Universitat Oberta de Catalunya

uoc.edu

Trabajo Fin de Master

Estudio de tecnologías Bitcoin y Blockchain

Ricardo Cámara Albuixech
Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones.
TFM-Ad hoc

Consultora: Angela María García Valdés.
Nombre Profesor responsable: Victor García Font.

Junio de 2018

FICHA DEL TRABAJO FINAL

Título del trabajo:	Estudio de tecnologías Bitcoin y Blockchain.
Nombre del autor:	*Ricardo Cámara Albuixech*
Nombre del consultor/a:	*Angela María García Valdés*
Nombre del PRA:	*Victor García Font*
Fecha de entrega (mm/aaaa):	06/2018
Titulación::	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones
Área del Trabajo Final:	*TFM-Ad hoc*
Idioma del trabajo:	*Castellano*
Palabras clave	*Criptomoneda, Minería, Consenso.*

Resumen:

El objetivo de este TFM es, primeramente, hacer un estudio del Bitcoin, tanto desde el punto de vista de moneda como de protocolo. Abarcará la historia sobre la creación del Bitcoin en 2008, por parte de Satoshi Nakamoto. Se estudiará, entre otras características, su carácter descentralizado, sus ventajas e inconvenientes, se describirá la criptografía aplicada a la tecnología de Bitcoin, como es la criptografía asimétrica y las direcciones de Bitcoin. Por último se tratará las criptomonedas más importantes surgidas como consecuencia de la aparición del Bitcoin.

Se continuará con la Blockchain de Bitcoin, y como esta se define como un registro distribuido de transacciones mantenido por una red descentralizada de nodos. A partir de aquí se explicaran la gran cantidad de conceptos que surgen para dar soporte a esta tecnología. Entre ellos se tratarán términos como la blockchain pública y privada, los elementos que la forman, como son transacciones, bloque y cadena de bloques. También se estudiarán los mecanismos de consenso que aseguran la integridad de la blockchain, así como el trabajo de los mineros para certificar dicha integridad.

Por último, se tratará la evolución de la Blockcahin. De cómo está yendo desde una tecnología meramente centrada en las transacciones con criptomonedas, a una tecnología donde se usan otros tipos de tokens, la cual da como resultado otros productos, como son, entre otros, el más importante, los Smart Contract o contratos inteligentes.

Abstract:

The objective of this TFM is, firstly, to make a study of Bitcoin, both from the point of view of currency and protocol. It will cover the story about the creation of Bitcoin in 2008, by Satoshi Nakamoto. It will be studied, among other characteristics, its decentralized character, its advantages and disadvantages, the cryptography applied to Bitcoin technology, such as asymmetric cryptography and Bitcoin addresses will be described. Finally, the most important cryptocurrencies arising as a result of the appearance of Bitcoin will be discussed.

We will continue with the Bitcoin Blockchain, and how it is defined as a distributed registry of transactions maintained by a decentralized network of nodes. From here we will explain the large number of concepts that arise to support this technology. Among them will be terms like the public and private blockchain, the elements that form it, such as transactions, block and block chain. The consensus mechanisms that ensure the integrity of the blockchain will also be studied, as well as the work of the miners to certify this integrity.

Finally, the evolution of the Blockcahin will be discussed. How is it going from a technology focused solely on transactions with cryptocurrencies, to a technology where other types of tokens are used, which results in other products, such as, among others, the most important one, the Smart Contract or smart contracts.

Indice

Lista de figuras

Lista de tablas

1. Introducción

1.1. Contexto y justificación del Trabajo.

Este Trabajo Fin de Master se desarrolla con el interés de profundizar en dos tecnologías que están llamadas a revolucionar el concepto que se tiene tanto del dinero como de las transacciones entre partes, como son el Bitcoin y el Blockchain.

Se pretende comprender lo que realmente significa y significará tanto a nivel tecnológico como social la irrupción de estos nuevos conceptos, como será el cambio en el comercio, el cambio en la mentalidad de la población, la revolución en los puestos de trabajo que manejen esta tecnología, los campos en los que se aplicará, etc.

1.2. Objetivos del Trabajo.

Este Trabajo Fin de Master (TFM) consistirá en la realización de un estudio general sobre las tecnologías Bitcoin y Blockchain, sobre los principios de operación de la red Bitcoin y el Blockchain en Bitcoin. Así como de los beneficios de la tecnología Blockchain y de la aplicación de dicha tecnología actualmente y en el futuro.

Para la consecución de estos objetivos se desarrollarán los siguientes puntos:

- Arquitectura y organización de la red de Bitcoin .
- Conceptos de transacción, bloque y cadena de bloques.
- Qué es el consenso y cómo se alcanza en la red Bitcoin.
- Diferentes mecanismos de consenso de Blockchain, sus ventajas y desventajas.
- Diferencias entre Blockchain público y privado.
- Concepto de Smart Contracts.
- Aspectos de seguridad de Bitcoin, Blockchain y Smart Contracts.
- Importancia y el uso de la criptografía.
- Introducción a otros Blockchains (Ethereum, Ripple, Litcoin. etc).
- Aplicaciones de la tecnología Blockchain ahora y en él futuro.

1.3. Enfoque y método seguido.

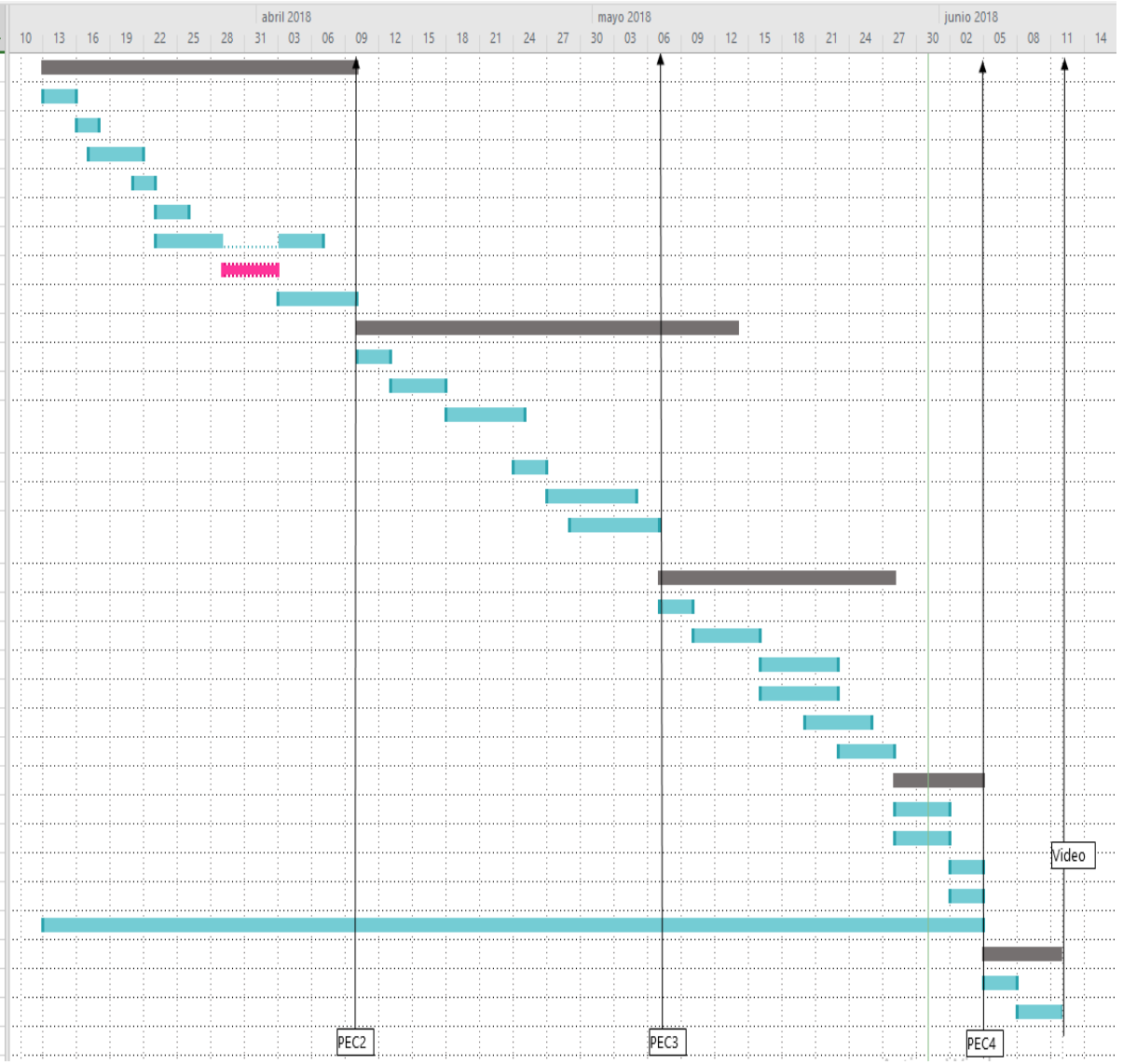
El TFM se irá desarrollando de manera secuencial, es decir, se empezará explicando lo concerniente al Bitcoin, siguiendo con lo relativo a la tecnología Blockchain y su relación con el Bitcoin y terminado con las aplicaciones que la tecnología Blockchain tiene o pudiera tener en un futuro en otros ámbitos más allá de las criptomonedas.

Todo ello se irá desarrollando con la lectura de libros, la búsqueda en Internet de documentos, publicaciones, blogs, etc, así como el visionado de videos que traten sobre Bitcoin y la tecnología Blockchain.

1.4 Planificación del Trabajo.

A continuación se presenta un diagrama de Gantt con la planificación de las tareas necesarias para la consecución del TFM, desde la fecha del comienzo de la PEC2, día 13/03/2018, hasta la presentación virtual de dicho TFM, día 11/06/2018. En este diagrama se detalla la duración, el comienzo y el fin de cada tarea.

Nombre de tarea	Duración	Comienzo	Fin
Estudio del Bitcoin.	28 días	mar 13/03/18	lun 09/04/18
Historia del Bitcoin.	3 días	mar 13/03/18	jue 15/03/18
Que es Bitcoin.	2 días	vie 16/03/18	sáb 17/03/18
Funcionamiento del Bitcoin.	5 días	sáb 17/03/18	mié 21/03/18
Quien controla Bitcoin.	2 días	mié 21/03/18	jue 22/03/18
Ventajas y desventajas del Bitcoin.	3 días	vie 23/03/18	dom 25/03/18
Criptografía y Seguridad de Bitcoin.	10 días	vie 23/03/18	vie 06/04/18
	5 días	jue 29/03/18	lun 02/04/18
Otras Criptomonedas (Altcoins).	7 días	mar 03/04/18	lun 09/04/18
Estudio de la Blockchain de Bitcoin.	34 días	mar 10/04/18	dom 13/05/18
Introducción a la Blockchain.	3 días	mar 10/04/18	jue 12/04/18
Blockchain pública y privada.	5 días	vie 13/04/18	mar 17/04/18
Concepto de transacción, bloque y cadena de bloques.	7 días	mié 18/04/18	mar 24/04/18
Minería de bloques.	3 días	mar 24/04/18	jue 26/04/18
Consenso en la blockchain de Bitcoin.	8 días	vie 27/04/18	vie 04/05/18
Diferentes mecanismos de consenso en blockchain.	8 días	dom 29/04/18	dom 06/05/18
Evolución de la Blockchain	21 días	lun 07/05/18	dom 27/05/18
Introducción.	3 días	lun 07/05/18	mié 09/05/18
Blockchain 2.0	6 días	jue 10/05/18	mar 15/05/18
Smart Contract.	7 días	mié 16/05/18	mar 22/05/18
Beneficios de los Smart Contract.	7 días	mié 16/05/18	mar 22/05/18
Usos de los Smart Contract	6 días	dom 20/05/18	vie 25/05/18
Blockchain 3.0	5 días	mié 23/05/18	dom 27/05/18
Conclusiones.	8 días	lun 28/05/18	lun 04/06/18
Descripción de las conclusiones	5 días	lun 28/05/18	vie 01/06/18
Cumplimiento de objetivos	5 días	lun 28/05/18	vie 01/06/18
Análisis de la planificación y metodologia	3 días	sáb 02/06/18	lun 04/06/18
Líneas para trabajos futuros	3 días	sáb 02/06/18	lun 04/06/18
Redacción de la memoria final.	84 días	mar 13/03/18	lun 04/06/18
Presentación Virtual.	7 días	mar 05/06/18	lun 11/06/18
Guión de la presentación.	3 días	mar 05/06/18	jue 07/06/18
Grabación del video de la presentación.	4 días	vie 08/06/18	lun 11/06/18



1.5 Descripción de los otros capítulos de la memoria.

Con el fin de conseguir explicar las tecnologías Bitcoin y Blockchain, se ha dividido el trabajo en tres capítulos principales:

- El primer capítulo, “Estudio del Bitcoin”, hablará de la historia y elementos del Bitcoin. De cómo funciona, las ventajas y desventajas del Bitcoin, la criptografía y seguridad, así como ejemplos y características de otras criptomonedas.

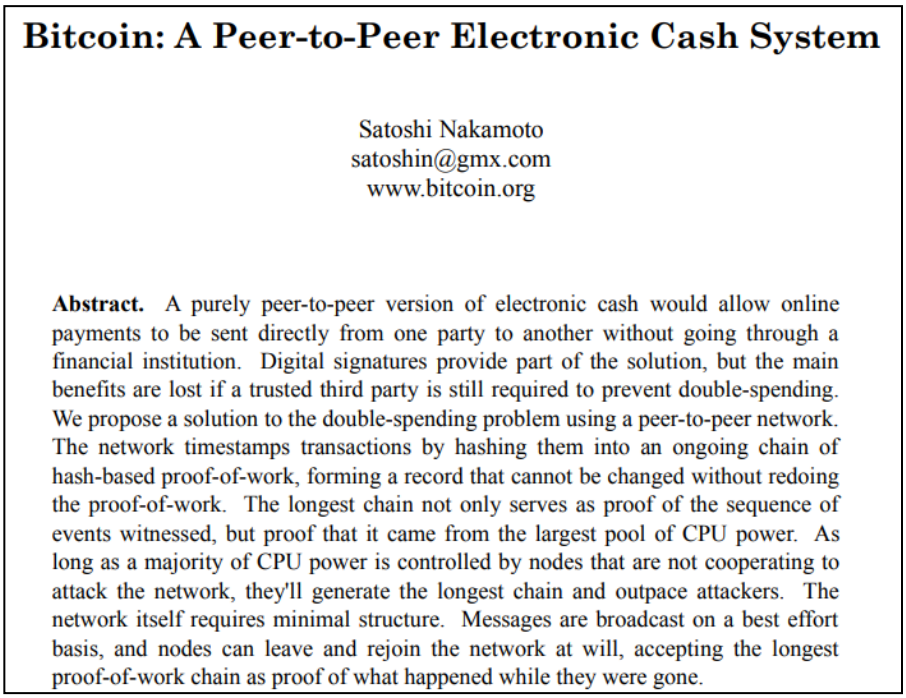
- El segundo capítulo tratará del “Estudio de la Blockchain de Bitcoin”. Comenzará con una introducción a la blockchain, seguirá hablando de la blockchain pública y privada, después el concepto de transacción, bloque y cadena de bloques, a continuación se tratará de la minería de bloques, consenso en la blockchain de Bitcoin y otros tipos de consensos.

- El tercer capítulo, “Evolución de la Blockchain”, desarrollará el presente y futuro de la tecnología del blockchain en campos distintos al de las criptomonedas. Se expondrá ejemplos de uso.

2. Estudio del Bitcoin

2.1. Historia del Bitcoin.

Bitcoin aparece en noviembre de 2008 con la publicación, en el dominio bitcoin.org, del *paper* titulado "Bitcoin: A Peer-to-Peer Electronic Cash System" escrito bajo el apodo de Satoshi Nakamoto. Dicha publicación describe los fundamentos de la primera criptomoneda y la red que la sustenta (Figura 2.1).



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Figura 2.1. Resumen de la publicación Bitcoin en bitcoin.org

Nakamoto combinó varias invenciones previas tales como b-money y HashCash para crear un sistema de efectivo electrónico completamente descentralizado, el cual no depende de una autoridad central para su emisión, liquidación o validación de transacciones. La innovación clave fue el uso de un sistema de computación distribuida como protocolo de seguridad, llamado algoritmo de prueba de trabajo o proof-of-work (PoW), el cual permite a la red descentralizada llegar a un consenso acerca del estado de las transacciones.

La invención de Satoshi Nakamoto es también una solución a un problema previamente sin solución en computación distribuida, conocido como

el “Problema de los Generales Bizantinos”. Brevemente, el problema consiste en tratar de llegar a un consenso al respecto de un plan de acción intercambiando información a través de una red poco fiable y potencialmente comprometida. La solución de Satoshi Nakamoto, representa un avance en computación distribuida y posee amplias aplicaciones más allá de las criptomonedas. Puede ser utilizada para alcanzar consenso en redes distribuidas, para probar la legitimidad de elecciones, loterías, registros de activos, autorizaciones bajo notarios digitales, etc.

La red Bitcoin fue iniciada en febrero de 2009, basada en una implementación de referencia publicada por Nakamoto en la página “P2P Foundation” (Figura 2.2), y que ha sido modificada por muchos otros programadores desde entonces.

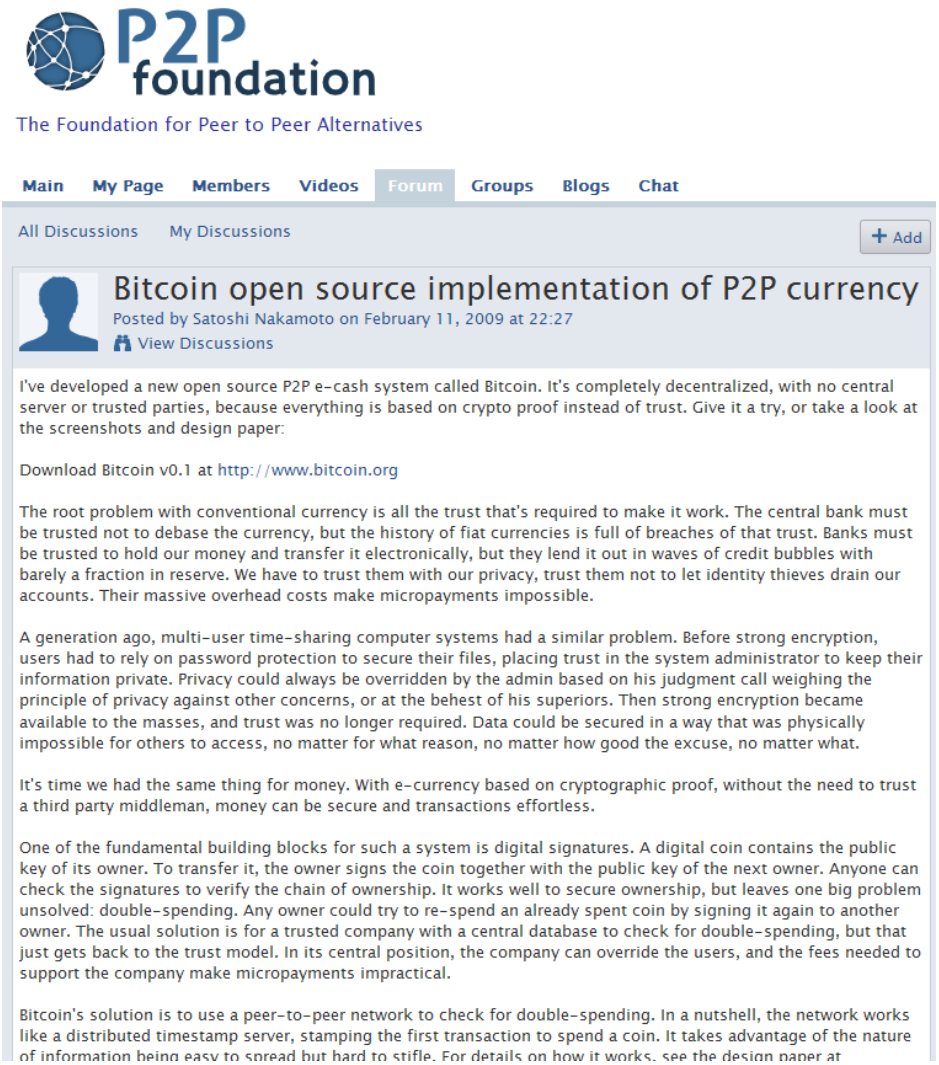


Figura 2.2. Publicación de Bitcoin en P2P Foundation

Satoshi Nakamoto se retiró del proyecto Bitcoin en abril de 2011, legando la responsabilidad de desarrollar el código y la red a un grupo creciente de voluntarios. La identidad de la persona o personas detrás de Bitcoin es aún desconocida. Sin embargo, ni Satoshi Nakamoto ni nadie más posee control sobre el sistema Bitcoin, el cual opera basado en principios matemáticos completamente transparentes.

2.2. Que es el Bitcoin.

Bitcoin es un conjunto de conceptos y tecnologías que conforman un ecosistema de dinero digital. Bitcoin es a la vez un protocolo, una red de pagos y una moneda. En este sentido Bitcoin, con B mayúscula, se utiliza para describir el concepto de Bitcoin, o la totalidad de la red, mientras que bitcoin, con b minúscula, se utiliza para describir la criptomoneda, la cual se abrevia como BTC.

