Universitat Oberta de Catalunya

TFM

Estudio de tecnologías Bitcoin y Blockchain

Alumno: Javier Ángel Caballero Gimeno

Consultora: Ángela María García Valdés

Profesor: Victor García Font

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Estudio de tecnologías Bitcoin y Blockchain*
Nombre del autor:	*Javier Ángel Caballero Gimeno*
Nombre del consultor/a:	*Ángela María García Valdés*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	06/2018
Titulación:	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)*
Área del Trabajo Final:	*TFM-Ad hoc*
Idioma del trabajo:	*Español*
Palabras clave	*Bitcoin Blockchain*

Resumen del Trabajo

Bitcoin es una criptomoneda y un sistema de pagos mundial. Fue la primera divisa digital descentralizada que solventó el problema del doble gasto. Además de ser la primera, también es la más conocida y usada en la actualidad.

El objetivo de este trabajo de fin de máster es realizar un estudio sobre las tecnologías Bitcoin y Blockchain. Se trata por tanto de descubrir como funciona, que beneficios genera y que aplicación tiene actualmente y podrá tener en el futuro.

Abstract

Bitcoin is a cryptocurrency and a global payment system. It was the first decentralized digital currency that solved the double spending issue. Besides being the first one it is also the best known and used nowadays.

The goal of this final thesis is to make a study on Bitcoin and Blockchain technologies. Therefore, is about discovering how it works, which benefits generates and which application has currently and may have in the future.

1. Introducción

1.1. Contexto y justificación del trabajo

Bitcoin es una criptomoneda y un sistema de pagos mundial. Fue la primera divisa digital descentralizada que solventó el problema del doble gasto. Además de ser la primera es la más conocida y usada en la actualidad. Su primera prueba de concepto apareció en el año dos mil nueve, expansionándose desde entonces hasta la amplia difusión de la que disfruta actualmente.

Dada la relevancia que ha adquirido, tanto por sus usos actuales como otros futuros, es un asunto del que merece realizar un estudio en profundidad, objetivo final de este presente trabajo de fin de máster.

1.2. Objetivo del trabajo

El objetivo de este trabajo de fin de máster es realizar un estudio sobre las tecnologías Bitcoin y Blockchain. Se trata por tanto de descubrir como funciona, que beneficios genera y que aplicación tiene actualmente y podrá tener en el futuro.

Siendo este un trabajo de fin de máster de carácter teórico los principales aspectos que se van a tratar son:

- ¿Qué es bitcoin?
- ¿Cómo funciona bitcoin?
- La red bitcoin.
- Cadena de bloques.
- Transacciones.
- Minado.
- Seguridad.
- Otros usos de la cadena de bloques.
- Otras cadenas de bloques.

1.3. Enfoque y método elegido

El presente trabajo de fin de máster, dado su carácter de estudio teórico, se basará en la investigación, recogida de información, consolidación de la misma y escritura como tal de la memoria y la presentación del trabajo.

La fase de investigación y recogida de información es indudablemente el primer paso. Para obtener esta información se partirá de los recursos disponible: documentación del proyecto, foros, redes sociales, libros, etc.

En esta fase es necesario conseguir recabar información suficiente para poder dar, al menos inicialmente, respuesta a las preguntas y temas descritos en el apartado anterior, que muestra los objetivos del trabajo.

Para poder obtener resultados intermedios y validar el grado de avance con la consultora del trabajo de fin de máster será necesario ir generando capítulos a la par que se avanza en el recabado de información. Por tanto, aunque a priori la búsqueda de información debería ocurrir al principio también ocurrirá intercalándose con la producción de capítulos de la memoria.

Como parte final se realizará la presentación del trabajo y la grabación de la misma.

1.4. Planificación del trabajo

Desde el punto de vista docente existen los siguientes hitos:

	Fecha inicio	Fecha fin
PEC 1	mié, 21 feb 2018	lun, 12 mar 2018
PEC 2	mar, 13 mar 2018	lun, 9 abr 2018
PEC 3	mar, 10 abr 2018	lun, 7 may 2018
Entrega final	mar, 8 may 2018	lun, 4 jun 2018
Presentación	mar, 5 jun 2018	lun, 11 jun 2018
Defensa	lun, 18 jun 2018	vie, 22 jun 2018

PEC 1

Documento que recoge principalmente los objetivos del trabajo junto con la planificación.

PEC 2

Primera parte de la memoria. Partiendo de los capítulos anteriormente descritos este avance de la memoria debería incluir al menos:

- ¿Qué es bitcoin?
- ¿Cómo funciona bitcoin?
- La red bitcoin.

PEC 3

Continuación del desarrollo de la memoria. Este fragmento debería incluir:

- Cadena de bloques.
- Transacciones.
- Minado.
- Seguridad.

Entrega final

Este hito constituye la entrega final en la que se incluyen todos los capítulos de la memoria.

Presentación

En este hito se elaborarán los materiales de apoyo para la presentación y el guión de la misma, además de la grabación en vídeo y edición del mismo.

Defensa

Durante el tiempo que dure el periodo de defensa se contestarán las preguntas acerca del trabajo de fin de máster.

1.5. Breve descripción de los otros capítulos de la memoria

1. **Introducción.** Introducción al TFM y su contenido.
2. **¿Qué es bitcoin?** Origen y descripción general de Bitcoin.
3. **¿Cómo funciona bitcoin?** Visión del funcionamiento general de Bitcoin.
4. **La red bitcoin.** Arquitectura, protocolo y nodos de la red Bitcoin.
5. **Cadena de bloques.** Descripción de la cadena de bloques.
6. **Transacciones.** Descripción general tratando las entradas, salidas, comisiones y la transacción *coinbase*.
7. **Minado.** Como se realiza el minado y se alcanza el consenso.
8. **Seguridad.** Aspecto relativos a la seguridad.
9. **Otros usos de la cadena de bloques.** Usos alternativos de la cadena de bloques a la moneda electrónica.
10. **Otras cadenas de bloques.** Otros sistemas al margen de Bitcoin que implementan una cadena de bloques.
11. **Conclusiones.** Conclusiones generales del trabajo realizado.
12. **Fuentes de información.** Fuentes usadas para la creación de este TFM.

2. ¿QUÉ ES BITCOIN?

2.1. ORIGEN

Bitcoin apareció por primera vez en un artículo titulado “Bitcoin: A Peer-to-Peer Electronic Cash System”, escrito bajo el alias de Satoshi Nakamoto. El autor combinó varias tecnologías previas como b-money y HashCash para conseguir crear un sistema electrónico financiero completamente descentralizado.

HashCash fue elaborado en mil novecientos noventa y siete por Adam Back. Su finalidad era crear un sistema para combatir el correo basura. La idea detrás de este sistema era evitar que un usuario pudiera enviar grandes cantidades de correo malintencionado: el envío de cada correo estaba asociado al cálculo de unas funciones computacionalmente costosas, no así la recepción. De esta manera se aseguraba que el emisor realmente tenía interés en mandar este correo, además de imponer cierta limitación en la cantidad que podía llegar a mandar rápidamente. Es la base del algoritmo de prueba de trabajo.

B-money fue una propuesta realizada por Wei Dai en mil novecientos noventa y ocho para crear un sistema anónimo y distribuido de efectivo electrónico. Propone dos protocolos: uno basado en difusión de las transacciones a todos los participantes y un segundo en el que sólo algunos participantes, los servidores, mantienen las cuentas, teniendo el resto de participantes que verificar las transacciones consultando varios servidores. Bitcoin toma la idea de consenso distribuido, además de la prueba de trabajo ya presente en HashCash.

La innovación clave de Bitcoin fue usar una red de iguales junto con el algoritmo de prueba de trabajo para obtener consenso en las transacciones cada diez minutos. Esto resuelve el problema del doble gasto, una de las carencias de los sistemas anteriores.

La red Bitcoin comenzó en el año dos mil nueve utilizando la implementación de referencia creada por Satoshi Nakamoto.

Sobre Satoshi Nakamoto existe mucha especulación acerca de su identidad real. Se desconoce si es un individual o un grupo de personas. Varios medios han tratado de revelar de su identidad, pero a día de hoy no es conocida.

2.2. Descripción

Bitcoin es un conjunto de conceptos y tecnologías que ha permitido crear una moneda electrónica descentralizada y anónima. La divisa como tal y la red en la que se basa son también llamadas Bitcoin.

Bitcoin es una moneda completamente virtual, no existen las monedas físicas equivalentes. Las monedas como tal aparecen en las transacciones que mueven valor de emisor a receptor. Estas transacciones son totalmente públicas, se pueden conocer todas las realizadas desde el origen del sistema hasta la actualidad.

El usuario no tiene Bitcoins en si, si no una clave privada que le permite demostrar dentro de la red que es el dueño de esos fondos. De esta manera puede firmar las transacciones con esos fondos. Estas transacciones se realizan entre direcciones, que en cierta medida se podrían considerar equivalentes a cuentas bancarias. Generalmente los usuarios utilizan monederos electrónicos para almacenar sus claves y generar las transacciones. Estos monederos además generan direcciones para recibir y enviar fondos.

Cuando se realiza una transacción está es compartida a través de la red Bitcoin a todos los usuarios. Aproximadamente cada diez minutos algún nodo de la red es capaz de validar todas las transacciones creando un bloque y es recompensado con un número determinado de Bitcoins. Además de la recompensa por creación de bloque existe otro incentivo menor que son las comisiones voluntarias, sufragadas por los usuarios, que envían las transacciones para incentivar al nodo minero a que incluya la transacción en el bloque que está generando.

Una vez que la transacción está incluida en el bloque cualquier nodo puede revisar todas las transacciones y determinar en qué orden han ocurrido. Entonces el receptor de un pago puede estar seguro de haber recibido los fondos por parte del emisor del pago.

El número total de monedas que podrán crearse en la red es limitado, concretamente veintiún millones. Además, la recompensa por la generación de cada bloque se divide aproximadamente cada cuatro años (dos cientos diez mil bloques). Por este motivo, a largo plazo, la moneda Bitcoin es deflacionista.

