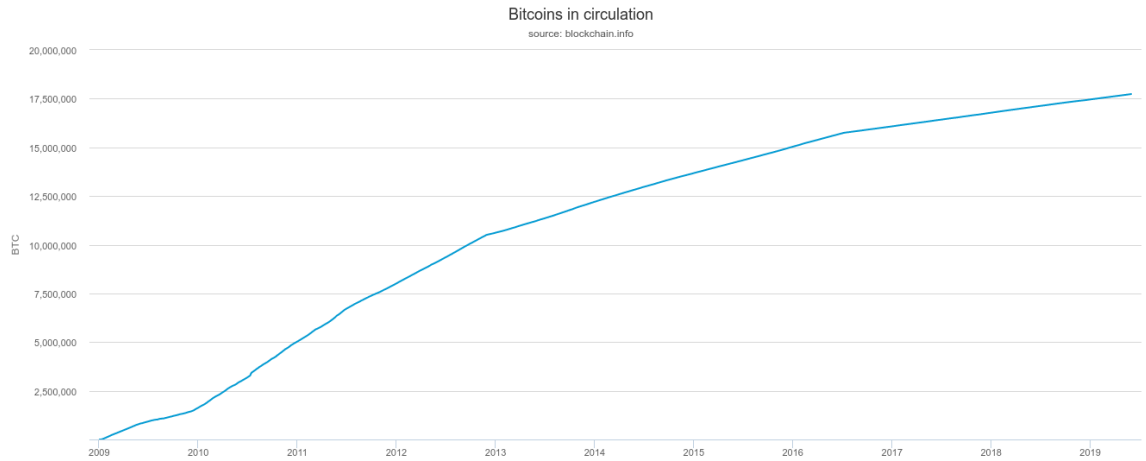

Figura 2: Bitcoins en circulación

El Bitcoin, como divisa, es una unidad divisible. Al igual que un euro está fraccionado en cien céntimos, un dólar está subdividido en cien centavos o una libra está formada por cien peniques, un Bitcoin se puede fraccionar hasta en 10^8 unidades más pequeñas e indivisibles conocidas como satoshis, en honor a su creador. Por tanto, 1 BTC = 100.000.000 satoshis, y 1 Satoshi = 0.00000001 BTC.

El precio del Bitcoin, está determinado por todo aquel que participe en el proceso de compra y venta, ya que se rige por la ley de oferta y demanda. Por tanto, no existe un valor único y fijo para el Bitcoin, sino que es variable con el tiempo.

Desde su inicio, en los dos primeros años apenas hubo evolución, pero fue en 2017 cuando comenzó una subida exponencial y el uso del mismo se aceleró [6]. Hasta esta época los principales usuarios de Bitcoins eran los mismos usuarios de la *Deep Web*. Todo el gran mercado negro de actividades ilegales de cualquier tipo (drogas, sicarios, armas, material pedófilo, etc.) estaba en la red oculta. Estos usuarios gozaban de un anonimato muy necesario para sus tareas en la red Tor, y cuando surgió una moneda que también guardaba su anonimato se lanzaron a utilizarla en masa. Por eso no se consideraba en un principio a Bitcoin como una alternativa seria. Tenía la reputación de ser una tecnología para pagar y financiar actividades ilícitas y no tenía muchos más usos que ese, por lo que en el mundo real no se aceptaban pagos con esta divisa, y cualquier operación realizada con Bitcoins de algo real y tangible se convertía en una noticia.

La primera ocasión en la que alguien logró comprar algo fuera de la red ocurrió el 22 de mayo de 2010, cuando un hombre llamado Laszlo Hanyecz compró a Domino's Pizza, dos pizzas grandes a cambio de 10.000 BTC. Este desarrollador entró en la historia tanto por haber realizado la primera transacción real de Bitcoin como por haber comprado las pizzas más caras de la historia, que llegaron a valer más de 19 millones de dólares al cambio en diciembre de 2017. Desde entonces, cada 22 de mayo se celebra en las redes el "*Bitcoin Pizza Day*", y las redes sociales se inundan de fotografías de gente comiendo pizzas o diferentes alimentos pagados con Bitcoins.

El valor máximo que hasta el momento ha logrado alcanzar el Bitcoin fue de más de 19.000$, a mediados de diciembre de 2017. El crecimiento durante ese año fue desmesurado. Una pequeña inversión de 100€ en enero de 2017 habría permitido retirar en diciembre más de 2.000€. Posteriormente sufrió una caída que hizo pensar que la burbuja había estallado, pero en el momento de escribir este trabajo, vuelve a estar de nuevo al alza, habiendo aumentado más del doble su valor en los últimos seis meses.

Figura 3: Precio del Bitcoin en dólares

Todas estas circunstancias anteriormente comentadas, el hecho de que las transacciones sean anónimas, el sistema descentralizado y basado en la *blockchain*, que no está regulado por ningún estado ni institución financiera sino por el propio protocolo que es de código abierto, el número limitado de Bitcoins en la red, y el valor que lo coloca como la croptomoneda más monetizada convierten a esta divisa en un interesante objeto de estudio, y es a lo que me he dedicado en este Trabajo de Fin de Grado.

2.2. Tecnología de bloques

Tanto el Bitcoin como las demás criptomonedas no serían nada sin el protocolo sobre el que se apoyan, que no es otro que el protocolo *blockchain.* Este protocolo utiliza una cadena de bloques como notario público, descentralizado y no modificable, en el que se almacenan todas las transacciones con el fin de evitar que no se puedan gastar dos veces las mismas monedas.

La estructura de datos de la cadena es una lista enlazada y ordenada de ficheros denominados como bloques. Los bloques están enlazados con el inmediatamente anterior, formando una cadena que comienza con el bloque génesis, el primero de la cadena. Una visualización habitual de esto es como si fuera una pila vertical, con los bloques apilados uno encima del otro, y el bloque génesis abajo sosteniendo a todos. Esta visualización nos ha hecho adoptar términos como "*height*", altura, para referirnos a la distancia de un bloque al primero, o "*top*" para hablar del último bloque minado, el último bloque en añadirse [7].

Esta cadena de bloques es un sistema de almacenamiento de información, como podría ser una base de datos tradicional, pero al ser descentralizado y poseer todos los miembros de la red una copia de la cadena completa, se trata de un sistema mucho más seguro, anónimo y libre de falsificaciones y dobles gastos, ya que para alterar un bloque

se deben alterar todos los que le siguen a lo largo de toda la cadena, lo que lo convierte en una tarea prácticamente imposible de realizarse.

Cada bloque dentro de la cadena está identificado por un *hash*, una especie de identificador que se genera usando el algoritmo critpográfico de *hash* conocido como SHA256 sobre el encabezado del bloque. El enlazado de los bloques para formar la cadena se realiza mediante este *hash*, de manera que cada bloque tiene una referencia al bloque anterior, conocido como su bloque padre, en el campo "*previous block hash*" del encabezado.

Es evidente entonces que cada bloque tiene únicamente un padre. Sin embargo, podría ocurrir que, temporalmente, tuviera varios hijos. Esto se conoce como una situación de *fork*. Ocurre cuando varios hijos distintos son minados casi simultáneamente por diferentes mineros, y todos tienen como bloque padre al último bloque que había en ese momento, por lo que el campo "*previous block hash*" del encabezado es igual para todos.

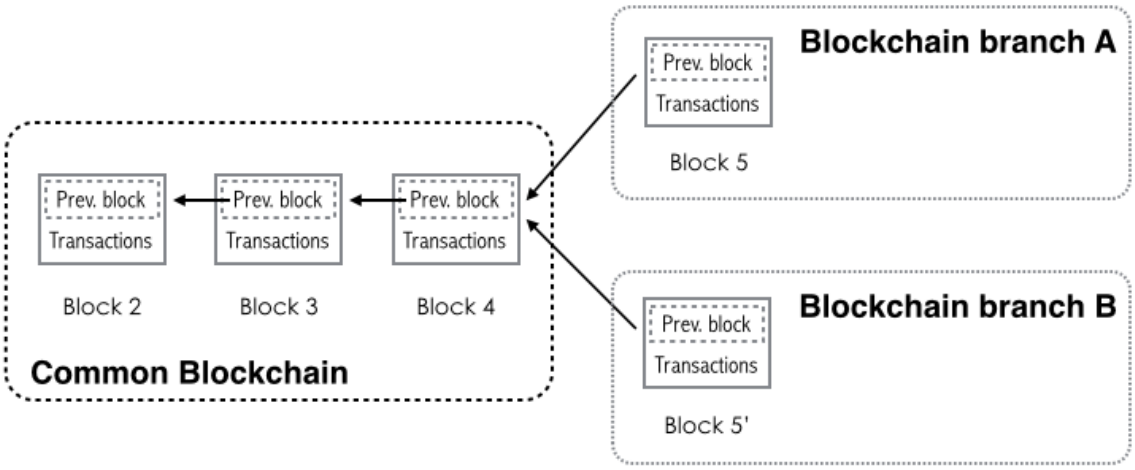

Figura 4: Fork de la cadena de bloques

Esto es una situación cotidiana, que se produce varias veces al día y se soluciona de forma natural con la propia minería de los siguientes bloques. Observemos la figura 4. Vemos que los bloques 2, 3, 4 pertenecen a la cadena de bloques común, pero al llegar al bloque 5 dos mineros lo han calculado prácticamente a la vez y se han formado por tanto dos ramas como las que vemos en la imagen superior. Lo que sucedería a continuación es que los mineros de la red seguirían esforzándose para obtener más bloques válidos y conseguir sus recompensas. Esto generaría nuevos bloques que se añaden a ambas ramas, y ambas van creciendo, lo que puede parecer un problema porque la división sería una realidad, pero no es así ya que de forma natural Bitcoin soluciona el problema dando más peso a la rama que consiga más cómputo, ya que ha solucionado más pruebas de trabajo con mayor dificultad, por lo que se considera una cadena más fiable. Automáticamente la rama perdedora se deshecha y se elimina de la cadena de bloques.

Esta posibilidad de que se produzcan forks que se solucionan con el tiempo y el propio minado, da lugar a que sean necesarias confirmaciones, antes de que una transacción sea considerada correcta e inmutable. Cada bloque posterior al que contiene a una transacción determinada se considera una confirmación. Está estipulado que a partir de seis confirmaciones, es decir, seis bloques minados posteriores a la transacción, esta se considera "inmutable". Puesto que el protocolo regula su dificultad de minado para que se genere un nuevo bloque cada aproximadamente 10 minutos, podemos hablar de que transcurrida una hora una operación está ya aceptada y confirmada por la red.

Minar es el proceso mediante el cual nuevos Bitcoins se incorporan a la red en funcionamiento, y nuevas transacciones se incorporan a la cadena de bloques, por lo que otros tantos Bitcoins cambian de dueño y de monedero en el que se encuentran. Minar también sirve para asegurar el sistema Bitcoin frente a transacciones fraudulentas y dobles gastos. Los mineros le proporcionan poder de procesamiento y de cómputo a la red a cambio de la oportunidad de obtener una recompensa monetaria.