El almacenamiento y transmisión de valor entre los participantes de la red Bitcoin se consigue mediante la utilización de las unidades monetarias, bitcoins (BTC). La moneda bitcoin es tan solo la primera aplicación de esta invención. Bitcoin es como una red para propagar valor y asegurar la propiedad de activos digitales vía computación distribuida.

Los usuarios de bitcoin se comunican entre ellos usando el protocolo Bitcoin, principalmente a través de Internet, aunque también se pueden utilizar otras redes de transporte. La pila de protocolos Bitcoin, disponible como software open source, puede ejecutarse sobre una amplia variedad de dispositivos, incluyendo laptops y smartphones, lo que hace que la tecnología sea fácilmente accesible.

Para el usuario final, bitcoin es un medio de pago más, como lo puede ser el euro y un activo en el que invertir, como lo puede ser una acción o el oro (Tabla 2.1). Los usuarios pueden transferir bitcoins a través de la red para hacer prácticamente cualquier cosa realizable con monedas convencionales, incluyendo comprar y vender bienes, enviar dinero a personas y organizaciones, o extender créditos. Los bitcoins pueden comprarse, venderse e intercambiarse por otras monedas en casas de cambio especializadas. En cierta forma bitcoin es la forma de dinero perfecta para Internet, ya que es rápido, seguro y carente de fronteras.

Características del dinero	Oro	Efectivo (Euro)	Crypto (Bitcoin)
Fungible (Intercambiable)	Alto	Alto	Alto
No Desgastable	Moderado	Bajo	Alto
Portabilidad	Moderado	Alto	Alto
Durabilidad	Alto	Moderado	Alto
Divisibilidad	Moderado	Moderado	Alto
Seguro (No puede ser falsificado)	Moderado	Moderado	Alto
Fácilmente Manejable	Bajo	Alto	Alto
Escaso (Suministro Predecible)	Moderado	Bajo	Alto
Soberano (Emitido por el Gobierno)	Bajo	Alto	Bajo
Descentralizado	Bajo	Bajo	Alto
Inteligente (Programable)	Bajo	Bajo	Alto

Tabla 2.1 Nivel de cumplimiento entre distintas formas de pago respecto de las características del dinero.

Un único BTC, dado su naturaleza digital puede ser dividido hasta alcanzar 8 cifras decimales. Esto significa que la mínima cantidad de bitcoins que se puede poseer es 0.00000001 BTC, que como homenaje al creador se conoce como 1 satoshi. De esta forma las demás divisiones posibles también tienen su propia denominación (Tabla 2.2).

1 BTC	A bitcoin
0.01 BTC	A bitcent
0.001 BTC	An mbit
0.000001 BTC	A ubit
0.00000001 BTC	A satoshi

Tabla 2.2 Divisiones de un BTC.

A diferencia de las monedas tradicionales, los bitcoins son completamente virtuales. No existen monedas físicas y en sentido estricto, ni siquiera existen monedas digitales. Las monedas están implícitas en transacciones que mueven valor de un remitente a un destinatario. Los usuarios de bitcoin poseen claves que les permiten demostrar la propiedad de las transacciones en la red Bitcoin, otorgando acceso a gastar su valor transfiriéndolo a un nuevo destinatario. Esas claves están normalmente almacenadas en una cartera digital o monedero (en inglés, "wallet") propiedad de cada usuario. La posesión de la clave que libera una transacción es el único

prerrequisito para gastar bitcoins, poniendo completo control en las manos de cada usuario.

2.3. Funcionamiento del Bitcoin.

Para empezar con la idea básica de cómo funciona el sistema, se presentará una breve descripción de los elementos, algunos ya citados anteriormente, del Bitcoin (en capítulos posteriores se profundizará más en dichos elementos):

- **Transacciones**: proceso por el cual se transfieren las criptodivisas. Especifica cuántas BTC fueron tomadas de cada dirección emisora y cuántas fueron acreditadas a cada dirección receptora.

- **Transacción Coinbase**: Un tipo especial de transacción sin inputs, creada por los mineros, es la primera transacción del bloque y solo existe una de su tipo en cada bloque. Su función es otorgar la recompensa al minero por el trabajo realizado (comisiones por transacción o el pago por bloque).

- **Confirmación**: acción de procesar y verificar una transacción, realizada por los nodos de la red. Las transacciones son confirmadas cuando son incluidas en un bloque.

- **Bloque/Block**: registro permanente que contiene las confirmaciones de transacciones pendientes, un número aleatorio (nonce) y un hash del bloque anterior. En promedio, cada 10 minutos, un nuevo bloque que incluye nuevas transacciones se anexa a la cadena de bloques a través de la minería. El primer bloque creado se llama “Génesis”.

- **Banco de memoria/Memory Pool (mempool)**: estructura local en cada nodo con todas las transacciones recibidas y aún no confirmadas. Si una transacción que aparece en el memory pool de un nodo específico, es confirmada en otro lugar, la transacción se elimina de ese memory pool.

- **Cadena de bloques/Blockchain**: registro cronológico de todas las transacciones realizadas y confirmadas en la red Bitcoin. Esta base de datos es pública, compartida y creada de forma colectiva por todos los nodos de la

red, es el medio por el cual se verifican las transacciones y se evita el doble gasto de las BTC.

● **Minería de bitcoins**: es el proceso de generación de nuevas divisas y de verificación de las transacciones en la red de Bitcoin. La verificación corresponde a un sistema de consenso distribuido mediante el cual los mineros otorgan procesamiento de CPU o GPU de sus equipos computacionales para resolver problemas matemáticos del esquema de proof-of-work utilizados para garantizar la seguridad y funcionalidad de la red.

● **Direcciones/Address**: concepto similar a una dirección física o correo electrónico, cada usuario puede poseer una cantidad ilimitada de direcciones, caracterizadas por ser el hash de una clave pública ECDSA (en el punto 2.6.1 se explicara este concepto). Estas se utilizan para las transferencias de BTC, pues es la única información que se debe brindar al receptor de transacción.

● **Monederos/billetera (wallet)**: archivo contenedor de la clave privada de una dirección en particular, la cual se utiliza para firmar la transacción y garantizar tanto el origen de esta como su integridad. Cada monedero puede mostrar la cantidad de bitcoins que contiene (balance de BTC) y permite pagar una cantidad específica a una o varias direcciones. Los monederos pueden ser en línea (gestionada por una empresa como un servicio a través de un navegador) o como un software cliente instalado en un dispositivo (smartphone, desktop,etc.).

● **Velocidad de hasheo (hashrate)**: unidad de medida de la potencia de procesamiento de la red Bitcoin.

● **Script**: sistema de scripting para las transacciones, que es esencialmente una lista de instrucciones grabadas en cada transacción donde el emisor puede crear requisitos muy complejos que el receptor debe cumplir con el fin de reclamar el valor del input. Ejemplo: scriptPubKey o Public Key Script, scriptSig o Signature Script.

● **Nodo completo (Full node)**: es un programa que ayuda a la red de dos maneras: al realizar la validación completa de transacciones/bloques y al permitir a clientes ligeros transmitir transacciones a la red. Es un trabajo voluntario que mantiene robusta la red y que solo requiere que el usuario interesado instale el programa Bitcoin Core y lo mantenga corriendo con el puerto 8333 abierto.

● **Prueba de trabajo (Proof-of-work/PoW)**: básicamente es un proceso aleatorio que requiere en promedio de mucha prueba y error, es difícil de ejecutar (en términos de costo/procesamiento/energía) pero genera una prueba válida de trabajo fácil de confirmar.

También es importante comentar el tipo de participantes que forman parte del sistema. Podemos encontrar tres tipos de participantes:

● **Usuarios normales**: son simples usuarios, compran y pagan bienes y servicios a través de transacciones.

● **Usuarios mineros**: el proceso que realizan los mineros es el que da origen a los nuevos bitcoins, son los encargados de validar las transacciones y el motor básico del sistema. Cualquier participante de la red bitcoin (cualquier persona utilizando un dispositivo con la pila de protocolos bitcoin completa) puede operar como minero, utilizando el poder de computo de su pc para verificar y registrar transacciones. Estos pueden trabajar de forma aislada o pueden establecer uniones entre ellos para así conseguir una potencia de cómputo mucho mayor. El cálculo que se ven sometido a realizar es de una complejidad muy alta y a la vez de un coste elevado de ahí que reciban una compensación en forma de bitcoins por cada resolución.

● **Desarrolladores**: este sistema se basa en un software que necesita un mantenimiento activo. Ellos son los encargados de hacerlo con un nivel de influencia muy limitado.

Una vez los bitcoins son generados, un usuario de los denominados normales puede adquirirlos a través de las numerosas plataformas que se han creado para ofrecer este servicio. Estas plataformas actúan como casas de cambio para que el usuario intercambie dinero tradicional por bitcoins. Antes de nada el usuario debe haberse creado un monedero o wallet.

Para explicar cómo funciona el sistema cuando un usuario realiza una transacción de bitcoins a otro, se utilizará la Figura 2.3. Aquí pueden verse con más claridad los participantes y los roles que estos desempeñan.

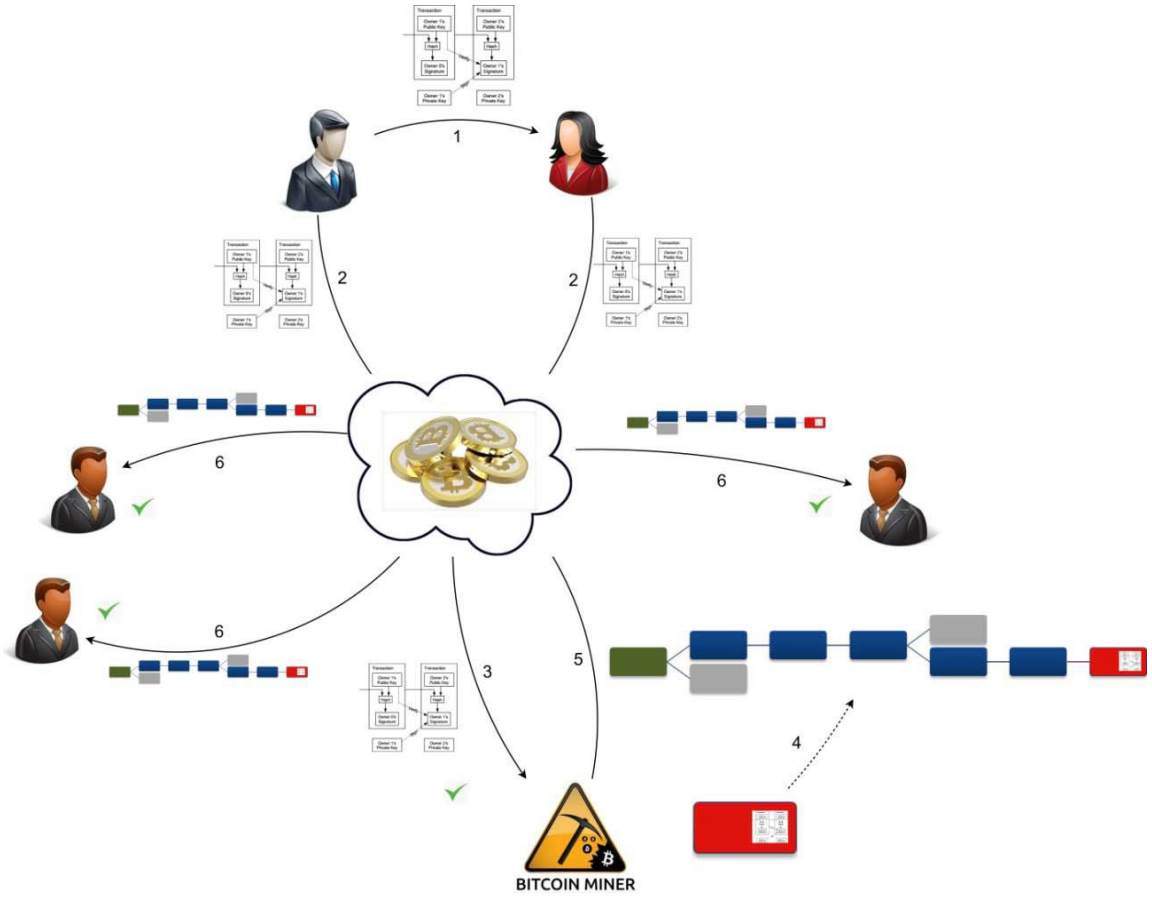


Figura 2.3. Funcionamiento de las transacciones en Bitcoin

Como bien se puede observar en esta imagen, existen varios agentes que participan en la acción.

En primer lugar todo comienza cuando el Usuario A realiza una transacción de bitcoins a la Usuaria B (1). Una vez realizada, tanto el Usuario A como la Usuaria B envían la información de la transacción a la red P2P (2).

Una vez la información ha sido enviada a la red es recibida por un minero que la verifica (3). Este minero crea un bloque de transacciones con la transacción que validó en el momento anterior y nuevas transacciones que recibe y trabaja para confirmarlas (4).

Una vez este minero haya conseguido confirmar el bloque de transacciones lo envía (5) a la red P2P, donde es recibido por todos los usuarios y mineros que forman parte del sistema.

El resto de mineros de la red reciben el bloque mandado por el minero que ha confirmado en primer lugar, analizándolo y validándolo, tras lo cual lo

incluyen en la cadena de bloques (6) y la transacción queda definitivamente confirmada.

Este procedimiento evita que se realice dos veces la misma transacción, puesto que en el momento en el que el bloque donde se encuentra la transacción duplicada llegue a los mineros estos la rechazarán por estar ya registrada en su cadena.

Todas estas transacciones que son confirmadas se almacenan en la blockchain. Aquí se registran todas las transacciones confirmadas, realizadas desde el 03 de enero de 2009 hasta hoy. Se almacenan de forma cronológica y siempre está actualizado. Este registro es público, puesto que si alguien quiere obtener una copia no tendrá ningún problema en hacerlo, de ahí nace su característica de transparencia.

Las transacciones almacenadas en la cadena de bloques lo hacen de manera anónima. Sólo aparecerá en el registro la dirección de origen, la dirección de destino y la cantidad transferida.

La transacción de bitcoins es casi instantánea. Sin embargo hay un retraso de 10 minutos de media antes de que la red empiece a confirmar esa transacción al incluirla en un bloque y antes de que se puedan gastar los bitcoins recibidos. Una confirmación significa que hay un consenso en la red en que los bitcoins recibidos no han sido enviados a alguien más y son ahora de tu propiedad. Una vez que tu transacción ha sido incluida en un bloque, esta irá siendo "enterrada" con más confirmaciones por los siguientes bloques que van añadiéndose a la cadena, lo que hará consolidarse este consenso y disminuir el riesgo de una revocar la transacción. Cada usuario es libre de determinar en qué punto se puede considerar una transacción como confirmada, pero normalmente 6 confirmaciones es considerado tan seguro como esperar 6 meses tras un pago con tarjeta de crédito.

El protocolo bitcoin incluye algoritmos que regulan la función de minería en toda la red. La dificultad de la tarea de procesamiento que los mineros deben ejecutar—para registrar con éxito un bloque de transacciones para la red bitcoin—se ajusta dinámicamente de forma que, en promedio, alguien podrá conseguirlo cada 10 minutos (Figura 2.4) sin importar cuantos mineros haya trabajado en la tarea en cada momento.

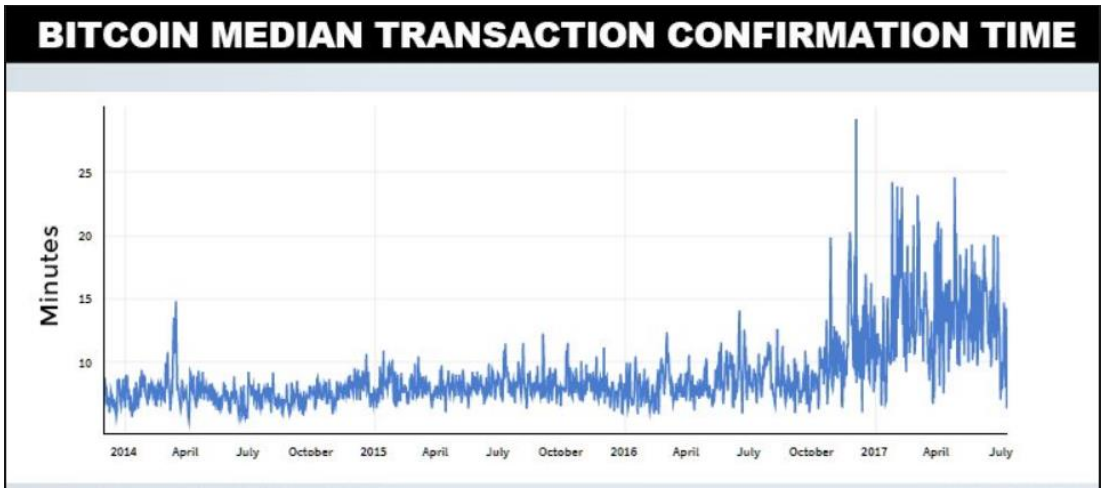


Figura 2.4. Tiempo para la confirmación de una transacción.

Cada cuatro años, el protocolo también reduce a la mitad la tasa a la que se crean nuevos bitcoins, asegurando que se seguirán creando bitcoins hasta un valor límite de 21 millones de monedas. En la actualidad se han minado ya unos 16 millones de Bitcoin, lo que es un 75% del valor final. Se estima que para 2032 se habrán minado un 99% de los Bitcoin (Figura 2.5), pero como el ritmo de producción será más bajo no será hasta aproximadamente 2140 cuando se mine el último de los 21 millones de Bitcoin.

Debido a la decreciente tasa de emisión, bitcoin es deflacionario en el largo plazo. Además bitcoin no puede ser inflado a través de la "impresión" de nuevo dinero por encima de la tasa de emisión esperada.

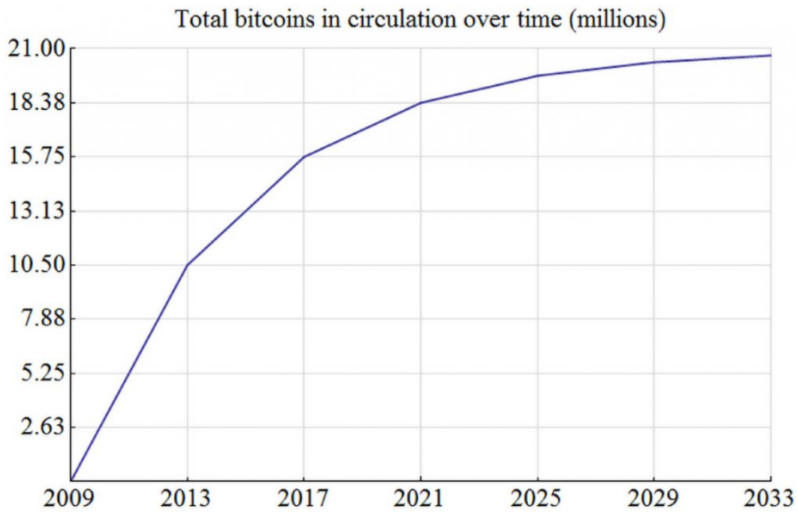


Figura 2.5. Evolución del número de bitcoins.

2.4. Quien controla Bitcoin.

El control del bitcoin recae en los propios usuarios. Son éstos quienes validan cualquier operación a través de intercambios peer-to-peer P2P, sin intervención estatal o de cualquier institución. De hecho, la propia estructura hace imposible manipular su valor. Para realizar cualquier cambio es necesario que toda la comunidad de usuarios lo apruebe.

El Bitcon es la primera moneda electrónica que logró implantarse con cierta solvencia, pero no la primera en aparecer. Lo que diferencia a bitcoin de otros intentos es su tecnología de cadena de bloques.

Aunque Bitcoin tenga desarrolladores, nadie controla la moneda virtual. Los programadores pueden mejorar el software de Bitcoin, pero no pueden imponer un cambio en el protocolo. Este debe seguir unas mismas reglas para todos y éstas se crean en consenso entre todos los usuarios con sus decisiones sobre qué plataformas eligen para operar.

El control de las transacciones se realiza a través de los propios usuarios, que son los que validan los bloques de la cadena y la seguridad de la transacción. Además, esta cadena no se puede alterar porque está presente en miles de ordenadores de todo el mundo.

2.5. Ventajas y desventajas del Bitcoin.

2.5.1. Ventajas.

A continuación se enumera las ventajas tanto de la tecnología Bitcoin como de la moneda bitcoin (BTC):

- **Libertad de pagos:** Con Bitcoin, podrá enviar y recibir cualquier cantidad de dinero instantáneamente desde y hacia cualquier lugar del mundo, en cualquier momento. Sin bancos con horarios, sin fronteras, sin límites impuestos. Los usuarios de Bitcoin siempre tienen un completo control sobre su dinero.

- **Tasas muy bajas:** Los pagos con bitcoin son actualmente procesados con tasas bajas o sin tasa alguna. Los usuarios pueden incluir una tasa en sus transacciones para recibir prioridad en el procesamiento de estas, lo que resulta en una confirmación más rápida de las transacciones por parte de la red. Además, los procesadores mercantiles están para asesorar en los

procesos de transacción a los comerciantes, convirtiendo bitcoins a la moneda fiduciaria y depositando fondos directamente en la cuenta bancaria del comerciante diariamente. Como estos servicios están basados en Bitcoin, son ofrecidos con cargos mucho más bajos que los que ofrecen PayPal o las redes de tarjetas de crédito.