3. ¿Cómo funciona Bitcoin?

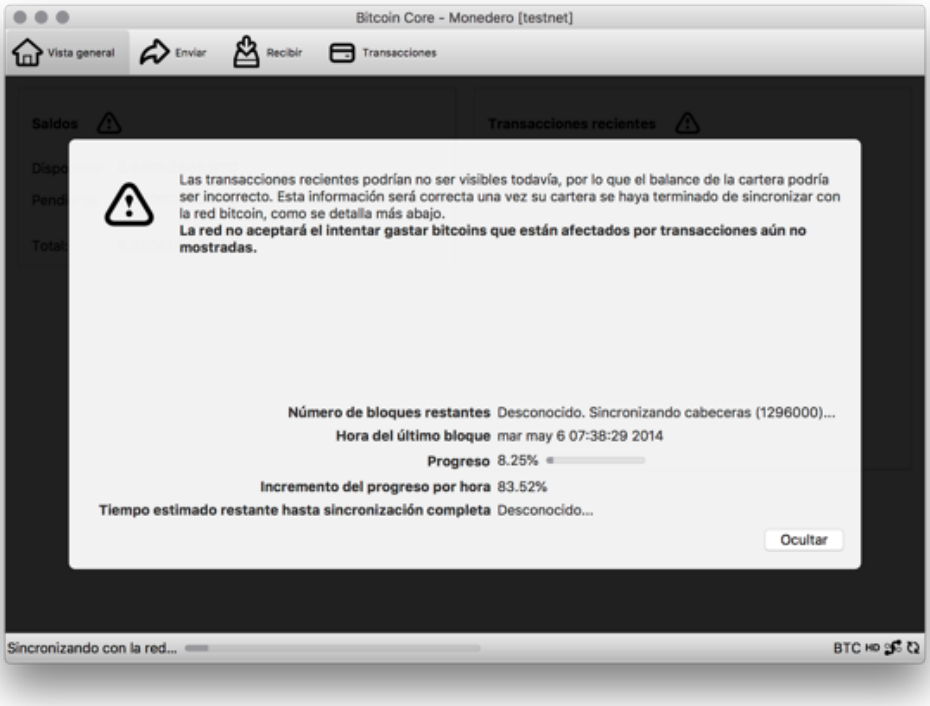
3.1. Visión general

Bitcoin difiere totalmente de la banca tradicional: estos se basan en una autoridad central de confianza, por contra Bitcoin es un sistema de confianza distribuido.

Los usuarios gestionan sus claves privadas haciendo uso de monederos electrónicos. Estos generan las transacciones que son propagadas a través de la red y son los nodos *mining* los que producen la cadena de bloques consensuada.

3.2. Ejemplo de uso

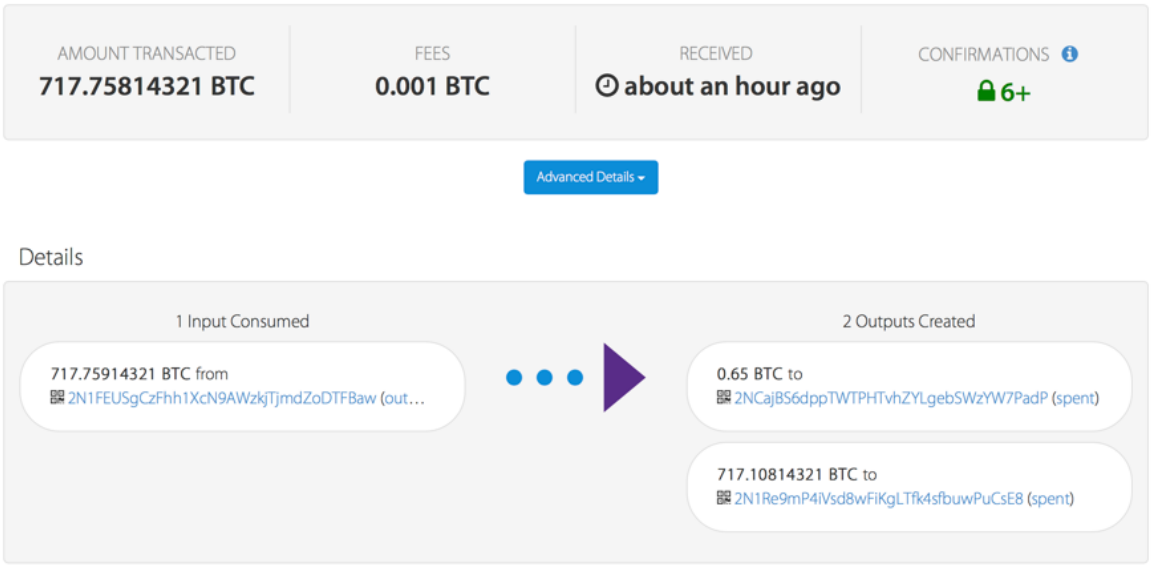
En la siguiente captura se puede observar el cliente Bitcoin Core realizando la sincronización inicial, necesaria antes de poder trabajar en la red:



Como se puede observar el cliente no está trabajando en la red real de Bitcoin sino en una de pruebas llamada testnet3. Esta red utiliza tanto direcciones distintas como otra cadena de bloques también independiente. Específicamente las direcciones de la red principal de Bitcoin, también conocida como Mainnet, comienzan por por 1 o por 3, frente a las de testnet3 que lo hacen por m o 2.

Realizar transferencias entre ambas redes no es posible ya que las direcciones son incompatibles. La verificación de la transacción, en el caso de que se propagara por la red, fallaría y no se incorporaría a la cadena.

Para poder realizar transacciones de pruebas se pueden usar *faucets* públicos que proporcionan Bitcoin, siempre en la red testnet3. En la siguiente imagen se puede observar una transferencia desde uno de estos *faucets* a una dirección generada por el cliente Bitcoin Core con anterioridad:

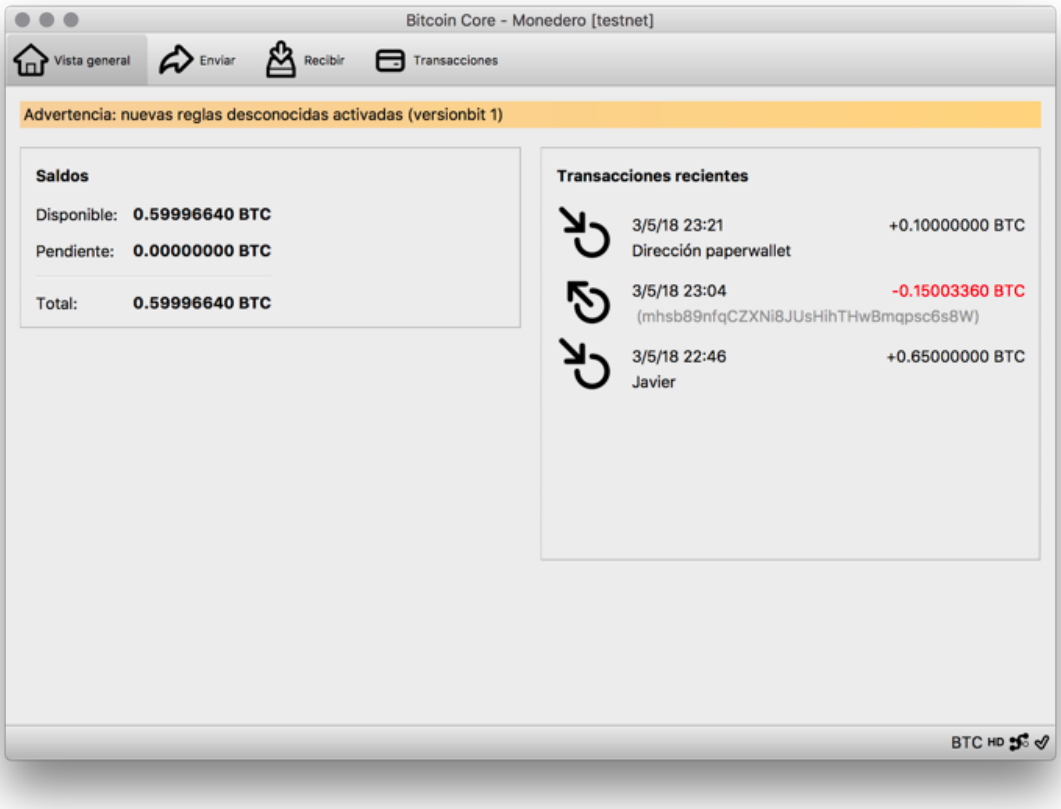


En esta transacción se aprecian varios aspectos relevantes:

- Comisión: se aplica un coste a la transacción, en este caso de 0.001 Bitcoin.
- Existe una dirección de origen de la que parte los Bitcoins a transferir.
- Existen dos salidas de esta transacción: por un lado el destino previsto, esto es, la dirección de Bitcoin a la que se desean transferir los fondos y por otro lado el resto de la operación que va a una nueva dirección, en este caso perteneciente al *faucet*.
- También se puede apreciar que la transacción está confirmada. Esto quiere decir que está incluida en un bloque y que está en la cadena de bloques correcta.

En esta transacción sólo existe un origen y dos salidas, pero puede darse el caso de múltiples entradas y salidas en la misma transacción. Cuanto más compleja es una transacción generalmente habrá que incrementar la comisión para incentivar a los nodos *mining* a incluirla en el bloque en el que están trabajando.

En esta otra captura se muestra el cliente Bitcoin Core tras haber realizado varias transacciones:



En estos ejemplos se ha trabajado como nodo completo puesto que el cliente disponía de la cadena de bloques integra. Hay monederos electrónicos más simples, por ejemplo, los utilizados en dispositivos móviles, los cuales utilizan un método denominado SVP (simplified payment verification) que no requiere contener la cadena completa.