Los mineros validan las nuevas transacciones y las graban en el registro global que es la cadena de bloques. Para ello, deben poseer acceso a toda la *blockchain* actualizada, para poder realizar las comprobaciones como que una cuenta tiene saldo suficiente, o que una transacción no se ha incluido ya en un bloque anterior. Las transacciones nuevas van llegando de forma constante a todos los nodos, y se almacenan en una base de datos de LevelDB que viene incluída en el software de Bitcoin. La misión del minero comienza con elegir, entre todas las transacciones que ahí se encuentran aquellas que sean correctas y válidas, ya que si realizara todo el esfuerzo que minar un bloque conlleva con alguna transacción errónea, el resto de mineros lo detectarían y todo su esfuerzo y su trabajo no habría servido para nada. Algunas de las validaciones que realiza el minero sobre cada una de las transacciones son [8]:

- La sintaxis es correcta
- Ni las entradas ni las salidas están vacías
- El tamaño es menor que el tamaño máximo del bloque (1MB)
- Ninguna de las salidas (ni el total de ellas) es inferior a 0 BTC ni superior a 21 millones BTC
- Ninguna de las entradas tiene *hash* igual a 0
- El tiempo de bloque tiene menos de 31 bytes
- El tamaño de la transacción es al menos 100 bytes
- Se rechaza si ya tenemos transacciones en el pool o en la cadena de bloques iguales (doble gasto)
- Para cada entrada, si la salida referenciada está en cualquier otra transacción del pool se rechaza
- Para cada entrada, si la salida referenciada no se encuentra en la cadena principal, se trata de una transacción huérfana. Se añade al pool de transacciones huérfanas
- Para cada entrada, si la salida referenciada es una transacción *Coinbase* (creación de monedas), esta debe tener al menos 100 confirmaciones, sino se rechaza
- Para cada entrada, si la salida referenciada no existe (nunca ha existido o ya se ha gastado), se rechaza
- Se rechaza siempre que la suma de los inputs sea menor que la suma de los outputs.
- El número de firmas debe ser inferior al límite de dos firmas
- Se rechaza si la propina de la transacción (definida como la suma de los inputs menos la suma de los outputs) es demasiado baja para incluirla en un bloque vacío

De entre todas las transacciones válidas disponibles, escoge todas las posibles hasta rellenar el tamaño máximo de un bloque, y comienza la búsqueda del *nonce* para superar la prueba del trabajo. Esta prueba de trabajo (*Proof-Of-Work*) es la base del modelo de seguridad de Bitcoin, y sirve para asegurar tanto la veracidad de las transferencias (aseguran que el emisor ha firmado correctamente el envío y que dispone de saldo suficiente como para realizarlo), como la veracidad de los bloques (la información de cada bloque es consistente y válida), y consensua la información en la cadena de bloques (deshaciendo *forks* y previniendo de posibles ataques).

La prueba de trabajo fue propuesta por Satoshi Nakamoto desde su primera publicación del *paper* en 2008. La idea era buscar "algo" que fuera muy difícil de calcular y muy fácil de comprobar, para así evitar que individuos con malas intenciones abarrotaran la red con bloques, correctos o no, lo que haría imposible comprobar todos ellos y podrían producirse irregularidades como dobles gastos o transacciones desde cuentas que no tienen los fondos suficientes como para realizarlas. Este "algo" se conoce como *nonce*, e introduce el concepto de complejidad al proceso de creación (y minado) de un bloque.

El *nonce* es un campo numérico de 32 bits (4 bytes) que se genera por los mineros de forma aleatoria o secuencialmente dentro del bloque, con el objetivo de que, al calcular el *hash* que representa a dicho bloque, éste comience por varios ceros consecutivos. Como ya sabemos, el algoritmo criptográfico de *hash* que se usa en este protocolo es SHA256, y tiene la peculiaridad de que hacer el camino inverso, es decir, a través del *hash* obtener la entrada es de una complejidad abrumadora. Por tanto, no hay otro método para calcular el *nonce* que el ensayo y error, es decir, ir probando números "a lo bruto", hasta que con alguno se consiga el objetivo de que el *hash* comience por un número determinado de ceros.

Aquí entra el concepto de dificultad. El algoritmo de prueba de trabajo define para toda la red la dificultad de crear un nuevo bloque válido y añadirlo a la red. Esta dificultad se guarda en el encabezado del bloque, para que pueda ser comprobada por otros mineros una vez que alguien haya encontrado la solución. Esta dificultad viene representada en una notación conocida como "bits de dificultad" o únicamente "bits", y se expresa en un formato coeficiente/exponente, con los dos primeros dígitos hexadecimales correspondientes al exponente y los seis siguientes dígitos al coeficiente. La fórmula para calcular la dificultad es : dificultad = coeficiente*$2^{(8*(\text{exponente}-3))}$, lo que nos proporcionará un número que. si lo convertimos a hexadecimal marca la cota superior para el *hash* del encabezado del bloque. Es decir, un bloque será válido (en cuanto a que cumple la prueba de trabajo) si el *hash* del encabezado es menor que la dificultad calculada anteriormente.

Hemos visto que la dificultad determina cuanto cuesta encontrar un *nonce* que sea solución para la prueba de trabajo, y sabemos que se va ajustando, pero la pregunta obvia que surge es: ¿por qué se ajusta, quién lo hace y cómo?

Los bloques de Bitcoin se generan cada aproximadamente 10 minutos de media. Esto regula la frecuencia con la que aparecen nuevas monedas y la velocidad con la que se aceptan y se realizan transacciones. Esto debe permanecer constante en la medida de lo posible no sólo a corto plazo, sino también a lo largo de toda la vida de esta

criptomoneda. Se espera que en el futuro cercano, la capacidad de cómputo se continúe aumentando a un ritmo rápido, y también el número de participantes tanto en la red como mineros y máquinas tratando de minar nuevos bloques. Para mantener la frecuencia de generación de bloques en los 10 minutos, la dificultad debe ser ajustada para hacerle frente a estos cambios. De hecho, es un parámetro que se ajusta periódicamente para conseguir esa frecuencia de 10 minutos.

Pero, ¿cómo se puede ajustar, si se trata de una red descentralizada en la que no hay ninguna autoridad central que estipule unas reglas únicas para todos los miembros? La respuesta es que este reajuste ocurre de manera automática y en cada nodo por si mismo. Cada 2016 bloques (aproximadamente 2 semanas), todos los nodos recalculan la dificultad de la prueba de trabajo usando una ecuación que mide el tiempo que ha costado obtener estos 2016 bloques y lo compara con los 20160 minutos esperados. Esta proporción se multiplica por la dificultad existente, y así se obtiene la nueva. De manera que, si los últimos 2016 bloques se han obtenido antes de lo previsto, el cociente será menor que 1, y por tanto al multiplicarlo por la dificultad veremos que se ha reducido, lo que hace que sea más difícil que el *hash* del encabezado sea menor que ese número y por tanto se tardará más tiempo en encontrar un *nonce* válido para cada bloque. En el caso contrario, si en los últimos 2016 bloques se ha tardado más de lo previsto, el cociente será mayor que 1, por lo que el número que marca el objetivo de dificultad será más alto, facilitando la tarea de encontrar un *hash* menor que él y reduciendo así el tiempo medio entre bloques para los próximos 2016.

Esta dificultad de la prueba de trabajo tiene su sentido, además de para garantizar la seguridad de la red y el correcto funcionamiento de la misma, para conseguir que no sea "un regalo" la obtención de nuevas monedas.

Los mineros recogen dos tipos de recompensa por minar: las nuevas monedas generadas en ese bloque y todas las propinas de todas las transacciones que hayan incluido en él. Para ganar estas recompensas y ser merecedores de ellas deben superar el complejo problema matemático anteriormente mencionado, la prueba de trabajo. La similitud con la búsqueda de recompensas como metales preciosos en cuevas es por lo que se conoce a este proceso como minado.

Como hemos comentado anteriormente, los Bitcoins tienen un número máximo de unidades que pueden existir, 21 millones, y puede pensarse que en el momento que se alcance esta cantidad, ya no será atractivo para ningún usuario tratar de minar nuevos bloques. Pero esto no es cierto, ya que cada transacción en la red incluye una propina, en el hecho de que la resta entre los *inputs* de una transacción y sus *outputs* nos da un valor que no está asignado a ninguna cartera. El minero que gana la competición es el encargado de "quedarse con las vueltas", es decir, añade a su monedero todas las diferencias entre los *inputs* y los *outputs* de todas las transacciones incluidas, además de las nuevas monedas generadas. En la actualidad, las propinas representan menos de un 0,5% de la ganancia de un minero, ya que la gran mayoría proviene de las monedas generadas. Pero en el momento que ya no haya más monedas que generar, las propinas deberán aumentarse, para así hacer tu transacción atractiva para que un minero la incluya en su nuevo bloque.

La primera transacción que se añade a cada bloque es entonces una transacción especial. Se la conoce como *Coinbase*, y contiene la recompensa por el esfuerzo para el

minero. Se compone de un pago a su cartera de las monedas generadas, que como sabemos se van reduciendo a la mitad cada 210.000 bloques, y el total de las propinas recolectadas de todas las transacciones que haya podido introducir en su bloque. Es una transacción especial porque no tiene como *inputs* salidas referenciadas de otras transacciones, sino que unicamente tiene un input, el *coinbase*, que genera los Bitcoins de la nada. También tiene un único output, hacia la dirección del monedero del minero. Además, este tipo de transacciones necesitan más confirmaciones que las demás. Si lo habitual es 6 confirmaciones, en las de *Coinbase* son necesarias al menos 100 confirmaciones para poder gastar los Bitcoins generados. Esto se debe a que en caso de haber un fork y tener que deshacer una serie de bloques, las transacciones normales vuelven al pool y entrarán en otro bloque tarde o temprano, pero las *Coinbase* desaparecen porque esos bloques dejan de ser válidos.

Hemos visto que cada bloque es una estructura de datos que agrega transacciones a la red incluyéndolas en la cadena pública, pero ahora vamos a ver la estructura y de qué se compone un bloque. Todos los bloques tienen un encabezado, que sirve para describir el contenido del mismo y para calcular el *hash*, y una larga lista de transacciones que conforman la mayor parte de su tamaño. El encabezado tiene 80 bytes, mientras que la media de transacciones incluidas son al menos 250 bytes, ya que un bloque medio contiene más de 500 transacciones.

Tamaño	Campo	Descripción
4 bytes	Tamaño del bloque	El tamaño del bloque, en bytes
80 bytes	Encabezado	Campos con información sobre el bloque
1-9 bytes (VarInt)	Número de transacciones	Cuántas transacciones contiene el bloque
Variable	Transacciones	Transacciones registradas en este bloque

Tabla 1: Estructura de bloque

El encabezado de cada bloque contiene tres conjuntos de metadatos. En primer lugar se encuentra una referencia al *hash* del bloque anterior, lo que conecta este bloque al anterior de la *blockchain*. A continuación se encuentra otro conjunto de metadatos, que contiene la dificultad, el tiempo Unix (segundos desde la medianoche UTC del 1 de enero de 1970) y el *nonce*, que se usan en el proceso de minado, como ya hemos visto con anterioridad. Por último, el tercer conjunto incluye el *Merkle Tree root*, una estructura de datos que se usa para agrupar eficientemente todas las transacciones del bloque, y que veremos más detalladamente más adelante.

Tamaño	Campo	Descripción
4 bytes	Versión	Número de version, útil para las actualizaciones del software y protocolo
32 bytes	Hash del bloque previo	Referencia al hash del bloque padre (anterior) en la cadena
32 bytes	*Merkle Root*	Hash de la raíz del arbol *Merkle* de las transacciones del bloque
4 bytes	*Timestamp*	Marca de tiempo del momento aproximado de su creación (tiempo Unix)
4 bytes	Dificultad	El objetivo de dificultad del algoritmo de prueba de trabajo para este bloque
4 bytes	*Nonce*	Número que resuelve el problema de la prueba de trabajo

Tabla 2: Estructura del encabezado de bloque

El identificador de cada bloque no es otro que su *hash* criptográfico, obtenido al pasar el encabezado de su bloque dos veces por el algoritmo criptográfico SHA256. La salida consiste en 32 bytes a los que se conoce como *hash* del bloque, aunque sería quizás más adecuado decir *hash* del encabezado del bloque. El *hash* identifica a un bloque de manera única e inequívoca, y es independiente del minero que lo haya calculado, ya que únicamente depende del encabezado del bloque, y todos los nodos de la red pueden calcularlo de la misma manera. De hecho, es lo que hacen para comprobar que el *nonce* que se ha propuesto es válido.