● **Menores riesgos para los comerciantes:** Las transacciones con bitcoin son seguras, irreversibles, y no contienen datos personales y privados de los clientes. Esto protege a comerciantes contra pérdidas ocasionadas por el fraude o devolución fraudulenta, y no es necesario el cumplimiento de las normas PCI. Asimismo, los comerciantes pueden operar en nuevos mercados en los que las tarjetas de crédito no están disponibles o los niveles de fraude sean demasiado elevados. Esto conlleva a mejores comisiones, mercados más extensos y menos costes administrativos.

● **Seguridad y control:** Los usuarios de Bitcoin tienen completo control sobre sus transacciones; es imposible que los comerciantes fuercen cargos no deseados o detectados, como puede suceder con otros métodos de pago. Los pagos de bitcoin pueden realizarse sin que estén asociados a información de carácter personal. Esto ofrece un alto nivel de protección contra el robo de identidad. Los usuarios de Bitcoin también pueden proteger su dinero con copias de seguridad y encriptación.

● **Neutral y transparente:** Toda la información sobre el suministro de bitcoin está disponible en la cadena de bloques para cualquiera que quiera verificarlo y usarlo. Ningún individuo u organización puede controlar o manipular el protocolo Bitcoin porque es criptográficamente seguro. Se puede confiar en Bitcoin por ser completamente neutral, transparente y fiable.

2.5.2. Desventajas.

A continuación se enumera las desventajas tanto de la tecnología Bitcoin como de la moneda bitcoin:

● **Grado de aceptación:** Mucha gente no conoce aún Bitcoin. Cada día, más negocios aceptan bitcoin para aprovechar sus ventajas, pero la lista aún es pequeña y necesita crecer para que puedan beneficiarse de su efecto de red.

● **Volatilidad:** El valor total de bitcoins en circulación y el número de negocios usando bitcoin son muy pequeños comparado con lo que puede llegar a ser. Por lo tanto, eventos relativamente pequeños, intercambios o actividades empresariales afectan significativamente en el precio (Figura 2.6). En teoría, esta volatilidad decrecerá conforme el mercado y la tecnología Bitcoin, madure.

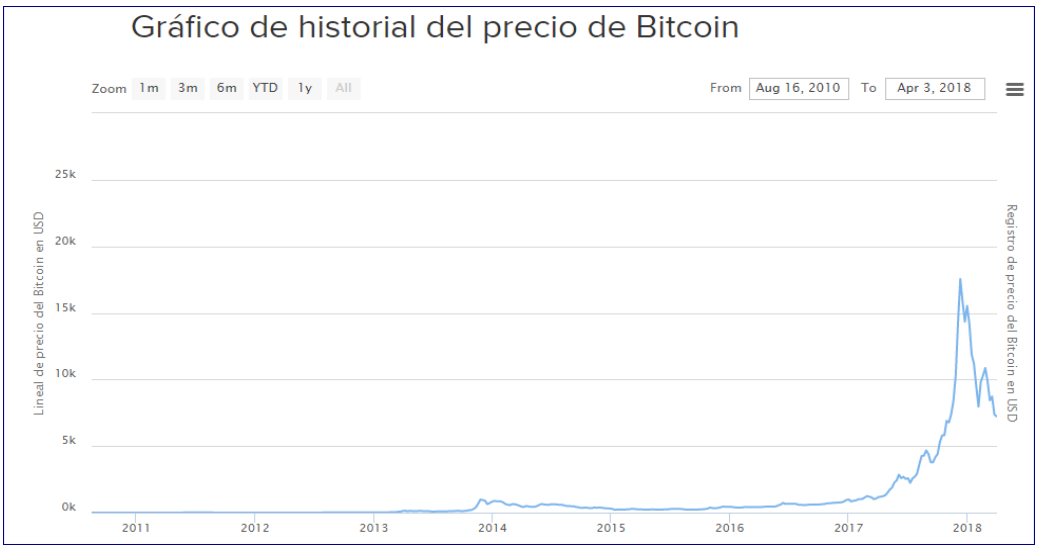


Figura 2.6. Evolución del precio del bitcoin.

● **Desarrollo en curso:** El software de Bitcoin aún está en fase beta con muchas características incompletas en desarrollo. Se están desarrollando nuevas herramientas, características y servicios para hacer Bitcoin más seguro y accesible a las masas. Muchos aún no están listos para el público. La mayoría de negocios con Bitcoin son nuevos y no ofrecen seguridad. En general, Bitcoin aún está en proceso de maduración.

2.6. Criptografía y Seguridad del Bitcoin.

2.6.1. Generación de direcciones Bitcoin.

El protocolo que da soporte a Bitcoin prescinde totalmente de un registro de usuarios. En su lugar se utiliza un sistema de direcciones basados en criptografía de clave pública o criptografía asimétrica

La criptografía asimétrica se basa en la generación de 2 claves para un usuario, una llamada clave pública y que el usuario puede distribuir libremente, y una clave privada que solo debe conocer el usuario. Para enviar un mensaje seguro al usuario cualquiera puede cifrar el mensaje con la clave pública, de forma que sólo el poseedor de la clave privada (el usuario) podrá descifrarlo y leerlo.

Los algoritmos de criptografía de clave pública se basan en problemas matemáticos de difícil solución para generar las 2 claves relacionadas sin que sea posible inferir una clave a partir de la otra.

Bitcoin, para la generación de claves de usuario, utiliza el algoritmo ECDSA (Elliptic Curve Digital Signature Algorithm), basado en criptografía de curva elíptica. En concreto utiliza la curva secp256k1 (Figura 2.7) con la forma y2= x3+0x+7, definida sobre el campo finito Fp donde p=2256-232-29-28-27-26-24-1, donde con el punto generador P de orden n es posible derivar la clave privada, la cuales es un número aleatorio s<n y la clave pública es un punto de la curva que cumple Q=s•P. Esta curva elíptica posee varias propiedades beneficiosas, permitiendo un 30% de optimización computacional en la implementación, ideal para dispositivos que disponen de pocos recursos y reduciendo la probabilidad de que el creador de la curva haya insertado algún tipo de puerta trasera en la misma. Las claves privadas son de longitud 256 bits (32 bytes) y el rango de claves válidas va de 0x1 a 0xFFFF FFFF FFFF FFFF FFFF FFFF FFFE BAAE DCE6 AF48 A03B BFD2 5E8C D036 4141.

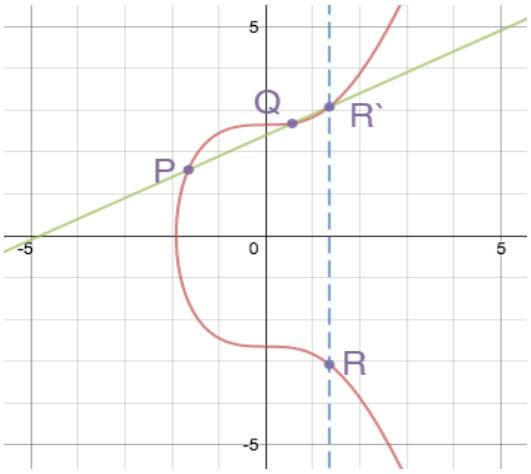


Figura 2.7. Curva secp256k1.

Básicamente cada usuario que quiera usar bitcoin, mediante este algoritmo criptográfico se genera un par de claves asimétricas. El usuario que

quiere recibir un pago puede enviar al pagador su clave pública, y éste vincula el pago a esta clave pública, de forma que sólo el usuario que tiene la clave privada puede acceder al pago y por tanto a esos fondos.

De las claves privadas del usuario se obtienen las direcciones Bitcoin aplicando un algoritmo de hash de 160 bits, sin embargo la obtención de las claves privadas a través de la direcciones es computacionalmente inviable. Cada usuario es responsable de mantener seguras sus claves privadas, siendo asistido en este proceso por su monedero. Para representar las claves privadas en Bitcoin se usa el formato Base58. Este formato es capaz de representar de una forma legible para humanos datos binarios, usando los caracteres ASCII 1-9, A-Z excluyendo la I mayúscula, y a-z excluyendo la l minúscula. Estas exclusiones se justifican en la legibilidad, para evitar confusiones del usuario.

El algoritmo de conversión de la clave privada a su dirección correspondiente (Figura 2.8) es el siguiente:

- Se obtiene la clave pública correspondiente a la curva elíptica, consistiendo en 65 bytes. El primer byte es siempre 0x04, y 32 bytes correspondiendo a la coordenada X y 32 bytes a la coordenada Y de la curva.

- Se realiza un hash SHA256 de la clave pública.

- Se realiza un hash RIPEMD-160 del resultado del SHA256.

- Se realiza un doble hash SHA256 del resultado del RIPEMD160, generando el llamado “checksum” de la dirección.

- La dirección se construye con un byte de versión al inicio (0x00 en la red Bitcoin), se concatena el resultado del RIPEMD-160 y por último se concatenan los 4 primeros bytes del checksum.

- El resultado es un vector de 25 bytes al que se le aplica una codificación BASE58 para que el resultado sea legible para los usuarios.

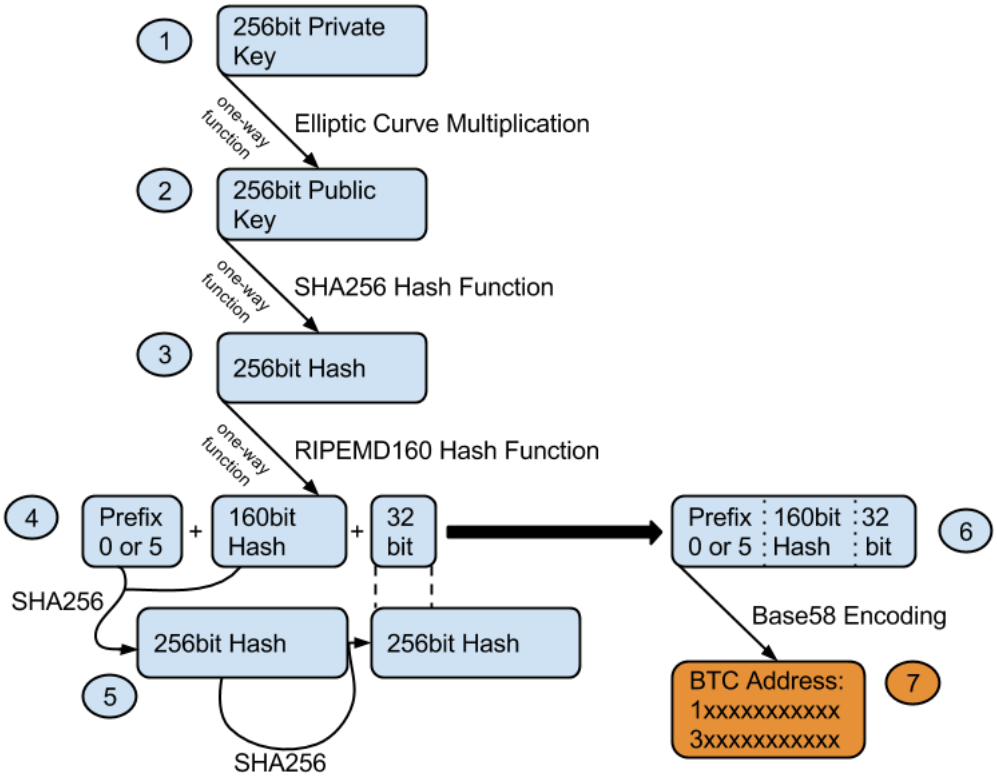


Figura 2.8. Generación de direcciones en Bitcoin.

2.6.3. Garantías de seguridad

Uno de los conceptos más importantes que establece el protocolo son las llamadas comisiones o incentivos que se otorgan a los mineros con el fin de asegurarse su honestidad, pues les resulta mejor, desde el punto de vista financiero, apoyar a la red que atacar al protocolo. Es decir, en caso de que un atacante logre mayoría en la cantidad de nodos en la red, será más beneficioso ganar las comisiones que se le darán por su trabajo que la ganancia por modificar bloques, confirmar transacciones inválidas o quebrantar el sistema. El costo computacional (gasto energético) que conlleva modificar un bloque en particular sobrepasa las ganancias que esta acción genera, pues el atacante debe alterar y rehacer el PoW de ese bloque y los demás subsiguientes a este, además de lograr alcanzar a la cadena de bloques legítima y sobrepasarla para atacar con éxito a la red.

Otro pilar del protocolo con respecto al tema de seguridad es el trabajo distribuido, colaborativo y regido por las reglas de consenso de la red. Mediante la participación sincronizada, pero no premeditada, de los nodos en la red al aceptar o no procesar una transacción según lo establecido por las reglas de consenso, se mantiene la red estable, pues se garantiza que los nodos trabajan siempre sobre las mismas premisas. Es importante resaltar que estas premisas son regularmente actualizadas y se tienen contramedidas para minimizar problemas por nodos desactualizados.

Por otro lado, se debe recordar que Bitcoin se basa en una red compuesta en su mayoría por nodos honestos. Según los fundamentos expuestos por Nakamoto en el paper original sobre Bitcoins, en el caso hipotético de que la mayoría de nodos en la red sean maliciosos y generen una cadena de bloques alternativa a la válida, el protocolo posee dos resguardos:

- El primero de ellos, el atacante solo puede revertir transacciones realizadas por él, no puede realizar cambios arbitrarios a otras transacciones ni direcciones pues existe una alta posibilidad de que algún nodo detecte el comportamiento nocivo del atacante y no acepte la transacción ni el bloque que contenga la transmisión inválida.
- El segundo de los resguardos es que mediante cálculos estadísticos se caracteriza la carrera entre una cadena deshonesta y una válida (por medio del método conocido como ‘Camino aleatorio binomial’ y el problema de la ruina del apostador o Gambler’s ruin problem) y se determina que si el intento de doble gasto no se inicia inmediatamente después de que se haga la transacción original, la posibilidad de tener éxito se hace exponencialmente pequeña.

A nivel técnico, la seguridad en comunicaciones y la red P2P son dos aspectos donde la criptodivisa se refuerza. En el primer caso los protocolos de pago usados por la red soportan los certificados X.509 y encriptación TLS para verificar la identidad de los receptores, encriptar comunicaciones entre nodos y así prevenir ataques man in the middle, etc., mientras que el segundo caso las redes P2P garantizan comunicaciones sin intermediarios de manera directa entre nodos y permite que toda la información sea transmitida a todos los nodos. La redundancia que brinda el sistema P2P es fundamental, pues al ser tolerante a pérdida de mensajes no es necesario que alcance a todos los nodos para funcionar adecuadamente, pues se actualizan con el último blockchain, al aceptar como legítimo el blockchain más largo en dificultad PoW.

A nivel de protocolo, se debe resaltar la actualización del nivel de dificultad del PoW. La actualización consiste en que cada 2016 bloques se

reevalúa el valor de dificultad del hash contra el cual se validan las confirmaciones. La red utiliza un marcador de tiempo guardado en cada block header para calcular el número de segundos entre la generación del primer y segundo de los 2016 bloques. Si toma más de 2 semanas, la dificultad se incrementa proporcionalmente (hasta 300%) y si toma menos de 2 semanas el valor se reduce proporcionalmente (hasta un 75%), ambas medidas con el fin de lograr que la generación de bloques se realice exactamente con el misma tasa.

Finalmente, mediante blockchain es posible garantizar que no haya un doble gasto de una misma moneda ni modificación de los registros previos. En el caso del doble gasto, este se previene gracias al encadenamiento entre transacciones. Por otro lado, la integridad de los bloques se garantiza gracias a la firma digital y al encadenamiento entre bloques, donde los hashes intermedios no pueden ser falsificados, pues en ese caso, la verificación de la transacción fallaría y esta sería rechazada.

2.7. Otras Criptomonedas (Altcoins).

Con la aparición del Bitcoin, son numerosos los usuarios o las comunidades que ven como un proyecto de futuro sólido e innovador, el sistema económico planteado por esta criptomoneda. Es por esto que tras la experiencia y gracias a la característica de Código abierto del Bitcoin bajo licencia MIT(Massachusetts Institute of Technology), lo que permite un estudio y análisis más profundo de su funcionamiento, los usuarios deciden llevar a cabo su propio proyecto de criptomoneda, creando otro tipo de moneda criptográfica con unos prototipos comunes que comparten con el Bitcoin, pero incluso añadiendo modificaciones, nuevos algoritmos, nuevos métodos de minería y objetivos o metas para su criptomoneda.

Es así como surgen los denominados Altcoins o monedas alternativas que son una variante del Bitcoin, con sus propios precios de mercado establecidos y su regulación por parte de la comunidad de usuarios que lo controla.

Sobre todo en los últimos años, estos Altcoins han ido cobrando fuerza e incluso algunos proyectos de criptomonedas se han convertido en competidores directos del Bitcoin.

Seguidamente se recogen algunas de las principales altcoins conocidas hoy en día que más compiten con el Bitcoin. En concreto se trata de las 4 altcoins más importantes por capitalización bursátil:

Ethereum

Ethereum es segundo por tamaño en comparación con Bitcoin. Fue lanzado en 2015 y fue desarrollado por un programador de Bitcoin que estaba desencantado con la funcionalidad de Bitcoin.

Su capitalización bursátil el 7 de abril de 2018 era de más de 36.000 millones de dólares, un poco menos de la mitad que Bitcoin y hay aproximadamente 750.000 propietarios individuales del Ether (como se conoce técnicamente la moneda). Como medio de pago, es aceptado por muy pocos puntos de venta o cualquier organización comercial. La esencia de Ethereum es que se trata de una tecnología de cadenas de bloques diseñada para realizar “contratos inteligentes” o “smart contract” (ver punto 4.3), que son protocolos informáticos destinados a facilitar, verificar o hacer cumplir la negociación o el cumplimiento de un contrato. La forma de pensar en el Ethereum es como una moneda para los contratos comerciales a través de Internet, a diferencia de Bitcoin, que pretende ser más una reserva de valor y medio de intercambio generalizado. Lo sorprendente de los “contratos inteligentes” es que se controlan a sí mismos: los contratos se anulan automáticamente cuando una parte no cumple con su obligación.

En otros aspectos, Ethereum es funcionalmente similar a Bitcoin. También es objeto de minería, pero las reglas que rigen su extracción en el futuro son menos claras que las reglas de Bitcoin. Ethereum tiene una imagen más corporativa y fue llevado al mercado por una empresa suiza. Ethereum ha tenido cierta publicidad negativa ya que su libro mayor ha sido pirateado con éxito y ha sufrido varias bifurcaciones duras o hard forks (ver punto 3.6), estando la primera destinada a recuperar los activos robados tras el ataque de los hackers. Sin embargo, algunos analistas de criptomonedas ven en Ethereum el potencial de superar a Bitcoin en capitalización bursátil en algún momento en el futuro. Aun así, en los últimos meses la capitalización de Bitcoin ha crecido proporcionalmente más rápido que la de Ethereum.

Ripple

Ripple es la tercera criptomoneda más grande del mundo. Su capitalización bursátil a 7 de abril de 2018 era de poco menos de 19000 millones de dólares.

Fue lanzado en 2012, pero había estado en

desarrollo durante 8 años. Ripple es bastante diferente de Bitcoin y Ethereum, ya que tiene una imagen y respaldo más corporativos, y en realidad es una red de transacciones descentralizada verificada por consenso en lugar de una criptomoneda. Fue desarrollado como un sistema de liquidación bruta en tiempo real, rápido y barato y puede verificar las transacciones en unos pocos segundos, mucho más rápido que cualquier otra criptomoneda. Ya es utilizado por varios bancos importantes, que lo consideran un sistema más seguro que Bitcoin y otras criptomonedas. Su divisa nativa es Ripple, pero puede admitir cualquier unidad de valor, ya sea moneda fiduciaria como el dólar estadounidense o incluso millas de vuelo y similares. Esta flexibilidad, así como su adopción por parte de los bancos, atrae a algunos inversores que sienten que la tecnología de Ripple dominará el mercado y finalmente superará a Bitcoin y Ethereum en capitalización bursátil. Sin embargo, debe tenerse en cuenta que su valor ha aumentado con mucha más lentitud en el segundo y tercer trimestres de 2017 que el valor de otras criptomonedas importantes

Bitcoin Cash

Bitcoin Cash o Bitcoin en efectivo, es la cuarta moneda más grande. Es una rama de Bitcoin, creada el 1 de agosto de 2017 a raíz de una bifurcación o hard fork (ver punto 3.5) en la cadena de bloques de Bitcoin. Esta bifurcación fue el resultado de las diferencias surgidas entre quienes priorizaban a Bitcoin como una reserva de valor (es decir, una inversión) sobre un medio de cambio (es decir, efectivo para hacer transacciones). Algunos mineros de Bitcoin querían que se eliminaran los límites, lo que aumentaría la velocidad en los tiempos de transacción. El resultado fue que Bitcoin se dividió para formar una nueva criptomoneda con un tiempo de transacción más rápido, llamado “Bitcoin Cash”. Se extrae y funciona de la misma forma que Bitcoin. Su capitalización bursátil a 7 de abril de 2018 era de más de 10000 millones de dólares, aproximadamente una octava parte del Bitcoin tradicional. Bitcoin Cash es generalmente más útil para las personas que necesitan derivar sus flujos de ingresos de la criptomoneda, o hacer muchas transacciones comerciales rápidas. Puede verse como un vehículo de inversión, ya que tiene un nicho de mercado y, desde la bifurcación, no hay duda de que su precio ha aumentado más rápido que el de Bitcoin.

