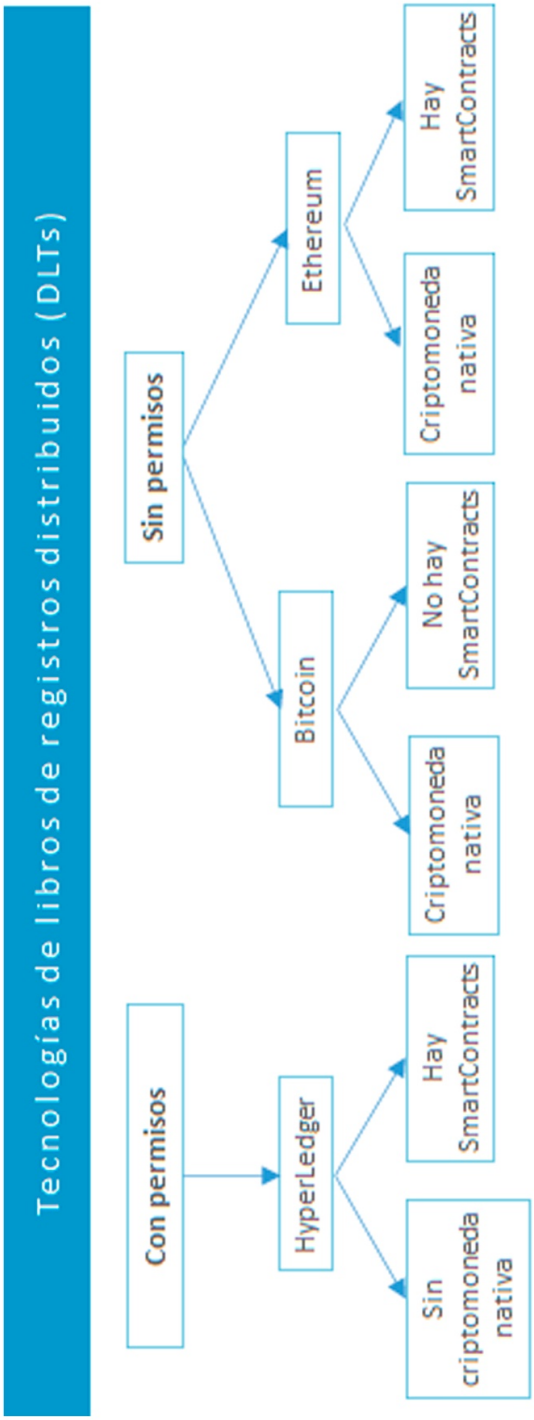
Tecnologías Emergentes

Tema 08. Blockchain

Índice

Esquema



8.1. ¿Cómo estudiar este tema?

Para estudiar este tema, nos basaremos en los siguientes conceptos:

- **La cadena de bloques o *Blockchain***, como elemento que hace posible la realización de transacciones sin intermediarios tradicionales.
- **Plataformas basadas en *Blockchain*:** se presentan criptomonedas reales como Bitcoin, Ethereum y sistemas como Hyperledger.
- **Los *Smart Contracts* o contratos inteligentes**: aplicaciones que se pueden ejecutar sobre una cadena de bloques y realmente se ocupan de realizar todas las transacciones incluidas en las condiciones de un contrato, programadas de manera autónoma para cuando se cumplan determinadas condiciones

8.2. Fundamentos de la cadena de bloques

La tecnología ***Blockchain*** o **cadena de bloques** hace posible incorporar a Internet algo de lo que ha carecido desde sus comienzos: la **confianza**.

Veamos algunos ejemplos: la confianza al traspasar un importe monetario para pagar a un restaurante sin involucrar comisiones bancarias, confianza para abrir automáticamente la puerta de un apartamento que acabamos de alquilar en Airbnb, o la confianza de poder votar electrónicamente en unas elecciones generales, sin que haya votaciones o manipulaciones fraudulentas, etc.

Prácticamente no existe ninguna industria actual para la que no se haya dicho que la aplicación de *blockchain* supondrá una revolución.

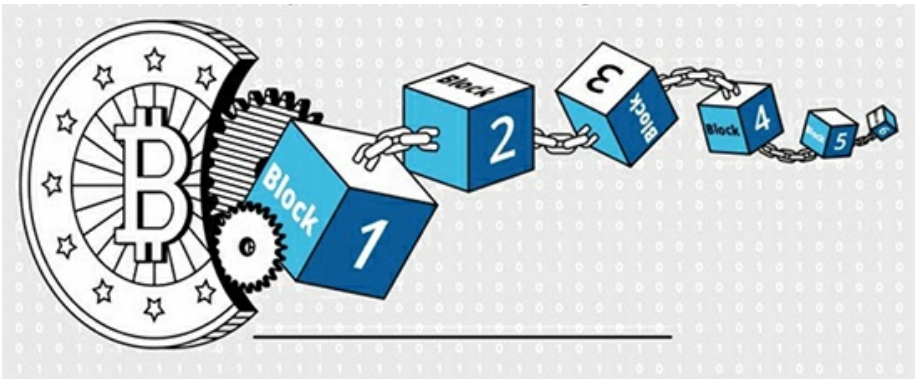


Figura 1. La criptomoneda Bitcoin se basa en la tecnología blockchain. Fuente: investopedia.com

Técnicamente, *blockchain* es un tipo **de libro de registro distribuido (DLT, *Distibuted Ledger Technology*)**. Explicándolo de forma sencilla, una cadena de bloques no es más que una lista. Cada registro de la lista, denominado bloque (que incluye una o más transacciones), está criptográficamente asegurado, y contiene un puntero *hash* que está enlazado de forma indestructible al bloque anterior de la cadena. No es posible alterar ningún bloque de la cadena sin que todos los bloques posteriores resulten alterados, por lo que es inútil intentar *hackear* un solo bloque.