Nos damos cuenta gracias a las tablas anteriores de que el *hash* de un bloque no se incluye en la estructura de bloques del mismo, ni cuando se transmite por la red, ni cuando se almacena en la cadena de bloques. En lugar de eso, se calcula en cada nodo cuando se recibe desde la red, y cada nodo lo puede (o no) guardar en una base de datos independiente, para facilitar el indexado y hacer más rápido el acceso a los bloques del disco.

Otra manera de identificar a un bloque es por su posición en la *blockchain*, lo que se conoce como la altura (*height*) de un bloque. Sin embargo, éste no es un identificador único, ya que puede que en una misma altura haya dos o más bloques compitiendo por esa posición en la cadena de bloques, cuando se haya producido un *fork*.

El primer bloque creado se encuentra en la altura 0, y se conoce como bloque génesis. Este bloque fue creado el 3 de enero de 2009, a las 18:15:05 (GMT), y supuso el verdadero pistoletazo de salida al protocolo Bitcoin. Tanto la estructura como los datos de este primer bloque son ligeramente distintos al resto. Al ser el primer bloque de la cadena, el campo donde debería ir el *hash* del bloque anterior está completamente relleno de ceros, ya que no tiene ningún predecesor. La dificultad también es especial en este

bloque, ya que se definió como 1. A partir de aquí, y cada 2016 bloques como hemos visto se ha ido actualizando en función de las necesidades de la red. La última peculiaridad del bloque génesis es que esconde un mensaje dentro de él. Mientras que el resto de bloques están pensados para almacenar transacciones, éste únicamente contiene la transacción *Coinbase*, en la que se le asignan 50 BTC (la recompensa en ese momento) a la cartera de Satoshi Nakamoto, y en el input de esta transacción se esconde el texto: "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*". Esto no es otra cosa que el titular de la portada del periódico británico *The Times* de aquel día en el que se creó el bloque, lo que proporciona una prueba de la fecha en la que se creó el bloque, y además sirve como recordatorio irónico de la importancia de un sistema monetario independiente y descentralizado, con el lanzamiento de Bitcoin a la vez que el mundo sufría una crisis económica global sin precedentes.

Cada bloque de la cadena contiene en su encabezado un resumen de las transacciones de ese bloque, conocido como *Merkle Tree*. Estos *Merkle Tree* son una estructura de datos que resumen y verifican la integridad de grandes conjuntos de datos de manera muy eficiente. Son árboles binarios que contienen *hashes* criptográficos. El término "árbol" se usa para describir una estructura de datos ramificada, pero normalmente se representan de arriba hacia abajo, de manera que la raíz está arriba y las hojas en la parte de abajo de los diagramas.

Estos árboles se usan en Bitcoin para resumir todas las transacciones de un bloque, generando una especie de huella digital que nos proporciona un eficiente proceso para verificar si una transacción se encuentra en un bloque o no. Se construyen *hasheando* recursivamente pares de nodos hasta que queda únicamente un *hash*, conocido como raíz o *merkle root*. Una vez más, el algoritmo de *hash* criptográfico que se usa es SHA256, aplicado dos veces en cada ocasión. Cuando un bloque contiene N transacciones, podemos comprobar si una transacción está incluida en él con, como mucho, $2*\log_2(N)$ operaciones, lo que convierte a los *Merkle Trees* en una estructura muy eficiente.

Para construir un árbol de *Merkle*, se comienza desde abajo hacia arriba, comenzando por las hojas (transacciones), hasta acabar en la raíz, que será el *hash* que se incluirá en el encabezado. El procedimiento que se sigue es el siguiente. Las transacciones se *hashean* y este *hash* que resulta se almacena en cada nodo hoja. Los pares consecutivos de nodos hojas se resumen en un único nodo padre. Para ello se concatenan los *hashes* anteriormente calculados y se *hashean* de nuevo. Este proceso continúa recursivamente hasta que únicamente queda un nodo arriba, el nodo raíz *Merkle*. Este *hash* de 32 bytes se almacena en el encabezado y resume todas las transacciones que contiene este bloque.

Como el árbol *Merkle* es un árbol binario, es necesario que exista un número par de hojas en la capa inferior. En caso de que haya un número impar de nodos hojas, el *hash* de la última transacción se duplica para crear un número par de hojas, lo que se conoce como árbol balanceado.

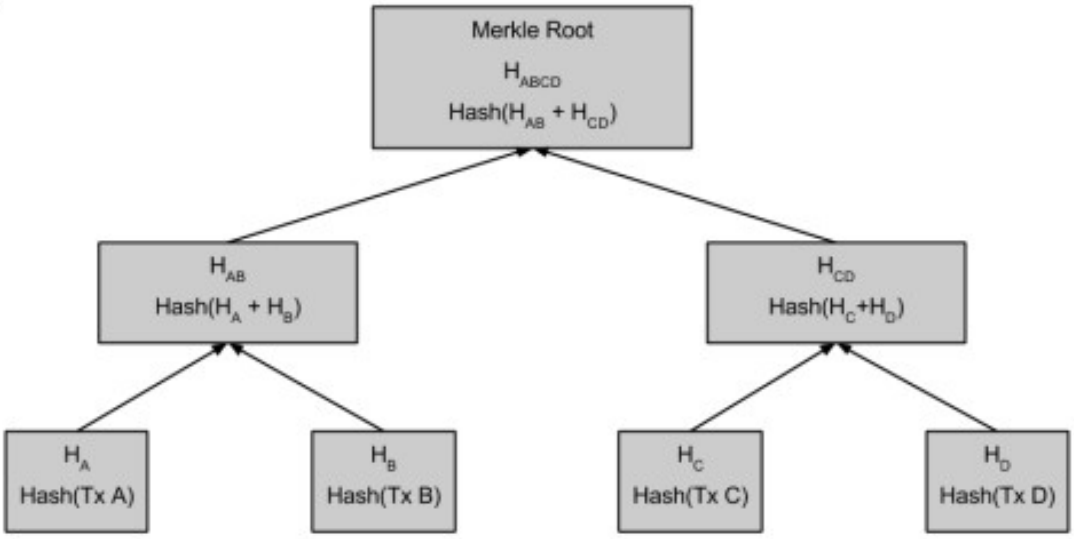

Figura 5: Árbol Merkle

Para probar que una transacción específica está incluida en un bloque, un nodo únicamente tiene que producir $\log_2$ (N) *hashes* de 32 bytes, que formen un "camino de autenticación" o "*merkle path*" para conectar la transacción específica con la raíz del árbol. Esta es la gran ventaja de los árboles *Merkle*, puesto que aunque se incremente el número de transacciones, el logaritmo en base 2 de ese número crece mucho más lentamente. Esto permite a los nodos producir eficientemente caminos de diez o doce *hashes* (320 – 384 bytes) que pueden demostrar evidencias de una única transacción entre las más de mil que caben en un bloque de tamaño máximo.

Estas son las características principales que posee la tecnología de bloques, esa revolución cuya primera piedra fue sentada por Satoshi Nakamoto y su protocolo Bitcoin en 2008, y que gracias a sus algoritmos de *hash* criptográficos (SHA256), a la dificultad ajustable y autorregulada, a las recompensas que se le otorgan a los mineros y a la descentralización en una red P2P (*peer-to-peer,* entre pares), supone un nuevo paradigma a la hora de garantizar la seguridad en la red y llevar un registro público de todas las transacciones.

El hecho de que ese registro de transacciones se encuentre de forma pública en la cadena de bloques, ha permitido que se puedan crear herramientas que nos ayuden a estudiar la trazabilidad, es decir, ver de dónde a dónde se producen transacciones, por cuánta cantidad de Bitcoins y detectar patrones en conductas sospechosas. Algunos ejemplos de este tipo de aplicaciones son *Mirror* [9] o *Chainalysis* [10]. La primera estudia la trazabilidad de una cadena de bloques de un modo más general, no únicamente para transacciones de criptomonedas, sino que también dispone de casos de uso para *blockchains en* otros sectores como por ejemplo en cadenas de producción y distribución, en procesos administrativos, en educación o en sanidad. La segunda, sin embargo, es más específica para este tema, ya que se trata de un *software* que sirve de ayuda a las instituciones legales y financieras para identificar y detener a los usuarios de criptomonedas que llevan a cabo un uso ilícito de ellas.

3. Diseño

En este capítulo vamos a describir el diseño y arquitectura del sistema web que he desarrollado, justificando alguna de las decisiones de diseño tomadas más importantes y destacables, así como un análisis de la información que obtenemos de cada una de las entidades que componen la *blockchain* de Bitcoin.

3.1. Arquitectura

Para desarrollar este sistema que sea capaz de analizar la cadena de bloques y permitirnos estudiar la trazabilidad de las operaciones realizadas en la red de Bitcoin, he decidido implementar un sistema cliente-servidor, y más específicamente una aplicación web.

La arquitectura cliente-servidor se basa en el hecho de que los clientes realizan peticiones a un sistema conocido como el servidor, que les proporciona las respuestas. Algunas de las ventajas de esta arquitectura, y por las que he decidido usarla en mi implementación son la centralización del control en un servidor único y el fácil mantenimiento al estar distribuidas las funciones y responsabilidades entre los posibles clientes y el servidor.

Una aplicación web es una herramienta que los usuarios utilizan accediendo a un servidor web a través de Internet o de una intranet mediante un navegador. Las aplicaciones web son muy populares debido a que son accesibles con independencia del sistema operativo desde cualquier navegador web, y es muy sencillo actualizar y mantener aplicaciones web sin la necesidad de distribuir e instalar *software* a los usuarios potenciales.

El sistema que he implementado se trata de una aplicación web que permite obtener toda la información que la cadena de bloques nos puede mostrar. Gracias a él, he sido capaz de llevar a cabo un estudio y análisis de la trazabilidad de las operaciones realizadas, de manera que se pueda seguir el rastro, en la medida de lo posible, de algunas operaciones “sospechosas”.

El objetivo es diseñar un sistema directamente utilizable por funcionarios policiales. Estos funcionarios, aunque son expertos en la resolución de crimenes, no son generalmente expertos en el uso de la tecnología. En este contexto, para dotar de facilidad de manejo al usuario, el sistema se compone de pocas pantallas, con pocos botones, desde los que podemos obtener mucha información. Esto lo convierte en un sistema muy intuitivo, de manera que cualquier persona pueda utilizarlo, sin ser necesario tener unos conocimientos muy avanzados sobre el protocolo Bitcoin, o sobre la tecnología de bloques que usa *blockchain.*

3.2. Organización de la funcionalidad e interfaz

Todas las páginas del sistema tienen en su parte superior una barra de navegación, que nos permitirá movernos entre las diferentes secciones y acceder de nuevo al inicio rápidamente. Las secciones que tenemos, además de la página principal son, bloque, transacción, dirección y grafo.

