

FUNDAMENTOS DE BLOCKCHAIN

TO THE MOON.



JOAN AMENGUAL

RESUMEN

En este libro se van a explicar las bases fundamentales y los pilares de Blockchain que actualmente se encuentran tan presentes en la vida de todos nosotros. Dichos conocimientos se han profundizado y se han explicado detalladamente en los cursos desarrollados en Udemy.

Los cursos de Blockchain en los que hemos estado trabajando durante meses los podéis encontrar rebajados un 90% en el siguiente enlace:

<https://frogames.es/rutas-de-aprendizaje/ruta-de-blockchain/>

En estos cursos además de entrar en detalle con las bases teóricas de la tecnología Blockchain también aprendemos las bases técnicas de criptografía para entender todo el mundo de las criptomonedas y su enorme potencial, entre otros muchísimos conocimientos.

Por si fuera poco, tenemos un curso donde aprendemos a desarrollar Smart Contracts con Solidity. Donde vas a aprender a crear tus propios proyectos y ser un experto como desarrollador en Ethereum.

CAPÍTULO 1: INTRODUCCIÓN A BLOCKCHAIN

NACIMIENTO Y EVOLUCIÓN DE LA TECNOLOGÍA BLOCKCHAIN



La primera publicación sobre la tecnología blockchain se remonta al año 1991. La idea de los autores consistía en tener un registro digital de archivos (de audio, imagen, video o texto) ordenado cronológicamente, permitiendo conocer con exactitud su fecha de creación.

En 2008, nace la primera red Blockchain, conocida como Bitcoin. La propuesta de esta criptomoneda consiste en utilizar la tecnología blockchain para proveer un método de pago electrónico que no necesita supervisión y elude el control de las instituciones financieras. El ingrediente fundamental y definitivo que incorpora Bitcoin, convirtiéndole en la más exitosa de todas las propuestas de dinero digital hasta la fecha, es la combinación de la inteligente idea de la tecnología blockchain junto con un

protocolo de consenso conocido como Proof-of-Work. A raíz del éxito, otros han seguido sus pasos siendo ya superior a 8500 el número de criptomonedas (a día 01 de agosto de 2021) funcionando con el mismo mecanismo, con diferentes variantes técnicas poco relevantes en general.

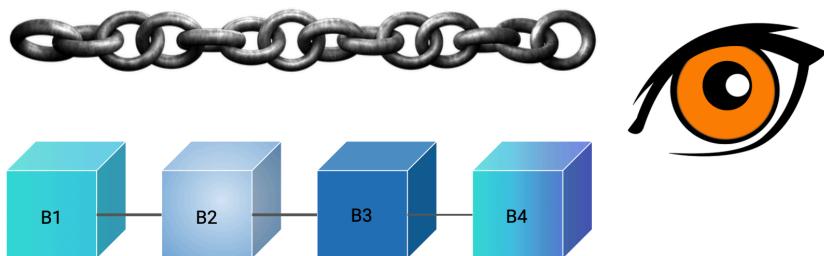


El uso de la tecnología blockchain como una herramienta con múltiples aplicaciones en muy diversos campos. Algunos de los más atractivos son el registro de documentos de forma descentralizada, historiales médicos, registro de propiedad, organización y distribución de recursos energéticos, control de aduanas, sistemas de votación, identidad digital o monitorización de procesos de producción [1].

QUÉ ES BLOCKCHAIN



En términos generales, blockchain se basa en el es registro de información distribuido tipo P2P (Peer-to-Peer) en donde los diferentes participantes no tienen por qué confiar los unos en los otros, puesto que hay un protocolo de consenso que garantiza la seguridad y la veracidad de las transacciones. Otra de las características principales, y sin duda una de las más relevantes, es la inmutabilidad de la cadena; en blockchain no es posible editar o borrar información.