Litecoin

Litecoin es la quinta criptomoneda más grande. Su capitalización bursátil a 7 de abril de 2018 era de más de 6500 millones de dólares. Fue lanzado en 2011 y fue una bifurcación de Bitcoin, es decir, una rama de Bitcoin. Su funcionamiento es casi idéntico al de Bitcoin en todos los sentidos, excepto que siempre ha tenido una velocidad de procesamiento mucho más rápida y actualmente puede procesar transacciones aproximadamente cuatro veces más rápido que Bitcoin.

Los principales elementos que diferencian a las cinco criptomonedas son su funcionalidad, capitalización bursátil, imagen, popularidad, seguridad y velocidades de procesamiento, como se detalla en la siguiente tabla (datos marzo de 2017):

	Bitcoin	**Ethereum**	**Bitcoin Cash**	**Ripple**	**Litecoin**
Lanzamiento	2009	2015	2017	2012	2012
Capitalización bursátil (USD)	77.000 millones	36.000 millones	10.000 millones	9000 millones	3000 millones
¿Moneda o Red?	**Moneda**	**Moneda**	**Moneda**	**Red**	**Moneda**
Seguridad del Registro	Buena	Cuestionable	Buena	Excelente	Buena
¿Famoso?	Mucho	Algo	Algo	Poco	Poco
Velocidad de Transacción	Lenta	Lenta	Rápida	Muy Rápida	Rápida
¿Respaldo Corporativo?	No	JPMorgan Chase, Microsoft, CME Group, BNY Mellon	No	Google Ventures, Standard Chartered, Accenture, Santander, InnoVentures	No
Imagen	Alternativa	Corporativa	Alternativa	Muy Corporativa	Alternativa
¿Enlace con Bitcoin?	N/A	No	Sí - *hard fork*	No	Sí - *fork*

Tabla 2.3 Elementos diferenciales de las altcoins.

No obstante, a parte de las criptomonedas descritas, existe una gran cantidad de altcoins en el mercado, las cuales han ido apareciendo a lo largo de los años. Así como muchas han aparecido, muchas otras han desaparecido, habiéndose creado miles de criptomonedas a lo largo de estos años. No obstante, en la actualidad se tiene conocimiento de unas 1.300 monedas, de las cuales sólo unas 100-200 gozan de popularidad en los principales exchangers, ya que éstas acaparan un 90% del mercado de criptomonedas.

3. Estudio de la Blockchain en Bitcoin

3.1. Introducción a la Blockchain.

Una blockchain no es otra cosa que una base de datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente. Expresado de forma más breve, es una base de datos descentralizada que no puede ser alterada. Otro elemento muy importante a tener en cuenta en ella es que, por definición, se trata de un sistema que permite que partes que no confían plenamente unas en otras puedan mantener un consenso sobre la existencia, el estado y la evolución de una serie de factores compartidos. El consenso es precisamente la clave de un sistema blockchain porque es el fundamento que permite que todos los participantes en el mismo puedan confiar en la información que se encuentra grabada en él. Se trata de un aspecto con un potencial increíble para transformar una infinidad de sectores clave de la industria y no menos de la sociedad en la que vivimos, de tal modo que podría llegar a cambiar incluso nuestra forma de entender el mundo.

La blockchain puede proporcionar robustez, seguridad, transparencia y escalabilidad a grandes sistemas de datos, lo que permite hacer frente a un amplio abanico de amenazas. Esto incluiría desde fugas de información a manipulación maliciosa del contenido. Mediante la blockchain, estas amenazas pueden combatirse trazando individualmente todas las acciones realizadas sobre los datos, resultando en una auditoría constante.

Desde un punto de vista técnico, ese sistema basado en la confianza y el consenso se construye a partir de una red global de ordenadores (nodos) que gestionan una gigantesca base de datos. Ésta puede estar abierta a la participación de cualquiera que lo desee (se habla entonces de una «blockchain pública») o bien limitada a sólo algunos participantes (caso de la «blockchain privada»), aunque siempre, en ambos casos, sin la necesidad de una entidad central que supervise o valide los procesos que se lleven a cabo. En el siguiente punto se analizará los diferentes tipos de Blockchain.

3.2. Blockchain pública y privada.

Aunque generalmente se habla de blockchain, lo cierto es que este concepto como tal no existe. O al menos no a secas, sino acompañado siempre de un adjetivo, de modo que se puede diferenciar entre blockchains públicas, blockchains privadas o, incluso, blockchains híbridas. No obstante, en general se puede hablar de una tecnología que ha llegado para quedarse y, más aún, para definir lo que será el mundo del futuro.

3.2.1. Características de la blockchain publica.

Las blockchains públicas fueron diseñadas para ser:

- **Públicas:** cualquier persona sin ser usuario puede acceder y consultar las transacciones realizadas.

- **Abiertas:** cualquier persona puede convertirse en usuario y participar del protocolo común si posee unos mínimos conocimientos técnicos.

- **Descentralizadas:** lo son en cuanto que no existe un usuario que tenga más poder que otro en la red y todos los nodos son iguales entre sí.

- **Pseudoanónimas:** los propietarios de transacciones no son identificables personalmente, pero sus direcciones sí son rastreables debido a su carácter público. Por eso, la mayoría de blockchains públicas no pueden ser anónimas, excepto aquellas expresamente diseñadas para ello.

Por definición, una blockchain pública es una red descentralizada de ordenadores que utilizan un protocolo común asumido por todos los usuarios y que permite a éstos registrar transacciones en el libro mayor (ledger, en inglés) de la base de datos. Esas anotaciones son inalterables, si bien los participantes en una blockchain de estas características pueden verificar de forma independiente y por consenso los cambios que se realizan en los registros.

Las unidades de cuenta que se utilizan en las blockchains públicas muchas veces se denominan tokens. Un token no es más que una serie de dígitos que representan un registro dentro de la cadena de bloques. Por ejemplo, una cadena alfanumérica como 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy es un token. Por tanto, un token en una blockchain pública puede ser cualquier cadena alfanumérica que

represente un registro en la base de datos descentralizada y que sea aceptada, por consenso, dentro de esa misma blockchain.

3.2.2. Características de la blockchain privada.

La propia tecnología blockchain ofrece la posibilidad de establecer una cadena de bloques con otras características distintas. Así que, de la misma forma, también puede construirse una blockchain privada, cerrada y con participantes identificados. O una privada, abierta y anónima, o una híbrida por asumir características propias de las blockchains públicas y privada.

Uno de los argumentos esgrimidos por el sector financiero y otros sectores regulados para el desarrollo de las blockchains privadas ha sido la imposibilidad de compartir, por razones regulatorias o de confidencialidad, sus bases de datos de forma abierta. Por tanto, estas blockchains privadas son:

- **Privadas:** porque no todos los datos inscritos en la blockchain tienen difusión pública y sólo los participantes o usuarios pueden acceder y consultar todas o algunas de las transacciones realizadas.

- **Cerradas:** sólo las personas o entidades invitadas a participar adquieren la condición de usuarios o registradores de las transacciones. En este sentido, el protocolo predeterminado podrá incluir distintos niveles de acceso a los usuarios, de modo que unos puedan tener la capacidad de registrar información y otros tener vetada esta opción. El diseño va siempre en función de los fines perseguidos.

- **Distribuidas:** el número de nodos de los que se componga la blockchain privada puede estar limitado al número de participantes o a cierto número de ellos. En cualquier caso, todos los nodos se conocen. La fortaleza de una blockchain se basa en gran medida en la cantidad de los nodos que la protegen y en los incentivos que éstos puedan recibir por cumplir este papel. A mayor número de nodos operativos, menor es la posibilidad de sufrir ataques. Pero, a diferencia de las blockchains públicas, donde el mantenimiento de los nodos depende de la voluntad de los usuarios, en las privadas son los participantes quienes se comprometen a mantener la estabilidad del sistema. Esto significa que una blockchain privada no está sujeta, por así decirlo, a las veleidades que puede sufrir una cadena pública, en la cual es sumamente importante definir correctamente medidas que trabajen a favor de su propia protección.

● **Anónimas:** una blockchain privada puede establecer el nivel de anonimato que quiera para realizar o proteger transacciones. Los usuarios que registran anotaciones pueden estar o no perfectamente identificados.

Los participantes en una blockchain privada, es decir, aquellos que hayan obtenido la condición de usuarios, están sujetos a un protocolo predeterminado que los podrá capacitar, según se establezca, para participar en el registro de las anotaciones y/o verificar los cambios introducidos en la cadena. En este sentido, una blockchain privada podría estar más centralizada y el número de nodos que componen la red podría limitarse al número de usuarios necesarios establecido por los promotores. Hablaríamos entonces de una base de datos conjunta gestionada por ese grupo de usuarios, en la que las anotaciones realizadas serán inalterables.

En la tecnología blockchain privada también se habla muchas veces de libro mayor en referencia a un registro global de transacciones, tal y como se conoce en la contabilidad tradicional. Tanto es así que las iniciativas de blockchains privadas se denominan con frecuencia en inglés Distributed Ledger Technology (DLT) o Tecnología de Libro Mayor Distribuido. Por otro lado, la blockchain privada es distribuida, en el sentido de que es una base de datos repartida en varios nodos, mientras que la pública es descentralizada, porque en ella no se controla quién participa en la misma.

De forma coloquial se puede decir que una blockchain es pública si cualquier usuario puede participar en ella libremente, de ahí que se la llame también “blockchain sin permiso” o permisionless. En cambio, en una privada la posibilidad de participar no está al alcance de todo el mundo, aunque el código utilizado sea público: la persona debe ser invitada a participar, razón por la cual en ocasiones se la denomina “blockchain con permiso” o permissioned. Con el tiempo se consolidarán multitud de blockchains con características distintas para cumplir con diferentes fines. Unas serán públicas, otras privadas y no faltarán tampoco las híbridas, dependiendo del modelo de uso para el que hayan sido diseñadas.

3.3. Concepto de transacción.

Para que se considere que un usuario posee una cierta cantidad de bitcoin, hay que tener en cuenta el concepto de transacción. Una transacción es una transferencia monetaria desde un usuario a la dirección de otro. Las

transacciones se agrupan en bloques que se integran en la cadena. Las transacciones se basan en los llamados “inputs” y “outputs”.

Se puede definir la moneda electrónica en sí como una cadena de firmas digitales. La firma digital permite la verificación del origen sin exponer la identidad del emisor o el receptor de la transacción (Figura 3.1). La transacción se firma con la clave privada asociada con la dirección del emisor y luego cualquier nodo de la red puede verificar con la clave pública que ese requerimiento de transacción proviene del dueño de esa dirección.

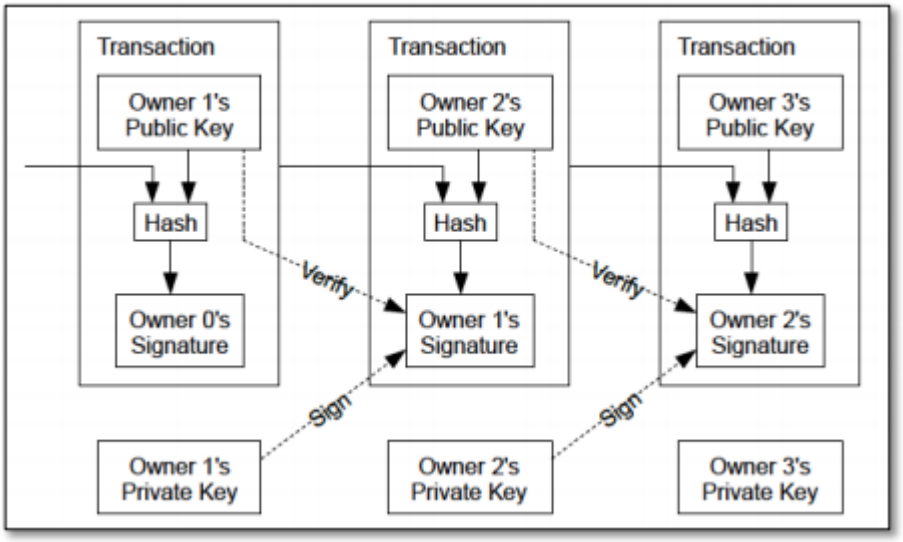


Figura 3.1 Transacciones.

Vemos de forma esquemática el contenido de cada transacción y su conexión con otras. Cada transacción incluye la firma digital del hash resultante de aplicar la correspondiente función hash criptográfica sobre el encadenamiento de la transacción anterior y la clave pública del receptor o beneficiario del valor. Una vez recibido este valor por el beneficiario, éste podrá transferirlo a su vez firmando con su clave privada un nuevo hash resultante de una nueva entrada para la función hash que incluiría la transacción que certifica su propiedad y la clave pública de aquel a quien desea transferir el valor.

Cualquier beneficiario (en realidad, cualquier tercero, aunque no participe en la transacción) puede comprobar la legitimidad de la transacción que le da el derecho de propiedad sobre el valor transferido mediante la verificación de la firma digital puesto que puede acceder a la clave pública del transmitente. En la Fig. 3.1, Owner 2 puede aplicar el proceso de verificación de la transacción comprobando que la clave pública de Owner 1 verifica la firma que este último realizó con la clave privada par de la pública conocida. En

caso de verificarse la firma, Owner 1 no podrá por tanto repudiar la emisión de la transacción.

Ahora bien, en lo que hemos visto no hay nada que impida a Owner 1 construir después de la transferencia a Owner 2 una nueva transacción basada de nuevo en la transacción que le aportó la propiedad del valor, pero esta vez utilizando una clave pública de otro beneficiario, que a su vez también podría validar satisfactoriamente la firma digital del transmitente. En resumen, nada impediría que Owner 1 cometiera un doble gasto transfiriendo el mismo valor a dos, o más, beneficiarios. Para solucionar este problema Nakamoto establece lo que podríamos denominar como el principio de prevalencia de la primera transacción registrada, que será la única válida y, por tanto, la única que cuente como transmisión efectiva del valor. Y lo complementa con la estrategia de que la única manera de confirmar la unicidad de la transmisión de un determinado valor es tener constancia de todas las transacciones, que en consecuencia deben ser anunciadas públicamente según se realicen para poder proceder a la comprobación de la deseada unicidad y evitar de esta manera el doble gasto. En conclusión, el beneficiario de cada transacción podrá sentirse confortable con la seguridad de su derecho siempre que la mayoría de los nodos involucrados en la gestión de la cadena consensuen que la transmisión de ese valor en concreto es la primera registrada. En caso de doble gasto, cualquier posterior beneficiario podrá descubrir de forma prácticamente trivial tal situación problemática al comprobar la existencia de una transmisión previa del valor.

Como herramienta para discriminar esta necesaria temporización entre transacciones, Nakamoto propone inicialmente y de manera conceptual un “servidor de marcas de tiempo” que actúe de la siguiente manera:

1. Reunir en un bloque un conjunto de ítems, que corresponderían en nuestro caso a las transacciones realizadas en un determinado periodo de tiempo.

2. Obtener como entrada de una función hash la concatenación entre el bloque en cuestión y el hash previo obtenido para el bloque anterior de manera similar al resultado de aplicar ahora la función hash.

3. Hacer público el resultado hash del punto anterior de manera que el momento de su publicación resulte indubitable, lo que probaría que en ese momento los datos que originaron el resumen hash existían.

Dado el mecanismo anterior, cada marca de tiempo referenciaría la marca anterior mediante el hash de esta última, lo que conformaría una cadena (Figura 3.2).

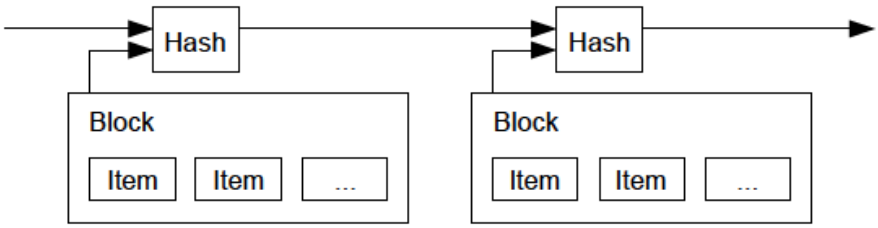


Figura 3. 2 Cadena de hash

Cada transacción puede ser dividida en dos partes: la entrada (de donde viene el dinero) o input y la salida (donde va el dinero) u output.

Una entrada o input es una referencia a la salida de una transacción pasada, pudiendo contener una transacción uno o más inputs. La cantidad de dinero que poseen las salidas referenciadas por las entradas de la transacción se suman y serán la cantidad de Bitcoins que se están transfiriendo.

Una salida u output es una indicación de a quien le debe llegar una cantidad de Bitcoins.

Además las transacciones, dentro del bloque, tienen las siguientes características:

- Pueden combinar distintas transacciones de entrada y salida. Es decir una única transacción puede coger fondos de distintas transacciones anteriores y repartirlos de la forma que estime oportuna a distintos destinatarios.

- La suma de importes de entrada debe ser mayor o igual que la suma de importes de salida. Es decir la suma de los fondos de las entradas debe ser igual (o mayor) a la suma de los fondos de las salidas. En la mayoría de los casos un usuario no tendrá transacciones anteriores cuyos fondos sumados den exactamente la cantidad que quiere enviar a la transacción. Lo que se hace es tomar como entradas transacciones anteriores cuyo importe sea superior al necesario, y en la transacción hacer la salida de los fondos que se quieran enviar al destinatario, más otra salida con el importe restante (el cambio) en la que el destinatario es el propio usuario que está haciendo la transacción.

- Comisión. Un usuario, además de las salidas a los destinatarios y a si mismo (el cambio) puede dejar pendiente un importe. Es decir, los importes de las entradas de la transacción son mayores que los importes de salida. Este excedente se denomina comisión y es totalmente voluntario (ya que el usuario que crea la transacción puede establecer

las entradas y salidas como prefiera). Esta comisión será para el nodo que procese la transacción, siendo un incentivo para que los diferentes nodos dediquen recursos a procesar las transacciones de los usuarios

Un ejemplo del funcionamiento de las transacciones se muestra en la siguiente figura (Figura 3.3):

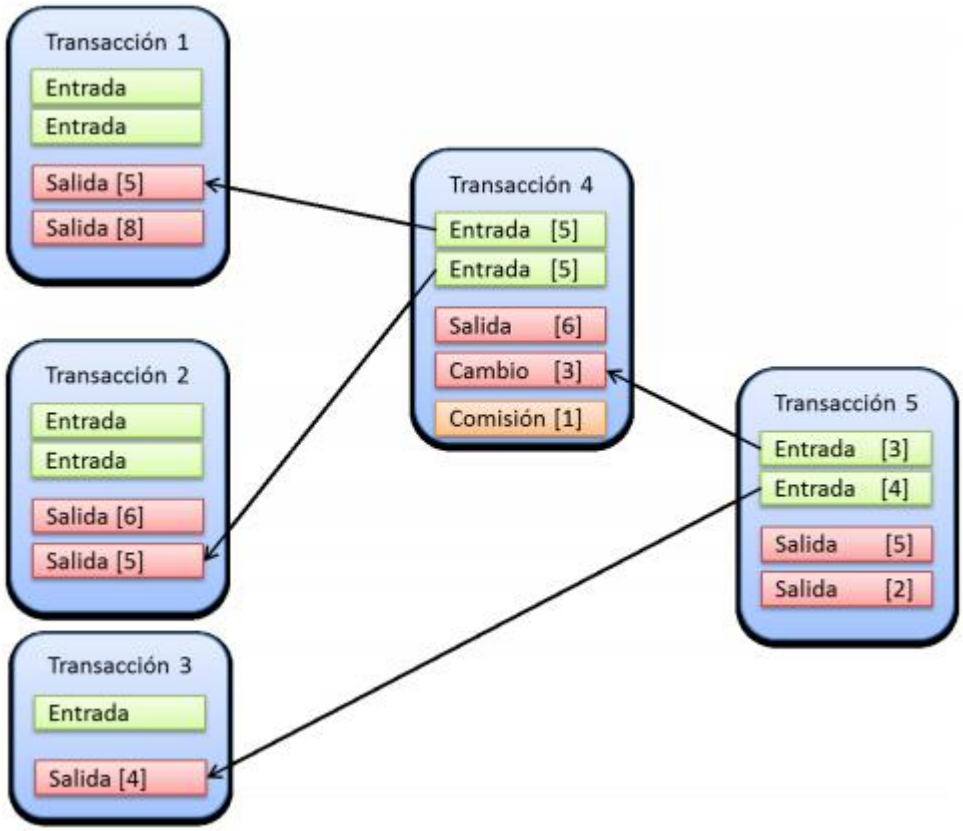


Figura 3.3 Funcionamiento de las transacciones.

En este ejemplo puede observarse:

● Unas transacciones iniciales (transacción 1, transacción 2 y transacción 3).

● Una transacción 4, en la cual el usuario tiene que pagar 6 bitcoin. Para ello la transacción:

- Recoge 5 bitcoin de la transacción 1.
- Recoge otros 5 bitcoin de la transacción 2.
- Realiza la transacción de salida (pago) de 6 bitcoin.

- Realiza otra transacción de salida a sí mismo (el cambio) de 3 bitcoin.

o La diferencia entre las entradas (5+5=10 bitcoin) y las salidas (6+3=9 bitcoin) deja una comisión de 1 bitcoin.

