Tecnología Blockchain

Servidores Web de Altas Prestaciones

Jose Luis Pedraza Román
Iván López Justicia
Pablo Jesús Martínez Ramírez

Wiki 23
Curso 2019/2020
Universidad de Granada
Horas aprox. dedicadas al proyecto: 85h

Índice

1 Introducción - Del internet de la información al internet del valor **3**

2 Marco histórico **4**

3 ¿Qué es Blockchain? **5**
3.1 Concepto . . . 5
3.2 Consenso . . . 5
3.3 Token, Criptomoneda y Smart Contracts . . . 6
3.4 Tipos de Blockchain: no permisionada, permisionada e híbrida . . . 7

4 ¿Cómo funciona Blockchain? **9**
4.1 Redes P2P . . . 9
4.2 Qué son y cómo funcionan los nodos de la red . . . 11
4.3 Transacciones . . . 13
4.3.1 Transacciones en Bitcoin . . . 14
4.3.2 Transacciones en Ethereum . . . 15
4.4 Firmas digitales (clave pública/privada, monederos/billeteras) . . . 16
4.4.1 Hash: funciones criptográficas . . . 17
4.5 Métodos de consenso . . . 21
4.5.1 Proof of Work . . . 21
4.5.2 Proof of Stake . . . 22
4.5.3 Obelisk . . . 22
4.6 Minería . . . 22
4.7 Sumario . . . 23

5 Debilidades **25**
5.1 Fallas Bizantizas . . . 25
5.2 Ataque del 51 %, dispositivos ASIC y ataque del doble gasto . . . 26
5.3 Robo de direcciones . . . 28
5.4 Vulnerabilidades software en Smart Contracts: caso DAO . . . 28
5.5 Pérdida de clave privada . . . 29

6 Aplicaciones de Blockchain **30**
6.1 Financiero . . . 30
6.1.1 Contratos inteligestes . . . 30
6.1.2 Identidad perpetua - DNI . . . 30
6.1.3 Pagos digitales - Stellar, Ripple . . . 30
6.1.4 Emisión de títulos y activos digitales . . . 30
6.2 Seguros . . . 31
6.3 Registro de la propiedad . . . 31
6.4 Uso futuro . . . 32

7 Empresas que usan e investigan la tecnología Blockchain **33**
7.1 Bitcoin . . . 33
7.2 Ethereum . . . 33
7.3 Alastria . . . 34
7.4 Hyperledger . . . 35

8 Conclusión **36**

9 Referencias Bibliográficas **37**

1. Introducción - Del internet de la información al internet del valor

El Internet que conocemos actualmente, llamado Internet de la información, empezó a aplicarse en los sectores militar y académico antes de expandirse al resto de industrias. En nuestro caso a abordar, el Internet del valor comenzó a aplicarse en el sector financiero con la aparición de Bitcoin, siendo este el primero en tomar la iniciativa. Pero como el caso anterior, la aplicación de esta tecnología no será exclusiva de un único sector, pues cada vez son más las industrias que investigan y aplican su potencial.

"Internet trivializa la distancia, Blockchain trivializa la confianza"

Antes de Internet las comunicaciones a distancia estaban monopolizadas por servicios como los de correos, telefonía, etc. Antes de Blockchain la confianza estaba monopolizada por abogados, notarios, bancos, etc. Esto es lo que pretende eliminar la Blockchain al igual que Internet eliminó la limitación de la distancia.

La cadena de bloques o Blockchain se utiliza para la verificación de las transacciones de datos (conceptos que definiremos más adelante) y su uso comprende todos aquellos procesos en los que hay que proteger, acreditar o distribuir cualquier tipo de dato. Además, las aplicaciones basadas en esta tecnología no requieren en un principio de intermediarios, lo cual supone una gran revolución a todos los niveles de aplicación.

Es así como, al menos en teoría, las transacciones de pagos, los movimientos de capital en los mercados, cualquier tipo de contrato, certificación, derechos de autor, patentes o registros, entre otros, se pueden gestionar sin la intervención de bancos, notarios, administradores u otras instituciones estatales, con su correspondiente ahorro en costes.

Como decíamos, la innovación de Blockchain está basada en algunos de los conceptos introducidos por Bitcoin, un verdadero sistema de votación abierto, en el que los votantes pueden confirmar que sus votos han sido adecuadamente contados y pueden, en cualquier momento, ver un completo conteo de los votos, garantizando así una gran transparencia. Por tanto, Bitcoin ha desencadenado claramente esta nueva revolución tecnológica del Internet del valor, capitalizando Internet tal y como lo conocemos.

2. Marco histórico

Hasta la aparición de Blockchain para la realización de transacciones a través de Internet se precisaba de un intermediario el cual sería el que daría el visto bueno a dicha transacción.

Este intermediario debía tener la confianza de ambas partes, de esta posición central, en ciertas ocasiones, se hace un uso abusivo velando por el interés propio. Un claro ejemplo de esta influencia ocurrió en 2010 cuando el portal de pago PayPal cerró la cuenta de la plataforma WikiLeaks.

La primera aproximación a la tecnología Blockchain fue creada en 1991 por los científicos Stuart Haber y W.Scott Stornetta al introducir una solución computacionalmente práctica para los documentos digitales con sello de tiempo para que no pudieran ser modificados o manipulados.

La tecnología Blockchain fue propuesta en 1997 por un informático y ex profesor de derecho Nick Szabo como solución a la falta de confianza entre los usuarios anónimos que realizaban intercambios de datos en Internet.

En el año 2008 un programador, o grupo de programadores, bajo el alias de Satoshi Nakamoto propuso la idea de Bitcoin, que en Enero de 2009 se convirtió en la primera criptomoneda descentralizada del mundo. Esta moneda es completamente revolucionaria, dado que realmente es un software que por primera vez en la historia permite hacer transferencias de valor entre un par de personas en cualquier parte del mundo sin recurrir a una entidad centralizada como puede ser un banco, un gobierno o una compañía.

Esta idea revolucionaria resolvió simultáneamente y por primera vez en la historia, dos problemas fundamentales, que son:

1. El problema del tercero confiable: No hay necesidad de que existan intermediarios porque todas las transacciones son anotadas en tiempo real en un registro público 100 % editable y que está distribuido de forma abierta y voluntaria en Internet. Cuando una computadora de esa red confirma un pago y realiza un cambio en su registro, al mismo tiempo se actualizan todos los demás registros distribuidos alrededor del mundo.
2. El problema del doble gasto: Basado en la idea de digitalizar transacciones de valor entre personas físicas. Por ejemplo, si yo te doy un objeto físico, la transacción termina ahí, yo dejo de tener ese objeto porque ya lo tienes tú. Pero para verificar en un caso digital que un archivo virtual es único e irrepetible debemos llevar un registro para verificar quién tiene qué, lo que se denomina “libro de contabilidad”.

3. ¿Qué es Blockchain?

3.1. Concepto

La definición de **Blockchain** más básica sería: *un registro compartido y digitalizado que no puede modificarse una vez que una transacción ha sido registrada y verificada. Todas las partes de la transacción, así como un número significativo de terceros, mantienen una copia del registro (es decir, la cadena de bloques), lo que significa que sería prácticamente imposible modificar cada copia del registro globalmente para falsificar una transacción.*

Una definición algo más técnica de Blockchain: *es una estructura de datos descentralizada basada en una concatenación de bloques de datos ampliable en todo momento. Estos bloques a su vez registran transacciones entre pares en orden cronológico e irreversible. Podemos entender los bloques de información de una Blockchain como los eslabones de una cadena que se entrelazan permanentemente. Esta concatenación tiene lugar gracias a procesos criptográficos, los cuales garantizan que se puedan añadir nuevos bloques sin sustituir o modificar los anteriores. Por esto que con el paso del tiempo la cadena de bloques será más y más larga, resultando así imposible modificar la información almacenada.*

3.2. Consenso

Blockchain debe entenderse como una **base de datos descentralizada** en la que cada participante tiene una copia completa de dicha base datos (todos los participantes tienen una copia de la cadena de bloques). Para añadir una modificación (transacción) en esta base de datos es necesario que todos los participantes validen dicha transacción, aquí entra en juego el concepto de çonsenso".

Este **consenso** se lleva a cabo a través de una forma definida en la Blockchain, por ejemplo, el 51 % de los participantes deben aceptar dicha transacción, corroborando que es correcta y que se puede incluir en la cadena.

El consenso en la red Blockchain hace referencia al proceso de lograr un acuerdo entre los distintos participantes de la red sobre las transacciones que van a escribirse en la cadena. Este consenso es el responsable de que todos los nodos de la red tengan los mismos datos, evitando así su manipulación.

La forma de implementar esto en la red es lo que se conoce como método o algoritmo de consenso (los cuales veremos después en mayor profundidad) y forma parte del núcleo de la misma red, aunque en algunas implementaciones de redes Blockchain se permite seleccionar este algoritmo entre varios disponibles.

Para entender este concepto mejor, imaginemos el comercio on-line de segunda mano, alguien desea vender un objeto que ya no utiliza y por tanto lo anuncia en una plataforma de venta de segunda mano. Otra persona deseará comprarlo por lo que se establecerá un precio de venta. Estas dos personas viven en lugares distintos, de modo que el intercambio “en mano” no puede realizarse. Ambas partes se muestran reticentes y no confían en la otra parte. El vendedor no enviará el producto hasta tener el dinero, pero el comprador no pagará sin tener el producto, por miedo a que la otra parte se retracte provocando la pérdida del dinero o el producto.

Una solución a esto podría ser el uso de un mediador, en el cual creemos y se encargará de realizar tanto la entrega del producto como del dinero a sus respectivos a cambio de cobrar unas tasas por la transacción.

Aquí es donde Blockchain nos ofrece una alternativa al uso de mediadores externos, dado que

estas transacciones en redes Blockchain no necesitan ser verificadas por terceros, ahorrandonos así los costes de gestión y el intercambio será más seguro y confiable ya que todo registro de una transacción se queda guardado en un historial donde sólo se pueden añadir nuevos, quedando registros de todo cambio distribuidos y actualizados en todos los nodos de la red. Esto es denominado **libro contable distribuido (distributed ledger)**.

Actualmente existen sistemas como *Bitcoin* o *Ethereum*, entre otros muchos, que se basan en la tecnología de Blockchain y que podrían ayudar en este caso del comercio on-line de segunda mano y prácticamente en todos los que estén basados en una relación de confianza entre los participantes. Basta con descargar el software cliente e instalarlo de forma local en el ordenador. A partir de entonces, tanto comprador como vendedor se convertirían en nodos de una red de Blockchain.

3.3. Token, Criptomoneda y Smart Contracts

Un **token** es históricamente entendido como una ficha, vale o pseudo moneda que es utilizado como sustituto de una moneda real dentro del espacio para el que están concebidos. Un ejemplo claro de token podrían ser las fichas de un casino, que sustituyen al dinero real, pero son válidas únicamente dentro del propio casino y solo tiene validez siempre que este casino esté en funcionamiento.

En la historia se han utilizado tokens en diversas ocasiones y por motivos similares. En Hispania y también en la época colonial, los tokens aparecieron para suplir la escasez de moneda oficial.

La diferencia fundamental entre un token y una moneda es que una moneda (o divisa) es emitida por una autoridad local o nacional y es de libre cambio de bienes u otras monedas, mientras que un token tiene un uso mucho más limitado y es a menudo emitido por una empresa privada, institución, grupo, asociación o persona, por lo que no son dinero de curso legal.

Todas las **criptomonedas** son por definición tokens. Son una unidad de valor, emitida por una entidad privada, que tiene el valor que se le otorga dentro de una comunidad. Un token en el contexto del Bitcoin puede ser cualquier cadena alfanumérica que represente un registro en la base de datos descentralizada de consenso de Bitcoin, por ejemplo, la clave pública:

“3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy”

es un token. Por tanto, un token es una representación dentro de esa base de datos que es Blockchain de un activo o de una propiedad que a día de hoy las entidades, como bancos, empresas o gobiernos, gestionan.

Los **contratos inteligentes** (*smart contracts* en inglés) eran una de las grandes promesas de las blockchain, ya que permiten un nuevo paradigma que va mucho más allá de las transferencias de dinero, y es que, Bitcoin y la tecnología de la cadena de bloques (Blockchain) hacen posible que, por primera vez, se pueda implementar este concepto, cuya teoría fue desarrollada hace casi veinte años, y que no ha sido hasta la invención de Bitcoin que haya sido potencialmente viable, ya que es necesario el uso de **dinero programable**.

Alex Puig, CEO de Alastria, una asociación sin ánimo de lucro que fomenta la economía digital a través del desarrollo de tecnologías de registro descentralizadas/Blockchain, explica muy bien estos conceptos con el siguiente ejemplo: “Si tengo una flota de vehículos podría enviarles litros de gasolina, así no tendría que darles tarjetas de crédito, ni pedirles tickets. Les doy los litros y los programo para que sólo se puedan gastar en un horario determinado, en una zona y con un vehículo

con una matrícula concreta. Realmente, afecta a todos los sectores. Y no necesitas que nadie lo certifique, lo certifica la tecnología porque Blockchain es un libro de contabilidad".

En este ejemplo, los litros de gasolina serían los tokens y el smart contract sería el "programa" que limita, condiciona y automatiza el uso de dichos tokens.

Los contratos inteligentes son scripts repetibles y autónomos que se ejecutan en la cadena de bloques (Blockchain) y representan promesas unilaterales de proporcionar una tarea informática determinada. Se almacenan en una dirección específica en la cadena de bloques. Dicha dirección se determina cuando los contratos son compilados y enviados a la cadena de bloques. Cuando se produce un evento contemplado en el contrato, se envía una transacción a esa dirección y la máquina virtual distribuida ejecuta los códigos de operación del script (o cláusulas) utilizando los datos enviados con dicha transacción.

Los contratos inteligentes pueden estar codificados de modo que reflejen cualquier tipo de lógica basada en datos, buen ejemplo de ello serían, gestión de préstamos, depósitos en garantía, controles de gasto, herencias y donaciones, etc.

3.4. Tipos de Blockchain: no permisionada, permisionada e híbrida

Con el tiempo se han ido desarrollando varios tipos o categorías de Blockchain orientados a diferentes casos de uso de esta tecnología:

- No permisionada o pública.

  Fue el primer tipo en aparecer, son las referentes a aquellas a las que tenemos fácil acceso a través de internet, como el ya mencionado Bitcoin o Ethereum, con un simple registro en la plataforma y la descarga del software necesario. Estas Blockchain tienen todos los datos, software y desarrollo abiertos al público, de modo que cualquiera puede revisar, desarrollar o mejorar los mismos.

  Esta misma razón acentúa la necesidad de implantar medidas de seguridad para prevenir cualquier tipo de ataque, aquí es donde entran en juego la tolerancia a fallas bizantinas, protocolos de consenso robustos, protección contra ataques DDos o contra ataques de 51 %.