4. La red Bitcoin

4.1. Arquitectura

Bitcoin se basa en una red de iguales (P2P o *peer to peer*) que se comunican a través de internet. Es decir, todos los nodos que participan en la red son iguales y se comunican entre ellos, no hay nodos especiales, pero si que existen distintos tipos de nodos en base a las funciones que pueden desempeñar.

Como red de iguales comparte las características de estas: no hay servidores, no existen servicios centralizados ni jerarquía entre los distintos nodos. Al ser una red abierta cualquiera puede incorporarse a la red en un momento dado, así como desparecer de la red sin que esto afecte al funcionamiento de la misma.

Todos los nodos consumen y proveen servicios recíprocamente. Para poder participar en la red al menos deben ejecutar el protocolo de red Bitcoin. Además de este protocolo pueden ejecutar otros, como Stratum, dependiendo del tipo de nodo que sean y las funciones que desempeñen.

Estos otros protocolos, como el anteriormente citado Stratum, son provistos por servidores que actúan como pasarela con la red Bitcoin. En concreto Stratum es un protocolo utilizando en grupos de minería (*mining pools)*. Estos nodos de minería Stratum están interconectados entre si usando este protocolo, pero utilizan un servidor de retransmisión para conectar a la red Bitcoin.

4.2. Tipos de nodos

Los nodos en la red Bitcoin se pueden agrupar en tres categorías:

- *Broadcast only node*
- *Relay node*
- *Mining node*

Los nodos del tipo *Broadcast only* son aquellos que sólo emiten transacciones. En general son dispositivos con reducida capacidad de cómputo, como un móvil, y que utilizan algún monedero electrónico simple. Utilizan sólo las cabeceras de los bloques, por lo tanto, no puede realizar una verificación completa de la cadena, dependiendo de esta manera de la verificación de los nodos completos para garantizar la seguridad.

Los nodos del tipo *Relay* transmiten y propagan transacciones. Cuando uno de estos nodos recibe una transacción la reenvía a otros nodos para que esté disponible de forma global. Como los nodos receptores también realizan está función la transacción pasa a estar disponible rápidamente en la red.

Estos nodos además revisan los formatos de las transacciones para verificar que sean válidas. Así mismo comprueban que las firmas son correctas y que los fondos transferidos realmente existen en la cuenta de origen, basándose para ello en la versión más reciente de la cadena de bloques. Un nodo se denominada además completo cuando dispone de la cadena de bloques integra, por contra los nodos que no tienen capacidad para almacenar la cadena al completo utilizan un método denominado SVP (*simplified payment verification*) para facilitar que puedan participar en la red y generar transacciones.

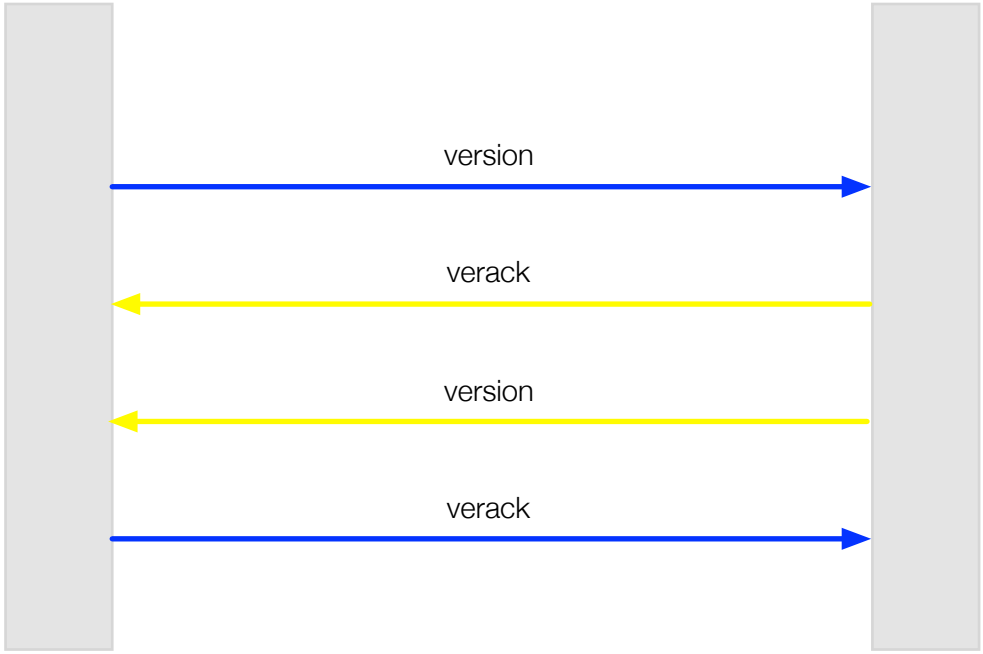
Por ultimo los nodos del tipo *Mining* son aquellos encargados de crear los nuevos bloques de la cadena. Son los nodos que más capacidad de procesamiento necesitan ya que compiten entre sí para resolver la prueba de trabajo e incorporar el bloque generado a la cadena. Actualmente los nodos *Mining,* en general, trabajan agrupados en grupos (*mining pool*). En estos casos las máquinas que realmente realizan el proceso no están directamente conectadas a la red Bitcoin sino que participan mediante servidores de retransmisión, que son los que están conectados a la red Bitcoin.

4.3. Protocolo

El protocolo Bitcoin funciona sobre TCP/IP, normalmente utilizando el puerto 8333 u otro alternativo. Para comenzar a participar en la red lo primero que debe hacer un nodo es encontrar al menos otro nodo y conectar.

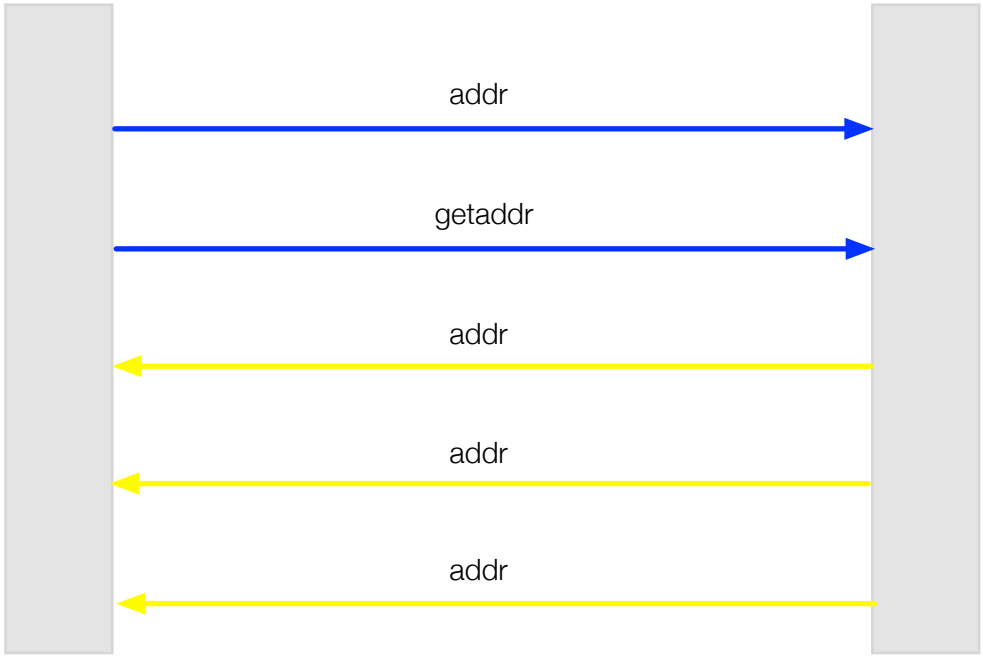
Para conseguir localizar un primer nodo se interroga un servidor DNS semilla. Estos nodos de inicialización de DNS sólo proporcionan una lista de las direcciones IP que se están ejecutando (o que se estaban ejecutando recientemente) en un cliente de Bitcoin. Si no es capaz de obtener una dirección mediante este método es necesario proporcionar al menos la dirección de un nodo ejecutando Bitcoin para poder comenzar.

Al establecer la conexión el primer mensaje que se intercambia indica el número de versión, el número de bloques además de la fecha y hora actual. El otro nodo responde con un mensaje *verack*, el cual es un acuse de recibo del mensaje de versión, mandando a continuación su propio mensaje de información si acepta conexiones desde la versión indicada. Del mismo modo el nodo que ha iniciado la conexión debe contestar con un mensaje *verack* al mensaje de versión del nodo con el que ha conectado.



Una vez que la conexión está establecida el nuevo nodo envía mensajes *addr,* que contienen su dirección IP a sus nodos vecinos. Estos nodos reenvían esta información así mismo a sus nodos cercanos, consiguiendo de esta manera que el nuevo nodo sea

reconocido en la red y pueda participar. Además del mensaje anterior un nodo puede enviar el mensaje *getaddr* a sus nodos vecinos para que estos le envíen una lista con las direcciones IP conocidas por otros nodos.



Los nodos no tratan de conectarse a todos los demás nodos existentes en la red ya que esto no es necesario. Así mismo los nodos tratan de mantener vivas las conexiones con los otros a los que está conectados mediante el envío de mensajes periódicos para verificar el estado. Cuando un nodo no contesta durante más de noventa minutos se le considera desconectado y se deja de intercambiar mensajes con el susodicho.