Además, todos estos bloques no se almacenan en una inmensa base de datos centralizada en un servidor, sino que **se distribuyen en una red de nodos P2P**, lo que evita un punto único de *hackeo*. La cadena de bloques solo se puede actualizar mediante **consenso** entre todos los nodos. Existen numerosas copias diferentes de la cadena de bloques sin que exista una copia principal o privilegiada, ya que todas merecen la misma confianza. Si alguien intenta modificar una copia de la cadena, será inmediatamente rechazada por las demás.

Bitcoin es quizás el ejemplo más conocido del uso de una cadena de bloques. Ha logrado ser un sistema de pagos P2P que permite realizar transacciones económicas sin intermediarios (tradicionalmente, bancos o cámaras de compensación).

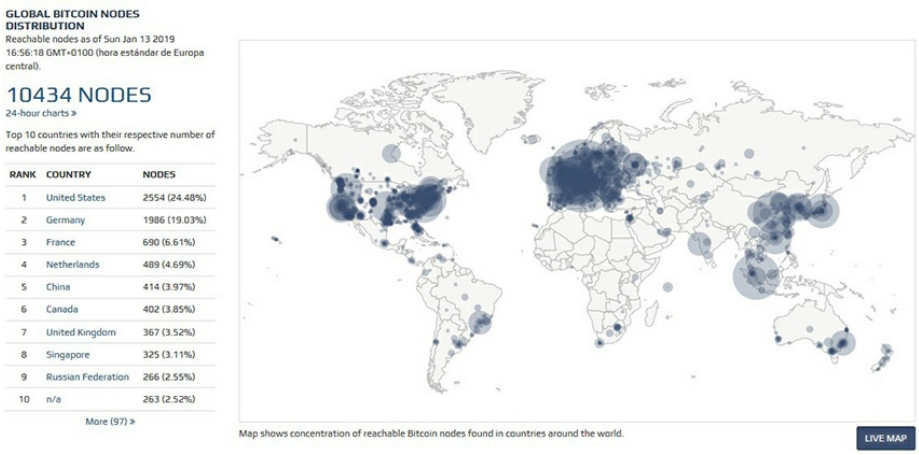


Figura 2. En enero de 2019 ya se alcanzaron 10434 nodos de soporte de Bitcoin. Fuente: bitnodes.com

Las transacciones de Bitcoins se registran en una cadena de bloques (registro o *ledger*) distribuida por todo Internet. Nadie es dueña de la misma y nadie la controla. Si un usuario tiene un monedero de Bitcoins en su PC, sería perfectamente posible que en su disco tuviera una copia completa de la cadena de bloques (actualmente ocupa casi 200GB, en enero de 2019) en su disco duro, con el registro de absolutamente todas las transacciones de Bitcoins realizadas hasta la fecha.

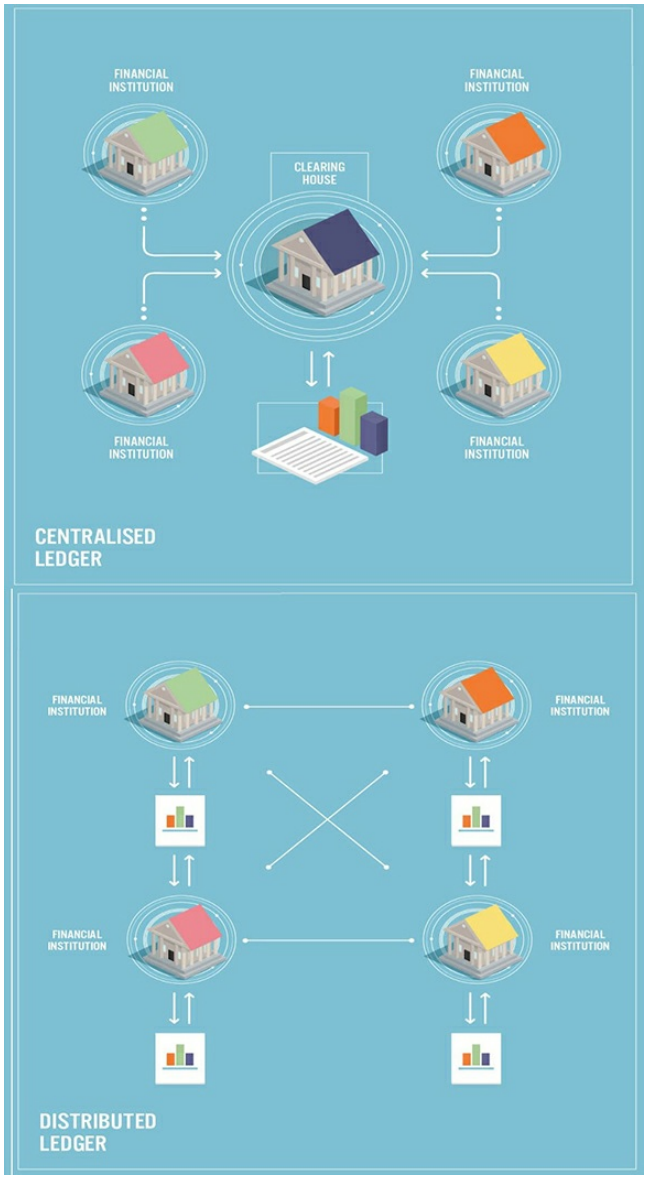


Figura 3. Libros de registro centralizados y distribuidos. Fuente: codeburst.com

Aparte de Bitcoin, han aparecido varias iniciativas nuevas basadas en cadenas de bloques. Las dos más importantes hasta la fecha son **Ethereum** e **Hyperledger**. Son diferentes tanto en los casos de uso como en su modelo de despliegue.

Hyperledger es la denominación paraguas de diversos proyectos gestionados por la Linux Foundation, e incluye varios proyectos basados en cadenas de bloques. Uno de los más importantes es **Hyperledger Fabric**, al que ha contribuido principalmente

IBM.