  Las características de estas redes son:

  - Permiten que cualquier persona pueda formar parte de la misma. Bien sea como usuario, minero o administrador de un nodo, las personas pueden acceder a la red y formar parte de ella sin restricción alguna.
  - El funcionamiento de la red es completamente transparente y abierto. Los datos de la Blockchain desde sus inicios están disponibles para todos sin restricciones. Cualquier persona puede revisar o auditar el funcionamiento de la red y su software.
  - No existen entidades centralizadas. Las redes públicas son completamente descentralizadas y no existe una autoridad central que regule su funcionamiento.
  - El mantenimiento económico de la Blockchain depende del sistema integrado en la misma. Generalmente este sistema económico depende de la minería y el cobro de comisiones por cada transacción que se realice dentro de la red.

- Permisionada o privada.

  Una vez las Blockchain fueron desarrollándose, muchas empresas comenzaron a interesarse por esta tecnología. Tanto éstas como las no permisionadas comparten los mismos elementos, con la diferencia de que en las permisionadas existe una entidad central que controla la actividad de la misma. Esta unidad central es la que da acceso a los usuarios, controlando sus funciones y permisos. Usualmente, con opciones de tipo software privativo, aunque con la existencia de software libre. Una de las Blockchain permisionada más importa es Hyperledger, proyecto iniciado por la Fundación Linux y varias empresas del sector tecnológico. Es el mayor ejemplo de Blockchain privada.

  Características de las Blockchain permisionadas:

  - Restringido acceso a la red a elementos que solo pueden ser autorizados por la entidad centra.
  - El acceso al libro de transacciones o cualquier otra información del Blockchain es privado.
  - El mantenimiento económico de la Blockchain depende generalmente de la empresa que sostenga el proyecto. Frecuentemente, las Blockchain privadas no cuenta con criptomonedas ni se realizan acciones de minería.

- Híbrida o federada.

  Estas Blockchain son un intento de aprovechar lo mejor de ambas opciones. Aquí la participación en la red es privada, es decir, el acceso de la red es controlado por una entidad, pero, como en las no permisionadas, el libro de contabilidad es público, de modo que cualquiera tiene acceso. Suelen ser utilizadas por gobiernos u organizaciones que deseen almacenar o compartir datos de una forma segura. En el ámbito sanitario, por ejemplo, se están comenzando a almacenar los datos de sus líneas de producción de medicamentos. Estos datos pueden ser revisados por las autoridades competentes con el fin de controlar la calidad y veracidad. El objetivo es ofrecer un alto nivel de transparencia y confianza.

  Las características de las Blockchain híbridas son:

  - Acceso a la red restringidos a elementos autorizados por la entidad controladora.
  - El acceso a la información de la Blockchain es público.
  - Ni minería ni criptomonedas. El consenso se da por otros medios que aseguran que los datos son correctos.
  - Parcialmente descentralizado, proporcionando un mejor nivel de seguridad y transparencia.

	No Permisionada	**Permisionada**	**Híbrida**
Nivel de Acceso	Sin restricción	Una o varias organizaciones	Una o varias organizaciones
Participación	Sin permisos Anónimo	Permisivo Usuarios conocidos	Permisivo Usuarios conocidos
Seguridad	Mecanismo de consenso Prueba de Trabajo/Participación	Pre-aprobación de participantes Votaciones/Consensos múltiples	Aprobación por autoridades competentes
Rendimiento	Baja velocidad de transaccionalidad	Livianidad Mayor velocidad	Velocidad intermedia

4. ¿Cómo funciona Blockchain?

4.1. Redes P2P

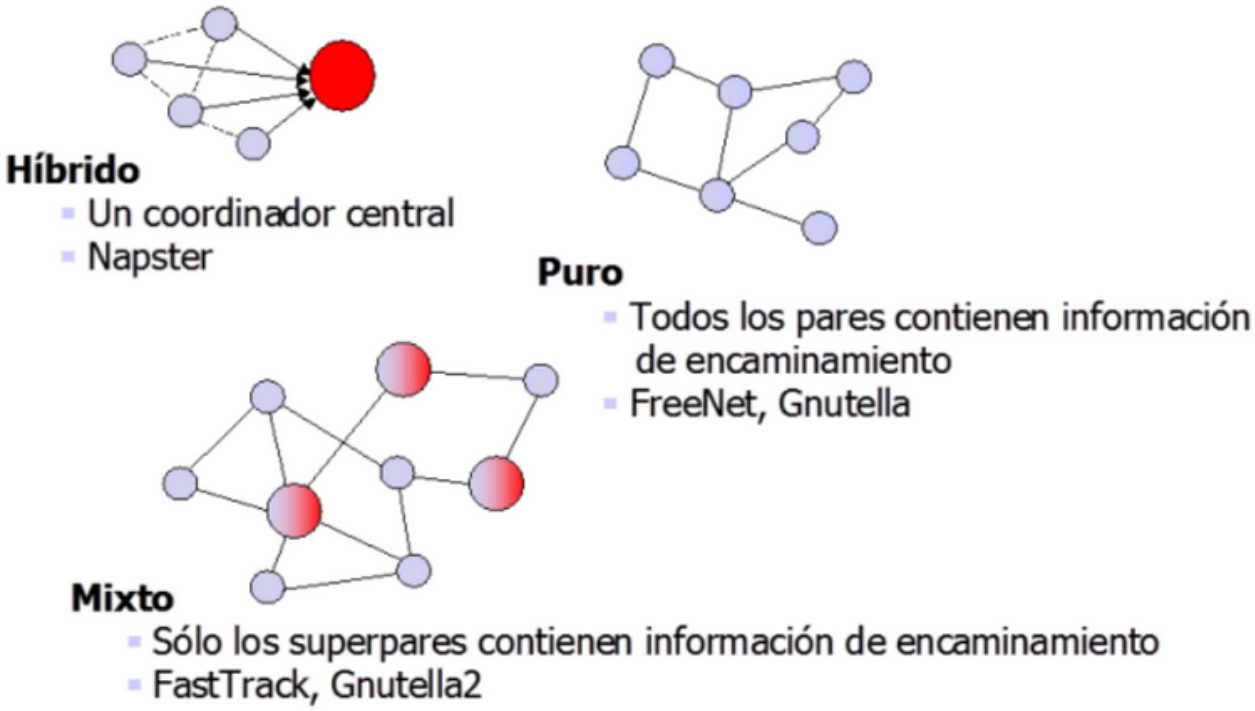
Antes todo, para entender cómo funciona y opera la tecnología Blockchain debemos conocer sobre qué está construida. Hemos hablado de la descentralización de la red lo cual nos lleva directamente al concepto de redes P2P (**Peer to Peer**) o "redes de comunicación de igual a igual". En una red centralizada, normalmente los ordenadores o clientes de la red están conectados a un servidor central, siguiendo así una arquitectura de cliente-servidor. En una red P2P, por el contrario, los ordenadores se conectan y comunican entre sí sin usar ningún tipo de servidor central, optimizando y administrando así la capacidad de la red, empleando la mejor ruta entre todos los nodos u ordenadores que la conforman. De esta manera, cada nodo de la red puede comportar como cliente y servidor a la vez.

Así mismo, el elemento fundamental de toda red P2P es el "par" (o más exactamente "el igual", si traducimos "peer" al español), el cual es la unidad de procesamiento básico de cualquier red de este tipo. Se tiende a pensar que un par es una aplicación ejecutándose en un ordenador conectado a una red como internet. Sin embargo, esta definición no engloba toda la potencialidad del concepto. Por ejemplo, esta definición no considera la posibilidad de que un par puede ser una aplicación distribuida a lo largo de varias máquinas trabajando en grupo, en lo que concretamente está basada parte de la tecnología Blockchain. Por esto, una definición más apropiada de par sería: una entidad capaz de desarrollar algún trabajo útil y de comunicar los resultados de ese trabajo a otra entidad de la red, ya sea directa o indirectamente.

Este tipo de redes han servido para hacer intercambios de archivos a través de internet, lo cual nos da la idea de disponer de un internet democrático dado que los intercambios se dan siempre entre pares. Cabe destacar el protocolo colaborativo BitTorrent para este tipo de tareas de intercambio de archivos, el cual permite el intercambio de datos a nivel mundial de forma anónima. También cabe destacar compañías como Skype y otras de telefonía, que también operan en base a este tipo de redes para la transmisión de voz y vídeo a través de internet.

Para conocer más en profundidad estas redes, y en consecuencia Blockchain, veremos los tipos de redes Peer to Peer:

- **Red centralizada**: Una red P2P es considerada centralizada cuando existe un servidor central al que los ordenadores conectados hacen peticiones para localizar los nodos que poseen el contenido deseado. La desventaja de este tipo de redes sigue siendo la centralización y consecuencia de esta es que ese servidor central es un punto crítico muy importante para la consistencia de toda la red.
- **Red descentralizada y estructurada**: También conocidas como redes P2P híbridas, ya que no existe ningún directorio en un servidor central. En su lugar, existen diversos "nodos centrales" que facilitan el acceso a otros nodos y sus contenidos. De este modo, digamos que hay nodos de mayor importancia que otros para el correcto funcionamiento de la red.
- **Red descentralizada y no estructurada**: Este tipo es el más interesante desde el punto de visto de Blockchain, dado que no existen ordenadores o nodos que actúan como controladores centrales de peticiones. Todos los nodos funcionan como clientes y como servidores según si están solicitando o compartiendo contenido.



Las aplicaciones que utilizan este tipo de redes poseen una serie de características muy interesantes, algunas de las cuales pueden ser apreciadas en las aplicaciones Blockchain en mayor o menor medida, estas son:

- **Descentralización**: Pueden gestionar conexiones variables y direcciones provisionales. Los ordenadores conectados se consideran iguales. Por el contrario, en el modelo cliente-servidor la información se concentra en servidores y los usuario acceden a ella a través de programas de clientes, los cuales se comportan como meras interfaces de usuario. La principal desventaja de esta arquitectura es que lleva inevitablemente a ineficiencias, cuellos de botella y recursos desperdiciados.

- **Anonimato**: Es una característica muy deseable. Los usuarios pueden conectarse de forma anónima a la red. Aunque no todas las aplicaciones basadas en Blockchain cumplen esta característica por completo. Existen varias técnicas para alcanzar el anonimato en las redes P2P como la creación de multicasting para que el receptor de un contenido no pueda ser identificado, ocultación de la dirección IP y la identidad del emisor, comunicación mediante nodos intermedios a pesar de que sea factible contactar directamente con el destinatario, o ubicación involuntaria, encriptada y fragmentada de los contenidos.

- **Escalabilidad**: Gracias a no depender de un servidor central son fácilmente escalables, es decir, se puede crear un aumento en la capacidad de trabajo o de tamaño del sistema sin comprometer el correcto funcionamiento del mismo, y manteniendo la calidad necesaria de los servicios ofrecidos.

- **Rendimiento**: Los sistemas P2P mejoran el rendimiento agregando mayor ancho de banda, capacidad de almacenamiento y ciclos de computación de los dispositivos diseminados por una red. Los sistemas descentralizados consiguen un mayor rendimiento, salvo para ciertas funciones como la búsqueda de recursos en la red (a veces tan necesaria). Por ello, las aplicaciones actuales P2P suelen tener una arquitectura mixta como hemos visto antes, incorporando el concepto de superpares, o pares en los que otros pares delegan las tareas de búsquedas de recursos en la red.

- **Seguridad**: La mayoría de requisitos de seguridad de este tipo de redes son comunes a los sistemas distribuidos tradicionales, como el establecimiento de relaciones de confianza entre nodos y objetos distribuidos y de esquemas de intercambio de claves de sesión. No obstante, en los sistemas P2P aparecen nuevos requisitos como la encriptación de las comunicaciones y almacenamiento de datos, gestión de derechos digitales, reputación e interoperabilidad con cortafuegos y NAT, etc. Esta característica es la razón principal de que las redes Blockchain se basen en la confianza entre los participantes que la conforman y de que hereden muchos de estos requisitos de seguridad anteriores.
- **Tolerancia a fallos**: En las arquitecturas cliente-servidor, si el servidor falla supone una pérdida total de la funcionalidad de la red (realmente es un punto muy crítico en este tipo de redes). Por el contrario, en las redes P2P no ocurre ya que el objetivo básico de diseño de estas redes es que esta no pierda su funcionalidad debido a fallos asociados a desconexiones de nodos o a nodos no alcanzables, caídas de red y fallos en los nodos. La forma en que se consigue esto es que varios nodos sean capaces de ofrecer los mismos recursos y servicios, replicándose espontáneamente en una serie de nodos de la red (de igual forma ocurre con Blockchain, como es el caso de la famosa hoja de contabilidad de la red Bitcoin).
- **Propiedad compartida**: Reduce el coste de la posesión de los sistemas y contenidos, así como el coste de su mantenimiento. El coste del sistema global se ve reducido porque en P2P se reducen las capacidades de cálculo, almacenamiento y ancho de banda ociosas.
- **Conectividad ad-hoc**: Las aplicaciones están preparadas para que en caso de que los nodos no estén disponibles todo el tiempo o que lo hagan de forma intermitente sigan funcionando correctamente. La naturaleza ad-hoc se reduce por ejemplo mediante proveedores de contenidos redundantes con técnicas de replicación espontáneas, o nodos de mayor peso que se encargan de mantener la información o mensajes destinados a pares temporalmente desconectados de la red.

Algunas de las aplicaciones P2P más conocidas siguen teniendo cierto grado de centralización, pudiendo ser completamente centralizadas, descentralizadas o un punto intermedio, pero es importante que el punto en común siempre es que todas siguen un sistema de computación de red distribuida donde todos los nodos o pares pueden actuar como clientes o servidores, comunicándose así de igual a igual.

4.2. Qué son y cómo funcionan los nodos de la red

Cada equipo informático que participa en esta red se denomina nodo y comparten la responsabilidad de proporcionar servicios de red. Esto significa que cada nodo debe tener descargado el software de la Blockchain en cuestión para participar esta red entre pares. El conjunto de nodos coordina de forma descentralizada y distribuida las acciones que cada usuario hace dentro de la red, lo que implica que esta red de dispositivos en todo el mundo se mantiene actualizada con las últimas transacciones realizadas y, como cada nodo tiene descargada la Blockchain, la red es redundante, segura y escalable.

Una vez el nodo tiene una copia actualizada, comienza a ser completamente operativo, permitiendo y verificando transacciones, que no son más que intercambios entre los nodos de la red que bien puede ser dinero, valor, veracidad, propiedades... Además, de respaldar una imagen completa o parcial de la Blockchain global. Normalmente las funciones de un nodo podrían resumirse en enrutamiento, base de datos de la Blockchain, minería y servicios de cartera o monedero, todo ello dependiendo de cada Blockchain en sí misma.

Los nodos son la mínima unidad de cómputo y los propietarios de los nodos contribuyen voluntariamente con sus recursos informáticos teniendo la oportunidad de cobrar las tarifas de transacción

y ganar una recompensa por hacerlo. Un nodo puede ser un punto final de comunicación o un punto de redistribución de la comunicación, enlazando a otros nodos. Hemos dicho que cada nodo de la red se considera igual aunque esto no quita que ciertos nodos mantengan diferentes roles en la forma en que soportan la red. Por ejemplo, no todos los nodos almacenarán una copia completa de una cadena de bloques ni validarán transacciones.