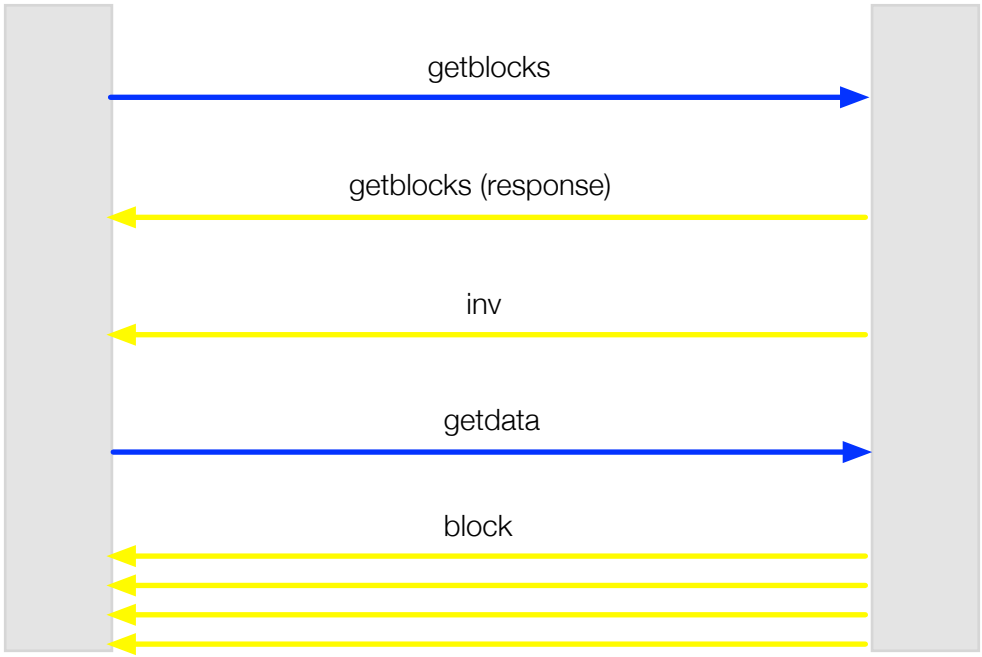
Para que un nodo pueda comenzar a validar nuevas transacciones es necesario que descargue y valide todos los bloques desde el bloque inicial o bloque génesis. Este proceso se denomina *Initial Block Download*. Este método no se utiliza únicamente cuando un nodo comienza por primera vez si no que también ocurre cuando el mejor bloque de un nodo tiene más de veinticuatro horas o cuando se encuentra ciento cuarenta y cuatro bloques por detrás respecto a las cabeceras recibidas.

Existen dos métodos para realizar el proceso de descarga de bloques inicial: las versiones de Bitcoin hasta 0.9.3 utilizan un método denominado *block-first* frente a las versiones más recientes que utilizan otro llamado *header-first*.

El método *block-first* comienza con la selección de otro nodo, al que se le llamada nodo de sincronización (*sync node*), para comenzar a solicitar bloques. Esto se realiza usando el mensaje *getblocks*. En este mensaje indica el hash de la cabecera del único bloque del que dispone, el bloque génesis, además señaliza también que desea el máximo número de bloques posible.

Cuando la petición llega al nodo de sincronización este busca en su cadena de bloques local y busca el bloque con el hash de la cabecera indicada. Al ser el bloque inicial lo localizará y responderá con quinientos inventarios de bloques mediante el mensaje *inv*. Estos inventarios son identificadores únicos que se utilizarán a posteriori por parte del nodo solicitante para conseguir los bloques.

El nodo solicitante entonces utiliza el mensaje *getdata* para solicitar bloques. Es importante recibir los bloques en orden, ya que estos deben ser validados por el receptor y para ello es necesario siempre el bloque previo. El solicitante trata de mantener una cola de petición de ciento veintiocho bloques. Cuando ha validado e incorporado todos los bloques de la solicitud original vuelve a realizar otra para obtener inventario de nuevo. Este proceso se repite hasta conseguir igualar la cadena de bloques.



Este método presenta algunas dificultades:

- Límite de velocidad. Dado que todas las peticiones se realizan al nodo de sincronización si este tiene la velocidad de envío limitada por ende la de descarga del nodo solicitante también lo será.
- Reinicios de las descargas. El nodo de sincronización puede enviar un nodo válido, pero no adecuado, forzando que el nodo solicitante tenga que volver a comenzar la descarga.
- Ataques para llenado de discos. Esta relacionado con lo anterior, si se envían bloques válidos pero inadecuados se fuerza a almacenar la cadena, pero con información innecesaria e inadecuada.
- Consumo de memoria. Tanto de forma accidental como malintencionadamente, el nodo de sincronización puede enviar los bloques fuera de orden. Esto obliga a mantenerlos en memoria ya que no pueden ser validados hasta que se reciba el predecesor, pudiendo causar problemas de excesivo consumo de memoria al receptor.

A causa de estos problemas a partir de la versión 0.10.0 se incorpora otro método de sincronización llamado *header-first*. La diferencia principal consiste en que en lugar de obtener la cadena de bloques correcta se buscan primero las cabeceras, una vez obtenidas estas se puede realizar la descarga de los bloques correspondientes en paralelo.

De forma análoga a lo que ocurre mediante el método *block-first* un nodo al iniciarse sólo dispone del bloque génesis. Para comenzar el proceso selecciona otro nodo, llamado nodo de sincronización (*sync node*), y se le envía un mensaje *getheaders*. El nodo responderá con el máximo posible de cabeceras, estos es, dos mil. Para ello utiliza el mensaje *headers*.

El nodo receptor puede validar parcialmente las cabeceras recibidas (la validación completa requiere los bloques). Una vez que se ha realizado esta validación puede realizar dos tareas en paralelo: continuar descargando más cabeceras usando el método *getheaders* y descargar los bloques cuyas cabeceras ha validado. Un aspecto importante es que además no tiene porque descargar los bloques del nodo de sincronización, con lo que puede realizar múltiples descargas en paralelo de distintos nodos y así no verse limitado por la velocidad de envío del nodo de sincronización.

Una vez realizada la sincronización inicial el nodo se encuentra disponible tanto para generar bloques y emitir su resultado como para recibirlos. Cuando un nodo *mining* consigue generar un bloque dispone de dos métodos para comunicarlo al resto de nodos:

- *Unsolicited Block Push*. El nodo envía un mensaje de tipo *block* message a todos los nodos a los que está conectado con el nuevo bloque encontrado.
- *Standard Block Relay*. El nodo envía un mensaje de tipo *inv* a todos sus nodos conectados indicando que cuenta en su inventario con un nuevo bloque. Los otros nodos pueden contestar solicitando el bloque mediante el mensaje *getdata*, también pueden enviar un mensaje *getheaders* para tratar de evitar bloques huérfanos.
- *Direct Headers Announcement*: un nodo de reenvío puede evitar el retraso introducido por mandar un mensaje *inv*, al que otros nodos contestarán con un mensaje *getheaders*, enviando directamente un mensaje *headers.* El nodo receptor en este caso valida la cabecera y solicita el bloque completo mediante un mensaje *getdata*.

Para enviar nuevas transacciones a un nodo se comienza con un mensaje de *inv*. El nodo puede aceptar o no la solicitud, si lo hace contestará con un mensaje *getdata*, al cual el generador de la transacción contestará enviando la transacción en si misma con un mensaje de tipo *tx*. El nodo que recibe la transacción reenvía esta transacción de la misma manera a otro tercero.

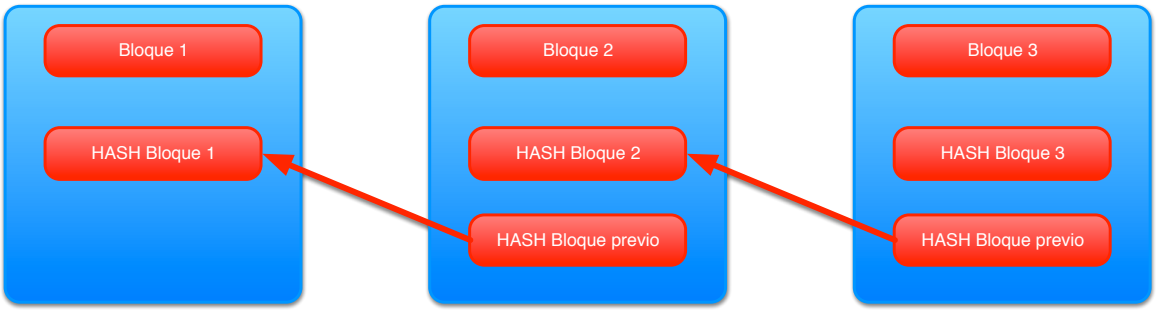
Los nodos completos mantienen en memoria todas aquellas transacciones que son susceptibles de ser incorporadas en el siguiente bloque. Los nodos *mining* necesitan esta información ya que son los que realmente las incluyen en los bloques que están tratando de generar, pero esa información también es útil para todos los nodos ya que así mantienen la información de las transacciones no confirmadas.

5. Cadena de bloques

5.1. Descripción

Blockchain, o cadena de bloques, es el elemento que proporciona el libro de cuentas (*ledger*) de Bitcoin. Es una lista ordenada de bloques (cada bloque tiene una referencia únicamente a su predecesor) siendo estos los que contienen las transacciones validadas.

Cada bloque se identifica con un hash generalmente generado mediante SHA256. Este elemento se utiliza para realizar el enlace con el bloque previo, ya que cada bloque incluye un campo que contiene el hash del bloque anterior:



Eventualmente se puede dar la posibilidad de que existan varios bloques apuntando al mismo bloque previo o padre. Esta situación ocurre cuando se generan bloques simultáneamente por parte de varios nodos *mining* distintos. Al propagarse a través de la red otros nodos recibirán estos bloques con el mismo bloque padre, conforme se vayan generando nuevos bloques que sigan una línea de descendencia u otra esto dará lugar una bifurcación. Cuando se genera un nuevo bloque, en función de quien descienda, el resto de nodos tendrán que descartar el otro bloque, ya que para resolver el siguiente bloque deben elegir la cadena de bloques más extensa, o lo que es lo mismo, con más dificultad.

Otra circunstancia que se puede dar es la aparición de bloques sin ascendencia, también denominados bloques huérfanos. Esto ocurre en situaciones similares a la anterior y en las que también concurre la circunstancia de un nodo recibe un bloque que desciende de un bloque que ese nodo aún no ha recibido. Este bloque debe quedar almacenado temporalmente hasta que se pueda incorporar a la cadena, al recibir el padre, o deba ser descartado definitivamente.