● Una transacción 5 en la cual el usuario debe hacer 2 pagos, de 5 y 2 bitcoins. Para ello la transacción:

- Recoge los 3 bitcoin de cambio de la transacción 4.
- Recoge 4 bitcoins de la transacción 3 o Realiza una transacción de salida (pago) de 5 bitcoin
- Realiza una transacción de salida (pago) de 2 bitcoin.
- En este caso todas las entradas (4+3=7 bitcoin) se convierten en salidas de pago (5+2=7 bitcoin) por lo que no queda comisión.

3.3. Concepto de bloque.

Un bloque es un conjunto de datos estructurado que contiene una determinada cantidad de transacciones. Estos bloques se pueden extraer, transmitir y confirmar. La blockchain es una cadena de todos estos bloques.

Una vez conocido el concepto de bloque, queda por conocer cómo se estructura la información dentro del bloque. En la representación en disco, un bloque es un fichero binario que utiliza el software de Bitcoin. Dicho fichero tiene una cabecera, como es habitual en los ficheros binarios, con el siguiente formato (Figura 3.4):

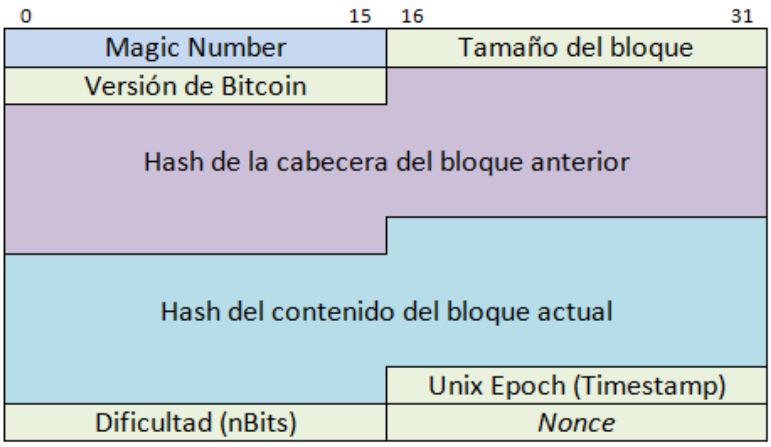


Figura 3.4 Cabecera de un bloque de Bitcoin.

En la siguiente tabla se detallan cada uno de los campos de la cabecera:

Campo	Descripción	Tamaño
Magic Number	Valor establecido siempre a 0xD9B4BEF9	4 bytes
Tamaño del Bloque	Número de bytes que siguen hasta el final del bloque	4 bytes
Versión de Bitcoin	Version de Bitcoin utilizada	4 bytes
Hash de la cabecera del bloque anterior	Cada bloque incluye la referencia y el hash del bloque anterior.	32 bytes
Hash del contenido del bloque actual	Se trata del hash del contenido del bloque actual. (No puede contener el hash de la cabecera porque se incluiría a si mismo)	32 bytes
Timestamp	Marca de tiempo de creación del bloque	4 bytes
Dificultad (nBits)	Contiene una representación del límite del hash, que modela la dificultad.	4 bytes
Nonce	Una serie de bytes modificables para hacer cumplir los criterios de dificultad. Es la que se utiliza para la prueba de trabajo.	4 bytes

Tabla 3.1 Campos de la cabecera del bloque de Bitcoin.

Justo después de la cabecera del bloque se encuentran los siguientes campos:

- **Número de transacciones que contiene el bloque:** El contador de transacciones no tiene una longitud fija. En realidad es de un tipo entero “compacto”, que es un tipo de dato utilizado por Bitcoin, y que tiene una longitud de bytes variable. Para poder obtenerlo (Figura 3.5) se lee el primer byte, si es 0xFD, entonces tendrá 3 bytes de longitud; si es 0xFE tendrá 5 bytes de longitud; si es 0xFF tendrá 9 bytes de longitud, y si no es ninguno de esos valores, ocupará un solo byte, con el valor correspondiente.

Value	Bytes Used	Format
<= 252	1	uint8_t
<= 0xffff	3	0xfd followed by the number as uint16_t
<= 0xffffffff	5	0xfe followed by the number as uint32_t
<= 0xffffffffffffffff	9	0xff followed by the number as uint64_t

Figura 3.5 Valor del contador de transacciones.

● **Transacciones que ha recibido el nodo:** Después del número de transacciones, se almacenan, una detrás de otra, las transacciones que ha recibido el nodo y que desea introducir en la cadena. Son transacciones que previamente debe validar para asegurarse de que pueden introducirse sin dar lugar a colisiones o incoherencias que provocarían que el resto de nodos rechazaran la introducción del bloque en la cadena. Los campos de una transacción son los siguientes (Figura 3.6):

● **Versión**: Entero de 4 bytes.

● **Total de inputs de esta transacción**: Entero compacto, tal y como se ha visto anteriormente con el número de transacciones.

● **Lista de inputs**: Cada input tiene el formato TxIn, el cual se explica como sigue:

- **Outpoint anterior**: Ocupa 36 bytes (32 del identificador de transacción TxID, y 4 del índice del output).

- **Bytes del script**: Entero compacto que representa el número de bytes del siguiente campo (signature script).

- **Signature script**: Firma de la transacción. Se utiliza para comprobar la autenticidad de la misma.

- **Número de secuencia**: Entero de 4 bytes.

● **Total de outputs**: Entero compacto, tal y como se ha visto anteriormente.

- **Lista de outputs**: Cada output tiene el formato TxOut, el cual se explica como sigue:

    - **Número de Satoshis**: Entero de 8 bytes. Representa el número de Satoshis de la transacción. Un Satoshi es 0,00000001 BTC.

    - **Bytes del script**: Entero compacto que representa el número de bytes del siguiente campo (pk_script).

    - **Pk_script**: Datos que contienen las condiciones que deben ser satisfechas para poder gastar esos satoshis. Se utiliza para verificar la autenticidad.

Description			Value	Hex
version			1	01000000
txin_count			1	01
txins[0]	outpoint	hash	030a05cd13f2b8cdacaafcc1391b54f78110c44036f5aea6c4963533815ad203 03d25a81333596c4a6aef53640c41081f7541b39c1fcaaaccdb8f213cd050a03	
		index	0	00000000
	script length		35	23
	signature_script		2102515ca98f0e0fc6ecf5a20554bbef48f86b249ec75154a4259e6d4ea8f1f4d654ac	
	sequence		4294967295	ffffffff
txout_count			1	01
txouts[0]	value		20800000 (0.20800000 BTC)	00623d0100000000
	pk_script length		25	19
	pk_script		76a91476a7d66e4617d488c39c1bd56ec546865059f4a888ac	
lock_time			0	00000000

Figura 3.6 Formato de una transacción.

- **Coinbase o Moneda base:** El último valor del bloque sería el Coinbase (Moneda base), es una transacción especial sin origen. En esencia es la generación de una nueva unidad de bitcoin, y es la forma en que se genera la masa monetaria en bitcoin. Cada bloque que se genera lleva una nueva cantidad para el nodo que ha generado el bloque.

3.4. Concepto de cadena de bloques (blockchain).

La cadena de bloques de la red Bitcoin es una lista creada de forma colectiva con todas las transacciones que han sido confirmadas y validadas por la propia red mediante la inclusión de transacciones en bloques y de estos últimos, en la cadena.

Cuando un nodo de la red consigue crear un nuevo bloque, lo transmite al resto de nodos. El resto de nodos verifican que el bloque es correcto, y en caso afirmativo, lo añaden a su cadena y lo difunden. Mediante la difusión del nuevo bloque, éste acabará añadiéndose siempre y cuando no se haya creado otra rama en la cadena de bloques en la que haya participado una cantidad de usuarios con más capacidad de cómputo.

Por la propia naturaleza de la cadena de bloques, se puede extraer el historial de posesión de todas las monedas, siguiendo la lista de transacciones. Así, un usuario no puede reutilizar monedas que ya usó, ya que la propia red rechazará la transacción.

Se puede dar el caso de que haya bitcoins reutilizadas de manera no malintencionada. Por ejemplo, por fallos de comunicación masivos, como caídas de redes de comunicaciones, o cuando se crean ramas en la cadena, conteniendo cada una aproximadamente la mitad de la potencia de cálculo del sistema. Por ello, es buena práctica esperar un tiempo determinado para confirmar una transacción y, por lo tanto, que el receptor de la bitcoin pueda considerar el pago como recibido. Por defecto, los clientes más extendidos incluyen un tiempo de espera de 6 bloques. Es decir, hasta que no se hayan validado 6 bloques desde el que incluyó la transacción, no se considera el pago como realmente efectuado. Dado que el tiempo medio de generación de bloques es de uno cada 10 minutos, esto supone que las transacciones tardan en confirmarse aproximadamente una hora.

Por otro lado, la blockchain almacena una gran cantidad de datos y además su tamaño es creciente con el tiempo ya que en la misma sólo se añade información. Por tanto, es aconsejable disponer de algún mecanismo que permita una consulta a la blockchain eficiente, es decir, que permita realizar consultas sin tener que descargar toda la información almacenada. Para este propósito, en la blockchain de bitcoin, se propone utilizar un árbol hash de Merkle (Figura 3.7).

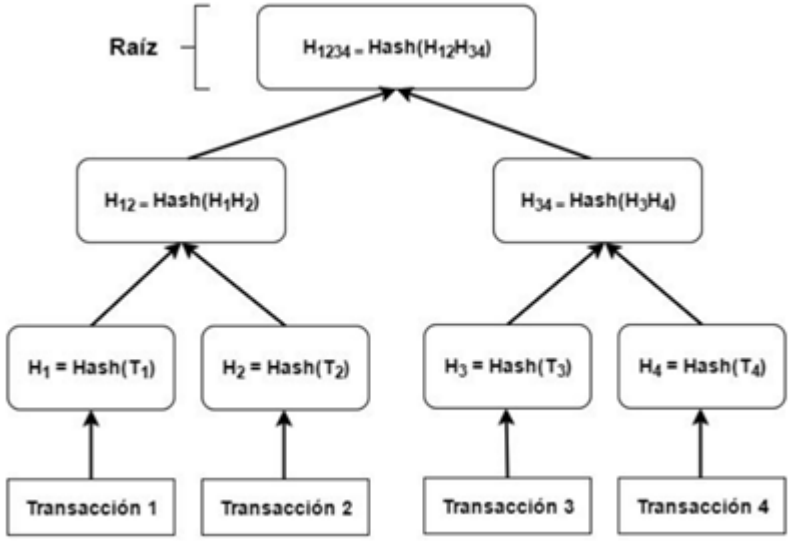


Figura 3.7 Arbol de Hash de Merkle

Como se muestra en la figura, el árbol de hash de Merkle permite almacenar diversas piezas de información independiente (en el caso de Bitcoin son transacciones de BTC) en las hojas de una estructura en árbol. Para formar el árbol, se hace un hash de la información contenida en cada nodo/ hoja. A continuación, para generar los nodos de cada nivel superior del árbol se concatenan diversos valores hash del nivel inferior (dos valores si el árbol es binario) y se le aplica la función hash a esta concatenación. Repitiendo este proceso se llega a un nivel donde hay un sólo nodo, denominado la “raíz” del árbol.

La ventaja de esta estructura en árbol es que podremos consultar la presencia en dicho árbol de los datos de un cierto nodo/hoja de forma autenticada y sin tener que disponer de toda la información que almacena el árbol. En particular, se puede consultar de forma autenticada cualquier contenido del árbol con una cantidad de valores hash proporcional al logaritmo del número de nodos del árbol.

Esto es porque para validar un contenido únicamente hay que proporcionar los nodos adyacentes en cada nivel y el nodo raíz (que tiene contribución de todos los datos almacenados en las hojas) autenticado. Entonces, para validar un contenido se calcula el valor raíz a partir de los nodos adyacentes proporcionados y se comprueba que coincide con el valor raíz autenticado. La estructura es segura porque no se puede generar un conjunto de nodos adyacentes a voluntad que dé como resultado el valor del nodo raíz autenticado.

La cadena de bloques, en lo que a estructura de datos se refiere, se establece mediante los campos “Hash de la cabecera del bloque anterior” y el “Hash del contenido del bloque actual“, de cada bloque. En la figura 3.8 se muestran los diferentes enlaces entre datos mediante el uso de hashes y posteriormente se detalla cada entrelazamiento para su mejor comprensión.

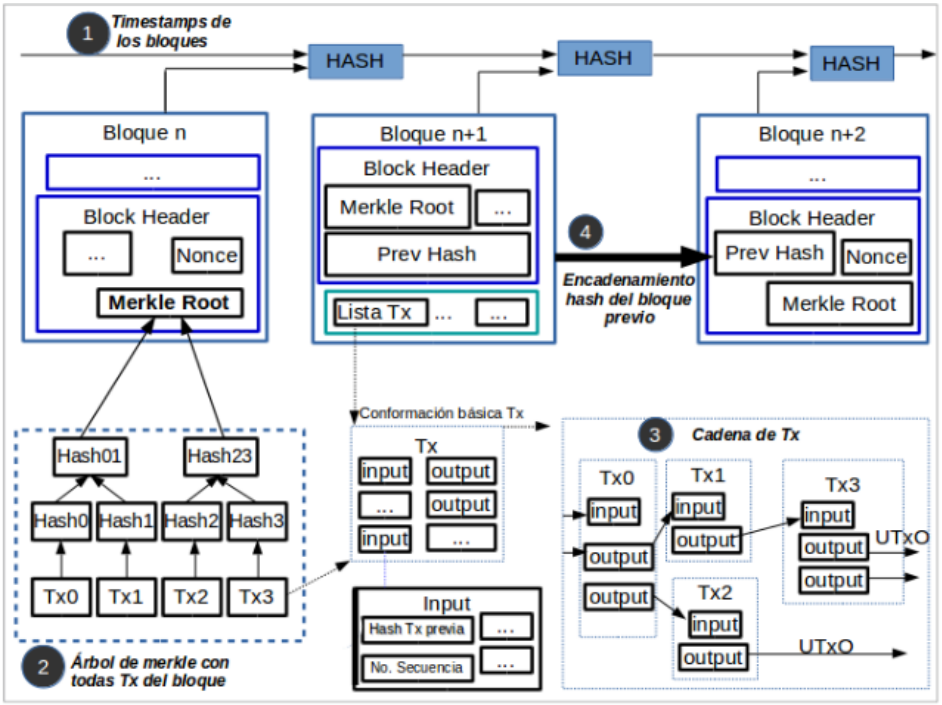


Figura 3.8 Cadena de bloques.

1. El servidor P2P distribuido de marca de tiempo (timestamp) se implementa utilizando PoW incrementando un nonce en el bloque hasta lograr llegar a un hash con el nivel de dificultad del reto (un hash con una cantidad determinada de ceros). El hash del bloque anterior se guarda en el block header de cada bloque.

2. El uso de funciones hash para enlazar bloques y transacciones anteriores con un bloque/transacción en particular y el ahorro de espacio en disco cuando se utiliza el árbol de Merkle con el hash de las transacciones apareadas.

3. Todo input corresponde a un output y el entrelazamiento entre transacciones se realiza a través de un campo en los inputs. Cada output de una transacción solo puede ser referenciado una vez por un input de una transacción subsiguiente.

4. Cada bloque en la cadena contiene un hash del bloque anterior creando así una cadena de bloques desde el primer bloque hasta el último

bloque en la cadena más larga. Así se asegura que no puede ser modificado un bloque específico sin antes modificar el bloque que lo tiene registrado y todos los bloques subsiguientes a este.

3.5. Minería de bloques.

Hasta el momento se han expuesto, entre otros, los detalles técnicos de las transacciones que se integran en la cadena de bloques. Pero un punto clave para el funcionamiento de la blockchain es la validación democrática de la misma. Sin ella, un agente malicioso podría validar por su cuenta transacciones que fueran provechosas para el mismo.

Para evitar esto, se promueve que haya un conjunto de agentes, los mineros, que invierten sus recursos en mantener un consenso sobre el estado de las finanzas de la moneda.

Para conseguir este consenso se parten de unas condiciones muy sencillas. Cualquier agente puede conectarse a otro nodo de la red, y recibir transacciones para formar un bloque con ellas. Un bloque tiene un tamaño máximo de un megabyte. Cuando tienen un bloque formado, intentan resolver un rompecabezas computacional. El rompecabezas consiste en encontrar un parámetro (nonce) que consiga que al hacer el hash sobre todo el bloque (incluido el nonce) se obtenga un valor inferior a la dificultad actual establecida por la red. Dicho de otra forma, se trata de encontrar un nonce que consiga un valor hash del bloque con un determinado número de ceros al inicio. Debido a las características de la función de hash, no es posible calcular estos valores analíticamente, es decir, para obtener un bloque válido, el minero debe recurrir a la fuerza bruta: probar valores del parámetro nonce hasta hallar uno válido. Además, en el caso de que el agente haya agotado todos los nonces sin cumplir el objetivo, puede actualizar la marca de tiempo que posee la cabecera del bloque para variar igualmente el resultado del hash.

Sin embargo, debido a la reducción del target de la red, es decir, al aumento de dificultad del problema, ha pasado a no ser suficiente un recorrido de todos los valores posibles del nonce en un segundo, que es la resolución de la marca de tiempo del bloque. Para solucionar esto, hay otro campo, llamado extra nonce, que se introduce dentro de la lista de transacciones, en concreto dentro de la llamada “generation transaction”.

La “generation transaction” es la primera transacción incluida en un bloque. Esta transacción es el motivo por el cual los mineros deciden invertir

sus recursos de cómputo en la resolución de bloques. En ella, los mineros obtienen Bitcoins por haber encontrado la solución al bloque, de dos maneras. La primera, es que en esta transacción se envían a sí mismos la suma de todos los excedentes de los inputs no gastados por los outputs de las transacciones, las llamadas cuotas de las transacciones. Las cuotas son un margen que los generadores de las transacciones pagan a los mineros para que les interese incluir su transacción y no otra en un bloque.

Por otra parte, en la “generation transaction” los mineros pueden asignarse una cantidad de Bitcoins como botín. Esta cantidad es actualmente 12,5 bitcoins pero se reduce a la mitad cada 210000 bloques, es decir, aproximadamente 4 años (Figura 3.9). Esto produce que la cantidad de moneda esté limitada, y que en 2024 se hayan minado el 93.75% de los Bitcoin. Está estimado que el último Bitcoin se mine en el año 2140 si no hay ningún cambio en las implementaciones de los protocolos de hash que rompan el funcionamiento de la red.

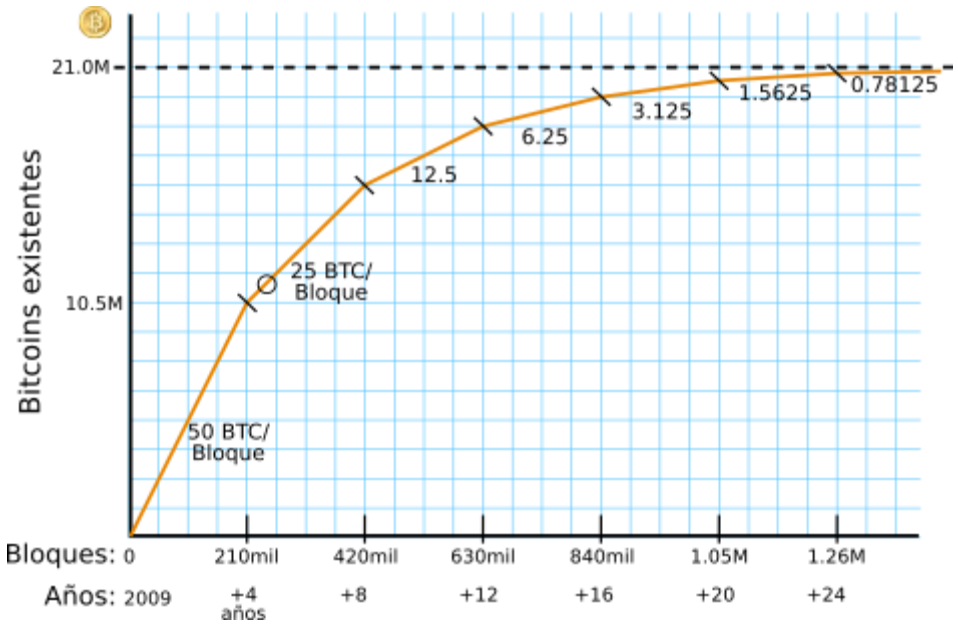


Figura 3.9 Evolución recompensa por bloque minado.

De esta forma, los mineros obtienen una recompensa si se dedican a validar bloques, pero un minero malicioso podría todavía ir en contra de las normas de Bitcoin y propagar el mensaje de que ha validado un bloque, aunque este realmente no sea válido. Pero aquí entra en juego el afán de obtener ventaja económica de los mineros. La rentabilidad de la validación de un bloque depende de la futura aceptación de dicho bloque como válido por el resto de mineros, los cuales si lo aceptan, empezarán a buscar un conjunto diferente de transacciones para continuar la cadena a partir de este.

Por todo esto, las normas de funcionamiento de la red Bitcoin dependen de los propios mineros, puesto que si todos se pusieran de acuerdo para seguir una nueva norma o dejar de seguir una antigua, los bloques que fueran conformes a la nueva normativa serían aceptados por la mayoría de los mineros haciendo que la secuencia más larga de la cadena de bloques se ajuste a la misma.