El término blockchain o, cadena de bloques en español, se debe a la estructura de esta base de datos, consistente en conjuntos de transacciones que son organizados y almacenados en bloques. Los bloques están ordenados cronológicamente y tienen un número de bloque, un código alfanumérico conocido como hash y están firmados digitalmente por la persona que encontró dicho código.

Desde la perspectiva inversa, pueden transacciones a las que se les ha asignado un número de bloque y un código hash. En cuanto a la inmutabilidad de la cadena, en el caso de que se quiera cambiar una información que ha sido introducida en un bloque ya validado, la única forma de hacerlo será emitiendo una nueva transacción que actualice la información deseada. En ningún caso será posible editar o borrar nada que haya sido previamente validado y añadido a la cadena.



TIPOS DE BLOCKCHAINS



Así como hemos visto en el curso de Blockchain de cero a experto pueden fácilmente distinguirse al menos tres tipos de redes blockchain: **las públicas, las federadas y las privadas.** Cabe mencionar asimismo la opción **Blockchain as a Service** para almacenamiento en la nube.

Públicas. Las redes blockchain públicas son aquellas a las que cualquier persona tiene acceso. En general, el procedimiento para participar es descargarse la aplicación correspondiente y conectarse, de forma automática, con un determinado número de nodos a los que se les pregunta por la versión más actualizada de la cadena. Una vez el nodo está actualizado, tiene los mismos derechos y deberes que el resto de participantes a la hora de proponer y validar transacciones, replicar las transacciones que escucha o minar (si desea hacerlo).

También en su mayoría, la seguridad de estas redes está basada en protocolos de consenso y funciones hash, y los usuarios interactúan con la red de forma anónima.

Públicas



Federadas. Las blockchain federadas son un concepto de red diferente a los públicos e incluso podrían considerarse una tecnología diferente, puesto que no satisfacen en muchas ocasiones la definición. Estas blockchain han ido surgiendo con la idea de servir como bases de datos descentralizadas que pueden generar confianza en entornos complejos, con entidades con diferentes intereses y usuarios sin conocimientos. En general no son públicas, sino que un número determinado de organizaciones, entidades o compañías se encargan de administrar la red y mantener copias sincronizadas. El acceso mayoritario es en este caso mediante una interfaz web que estos administradores ponen a disposición del usuario medio.

Es por eso de vital importancia, a la hora de diseñar e implementar soluciones de este tipo, acompañar a la herramienta blockchain con un plan estratégico adecuado consistente en definir desde quiénes y cómo van a

administrar la red hasta qué información se les va a mostrar a los usuarios vía interfaz web.

En muchos casos el usuario que accede vía web puede no tener interés ni conocimiento sobre blockchain, pero sí necesitar una plataforma que involucre entidades diferentes, necesidad de confianza y transparencia. Una blockchain federada puede ser entonces una buena opción siempre que las reglas del juego establecidas en la administración y mantenimiento de la cadena sean las adecuadas y se ofrezca al usuario, a través de la interfaz web, el grado de transparencia requerido.

Queda claro entonces que, al ser su acceso vía web y no como nodos de pleno derecho, los usuarios comunes tendrán acceso a tanta información como se les decida mostrar a través de la misma. Se tendrán entonces opciones que varien desde un gran nivel de transparencia hasta una transparencia nula.

En minado de bloques actúa aquí también de forma diferente. En general ahora la red ni siquiera tendrá una criptomonedas asociada, de forma que el minado de bloques con recompensa que tenía lugar en las redes públicas es inexistente. Sin embargo, sigue siendo necesario que los bloques tengan un hash. ¿Quién es entonces el encargado de encontrarlo? Una opción razonable es que las propias organizaciones o entidades al mando de la red se encarguen de proporcionar y mantener servidores que cumplan con este

propósito. Es decir, la labor del minado que en las redes públicas es el corazón que las mantiene vivas y es responsabilidad de los usuarios, ahora pasa a jugar un papel secundario y son los administradores de la red quienes se encargan de proporcionar los recursos energéticos necesarios para encontrar hashes -o minar-.