Cada nodo de la red contiene una lista que ha sido validada por este. Cuando varios nodos contienen los mimos bloques se considera que han alcanzado consenso. Para alcanzar este consenso se aplican diversas reglas denominadas *consensus rules*.

Existe un bloque inicial denominado bloque génesis. Todos los bloques dependen de este, si se recorren sucesivamente desde el más reciente se pasaría por todos hasta llegar al susodicho bloque génesis. Todos los clientes contienen la información del bloque génesis, de esta forma y a partir de este pueden reconstruir la cadena de bloques completa.

5.2. Bloque

El bloque se compone básicamente de una cabecera, cuyo tamaño es 80 bytes, junto con el conjunto de transacciones que incorpora. La cabecera contiene la siguiente información:

Nombre	Tamaño	Tipo	Descripción
version	4 bytes	int32_t	Número de versión que indica las reglas de validación utilizadas.
previous block header hash	32 bytes	char[32]	Referencia al hash del bloque previo en la cadena.
merkle root hash	32 bytes	char[32]	Hash del árbol merkle de las transacciones del presente bloque.
time	4 bytes	int32_t	Fecha y hora del comienzo de la creación del bloque por parte del nodo *mining*.
nBits	4 bytes	int32_t	Valor codificado del umbral objetivo del hash del encabezado.
nonce	4 bytes	int32_t	Valor variable decidido por el nodo *mining* con el objetivo de conseguir un hash menor o igual que el definido en el umbral.

Existen cuatro versiones de bloque:

- Versión 1, corresponde con la introducida en el bloque génesis siendo la original del protocolo.
- Versión 2, introducida en la versión 0.7.0.
- Versión 3, usada a partir de la versión 0.10.0.
- Versión 4, en uso dede la versión 0.11.2

Además de las transacciones como tal cada bloque incluye un resumen de estas usando una estructura de árbol *merkle*. Este tipo de estructura permite que gran número de datos separados puedan ser ligados a un único valor de hash, el hash del nodo raíz del árbol. De esta forma proporciona un método de verificación segura y eficiente de los contenidos de grandes estructuras de datos.

5.3. Direcciones

Una dirección Bitcoin se compone de un conjunto de dígitos y caracteres, estas comienzan por por 1 o por 3. Esta puede ser compartida con cualquier otro usuario para recibir fondos.

La dirección Bitcoin deriva de la clave pública, que a su vez parte de la clave privada, mediante el uso de una función hash y otras operaciones como codificaciones. La función hash garantiza que el flujo es irreversible, esto es, a partir del resultado de la función hash es imposible volver a obtener el origen. Específicamente el proceso para conseguir una dirección a partir de una clave privada es el siguiente:

1. Generar una clave pública a partir de la clave privada.
2. Calcular el hash de la clave pública mediante SHA-256.
3. Calcular el hash del resultado anterior mediante RIPMED-160.
4. Añadir el byte de versión delante del hash que ha creado RIPEMD-160.
5. Calcular el hash sobre el resultado anterior mediante SHA-256.
6. Nuevamente calcular el hash sobre el resultado anterior mediante SHA-256.
7. Seleccionar los primeros 4 bytes del último hash SHA-256. Ese es el identificador checksum de la dirección pública.
8. Añadir los 4 bytes del checksum del punto anterior al hash extendido RIPEMD-160 del punto 4.
9. Codificar la cadena resultante mediante Base58Check. Este paso proporciona el como resultado final la dirección de Bitcoin.

5.10. Cadena de bloques publica y privada

Las cadenas de bloques públicas, como Bitcoin, están abiertos para cualquiera sin excepciones. Así pues, es posible unirse a esta cadena de bloques y obtener la historia completa de la cadena, hacer uso de la misma intercambiando transacciones, utilizar contratos inteligentes, etc. En definitiva, está abierto a la participación de quien así lo desee.

La ventaja de un sistema como este es la total descentralización: la cadena de bloques es pública, inmutable y no existe ninguna entidad que pueda manipularla. Además, al ser un sistema distribuido es mucho más resistente a ataques ya que no existe un único objetivo central que controle la red al completo. Cuantos más nodos participan en la cadena de bloques más difícil es atacarla porque además cada nodo guarda una copia de la misma.

Por contra las cadenas de bloques privadas, conocidas como *Permissioned Blockchains*, si están controladas por una entidad. El acceso a las mismas ha de ser autorizado, además no todos los participantes disponen de los mismos permisos.

En el caso de las cadenas de bloques privadas se puede dar la circunstancia de que no se requiera la prueba de trabajo, siendo por tanto cadenas de bloques sin nodos *mining*. Por este hecho muchos no consideran este tipo de redes como cadenas de bloques reales.

Un ejemplo de una cadena de bloques privada lo constituye Hyperledger. Es un proyecto de código abierto que comenzó a finales del dos mil quince con el objetivo de crear un ecosistema centrado en crear soluciones de código abierto en el ámbito corporativo con DLT (*Distributed Ledger Technology*) para diversos usos. Actualmente no cuenta con una moneda electrónica.

6. TRANSACCIONES

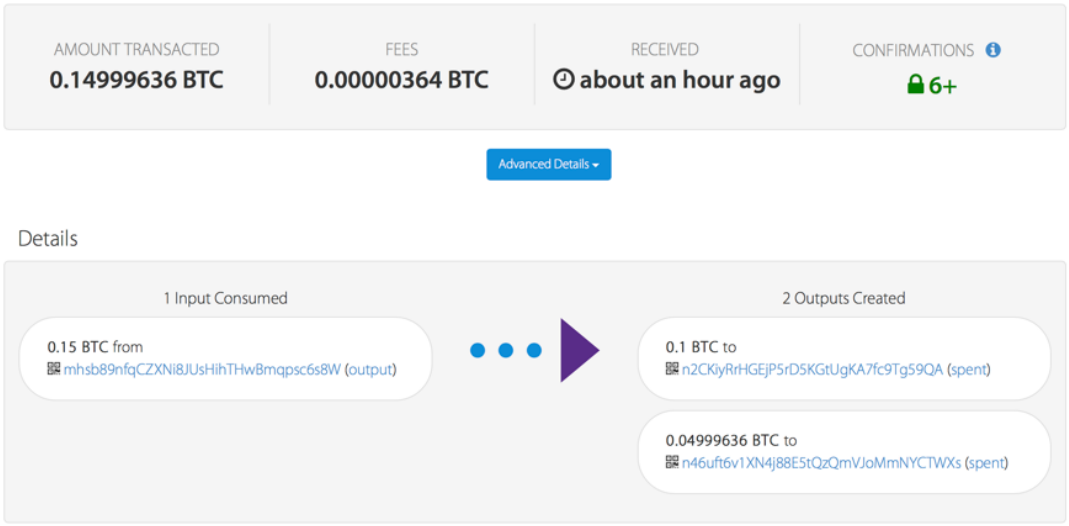
6.1. DESCRIPCIÓN

Cada transacción representa una transferencia de fondos entre participantes de la red Bitcoin. Son la parte fundamental de Bitcoin y realmente para lo que está creado todo el sistema. Estas transacciones son las que se muestran públicamente en el libro de cuentas (*ledger*).

Cada transacción cuenta con tres partes principales:

- Entrada o entradas: direcciones de origen de los Bitcoin a transferir.
- Cantidad: cuantía a transferir.
- Salida o salidas: direcciones de destino de los Bitcoin a transferir o sobrantes (que se devuelven al emisor de los fondos en otra dirección).

En la siguiente captura se puede observar una transacción, realizada en la red de pruebas testnet3, en la que que se envían 0.1 Bitcoins. Es importante destacar que el importe total transferido es superior, pero una de las direcciones de salida pertenece al emisor de la transferencia. El resultado es que el receptor obtiene los 0.1 Bitcoins que se desean transferir y el emisor recibe la cantidad sobrante (UTXO) menos las comisiones (0.00000364 Bitcoins en este caso).



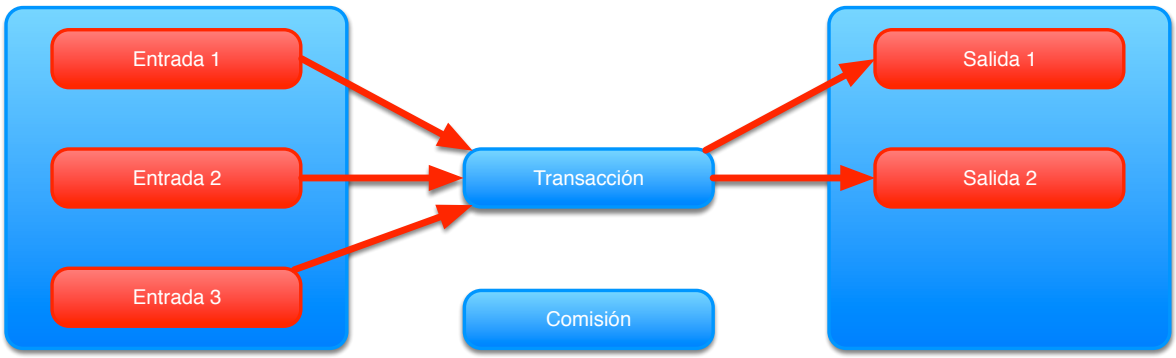
6.2. Entradas y salidas

Como se ha indicado anteriormente una transacción se compone fundamentalmente de estos elementos: el origen u origines de los fondos a transferir, destino o destinos de los mismos y las comisiones aplicadas.

Estos orígenes o entradas (*inputs*) realmente provienen de transacciones previas, es decir, parten de salidas de transacciones anteriores. Es necesario disponer de la clave de firma para poder usar esas direcciones.

Las salidas determinan el nuevo propietario de los fondos transferidos. Cada salida consta de dos datos: la cantidad de fondos que se envían y la dirección de destino. Como sólo el propietario de los fondos puede dar la autorización para que los reciba la nueva dirección, es necesario que la transacción sea firmada con la clave privada del emisor.