Cuando un usuario intenta agregar un nuevo bloque de transacciones a la cadena de bloques, este nodo transmite el bloque a todos los nodos que forman la red. Sobre la base de la legitimidad del bloque (validez de las transacciones), los demás nodos pueden aceptar o rechazar el bloque. Cuando un nodo acepta un nuevo bloque de transacciones, lo guarda y lo almacena sobre el resto de los bloques que ya ha almacenado, actualizando toda la cadena. El funcionamiento de un nodo a grandes rasgos se pueden resumir en los siguientes puntos:

1. Comprueban si un bloque de transacciones es válido y lo aceptan o lo rechazan según esta validez.
2. Guardan y almacenan bloques de transacciones, manteniendo así una copia del historial de transacciones de la Blockchain a la que pertenezcan.
3. Transmiten este historial de transacciones al resto de nodos de la red que pueden necesitar sincronizarse con la cadena de bloques actual debido a que su historial esté desactualizado.

Según la cantidad de información que poseen, podemos clasificar los nodos de una red Blockchain en diferentes tipos:

- **Nodos completos**: Son los que realmente admiten y proporcionan seguridad a la red y son indispensables para la misma. Son los encargados de comprobar cada bloque dentro de la cadena y verificar que este cumpla con las normas y los parámetros establecidos para poder incorporarse. Este tipo de nodo tiene la potestad de rechazar una transacción que no cumpla con cualquiera de las normas previamente establecidas en la red. Cuando instalas un software de nodo completo (como Bitcoin Core, en el caso de la red Bitcoin), además de disponer del monedero más seguro, estarás descargando una copia completa de la Blockchain y pasará a ser un nodo más de la red. Así, emitirás tus transacciones, propagarás las emitidas por el resto de nodos y comprobarás que se cumplen con las reglas de consenso específicas de cada red.
- **Nodos livianos o parciales**: Estos no almacenan toda la información, como los nodos completos, por lo que no son tan seguros como estos y tampoco son completamente independientes, lo cual los hace más vulnerables ante ataques, llegando a aprobar transacciones que realmente no cumplían con todos los protocolos de seguridad de la red. Es por esta razón que todas las transacciones deben pasar por nodos completos, ya que son estos los que disminuyen la vulnerabilidad de la red. Por tanto, podemos decir que estos nodos solo emiten transacciones y reciben la información de la Blockchain de manos de un tercero. Siguen lo que les dicta la mayoría de los nodos y son conocidos como “monederos ligeros”, más usados en dispositivos móviles o simplemente por personas que no tienen la necesidad de descargarse la Blockchain al completo.

Una vez que tenemos el concepto más claro, podemos pasar a hablar sobre la seguridad que los nodos proporcionan a la red. Los nodos pueden estar online u offline dependiendo de si están recibiendo, guardando y transmitiendo los últimos bloques de transacciones desde y hacia otros nodos o no. Lo primero que debe hacer un nodo que ha estado offline durante un tiempo es ponerse al día con el resto de la cadena de bloques, actualizando así la que contenía antes de la desconexión del nodo, y efectuando la sincronización con la cadena de bloques actual de la red.

Teóricamente, una Blockchain completa puede ejecutarse en un solo nodo lo cual conlleva un serio problema de seguridad, dado que al ejecutarse en un solo dispositivo sería vulnerable a situaciones

como cortes de energía, piratas informáticos o fallas del sistema. Esto nos conduce a la conclusión de que cuanto más nodos ejecuten la red Blockchain, esta será más segura y mejor será su capacidad de recuperación ante tales catástrofes. Cuando los datos de la red se distribuyen en tantos dispositivos, será extremadamente difícil para una entidad corrupta borrar o modificar todos los datos a la vez. Incluso si una gran cantidad de nodos se cae repentinamente y se vuelven inaccesibles debido a una gran crisis global, teóricamente un solo nodo podría mantener operativa toda la cadena de bloques de la red. E incluso si todos los nodos se desconectasen, teóricamente solo se necesita un nodo con el historial completo de Blockchain para volver a estar en línea y hacer que todos los datos sean accesibles de nuevo para todos los nodos.

A pesar de todo, los nodos pueden sufrir ataques, por ejemplo, un “pirata informático” puede romper la seguridad de un software en cuestión sin necesidad de alterar los datos contenidos en la Blockchain, redirigiendo la información o ganancias de dichos nodos a direcciones distintas a las programadas por sus dueños. Este es uno de los ataques más comunes a este tipo de software denominados “stealing address” (que profundizaremos más adelante), y es por ello que los desarrolladores de las diferentes Blockchain instan a sus usuarios a mantener actualizadas las versiones del software utilizado por la red.

4.3. Transacciones

Como ya sabemos, las **transacciones** son una parte fundamental dentro de una cadena de bloques ya que todo lo que rodea a la cadena está diseñado para asegurar que las transacciones puedan ser creadas, propagadas por la red, validadas y añadidas al registro o cadena de bloques.

Las transacciones son agrupaciones de datos con firma digital que almacenan las transferencias de datos entre los remitentes (conocidos como entradas dentro de esas agrupaciones) y los destinatarios (salidas). Se transmiten a la red y, a medida que son validadas, se juntan y ordenan para formar los bloques de la Blockchain.

El **ciclo de vida de una transacción** comienza con la creación de la misma, que es luego firmada con una o más firmas indicando la autorización para gastar fondos o ejecutar cierto código en el contrato al que va dirigido. La transacción es entonces transmitida a la red, donde cada nodo participante en la red valida y propaga la transacción a los nodos a los que está conectado y así sucesivamente hasta que alcanza al resto de nodos en la red. Finalmente la transacción es procesada por los nodos mineros o validadores e incluida en un bloque de transacciones registrado en la cadena de bloques.

Cada Blockchain posee una estructura diferente para sus transacciones, de modo que no se puede definir una estructura de una transacción para Blockchain. Por ello existen diferentes **modelos de transacciones**.

Uno de estos modelos de transacciones, utilizado por Bitcoin y la mayoría de las Blockchains, es el **UTXO (Unspent Transaction Output)**. Una UTXO, o transacción pendiente de gasto, es una salida (de fondos) que un usuario recibe para poder gastar en el futuro como una entrada para alguien más. El balance total en la cartera de cualquier usuario está compuesto por UTXOs de distinto tamaño, o bien por una sola que puede recibir a cambio cuando es gastada a menos de su totalidad. Para verlo algo más claro, podemos pensar que las UTXO son el equivalente a monedas o billetes individuales dentro de la red. Tal como el sistema de dinero en efectivo está diseñado sólo con billetes o monedas de determinado valor (en el dólar, por ejemplo, sólo existen seis billetes distintos), que se combinan para formar nuevas cantidades o se entregan en su totalidad esperando recibir el remanente de la compra a cambio, en la Blockchain también se combinan distintas UTXO, o bien se otorga un cambio

a una UTXO más grande cuando se realiza una transferencia.

Por ejemplo, supongamos que tienes 100$ en Bitcoins dentro de tu cartera y necesitas pagar 45$. Como usuario común no lo ves a simple vista pero esos 100$ puede que estén conformados por varias UTXO: quizás dos de 50$, o cuatro de 25$. En este último caso, al realizar el pago de 45$, estarías enviando en realidad dos UTXO de 25$ cada una y recibiendo otra a cambio de 5$.

A diferencia el dinero en efectivo, además de los fondos que damos para un pago o una compra, debemos incluir también un pago de una comisión para quienes mantienen la red ayudando a validar las transacciones para incluirlas en nuevos bloques (los mineros de los que hablaremos después).

Por otro lado, Ethereum, en lugar de utilizar UTXO's, utiliza un modelo diferente, el **modelo basado en cuentas (Account Based Model)**. Este modelo es similar a como funciona el sistema de banca tradicional. Básicamente cada cuenta vive mediante transferencias directas de valor e información con transiciones de estado.

Este modelo puede ser explicado de una forma muy simple: supongamos que Bob y Alice son amigos y Bob quiere mandarle 5 tokens a Alice. Partimos de que Bob posee 10 tokens en su cuenta y Alice ninguno. Entonces, Bob le manda 5 de sus 10 tokens a Alice, de modo que Bob se queda con 5 tokens, el resto tras extraer los 5 que se envían a Alice. Finalmente, tanto Bob como Alice tienen 5 tokens cada uno. Cabe destacar que existen dos tipos de cuentas: cuentas de usuario controladas por clave privada y cuentas de usuario controladas por código de contrato (smart contracts). Y es por ésto que Ethereum utiliza este modelo basado en cuentas. Ethereum utiliza un lenguaje de programación completo (Solidity) y una de sus características principales son los smart contracts, obteniendo una mayor simplicidad utilizando este modelo sobre UTXO. Hay una gran cantidad de aplicaciones descentralizadas que poseen código y estado arbitrario y propio, es por ello que utilizar UTXO disminuiría la habilidad de ejecución de los smart contracts.

Cada una de estas cuentas tiene su propia contabilidad, almacenamiento y espacio de código para llamar a otras cuentas o direcciones. Una transacción será válida inicialmente si el remitente de la misma posee suficientes medios (fondos, por ejemplo) para pagar por ello.

Para hacernos una idea de la posible estructura de una transacción y entender mejor este concepto, veremos la composición de una transacción de la red Bitcoin y de la red Ethereum, ya que son las más conocidas y nos puede ayudar a notar las diferencias entre una Blockchain enfocada en criptomonedas y otra que implementa Smart Contracts.

4.3.1. Transacciones en Bitcoin

En esta famosa Blockchain de criptomonedas, una transacción se divide en tres partes:

- El encabezado: Que a su vez está compuesto por cuatro partes: el hash de la transacción, la versión del software que debería usarse para validar ese bloque, el número de entradas y salidas y una fecha o bien una altura de bloque (una de las dos) para indicar cuando fue añadida esa transacción a la cadena.
- Las entradas: Incluyen el hash de la salida previa apuntando hacia la o las UTXO disponibles, un índice de la lista de salidas de la transacción previa para identificar la que puede gastarse en la nueva entrada y el ScriptSig, un "programa simple" de desbloqueo que solicita cierta condición para acceder a los fondos. La condición principal en Bitcoin es la llave privada personal del destinatario.
- Las salidas: Incluyen el monto a pagar en satoshi (submoneda de Bitcoin) y el ScriptPubKey,

el par contrario al ScriptSig, que es el encargado de bloquear los fondos con la clave pública del destinatario para que sólo él pueda desbloquearlos después con su clave privada.

Una vez realizada la transacción, ésta se envía a los nodos mineros, que son los encargados de validarla, entre otros pasos, comparando ambos scripts.

4.3.2. Transacciones en Ethereum

El término transacción en Ethereum hace referencia a un paquete de datos firmados que almacena un mensaje enviado desde una cuenta externa (contratos inteligentes). Las transacciones contienen la siguiente información:

- El receptor del mensaje.
- La firma digital que identifica al emisor.
- La cantidad de fondos (en ether) que se transfieren desde la cuenta del emisor a la del receptor.
- Un campo opcional de datos.
- Un valor STARTGAS que indica el máximo número de pasos computacionales que se permite ejecutar a la transacción.
- Un valor GASPRICE, que representa el valor máximo que se desea pagar en forma de comisión por cada paso computacional.

Los tres primeros campos son prácticamente estándar y pueden encontrarse en cualquier Blockchain con monedas digitales (como hemos visto anteriormente para Bitcoin).

El campo de datos (PAYLOAD) de una transacción en Ethereum se usa para indicar a la EVM (Ethereum Virtual Machine) que ejecuta la transacción si debe transferir fondos, crear un nuevo contrato, ejecutar un contrato existente o realizar algún tipo de cálculo.

Ethereum introdujo el concepto de gas y por ello las transacciones incluyen los campos STARTGAS y GASPRICE. El concepto de gas en Ethereum se asemeja a la gasolina necesaria en un coche para funcionar, es una forma de pagar por tiempo de uso y recursos.

El gas fue introducido con una doble finalidad:

- Pagar a los minero por validar transacciones.
- Evitar que la ejecución de una transacción bloquee el sistema. Ésto se debe al hecho de que el lenguaje de programación en el que se programan los contratos de Ethereum es Turing completo (al contrario que Bitcoin, por lo que este concepto no es necesario) y podría darse el caso de que un contrato se ejecutará indefinidamente, con un bucle infinito por ejemplo, bloqueando así la red.
- Evitar que malos actores intenten saturar la red enviando una inmensa cantidad de transacciones haciendo que paguen por el uso del sistema.

Dado que las transacciones requieren de gas para ser ejecutadas en la red de Ethereum, Este gas se paga como comisión en forma de ether (la moneda de Ethereum) por el uso de la red. Las transacciones necesitan proveer gas suficiente para cubrir toda la computación y almacenaje requerida por la transacción. Si durante la ejecución de la transacción se requiere más gas de la cantidad máxima indicada, la ejecución será abortada y el contrato quedará en el mismo estado que estaba previo a la ejecución de dicha transacción. Es decir, las instrucciones enviadas con una transacción se ejecutan de forma atómica.

Además de la cantidad de gas máxima, el usuario debe indicar el precio que está dispuesto a pagar por cada unidad de gas. El precio indicado es importante porque hará que un minero esté dispuesto a procesar nuestra transacción antes o después de otras transacciones dependiendo del precio que estemos dispuestos a pagar.

Terminar diciendo que Ethereum además permite la comunicación entre contratos mediante mensajes. Un mensaje es un conjunto de instrucciones enviadas a un contrato desde otro contrato y es muy importante tener claro que un mensaje no constituye una transacción y es enviado cuando un contrato está siendo ejecutado por la EVM.

4.4. Firmas digitales (clave pública/privada, monederos/billeteras)

Un monedero es una cadena de números y letras del tipo: 18c177926650e5550973303c300e136f22673b74. Esta es una dirección que aparecerá en varios bloques dentro de la Blockchain cuando se realicen transacciones. No hay registros visibles de quién realizó qué transacción con quién, únicamente el "número" de monedero o billetera. La dirección de cada monedero en particular también es llamada una clave pública.

La criptografía de clave pública fue inventada en la década de 1970 y es la base matemática de la seguridad informática. Desde la invención de esta criptografía de clave pública, se han descubierto varias funciones matemáticas adecuadas, tales como exponenciación de números primos y multiplicación de curvas elípticas. Éstas funciones matemáticas son prácticamente irreversibles, lo cual significa que son fáciles de calcular en una dirección e inviables de calcular en la dirección contraria. Basada en estas funciones matemáticas, la criptografía permite la creación de secretos digitales y firmas digitales prácticamente infalsificables.