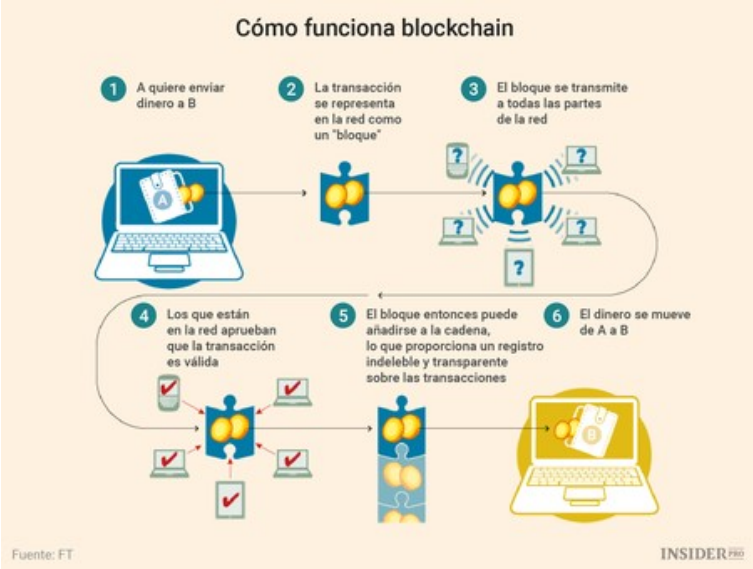


Figura 4. Funcionamiento general de Blockchain. Fuente: xataka.es

Tanto Bitcoin como Ethereum son **DLTs sin permisos**, lo que significa que un nodo puede unirse y abandonar las redes Bitcoin y Ethereum en cualquier momento. Al unirse a las redes, ayudan y contribuyen mejorando la robustez, y al abandonarlas, realmente no hacen apenas ningún daño. Hyperledger es un **DLT con permisos**: tanto el control de acceso como el uso de la cadena de bloques lo determinan el propietario o la organización.

Por otro lado, tanto Bitcoin como Ethereum disponen de una criptomoneda nativa. En el caso de Hyperledger, no la hay, y no por ello es menos útil. En despliegues corporativos o de consorcios, realmente no se necesitan monedas propias para los fondos asociados a las transacciones.

Figura 5. Cotización en euros de las criptomonedas. Fuente: coinbase.com

Finalmente, hay que señalar que solo Ethereum e Hyperledger disponen de la capacidad de usar **contratos inteligentes** (*Smart Contracts*), de los que nos ocuparemos a continuación.

Los contratos inteligentes **son aplicaciones** que se pueden ejecutar sobre una cadena de bloques. Realmente se ocupan de realizar transacciones incluidas en las condiciones de un contrato, programado de manera autónoma. Estos contratos inteligentes logran encapsular la lógica de negocio, y pasan a ejecutarse cuando se cumplen ciertas condiciones.

Ethereum se ha convertido en la plataforma por excelencia para el desarrollo de *smart contracts*, pues se dispone de un potente lenguaje de programación para crearlos, denominado **Solidity**. Se pueden crear desde combinaciones muy sencillas —como un contrato de apuesta con dos partes—, hasta relaciones mucho más complejas multiparte, similares a contratos societarios.

La cuestión relevante es si un *Smart Contract* puede ser calificado jurídicamente como un contrato o no. Muchos consideran que la parte «*smart*» está más allá del concepto jurídico de contrato. De hecho, no es que no sea un contrato, es que no

pretende serlo. Para estos, el *smart contract* es autosuficiente, no necesita ni demanda el apoyo de jurisdicción estatal alguna.

También se puede pensar que, de conformidad con nuestro derecho actual, una herramienta en la que se prescinde de la idea de obligarse uno jurídicamente en el marco de una determinada jurisdicción no sería un «contrato» y, por tanto, nunca podría buscar el apoyo del derecho del Estado. La propia lógica jurídica expulsaría al *smart contract* de su ámbito de actuación.

Un planteamiento intermedio entre ambos sería el siguiente: las partes de un *smart contract* quieren beneficiarse de las ventajas prácticas de este instrumento, pero no por ello han de renunciar a los remedios del derecho contractual tradicional si el mecanismo no llega a funcionar como habían previsto.

Fundamentos criptográficos aplicados en Blockchain

Nos centraremos ahora en conocer el funcionamiento de *Blockchain* y cómo se aplican los conceptos generales de criptografía de clave pública y privada.

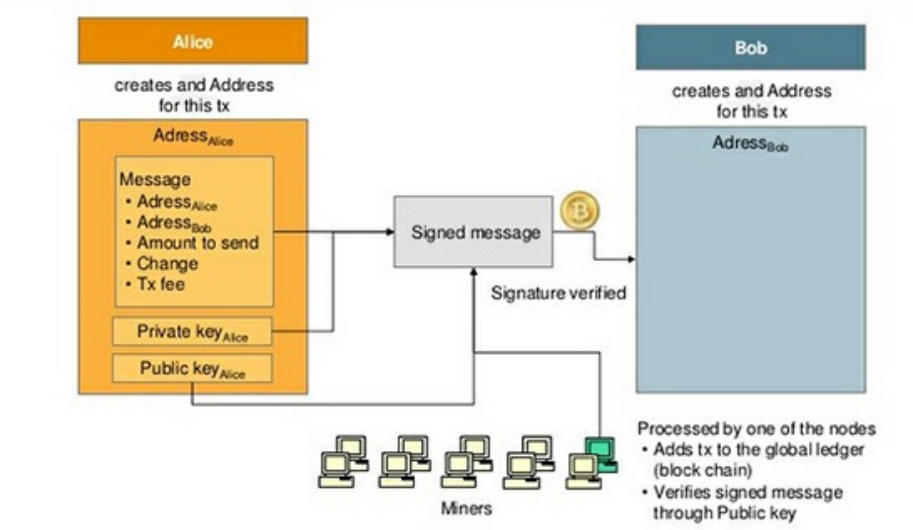


Figura 6. Transacción con Bitcoins. Fuente: bbc.co.uk

Para ello vamos a ver de qué manera se realiza una transacción con Bitcoins bajo el

esquema de clave pública.