La siguiente imagen representa el modelo de una transacción con múltiples entradas, múltiples salidas y comisiones:



Cada transacción de Bitcoin usa todos los fondos existentes en las direcciones de entrada. Por tanto, la suma de todas las entradas no se puede fraccionar, aunque sea superior a la cantidad que se desea transferir. En esta situación lo que se genera es una dirección de salida a través de la cual el emisor recibe el resto sobrante de la transferencia de fondos.

En este punto aparece la comisión. La suma de los valores de entrada es igual a la de los valores de salida más la comisión. Esta comisión es el incentivo para que el nodo *mining* incorpore esta transacción en el bloque que está procesando. Si se pagan más comisiones los nodos *mining* priorizan incorporar esa transacción al bloque que están generando, por

tanto, si deseamos incorporar esa transacción cuanto antes se deberá incrementar la comisión.

No obstante, el pago por transacción no es el único factor para determinar la prioridad de incorporación de la misma al bloque. Por ejemplo, generalmente se espera una mayor comisión de una transacción más compleja ya que ocupa más espacio. Por tanto, aunque una transacción vaya a pagar mayor comisión que otra, se puede dar el caso que se incorpore la más simple. Hay otros factores como dependencias de transacciones dentro del mismo bloque que también puede alterar el orden de incorporación.

Para que una transacción se considere como válida deben concurrir varios factores:

- La suma de las entradas debe ser igual o superior a la suma de las salidas.
- Las firmas de cada entrada deben ser válidas, es decir, han sido firmadas por la clave privada correspondiente con la clave pública de la dirección usada.
- Las entradas existen y no han sido gastadas (se debe evitar la doble imposición o gasto). Este proceso se realiza consultando la información denominada *Unspent Transaction Outputs Cache*. Cuando una transacción llega a un nodo se verifica que las entradas existen dentro de *UTXO*, si todas lo están esto quiere decir que estas entradas corresponden a salidas previas de transacciones anteriores y por tanto todo es correcto.

6.3. Comisiones

Prácticamente todas las transacciones incluyen comisiones. Estas comisiones, junto con el premio de obtener nuevos Bitcoins, son la recompensa que reciben los nodos *mining* por prestar sus capacidades y colaborar en la red Bitcoin. Es cierto que hay nodos que pueden llegar a aceptar transacciones sin comisiones, por ello se indica que no todas las transacciones comportan pago de comisiones, pero tal como evoluciona la red es probable que finalmente sean el único sustento posible de la misma.

Las comisiones actúan como incentivo para que la transacción sea incorporada en el próximo bloque sobre el que está trabajando el nodo. Un detalle diferenciador con la banca tradicional es que el cálculo de estas comisiones no se realiza en función de la cantidad de fondos transferidos sino del tamaño en bytes de la transacción. Esto da lugar a que una

transacción con mayor número de entradas y salidas tenga un coste superior a otra más simple, por ejemplo, con una única entrada y una única salida.

Aproximadamente una transacción sencilla, con una sola entrada y una sola salida, ocupa alrededor de 137 bytes. Cada entrada adicional supone 113 bytes y cada salida extra 34 bytes. Combinando estos elementos es claro ver que una transacción con mayor cantidad de entradas y salidas requiere un mayor esfuerzo por parte del nodo *mining* y por tanto la expectativa de este será una mayor comisión.

El coste de la comisión no es fijo. Por ejemplo, Bitcoin Core tiene fijado por defecto una comisión de 0.0001 Bitcoin, así que las comisiones inferiores a esta se consideran gratuitas y tienen la menor prioridad.

Existen algoritmos para calcular la comisión adecuada que se basan en la capacidad del sistema y las comisiones ofrecidas por otras transacciones con las que se esta compitiendo en ese momento para incorporarse al bloque. También existen servicios de terceros que calculan en tiempo real que comisión se debe aplicar, teniendo en cuenta que prioridad se necesita o desea para incorporar la transacción.

Un aspecto importante del cobro de comisiones, aparte del beneficio en si mismo para el nodo *mining*, es que ayudan a evitar ataques por denegación de servicio. Un ataque a la red podría realizarse generando una gran cantidad de transacciones, pero al existir las comisiones esto tiene un impacto económico y limita la posibilidad de que ocurra.

6.4. Transacción coinbase

Es la primera transacción que se añade en un bloque. La construye el propio nodo *mining* y constituye la recompensa en Bitcoins si es capaz de añadir el bloque a la cadena.

Esta transacción recoge tanto las comisiones por las transacciones añadidas como la recompensa de creación de Bitcoin y transfiere esa cantidad a una dirección del dueño o usuario del nodo. De esta manera cuando se confirma la transacción y se añade a la cadena de bloques esos fondos pasar a ser del nodo *mining* que incorporó el bloque.

A diferencia de las transacciones normales la entrada no parte del *UTXO* sino que la única entrada se denomina *coinbase*.

El cálculo de la recompensa en Bitcoins se realiza teniendo en cuenta el *block height* (número de bloques entre el presente bloque y el bloque génesis). La recompensa inicial era cincuenta Bitcoins, esta se va reduciendo a la mitad cada dos cientos diez mil bloques. Actualmente es de doce Bitcoins y medio, se estima que al ritmo actual se reducirá de nuevo en el año dos mil veinte.

En esta web se puede consultar tanto estadísticas como previsiones de la red Bitcoin, incluyendo el momento aproximado en el que se dividirá la recompensa:

http://www.bitcoinblockhalf.com

7. Minado

7.1. Descripción

En muchas ocasiones al tratar de Bitcoin se establecen paralelismos con la minería que se realiza para obtener materias primas o metales preciosos. En cierto modo es acertado ya que ambos tipos de minería obtienen una recompensa, ya sea en forma de los productos físicos y tangibles obtenidos o ya sea mediante la moneda virtual.

Realmente el objetivo del minado en Bitcoin no es la generación de nuevos Bitcoins, estos son la recompensa. El minado realmente asegura la red y da lugar a la existencia del consenso sin una autoridad central, clave fundamental del funcionamiento de Bitcoin.

Los nodos *mining* son los encargados de crear los nuevos bloques, a los que incorporan las transacciones que validan, y a su vez tratan de añadir a la cadena de bloques. Reciben dos tipos de incentivos: las nuevas monedas creadas en el bloque y todas las comisiones de las transacciones incluidas en el bloque.

Para obtener la recompensa los nodos compiten para resolver un problema matemático. Esto da lugar a la prueba de trabajo, lo cual es la base de la seguridad en Bitcoin.

La generación de moneda en Bitcoin se realiza mediante este proceso. No existe otra forma de crear Bitcoins. Además, como la cantidad es fija se estima que sobre el año dos mil ciento cuarenta (debido a la reducción paulatina de la recompensa) se habrán generado todos los Bitcoin. Llegado esta situación los nodos *mining* sólo percibirían las comisiones de las transacciones que procesaran e incorporaran a la cadena de bloques.

7.2. Consenso

Bitcoin se caracteriza por la inexistencia de una autoridad central que verifica todas las transacciones, aunque todos los nodos disponen de la cadena completa sobre la que pueden comprobar la validez de las transacciones.

Para alcanzar el consenso entre todos los nodos ocurren las siguientes acciones de forma independientemente en cada nodo:

- Verificación por parte de cada nodo completo de cada transacción.
- Incorporación, por parte de los nodos *mining*, de estas transacciones en los nuevos bloques junto con la prueba de trabajo.
- Verificación por parte del resto de nodos de los nuevos bloques antes de añadirlos a la cadena.
- Selección de la cadena optima por parte de todos los nodos en base a la prueba de trabajo acumulada.

La verificación de las transacciones se realiza validando una serie de criterios:

- Correcta sintaxis y estructura.
- Verificación que tanto entradas como salidas no son nulas.
- Tamaño inferior al máximo del bloque.
- Valores dentro de rango posible.
- No se aceptan entradas con hash igual a 0.
- nLockTime <= INT_MAX, tamaño en bytes >= 100y sig opcount <= 2
- Rechazar transacciones no estándar.
- Rechazar la transacción si ya existe en el *transaction pool* o en un bloque ya incorporado a la cadena.
- Si para una entrada, la salida referenciada existe en otra transacción en el *transaction pool*, se rechaza.
- Cada entrada si no existe la salida previa se considera una transacción huérfana y se añade al *transaction pool* en espera.
- Para cada entrada la salida referenciada debe existir y no haber sido consumida.
- Se rechaza si la suma de entradas es inferior a la suma de salidas.

- Si la comisión es muy baja (en base a un parámetro definido) la transacción también se rechaza.

Como se puede apreciar la lista de verificación es compleja y larga. Conforme se van validando las transacciones estas se añaden al *transaction pool* con el objetivo de ser incorporadas a un nuevo bloque. Este proceso se realiza en paralelo al proceso de generación de otro bloque con el objetivo de tener todas esas transacciones disponibles para agregarlas en el siguiente bloque.

Los bloques sobre los que está trabajando un nodo *mining* se denominan bloques candidatos. El bloque se convierte en válido cuando el nodo es capaz de encontrar la solución a la prueba de trabajo.

El algoritmo de la prueba de trabajo consiste en la búsqueda de un valor, denominado *nonce*, que hace que la función hash SHA-256 sea menor que un valor determinado denominado *target*. Como la función hash es unidireccional no hay forma de saber el *nonce* correcto o de diseñar de cualquier modo el bloque correcto. La única forma de encontrar un *nonce* valido es intentarlo aleatoriamente hasta que uno genera un valor válido.

La dificultad viene dada en función del valor *target* buscado. Esta se ajusta para que cada bloque se genere aproximadamente cada diez minutos. Esta operación se realiza en cada nodo de forma automática e independiente. Este valor no está relacionado con el número de transacciones, sino con la capacidad de cálculo de la red. Si esta bajara el objetivo también lo haría y de esta forma se podría continuar trabajando, si por el contrario la capacidad de calculo sube será necesario que el *target* aumente la complejidad para seguir produciendo nuevos bloques con la cadencia prevista de aproximadamente diez minutos.