Como página de inicio tenemos un index, donde encontraremos un formulario con una serie de *inputs* que actúan como buscadores, que nos permiten encontrar la información deseada, bien buscando por *hash* de bloque, por posición en la cadena, por *hash* de transacción o por dirección de una cartera. Además, podremos obtener la información actualizada sobre el último bloque que haya sido minado y añadido a la cadena principal, por si tuviéramos algún interés en ver las últimas transacciones, aunque éstas aún no hayan recibido todas las confirmaciones necesarias.

La sección del bloque nos muestra dos campos de entrada para buscar bien por el *hash* de un bloque, o bien por el número que ocupa en la cadena principal, siendo el bloque 0 el conocido como bloque génesis, publicado por Satoshi Nakamoto en 2009 y que es el origen del protocolo Bitcoin. Desde cualquier bloque de la cadena, siguiendo los enlaces hacia el bloque anterior, llegaríamos a este bloque, observando durante el camino todas las operaciones realizadas durante la corta pero productiva historia de esta criptomoneda. Además, en caso de que hayamos introducido algún campo correcto en estos buscadores (o en los de la página de inicio), obtendremos la información del bloque buscado.

La sección de las transacciones cuenta con un buscador en el que podremos introducir el *hash* de una transacción, y se nos mostrará la información de dicha operación.

En la sección de dirección también aparece un buscador, para esta vez introducir la dirección pública, y poder sacar la información acerca de las operaciones en las que ha participado o el dinero que ha movido o posee aún en su poder.

Por último, la sección de grafo nos muestra con un simple grafo dirigido las operaciones en las que se vea involucrada la dirección que se haya tratado de localizar en el buscador que esta página dispone. Además, también incluye una tabla donde se pueden ver todos los nodos que forman parte de este grafo, además del tipo de transacciones que realizan (entrada, salida…)

En la sección 4 encontraremos capturas de pantalla de todas las páginas de la aplicación, así como breves explicaciones de la información mostrada.

3.2.1. Bloque

Los campos que considero importantes, y por lo tanto, se muestran al realizar la búsqueda por bloque son los que se observan en la tabla 3. Aunque existan dos métodos para buscar un bloque, tanto por *hash* del bloque como por su altura o posición en la cadena principal, los campos que se muestran en ambos casos son los mismos. He decidido pasar por alto información como el index, el *nonce*, o la dificultad, porque creo que la información que aportaban era irrelevante.

Campo	Descripción
Versión	Número de version, útil para las actualizaciones del software y protocolo
Bloque Anterior	Referencia al hash del bloque padre (anterior) en la cadena. Contiene un hipervínculo para obtener su información
Raíz Merkle	Hash de la raíz del arbol *Merkle* de las transacciones del bloque
Momento de Publicación	Fecha de publicación del bloque en la cadena de bloques. Horario peninsular español
Cadena Principal	Campo booleano que indica si este bloque pertenece a la cadena principal o por el contrario se encuentra en alguna rama de un fork
Altura	Posición del bloque en la cadena, siendo el 0 el bloque génesis
Tamaño	Tamaño en bytes que ocupa el bloque, incluyendo el encabezado
Bits	Bits que componen el bloque
Número de Transacciones	Número de transacciones registradas por este bloque en la *blockchain*
Total Valor	Suma del total de BTCs en todas las operaciones que incluye este bloque
Propina	Suma total de las propinas de todas las transacciones que va a recolectar el minero
Recompensa	Recompensa ganada por el minero por minar este bloque
Transacciones	Lista de transacciones que se incluyen en este bloque

Tabla 3: Información obtenida de bloques

Para mostrar la lista de transacciones, que suele ser muy larga y extensa, he decidido que se muestre únicamente el *hash* de la transacción, con un hipervínculo para acceder a ella y obtener toda la información, el momento en que fue realizada y una lista con el valor de los *outputs* que se envían en dicha transacción, por si fuera interesante ver las que más dinero mueven o las que lo reparten entre más direcciones.

3.2.2. Transacción

En el caso de las transacciones, al realizar la búsqueda por el *hash* de transacción, o acceder a través de algún enlace a esta página, nos encontramos con los campos que se describen en la tabla a continuación.

Campo	Descripción
Versión	Número de versión, útil para las actualizaciones del software y protocolo
Altura de su Bloque	Posición del bloque que la contiene en la cadena, siendo el 0 el bloque génesis. Contiene un hipervínculo, para obtener su información
Momento de la Transacción	Momento en que se realizó la transacción. Horario peninsular español
Hash de la Transacción	Hash de la transacción. Útil para identificarlas dentro de la cadena, y poder obtener comprobar que no se produzcan dobles gastos
Tamaño	Tamaño en bytes que ocupa la transacción dentro del bloque
Doble gasto	Campo booleano que indica si alguna de las monedas usadas en esta transacción se han usado en otras transacciones, intentando un fraude que la red evitaría
Total Valor Entrada	Suma total de los valores de las entradas de la transacción
Total Valor Salida	Suma total de los valores de las salidas dela transacción
Propina	Diferencia entre los dos valores anteriores. Las monedas no asignadas a ninguna salida las recoge el minero a modo de propina por haber incluido esta transacción en el bloque
Entradas	Lista con las entradas de la transacción
Salidas	Lista con las salidas de la transacción

Tabla 4: Información obtenida de transacciones

Para que sea fácil comprobar si una cantidad de dinero se está usando por primera vez, o si por el contrario ha sido ya utilizada y se está tratando de cometer un doble gasto, las transacciones se almacenan sin encriptar en la cadena. Las entradas o *inputs* son referencias a salidas o *outputs* de transacciones anteriores, de manera que es muy sencillo comprobar si esa dirección dispone aún de ese dinero o ya lo ha gastado en otra operación.

En esta página se muestra la lista de *inputs* y de *outputs*, dando de cada uno la dirección de la que provienen y la cantidad que aportan. La suma total de las cantidades de los *outputs* no puede ser superior a la de los *inputs*, pero si podría ser inferior, y esta sería la cantidad que se aportaría como propina al minero. Este hecho implica que pueda darse el caso de que una dirección esté tanto en la lista de *inputs* como de *outputs*. Si por ejemplo tuviéramos 5 BTC disponibles en nuestra cartera de una transacción anterior, pero entre todos los *outputs* solo asignamos 3 BTC, y nos parece demasiada propina 2 BTC, podríamos añadir un nuevo *output* con nuestra dirección y enviar ahí los 2 BTC restantes como si fuera el cambio en una compra tradicional.

3.2.3. Dirección

Al entrar en la página en la que podemos apreciar los datos sobre una dirección de una cartera de Bitcoin, los campos que obtendremos los podemos ver en la siguiente tabla. Además, dispondremos de un botón que nos permitirá observar el grafo de las transacciones en las que esta dirección se ha visto involucrada, para una comprensión mucho más visual que con direcciones *hasheadas*.

Campo	Descripción
Hash 160	Hash de la transacción usando doble hash (SHA256 + RIPEMD160)
Número de Transacciones	Número de operaciones en las que la dirección ha participado, tanto de entrada como de salida
Total Recibido	Cantidad total de Bitcoins que han entrado en la dirección analizada
Total Enviado	Cantidad total de Bitcoins que han salido de la dirección analizada
Balance Final	Diferencia entre los dos campos anteriores, indica la cantidad de dinero disponible actualmente en esta dirección
Últimas Transacciones	Lista con las 50 últimas transacciones en las que esta dirección ha participado

Tabla 5: Información obtenida de direcciones

Las direcciones de Bitcoin deben ser compartidas públicamente, es decir, para enviar una cantidad a alguien debes conocer su dirección. Se construyen a partir de la clave pública de cada usuario, que anteriormente se ha calculado a partir de la clave privada y consiste en una serie de números y caracteres (a excepción de la letra 'O' mayúscula, el número '0', la letra 'I' mayúscula y la letra 'l' minúscula, para evitar confusiones visuales entre sí y con la letra 'o' minúscula o el número '1', lo que se conoce como codificación *Base-58*). Todas las direcciones tienen entre 27 y 34 caracteres, y comienzan por el número '1' o por el número '3'.

En el sistema he decidido que tan solo se muestren las 50 últimas transacciones en las que ha intervenido la dirección buscada, por simplificar y obtener únicamente los movimientos más recientes, que aporten más información. Se muestra el *hash* de la transacción (con un enlace para ver toda su información), la fecha y hora en la que se realizó y el balance para la dirección que estamos analizando, que es un número positivo si obtiene ese dinero en su cuenta y negativo si envía ese dinero.

3.2.4. Grafo

En la sección de grafo se muestra, además de un buscador como en todas las demás, un grafo dirigido que nos permite visualizar, de manera más cómoda y sencilla las transacciones entrantes y salientes de una dirección determinada. También incluye una tabla con enlaces a los gráficos de las direcciones con las que está conectada la dirección que estamos expandiendo. Esto facilitará la navegación entre direcciones con transacciones en común para el usuario, ya que no tendrá que copiarlas en el buscador.

En esta página he necesitado tomar una serie de decisiones de diseño que me dispongo a explicar a continuación. En primer lugar, para evitar un cúmulo inentendible de nodos y enlaces, he truncado los datos a las 50 últimas transacciones, de manera que nos permita ver los movimientos más recientes y las últimas tendencias en las operaciones de la transacción.

Aún así, en algunos casos en los que las transacciones que una dirección realiza reparte dinero entre muchas otras direcciones, o recibe dinero de muchos *inputs,* como es un caso habitual en los *mixers* o *tumblers*, la disposición inicial queda un gran circulo de nodos casi solapados. Para poder obtener información en estos casos, he añadido la posibilidad de poder mover los nodos y colocarlos en la disposición que el usuario prefiera. Para ello basta con *clickar* y arrastrar un nodo a una zona libre de la página, y éste se fijará en ese lugar, mientras los demás actualizan su posición en función de la fuerza de repulsión que sobre ellos actúa.

En cuanto a los casos en los que hay envíos o recepciones entre las mismas direcciones en distintas transacciones, he optado por sumarlos y agruparlos en uno solo, de manera que si la dirección A envía 1 BTC a la dirección B en la transacción 1, y 3 BTC en la transacción 2, el grafo mostrará únicamente una flecha que una los nodos A y B, con la punta apuntando hacia B, y el valor total de 4 BTC.

Para el valor que muestra la flecha que une dos nodos que sólo están conectados por una transacción, hay cuatro casos distintos:

- En caso de ser una transacción de una dirección a otra, se muestra el valor total de entrada/salida de la transacción analizada
- En caso de ser una transacción de varios *inputs* a un único *output:*
  - Si nuestra dirección forma parte de los *inputs*, se añade el enlace hacia el *output* con el valor total de salida de la dirección en esa transacción
  - Si nuestra dirección es el *output*, se añade un enlace por cada *input*, con el valor correspondiente a cada uno de ellos
- En caso de ser una transacción de un único *input* a varios *outputs*:
  - Si nuestra dirección es el *input*, se añade un enlace por cada *output*, con el valor correspondiente de entrada a cada uno de ellos.
  - Si nuestra dirección forma parte de los *outputs*, se añade enlace desde el *input* con el valor total de entrada de nuestra dirección en esa transacción
- En caso de ser una transacción de varios *inputs* a varios *outputs:*
  - Si nuestra transacción forma parte de los *inputs*, se calcula el valor porcentual que recibe cada *output* sobre el total de los *outputs*, y se añade al enlace con ese *output* un valor igual al porcentaje calculado de la salida total de nuestra dirección en esta transacción.

- Si nuestra transacción forma parte de los *outputs*, se calcula el valor porcentual que aporta cada *input* al total de los *inputs*, y se añade al enlace con ese *input* un valor igual al porcentaje calculado de la entrada total de nuestra dirección en esta transacción.