Supongamos a modo de ejemplo el caso en el que Alicia quiere realizar una transacción de pago a Bernardo:

- Al igual que sucede en los sistemas de clave pública, el receptor (Bernardo) envía su clave pública al emisor (Alicia).
- Cuando Alicia realiza la transacción, incluye la clave pública de Bernardo (indicando el destinatario) y la cantidad de dinero a transferir.
- Alicia firma la transacción con su clave privada secreta. De esta forma declara que esa cantidad, que antes le pertenecía a ella, ahora le pertenece a Bernardo.
- La transacción de Alicia se difunde a todos los nodos a los que ella está conectada. Los nodos que reciben esta transacción validan las firmas criptográficas y el valor de la transacción antes de aceptarla y retransmitirla.
- Si la transacción es correcta, estos nodos a su vez transmitirán la transacción, de modo que se propaga de unos nodos a otros sucesivamente por toda la red. De esta forma, la moneda queda definida como una cadena de firmas digitales.
- En caso de que haya un error o intento de falsificación, la transacción no se transmitirá, de manera que son los propios usuarios los que aseguran el correcto funcionamiento de la red.

Una vez visto cómo Bitcoin utiliza el esquema de clave pública, se **comprende la importancia de que las claves públicas sean cortas**, para que el intercambio de claves públicas pueda hacerse de una forma ágil y puedan compartirse mediante códigos QR o por teléfono.

Pero, aparte de ser cortas es necesario que sean seguras. La criptografía de curva elíptica encaja perfectamente para la resolución de este problema, puesto que permite crear claves más cortas con el mismo nivel de seguridad. Se hace la

semejanza de que una clave de curva elíptica de 256 bits proporciona una seguridad equivalente a la de una clave RSA de 2048 bits.

Minería de Bitcoins

El término «minado» se utiliza como una metáfora que hace referencia a la minería del oro. Un **minero de Bitcoin** es una persona que ejecuta un programa en su ordenador y que ayuda a verificar las transacciones Bitcoin al incluirlas en un registro inalterable (la cadena de bloques). Por tanto, los mineros colaboran en el funcionamiento y seguridad de la red, confirmando y transmitiendo transacciones a través de la red.

El proceso de minado requiere hoy día una capacidad de cómputo elevada. Por ello, no es algo que se pueda hacer con un ordenador convencional, sino que el aumento de la complejidad para resolver los cálculos requiere de equipos potentes y sofisticados, con *hardware* muy específico.

Figura 7. Equipos domésticos especializados en minería de Bitcoins, con múltiples GPUs. Fuente: mit.edu

Esta fuerza computacional está destinada a resolver el problema criptográfico en el que está basado el sistema de consenso usado, (denominado «prueba de trabajo» o *Proof of Work*).

Los mineros compiten por ser el primero en encontrar la solución al problema criptográfico. El ganador es recompensado con una cierta cantidad de Bitcoins que se obtiene por el minado. Estos Bitcoins son nuevas monedas que se generan y que entran a formar parte del sistema. Pero no hay una cantidad infinita de Bitcoins, sino que pueden existir como máximo 21 millones de Bitcoins.

Árboles de Merkle

El gran volumen de datos que típicamente forma parte de los sistemas que utilizan *Blockchain* requiere buscar una estructura para almacenarlos de forma eficiente. Para ello se eligió el árbol de Merkle. Esta estructura de datos cuenta con varias propiedades que lo hacen muy adecuado para su utilización en la cadena de bloques.

E l **árbol de Merkle** fue patentado en 1979 por Ralph Merkle. Se trata de una estructura de datos en forma de árbol, que puede ser o no binario. En él, los nodos que no son hojas están etiquetados con el *hash* de la concatenación de las etiquetas de sus nodos hijo.

En la cadena de bloques el árbol se construye de esta manera: las transacciones se agrupan en pares y se calcula el hash SHA-256 de las mismas. Los hashes generados se vuelven a agrupar y se calcula el hash de los mismos. Prosiguiendo de esta forma se va construyendo el árbol, hasta que se llega a la raíz del árbol, representada por un único *hash*.

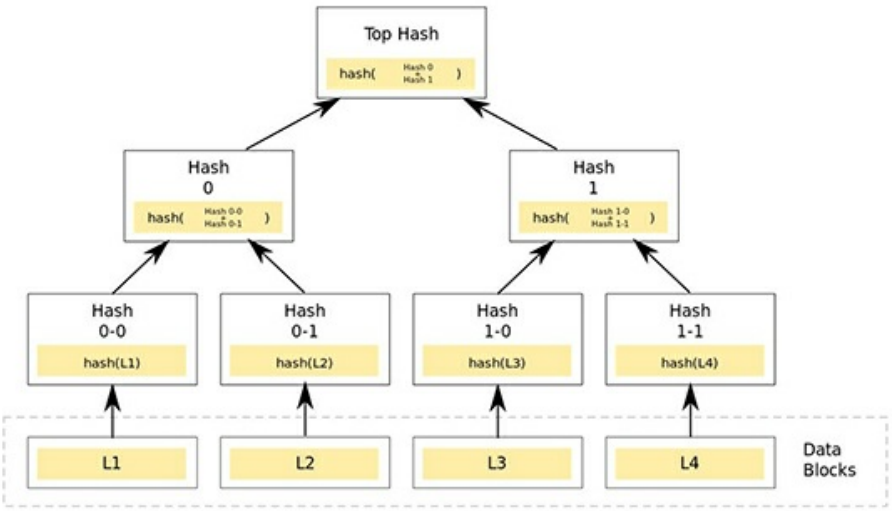


Figura 8. Ejemplo de árbol de Merkle binario. Fuente: https://goo.gl/images/Nfqn8t

De este modo una gran cantidad de datos quedan asociados al *hash* del nodo raíz. De hecho, como este es el que interesa solo es necesario almacenar el nodo raíz. Esta es una gran ventaja en su aplicación a la cadena de bloques, dado el alto número de transacciones que se generan. Una medida de seguridad frecuentemente utilizada es firmar el nodo raíz para garantizar la integridad.