Cuando un nodo obtiene un *nonce* adecuado para cumplir el *target* establecido este nodo transmite el bloque al resto de nodos a los que está conectado. Conforme se propaga por la red el resto de nodos lo incorporan a su cadena de bloques, abandonando por su parte la búsqueda del valor para el bloque de la misma altura (es decir, el que tendría que ir en la posición del recibido). Estos nodos comienzan a trabajar en un nuevo bloque y relacionándolo con el recibido (el recibido es el padre del bloque sobre el que se ponen a trabajar).

Este bloque ha de ser validado por todos los nodos de la red de forma independiente. Sólo lo retransmiten si las pruebas de validación resultan satisfactorias. Para validar un bloque se aplican varios criterios:

- La estructura es válida.
- Cumple el objetivo definido para la prueba de trabajo.
- La fecha y hora es menor a dos horas en el futuro.
- El tamaño está dentro de los márgenes correctos.
- La primera transacción, y sólo esta, en una transacción *coinbase*.
- Las transacciones incluidas son válidas.

Al validar todos los bloques por parte de todos los nodos se evita que existan nodos que acusen deshonestamente.

A continuación, se busca el consenso de la propia cadena de bloques. Cuando un nodo termina de validar el bloque recibido intenta adicionarlo a la cadena de bloques. La cadena válida es la que acumula mayor prueba de trabajo acumulada. De esta forma los nodos pueden llegar a alcanzar consenso global en la red. Las discrepancias que puedan aparecer son temporales y se van resolviendo conforme se añade más trabajo.

8. Seguridad

8.1. Sistema descentralizado

La seguridad de Bitcoin gira en gran media en ser un sistema totalmente descentralizado, que no depende de ninguna entidad central para funcionar. Las transacciones que se registran en la red Bitcoin son públicas y no pueden ser manipuladas. Dado que la seguridad no se basa en el control de acceso a la red si no en la prueba de trabajo esta puede ser totalmente pública y sin cifrado en las comunicaciones.

Al ser un sistema descentralizado también se evita que exista un único punto de ataque. Además, cuantos más nodos participan en la red la dificultad del ataque se incrementa, especialmente si se tiene en cuanta que cada nodo dispone de la cadena de bloques al completo, pudiendo restaurarse la red a partir de los nodos que sobrevivieran a un teórico ataque.

8.2. Integridad cadena de bloques y transacciones

La cadena de bloques, como su nombre indica, es una sucesión de bloques enlazados. Estos bloques contienen las transacciones y están vinculados entre si. Por tanto modificar la cadena de bloques para introducir un bloque modificado es prácticamente imposible. Teóricamente un sistema necesitaría el 51% o más de capacidad de cálculo de la red para actuar fraudulentamente.

Por otro lado, alterar una transacción concreta de un bloque es imposible ya que se debería generar un bloque con exactamente el mismo hash habiendo alterado su contenido. Además cada transacción está firmada por una clave. Cualquier alteración en la transacción daría lugar a que la firma sea inválida y por tanto el bloque también.

Cada bloque contiene también un sello de tiempo. Para que se pueda aceptar un bloque el sello de tiempo (*timestamp*) debe encontrarse en un rango comprendido entre la mediana de los sellos de tiempo de los últimos once nodos y dos horas después de la hora de la red. Este también previene que se pueda alterar la cadena de bloques.

8.3. Seguridad claves y usuarios

Un aspecto clave es la seguridad en la gestión y almacenaje de las claves privadas. Sin estas claves privadas no es posible realizar transacciones con las direcciones asociadas, con lo que la pérdida de estas es sinónimo de perder los fondos. Si las claves se pierden o destruyen no hay forma de recuperarlas y los fondos asociados a esas direcciones nunca se podrán utilizar. Si las claves son obtenidas por un tercero podrá hacer uso fraudulento de todos los fondos asociados.

Por ello es importante gestionar y almacenar adecuadamente las claves. Por ejemplo, si están almacenadas en un ordenador y este es comprometido se podría dar el caso de que las claves fueran capturadas y utilizadas. Otro problema sería la pérdida o destrucción de este ordenador, ya que si las claves no están almacenadas en otro lugar, no habría forma de recuperar el control de las direcciones asociadas a las claves.

Existen varias alternativas desde dispositivos electrónicos que salvaguardan esta información hasta la impresión en papel de las propias claves y posterior custodia de las mismas en formato papel. El usuario debe encontrar un balance adecuado para asegurar sus activos. Muchas veces una buena opción pasa por combinar distintos sistemas y no agregar todos los fondos en un único monedero electrónico.

8.4. Computación cuántica

La computación cuántica se basa en el uso de cúbits en lugar de bits, lo que da lugar a una nueva lógica que permite otros algoritmos. Lo interesante es que ciertas tareas pueden ser resueltas con mayor efectividad bajo el paradigma de la computación cuántica frente a la tradicional.

En el caso de Bitcoin un ordenador cuántico podría realizar un ataque contra la criptografía de clave privada. En un sistema tradicional el número de operaciones a realizar para un ataque de fuerza bruta y obtener la clave privada de una dirección Bitcoin necesita ejecutar del orden de 2^{128} operaciones, lo cual imposibilita este tipo de ataque. Sin embargo con un ordenador cuántico necesitaría sólo 128^3 operaciones para romper una clave privada de Bitcoin mediante el algoritmo Shor.

Es cierto que la tecnología actual de ordenadores cuánticos todavía no es capaz de manejar la cantidad de cúbits necesarios para realizar este tipo de ataque y probablemente pasen muchos años hasta que esto ocurra.

9. Otros usos de la cadena de bloques

9.1. Contratos inteligentes

Detrás de un contrato inteligente (*Smart contracts*) existe un programa que, sin estar controlado por ninguna de las partes involucradas en un contrato, asegura y hace cumplir los acuerdos establecidos entre las partes.

Los contratos tradicionales son documentos, verbales o escritos, sujetos a leyes y jurisdicciones, que muchas veces requieren notarios para refrendarlos. Además, pueden estar sujetos a interpretaciones contradictorias y generar de esta forma conflictos. Por contra los contratos inteligentes se ejecutan por si mismos sin intermediarios ni mediadores. Al final se tratan de elementos cuya programación determina en si misma el contenido del contrato.

Conjugando la existencia de estos contratos con la cadena de bloques se obtiene un sistema en el que los contratos son públicos y además están validados por las partes que los han suscrito. De esta manera se evitan fraudes y dificultades en la ejecución de los mismos.

Algunos de los posibles usos de los contratos inteligentes que se pueden producir:

- Testamento inteligente. Son contratos que se ejecutan al fallecer una persona y que reparten sus bienes y activos además de si es necesario publicar información.
- Préstamos. Al fijarse unos plazos y cantidades a devolver, ante un incumplimiento de los compromisos, el contrato inteligente podría ejecutar acciones como retirar las garantías que lo avalaban.
- Automatización de pagos. Si se desea realizar un pago periódico o en un función de alguna circunstancia el contrato verificaría que se dan las condiciones para realizar el pago y hacerlo efectivo en tal caso.
- Seguimiento salud personal. Mediante dispositivos que permiten seguir la evolución de la salud del individuo se pueden dar recompensas. Por ejemplo existen sistemas que generan logros por acudir al gimnasio o realizar una cantidad determinada de ejercicio.
- Distribución de royalties. El contrato puede calcular los royalties que corresponden a cada artista en función de los criterios que se establezcan y realizas los pagos de forma automática.

Ethereum es probablemente el sistema basado en cadena de bloques más popular para crear contratos inteligentes. Una de las claves de diseño de Ethereum fue precisamente soportar este tipo de contratos, por el contrario Bitcoin fue creado principalmente como una moneda electrónica descentralizada. No obstante Bitcoin ha evolucionado para poder incluir funcionalidad de contratos inteligentes, aunque no de forma tan completa como Ethereum.

9.2. Registro y verificación de datos

La cadena de bloques es útil para almacenar transacciones en la red Bitcoin de forma inmutable, de la misma manera se puede utilizar para conservar cualquier otro tipo de información. De esta forma los datos no se tienen que gestionar por un tercero ya que se genera un registro de la información distribuido e inalterable.

Existen diversos casos de uso posibles:

- Registro de la propiedad. Mediante este registro se conocería que es el dueño de cada inmueble además de todas las transacciones de compraventa realizadas.
- Registros de nacimientos, defunciones, matrimonios, divorcios, etc. El gobierno de Estonia es pionero aplicando esta tecnología permitiendo que sus ciudadanos registren esta actividad en una cadena de bloque denominada *Horizon*.
- Registros de la propiedad intelectual. Al igual que transacciones u otras operaciones se podría disponer de información relacionada con la propiedad intelectual tal como fecha de registro, autor, título, etc.

9.3. Voto electrónico

Tal y como ocurre con Bitcoin el uso de la cadena de bloque permite resolver dos de los principales desafíos de una votación: anonimato y uso único (en moneda se trata de evitar el doble gasto). Al no existir ninguna autoridad central es imposible de manipular e incluso todo el sistema es verificable por terceros.

Un factor clave sería el abaratamiento de las votaciones, así como la rapidez en conseguir evaluar los resultados. De esta forma se podrían realizar mayor número de elecciones y

referéndums sin incrementos de coste. La primera votación con este sistema la realizó el partido danés Liberal Alliance en una votación interna.

9.4. IoT

El internet de las cosas (*Internet of Things*) hace referencia a todos aquellos objetos o dispositivos del ámbito cotidiano que se encuentran conectados a Internet y que cuentan con algún tipo de inteligencia. De esta manera permite que cualquier objeto pueda comunicarse con otro de su alrededor y llevar a cabo una determinada tarea o función.

Generalmente las plataformas IoT están basadas en modelos centralizados, así pues, existe una entidad que controla las conexiones entre los dispositivos. Mediante la cadena de bloques se puede realizar el intercambio de información de forma segura y fiable al tiempo que se crea un registro permanente de todos los mensajes intercambiados entre los distintos dispositivos inteligentes conectados. De esta manera se salva la dependencia de un sistema central y a su vez se mejora la seguridad.