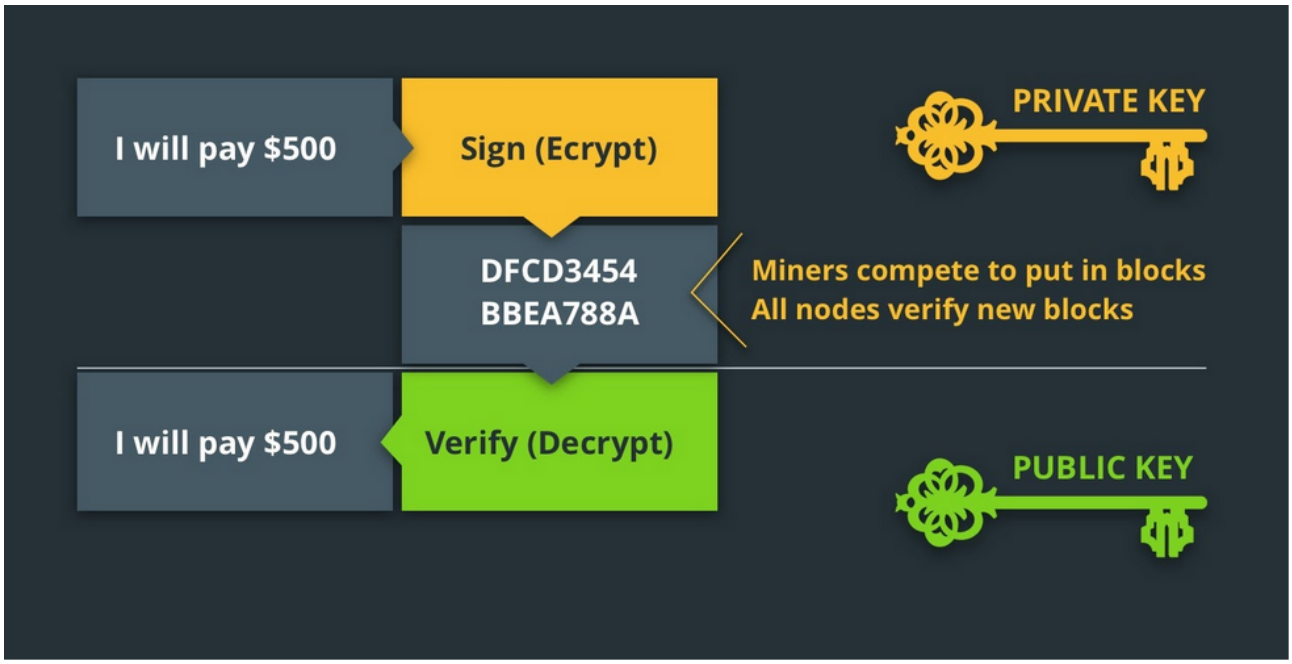
En la mayoría de Blockchain se utiliza la criptografía de clave pública. El par de claves consiste en una clave privada y una clave pública derivada de la privada. La clave pública se usa para recibir transacciones, y la clave privada para firmar transacciones y gastar los fondos asociados a la cuenta (en caso de haberlos). Lo verdaderamente potente de este concepto es que existe una relación matemática entre las claves pública y privada que permiten que la clave privada sea utilizada para generar firmas en mensajes. Estas firmas pueden ser validadas contra la clave pública sin necesidad de revelar la clave privada.

Cuando los fondos son gastados, el dueño actual de dichos fondos presenta su clave pública y firma (diferente cada vez, pero creada a partir de la misma clave privada) la transacción. A través de la presentación de la clave pública y firma, todos los participantes en la red pueden verificar y aceptar la transacción como válida, confirmando que la persona que transfiere los fondos los posee al momento de la transferencia.

Entonces, una **clave privada** es simplemente un número escogido al azar. La propiedad y control de una clave privada es la raíz del control del usuario sobre los fondos asociados con la dirección correspondiente. Se usa para crear las firmas requeridas para firmar transacciones demostrando la pertenencia de los fondos usados en una transacción. Por lo tanto, la clave privada debe permanecer en secreto en todo momento, ya que revelarla a terceros equivale a darles el control de la cuenta asegurada por dicha clave. También es conveniente hacer copias de respaldo de las claves privadas para protegerlas de pérdidas accidentales, ya que si se pierde no puede ser recuperada y los fondos asegurados por dicha clave se perderán para siempre.

La **clave pública** es generada a partir de la clave privada usando multiplicación de curva elíptica, la cual es irreversible: K = k * G donde k es la clave privada, G es un punto constante llamado el

punto generador y K es la clave pública resultante. La operación inversa, conocida como “búsqueda del logaritmo discreto”, es decir, calcular k a partir de K, es tan difícil como probar todos los valores de k, es decir, una búsqueda por fuerza bruta.



Una **dirección** es una cadena de dígitos y caracteres que puede ser compartida con cualquiera que desee enviarte transacciones (por ejemplo, en Bitcoin, las direcciones producidas a partir de una clave pública consisten en una cadena de números y letras, comenzando siempre por el dígito “1”). Esta dirección se obtiene a partir de la clave pública a través del uso de hashing criptográfico de sentido único, que comentaremos posteriormente.

En definitiva, para poder gastar/mandar transacciones desde una dirección necesitados demostrar que conocemos la clave privada, de la clave pública a la que se refiere dicha dirección. Y para poder demostrar que conocemos la clave privada sin revelarla públicamente es para lo que se utiliza la **firma digital**. Las firmas son elementos criptográficos que se calculan a partir de la clave privada y de una combinación de otra información incluida en la transacción. Es aquí donde entra en juego la magia de la criptografía, ya que gracias a ello es posible que una clave pública pueda usarse para verificar que dicha firma se ha creado usando la clave privada correspondiente. Además, permiten demostrar además del conocimiento de la clave privada, que el poseedor de la misma confirma los datos de dicha transacción. Por lo tanto, cada firma es únicamente válida para una transacción específica.

Por lo tanto, el dueño de la clave privada puede firmar una transacción y gastar fondos sin preocuparse de que nadie vaya a conocer su clave privada porque la clave privada en sí nunca queda expuesta públicamente y es prácticamente imposible de averiguar. La firma y la clave pública de la dirección de la que se envía la transacción se añaden al campo de inputs de la transacción, esto demuestra que el propietario de la clave privada tiene realmente la intención de efectuar esa transacción y se asegura de que no puede ser alterada.

4.4.1. Hash: funciones criptográficas

Hash es el nombre utilizado para identificar un tipo de función criptográfica utilizado en Blockchain (entre otros). Una función hash es un algoritmo que posee una serie de propiedades muy útiles para el cifrado de datos. ¿En qué consiste una función de este tipo?

Entender estas funciones es relativamente sencillo, pero veamos sus propiedades primero:

- **Eficiente computacionalmente**. Este es un requisito esencial ya que un ordenador debe ser capaz de resolver una función hash en un corto periodo de tiempo.
- **Determinismo**. Las funciones hash deben ser determinista, es decir, dada una entrada, siempre debe obtenerse el mismo resultado. Obviamente, si tenemos una entrada pero nos da varias salidas diferentes, validar si esa entrada ha sido modificada o no, sería imposible.
- **Pre-imagen resistente**. Esto quiere decir que una salida de una función hash no debe revelar nada acerca del contenido de la entrada. Dicha entrada puede ser cualquier cosa: números, letras, palabras completas y un largo etc. A pesar de ello, la salida será una combinación alfanumérica de una longitud fija, evitando dar pistas de la longitud de la entrada.
- **Resistente a colisiones**. Esto quiere decir que debe ser imposible obtener la misma salida de dos entradas diferentes. De todos modos, la salida es de una longitud fijada, de modo que hay un límite de salidas (a pesar de que es una cifra muy elevada) que pueden ser producidas por una función hash, de modo que, estadísticamente hablando, más de una entrada, producirá la misma salida.
- **Imposible aplicar ingeniería inversa**. Debe ser imposible utilizar esta técnica para revertir el proceso matemático que crea la salida. No existe la una función inversa para las funciones hash.

Las funciones hash son llamadas **funciones unidireccionales** porque, como hemos visto en las propiedades, no puede ser reversible. La forma más simple de presentar una función unidireccional serían por ejemplo las funciones modulares (de la forma X mod Z = Y). Tomemos de ejemplo la ecuación X mod 5 = Y, obtendremos:

Entrada (X)	0	1	2	3	4	5	6	7	8	9	10
Salida (Y)	0	1	2	3	4	0	1	2	3	4	0

Como podemos ver, el patrón es muy sencillo de averiguar ya que solo hay 5 posibles opciones, la cuales rotan hasta el infinito. Todo esto es importante porque tanto la función como la salida pueden hacerse públicas pero nunca será posible obtener la entrada asociada siempre y cuando, en la función utilizada de ejemplo, se mantenga en secreto el número elegido como 'X'.

Por ejemplo, si X = 17, el resultado es 2. Ahora publicamos nuestra función X mod 5 = Y, y que el resultado que nos da es 2. Nadie podría ya que hay una cantidad infinita de posibles X que nos den 2 como resultado: 7, 52, 3492... Podemos ver que es un proceso irreversible que, aplicado a funciones más sofisticadas y mayores valores, se convierte en una tarea imposible el averiguar la entrada.

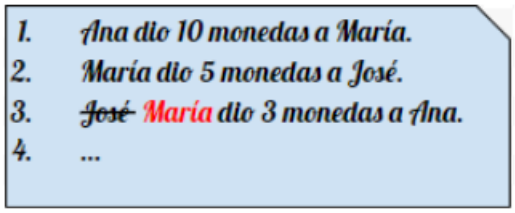
Dentro de las funciones hash podemos encontrar muchas clases, siendo las más comunes:

- **SHA**: Algoritmo de hash seguro (del inglés: Secure Hashing Algorithm) (SHA-2 y SHA-3).
- **RIPEMD**: Resumen de mensajes de evaluación de primitivas de integridad RACE (del inglés: RACE Integrity Primitives Evaluation Message Digest).
- **MD5**: Algoritmo de resumen de mensaje 5 (del inglés: Message Digest Algorithm 5).
- **BLAKE2**

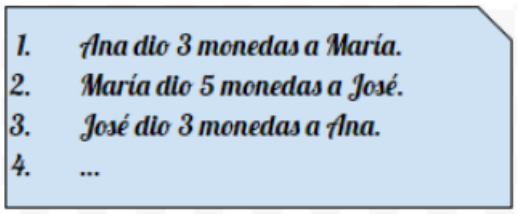
Todas ellas son similares entre sí, pero con ciertas diferencias en cuanto a cómo el algoritmo genera un resumen o salida dada una entrada, además de diferir en las tamaños de las salidas.

Una vez entendido el concepto de función Hash veremos, mediante un ejemplo con intercambio de monedas, como se aplica en Blockchain.

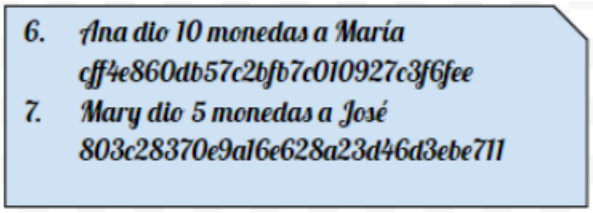
Partimos de un grupo de personas que deciden hacer una moneda ajena a cualquier otra para ellos. Para tener un seguimiento, uno de ellos, llamado Bob, decide llevar una contabilidad en un diario:



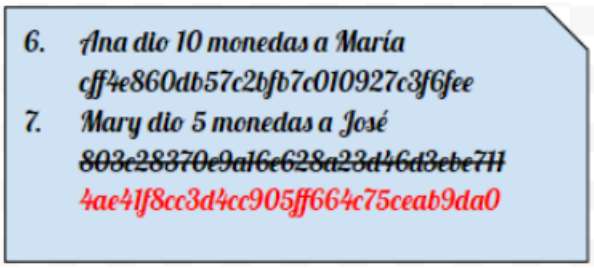
Uno de ellos, José, quería robar dinero, para ello modificó el diario:



Evidentemente, Bob, el contable, nota que alguien había modificado el diario. Para evitar ello, decide utilizar una cosa muy útil llamada función hash, que convierte el texto en un aparente sinsentido de letras y números. Entonces Bob añade a cada nuevo registro en el diario, un hash:



José decide cambiar de nuevo algunos registros. De noche, coge el diario, cambia el registro y genera un nuevo hash:



De nuevo, Bob, notó cambios y por lo tanto, decidió añadir un extra de seguridad, cada nuevo hash, será generado a partir del nuevo registro y el hash del registro anterior:

Entrada	Hash
Ana dio 10 monedas a María	8977e7c112aea5b0a62e9c5f30840203
María dio 5 monedas a José 8977e7c112aea5b0a62e9c5f30840203	e37a8d1cc39ed9f54afadb6c6cafe139
María dio 3 monedas a Ana e37a8d1cc39ed9f54afadb6c6cafe139	5b9f0e325f58766f5a2dfe7eec623f6d
Ana dio 1 moneda a Andrés 5b9f0e325f58766f5a2dfe7eec623f6d	55f28e65412b22aa3d6002bcf7d67201

Ahora, para que José haga trampas, debería cambiar el Hash en todas las entradas siguientes, ya que sus hashes dependen del mismo. Pero como José quiere más dinero, se pasó toda la noche haciendo las modificaciones pertinentes.

Aquí entra en juego un nuevo concepto: **Nonce**. Este es el nombre que se le da a un número que se añade al registro el cual provoca que el hash generado tenga una terminación deseada, en este ejemplo, el nonce será un número el cual provocará que el hash termine en dos ceros.

Entrada	Hash
Ana dio 10 monedas a María 451	219711e62645a21f2742ada2c6f2a900
María dio 5 monedas a José 13 219711e62645a21f2742ada2c6f2a900	1cc4c07fa0757848b439e2396ce87d00
María dio 3 monedas a Ana 1cc4c07fa0757848b439e2396ce87d00	e43aa132f4b67c65ba6914824a39b3900
Ana dio 1 moneda a Andrés e43aa132f4b67c65ba6914824a39b3900	99012fe16897c1946594 1d3530afa900

Ahora, la falsificación de registros es muy difícil, y no solo para una persona, si no también para una máquina, ya que no pueden descifrar el nonce rápidamente.

En conclusión, una función hash es una función de sentido único que produce una huella o “hash” a partir de una entrada de tamaño arbitrario y se usan extensivamente en Blockchain para:

- Obtención de una dirección a partir de una clave pública como se ha descrito anteriormente.
- Durante el minado, en la prueba de trabajo para ganar el reto (en caso de usar este algoritmo de consenso que describiremos posteriormente).
- Para generar árboles Merkle que se incluyen en los bloques minados y que se explicarán también posteriormente.

4.5. Métodos de consenso

Los métodos de consenso son el mecanismo a través del cual una red Blockchain alcanza un acuerdo. Este consenso se lleva a cabo entre los distintos participantes (nodos) de la red Blockchain sobre las transacciones que van a escribirse en la cadena, debido a que no dependen de una autoridad central, es decir, el consenso es el responsable de que todos los nodos de la Blockchain tengan los datos verificados, evitando a su vez su manipulación. Es aquí donde los algoritmos de consenso entran en juego, encargándose de asegurar que las reglas del protocolo son respetadas y garantizando que todas las transacciones tienen lugar de una forma fiable.