El árbol de Merkle permite reproducir el proceso y comprobar si una transacción pertenece al árbol. Esto proporciona integridad, dado que si una transacción se modifica cambiarán los *hashes* y, por tanto, este hecho puede ser detectado. Esta es una de las razones por las que la cadena de bloques es inmutable. La verificación de que una hoja forma parte del árbol es de complejidad O(log(n)), siendo n el número de nodos del árbol.

8.3 Aplicaciones y Servicios basados en Blockchain

Desde el punto de vista del usuario existen dos conceptos fundamentales para la utilización de criptomonedas:

- Cómo recibir y enviar criptomonedas.
- Cómo comprarlas o venderlas.

Aunque existen distintos proveedores de servicio que permiten integrar ambas funciones, en líneas generales utilizaremos aplicaciones específicas denominadas «monederos» o «*wallets*» para gestionar criptomonedas y «casas de cambio» o «*exchanges*» para obtener criptomonedas.

Monederos ligeros (*light wallets*)

Los monederos más utilizados, por su sencillez, son los denominados ***light wallets***. La principal característica de estas aplicaciones es la posibilidad de empezar a utilizar criptomonedas desde el primer momento, sin necesidad de descargar toda la cadena de bloques, que en realidad no necesitan (puesto que solo requieren para su funcionamiento la información relacionada con las direcciones que gestionan).

Para ello, estos monederos requieren de una funcionalidad ya descrita en el *paper* original publicado por Satoshi Nakamoto, denominada *Simplified Payment Verification (SPV)*, por la cual obtienen de otros nodos de la red información sobre las transacciones de entrada, que tienen como destino alguna de las direcciones gestionadas, y transacciones de salida originadas en alguna de estas direcciones, verificando que los bloques donde están incluidas estas transacciones existen y son válidos. Esto permite evitar la descarga de la cadena de bloques en dispositivos móviles, que no tienen espacio suficiente, y la necesidad de mantener actualizada la información para poder operar en la red.

Como contrapartida, los *wallets* que utilizan SPV dependen de información externa para su funcionamiento y, potencialmente, podrían ser susceptibles de ataques relacionados con esta dependencia.

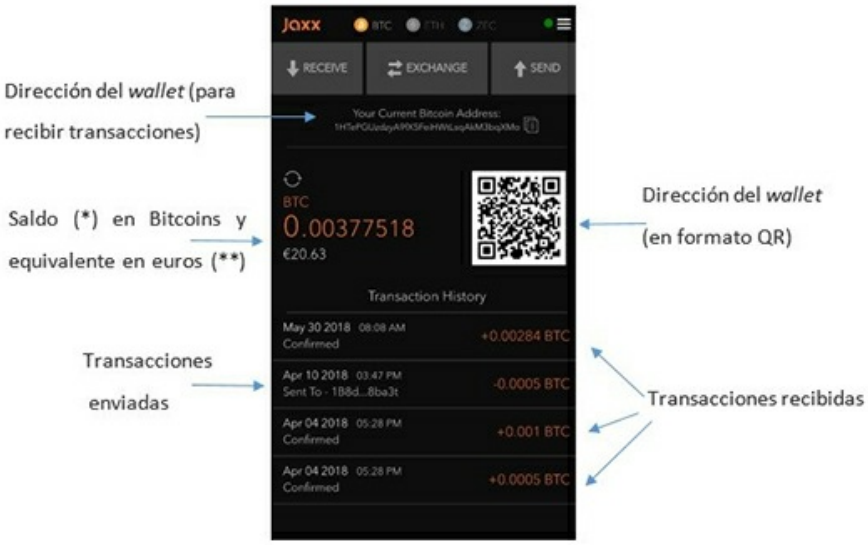


Figura 9. Wallet ligero (Jaxx) en Android. Fuente: Elaboración propia

(*) En realidad, no existe el concepto de «saldo». El total de Bitcoins asociados a una dirección es la suma de las transacciones de salida generadas con destino a dicha dirección que no han sido todavía utilizadas como entradas de nuevas transacciones.

(**) El equivalente en euros se calcula en tiempo real, en función de la cotización de Bitcoin (cada monedero puede calcular un valor distinto, en función del mercado de referencia que pueda utilizar, ya que la cotización varía).

Para incrementar el anonimato, la mayoría de los monederos actuales implementan direcciones HD (*Hierarchical Deterministic*), de forma que se origina automáticamente una nueva dirección por cada transacción generada, impidiendo de esta manera analizar los pagos realizados desde una misma aplicación con base en la reutilización de una misma dirección.

Estos ***wallets*** utilizan una semilla (compuesta por un conjunto de 12 palabras) para derivar, a partir de esta información, un conjunto ilimitado de claves privadas con su correspondiente dirección pública.