Actualmente hay varias opciones de código abierto para construir una blockchain federada como Hyperledger, Corda, EFW o Multichain donde puedes descargar la aplicación de blockchain y programar la cadena a tu gusto, decidiendo quién quieras que participe, bajo qué reglas se regulan las transacciones, etc. Las redes públicas como Ethereum o Litecoin también ofrecen la oportunidad de hacer un fork para crear entornos federados o privados.

Permisionadas / Federadas



Privadas. Las blockchain privadas son aquellas en las que el control está reducido a una única entidad que se encarga de mantener la cadena, dar permisos a los usuarios que se desea que participen, proponer transacciones y aceptar los bloques. Son iguales que las federadas pero con solo una entidad a cargo, de forma que además de todas las diferencias que las federadas y las públicas tienen, hay que añadir también que se pierde la descentralización.

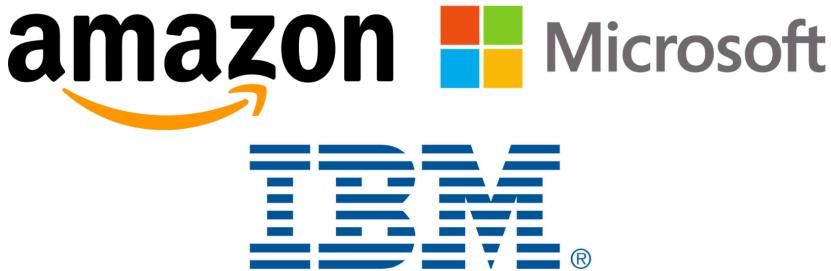
Privadas



HYPERLEDGER

Blockchain as a Service (BaaS). Algunas grandes compañías ofrecen servicios de almacenamiento de los datos de tu blockchain en la nube. Algunos ejemplos son IBM especializada en Hyperledger Fabric, Amazon colaborando con Digital Currency Group, o Microsoft ofreciendo servicios de R3, Hyperledger Fabric o Quorum, entre otras. Generalmente, las ventajas de este tipo de servicios son un aumento en la seguridad, la no necesidad de invertir en hardware y la posibilidad de un entorno más amigable con el que trabajar, pudiendo crear tu propio canal de blockchain sin necesidad de programar [1].

Blockchain as a Service (BaaS)



APLICACIONES DE LA TECNOLOGÍA BLOCKCHAIN



Entre las características que convierten a blockchain en una herramienta útil pueden destacarse **transparencia, descentralización y no necesidad de intermediarios**.

En concepto de transparencia, o la forma en que se consigue, es diferente dependiendo del tipo de red que estemos utilizado. En las redes públicas, en general, la transparencia es total puesto que cualquier usuario que se registre en la cadena es provisto de una copia de todo el blockchain, pudiendo ver en ella el estado actual de los activos y el historial de transacciones. En las redes privadas y federadas el acceso es restringido y mediante vía web para la mayoría de los usuarios, como comentábamos en la sección previa. Para estos usuarios el nivel de transparencia es el que los administradores de la red decidan ofrecerles mediante esta interfaz web.

La descentralización es un requisito determinante a la hora de decidir si blockchain es o no una buena herramienta para un caso concreto. En la medida en que la descentralización es

deseada, blockchain gana enteros. Si, en cambio, se pretende tener una base de datos centralizada, entonces blockchain en general no va a ser en absoluto la mejor opción. La descentralización consiste básicamente en determinar el número de nodos que van a mantener la cadena. Sin embargo, es interesante mencionar que esto no implica necesariamente transparencia, puesto que los propios nodos pueden tener diferentes roles dentro del sistema que les den acceso a un tipo determinado de información, teniendo vetado el acceso a cierto contenido de la red.