Es importante entender la diferencia entre un algoritmo y un protocolo, ya que a menudo ambos términos son utilizados de forma indiferente, sin embargo, no se tratan de lo mismo.

- **Protocolo**: reglas primarias de una Blockchain.
- **Algoritmo**: mecanismo a través del cual el protocolo será seguido.

La red siempre funcionará sobre un protocolo que definirá la forma de funcionamiento del sistema, haciendo que tanto los elementos como los participantes de la red tengan unas reglas fijas que seguir. Teniendo este protocolo, el algoritmo se encarga de decirle al sistema qué y cómo se puede hacer algo de modo que se produzcan los resultados deseados. En una Blockchain, estos algoritmos determinan la validez de las transacciones y los bloques. Proof of Work y Proof of Stake son los dos ejemplos más característicos de algoritmos de consenso, mientras que Bitcoin y Ethereum serían protocolos.

4.5.1. Proof of Work

Fue el primer algoritmo de consenso que apareció, remontándose 20 años atrás con la aparición de Hashcash, que fue una propuesta realizada por Adam Back en 1997 para combatir el correo basura o spam, el cual inspiró el mecanismo de prueba de trabajo usado en Bitcoin. Consiste en un mecanismo rápido de verificación en el que el remitente del mensaje tiene interés suficiente en dicho envío como para “pagar” con tiempo de CPU para poner una marca que demuestre que se manda por algún motivo.

Este pago con tiempo de CPU consiste en la realización de complejas operaciones de cómputo que después, son verificadas por la red. La principal característica de esta esta estrategia es su asimetría. La prueba de trabajo del cliente es ciertamente complicada, mientras que la verificación por parte de la red es sencilla. Es decir, se tarda en producir y es computacionalmente costoso, pero la verificación es sencilla, ya que la prueba diseña patrones que facilitan la verificación.

El funcionamiento de este algoritmo se puede separar en distintas etapas:

- **Etapa 1**: En el momento en el que el nodo se conecta a la red, ésta le asigna una tarea computacionalmente costosa que debe ser resuelta con el fin de obtener incentivos.
- **Etapa 2**: Se procede a la resolución de la tarea, lo cual necesita de mucha potencia de computación. A este proceso se le conoce como minería.
- **Etapa 3**: Resuelta la tarea, la solución se comparte con la red para ser verificada, comprobando que la tarea cumple los requisitos exigidos.Tiene acceso a los recursos de la red si los cumple o, por el contrario, es rechazado tanto el acceso a la red como la solución a la tarea. Aquí entra el juego el concepto de **protección contra el doble gasto**. Esta protección evita que, una vez presentada y verificada una tarea, esta sea utilizada más de una vez.
- **Etapa 4**: Con la confirmación de que la tarea se ha cumplido, el cliente consigue acceso a la red y sus recursos, recibiendo una ganancia por el trabajo computacional realizado.

4.5.2. Proof of Stake

Es un protocolo de consenso creado para reemplazar al conocido Proof of Work aportando una mejor seguridad y escalabilidad a las redes que lo implementen.

A los nodos que minan en PoS se les llama validadores. La decisión sobre qué nodo ha de validar un bloque se hace de forma aleatoria pero dando mayor probabilidad a quienes cumplan una serie de criterios. Entre estos criterios podemos mencionar la cantidad de moneda reservada y el tiempo de participación en la red, pero pueden definirse otros. Una vez establecidos, se inicia el proceso de selección de nodos de forma aleatoria. Una vez terminado el proceso de selección, los nodos elegidos podrán validar transacciones o crear nuevos bloques.

Esto revela que Proof of Stake es un proceso completamente distinto al conocido protocolo de Prueba de Trabajo (PoW). Donde cada uno de sus nodos realizan un arduo trabajo de cómputo para resolver acertijos criptográficos. Lo que significa que PoW, a diferencia de PoS, necesita de grandes cantidades de energía y equipo especializado para realizar sus operaciones. En PoS, por el contrario, esto no es necesario. En PoS el proceso es mucho más sencillo y energéticamente amigable. Son estas razones por la que muchos proyectos Blockchain en la actualidad se interesan por este nuevo protocolo.

El funcionamiento de este protocolo de Prueba de Participación es bastante particular. Este sistema busca incentivar a los participantes para que posean en todo momento, una determinada cantidad de monedas. La posesión de monedas, les permite ser elegidos por el proceso de selección aleatoria que se realiza para designar tareas. Bajo este esquema, aquellos que tengan más reservas, tienen mayor peso en la red y mayores oportunidades de ser elegidos. Una vez elegidos pueden validar transacciones y crear nuevos bloques dentro de la red. Permitiéndoles recibir ganancias e incentivos por el trabajo realizado.

Vistos estos dos ejemplos más característicos cabe mencionar otro tipo de algoritmos los cuales surgieron a raíz de estos, como el siguiente descrito.

4.5.3. Obelisk

Este algoritmo presenta como principal objetivo el eliminar las deficiencias de los algoritmo previamente descritos. Esto hace posible que una Blockchain se mantenga distribuidamente sin necesidad de participación y tanto poder de cómputo. Se reduce la necesidad de minería, mejorando la velocidad de las transacciones y su seguridad. Distribuye la influencia en la red de acuerdo a un concepto denominado **“red de confianza”**, donde la densidad de la red de suscriptores de un nodo determina su influencia en la cadena. Como ejemplo de uso nos encontramos con el proyecto SkyCoin.

4.6. Minería

Dentro de Blockchain, la **minería** es la parte encargada de permitir que la red funcione de una forma descentralizada de igual a igual, sin necesidad de una autoridad controladora. Este proceso consiste en verificar las transacciones entre usuarios y agregarlas a la cadena que conforma la red. Además, es un proceso que se utiliza para introducir nuevas monedas, en caso de criptomonedas, por ejemplo.

Su funcionamiento consiste en que un nodo minero en la red recopila transacciones y trabaja para organizarlas en bloques. Cada vez que se realizan transacciones, los nodos mineros reciben y verifican las transacciones, las agregan a la agrupación de memoria y comienzan a ensamblarlas en un bloque de transacciones múltiples.

Antes de comenzar el proceso, al nuevo bloque se añade la primera transacción conocida como la transacción coinbase, que es una transacción cuyo valor base es el equivalente al de la recompensa activa en ese momento por la minería de dicho bloque. Es por esto que son llamadas **transacciones generadoras**, pues la recompensa por añadir dicha transacción al nuevo bloque, es una recompensa "virgen" que en el caso de criptomonedas, por ejemplo, se trata de nuevas monedas que no están en circulación. Así, una transacción coinbase, contiene única y exclusivamente nuevas monedas que nunca han estado en la blockchain.

Una vez que se ha hasheado cada transacción, estos hashes se organizan en algo llamado *árbol Merkle* o *árbol hash*, lo que significa que los hashes se organizan en pares y se concatenan hasta que se alcanza "la parte superior del árbol", también llamado *hash raíz* o una *raíz de Merkle*.

El hash raíz junto con el hash del bloque anterior y un número aleatorio llamado nonce se colocan en el encabezado del bloque. El encabezado de los bloques se procesa como un hash y produce una salida que servirá como identificador de los bloques.

El identificador de bloques debe ser menor que un determinado valor objetivo establecido por el protocolo. En otras palabras, el hash de encabezado de bloque debe comenzar con un cierto número de ceros.

Este valor objetivo, también conocido como la dificultad de hash, se escala, asegurando que la velocidad a la que se crean los nuevos bloques se mantenga proporcional a la cantidad de poder de hashing en la red.

Los mineros mantienen el hash del encabezado una y otra vez mediante la iteración a través del nonce hasta que un minero en la red finalmente produce un hash válido. Cuando se encuentra un hash válido, el nodo fundador transmitirá el bloque a la red. Todos los demás nodos comprobarán si el hash es válido, agregarán el bloque a su copia de la cadena de bloques y continuarán con la minería del siguiente bloque.

Sin embargo, a veces sucede que dos mineros emiten un bloque válido al mismo tiempo y la red termina con dos bloques en competencia. Los mineros comienzan a explotar el siguiente bloque basándose en el bloque que recibieron primero. La competencia entre estos bloques continuará hasta que el siguiente bloque se mine según uno de los bloques competidores. El bloque que se abandona se llama bloque huérfano o bloque obsoleto. Los mineros de este bloque volverán a minar la cadena del bloque ganador.

Cabe destacar los grupos de minería, ya que mientras que la recompensa en bloque se otorga al minero que descubre el hash válido primero, la probabilidad de encontrar el hash es igual a la porción del poder minero total de la red. Los mineros con un pequeño porcentaje del poder minero tienen una probabilidad muy pequeña de descubrir el siguiente bloque por su cuenta. Los grupos de minería se crean para resolver este problema, lo que significa que los mineros, que comparten su poder de procesamiento a través de una red, comparten la recompensa por igual entre todos los miembros del grupo, de acuerdo con la cantidad de trabajo que contribuyen a la probabilidad de encontrar un bloque.

4.7. Sumario

1. Si un usuario de la Blockchain posee activos digitales, entonces, necesariamente tendrá un "monedero".

2. Un monedero es una dirección en la Blockchain, es decir, una llave/clave pública de la misma.

3. Un usuario que desee realizar una transacción debe enviar un mensaje con la transacción firmada con su clave/llave privada.

4. Antes de que se apruebe dicha transacción, ésta será revisada por cada nodo que la “vota” según el algoritmo de consenso (o protocolo) implementado por esta Blockchain.

5. La transacción es colocada en la cadena de bloques por los nodos mineros que validan con sus “votos” la transacción.

6. Los equipos de la red que sostienen la Blockchain se denominan nodos (como hemos visto, por lo general, no todos los nodos son iguales).

7. Los mineros colocan las transacciones en bloques en respuesta a los desafíos de prueba de trabajo (es decir, algoritmo de consenso que se haya superado implementado en dicha Blockchain, gracias a los que se produce la interacción).

8. Por lo general, después de que los mineros cierran con éxito un bloque de transacciones, reciben una recompensa por el trabajo realizado (debido a que el costo computacional es realmente alto para hacerlo “gratis”).

9. Un bloque contiene una marca de tiempo, una referencia al bloque anterior, las transacciones y el problema de cómputo que tuvo que ser resuelto antes de que el bloque se incluyera a la cadena de bloques o Blockchain.

10. La criptografía es esencial en las Blockchain para frustrar a los ladrones que quiesieran “hackear” la red. Éstas claves suelen estar hechas por generadores o keygens. que utilizan matemáticas muy avanzadas que involucran números primos para crear claves.

11. La red distribuida de nodos que necesitan llegar a un consenso definido por el protocolo de la red hace que el fraude sea prácticamente imposible dentro de la red Blockchain.

5. Debilidades

5.1. Fallas Bizantizas

Este es uno de los conceptos más importantes de la Blockchain. Sin la tolerancia a fallas bizantinas no sería posible esta tecnología tal y como la conocemos.

El término de falla bizantina, se deriva del Problema de los Generales Bizantinos. Es un problema lógico que supone, en resumidas cuentas, que los actores deben acordar una estrategia concertada para evitar una falla catastrófica del sistema. El problema viene cuando existe la posibilidad de que los actores que conforman el sistema puedan ser no confiables. Ante este hecho, el sistema debe crear los mecanismos necesarios que garanticen que esos actores maliciosos no puedan conducir a la falla sin más remedio. La creación de estos mecanismos de seguridad son los que precisamente otorgan la tolerancia a las fallas bizantinas.

Este es uno de los desafíos más complicados no solo de la tecnología Blockchain sino de cualquier sistema informático distribuido. Hasta el punto en que el primer diseño en resolverlo de forma satisfactoria fue la Blockchain de Bitcoin, de Satoshi Nakamoto, lo cual marcó un hito que acompaña a la tecnología Blockchain hasta nuestros días.

En concreto, la **Tolerancia a Fallas Bizantinas** es la capacidad de un sistema informático distribuido de soportar las llamadas fallas bizantinas, que pueden ser:

- Fallas de consenso.
- Fallas de validación.
- Fallas de verificación.
- Fallas de verificación de datos.
- Fallas en el protocolo de respuesta frente a situaciones comprometidas de la red.

Esta tolerancia está ligada a la capacidad de que la red, entendida como un todo, pueda crear un mecanismo general de consenso con la finalidad de dar una respuesta coherente ante una falla del sistema.

Esto se consigue mediante la definición de un conjunto de reglas que permite resolver el complejísimo Problema de los Generales Bizantinos de forma satisfactoria. En las Blockchain (públicas por lo general) ésta tolerancia se considera un requisito y para poder alcanzarlo, un sistema o algoritmo tolerante a fallos bizantinos debe cumplir al menos con lo siguiente:

1. Se debe iniciar cada proceso con un estado no decidido (ni SI ni NO): En este punto la red propone una serie de valores determinísticos aplicables al proceso.
2. Para compartir valores, se debe garantizar un medio de comunicación: Con el fin de desplegar mensajes de forma segura, por lo que el medio también servirá para comunicar e identificar de forma inequívoca las partes involucradas.
3. Los nodos computan los valores y pasan a un estado decidido (SI o NO): Cada nodo debe generar su propio estado, el cual es parte de un proceso puramente determinista.
4. Una vez decididos, totalizan y gana el estado con mayor cantidad de decisiones a favor.

Pongamos un ejemplo simplificante de lo anterior, aplicado a la Blockchain de Bitcoin por ejemplo:

Imaginemos que Pablo realiza una transacción en Bitcoin. Cada nodo en la red, comienza a compilar la transacción en un estado no decidido (transacción no confirmada). Como hemos visto la confirmación de esa transacción pasa por un trabajo de minería (aplicando el protocolo de consenso de la Blockchain). El proceso de minería, verifica que el hash de la transacción sea correcta y lo incluye en un bloque. Este proceso de verificación es intensivo en cálculos y solo es posible por medios determinísticos. Con cada nueva confirmación (estado decidido) de la transacción dada por la mayoría de la red, Pablo puede estar seguro de que la transacción ha sido tomada como válida.

La tolerancia a fallas bizantinas tiene la capacidad de resolver diversos problemas en diferentes casos de uso como pueden ser: compiladores de software, sistemas de almacenamiento de datos, sistemas de aviónica, protocolos de consenso en redes Blockchain, etc.

Cabe destacar este último aunque consideremos todos de igual importancia, debido a que los protocolos de consenso en Blockchain como PoW en Bitcoin permiten alcanzar a una red distribuida un consenso en condiciones bizantinas. Cuando Satoshi Nakamoto diseñó Bitcoin, tomó en cuenta este tipo de tolerancia, creando una serie de reglas y aplicó el PoW para crear un software con tolerancia a estas fallas. Sin embargo, esta tolerancia no es del 100 %. Pese a ello, PoW ha demostrado ser una de las implementaciones más seguras y confiables para redes Blockchain. En este sentido, el algoritmo de consenso de prueba de trabajo, es considerado por muchos como una de las mejores soluciones para las fallas bizantinas. PoS y DPoS por su parte no son completamente tolerantes a fallos bizantinos, razón por la cual suelen complementarse con otras medidas de seguridad.