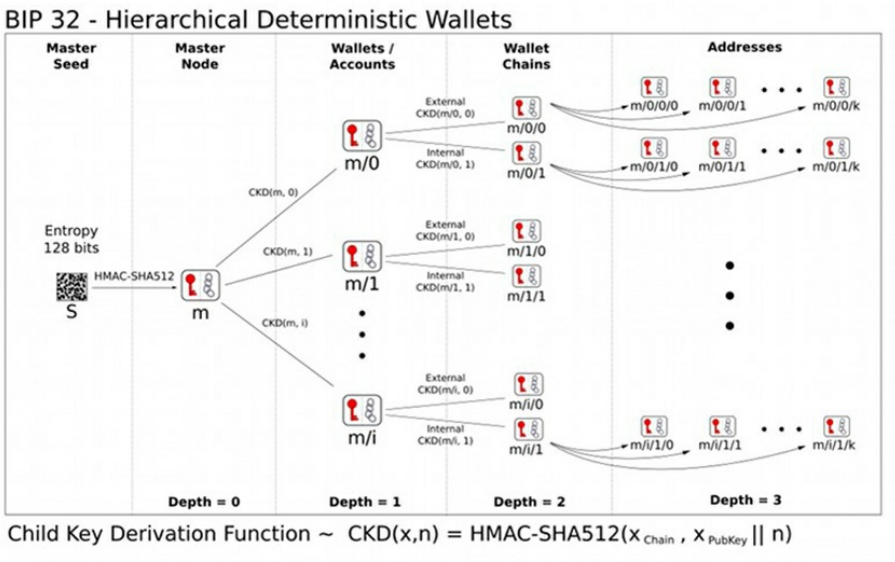


Figura 10. Esquema de derivación de claves en wallets HD según el estándar BIP 32. Fuente: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

Dicha semilla permite, además, restaurar el *wallet* en otro dispositivo, así como disponer de distintas instancias del mismo wallet en múltiples dispositivos.

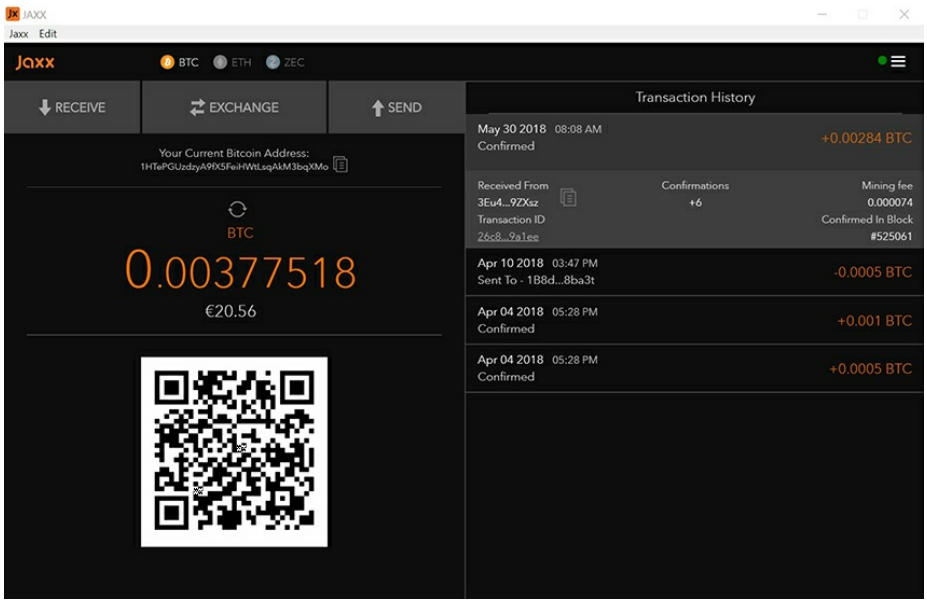


Figura 11. Wallet ligero (Jaxx) en Windows (nótese que es idéntico al wallet para Android. Al usar la semilla para restaurarlo en PC, permite gestionar las mismas direcciones HD.)

Monederos fríos (*cold wallets*)

Cualquier dispositivo que contenga una clave privada correspondiente a una dirección Bitcoin es susceptible de sufrir algún ataque, que en caso de resultar exitoso permitirá al atacante firmar transacciones y, por tanto, disponer de los Bitcoins asociados a dicha dirección.

Para evitar este riesgo es posible generar un «**monedero frío**» o «***cold wallet***», un soporte no electrónico donde se registra la clave privada. Uno de los formatos más habituales para este tipo de monederos son los denominados *paper wallets* o monederos en papel, como el que podemos ver en la siguiente imagen.

Figura 12. *Paper wallet.* Fuente: https://walletgenerator.net/

Distinguiremos dos códigos QR diferentes, uno corresponde a la dirección pública y otro a la clave privada.

Figura 13. Clave privada y dirección pública usando QR.

Podemos consultar la información asociada a la dirección pública generada en la cadena de bloques de Bitcoin, con exploradores como Blockchain.info.

Para poder utilizar los fondos, basta con importar la clave privada escaneando el código QR correspondiente en el *paper wallet* para incorporarla al conjunto de claves

privadas gestionadas por un monedero o bien «barrer» el *paper wallet*, desde el menú correspondiente de la aplicación. De esta forma se genera una transacción utilizando la clave privada para transferir los Bitcoins a una dirección gestionada por el *wallet*, de modo que el *paper wallet*, una vez procesado, ya no tiene valor y por tanto no hay riesgo de que alguien pueda utilizar esa misma clave privada.

Hardware wallets

Otra alternativa para incrementar la seguridad en el uso de criptomonedas pasa por utilizar dispositivos específicamente diseñados para almacenar de forma segura las claves privadas que se utilizan para firmar transacciones. Este tipo de dispositivos se denominan ***hardware wallets***.

Figura 14. Ledger Nano S hardware wallet. Fuente: ledger.com

Este tipo de artefactos se conectan mediante un cable USB al dispositivo donde reside el monedero. En el momento en que se genera una transacción, el *wallet* no tiene acceso a la clave privada, sino que el proceso de firma se realiza en la aplicación que reside en el propio dispositivo (para garantizar que nadie tenga acceso a esta información). Realizada la transacción y retirado el dispositivo del puerto USB, no hay posibilidad de que alguien pueda comprometer o utilizar la clave

privada (salvo teniendo acceso al *HW wallet*).