IBM y Samsung han desarrollado una plataforma, denominada *ADEPT*, para construir una red distribuida de dispositivos basada en la cadena de bloques. Utiliza tres protocolos:

- Ethereum para los contratos inteligentes.
- BitTorrent para el intercambio de ficheros.
- Telehash para mensajería.

Como ejemplo IBM cita que “una simple lavadora puede llegar a ser un dispositivo semi-autónomo, capaz de gestionar su propio suministro de consumibles, realizar el auto-servicio y su mantenimiento, e incluso negociar con otros dispositivos pares, tanto en el hogar, como fuera, para optimizar su entorno”. Según se explica en la descripción de la plataforma una lavadora puede ser capaz de, mediante contratos inteligentes, realizar órdenes de compra de, por ejemplo, detergente.

9.5. Usos militares

Existen varias iniciativas para usar la cadena de bloques en aplicaciones y usos relacionados con el ejército y la seguridad. Por ejemplo DARPA, la agencia desde la que surgió Internet, busca utilizar esta tecnología para crear un sistema de mensajería. Mediante este sistema se persigue disponer de una plataforma totalmente segura que permita enviar mensajes cifrados a los operarios en situaciones de combate.

Otro ejemplo proviene de la OTAN, que ofrece unos desafíos tecnológicos y entre las propuestas cita tres posibles temáticas relacionados con el uso de la cadena de bloques en el ámbito militar:

- Aplicación de la cadena de bloques en la logística militar.
- Aplicación de la cadena de bloques en finanzas.
- Cualquier otra utilidad de la cadena de bloques para el ejército.

10. Otras cadenas de bloques

10.1. Ethereum

Ethereum es una de las cadenas más bloques más populares tras Bitcoin. Desde su origen fue concebido para mejorar a este. Dispone de un lenguaje Turing completo integrado, lo que permite escribir contratos inteligentes y aplicaciones descentralizadas. También difiere de Bitcoin en el algoritmo utilizado, ya que Ethereum usa propio denominado *Ethash* basado en SHA3 frente a SHA2 de Bitcoin.

La moneda utilizada en la red Ethereum se denominada *Ether*. Al contrario que con Bitcoin no existe un límite en la creación de moneda, el ritmo de creación de la misma es de 18 millones anuales. Actualmente su capitalización de mercado es sólo superada por Bitcoin.

La creación de bloques es extremadamente rápida en Ethereum, ya que se genera uno nuevo cada dieciséis segundos, lo que permite validar las transacciones con mucha rapidez. Los nodos *mining* reciben recompensa tanto por el bloque creado como por las comisiones. La dificultad de creación de bloque se recalcula tras cada bloque generado, por el contrario Bitcoin ajusta la dificultad cada dos mil dieciséis bloques.

10.2. Litecoin

Litecoin es una alternativa a Bitcoin, siendo muy similar a este en el planteamiento técnico. Fue creada por Charlie Lee y se introdujo en octubre de dos mil once.

Existen ciertas diferencias entre ambas:

- Velocidad de las transacciones. En Litecoin se procesa un bloque cada dos minutos y medio frente a los diez de Bitcoin. Esto da lugar a que las transacciones puedan ser confirmadas con mayor rapidez.
- Cantidad posible de monedas en circulación. Frente a los 21 millones de Bitcoin, Litecoin alcanzará los 84 millones.

- Algoritmo *scrypt* en lugar de *hash*. El uso de este algoritmo permite en cierta medida la capacidad de realizar minería con menos potencia de cálculo, ya que es un algoritmo más rápido y más intensivo en memoria, lo que limita la creación de ASICs (pero no lo impide).

Su capitalización de mercado esta por debajo tanto de Bitcoin como de Ethereum. En el momento actual es la sexta moneda electrónica en cuanto a capitalización de mercado.

10.3. Bitcoin Cash

Bitcoin Cash es una versión alternativa de Bitcoin. Surgió como una bifurcación de Bitcoin en agosto del dos mil diecisiete, momento en el que se separó de la cadena de bloques de Bitcoin creando una paralela a la de este. Esta separación vino motivada por la disconformidad de grupos de participantes en la red Bitcoin acerca de la sostenibilidad y escalabilidad de esta.

Bitcoin Cash hace uso de un tamaño de bloque mayor para poder incorporar más transacciones en cada bloque y de esta manera aumentar globalmente la velocidad de procesamiento de transacciones de la red. Se partió de un tamaño inicial de ocho megabytes frente a un megabyte de Bitcoin, aunque actualmente este tamaño se ha vuelto a incrementar hasta los treinta y dos megabytes.

Su capitalización de mercado actual está sólo por debajo de Bitcoin, Ethereum y Riple.

10.4. Cardano

Cardano es una cadena de bloques, moneda electrónica y plataforma de contratos inteligentes. Su desarrolló se inició en el año dos mil quince por parte de la empresa *IOHK*, la cual se dedica al desarrollo de soluciones basadas en cadena de bloques. Se considera una tecnología de tercera generación dentro del ámbito de las cadenas de bloques (Bitcoin sería primera generación y Ethereum segunda generación).

Cardano no utiliza el algoritmo de prueba de trabajo, sino que se basa en un algoritmo de prueba de participación denominado *Ouroboros*. En el caso del algoritmo de prueba de

trabajo los nodos *mining* compiten por encontrar la solución creando el siguiente bloque, por contra con *Ouroboros* se selecciona al azar el nodo que creará el siguiente bloque. Cuanto mayor sea la cantidad de monedas que este posea, más probabilidad tendrá de ser seleccionado. De esta manera se reduce la cantidad de potencia computacional necesaria y se limita la cantidad de energía necesaria para sustentar la red.

Su moneda electrónica se denomina *Ada* y ocupa el séptimo puesto en la actualidad en cuanto a capitalización de mercado. Es importante hacer notar que dado que no hay prueba de trabajo no se genera moneda de esta manera, los nodos eso si reciben comisiones. La cantidad de moneda disponible en la red es fija, específicamente cuarenta y cinco mil millones.

11. Conclusiones

11.1. Resumen

La tecnología sobre la que se sustenta Bitcoin, la cadena de bloques, ofrece muchas posibilidades al margen de una moneda electrónica. Lamentablemente Bitcoin en la actualidad está siendo utilizado en gran medida para especular e intentar ganar dinero con la plataforma, traicionando en cierta manera el espíritu original de un sistema monetario totalmente independiente. Según algunos estudios se estima que la red Bitcoin puede llegar a consumir el 0,5% de la producción eléctrica global:

https://www.sciencedirect.com/science/article/pii/S2542435118301776

En opinión de muchos esto puede llegar a condenar a la plataforma como tal, pero si es cierto que, la tecnología de cadena de bloques, puede ser aprovechada para múltiples usos distintos al margen de la moneda electrónica Bitcoin.

Los objetivos del presente trabajo de fin de máster consistían en describir Bitcoin y la cadena de bloques. Realmente son muchísimos los aspectos sobre los que se puede incidir: como funciona, que puede aportar, otros usos posibles, aspectos de seguridad, etc. En general no he profundizado en ningún tema concreto para tratar de al menos relatar todos los aspectos más relevantes.

El seguimiento de la planificación ha sido especialmente problemático hasta el punto de no ser capaz de realizar las entregas intermedias. Obligaciones laborales y personales han impedido realizar un adecuado plan de entregas, lo que ha dado lugar a tener que realizar una entrega única final.

En cuanto a las líneas de trabajo futuro se pueden citar varias:

- Ampliación del detalle de los diversos capítulos.
- Incorporación de información relevante sobre aspectos financieros.
- Análisis del negocio de la minería.
- Estudio de implementaciones de cliente y/o monederos electrónicos.

12. Fuentes de información

12.1. Bibliografía

Satoshi Nakamoto (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
https://bitcoin.org/bitcoin.pdf

Wei Dai (1997), *B-money.*
http://www.weidai.com/bmoney.txt

Adam Back (2002). *Hashcash - A Denial of Service Counter-Measure*
http://www.hashcash.org/papers/hashcash.pdf

Santiago Márquez Solís (2016). *Bitcoin Guía completa a la moneda del futuro.*

Andreas M. Antonopolous (2017). *Mastering Bitcoin.*

Diversos autores. *Wikipedia Bitcoin.*
https://en.wikipedia.org/wiki/Bitcoin

Diversos autores. *Bitcoin core.*
https://github.com/bitcoin/bitcoin

Diversos autores. *Bitcoin developer documentation.*
https://bitcoin.org/en/developer-documentation

Diversos autores. *Bitcoin.org*
https://bitcoin.org/es/

Diversos autores. *Wikipedia Contrato inteligente.*
https://es.wikipedia.org/wiki/Contrato_inteligente

Diversos autores. *Bit2me - Smart Contracts.*

https://blog.bit2me.com/es/que-son-los-smart-contracts/

Diversos autores. *Integrate device data with smart contracts in IBM Blockchain.*

https://www.ibm.com/developerworks/cloud/library/cl-blockchain-for-cognitive-iot-apps-trs/index.html

Diversos autores. *Wikipedia Computación cuántica.*

https://es.wikipedia.org/wiki/Computación_cuántica

Diversos autores. *Mi Ethereum.*

https://miethereum.com/

Diversos autores. *BitcoinCash.*

https://www.bitcoincash.org

Alexde Vries (2018). *Bitcoin's Growing Energy Problem*

https://www.sciencedirect.com/science/article/pii/S2542435118301776

Antonio Sánchez. *CARDANO: La revolución tecnológica que sustituirá a Ethereum*

https://medium.com/agorachain-mag/cardano-la-revolución-tecnológica-que-sustituirá-a-ethereum-7558f8b42cb7

Arturo Muñoz. *Criptomonedas Esenciales: Cardano, tecnología revolucionaria*

https://criptonetwork.com/analisis-criptomonedas/criptomonedas-esenciales-cardano-tecnologia-revolucionaria/