En cuanto a los colores utilizados, el nodo de la transacción que se ha buscado se representa en color verde, el resto de nodos con los que tiene transacciones en común aparecen con el color azul, y si se trata de un minero, hay un nodo de color rojo que indica la cantidad total de monedas que ha generado, sumada con todas las propinas que ha recolectado.

4. Implementación, pruebas y resultados

Para construir este sistema capaz de llevar a cabo un análisis sobre la trazabilidad de las operaciones con criptomonedas, más específicamente con Bitcoins, he construido una aplicación web usando el *framework* Django [11]. Éste se basa en el patrón de diseño conocido como Modelo-Vista-Controlador, está escrito en Python, y su mayor meta es facilitar la creación de sitios webs complejos.

Para la obtención y manipulación de datos técnicos acerca de la cadena de bloques de Bitcoin, he usado la API gratuita de blockchain para desarrolladores de Bitcoin [12]. Esta API permite obtener la información realizando algunas consultas a través de urls determinadas, pero también dispone de una serie de repositorios en *GitHub* [13], donde se encuentran los módulos oficiales en distintos lenguajes de programación para interactuar con ella, además de las respectivas documentaciones, que son de gran utilidad para comprender su correcto funcionamiento.

En mi caso, he usado el módulo para el cliente en Python llamado *api-v1-client-python*, y más concretamente las funciones que se encuentran implementadas dentro del fichero *blockexplorer.py*, y que a continuación procedo a detallar.

Función	Descripción	Parámetros	Retorno
get_latest_block	Devuelve el último bloque añadido a la cadena principal		Objeto *LatestBlock*
get_block	Devuelve el bloque con el hash indicado	- Hash del bloque (string)	Objeto *Block*
get_tx	Devuelve la transacción con el hash indicado	- Hash de la transacción (string)	Objeto *Transaction*
get_block_height	Devuelve un array de bloques a partir de la altura indicada	- Altura del bloque (int)	Array de objetos *Block*
get_address	Devuelve una dirección y sus transacciones	- Dirección a buscarse en base58 o hash160 (string) - Opcional: filtro para transacciones (FilterType) - Opcional: límite de transacciones a mostrarse (int) - Opcional: Número de transacciones que no se muestran (int)	Objeto *Address*

Tabla 6: Funciones de la API utilizadas

En el fichero *views.py*, dentro de mi aplicación *Criptotracker*, es donde se encuentra toda la lógica del sistema. Es ahí donde se recogen los valores introducidos en los distintos campos de los formularios de búsqueda, donde se llama a las funciones de la API anteriormente comentadas, donde se desglosa la información de los objetos que las funciones devuelven en diferentes variables que son enviadas posteriormente a las *templates*, que actúan como las vistas del patrón Modelo-Vista-Controlador (archivos .html), o donde se opera con alguna de las variables obtenidas para conseguir algún tipo de información de interés para mostrarse, o para conseguir el formato correcto en el que queremos que lleguen a las vistas, como el caso de la creación de un *JSON* para el gráfico de transacciones.

En el fichero *forms.py* se definen los formularios utilizados para realizar las búsquedas. Hay uno general, con campos para el *hash* del bloque, la altura en la cadena, el *hash* de la transacción y la dirección, y un formulario individual para cada uno de ellos, para optimizar el proceso cuando se trate de una búsqueda específica desde una de las páginas de la aplicación.

En las *templates*, los ficheros html que sirven de vistas de la aplicación, he usado *boostrap* [14], en concreto en su versión 3.4.1. Se trata de un *framework*, que facilita considerablemente la maquetación de sitios web. Esto me ha permitido colocar de manera sencilla una barra de navegación en la parte superior para facilitar la experiencia y uso al usuario.

Además, para representar el grafo he usado *d3.js* [15], que es una potente biblioteca de *JavaScript* que sirve para construir una gran variedad de gráficos dinámicos e interactivos para visualizarse en navegadores web, haciendo uso de tecnologías como *svg*. Esta biblioteca permite añadir atributos como fuerza de repulsión a los nodos, lo que lo hace más agradable visualmente ya que tratan de separarse en la medida de lo posible.

4.1. Casos de uso

Procedemos a mostrar ahora el funcionamiento del sistema web mediante una serie de capturas de pantalla de los casos de uso que recoge la aplicación.

4.1.1. Búsqueda de un bloque por hash

Para buscar un bloque a través de su *hash*, introducimos este valor en el buscador de la pantalla principal (Figura 6). En este caso vamos a buscar el bloque con *hash* `000000000000000b9cbeade5667ccd98d1ca489e121ff94011741b75aee980d1`, para que nos sirva de ejemplo. Observamos en las figuras 7 y 8 los resultados e información obtenida. En ellas podemos ver los campos anteriormente citados, además de las primeras transacciones de la lista que contiene.

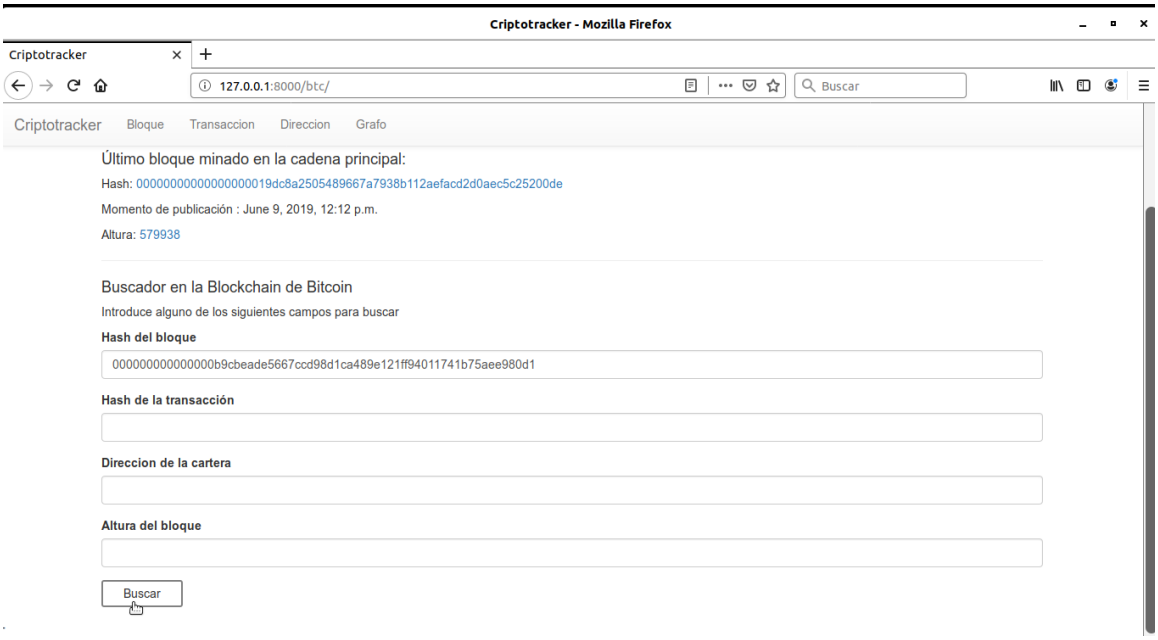

Figura 6: Búsqueda de hash de bloque desde la página principal

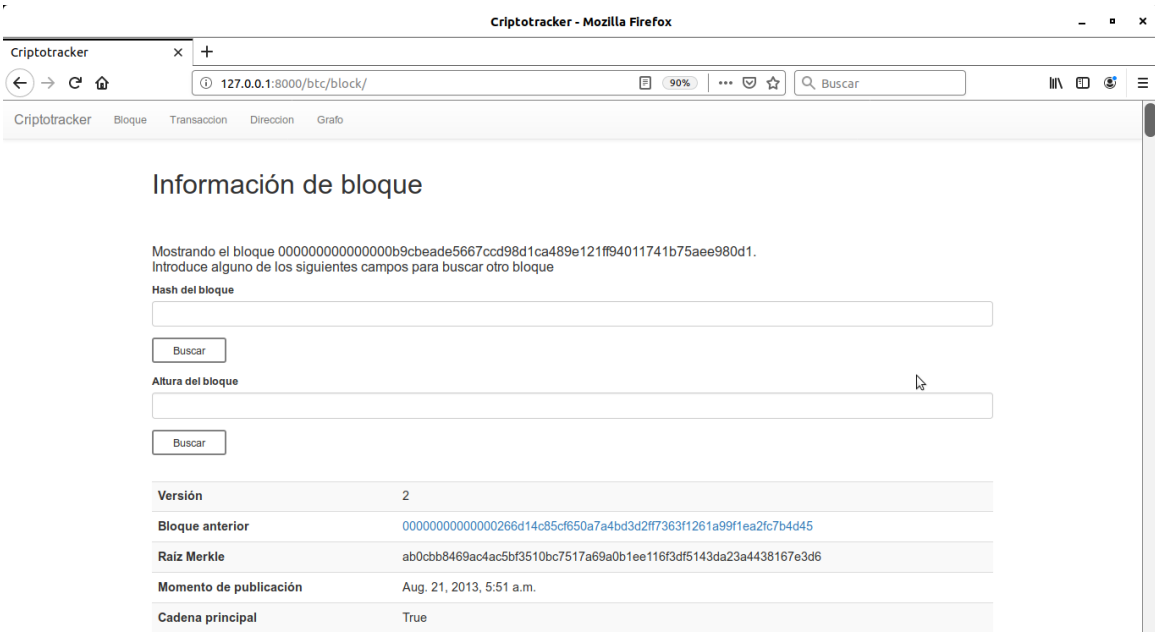

Figura 7: Información obtenida búsqueda de bloque por hash (1)

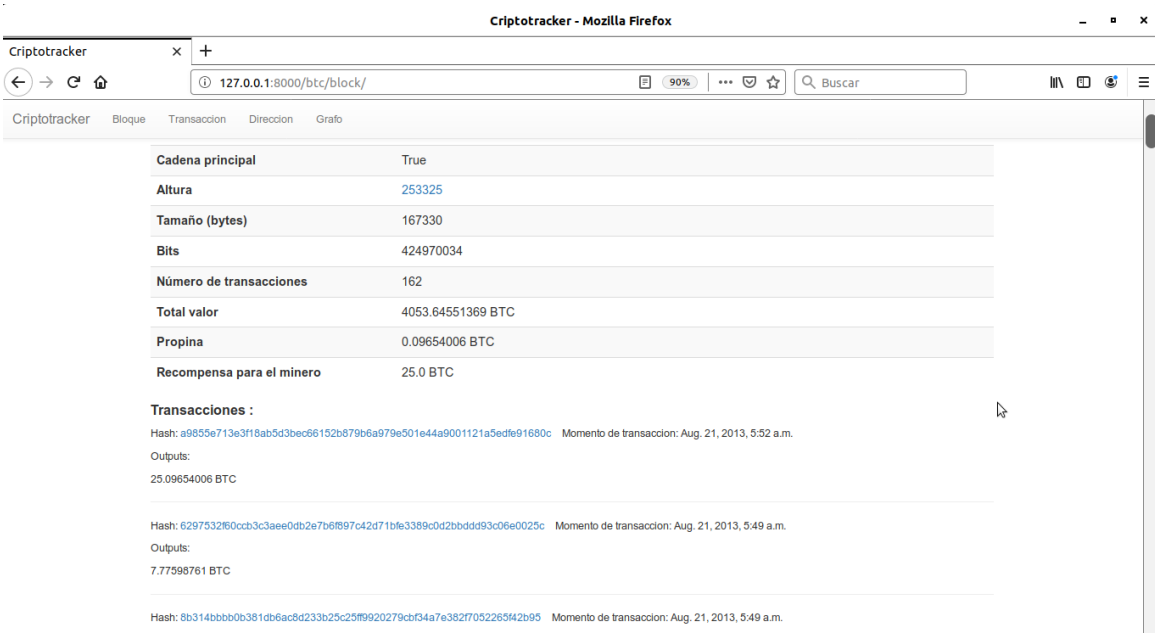

Figura 8: Información obtenida búsqueda de bloque por hash (2)

4.1.2. Búsqueda de bloque por altura en la cadena

Desde la página donde nos encontramos, existe la posibilidad de buscar otro bloque para obtener su información. En esta ocasión vamos a buscar usando el número que ocupa en la cadena. Buscamos el bloque número `200321`, siendo el 0 el bloque génesis. En la figura 9 vemos como se procede a su búsqueda, y en las figuras 10 y 11 los resultados obtenidos. Observamos que el formato de presentación es el mismo tanto si la búsqueda se ha realizado por *hash* o por altura en la *blockchain*.