Casas de cambio (*exchanges*)

Uno de los actores principales para dotar de liquidez al ecosistema de monedas virtuales son las **casas de cambio** o ***exchanges***, que facilitan a los usuarios el intercambio de monedas de curso legal (FIAT) por criptomonedas, y viceversa, así como la compraventa entre distintas monedas virtuales y/o *tokens*.

Las empresas que ofrecen este servicio facilitan a sus clientes una plataforma donde, una vez registrados, pueden operar en el mercado. A cambio de este servicio, estas empresas obtienen comisiones por cada operación que se realiza (compraventa, depósito, retirada, etc).

Una vez el cliente dispone de una cuenta validada, puede realizar una transferencia desde su entidad financiera hacia la cuenta de la casa de cambio o bien transferir criptomonedas para poder operar en el mercado. El tipo de órdenes que pueden realizarse en los *exchanges* permite comprar o vender a precio de mercado (el valor al que se intercambia en el momento en que se genera la orden), o bien establecer otros criterios que dependen de cada casa de cambio (algunas posibilitan incluso apalancamiento o ventas a corto, entre otras opciones).

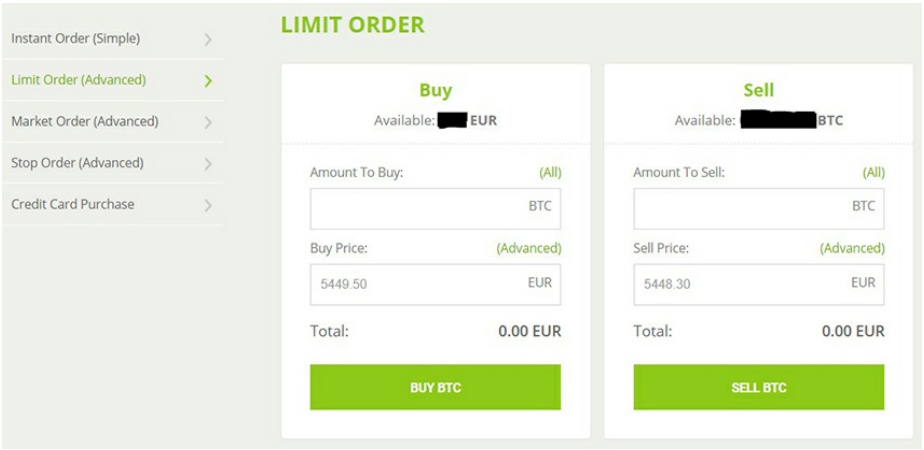


Figura 15. Formulario para realizar distintos tipos de órdenes de compra/venta en Bitstamp.

A diferencia de un *wallet*, las casas de cambio tradicionales son quienes custodian los fondos de sus clientes, estableciendo apuntes contables en su base de datos para reflejar la posición de estos en cada moneda y las transacciones que realizan, así como el estado del mercado y el libro de órdenes existente.

Cuando un usuario deposita criptomonedas en su cuenta para operar en el mercado, en realidad transfiere a la empresa el control de estos activos (realiza una transacción hacia una dirección controlada por el *exchange*, que es quien posee la clave privada que permite generar transacciones hacia la red).

Para incrementar la seguridad y minimizar las consecuencias del robo de estas claves (que se ha producido en múltiples ocasiones) la mayoría de los *exchanges* utilizan **direcciones multifirma** distribuyendo las claves entre varios actores (la propia casa de cambio, el usuario y una tercera parte de confianza), de forma que en el caso de compromiso de una de las partes sea imposible movilizar los fondos al requerir la firma de varias partes para generar una transacción.

En todo momento los clientes de los *exchanges* pueden retirar sus fondos hacia sus propios *wallets*, generándose al finalizar el proceso de verificación (en el que el cliente debe proporcionar típicamente una clave y un segundo factor de autenticación, vía SMS, TOTP, etc.) una transacción desde las direcciones donde la casa de cambio almacena los activos de sus usuarios hacia la aplicación del cliente, momento en el que este pasa a controlar sus criptomonedas.

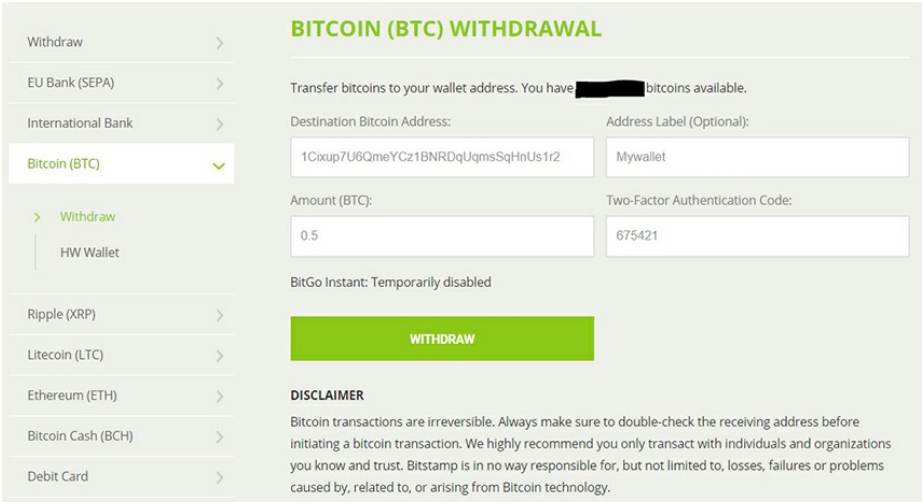


Figura 16. Formulario para retirada (withdraw) de Bitcoins en Bitstamp a la cartera del usuario.

Adicionalmente, las casas de cambio solo disponen de una fracción de sus reservas en criptomonedas *online* disponibles en el mercado. **El grueso de los activos se almacena en *cold wallets*** custodiados con medidas de seguridad físicas y se activan únicamente cuando es necesario para garantizar la liquidez, evitando que las claves privadas puedan ser sustraídas por medios electrónicos.