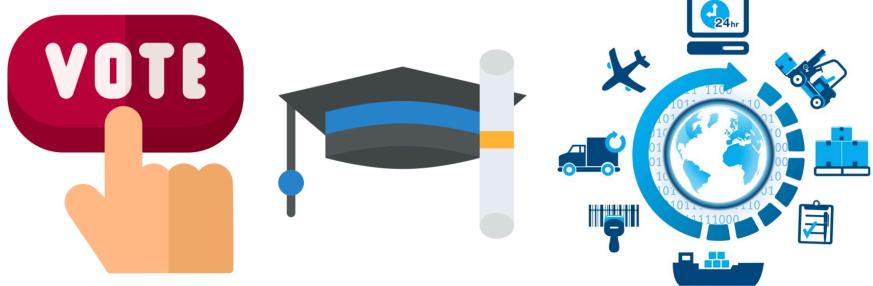
El tener distintos servidores con una copia sincronizada de la cadena añade un gran valor en cuanto a seguridad, dado que si alguna consiguiese modificar o corromper una de las copias, sería tan sencillo como re-sincronizarla con las demás.

En cuanto a la no necesidad de intermediarios, conviene hacer énfasis en las palabras “no necesidad”. Blockchain nace con Bitcoin para evitar necesidad de que instituciones financieras tengan que intervenir o verificar transacciones monetarias (o cryptomonetarias) entre individuos, de forma que aquí la eliminación de la intermediación de las mismas era un objetivo deseado y conseguido.

Sin embargo, a la hora de diseñar una blockchain privada o federada la situación es diferente. Podría ser que, en un sistema funcionando con blockchain consistente en el envío de un producto o un material determinado de un lugar a

otro, sea de interés para las dos partes realizar ciertos controles intermedios. Digamos, por ejemplo, que se pretende llevar a cabo un envío de productos alimenticios que requiere unos ciertos controles de humedad y temperatura durante su transporte en avión y barco. Las dos partes establecerían entonces el acuerdo (en forma de Smart Contract) de los parámetros a evaluar en los controles y el pago a realizar en caso de que todo siga su curso de la forma deseada.

Estas instituciones podrían tener su propio nodo provisto solo con permisos para ver información sobre las condiciones de temperatura y humedad que tienen que verificar, y no podrían saber en ningún momento cuál es el precio que se ha acordado pagar por el cargamento, por ejemplo. Al finalizar satisfactoriamente el proceso establecido en el Smart Contract, el dinero se transferiría automáticamente al vendedor [1].



Sistema de votación

Validación de títulos universitarios

Cadenas de suministro

BITCOIN



Bitcoin (BTC) es la primera criptomonedera que se desarrolló y también la primera y única aplicación basada en la tecnología blockchain que funciona 24/7 los 365 días del año desde 2009.



Bitcoin es un software, un protocolo y una moneda.

Estas tres características permiten que una de las aplicaciones de Bitcoin sea la de conformar una red de pagos global, transparente, basada en código abierto y de moneda única.

La moneda se ideó como un sistema económico descentralizado y abierto a todos, que proponía a los usuarios del mismo un sistema monetario y de intercambio de valor mejor que el actual sistema del dinero fiduciario. El valor de esta moneda depende de la confianza de los usuarios y no está controlado o regulado por ningún banco, por eso mismo su valor es tan volátil. Una de las grandes particularidades de Bitcoin es que se desconoce quién es su creador.

El 31 de octubre de 2008 aparece una propuesta de dinero Peer-2-Peer (P2P) que se basaba en la criptografía y en algo que se denominó blockchain.

Otra gran particularidad de Bitcoin es que por primera vez en la historia existe una forma de dinero que se crea, distribuye y custodia mediante una red de ordenadores a la que se puede unir cualquier persona y entre todos ellos constituyen actualmente el ordenador con más poder de cálculo del planeta.