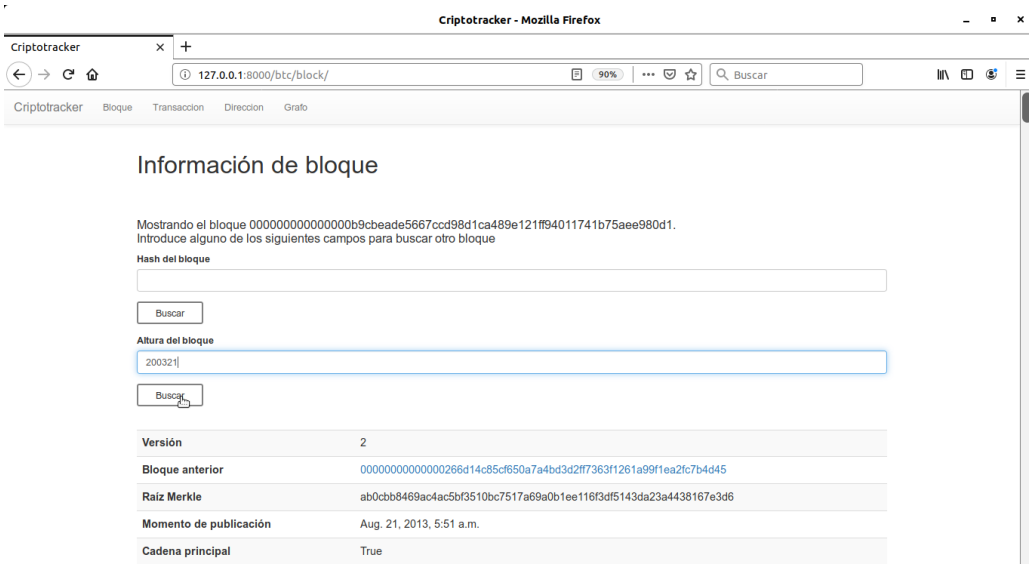

Figura 9: Búsqueda por la altura de bloque desde la página de bloque

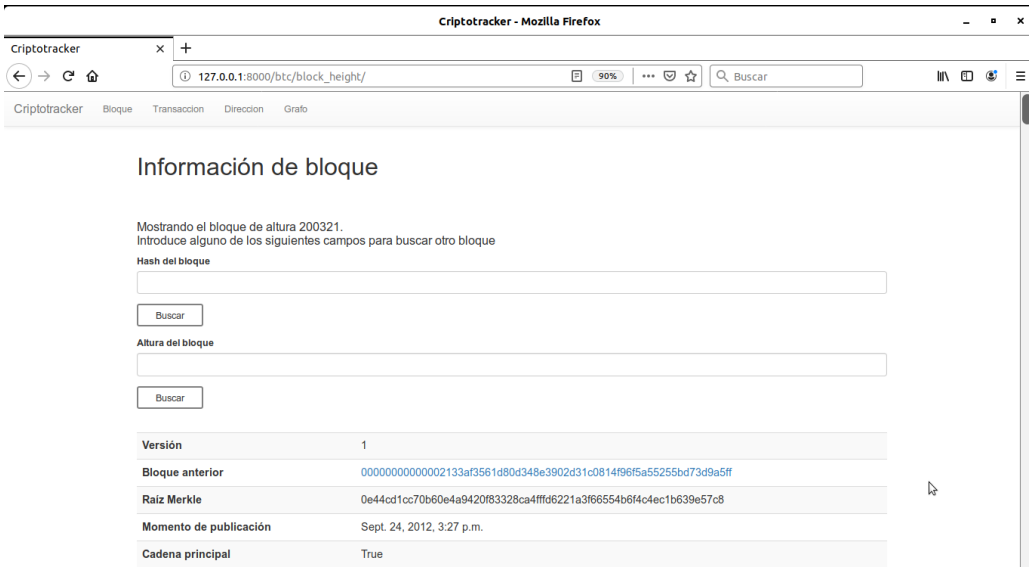

Figura 10: Información obtenida en la búsqueda de bloque por altura (1)

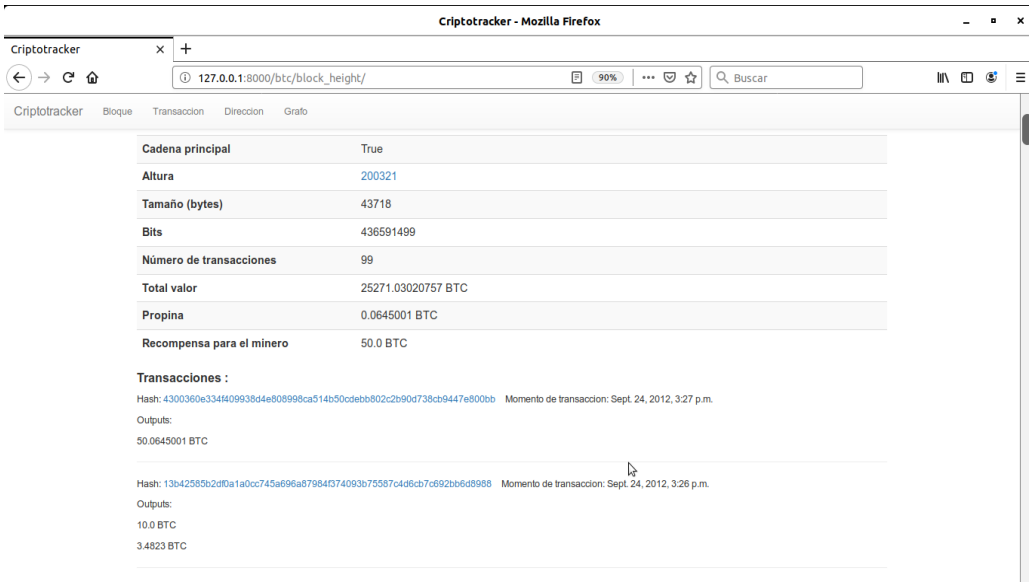

Figura 11: Información obtenida en la búsqueda de bloque por altura (2)

Observamos que en este caso se trata de un bloque anterior al que hemos buscado por *hash*, además de por la fecha, se puede ver en que en el momento de minado de este bloque, la recompensa que se obtenía era de 50 BTC, mientras que en el caso anterior ya se había reducido y solo se trataba de 25 BTC.

4.1.3. Búsqueda de hash de transacción

Para el caso de búsqueda de una transacción debemos introducir su *hash* en su campo correspondiente de la página principal. Omitimos esta vez esa imagen y mostramos únicamente el resultado obtenido al buscar la transacción con *hash* `737337c4aeab6c2dc801f0ee7475e278b875354f0ef12603117834430547f772`, en las figuras 12 y 13.

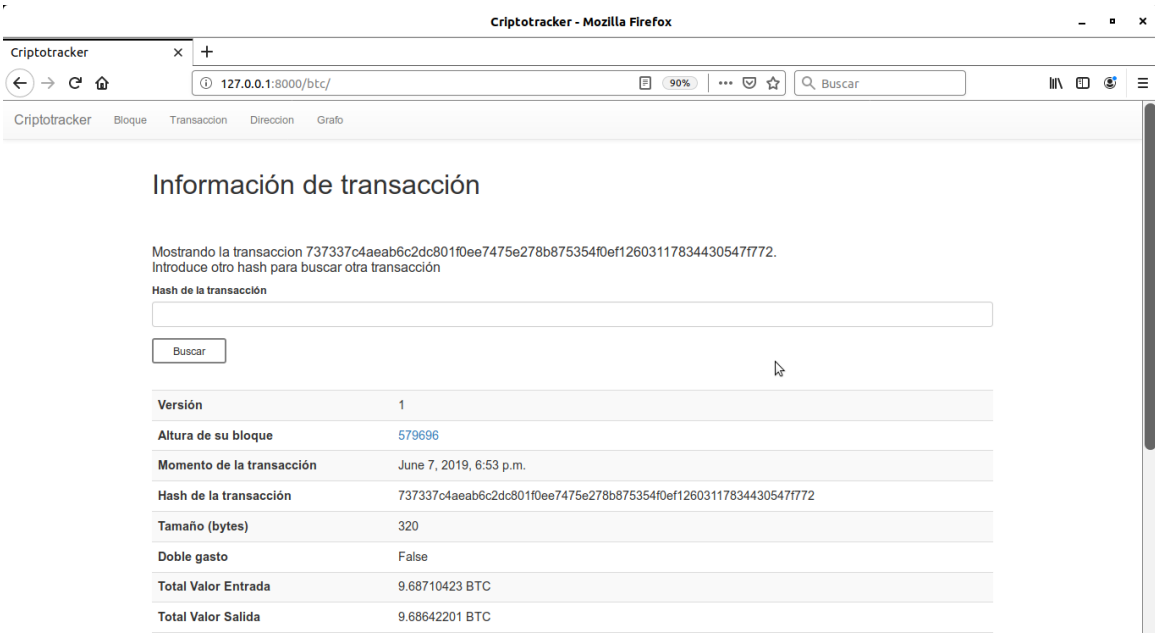

Figura 12: Información obtenida en la búsqueda de transacción (1)

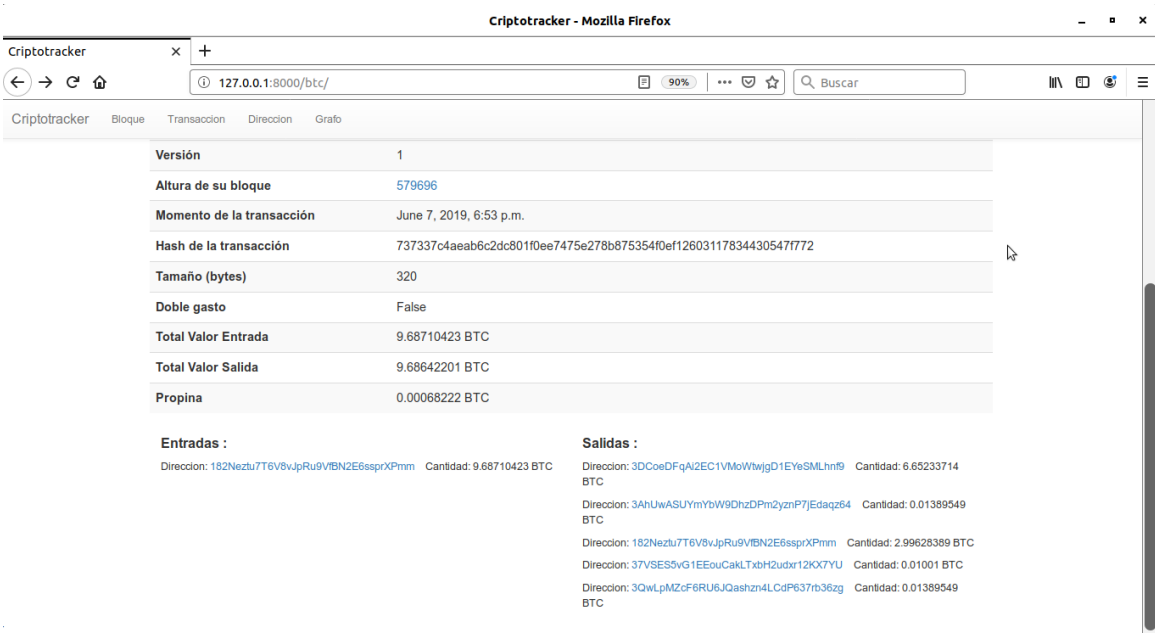

Figura 13: Información obtenida en la búsqueda de transacción (2)

En esta transacción vemos como la dirección `182Neztu7T6V8vJpRu9VfBN2E6ssprXPmm`, reparte 9.68710423 BTC entre otras cuatro direcciones, asignándole a la que más 6.65233714 BTC, y a la que menos 0.01001 BTC. Además, también se asigna a sí misma un total de 2.99628389 BTC, a modo de vueltas de la operación, y deja 0.00068222 BTC de propina para el minero que la incluya en un bloque. Observamos que el bloque en el que se incluye se sitúa en la posición 579696 de la cadena de bloques.