A lo largo del tiempo, los controles exigidos por parte de distintos países (como es el caso de EE. UU.) a las empresas que prestan estos servicios a sus ciudadanos se han incrementado con el objetivo de cumplir la legislación y reducir el riesgo de actividades fraudulentas.

Las casas de cambio deben cumplir, en estos casos, las normativas **AML/KYC (*Anti Monery Laundering* / *Know Your Customer*)** solicitando a sus clientes en el proceso de registro la documentación necesaria para identificar de forma fehaciente su identidad y domicilio, y registrando todas las operaciones que realizan (información que podrá ser solicitada por las autoridades en los casos contemplados por la ley).

Aplicaciones de Blockchain

En esta lección magistral se ofrecerán ejemplos muy variados, en distintos ámbitos de actuación y sectores, de aplicaciones de la cadena de bloques.

Qué es Blockchain

Pastor, J. (26 de noviembre de 2018). Qué es el Blockchain: la explicación definitiva para la tecnología más de moda. *X a t a k a* [Recurso electrónico]. https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda

Interesante y claro artículo divulgativo en el que se ofrece una visión muy directa de lo que es *blockchain* y sus ámbitos de aplicación, así como sobre la minería de criptomonedas

Todo lo que vamos a poder hacer con Blockchain

Mora, J. J. (14 de mayo de 2017). Todo lo que vamos a poder hacer con Blockchain. *Futurizable* [Recurso electrónico]. https://futurizable.com/blockchain/

Artículo interesante en cuanto a la descripción de toda la nomenclatura existente en torno a la cadena de bloques, y algunos de los ejemplos de sus aplicaciones

Manual para entender Blockchain

RETINA Tendencias. (21 de julio de 2017). *Manual para entender blockchain | EL PAIS RETINA* [Vídeo]. YouTube. https://youtu.be/tRymoSFfOnA

Vídeo sintético y con cierto tono humorístico que explica el fundamento de la cadena de bloques, resaltando el punto más relevante: permite eliminar la intermediación, haciendo ver qué implicaciones tiene esto.

Securing the Blockchain against hackers

Boireau, O. (enero, 2018). Securing the blockchain against hackers. *Network Security, 1* (2018), 8-11. doi: 10.1016/S1353-4858(18)30006-0. Recuperado de: https://www.sciencedirect.com/science/article/pii/S1353485818300060

Este artículo científico, publicado en la prestigiosa revista Network Security, aporta puntos de vista interesantes sobre las necesidades adicionales de protección de *Blockchain* frente a intentos conocidos de *hacking.*

1. Técnicamente, *Blockchain* es:

   A. Una cadena de bloques de granito en los que se inscriben las claves privadas de todos los miembros de una empresa, como mecanismo sólido para probar identidades digitales.

   B. Es un tipo de Libro de Resgisto Distribuido (DLT, Distributed Ledger Technology).

   C. Un mecanismo que permite asegurar la confidencialidad de dos partes que se comunican a través de Internet.

   D. Ninguna de las anteriores es cierta.

2. Los bloques de una cadena en *blockchain*:

   A. Se almacenan en una inmensa base de datos centralizada.

   B. Se almacenan en las bases de datos de los distintos Bancos Centrales europeos.

   C. Se distribuyen en una red de nodos P2P (peer to peer, entre iguales).

   D. Ninguna de las anteriores es cierta.

3. Bitcoin es:

   A. La nueva moneda oficial de la República Bolivariana de Venezuela, creada para revolucionar las tradicionales estructuras capitalistas de intercambio de dinero.

   B. Una criptomoneda específicamente diseñada para que los Estados controlen todas las transacciones económicas entre particulares.

   C. Un sistema de pagos P2P que permite realizar transacciones económicas sin intermediarios.

   D. Ninguna de las anteriores es cierta.

4. Sobre el conjunto de transacciones histórico de la cadena de bloques de Bitcoin:

   A. Se podrían almacenar localmente en nuestros ordenadores.

   B. Su tamaño actual ronda los 200GB como mínimo.

   C. Nadie es dueño de esta cadena de bloques.

   D. Todas las anteriores son ciertas.

5. Son alternativas de Bitcoin:

   A. Ethereum e Hyperledger.

   B. Ethereum y MegaBitCoin 2.0.

   C. Ethereum para monedas, y GalaxyNote para billetes.

   D. Ninguna de las anteriores es cierta.

6. Son DLTs sin permisos:

   A. Ethereum y Bitcoin.

   B. Ethereum e Hyperledger.

   C. Ethereum y MegaBitCoin 2.0.

   D. Ninguna de las anteriores es cierta.

7. Para desarrollar *Smart Contracts* con Ethereum se usa:

   A. Solidity.

   B. Liquidify.

   C. Gasify.

   D. Ninguna de las anteriores es cierta.

8. En bitcoin, es importante que las claves públicas:

A. Sean cortas.

B: Sean largas.

C. No se utilicen, como medida de seguridad.

D. Ninguna de las anteriores es cierta.

9. En el contexto de bitcoin, un minero es:

A. Una persona que ejecuta un programa en todos los servidores de Internet y que ayuda a verificar las transacciones Bitcoin al incluirlas en un registro inalterable.

B. Una persona que ejecuta un programa en su ordenador y que ayuda a verificar las transacciones Bitcoin al incluirlas en un registro inalterable.

C. Una persona que ejecuta un programa en todos los servidores de Internet para intentar hackearlos y tener beneficios económicos muy elevados.

D. Ninguna de las anteriores es cierta.

10. Un monedero frío o *cold wallet* es:

A. Un monedero de bitcoins que se guarda con refrigeración constante para evitar que el calor destruya los enlaces de la cadena de bloques.

B. Un soporte no electrónico donde se registra una clave privada, como los monederos en papel.

C. Un monedero electrónico de bitcoins, diseñado con especificaciones militares y apto para su uso en países nórdicos, especialmente en invierno.

D. Ninguna de las anteriores es cierta.