La minería de Bitcoin ha pasado por varias fases (Figura 3.10). El problema a resolver no deja de ser un sorteo en el que el minero tiene más papeletas cuantos más hashes es capaz de hacer por segundo. Las implementaciones iniciales de los programas usaban la CPU de los ordenadores para minar, con una implementación software del algoritmo sha256, permitiendo incluso el cliente oficial de Bitcoin minar simplemente con pulsar un botón. Posteriormente, conforme la moneda fue ganando popularidad, y con el consiguiente aumento del número de mineros, la dificultad exigida por la red Bitcoin aumentó, quedando obsoleto el minado por CPU, al no ser rentable por la electricidad consumida.

Posteriormente, diversos programas de minado implementaban el algoritmo sha256 utilizando la GPU (Graphics Processing Unit), lo que permitía paralelizar la búsqueda entre todas las ALUs de la tarjeta gráfica, aumentando drásticamente el número de hashes por segundo que un minero podia realizar. El minado por GPU fue muy utilizado hasta la llegada de los ASICS, que han convertido el minado por GPU en un proceso no rentable en la mayoría de los casos. Los llamados ASICS (application specific integrated circuits) son dispositivos Electrónicos diseñados para implementar en hardware una función concreta, en este caso, el minado de Bitcoin, siendo órdenes de magnitud más rápidos que las GPU, y con una mucho mayor eficiencia energética. Brevemente también se usaron FPGAs (Field Programmable Gate Array) para minar, siendo un paso intermedio entre las GPU y los ASIC, pero nunca fueron muy populares.

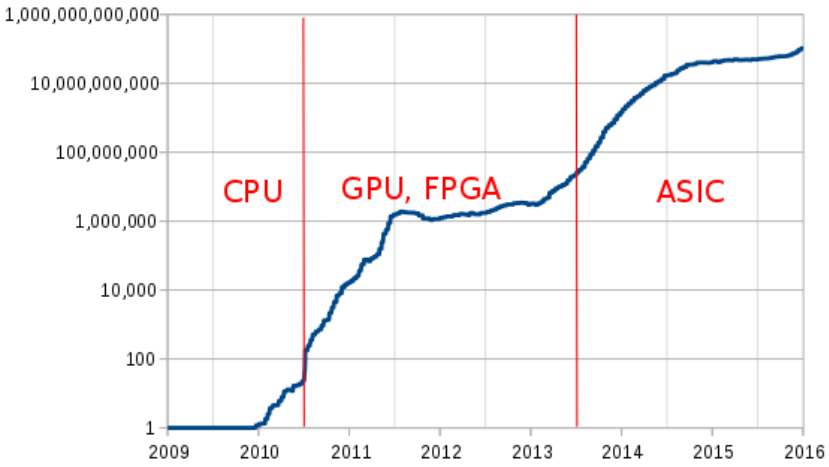


Figura 3.10 Evolución del hardware usado por los mineros.

Por último se enumeraran los distintos caminos por los que un usuario puede formar parte de esta red de procesamiento:

- La primera opción que tiene para incorporarse a la red de procesamiento es la disponibilidad de un equipo independiente para realizar el procesamiento necesario. No es muy aconsejable puesto que existen nuevos y potentísimos ordenadores específicos para este tipo de trabajo, y supondría una inversión muy elevada. Los beneficios al encontrar un bloque en solitario serían mucho mayores que si trabaja en grupo, pero la probabilidad es infinitamente menor.

- La segunda opción sería añadir un equipo específico en un pool de minado para contribuir a una mayor potencia de procesamiento. Un pool de mineros puede definirse como una unión de potencia de procesamiento, con lo que sería más fácil encontrar un nuevo bloque. En este caso el beneficio se dividirà entre los miembros del pool según la potencia de procesamiento que cada minero haya aportado al grupo.

- Por último existe la posibilidad de alquilar potencia de procesamiento (Cloud Mining) que habrá que pagar en bitcoins o en moneda tradicional. Los beneficios en este caso también se repartirán entre todos aquellos que hayan contribuido.

3.6. Consenso en la blockchain de Bitcoin.

Como se ha visto en puntos anteriores el algoritmo de consenso de la red de blockchain de Bitcoin es la “Prueba de Trabajo”, “Proof of Work” o PoW.

El PoW requiere que los participantes realicen un trabajo intensivo desde el punto de vista computacional pero fácil de verificar por otros miembros en la red. En el caso del bitcoin, los mineros compiten por añadir un conjunto de transacciones (el bloque), al blockchain global mantenido por la red. Para hacer esto, un minero debe ser el primero en descifrar correctamente el "nonce", para crear un hash que comienza con un número requerido de ceros. El minero ganador se anuncia públicamente y el resto puede comprobar fácilmente que hizo bien la prueba de trabajo. Una vez que todos están de acuerdo agregan el bloque a la cadena y el ciclo se repite (Figura 3.11).

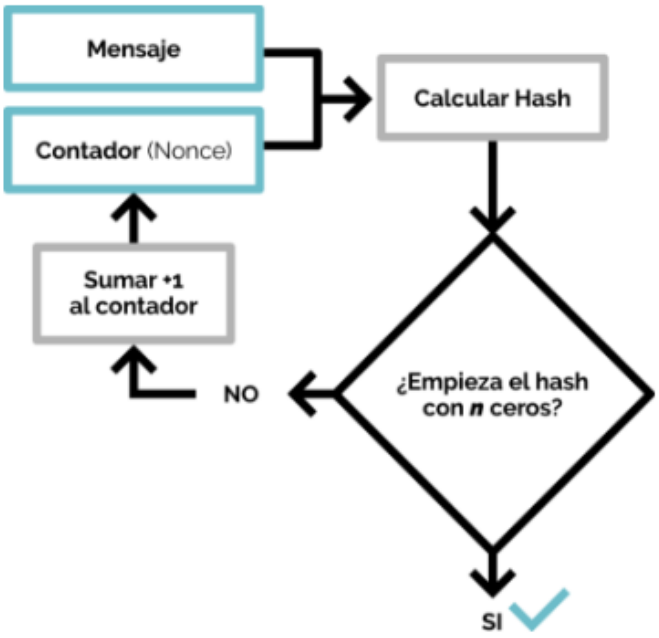


Figura 3.11 Ciclo calculo hash.

A medida que la red crece, enfrenta cada vez más dificultades. Los algoritmos necesitan cada vez más poder hash para resolverse. Entonces, la complejidad de la tarea es un tema delicado. El trabajo preciso y la velocidad del sistema Blockchain dependen de ello. Si la tarea es demasiado complicada la generación de bloques lleva mucho tiempo. Las transacciones se bloquean sin ejecución y, como resultado, el flujo de trabajo se bloquea durante un tiempo. Si el problema no puede resolverse en un período de tiempo definido, la generación de bloques será una tarea casi imposible. Si por el contrario es

demasiado fácil, es propenso a las vulnerabilidades y ataques de DoS (Deny of Service.

La solución necesita ser revisada fácilmente. De lo contrario, no todos los nodos son capaces de analizar si los cálculos son correctos. En este caso se tendrá que confiar en otros nodos y eso violaría una de las características más importantes de Blockchain: la transparencia. En este sentido fue Bitcoin el que sentó las bases para este tipo de consenso. El rompecabezas es Hashcash. Este algoritmo permite ajustar, cada 10min, la complejidad del problema a resolver en función de la potencia total de la red.

Como principales beneficios al usar PoW como algoritmo de consenso en la blockchain de Bitcoin, están:

- Defensa contra ataques DoS. La PoW impone algunos límites a las acciones en la red. Necesitan mucho esfuerzo para ser ejecutados. Un ataque eficiente requiere una gran cantidad de potencia computacional y mucho tiempo para hacer los cálculos. Por lo tanto, el ataque es posible pero inútil ya que los costos son demasiado altos en comparación con los beneficios.

- Posibilidades de minería. No importa cuánto dinero se tenga en la billetera (wallet). Lo que importa es tener un gran poder computacional para resolver los rompecabezas y formar nuevos bloques. Por lo tanto, los titulares de grandes cantidades de dinero no están a cargo de tomar decisiones para toda la red.

Por otra parte, también hay que tener en cuenta los defectos en el algoritmo de consenso PoW:

- Grandes gastos. La minería requiere hardware informático altamente especializado para ejecutar los algoritmos complicados. Los costos son inmanejables. La minería está disponible sólo para grupos mineros especiales. Estas máquinas especializadas consumen grandes cantidades de energía para funcionar que aumentan los costos. Los grandes costos amenazan la centralización del sistema, ya que beneficia a los mineros con más recursos (Figura 3.12).

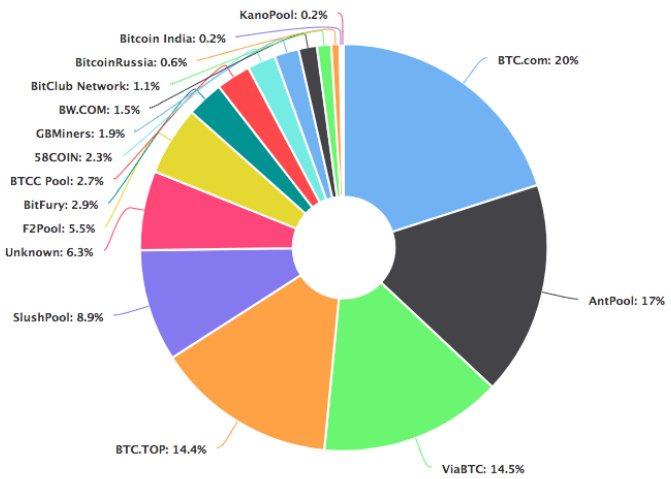


Figura 3.12 Distribución de los principales pooles de minería.

● Ataque del 51%. Derivado del costo elevado que implica participar en el trabajo de un sistema PoW, es que cada vez menos personas pueden adquirir los equipos necesarios y por lo tanto la comunidad se vuelve más exclusiva. Esto viola la idea de la descentralización que justamente busca distribuir al poder, no centralizarlo. La centralización en los sistemas de consenso puede llevar a un ataque del 51% (Figura 3.13). El ataque del 51% podría pasar si un nodo controla el 51% del poder de computación que le dejaría hacer todo tipo de trampas como bloquear transacciones o gastar el mismo dinero dos veces. La manera de hacer esto, sería creando y formando sus propios bloques fraudulentos. Los demás simplemente aunque generen bloques válidos, simplemente serían invalidados por el agresor.

El ataque del 51% no es una opción rentable. Requiere una enorme cantidad de poder de minería. Y una vez que se expone públicamente, la red se considera comprometida, lo que lleva a la salida de los usuarios. Esto inevitablemente moverá el precio de la criptomoneda hacia abajo. Todo en consecuencia, los fondos pierden su valor.

Por último se tratará el problema de la modificación de las reglas de consenso. Las reglas de consenso son las reglas más importantes de Bitcoin. Establecen, entre muchas otras cosas, la cantidad de bitcoins incluidos en la recompensa minera (coinbase), la dificultad de minado, el tipo de PoW requerido, y, también, el límite del tamaño de los bloques.

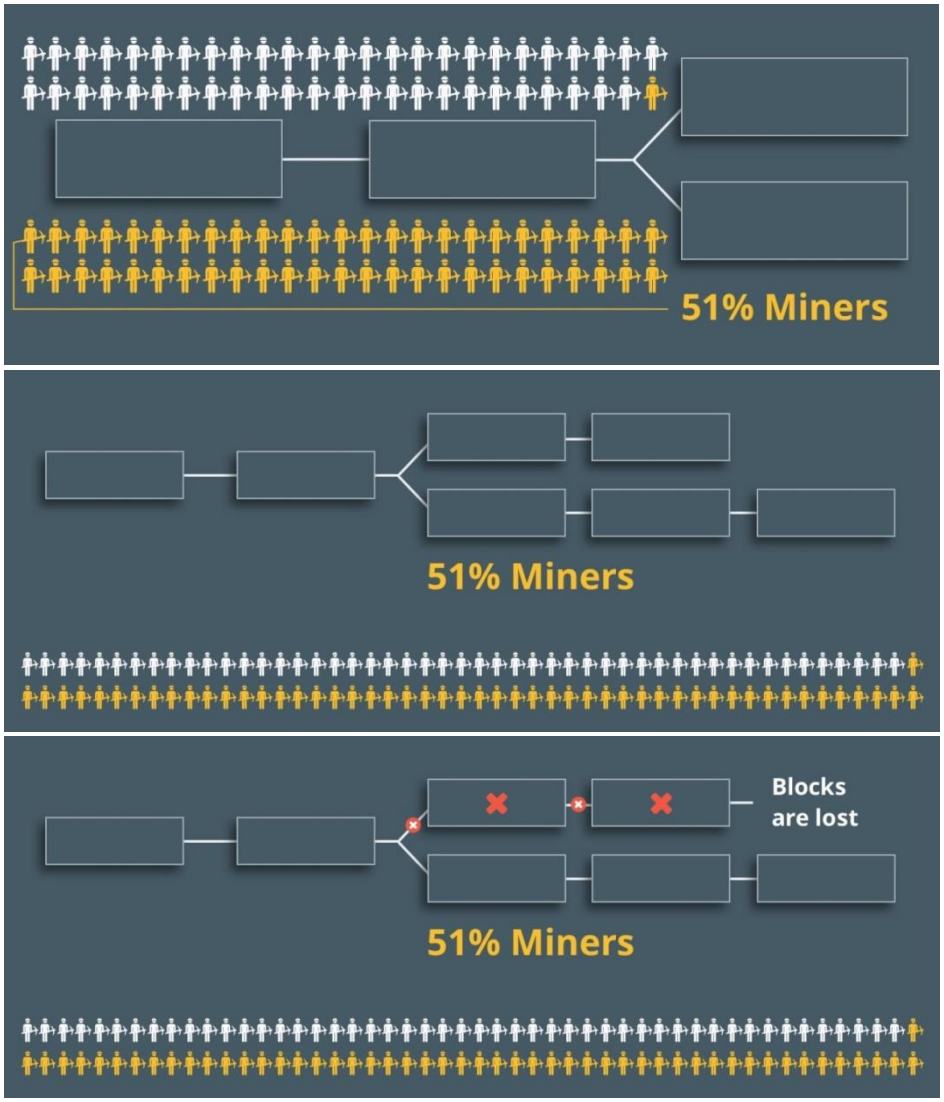


Figura 3.13 Ataque del 51%.

Estas reglas son tan importantes porque determinan qué bloques son considerados válidos por todos los nodos completos. Y si todos los nodos completos aplican las mismas reglas de consenso, se asegura que todos ellos mantienen una copia idéntica de la cadena de bloques.

En cambio, si los diferentes nodos aplican diferentes reglas de consenso, se corren el riesgo de que unos acepten unos bloques y otros los rechacen, lo que implicaría que los nodos de la red mantienen versiones completamente incompatibles de la cadena de bloques, lo que supondría que la red Bitcoin quedaría dividida. Las reglas del consenso de Bitcoin se pueden modificar de dos maneras:

● A través de un cambio que añade reglas adicionales al protocolo (haciendo que los bloques actuales sean inválidos). Es lo que se conoce como softfork o bifurcación blanda (Figura 3.14). Estos tipos de cambio requieren de la mayoría de la potencia de hash de la red para que sean efectivos. Y en este caso, los bloques que se producen bajo las nuevas normas serán válidos también bajo las viejas reglas, por lo que los nodos que no actualizan continuarán considerando la cadena más larga como válida.

En cualquier caso, los mineros no actualizados podrán producir bloques que no son válidos bajo las nuevas reglas, lo que implicará un desperdicio de la potencia de hash. Y los nodos completos no actualizados ya no serán capaces de verificar los nuevos bloques bajo las nuevas reglas, por lo que tendrán que esperar confirmaciones adicionales para alcanzar el mismo nivel de seguridad.

Por estas y otras razones, el equipo de desarrollo del Bitcoin Core ha asegurado que se requerirá normalmente una súper mayoría del 95% de la potencia de hash para ponerse de acuerdo en los soft forks.

Figura 3.14 Soft Fork.

● A través de un cambio que elimina las reglas del protocolo (haciendo que los bloques que antes no eran válidos, sí lo sean ahora). Es lo que se conoce como hard fork o bifurcación dura (Figura 3.15). Un hard fork requiere que todos los nodos completos de la red adopten dichos cambios, es decir que actualicen el software. Cualquier nodo que no implemente el cambio podría no seguir la cadena más larga, ya que podría considerar que dicha cadena es inválida y permanecerá en la cadena “vieja” que es la que reconoce como válida. Esto podría dividir la

red Bitcoin. El tiempo que esa división de la cadena de bloques dure no es en realidad una cuestión técnica, sino más bien un debate sobre política, sociología, economía, teoría de juegos y mucho más.

Figura 3.15 Hard fork.

Los cambios a través de soft forks a las reglas de consenso sin un consenso, podrían en el peor de los casos, provocar que una minoría de los mineros desperdicien potencia de hash y ligeramente degradar la seguridad de los nodos completos.

Los cambios a través de hard forks de las reglas de consenso sin consenso podrían en el peor de los casos dividir la red Bitcoin en dos.

3.7. Diferentes mecanismos de consenso en blockchain.

Hasta ahora se ha visto el algoritmo de consenso que utiliza la blockchain de Bitcoin. A continuación se presentarán otros mecanismos de consenso:

● **Proof-of-stake**. En este caso se utilizan algoritmos que hacen que la probabilidad de que un nodo sea elegido para generar o validar el siguiente bloque sea proporcional a lo que tiene invertido en el blockchain, normalmente en forma de monedas. La recompensa suele ser en forma de comisiones por transacción.

El algoritmo se basa en la preselección del nodo que generará el siguiente bloque de entre una serie de nodos validadores que deben bloquear parte de su criptomoneda para poder optar a crear nuevos bloques. Tras la generación, el bloque debe ser aceptado por el resto de los nodos validadores mediante un proceso de votación. Los nodos reciben recompensa por participar en la generación y en la validación de la cadena.

En cuestión de seguridad, el principio en el que se basa es que un posible atacante necesitaría invertir mucho para llegar a ganar el control del proceso de creación y aceptación de nuevos bloques. Además, un ataque devaluaría muy significativamente la inversión, por lo que un atacante que hubiera invertido lo suficiente para atacar el blockchain vería su inversión perdida.

Un posible riesgo que debe tenerse en cuenta al implementar este tipo de algoritmos es el posible beneficio que un nodo puede obtener de votar en varios bloques a la vez, aun sabiendo que uno de ellos no es válido.

Este tipo de comportamiento podría llegar a hacer el consenso imposible, por lo que los nodos con mucho invertido en el blockchain normalmente no estarán interesados en llevarlo a cabo, ya que haría su inversión inservible. Sin embargo, aquellos nodos con una inversión pequeña y con poco que perder, podrían utilizar este tipo de técnicas para obtener recompensa más rápidamente. De ahí que este problema se denomine “nothing at stake” que podría traducirse como “nada que perder” (Figura 3.16).

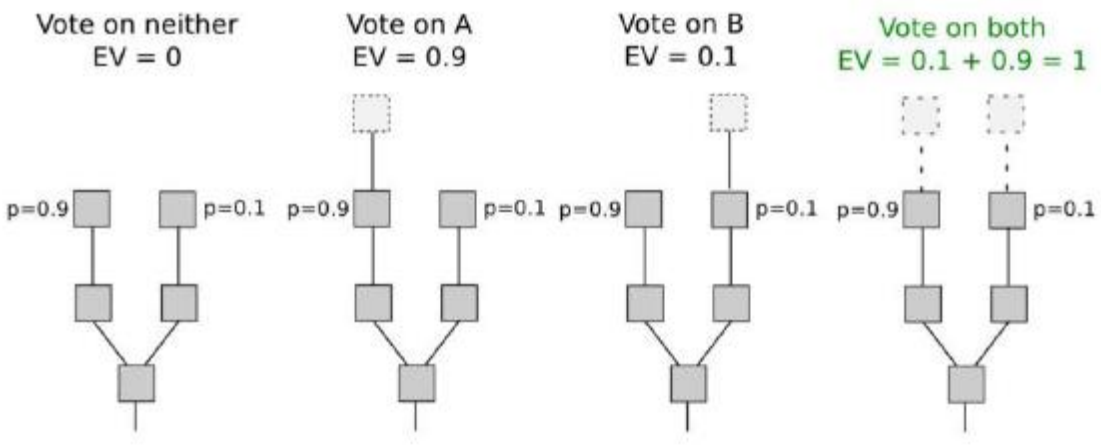


Figura 3.16 "Nothing at stake".

Por ello, casi todos los mecanismos de tipo proof-of-stake implementan algún tipo de penalización para aquellos nodos que votan por votos que no se llegan a confirmar en la cadena de bloques.

Existen diferentes implementaciones de este tipo de mecanismo de consenso pero, en comparación con PoW, todos requieren de menor consumo de energía y son más rápidos a la hora de generar nuevos bloques.

● **Delegated Proof-of-stake.** Aunque el nombre del Delegated Proof-of-Stake (DPoS) es parecido al del Proof-of-Stake, los detalles de su implementación son significativamente diferentes. En el DPoS, en lugar de apostar monedas para validar transacciones, los propietarios de tokens votan por un grupo selecto para que cumpla la función de validar transacciones.