4.1.4. Búsqueda de dirección

Para la búsqueda de una dirección procedemos del mismo modo que en las ocasiones anteriores, introduciendo su *hash* en el buscador correspondiente. La pantalla donde se nos muestran los datos se muestra en las figuras 14 y 15. La dirección que hemos buscado es la que está identificada por el *hash* `1B9W7Azu5uAeTnQ1VV55sA2v8fUnoxJ6RU`.

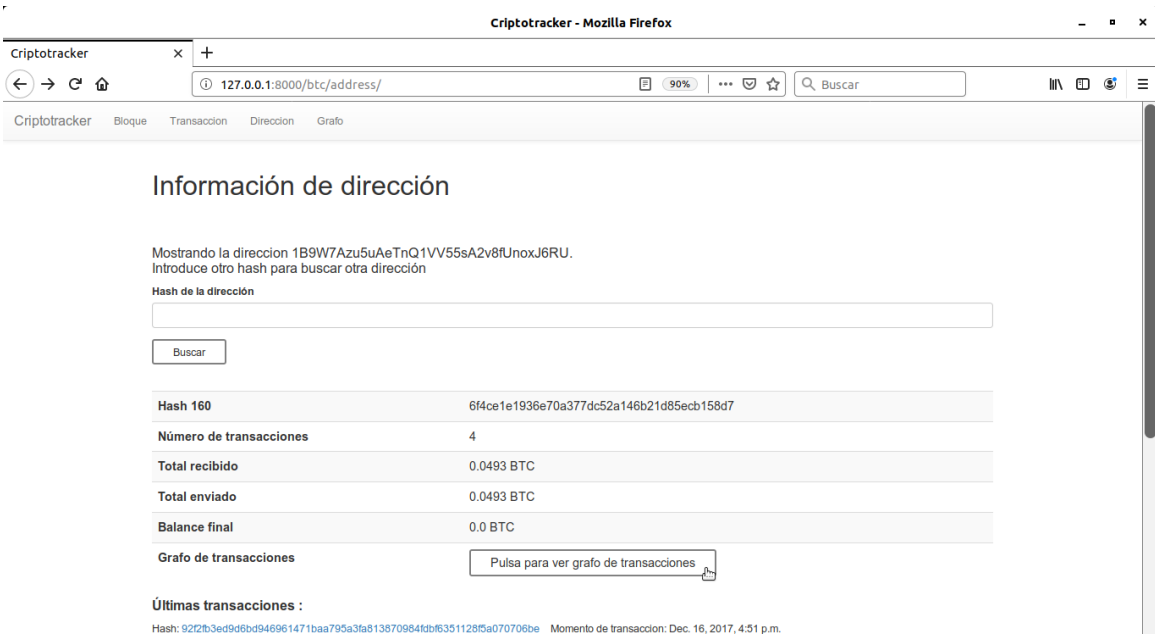

Figura 14: Información obtenida en la búsqueda de dirección (1)

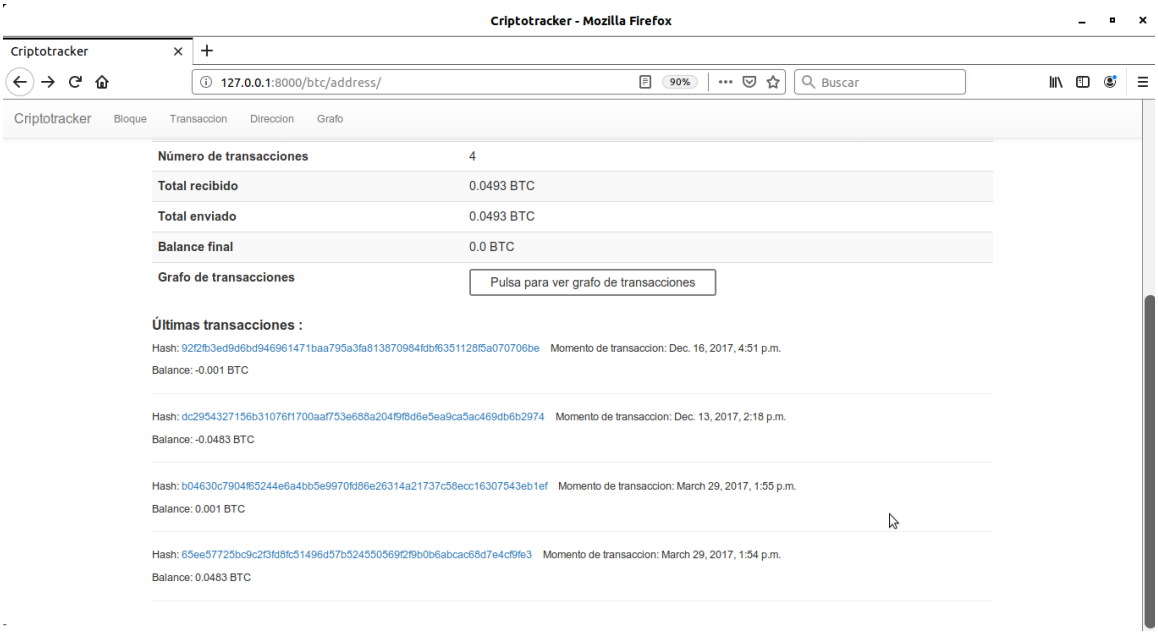

Figura 15: Información obtenida en la búsqueda de dirección (2)

Observamos que esta dirección, inactiva desde diciembre de 2017, únicamente ha realizado cuatro transacciones, dos de entrada en marzo de 2017 y dos de salida por el mismo valor en diciembre de 2017, quedándose con un balance de 0 BTC en su poder.

4.1.5. Grafo de transacciones

Para visualizar el grafo de transacciones de una dirección podríamos buscar cualquiera en el buscador, pero he preferido por sencillez continuar con el caso anterior, y mostrar el gráfico de la dirección `1B9W7Azu5uAeTnQ1VV55sA2v8fUnoxJ6RU`, simplemente pulsando el botón con dicha funcionalidad que se aprecia en la figura 14.

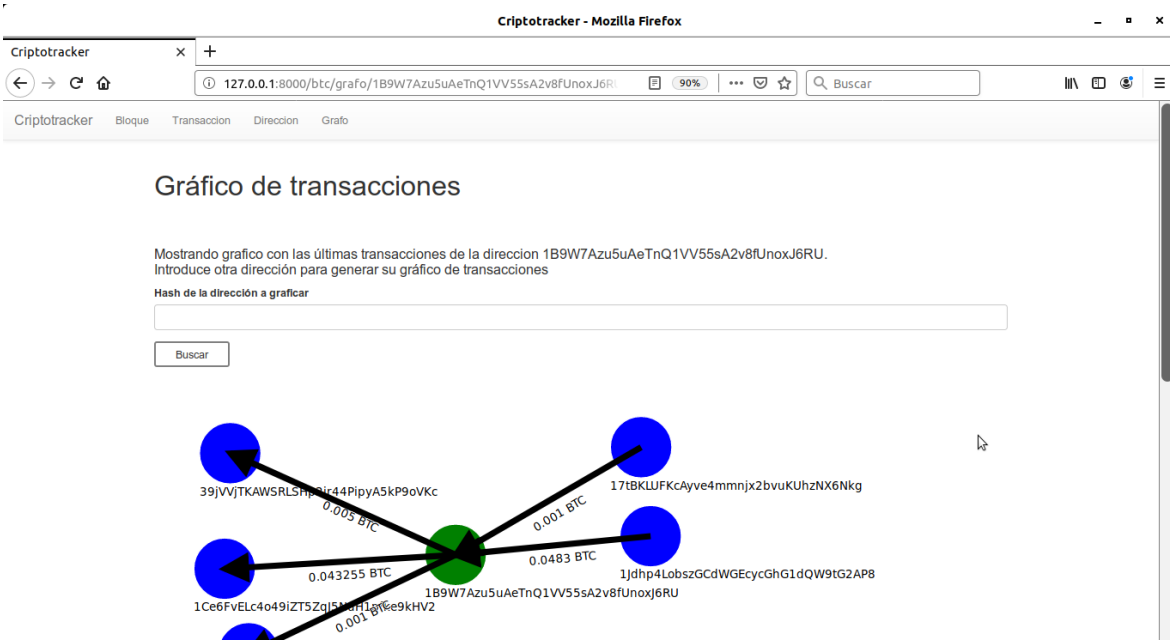

Figura 16: Grafo de transacciones (1)

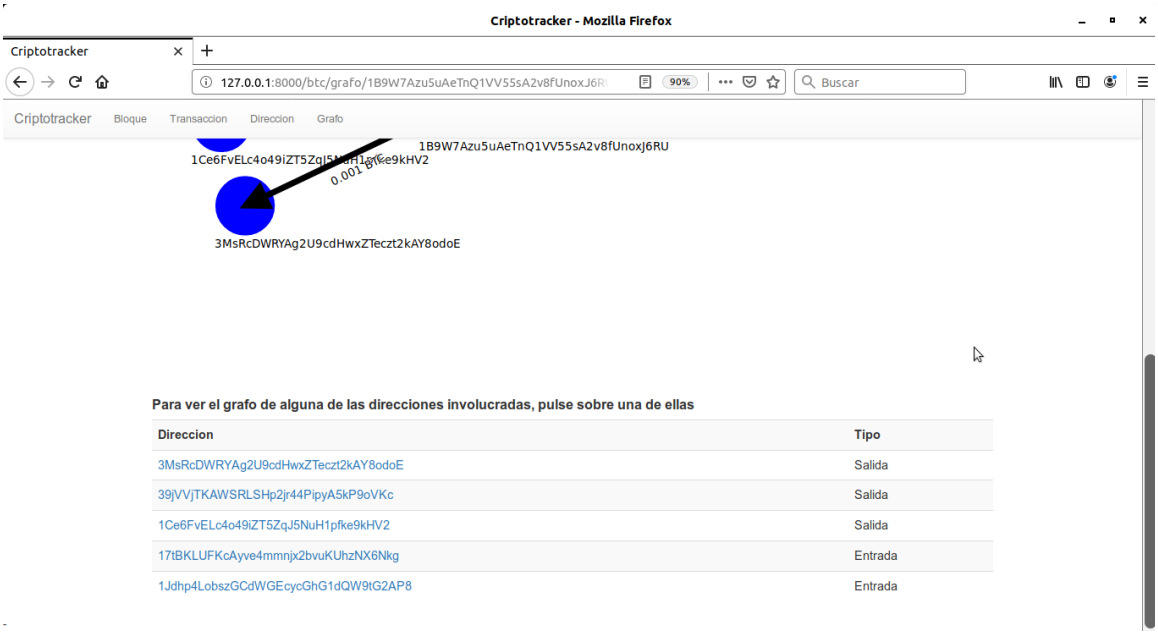

Figura 17: Grafo de transacciones (2)