Para concluir esta debilidad (o en algunos casos virtud) veremos sus ventajas y desventajas:

En las ventajas cabe destacar: la capacidad para garantizar correctitud de datos e información en sistemas distribuidos, solución al problema de procesamiento de información en ambientes heterogéneos, alta eficiencia en términos computacionales y energéticos, ofrece implementaciones que impactan positivamente en la escalabilidad si son bien construidas y mientras más nodos aplicando la tolerancia a fallos bizantinos mejor y más seguro será el modelo.

Entre las desventajas que podemos encontrar tenemos que la creación de estas soluciones es bastante compleja lo que puede incurrir en otros problemas de seguridad con su implementación y que garantizar su correcto funcionamiento requiere de que la distribución del sistema sea creciente, es decir, mientras más nodos aplicando el proceso, más seguro será, lo cual también tiene un impacto negativo en la escalabilidad y el ancho de banda de la red.

5.2. Ataque del 51 %, dispositivos ASIC y ataque del doble gasto

Un **ataque del 51 %** sobre una red Blockchain ocurre cuando una entidad toma el control de más del 51 % de la red, convirtiéndose en su centro y tomando el control sobre ella rompiendo las características de descentralización y seguridad que ésta proporciona. Si una sola entidad controla el 51 % de la capacidad de decisión de la Blockchain, tiene autoridad sobre ella durante el tiempo que la controle.

Las dos principales características detrás de un ataque de este tipo son la existencia de fallos de seguridad concretos que simplifican el proceso para el atacante y la manera de validar los bloques, es decir, el tipo de algoritmo de consenso que usa la red.

Un ejemplo de lo que puede hacer alguien con el 51 % de la red es el **ataque del doble gasto**: se envía un pago con una transacción y justo antes empiezan a minar bloques en secreto. La tran-

sacción es validada por toda la red y llega a su destino, con el pago aceptado como tal. Una vez lo que se haya comprado esté asegurado, el atacante hace pública la cadena de bloques que minó en secreto (también llamado **shadow mining** o minería en la sombra). Al tener el 51 % de la red, esa cadena de bloques será validada por el resto de la red, en una especie de proceso democrático explicado con anterioridad. Al ser aceptada, la transacción que se hizo justo después desaparecerá, y el dinero del pago volverá al atacante, que podrá gastarlo otra vez. Además, reescribirán todos los bloques posteriores, en lo que se conoce como reorganizaciones de cadena profunda o **deep chain reorganizations**, lo que suele ser un auténtico caos para los usuarios de la red.

Los dos ataques más importantes de este tipo fueron contra la Blockchain de Verge que fue atacado en al menos dos ocasiones y el que más destaca por su popularidad, el ataque sufrido por Bitcoin Gold en mayo de 2018, cuando en uno de los forks de Bitcoin, el atacante hacía gastos por valor de 18 millones de dólares que luego eliminaba de la red. En total el atacante vendió Bitcoin Gold y volvió a recuperarlos 76 veces antes de que se detuvieran las transacciones con este activo.

En este enlace se mantienen actualizados los costes en dólares de controlar el 51 % de la red en una serie de Blockchains. Dado que el coste en hardware de estas operaciones es muy alto y haría la operación muy costosa, se incluye el tanto por ciento que podría alquilarse a través del servicio más popular de poder de minado NiceHash, donde cualquier persona puede alquilar la capacidad de minar en las principales Blockchain, o de ceder recursos recibiendo pagos por ello.

En el caso de Bitcoin el tanto por ciento de poder de minado que puede conseguirse con NiceHash es virtualmente cero, ya que su red es demasiado grande, y controlar un tanto por ciento significativo (más del 50 %) tendría un coste hardware inmenso. En menor medida, la situación es parecida con casi todas las Blockchain relativamente conocidas. Pero esto es mucho más preocupante para Blockchain pequeñas ya que por cantidades a menudo ínfimas se puede controlar la red. Pero si el mercado no es muy grande tampoco será rentable para el atacante. Son las monedas con fuerte potencia en el mercado pero pocos mineros, o un algoritmo de cifrado mejorable las que más tienen que perder por este tipo de ataques.

Algunos de los mecanismos de defensa contra estos ataques son: la modificación del protocolo de consenso, la desincentivación y en el que nos centraremos ahora, el cifrado y resistencia a **dispositivos ASIC** (Application Specific Integrated Circuits).

La idea es combatir la centralización del minado, lo cual actualmente se consigue a través de estos dispositivos hardware contra los que no existe competencia alguna. Estos dispositivos son diseñados para un propósito único, un único cálculo en el que son mucho mejores que cualquier dispositivo genérico (como una CPU o algo más eficiente como una GPU), incluso los más potentes supercomputadoras no pueden competir con un pequeño grupo de ASICs operando en paralelo. Están específicamente creados para minar un algoritmo de cifrado concreto, lo cual es extremadamente más eficiente.

Esto es completamente legal, y además tiene un grave riesgo el montar una granja con estos dispositivos de minado hardware si se hace a pequeña escala: si el valor de la Blockchain baja, el beneficio bajará mucho pero el coste del hardware y de la electricidad que consume será el mismo. Además, un fork en la red puede actualizar el mecanismo de cifrado y hacer que todas las ASICs fabricadas para ello se vuelvan completamente inútiles.

Todo esto hace que los tokens que se minan con ASIC tiendan a concentrarse en un pequeño grupo de mineros, y una fuerte inversión puede permitir a un pequeño grupo dominar la red. Esto afecta a casi todas las Blockchain que funcionan con PoW, empezando por Bitcoin y Ethereum.

Ante esto tenemos varias soluciones:

- La primera es la creación de algoritmos de cifrado específicamente diseñados para no poder minarse con un ASIC. Son los algoritmos y tokens denominados ASIC-resistentes.
- La segunda es la realización de forks frecuentes pero por sorpresa, para desincentivar a la red. Y sobre todo al anunciarse un dispositivo cuyo objetivo es tu red (mayor problema es cuando no se anuncian y se desarrolla y pone en funcionamiento el hardware en secreto, como ocurrió con Monero).

Es habitual combinar las dos cosas. La lista de Blockchain que han implementado algoritmos para solucionar estos es muy larga y podemos encontrar en ella a Ethereum y Bitcoin Gold, entre otras.

Por todo ello, en el mundo de Blockchain, se dice que la resistencia a ASICs es prácticamente imposible al 100 %.

5.3. Robo de direcciones

A pesar de la seguridad que tiene la red debido a la encriptación, redundancia de datos y demás sistemas de protección mencionados en este documento, los equipos informáticos no dejan de ser vulnerables a ataques, de modo que al igual que un atacante puede forzar un sistema para obtener acceso a una cuenta en una red social, el software cliente de una Blockchain también puede ser atacado, de modo que ese nodo tendría un funcionamiento que la red no desea. En este caso, sin necesidad de alterar la cadena, se pueden redireccionar los beneficios de un nodo minero, por ejemplo, llevando esos beneficios a direcciones distintas a las programadas por sus dueños. Estos ataques son de los más comunes que sufren este tipo de software.

5.4. Vulnerabilidades software en Smart Contracts: caso DAO

Ya se ha hablado en este documento de que son y cómo funcionan los Smart Contracts, que a grandes rasgos son programas software que se ejecuta de forma transparente al usuario y que, básicamente, dice que “si algo pasa, se haga esto otro”, por lo que finalmente no pueden evitar tener fallos en el software. La red Ethereum, como hemos expuesto, utiliza smart contracts.

Un caso muy famoso con el que ilustrar estas vulnerabilidades es “el caso DAO”. “The DAO” es una organización creada por un grupo de desarrolladores liderado por Christoph Jentzsch. Esta organización creó un Smart Contract que fue desplegado sobre la red Ethereum, de modo que cualquiera pudiera vincular Ethers a él, algo que hicieron varios miles de personas a nivel mundial, con la intención de utilizarlo como un ahorro o inversión a largo plazo.

“The DAO” se regía por su código, siendo este la ley y este programa marcaba las normas de todo lo que se puede hacer o dejar de hacer. Todas las personas que utilizaron “The DAO” aceptaron el código fuente abierto de este programa, tanto como las normas a cumplir. Como se ha mencionado, al fin y al cabo es software, y ninguna de estas personas se percató de un error en el código. Sin embargo, hubo alguien que detectó el error, el cual permitía extraer Ethers sin necesidad de permiso de los demás. No se trataba de una letra pequeña que nadie leyese, se trató de un error de programación del que nadie se percató.

Este error permitió que el atacante retirarse pequeñas cantidades de Ethers, hasta obtener cerca de 50 millones de dólares. Este mismo atacante publicó una nota abierta en Internet en la que declaraba que todo lo que había hecho estaba en el código y por tanto, al ser ley, no podían retirarle todo ese dinero.

Este caso se llevó ante tribunales, los cuales respondieron que en ese tipo de programas el código no siempre es la ley, y que si tantas personas habían puesto su dinero en un fondo común, tenían derecho a recuperar lo que es suyo. Aquí entra en juego el funcionamiento de la Blockchain, Ethereum en este caso, ya que por gracia para el atacante y desgracia de las víctimas, no es posible identificar quién fue.

5.5. Pérdida de clave privada

Perder los fondos almacenados en una cartera por un descuido o accidente, de modo que sean irrecuperables, es una posibilidad muy lejana, y eso es positivo y habla muy bien de los criptoactivos y su tecnología subyacente como herramientas disruptivas; pero la posibilidad existe aún, remotamente, pero sigue allí. La diferencia yace en que en Blockchain, cada individuo es enteramente responsable de los activos que posea. En casos extremos, las compañías no pueden hacer más que desearte suerte.

En caso de perder esta clave privada el intento de recuperarla puede llegar a ser una odisea, ya que si no la recuerdas y fallas numerosas veces los intentos se podría generar una cuenta de espera que se multiplicará, haciendo a su vez que quien robar tendría que pasar toda su vida intentando acceder a la cuenta.

6. Aplicaciones de Blockchain

6.1. Financiero

La cadena de bloques no solo tiene aplicación en las criptomonedas. Estas son algunas de las posibilidades que ofrece la cadena de bloques en las finanzas:

6.1.1. Contratos inteligestes

Un Smart-Contract es un código software que se ejecutará por sí mismo bajo ciertas circunstancias acordadas entre las partes de antemano. Normalmente incluyen una transacción financiera. Por ejemplo, si el valor del petróleo baja hasta un precio fijado se invierte una cantidad de dinero en una determinada acción.

Los contratos inteligentes aportarán en un futuro servicios financieros sin necesidad de intermediarios. Tienen un sinfín de posibilidades: sistemas de votación online, seguros, apuestas... Los Smart-Contracts incorporan las principales características de Blockchain (inmutabilidad, seguridad y transparencia).

6.1.2. Identidad perpetua - DNI

La identificación digital cada vez es más importante en el mundo financiero. Tener la seguridad de que un usuario es realmente el titular de un contrato financiero digital es vital. Con todo esto, la introducción de una identidad personal (DNI, Pasaporte, escritura) en Blockchain garantiza la veracidad de la identificación.

En un futuro próximo existirá una cadena de bloques accesible para todos los intervinientes financieros, donde será posible la obtención de la identificación digital. De forma, que una vez introducido el DNI en ese registro o cadena de bloques, cualquier banco o fintech podrá acceder a la identificación (con autorización del usuario). Por consiguiente, cualquier usuario solo necesitará introducir su DNI o pasaporte una única vez.

6.1.3. Pagos digitales - Stellar, Ripple

Existen monedas digitales muy eficientes en los pagos internacionales y micropagos:

- Ripple está especializada en pagos transfronterizos (pagos entre distintos países). El sistema de Ripple está diseñado para entidades financieras y proveedores de pagos de todo el mundo. Esta tecnología evita que las transacciones transfronterizas pasen por intermediarios.
- Stellar es una plataforma ideal para lo micropagos, debido a su rapidez, bajo comisionamiento e igualdad de trato entre los usuarios.

Algunas entidades financieras están empezando a desarrollar procesos a través de Blockchain en diversas áreas de negocio. Sin duda alguna, los pagos digitales es el área financiera que más se está implantando.

6.1.4. Emisión de títulos y activos digitales

La cadena de bloques permite a las empresas la emisión de títulos o activos digitales (una propiedad, un activo financiero, una criptomoneda...). Una vez introducidos los activos en Blockchain, estos pueden ser comercializados entre distintas compañías. Esta transmisión de activos digitales facilita el comercio y colaboración entre empresas.

6.2. Seguros

Estamos viendo que muchas industrias están comenzando a subirse al carro de la blockchain, de modo que la industria de los seguros no iba a ser menos. Muchas aseguradoras como Allianz o Zurich están experimentando formas de aprovechar todas las ventajas que brinda una blockchain en seguridad, transparencia y trazabilidad para mejorar la experiencia del cliente.

Uno de los objetivos es el de reducir procesos de verificación y papeleo, ya que hay una gran cantidad de clientes que prefieren utilizar la tecnología y resolver todos los trámites a través de dispositivos informáticos, como dispositivos móviles. Hoy en día la verificación e identificación a través de estos dispositivos suele ser muy tediosa, de modo que se busca reducir dichos procesos a través del uso de blockchain para conseguir captar un mayor número de clientes.

Además, las compañías se sienten muy atraídas por el gran potencial de una red blockchain para calcular mejor los riesgos que asume la empresa y automatizar procesos, por ejemplo, reduciendo muchos costes mediante la utilización de un smart contract en el que tanto la empresa com el usuario están deacuerdo. Esto agilizaría también cualquier tipo de necesidad, como por ejemplo, al tener un accidente, el usuario podría activar el sistema mediante un smart contract que inmediatamente movilizará todo lo necesario para solventar el problema: tramitar documentos asociados, avisar a terceros, reevaluar precios... Todo esto facilitará y agilizará todo proceso para el cliente, además de tener la certeza de que todo funcionará correctamente, ya que no hay intervención de nadie más que el usuario y el smart contract (sin contar, por supuesto, de la necesidad de intervención humana en el caso de necesitar una grúa, por ejemplo).

Es por ello, que en 2018 surgió B3i, lo que era una iniciativa en sus inicios para facilitar el camino hacia la utilización de blockchain. Desarrolla estándares, protocolos e infraestructuras de red para eliminar la fricción en la transferencia de riesgos. El principal objetivo es el de optimizar y automatizar los procesos de todo el mercado, consiguiendo mejoras en tiempo y costo, que hasta ahora no son posibles de obtener. Actualmente, más de 40 compañías apoyan B3i.

6.3. Registro de la propiedad

La transparencia, la inmutabilidad y la trazabilidad son las tres características que facilitan el uso casi perfecto de la tecnología Blockchain aplicada al registro de la propiedad sobre bienes raíces. Esta tecnología permite que, en procesos de compra-venta, no sea necesario siquiera que el comprador y el vendedor se encuentren en el mismo país.