El DPoS permanece "descentralizado" en el sentido de que todos los participantes de la red participan en la selección de los nodos que validan las transacciones, pero centralizado en el sentido de que un grupo más pequeño toma decisiones que aumentan la velocidad y la verificación de las transacciones.

Las implementaciones del DPoS mantienen una reputación, un proceso de votación continuo y un sistema de reorganización que mantiene a los validadores electos responsables y honestos.

Las ventajas del DPoS son que es escalable y proporciona una rápida verificación de las transacciones, pero la desventaja es que está parcialmente centralizado y el modelo de gobernanza no ha demostrado ser eficaz en un proyecto de gran envergadura. El DPoS es empleado por los implementadores Steemit, EOS y BitShares.

● **Proof-of-activity.** Este tipo de consenso propone una combinación de los dos anteriores para reforzar la seguridad. Se busca que un posible atacante no sólo necesite capacidad de cómputo sino también poseer criptomoneda para hacerse con el control de la cadena de bloques. El problema que se intenta atajar es una posible debilidad futura de la red de bitcoin, causada por una potencial disminución del número de nodos mineros al reducirse la recompensa por minar bloques. Partiendo del PoW de bitcoin, se propone un paso adicional para la validación de bloques, en el que una serie de nodos, que deben poseer o haber poseído bitcoins para ser seleccionados, confirman el bloque generado por un nodo minero.

La Figura 3.17, muestra la relación entre el número de nodos que deben confirmar en este segundo paso(N), el porcentaje de la capacidad total de cómputo que necesitaría el atacante (en el eje de ordenadas) y el número de monedas que debería poseer (en el eje de abscisas).

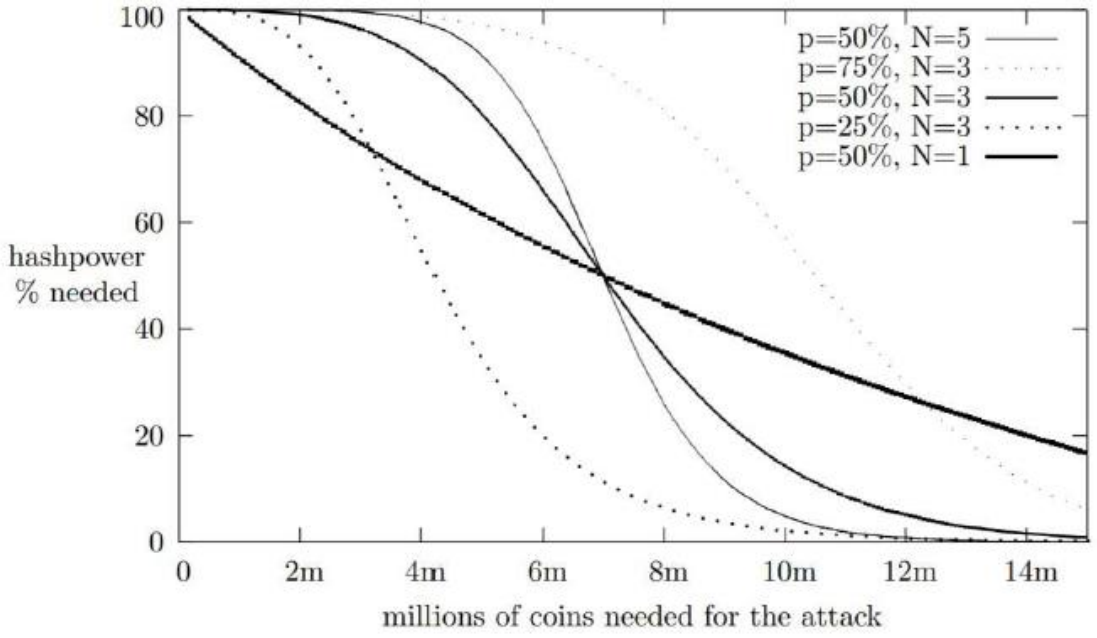


Figura 3.17 Relación entre monedas y potencia de hash para un ataque.

Actualmente únicamente la moneda Decred utiliza este mecanismo.

● **Proof-of-elapsed-time.** Se trata de una variedad de los mecanismos proof-of-work que busca reducir el consumo de electricidad.

La elección del nodo que generará el siguiente bloque se realiza mediante la ejecución de un código en un tipo especial de entorno controlado (Trusted Execution Environment) que garantiza que el tiempo de ejecución no depende de la potencia del procesador. De esta forma, se intenta que cada CPU tenga las mismas opciones de minar nuevos bloques.

La principal crítica a la seguridad de este tipo de consenso es el hecho de que actualmente únicamente un fabricante de microprocesadores (Intel) produce CPUs compatibles con este algoritmo, lo que genera dudas sobre la capacidad de este fabricante para alterar el funcionamiento del algoritmo. Esto hace que no sea muy atractivo para la implementación de blockchains públicas.

● **Proof-of-capacity/Proof-of-space.** Este tipo de mecanismos de consenso son otra variedad de proof-of-work, pero en lugar de requerir capacidad de cómputo elevada, los nodos mineros obtienen ventaja de tener mayor espacio en disco.

En cuestión de seguridad, no hay diferencias reseñables con proof-of-work. La ventaja principal es que, al no ser necesario disponer de hardware específico para minar bloques, el riesgo de centralización es menor.

La criptomoneda burstcoin implementa este mecanismo.

● **Byzantine Fault Tolerance (BFT).** En general, los algoritmos de consenso BFT empleados por los proyectos de criptomonedas permiten a los validadores gestionar el estado de una cadena y compartir mensajes entre sí para llegar al registro de transacciones correcto y asegurar la honestidad.

El BFT es implementado principalmente por Ripple (donde los validadores son preseleccionados por la fundación Ripple) y Stellar (donde cualquiera puede ser validador y la confianza es establecida por la comunidad).

Unas de las ventajas del BFT es que permite la escalabilidad y las comisiones de las transacciones son muy bajas.

● **Decentralized acyclic graphs (DAGs).** Como algoritmo de consenso emergente, DAG están recibiendo actualmente mucha atención y presentan una solución prometedora para la escalabilidad.

Es una forma de consenso que en realidad no usa la estructura de datos blockchain y maneja las transacciones de forma asincrónica. Un gran beneficio de este tipo de consenso es que (teóricamente) pueden tener un número infinito de transacciones por segundo (Figura 3.18). A pesar de eso, los DAG, como todos los demás algoritmos de consenso aquí, tienen sus fortalezas y debilidades.

DAG es una estructura de datos de gráficos dirigidos que utiliza un orden topológico. La secuencia solo puede ir de más temprano a más tarde. DAG a menudo se aplica a problemas relacionados con el procesamiento de datos, la programación, la mejor ruta de navegación y la compresión de datos.

La primera comunidad que tuvo la idea de cambiar la estructura de almacenamiento tipo cadena en un DAG de bloques fue NXT . Si el tiempo de

minería no cambia, el almacenamiento podría extenderse X veces con X bloques en la red al mismo tiempo.

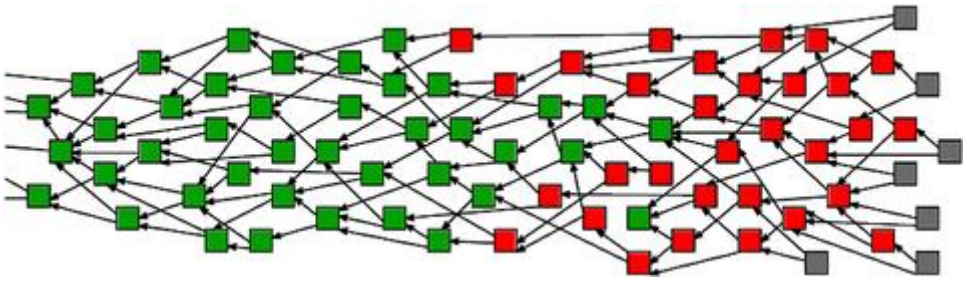


Figura 3.18 Estructura de bloque de DAG.

La combinación blockchain con DAG aún proviene de la idea de cadenas laterales. Diferentes tipos de transacciones se ejecutan en diferentes cadenas simultáneamente. DAG de bloques todavía se basa en el concepto de bloques.

Pero, la pregunta sería el por qué necesitamos un bloque. En la red bitcoin, muchas transacciones se extraen en bloques y la secuencia de transacción se mantiene mediante los pre-ajustes entre bloques. ¿Qué sucede si combina bloques y transacciones juntos? Haga que cada transacción participe directamente en el mantenimiento de las secuencias. Después de realizar la transacción, puede omitir el proceso de minería. Esto lo hace sin bloque y más eficiente.

4. Evolución de la Blockchain

4.1. Introducción.

Como se ha visto, la llegada de Bitcoin introdujo un nuevo concepto que sirvió de base para construir un sistema monetario digital que ha traído consigo nuevos modelos económicos. Debido al gran potencial que posee, la blockchain ha sido analizada con el objetivo de extender los beneficios que esta tecnología puede proporcionar.

A raíz de dicho análisis, y dado que el diseño de la estructura desarrollada para Bitcoin es extremadamente extensible, surge lo que se conoce como Blockchain 2.0, una segunda versión del concepto de cadena de bloques. Blockchain 2.0 es la evolución de la cadena de bloques diseñada para Bitcoin.

4.2. Blockchain 2.0

En las comunicaciones realizada por Satoshi Nakamoto en 2009 con la especificación de Bitcoin, se comentaba lo siguiente:

"…el diseño soporta una gran variedad de posibles tipos de transacción que diseñé hace años. Transacciones de fideicomisos, contratos, arbitrajes de terceras partes, firmas de varias entidades, etc. Esto son cosas que habrá que explorar con Bitcoin en el futuro, pero deberán estar diseñadas desde el principio para asegurarse que será posible hacerlas..."

Estas palabras de Satoshi Nakamoto en 2009 suponían el preludio a lo que conocemos como Blockchain 2.0. Si se parte de la base que Blockchain 1.0 está pensado para las transacciones económicas y pagos básicamente, se puede pensar que Blockchain 2.0 (Figura 4.1) está pensado para la gestión y transferencia de activos y cualquier otro tipo de bien que pueda estar en un registro público.
Igualmente se puede utilizar para gestión y transferencia de activos físicos siempre que los mismos puedan ser codificados de alguna manera.

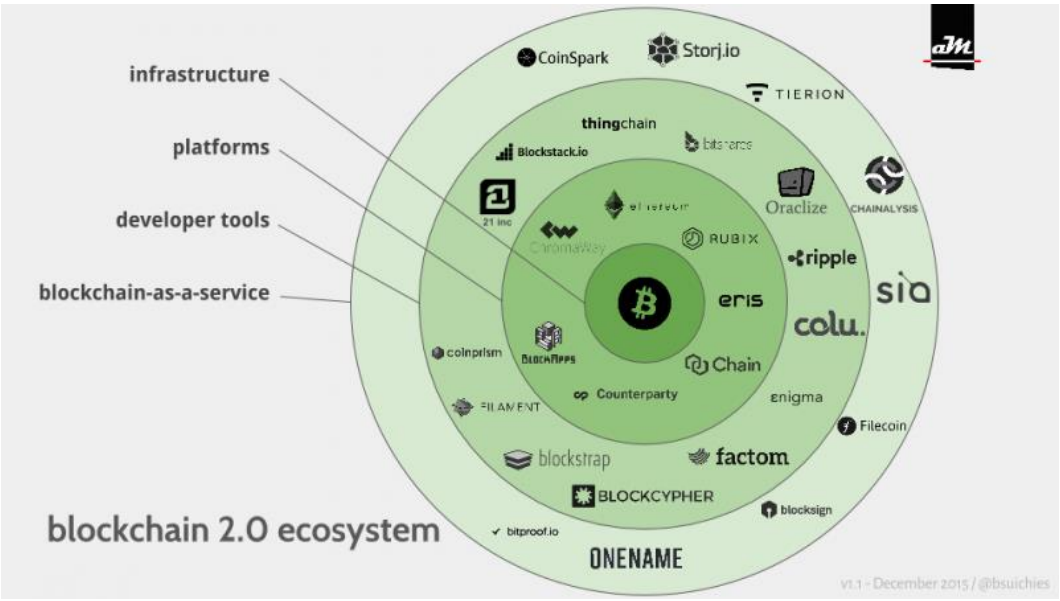


Figura 4.1 Elementos de la Blockchain 2.0

Blockchain 2.0 supone el paso de las criptomonedas al mundo de las aplicaciones reales. La base del blockchain 2.0 son los Smart Contract o contratos inteligentes que se encargan de ejecutar de forma automática acciones programadas sobre el blockchain que se ejecutan.

4.3. Smart Contract

Un contrato inteligente es un programa informático que ejecuta acuerdos establecidos entre dos o más partes haciendo que ciertas acciones sucedan como resultado de que se cumplan una serie de condiciones específicas. Es decir, cuando se da una condición programada con anterioridad, el contrato inteligente ejecuta automáticamente la cláusula correspondiente.

Los smart contracts llevan desarrollándose desde 1993, cuando el famoso criptógrafo Nick Szabo acuñó el término por primera vez. Nick propuso este sistema de contratos por aquel entonces, sin embargo la infraestructura tecnológica del momento lo hacía inviable.

Era necesario un sistema de pagos que los pudiese llevar a la práctica y esa situación no apareció en escena hasta la creación del Bitcoin en el año 2009. No obstante, Bitcoin no estaba pensado para nada más que ser una herramienta financiera, una criptomoneda. Por el contrario, la tecnología con la que funcionaba, el blockchain, sí que hacía posible estos contratos inteligentes

y fue a principios de 2014, con la creación de Ethereum, cuando, por fin, pasaron a ser una realidad.

Antes de nada, aclarar que aunque los smart contracts se han convertido en una seña de identidad de Ethereum (Figura 4.2), no son exclusivos de este blockchain. Otras blockchain que permiten la ejecución de estos contratos son BitHalo(https://bithalo.org/), Codius (https://codius.org/), Counterparty (http://counterparty.io/) o RootStock (http://www.rootstock.io/).

Figura 4.2 SmartContract de Ethereum.

Lo mejor para entender el concepto de un smart contract en Ethereum es hacer una analogía con una máquina de bebidas. Cuando se introduce una moneda en la máquina por el valor de una bebida, la maquina ejecuta un código de forma inexorable que acaba finalmente con la provisión de la bebida. En el caso de esta máquina, si no se deposita el precio de la bebida no se dispara el evento que hace que se pueda tener acceso a la misma. En caso de que se deposite la cantidad necesaria, la provisión de la bebida de realiza de forma automática. No hay intervención humana, no hay dialogo posible, no hay precio negociable. Si se cumplen las condiciones la bebida se obtendrá, si no se cumplen es sencillamente imposible.

La idea de un smart contract es que son aplicaciones programables que permiten la ejecución automática de tareas utilizando el blockchain de

Ethereum. Estos contratos se ponen en marcha cuando se producen determinados eventos y utilizan el blockchain de Ethereum como la fuente de datos para realizar las transacciones para las que están programados. Los smart contracts de Ethereum se pueden realizar en varios lenguajes y compilarse posteriormente para la máquina virtual de Ethereum (EVM – Ethereum Virtual Machine) antes de ser depositados en la blockchain.

Ethereum utiliza un mecanismo denominada gas para limitar el tiempo de ejecución de estos contratos. Cada contrato debe pagar una cierta cantidad de gas por su computación. A mayor tiempo de computación mayor gas tendrá que emplear. Hay que considerar que la ejecución de contratos en Ethereum es cara ya que debe ser ejecutada en cada nodo completo de Ethereum. La idea tras el gas es limitar la posibilidad de loops infinitos en contratos que hicieran caer la EVM. Un gas es equivalente aproximadamente a 0,00001 ether y permite la ejecución de una línea de código o un comando. Cuantas más líneas de código tenga un contrato más cara será su ejecución y por tanto más gas habrá que pagar por cada ejecución. Por ejemplo, si A quiere enviar 1 ether a B, en realidad A tendrá que enviar 1,00001 ether para hacer posible la transacción ya que el coste de transferir ethers es de 1 gas al tratarse de una operación muy simple de un solo comando. Hay contratos en Ethereum que precisan de cientos o miles de gas para poder ejecutarse. Si A quiere ejecutar un contrato en Ethereum que está asociado a una dirección B y no incluye el suficiente gas en las transferencia, esta no se realizara y por tanto no se hará efectiva la acción del contrato.

A nivel de Ethereum un contrato queda vinculado a una dirección del blockchain una vez que son compilados y enviados. Cuando se produce cualquier evento que este contemplado en el contrato, se enviará la transacción correspondiente a la dirección y la EVM de Ethereum ejecutará la programación asociada a dicho contrato utilizando los datos que hayan sido enviados.

Los contratos pueden ser tan simples y tan complejos como lo determine su programación (Figura 4.3). La única diferencia sustancial es que los contratos más complejos requieren más gas para su realización.

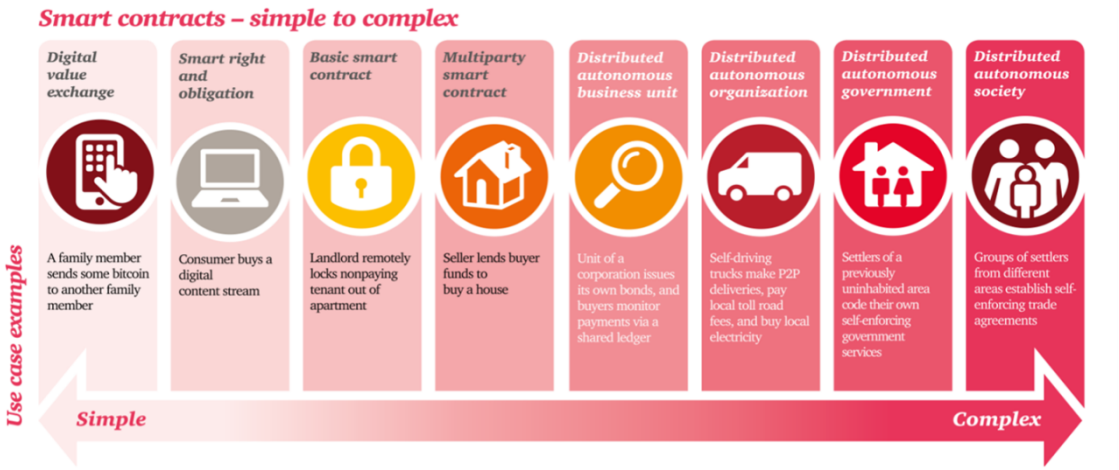


Figura 4.3 Complejidad de los SmartContract.

En principio cualquier tipo de operación que pueda ser vinculada a la automatización permite un contrato: votos, apuestas, compras digitales, préstamos, etc.

4.4. Beneficios de los Smart Contract

Después de haber definido qué son, se describirá los beneficios que tienen:

- **Autonomía**

  Estos contratos se dan siempre entre una o varias personas o entes legales, pero sin ningún intermediario. No es necesario alguien que valide el contrato, como podría ser un abogado. Por ello reducen, e incluso pueden llegar a eliminar cualquier persona extra que no esté implicada en el contrato.

- **Costes**

  Al ser contratos en los que no se depende de un tercero, se reducen los costes. Menos intervención humana resulta en costes reducidos.

- **Confianza**

  Todos los contratos inteligentes van directos a la cadena de bloques. Esto hace que: 1) esté encriptado, por lo que solo las personas implicadas pueden leerlo, y 2) permite la interacción entre personas que no se conocen entre sí sin que haya riesgo de estafa.

● **Velocidad**

Los contratos inteligentes utilizan código de software para automatizar las tareas que de otro modo se realizarían por medios manuales. Por lo tanto, aumentan la velocidad de los procesos de negocio y son menos propensos a errores manuales.

● **Seguridad**

Al basarse estos contratos inteligentes en la cadena de bloques pública de Ethereum no se pueden perder. Todo queda registrado de forma inmutable. Nada ni nadie lo pueden hacer desaparecer y siempre se tiene acceso a ellos.

El proceso de ejecución descentralizado elimina el riesgo de manipulación, ya que la ejecución es gestionada automáticamente por toda la red, en lugar de por una parte individual.

● **Nuevos modelos de negocio**

Los contratos inteligentes, a través de sus bajos costos para asegurar transacciones confiables, permiten nuevos tipos de negocios como el acceso automatizado a vehículos y unidades de almacenamiento.

Esto puede abrir nuevas vías de emprendimiento si lo juntamos con otras tendencias emergentes como el Internet de las cosas (IoT).

4.5. Usos de los Smart Contract.

A continuación, se presenta algunos de los posibles usos que se le podrían dar:

● **Servicios financieros:**

- Préstamos: si la persona que contrata el préstamo no realiza el pago en el tiempo estipulado, se ejecutaría el contrato para retirarle las garantías.

- Liquidación de operaciones: los contratos calculan importes de liquidación y transfiere fondos automáticamente.

- Pagos de cupones y bonos: los contratos calculan y pagan automáticamente de forma periódica los cupones y devuelve el capital al vencimiento de los bonos.

- Microseguros: Calculan y transfieren micropagos basados en datos de uso de un dispositivo conectado a Internet (por ejemplo, un seguro automotriz de pago por uso)

- Depósito en garantía en el registro de la propiedad: el contrato supervisa la información externa a la cadena de bloques y una vez transferida la propiedad de un vendedor a un comprador, el contrato ingresa automáticamente los fondos al vendedor.

- Herencias: una vez que el contrato puede verificar el fallecimiento de la persona, automáticamente las propiedades quedan repartidas y asignadas entre los herederos.