Observamos que esta dirección, que participaba en 4 transacciones, recibe dinero de dos direcciones, `17tBKLUFKcAyve4mmnjx2bvuKUhzNX6Nkg`, un total de 0,001 BTC, y `1Jdhp4LobszGCdWGEcycGhG1dQW9tG2AP8`, un total de 0,0483 BTC, y lo reparte entre tres direcciones. En la transacción en la que daba 0.0483 BTC se lo reparte a las direcciones `39jVVjTKAWSRLSHp2jr44PipyA5kP9oVKc` y

1Ce6FvELc4o49iZT5ZqJ5NuH1pfke9kHV2, otorgando a cada una 0.005 BTC y 0.043255 BTC respectivamente. Por último, a la dirección 3MsRcDWRYAg2U9cdHwxZTeczt2kAY8odoE, le envía los últimos 0,001 BTC que poseía en su cartera.

La tabla de la parte inferior de la página nos da la posibilidad de con un simple click observar gráficamente que han hecho las demás direcciones con ese dinero, o de donde procedía antes de llegar a donde está. Sería algo así como expandir el nodo, pero para garantizar una mejor visualización y tener un gráfico más limpio, he decidido que se borre de la imagen todo lo anterior para eliminar nodos y enlaces que puedan resultar inútiles y entorpezcan la correcta visualización.

5. Conclusiones y trabajo futuro

5.1. Conclusiones

Este Trabajo de Fin de Grado sobre el Estudio y Análisis de la Trazabilidad en operaciones con criptomonedas me ha permitido obtener muchos conocimientos sobre el protocolo *blockchain*, que según indican algunos expertos, se trata de la tecnología que está revolucionando y revolucionará el futuro.

Esta tecnología es capaz de hacer los procesos más eficientes, transparentes y seguros. Se trata de una especie de base de datos distribuida que mantiene un listado de registros en forma de bloques. Estos bloques son prácticamente inmutables, ya que para modificar uno habría que modificar también todos los que le siguen, ya que están enlazados todos con el bloque previo mediante un *hash* que se obtiene de su encabezado.

Aunque su uso comenzó únicamente con las criptomonedas y en particular el Bitcoin, actualmente se encuentra presente en multitud de sectores y múltiples tareas. Desde controlar la disponibilidad de historiales médicos en la Sanidad, como la firma y almacenamiento de "contratos inteligentes" en servicios legales, hasta ayudar en la reducción de la corrupción y fraudes y el aumento de la transparencia en distintos gobiernos e instituciones de todo el mundo.

En el caso que nos ocupa, el de cadena de bloques de criptomonedas, y más concretamente del Bitcoin, la tecnología *blockchain* nos proporciona una buena lista de ventajas. Algunas de las más importantes son la eliminación de entidades intermediarias gracias a la descentralización de la cadena en una red *peer-to-peer*, la seguridad que proporciona el sistema de minado mediante prueba de trabajo y sus *hashes* criptográficos para evitar que una misma cantidad de monedas sea gastada simultaneamente dos o más veces en dos o más operaciones distintas o el anonimato que proporciona esta red gracias a que las transacciones se realizan de unas direcciones públicas a otras, sin añadir datos de las personas físicas que hay detrás ni de su ubicación. Estas direcciones se generan de forma "ilimitada" a partir de una clave pública y privada que posee cada usuario, y que son las que le permiten poder usar el dinero que posee.

Gracias a este trabajo he conseguido desarrollar un sistema que es capaz de obtener y descodificar toda la información que se encuentra en cada bloque, así como en cada transacción o dirección de cartera, siendo capaz también de crear un grafo dirigido para observar gráficamente y de manera más sencilla donde dirige el dinero cada una de las direcciones que hay en la red.

Con este sistema se puede llevar un seguimiento bastante completo de las transacciones realizadas por una dirección en concreto, que pueda considerarse sospechosa de pertenecer a un criminal o a una organización que se dedique a prácticas de dudosa legalidad.

Sin embargo, la existencia en la red de los conocidos como "*mixers*" dificulta esta tarea, ya que cuando llegamos a una dirección de este tipo podemos ver que participa en multitud de operaciones, tanto de entrada como de salida, pero perdemos el rastro del origen de los fondos que se mueven. El funcionamiento de este tipo de agentes es sencillo, únicamente reciben diferentes cantidades desde múltiples direcciones, y se las asignan a otras, mezclando las monedas y sirviendo como método de lavado de dinero negro, o simplemente para encubrir alguna compra u operación ilegal.

Por tanto, creo que, mientras este tipo de actividades sean legales, y los criminales se amparen en ellas para borrar las huellas o limpiar sus ingresos, será muy complicado para las Fuerzas y Cuerpos de Seguridad seguir su rastro únicamente usando la información registrada en la cadena de bloques. Sin embargo, si se pueden acercar a ellos gestionando la información que puedan encontrar en las casas de cambio que monetizan los Bitcoins a Euros o Dólares, u observando si hubiera algún tipo de patrón en la repetición de algunas operaciones por parte de las mismas direcciones.

5.2. Trabajo futuro

Este sistema para el análisis de la trazabilidad y estudio de las operaciones realizadas extrae toda la información sobre la criptomoneda Bitcoin, ya que, tal y como se menciona en la sección 2.1, fue la primera en nacer, la más popular, la que más valor tiene y la que su uso está más extendido, por lo que creí que realizar el estudio sobre ella era lo que más sentido tenía.

Sin embargo, aunque fue la pionera, Bitcoin no es la única criptodivisa existente en la actualidad. Aunque hay voces críticas que apuntan que el Bitcoin ya se encuentra tecnológicamente obsoleta, la realidad es que ninguna otra moneda ha estado nunca ni cerca de su valor en el mercado, y el valor de Bitcoin afecta al resto, de manera que cuando esta moneda sufre una bajada, las demás se desploman, y si la caída es grande, puede que hasta alguna moneda desaparezca.

De estas criptomonedas posteriores, muchas proceden de un "*fork*" irreparable de la cadena principal. Es cierto que algunas únicamente introducen pequeñas variaciones en el protocolo Bitcoin, mientras que otras tienen por si mismas características nuevas que las hacen interesantes y podrían ser prometedoras líneas de trabajo futuro para llevar a cabo este estudio con ellas, o adaptar el sistema para que sea compatible con ellas.

Algunas de las más relevantes son:

- Namecoin: Fue la primera copia que surgió de Bitcoin. Aunque las modificaciones que aporta son muy pequeñas, la más destacable es que permite almacenar datos dentro de su propia cadena de bloques, lo que permite usarla como un registro de DNS.
- Litecoin: Genera nuevos bloques cada 2 o 3 minutos, lo que proporciona confirmaciones más rápidas, y para su algoritmo de prueba de trabajo usa una función scrypt que facilita la minería con respecto a Bitcoin.

- Dogecoin: Además de generar muchas más monedas en el mercado, se generan mucho más rápido nuevos bloques, aproximadamente uno cada minuto, lo que hizo crecer a esta moneda rápidamente. También usa la tecnología scrypt en su prueba de trabajo.
- Monero: Prioriza la privacidad, ocultando la identidad de emisores y receptores y las cantidades de las operaciones. Esto ha provocado que sea una de las favoritas para el uso ilegítimo. Además, su proceso de minado es más igualitario.
- Ethereum: Su diseño e implementación es independiente del de Bitcoin. Se trata de una nueva forma de aprovechar la *blockchain*, ya que propone que la red no sirva únicamente para almacenar y validar transacciones, sino que también pueda actuar de intermediaria en la ejecución de contratos. Con ella nace el concepto de "*Smart Contract*", que pueden almacenar datos, recibir y enviar *Ethers*, almacenarlos y ejecutar numerosas actividades sobre las transferencias o eventos que ocurren dentro de la red.

Añadir estas divisas al sistema le dotaría de un mayor mercado donde poder obtener información, lo que lo haría aún más completo, y de mayor utilidad para la detección de operaciones delictivas y el estudio de la trazabilidad de las transacciones en las diferentes criptomonedas.

Referencias

[1] Nikita Malik, “how Criminals And Terrorists Use Cryptocurrency: And How To Stop It”, 2018, https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#1d1eb8cc3990

[2] EUROPOL, “The Internet Organised Crime ThreatAssessment (IOCTA)”, 2015

[3] Mariano Puigvert, “Mixers: el servicio para lavar Bitcoins”, 2016, https://www.criptonoticias.com/colecciones/mixers-el-servicio-para-lavar-bitcoins/

[4] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 31 octubre 2008

[5] Andrés Cisneros Campos, “Estudio de la red Bitcoin”, Junio 2014.

[6] María Isabel Rojo, “Blockchain. Fundamentos de la cadena de bloques”, Ra-Ma, 2018

[7] Andreas M. Antonopoulos, “Mastering Bitcoin. Unlocking digital crypto-currencies”, O’Reilly, 2014

[8] Bitcoin wiki, https://en.bitcoin.it/wiki/Protocol_rules#.22tx.22_messages

[9] Mirror, https://getmirror.io/

[10] Chainalysis, https://www.chainalysis.com/

[11] Django, The web framework for perfectionists with deadlines https://www.djangoproject.com/

[12] Blockchain Data API, https://www.blockchain.com/es/api/blockchain_api

[13] Blockchain.com / Blockchain.info, GitHub https://github.com/blockchain

[14] Boostrap, https://getbootstrap.com/

[15] D3.js, https://d3js.org/

Glosario

API	*Application Programming Interface*. Conjunto de subrutinas, funciones y procedimientos que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.
Clave privada	Clave secreta usada para habilitar el uso de monedas que llegan a tu dirección, confirmando ser el dueño de la clave pública que generó esta dirección. Es la encargada de generar la clave pública
Clave pública	Generada a partir de la clave privada y encargada de generar direcciones, se usa para cifrar envíos de monedas
Criptografía	Técnica de cifrado o codificado de mensajes
Deep Web	Contenido de Internet que no está indexado por los motores de búsqueda habituales
Framework	Estructura conceptual y tecnológica que sirve de base para la organización y desarrollo de software
Fork	Bifurcación de un proyecto en una dirección distinta de la principal
Función Hash, Hash	Algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija
Inputs	Entradas de una transacción. Son referencias a salidas de transacciones anteriores
JSON	*JavaScript Object Notation*. Formato de texto sencillo para el intercambio de datos
MVC	Modelo-Vista-Controlador. Estilo de arquitectura de software que separa los datos de la aplicación, la interfaz de usuario y la lógica de control en tres componentes distintos.
Outputs	Salidas de una transacción
Peer-to-peer, P2P	Red en la que todos sus nodos se comportan como iguales entre sí, actuando simultáneamente como clientes y como servidores para el resto de nodos de la red.