El uso de la Blockchain para el registro de la propiedad en bienes raíces solventa los problemas causados por la lentitud y los márgenes de error en los trámites burocráticos que tan poco nos gustan a todos, permitiendo a los distintos actores como: agentes de bienes, bancos, aseguradoras, notarías, juzgados, compradores y vendedores puedan hacerle un seguimiento confiable a todos los procesos aplicados sobre una tierra o inmueble. Estos procesos pueden ser: registro de títulos, compra-venta, traspasos, herencia, demandas, hipotecas, cobros de seguros, etc.

Es por esto que multitud de países llevan experimentando unos años (desde 2016 más o menos) con esta tecnología para agilizar los trámites públicos y privados sobre bienes raíces.

Algunos de los países desarrollados que con más fuerza están implementando esta tecnología en el registro de la propiedad sobre bienes raíces son: Japón, Emiratos Árabes, Suecia, Reino Unido y España.

Respecto a este último, el Colegio de Registradores de España y la asociación Alastria, la primera nacional regulada basada en el mundo Blockchain, están diseñando los métodos para agilizar la

gestión mediante esta tecnología de los millones de documentos que tramita dicho colegio. Documentos relacionados con los registros de la propiedad, el mercantil y el de bienes raíces, para lo cual utilizan el nodo Blockchain de la Universidad Pontificia Comillas (Cantabria).

Como hemos visto, los múltiples usos de la Blockchain se están extendiendo entre los países más desarrollados, lo cual abre una oportunidad no solo para la administración pública, sino para las empresas que deseen optimizar sus procesos comerciales con esta tecnología. Y como es lógico, las ventajas de esta tecnología para el registro de la propiedad se extrapolan a prácticamente cualquier iniciativa de negocios, producción y servicios.

6.4. Uso futuro

Aunque la tecnología Blockchain se utilizaba sobre todo para llevar a cabo transacciones financieras, en un futuro muy próximo casi actual, se multiplicará su potencial, como hemos visto en apartados anteriores, para intercambiar información, contratos y registros oficiales.

Las aplicaciones de esta tecnología van mucho más allá de sostener las transacciones de una criptodivisa, desde perseguir bacterias hasta presentar declaraciones de impuestos, firmar contratos de modo seguro o optimizar los procesos ligados al sistema sanitario, así como implementar soluciones de alto valor con componentes de Blockchain en las cadenas de suministro logístico y las industrias reguladas, como energía, productos farmacéuticos y la cadena de frío, lo que podemos generalizar como asegurar la trazabilidad de cualquier producto de manera transparente y segura.

Esta tecnología también dará un vuelco al panorama de industrias tan diversas como la salud, los transportes, el alimentario o el educativo. Por ejemplo, en el apartado de la salud se podrán compartir los registros de los pacientes de forma segura entre proveedores, tener diagnósticos más precisos y desarrollar planes de tratamiento más completos para pacientes individuales, gracias a cómo ésta tecnología maneja los datos. Por supuesto el campo de la investigación sobre todas estas aplicaciones es muy amplio y recibirá sofisticadas mejoras.

También se estudia el potencial de la tecnología Blockchain para la toma de negocios gubernamentales, la agilización de la burocracia o la reducción de la corrupción sistémica, abarcando por ejemplo, desde los acuerdos de alquiler hasta las elecciones nacionales.

El robo de identidad también podría convertirse en una cosa del pasado con la alianza entre la tecnología Blockchain y la biometría. Toda la información personal, abarcando el pasaporte, los registros educativos o la licencia de conducir, se podrá salvaguardar evitando fraudes y falsificaciones.

Cabe destacar que el gasto mundial en soluciones de Blockchain se ha ido duplicando anualmente desde 2018, y las previsiones para años posteriores apuntan a un crecimiento exponencial. Los datos de la consultora española IDC señala un gasto mundial de 11.700 millones de dólares para el año 2022, con una tasa de crecimiento anual compuesto del 73,2 % para el periodo 2017-2022.

Las expectativas de futuro que trae consigo esta tecnología son altísimas y analizando su evolución desde su creación parecen ciertas y perfectamente alcanzables. Ya veremos en unos años hasta donde ha conseguido llegar y si encuentra algún techo de desarrollo, aunque a estas alturas parece difícil que lo haga.

7. Empresas que usan e investigan la tecnología Blockchain

7.1. Bitcoin

Bitcoin se trata tanto de una moneda como de un sistema digital. Como moneda puede ser empleada como cualquier moneda, pero en lugar de tener un ente gubernamental, como podría ser un banco central, que lo emita y lo respalde, se basa por completo en el sistema digital que fue ideado por su creador, Satoshi Nakamoto, el cual lo difundió con su libro blanco (whitepaper) en un foro especializado de internet. En consecuencia tenemos que bitcoin no pertenece a ningún país o gobierno ni a ningún individuo o compañía privada, ya que su creador es anónimo y es de libre licencia. Son los usuarios quienes mantienen en funcionamiento su plataforma.

Como ya hemos dicho, Bitcoin es una moneda, tal como puede ser el dólar o el euro. Sus usos son exactamente los mismos. Lo que marca una gran diferencia entre ambas es que Bitcoin no existe de forma física. Se trata de una moneda digital que solo existe en la cadena de bloques o blockchain que la soporta y debido a un sofisticado proceso de verificación (consenso) de transacciones, no puede gastarse dos veces.

Los usuarios pueden manejar sus fondos con monederos digitales que tienen tanto una llave pública como una llave privada. Con ambas es posible realizar transacciones financieras desde cualquier lugar del mundo y en todo momento, por lo que, además, resulta una moneda que no posee ataduras territoriales. Del mismo modo que cualquier otra moneda, es posible intercambiarla por dinero local, para lo que existen casas de cambio o plataformas como LocalBitcoins, que funcionan en todo el mundo.

Se abrevia como BTC, y mientras que la plataforma en su totalidad se escribe con B mayúscula, 'bitcoin' en minúscula alude sólo a las unidades de la moneda.

Bitcoin además de ser una moneda tiene un valor muy importante como sistema digital, ya que se trata de la primera Blockchain existente. La tecnología de contabilidad distribuida es una base de datos encriptada donde puede almacenarse cualquier información, desde cada bitcoin gastado hasta programas informáticos como los contratos inteligentes. Su valor reside en que cada dato registrado — y protegido con un poderoso sistema criptográfico — se marca con una huella digital única que lo hace irrepetible e inmutable; por lo que, más allá de Bitcoin, esta tecnología está en desarrollo en múltiples aplicaciones por cientos de compañías muy importantes en todo el globo.

La revolución que trae bitcoin con respecto a las monedas y métodos de pago ya existentes es que elimina la necesidad de confianza en entes centrales para poder sustentar la economía. Ahora mismo, el dinero es controlado por los gobiernos y bancos de todo el mundo: son ellos los encargados de emitirlo, distribuirlo, regularlo y, por ejemplo, asegurar que una transacción entre dos desconocidos no resulte en un fraude. Ellos, como intermediarios, son necesarios para validar el proceso económico. Bitcoin, en cambio, confía en su propio código para brindar esta confianza. La blockchain es un sistema criptográfico que permite almacenar y transferir cualquier activo digitalizado entre dos o más personas directamente, pues todo queda registrado en línea, donde cualquiera puede ver que los fondos existen y realmente se movieron de una dirección a otra. De esta forma, se elimina el estricto control de los bancos, que pueden llegar incluso a congelar las cuentas de sus clientes, y las altas comisiones que cobran, pues Bitcoin fue diseñado para cobrar una ínfima o nula comisión. Es por todo esto que Bitcoin es descentralizado.

7.2. Ethereum

En su forma más simple, Ethereum es una plataforma abierta de software basada en la tecnología de cadena de bloques que permite a los desarrolladores crear e implementar aplicaciones descen-

tralizadas.

Como Bitcoin, Ethereum es una red distribuida de cadena de bloques pública. Si bien existen algunas diferencias técnicas importantes entre las dos, la distinción más importante es notar que Bitcoin y Ethereum difieren sustancialmente en propósito y capacidad. Bitcoin ofrece una aplicación particular de la tecnología de bloques, un sistema de efectivo electrónico entre pares que permite pagos de Bitcoin en línea. Si bien la cadena de bloques de Bitcoin es usada para mantener un seguimiento de la moneda digital (Bitcoins), la cadena de bloques de Ethereum se enfoca en ejecutar el código de programación de cualquier aplicación descentralizada.

En la cadena de bloques de Ethereum, en lugar de minar Bitcoin, los mineros trabajan para ganar Ether, un tipo de criptotóken que alimenta a la red. Más allá de una criptomoneda comerciable, el Ether también es usado por desarrolladores de aplicaciones para pagar tarifas de transacción y servicios en la red de Ethereum.

Existe un segundo tipo de tóken que es usado para pagar las tarifas de mineros por incluir transacciones en su bloque, se llama gas, y cada ejecución de contrato inteligente requiere cierta cantidad de gas enviada junto con este para atraer a los mineros a colocarlo en la cadena de bloques.

Si bien todas las cadenas de bloques tienen la capacidad de procesar código, la mayoría están grandemente limitadas. Ethereum es diferente. En lugar de dar un conjunto limitado de operaciones, Ethereum permite a los desarrolladores crear cualquier operación que deseen. Esto significa que los desarrolladores pueden crear miles de aplicaciones diferentes que van más allá de cualquier cosa que hayamos visto antes.

7.3. Alastria

Alastria es una organización sin ánimo de lucro que fomenta la economía digital desarrollando tecnologías blockchain. Es totalmente abierta y pretenden crear un ecosistema de innovación lo más diverso posible.

El proyecto se inició en 2017, lanzándose bajo el nombre de Red Lyra, con la visión de democratizar el acceso a blockchain en España, expandiéndose rápidamente al resto del mundo. Son pioneros en la generación de nuevos modelos de economía digital, promoviendo una metodología de innovación propia que pretende adelantarse a las necesidades de nuestra sociedad.

Alastria cuenta con dos redes operativas, **Red T** y **Red B**, sobre las que pueden desplegarse dos tipos de nodos:

- Nodos regulares.
- Nodos críticos validadores y permisionadores.

Cualquiera puede poner un nodo en cualquiera de las redes siempre y cuando se sea socio y se acepten las Políticas de Gobierno y Buen uso de los nodos.

La red T está construida sobre tecnología Quorum, mientras que la red B está montada sobre Hyperledger Besu. Esta plataforma ha sido definida por los socios de la misma como una blockchain agnóstica, en la que no confían el desarrollo a una sola plataforma, por lo que se han iniciado trabajos de creación de otro tipo de red basada en HyperLedger Fabric y en cómo interconectar esas tres redes, además de interconectar más en un futuro.

7.4. Hyperledger

Hyperledger es un proyecto de código abierto albergado en la Fundación Linux. Trata de crear soluciones de código abierto para Blockchain privadas. Principalmente trata de aunar todos los esfuerzos en este ámbito para conseguir desarrollar protocolos y estándares abiertos, tratando de crear un ecosistema variado para diferentes usos. Promueve una gran variedad de negocios basados en la tecnología blockchain como redes blockchain privadas, motores de smart contracts o aplicaciones, entre otras. El proyecto cuenta con más miembros cada vez, contando con importantes empresas como Cisco, IBM o Intel, además de muchos bancos como BBVA.

Existen tres tipos de miembros en Hyperledger (que además deben ser miembros de Linux Foundation:

- **Premier**: Hacen donaciones de 250.000 dólares anuales.
- **General**: Pagan una tarifa en función del tamaño de la empresa.
- **Associate**: No necesitan realizar donaciones pero deben ser previamente aprobados y ser proyectos open source, organismos gubernamentales u ONGs.

A su vez, Hyperledger está compuesto por diferentes proyectos, divididos en plataformas blockchain y herramientas para la interacción con dichas plataformas. Entre ellas encontramos, por ejemplo:

- **Hyperledger Burrow**: Fue impulsada por Monax Industries y es una blockchain privada basada en el código de Ethereum, es decir, permite el uso de smart contracts desarrollados en Solidity.
- **Hyperledger Fabric**: Orientada al mundo empresarial y sus contribuciones iniciales son de IBM principalmente. Es una plataforma multidisciplinar que aspira facilitar la implementación de cualquier modelo de uso. Permite el despliegue de smart contracts (llamados en este caso chaincodes) desarrollados en el lenguaje de programación de Google: 'Golang'. Un punto muy a favor de esta blockchain es que posee un diseño muy flexible ya que incorpora capacidades como crear chaincodes en cualquier lenguaje o decidir qué algoritmo de consenso usar ('pluggable consensus'). Es una de las blockchain privadas más conocidas ahora mismo en el mercado.

Debido a la gran amplitud que Hyperledger ofrece en cuanto a servicios y flexibilidad, es muy atractiva para muchas empresas ya que además solventa diferentes problemas dentro de las blockchain como por ejemplo los costes de mantenimiento de la red y de equipos, ya que, al ofrecer sus servicios a corporaciones privadas, la financiación proviene de fuera de la red, abaratando costes.

8. Conclusión

Si has llegado hasta aquí seguramente tengas una idea mucho más clara de los conceptos básicos acerca de esta novedosa tecnología y de cómo funciona a grandes rasgos. Para tener un conocimiento global acerca de Blockchain después de leer este trabajo es necesario preguntarse acerca de los conceptos básicos tratados en el mismo:

- Si comprendes el funcionamiento de las redes P2P o torrent, ya entendiste la cuarta parte.
- Si comprendes la encriptación prácticamente infalible de esta tecnología, ya entendiste la segunda cuarta parte.
- Si en este punto comprendes que el funcionamiento de esta tecnología necesita de electricidad para mantener funcionando los equipos hardware cuya computación es imprescindible; y de un sistema de recompensas como pagos por la utilización de dichos recursos, ya has entendido la tercera cuarta parte.
- Y si comprendes el valor del dinero (FIAT) aplicado a estos archivos encriptados en lugar de a un papel o billete, y que esto se puede extender a contratos de todo tipo, al que aplicar las leyes bursátiles, que no son más que entender que el precio de mercado está basado en una subasta continua: lo has entendido todo.

Después de haberlo comprendido todo, podemos sacar una serie de conclusiones respecto a la tecnología Blockchain y a la transformación digital que ésta conlleva:

- La implantación de sistemas Blockchain a nivel público y privado podría conllevar un beneficio interesante para los usuarios de ciertos servicios, además de gran seguridad en la realización de transacciones y el cumplimiento automático de contratos.
- Estamos ante una tecnología disruptiva susceptible de alterar en mayor o menor medida una serie de profesiones tradicionales consolidadas (notarios, registradores...) por presentar riesgos altos de desintermediación.
- Existen algunos países como Japón o Emiratos Árabes en los que su utilidad a modo de registro de la propiedad ya se han implantado.
- Esta tecnología puede ayudar a las administraciones a mantener registros actualizados, seguros e inmutables.
- En cualquier caso, se debe ser consciente de los peligros que esta tecnología puede traer consigo. Uno de los que más preocupan es precisamente su carácter de registro “inmutable”. Esto que puede ser claramente positivo para algunos campos, puede llegar a ser negativo para otros. Por ejemplo, si un registros basado en Blockchain incluyese una entrada con contenido erróneo o que vulnera la privacidad o el honor de una persona, tal intromisión no desaparecería nunca porque el registro es inmutable. De ahi que surjan ciertos recelos para determinados usos.
- Otro aspecto que ha preocupado es el uso del Blockchain como base para las criptomonedas y el mal uso que pueda hacerse para fines de financiación de terrorismo o blanqueo de capitales. Evidentemente, el derecho penal juega un papel clave en la persecución de estos delitos, lo que no es tarea fácil por la complejidad técnica.
- Por último, también parece importante que las empresas series que operan en el sector de las criptomonedas de forma lícita tienen que colaborar con las autoridades de investigación de delitos tan graves. La ética y la búsqueda del bien público común no es incompatible con la libertad de empresa y la búsqueda de beneficios económicos.
- El capitalismo responsable debe ser asumido por los operadores más serios de este tipo de redes.