- Automatización de pagos y donaciones: se pueden acordar pagos o donaciones periódicas o puntuales a personas o entidades. El contrato inteligente lo que haría es verificar que se cumplen las reglas para realizar automáticamente la donación.

● **Servicios de la salud**

- Expedientes médicos electrónicos: los contratos proporcionan transferencias y accesos a los historiales médicos tras la aprobación de múltiples firmas entre pacientes y proveedores.

- Acceso a los datos sanitarios de la población: se conceden a las organizaciones de investigaciones sanitarias el acceso a determinada información sanitaria personal. A cambio, a través de los contratos, se realizan micropagos automáticamente al paciente para su participación.

- Seguimiento de la salud personal: se realiza un seguimiento de las acciones relacionadas con la salud de los pacientes a través de dispositivos IoT -Internet of Things- (conectados a Internet). Los contratos generan automáticamente recompensas basadas en hechos específicos.

● **Servicios de propiedad intelectual**

- Distribución de royalties: el smart contract calcula y distribuye los pagos de royalties a artistas y otras partes asociadas según los términos acordados.

● **Servicios energéticos**

- Estaciones autónomas de recarga para vehículos eléctricos: el contrato procesa un depósito, habilita la estación de recarga y devuelve los fondos restantes una vez completados.

● **Servicios del sector público**

- Votación: valida los criterios del votante, registra el voto en la cadena de bloques e inicia acciones específicas como resultado del voto mayoritario. Esto es posible en una votación tanto a nivel de encuesta como a nivel estatal.

- Apuestas: dos o más partes pueden apostar sin que se resienta su seguridad y sin necesidad de un tercero a través de un contrato inteligente que asegure unas condiciones concretas.

- Propiedades inteligentes: una casa, un coche, una nevera, una lavadora…todos los objetos que se puedan conectar a Internet se consideran propiedades inteligentes (del inglés, *smart property*). Y todos pueden ser gestionados con contratos inteligentes para poder venderlos o alquilarlos de forma automatizada.

4.6. Blockchain 3.0

En los capítulos anteriores se hablaba de blockchain 1.0 como un nuevo sistema eficaz y válido para el intercambio financiero sin intermediarios y de blockchain 2.0 como un nuevo sistema para el desarrollo de contratos inteligentes y el desarrollo de mercados con aplicaciones similares a las que tenemos en la actualidad en los mercados digitales pero utilizando la potencia del blockchain.

En el caso del 3.0 (Figura 4.4) el reto tiene que ver con el desarrollo de nuevas tecnologías basadas en la identidad, la libertad, la democracia y la contabilidad de activos de cualquier tipo. Blockchain 3.0 tratará de solucionar las restricciones que actualmente existen en los mercados a nivel local, regulatorio y de entornos macroeconómicos. Es decir, mientras que blockchain 2.0 está tratando de migrar aplicaciones del mundo digital utilizando la trazabilidad y posibilidades de contabilidad en mercados masivos, blockchain 3.0 va a tratar de cambiar el status quo establecido utilizando la potencia, la deslocalización y la ubiquidad que generan las tecnologías blockchain.

No se trata de reinventar aplicaciones de mercado ya existentes, se trata de cambiar el mercado y de generar nuevos modelos de contabilidad y trazabilidad sobre activos de cualquier tipo desconocidos hasta el momento.

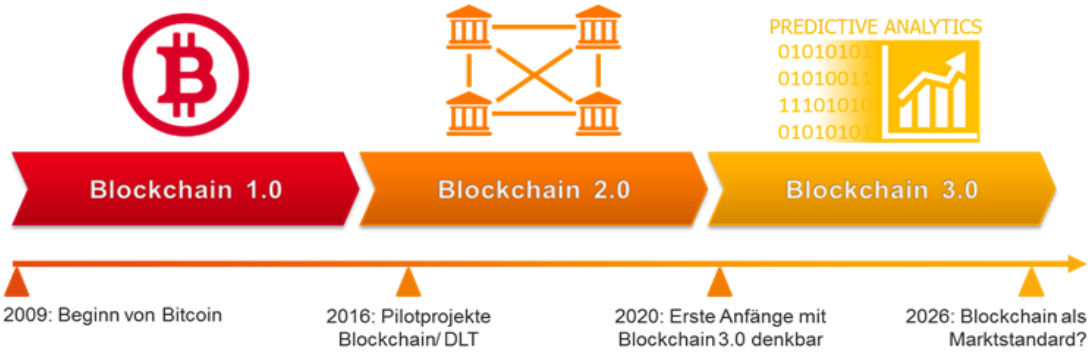


Figura 4.4 Evolución de la Blockchain.

Si se puede hablar de blockchain 2.0 como una evolución, en el caso de blockchain 3.0 se debe hablar de revolución. Esta revolución está por llegar, es algo que se va a ir produciendo en los próximos años, pero cuyas bases se están asentando en la actualidad.

Hará falta bastante trabajo adicional para tener estos sistemas transaccionales completamente listos y en funcionamiento, no se ha hecho más que empezar. Las herramientas están parcialmente preparadas pero aún hacen falta bastantes elementos que en la mayoría de los casos tienen que ver con la interfaz de los activos del mundo real o digital y con la capacidad de trazabilidad y contabilidad que posee blockchain.

Adicionalmente existe un problema de conocimiento general sobre estas tecnologías que se irán introduciendo en los próximos años. Las empresas TIC que se tendrán que encargar de desarrollar la base tecnológica del blockchain 3.0 no están todavía preparadas completamente y las empresas y organizaciones que se beneficiarán de la aplicación de las mismas están aún identificando las estrategias necesarias para ponerlo en marcha.

5. Conclusiones

Las conclusiones a las que se ha llegado con la realización de este TFM, son el conocimiento de la tecnología que hace realidad la primera criptomoneda creada, como es el Bitcoin. Las ventajas y desventajas de su utilización, la manera en la que crea valor, las otras criptomonedas surgidas a raíz de la aparición de esta, así como el uso de la criptografía como elemento fundamental para el surgimiento del Bitcoin.

Al mismo tiempo se ha tratado la base que la sustenta y la hace posible, como es la cadena de bloques para Bitcoin, y desde ahí a la evolución de la bockchain hacía otros tipos de usos en otros tipos de campos, que son el presente y será el futuro de la blockchain.

En cuanto a los objetivos planeados, centrados en el conocimiento de los fundamentos del Bitcoin y Blockchain, pienso que en este TFM han sido cubiertos de una forma detallada, sin entrar en explicaciones altamente especializadas que dificulte su comprensión.

Respecto a la planificación, del primer diagrama de Gantt, al último presentado en este TFM, ha habido modificaciones según iba tomando forma el trabajo, tanto en tiempos de realización de tareas como en su contenido, ya sea por considerar unos temas más importantes que otros, o por la propia organización del contenido.

Como trabajo futuro, me hubiera gustado profundizar más en el futuro de la blockchain (Blockchain 2.0, Smartcontract, Blockchain 3.0), pero pienso que no era el objetivo principal de este TFM, por lo que su tratamiento ha sido meramente descriptivo.

6. Glosario

- **Altcoin**: una criptomoneda con un funcionamiento muy parecido al de Bitcoin pero con algunas diferencias, como la capacidad de procesar transacciones más rápido.

- **Bloque**: Conjunto de transacciones de bitcoins agrupadas para ser verificadas y unirlas a la cadena de bloques.

- **Bloque génesis**: Nombre que recibe el primer bloque de la cadena de bloques.

- **BTC**: Es el símbolo del bitcoin.

- **Cadena de bloques**: Es un registro histórico de todas las transacciones válidas de Bitcoin realizadas y, de manera cronológica y pública, la podemos considerar como la contabilidad de la red Bitcoin.

- **Clave privada**: Es un número secreto que permite gastar los bitcoins. Cada dirección Bitcoin tiene asociada una clave privada. La clave privada está relacionada matemáticamente con la dirección Bitcoin, de tal modo que la dirección Bitcoin se deriva de la clave privada siguiendo unas reglas fijas, mientras que la operación inversa, deducir una clave privada a partir de la dirección Bitcoin, es imposible.

- **Clave pública**: Un texto alfanumérico del cual se obtiene trivialmente una dirección y que es conocido por todos. Al ser conocido por todos, cualquiera puede enviarle bitcoins a la dirección asociada. Pero solo quien tenga la clave privada asociada podrá disponer de ellos. La clave pública es generada fácilmente a partir de la clave privada.

- **Comisión**: Una pequeña suma de bitcoins que se entrega al minero que resuelve el bloque como recompensa

- **Confirmación**: Es el hecho de resolver un bloque e incluirlo en la cadena de bloques, estableciendo así la validez de las transacciones incluidas en él y afianzando más aún la confianza de los bloques anteriores.

- **Contrato inteligente**: un programa informático almacenado en una cadena de bloques que, si se cumplen las condiciones codificadas en el programa, mueve de manera automática los activos digitales entre las cuentas. Sirve

como una forma de crear una promesa matemáticamente garantizada entre dos partes.

• **Criptomoneda**: Monedas digitales que funcionan en redes descentralizadas, donde las partes actúan directamente entre sí. El bitcoin es la más conocida de estas monedas, pero no la única.

• **Criptografía**: Utilización de las matemáticas para crear mensajes de forma tal que solo el destinatario pueda comprender su significado. Si un tercero interceptara el mensaje, no podría comprenderlo.

• **Descentralización**: una medida difícil de cuantificar de la resistencia de una red frente a ataques. Se mide en función de la distribución del control de la cadena de bloques entre sus distintos usuarios, una función de qué tan amplio se distribuye el control entre los diferentes actores

• **Dificultad**: Número que determina cuántos hashes en promedio se necesitan crear hasta encontrar aquel que resuelve el bloque. La propia red ajusta la dificultad para asegurar que en promedio se resuelva 1 bloque cada 10 minutos, de manera si más gente pone su ordenador a buscar Bitcoins esa dificultad se ajusta automáticamente para mantener esa velocidad.

• **Dirección**: Es un identificador que tiene entre 27 y 34 caracteres alfanuméricos, comenzando por el número 1 o el 3, que representa un destino de Bitcoins, es decir, se utiliza para enviar y recibir Bitcoins.

• **Doble gasto**: Se refiere al acto de realizar dos pagos con una misma moneda. Supone una operación fraudulenta y, aunque no resulta fácil de hacer en la red Bitcoin, se ha de tratar de evitar no aceptando el pago hasta que se lleve a cabo un mínimo de confirmaciones, que suelen ser entre tres y seis

• **ETHER (Éter):** Es el token nativo de la cadena de bloques de Ethereum, que se utiliza para pagar tarifas de transacción, recompensas de mineros y otros servicios en la red.

• **Ethereum:** Plataforma descentralizada desprendida desde la red de Bitcoin y que permite la ejecución de contratos inteligentes. Su criptomoneda (ether) es una de las más populares y de mayor capitalización del mercado.

• **Firma digital**: Proceso matemático que comprueba la autenticidad del remitente de un mensaje de forma tal que el receptor puede verificar que el mensaje fue escrito por este y por nadie más, y que el éste no fue alterado o modificado por otra persona.

- **Fork (bifurcación)**: es una versión de la cadena de bloques alternativa a la actual. Se puede obtener de forma maliciosa si un minero obtiene demasiado poder de cómputo, de forma accidental en caso de un error en el sistema, o de forma intencional si se introduce una modificación del protocolo. Para que un fork tenga éxito es necesario que cuente con el apoyo de suficientes mineros como para obtener la cadena más larga dentro de la cadena de bloques

- **GAS**: Precio interno para ejecutar una transacción o contrato en Ethereum. Se usa para desacoplar la unidad ether (ETH) y su valor de mercado de la unidad para medir el uso computacional (gas).

- **Hash**: Un hash de un objeto es el equivalente de nuestra huella dactilar. Es una identificación única y constante. Dos objetos distintos tienen (teóricamente) hashes distintos. Además, tiene la peculiaridad de que, si tienes el objeto es muy fácil obtener su hash. Sin embargo, si tienes el hash es extremadamente difícil obtener el objeto original del que proviene. En el caso de Bitcoin, el algoritmo es SHA256.

- **Input (entrada)**: se refiere al origen de una transacción. Suele tratarse de la dirección perteneciente al emisor del pago, excepto en el caso de una transacción por recompensa a la minería.

- **Minería**: Resolución de un bloque, certificando todas las transacciones que contiene. A cambio, el minero recibe una recompensa en Bitcoins nuevos Bitcoins. De esta forma se generan nuevas monedas en la red.

- **Minero**: se conoce con este nombre a quienes realizan la minería.

- **Monedero/Wallet**: Programa que guarda los Bitcoins que una persona posee y permite transferir y recibir Bitcoins sin intermediarios mediante las claves privadas, es más o menos como un monedero físico pero en la red Bitcoin. El monedero puede utilizarse online o se puede descargar mediante una aplicación y se queda guardado en el propio ordenador.

- **Nodo**: es un ordenador conectado a la red Bitcoin que transmite transacciones a otros

- **Nonce**: Un número que se añade al hash del bloque anterior para intentar resolverlo. Si el hash encontrado no resuelve el bloque, se incrementa el nonce y se vuelve a intentarlo.

- **Output (salida)**: es el destino de una transacción. Lo más habitual es que se trate de una dirección, pero también puede haber transacciones con más de una dirección de destino y, por tanto, varias salidas.

- **P2P**: hace referencia a una red peer-to-peer, es decir, una red descentralizada donde todas las partes interactúan entre sí.

- **Pool de minería**: Es la agrupación de un conjunto de mineros que se unen para generar hashes de manera más rápida y así aumentar la probabilidad de resolver el bloque y obtener la recompensa, la cual se divide de forma proporcional entre los mineros.

- **Prueba de trabajo**: el protocolo de consenso que utiliza Bitcoin y muchas otras criptomonedas. Para agregar un nuevo bloque, los mineros deben calcular un *hash* que cumpla ciertos criterios. Este cálculo consume mucha energía y tiempo, ya que para llegar a él hay que hacer un montón de conjeturas aleatorias, lo que disuade los intentos de fraude.

- **Satoshi Nakamoto**: Es el pseudónimo de la persona o grupo de personas que inventaron el Bitcoin. Nadie conoce su verdadera identidad.

- **Volatilidad**: La medida en que fluctúa una divisa a lo largo del tiempo.

7. Bibliografía

[1] Dominando Bitcoin. https://es.scribd.com/doc/298016780/Dominando-Bitcoin-Andreas-Antonopoulos

[2] Bitcoin: “Una moneda criptogràfica”. https://es.scribd.com/document/217063215/Int-Bitcoin

[3] Bitcoin: “La moneda del futuro”. https://es.scribd.com/doc/149481323/Bitcoin-La-Moneda-Del-Futuro-Que-Es-Bitcoin-en-Espanol

[4] El Bitcoin. https://es.scribd.com/search?content_type=tops&page=1&query=228562817

[5] Bitcoin, revolución monetaria. https://es.scribd.com/document/290817011/BITCOIN-REVOLUCION-MONETARIA

[6] Características criptográficas y potenciales debilidades de la criptodivisa Bitcoin. https://es.scribd.com/document/370120459/350862552-Tesis-de-Fernandez-sobre-criptomonedas-pdf

[7] Bitcoin, ¿la moneda del futuro? http://ruc.udc.es/dspace/bitstream/handle/2183/18055/MechebaMolongua_Jessica_TFG_2016.pdf?sequence=2

[8] Documentos electrónicos para el intercambio de bienes y servicios https://gredos.usal.es/jspui/bitstream/10366/130135/1/TFG_InfyDoc_GarciaAlejo_LuisAntonio_SI_85_2015-2016.pdf

[9] La nueva moneda virtual que esta revolucionando el mundo de las divisas digitales. http://repositori.uji.es/xmlui/bitstream/handle/10234/112560/TFM_2014_AsensioGrauY.pdf?sequence=1

[10] Estudio de la red Bitcoin. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/23341/6/acisneroscTFM0613memoria.pdf

[11] Bitcoin, Oro electrónico. http://dspace.umh.es/bitstream/11000/3689/1/ALMARCHA%20NAVIDAD%20CARLOS.pdf

[12] Criptodivisas y pagos online. https://repositorio.unican.es/xmlui/bitstream/handle/10902/10715/CUARTASMICIECESJAVIERA.pdf?sequence=1

[13] El Bitcoin, ¿Presente y futuro del dinero? https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/4523/TFG001313.pdf?sequence=1

[14] Blockchain y su aplicación a una industria bajo regulación. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64766/6/aisasaTFM0617memoria.pdf

[15] ¿Qué es Bitcoin? ¿Cómo funciona? ¿Dónde se compran?

https://computerhoy.com/noticias/internet/que-es-bitcoin-como-funciona-donde-compran-5389
[16] ¿Qué es el bitcoin? ¿Es seguro invertir en bitcoins? 10 claves https://www.elperiodico.com/es/economia/20171203/bitcoin-que-es-6467132
[17] Invertir en bitcoins: lo que debes saber. https://www.finect.com/blogs/aprendiendo-sobre-inversiones/articulos/invertir-bitcoins-debes
[18] Encuentre respuestas a mitos y preguntas comunes sobre Bitcoin. https://bitcoin.org/es/faq#como-se-compran-bitcoins
[19] La blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptives. http://www.minetad.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/DOLADER,%20BEL%20Y%20MU%C3%91OZ.pdf
[20] BLOCKCHAIN: La revolución industrial de internet. https://static0planetadelibroscom.cdnstatics.com/libros_contenido_extra/36/35615_Blockchain.pdf
[21] Bitcoin 101: Fundamentos técnicos. https://estacioninformatica.blogspot.com.es/2017/04/bitcoin-101-fundamentos-tecnicos.html
[22] Diseño e implementación de una plataforma para la gestión de transacciones comerciales usando moneda virtual. http://oa.upm.es/42913/1/PFC_ALVARO_RODRIGUEZ_VILLALBA_2016.pdf
[23] Estudio de la utilización de protocolos blockchain en sistemas de votación electrónica. https://upcommons.upc.edu/bitstream/handle/2117/98545/PFC%20Blockchain_Evoting_v01.pdf
[24] Prueba de Trabajo (PoW), Explicado. https://es.cointelegraph.com/explained/proof-of-work-explained
[25] Consenso. http://libroblockchain.com/consenso/
[26] ¿Qué es Bitcoin?: El Protocolo de Consenso Distribuido. https://medium.com/@coinest.co/bitcoin-101-el-protocolo-de-consenso-distribuido-211800161cbd
[27] Los diferentes tipos de consenso del Blockchain. https://www.karlbooklover.com/consensos-del-blockchain/
[28] Consenso descentralizado o la salsa mágica de Bitcoin y Ethereum. http://www.eleconomista.es/firmas/noticias/8788708/12/17/Consenso-descentralizado-o-la-salsa-magica-de-Bitcoin-y-Ethereum.html
[29] Las 4 capas de la red Bitcoin: ¿Por qué es importante el consenso en algunos de los cambios y en otros no? https://www.oroyfinanzas.com/2016/03/4-capas-red-bitcoin-por-que-importante-consenso-cambios/
[30] Del PoW al BFT: ¿cuáles son los algoritmos para lograr el consenso? https://es.insider.pro/tutorials/2018-03-21/del-pow-al-bft-cuales-son-los-algoritmos-para-lograr-el-consenso/
[31] Explicando el gráfico acíclico dirigido (DAG), The Real Blockchain 3.0.

https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/#5d6e0ce0180b
[32] Blockchain y la Prueba de Trabajo –PoW– https://steemit.com/cryptocurrency/@juanfb/blockchain-y-la-prueba-de-trabajo-pow
[33] What are consensus algorithms in mining? https://cryptodaddyshop.com/blogs/news/what-consensus-algorithms-exist
[34] Estudio sobre Bitcoin y Tecnología Blockchain . https://www.researchgate.net/publication/321058652_Estudio_sobre_Bitcoin_y_Tecnologia_Blockchain
[35] Qué es blockchain: la explicación definitiva para la tecnología más de moda. https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda
[36] Blockchain: mirando más allá del Bitcoin. http://marketing.asobancaria.com/hubfs/Asobancaria%20Eventos/Asobancaria%20-%20Semanas-Economicas/1084.pdf
[37] La economía del Blockchain. http://trbc.es/wp-content/uploads/2017/10/La-economi%CC%81a-de-Blockchain.pdf
[38] El Blockchain y Sus Aplicaciones. https://sg.com.mx/revista/47/el-blockchain-y-sus-aplicaciones
[39] Blockchain: Economía de confianza https://miethereum.com/wp-content/uploads/2017/11/Blockchain-Economia-de-Confianza-Deloitte.pdf
[40] Blockchain 2.0. The Purpose of Blockchain https://medium.com/polys-blog/blockchain-2-0-the-purpose-of-blockchain-e84e5a95cdd9
[41] WHAT IS BLOCKCHAIN 3.0? https://the-blockchain-journal.com/2018/03/17/what-is-blockchain-3-0/
[42] ¿Para qué sirven los 'Smart Contracts'? https://ecija.com/wp-content/uploads/2017/03/Para-que-sirven-los-Smart-Contracts_.pdf
[43] SMART CONTRACTS O CONTRATOS INTELIGENTES https://miethereum.com/smart-contracts/
[44] Smart contracts: ¿el futuro de los negocios? http://www.agiliacenter.com/smart-contracts-futuro-negocios/