9. Referencias Bibliográficas

Referencias

[1] "Blockchain: definición y ámbitos de aplicación - IONOS."24 sept.. 2018, https://www.ionos.es/digitalguide/online-marketing/vender-en-internet/blockchain/. Se consultó el 24 may.. 2020.

[2] Preukscha, A.. (2017). *Blockchain: la revolución industrial de internet*. España: Grupo Planeta.

[3] "¿Qué es blockchain y cómo funciona la cadena de bloques?."https://es.cointelegraph.com/bitcoin-for-beginners/how-blockchain-technology-works-guide-for-beginners. Se consultó el 24 mar.. 2020.

[4] "Blockchain, así funciona la tecnología que va a cambiar el ...."23 ene.. 2018, https://www.emprendedores.es/gestion/a76448/blockchain-bitcoin-cambiar-mundo-negocios/. Se consultó el 24 mar.. 2020.

[5] "¿Que son los Tokens? Significado de Tokens Criptomonedas."https://www.brokerdeforex10.com/criptomonedas/que-son-los-tokens/. Se consultó el 10 may.. 2020.

[6] "Qué es un token en Bitcoin? – Criptomonedas - OroyFinanzas ...."23 oct.. 2014, https://www.oroyfinanzas.com/2014/10/que-token-bitcoin-criptomonedas/. Se consultó el 24 mar.. 2020.

[7] "¿Qué son los contratos inteligentes o smart contracts?."17 nov.. 2015, https://www.oroyfinanzas.com/2015/11/que-son-contratos-inteligentes-smart-contracts/. Se consultó el 24 mar.. 2020.

[8] ”Cuántos tipos de blockchain hay | Bit2Me Academy."5 may.. 2020, https://academy.bit2me.com/cuantos-tipos-de-blockchain-hay/. Se consultó el 30 mar.. 2020.

[9] "Blockchain Privada vs. Pública: ¿Cual es la mayor diferencia ...."19 dic.. 2018, urlhttps://nemespanol.io/blockchain-privada-vs-publica-cual-es-la-mayor-diferencia/. Se consultó el 30 mar.. 2020.

[10] ”Características de las redes P2P - Ramon Millan."http://www.arianamillan.com/libros/librodistribucionlibrosredesp2p/distribucionlibrosredesp2p_caracteristicasp2p.php. Se consultó el 30 mar.. 2020.

[11] "¿Qué son los nodos? | Binance Academy."https://www.binance.vision/es/blockchain/what-are-nodes. Se consultó el 30 mar.. 2020.

[12] "Los nodos de blockchain y su influencia en la minería ...."25 ene.. 2019, https://blog.mercury.cash/es/2019/01/25/los-nodos-de-blockchain-y-su-influencia-en-la-mineria/. Se consultó el 30 mar.. 2020.

[13] "¿Qué son Nodos y Supernodos? - Criptotendencias ...."11 dic.. 2018, https://www.criptotendencias.com/base-de-conocimiento/que-son-nodos-y-supernodos/. Se consultó el 30 mar.. 2020.

[14] "¿Qué es el P2P? - Máster en Blockchain, Smart Contracts y ...."https://masterethereum.com/que-es-p2p/. Se consultó el 5 abr.. 2020.

[15] "¿Qué es un Algoritmo de Consenso Blockchain? | Binance ...."https://www.binance.vision/es/blockchain/what-is-a-blockchain-consensus-algorithm. Se consultó el 5 abr.. 2020.

[16] "¿Quién manda en una red blockchain? - Paradigma Digital."https://www.paradigmadigital.com/techbiz/quien-manda-en-una-red-blockchain/. Se consultó el 5 abr.. 2020.

[17] "Qué es Prueba de trabajo / Proof of Work (PoW) | Bit2Me ...."18 may.. 2020, https://academy.bit2me.com/que-es-proof-of-work-pow/. Se consultó el 5 abr.. 2020.

[18] "Qué es Prueba de participación / Proof of Stake (PoS) | Bit2Me ...."5 may.. 2020, https://academy.bit2me.com/que-es-proof-of-stake-pos/. Se consultó el 11 may.. 2020.

[19] "Tipos de cuentas y transacciones – APRENDE BLOCKCHAIN."https://aprendeblockchain.wordpress.com/fundamentos-tecnicos-de-blockchain/cuentas-y-transacciones/. Se consultó el 11 abr.. 2020.

[20] "Blockchain: bloques, transacciones, firmas digitales y hashes."https://www.criptonoticias.com/criptopedia/blockchain-bloques-transacciones-firmas-digitales-hashes/. Se consultó el 11 abr.. 2020.

[21] ”Comparing Bitcoin & Ethereum: UTXO vs Account Based ...."23 jul.. 2018, https://blockonomi.com/utxo-vs-account-based-transaction-models/. Se consultó el 14 abr.. 2020.

[22] ”Comparing Bitcoin & Ethereum: UTXO vs Account ... - Reddit."https://www.reddit.com/r/ethereum/comments/915hmu/comparing_bitcoin_ethereum_utxo_vs_account_based/. Se consultó el 14 abr.. 2020.

[23] .El modelo UTXO - Horizen Academy."https://academy.horizen.global/es/technology/advanced/the-utxo-model/. Se consultó el 14 abr.. 2020.

[24] ”Cryptographic Hash Functions Explained: A ...."14 ago.. 2018, https://komodoplatform.com/cryptographic-hash-function/. Se consultó el 14 abr.. 2020.

[25] "Los nodos de blockchain y su influencia en la minería ...."25 ene.. 2019, https://blog.mercury.cash/es/2019/01/25/los-nodos-de-blockchain-y-su-influencia-en-la-mineria/. Se consultó el 16 abr.. 2020.

[26] ”El minado en Blockchain ¿Quiénes son y qué hacen ... - Cysae."17 oct.. 2018, https://www.cysae.com/el-minado-en-blockchain/. Se consultó el 16 abr.. 2020.

[27] "¿Qué es la minería de criptomonedas? | Binance Academy."https://www.binance.vision/es/blockchain/what-is-cryptocurrency-mining. Se consultó el 24 may.. 2020.

[28] "¿Cuantos algoritmos de consenso existen para las Blockchain?."23 sept.. 2019, https://es.cointelegraph.com/news/cuantos-algoritmos-de-consenso-existen-para-las-blockchain. Se consultó el 19 abr.. 2020.

[29] ”Activity Report 2015-2016."https://www.fidefundacion.es/attachment/729944/. Se consultó el 24 may.. 2020.

[30] "¿Qué es blockchain y cómo funciona la cadena de bloques?."https://es.cointelegraph.com/bitcoin-for-beginners/how-blockchain-technology-works-guide-for-beginners. Se consultó el 19 abr.. 2020.

[31] "Hyperledger: la Blockchain privada que todos tenemos que ...."29 ene.. 2018, https://www.eleconomista.es/economia/noticias/8899454/01/18/Hyperledger-la-Blockchain-privada-que-todos-tenemos-que-conocer.html. Se consultó el 20 abr.. 2020.

[32] "¿Qué es PoW, PoS y PoI? - Bitcoin.es."21 mar.. 2018, https://bitcoin.es/mineria/pow-pos-y-poi/. Se consultó el 20 abr.. 2020.

[33] "P versus NP. ¿Nunca lo entendiste? - Xataka Ciencia."26 ago.. 2006, https://www.xatakaciencia.com/matematicas/p-versus-np-nunca-lo-entendiste. Se consultó el 24 abr.. 2020.

[34] ”Conceptos de seguridad y criptografía en blockchain ...."https://aprendeblockchain.wordpress.com/fundamentos-tecnicos-de-blockchain/fundamentos-basicos-de-criptografia-en-blockchain/. Se consultó el 24 abr.. 2020.

[35] ”Criptografía de curva elíptica - INT Chain Spanish ... - Medium."18 sept.. 2019, https://medium.com/articulos-de-la-comunidad/criptograf%C3%ADa-de-curva-el%C3%ADptica-99b8c8c1657c. Se consultó el 24 abr.. 2020.

[36] "Qué es la Tolerancia a Fallas Bizantinas (BFT) | Bit2Me ...."5 may.. 2020, https://academy.bit2me.com/que-es-tolerancia-fallas-bizantinas-bft/. Se consultó el 14 may.. 2020.

[37] "Qué es el ataque del 51 % - El CriptoBlog de Tutellus."18 dic.. 2018, https://criptoblog.tutellus.com/el-ataque-del-51-1/. Se consultó el 26 abr.. 2020.

[38] ”ASIC Miner Value."https://www.asicminervalue.com/. Se consultó el 26 abr.. 2020.

[39] "NiceHash". https://www.nicehash.com/. Se consultó el 27 abr.. 2020.

[40] ”Cryptocurrency Value and 51 % Attacks - papers in the SSRN". 2 dic.. 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3290016. Se consultó el 29 abr.. 2020.

[41] ”Cryptocurrency mining insider: All PoW coins have secret ASICs". 14 may.. 2018, https://www.finder.com.au/cryptocurrency-mining-insider-all-pow-coins-have-secret-asics. Se consultó el 29 abr.. 2020.

[42] "The State of Cryptocurrency Mining - Sia Blog". 13 may.. 2018, https://blog.sia.tech/the-state-of-cryptocurrency-mining-538004a37f9b. Se consultó el 29 abr.. 2020.

[43] "Qué es el doble gasto | Bit2Me Academy". 5 may.. 2020, https://academy.bit2me.com/que-es-doble-gasto/. Se consultó el 1 may.. 2020.

[44] "¿Qué son Nodos y Supernodos? - Criptotendencias ...". 11 dic.. 2018, https://www.criptotendencias.com/base-de-conocimiento/que-son-nodos-y-supernodos/. Se consultó el 1 may.. 2020.

[45] ”Ataques a blockchains, minería encubierta y robos a casas de...". 22 dic.. 2018, https://www.criptonoticias.com/seguridad-bitcoin/robo-fraude/ataques-blockchains-mineria-encubierta-robos-casas-cambio-2018/. Se consultó el 1 may.. 2020.

[46] "Seis herramientas utilizadas por los hackers para robar ...."29 jul.. 2018, [linebreak]https://es.cointelegraph.com/news/six-tools-used-by-hackers-to-steal-cryptocurrency-how-to-protect-wallets. Se consultó el 4 may.. 2020.

[47] "Blockchain para registro de la propiedad: países pioneros en ...."29 may.. 2019, https://blog.enzymeadvisinggroup.com/blockchain-registro-propiedad. Se consultó el 4 may.. 2020.

[48] ”Comillas y CEU estrenan blockchain universitario con Alastria."13 jun.. 2018, https://www.blockchaineconomia.es/blockchain-universitario/. Se consultó el 4 may.. 2020.

[49] "Japan Could Place Its Entire Property Registry on a Blockchain.". 22 jun.. 2017, https://www.ccn.com/japan-place-entire-property-registry-blockchain/. Se consultó el 4 may.. 2020.

[50] "100 %: Dubai Will Put Entire Land Registry on a Blockchain.". 9 oct.. 2017, https://www.ccn.com/100-dubai-put-entire-land-registry-blockchain/. Se consultó el 7 may.. 2020.

[51] "Sistema de Registro de la Propiedad Basado en la ... - YouTube."25 jun.. 2019, https://www.youtube.com/watch?v=1zK43cBboMI. Se consultó el 7 may.. 2020.

[52] "Nunca pierdas tu llave privada: una odisea para recuperar ....". https://www.criptonoticias.com/seguridad-bitcoin/nunca-pierdas-llave-privada-odisea-recuperar-30000-bitcoins/. Se consultó el 7 may.. 2020.

[53] "The DAO y el caso del robo de los 50 millones de dólares en ....". 25 ago.. 2017, [linebreak]https://www.xataka.com/seguridad/the-dao-y-el-caso-del-robo-de-los-50-millones-de-dolares-en-ethereum-insert-coin-1x01. Se consultó el 9 may.. 2020.

[54] "Qué es Ethereum Classic (ETC) | Bit2Me Academy."21 feb.. 2020, https://academy.bit2me.com/que-es-ethereum-classic-etc-criptomoneda/. Se consultó el 9 may.. 2020.

[55] "¿Qué es una transacción coinbase? | Bit2Me Academy."11 may.. 2020, https://academy.bit2me.com/que-es-coinbase-transaccion/. Se consultó el 11 may.. 2020.

[56] "Blockchain, la tecnología que revolucionará las finanzas ...."https://nuevofinanciero.com/blockchain-tecnologia-finanzas/. Se consultó el 11 may.. 2020.

[57] "Radiografía de los usos futuros de la tecnología blockchain."10 sept.. 2018, https://www.ticbeat.com/innovacion/usos-futuros-blockchain/. Se consultó el 11 may.. 2020.

[58] "Cómo la tecnología blockchain cambiará el mundo para ....". 5 sept.. 2018, https://www.ticbeat.com/innovacion/como-la-tecnologia-blockchain-cambiara-el-mundo-para-siempre/. Se consultó el 14 may.. 2020.

[59] "IDC Research España busca las empresas más innovadoras ....". 9 dic.. 2019, [linebreak]https://es.cointelegraph.com/news/idc-research-spain-seeks-the-most-innovative-companies-including-those-who-work-with-blockchain. Se consultó el 14 may.. 2020.

[60] "Who We Are - B3i."https://b3i.tech/who-we-are.html. Se consultó el 14 may.. 2020.

[61] "Qué es Bitcoin (BTC) | CriptoNoticias - blockchains y ...."https://www.criptonoticias.com/criptopedia/que-es-bitcoin-btc/. Se consultó el 14 may.. 2020.

[62] "¿Qué es Ethereum? ¡La guía más completa que ... - Blockgeeks". https://blockgeeks.com/guides/es/que-es-ethereum/. Se consultó el 14 may.. 2020.

[63] "Paso a paso: así se crea un nodo regular en Alastria - Medium". 8 may.. 2018, https://medium.com/@alastria_es/paso-a-paso-as%C3%AD-se-crea-un-nodo-regular-en-alastria-e9ef9a47b07f. Se consultó el 14 may.. 2020.

[64] "Qué es Ethereum Classic (ETC) | Bit2Me Academy". Se consultó el 14 may... 2020 de https://academy.bit2me.com/que-es-ethereum-classic-etc-criptomoneda/.