El ritmo de la creación de monedas bitcoin es constante y bien conocido debido a la naturaleza abierta del código de su software. Gracias al conocimiento de estos datos, se puede estimar que en 2140 se minaría el último Bitcoin existente, que la dificultad para la creación de bitcoins irá aumentando

de la misma forma que la recompensa por la creación de bitcoins irá reduciéndose cada 210.000 bloques minados.

Según el whitepaper de Bitcoin, cada bloque de esta criptomonedas se crea cada diez minutos y contiene todas las transacciones realizadas durante ese periodo de tiempo. Debido a que es la primera criptomonedas desarrollada en el mercado, es la que se utiliza como valor de referencia.

Todas las criptomonedas del mercado tienen cambio al bitcoin, ya que es la primera criptomonedas desarrollada con utilidad demostrada y se ha establecido como el token de referencia. A su vez, el bitcoin se puede cambiar a cualquier moneda de uso corriente, aunque normalmente se utiliza el dólar, como referencia, seguido del euro.

La base del bitcoin es el intercambio directo entre usuarios. La validación de las transacciones que estos realizan se efectúa mediante la minería de esta criptomonedas mediante un algoritmo llamado Proof-of-Work (PoW).

Hay muchas tiendas, tanto físicas como digitales, que admiten el pago mediante BTC, ya que se ha establecido como la principal moneda para pagos. El primer pago conocido por un bien o servicio en la historia se realizó el 22 de mayo de 2010, cuando un programador pagó por dos pizzas un total de 10.000 BTC, que por aquel entonces eran unos 80\$, pero que hoy en día equivaldrían a unos 500 millones de dólares.



12 DIC 2017 / SERIES

En 2010 pagaron 10 mil bitcoins por dos pizzas: Hoy equivale a más de 165 millones de dólares

En una época en que la divisa digital tenía una baja valoración un programador de Florida decidió pagar 10,000 bitcoins a quien le llevara un par de pizzas.

Por todo esto, es obvio que Bitcoin ha despertado todo tipo de sentimientos entre las élites financieras y la banca, que no veían con buenos ojos al bitcoin y el resto de criptomonedas, ya que les quitaría parte del poder que tienen y rompe el monopolio de la creación del dinero.

Actualmente los estados y organismos económicos gubernamentales tienen profundos debates sobre el desarrollo de un marco regulador que permita el uso de criptomonedas y un control eficiente de las mismas [2].

Así como hemos visto en el curso de Blockchain de cero a experto el funcionamiento de Bitcoin es revolucionario.

CAPÍTULO 2: ARQUITECTURA

ARQUITECTURA DISTRIBUIDA

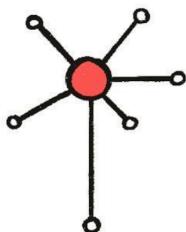


En la tecnología blockchain no hay un almacenamiento de datos centralizado ni una autoridad central sobre la gestión de datos. En el almacenamiento de datos tradicional, hay un servidor de datos y personas que tienen autoridad para acceder a los datos y manipularlos.

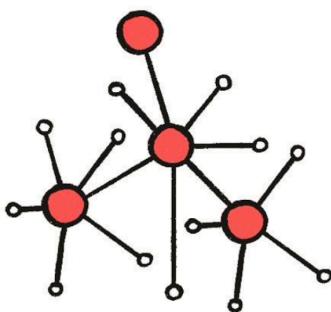
En la tecnología de cadena de bloques, la copia de la cadena de bloques o la base de datos de la cadena de bloques se almacena en todos los ordenadores de la red de cadena de bloques. Si alguien destruye de alguna manera un ordenador, miles de otros ordenadores de la red tienen la copia de la cadena de bloques.

Si alguien consigue cambiar algún dato de cualquier bloque de la cadena de bloques más larga, lo que es prácticamente imposible, los demás ordenadores de la red compararán su copia de la cadena de bloques con la modificada. Si no

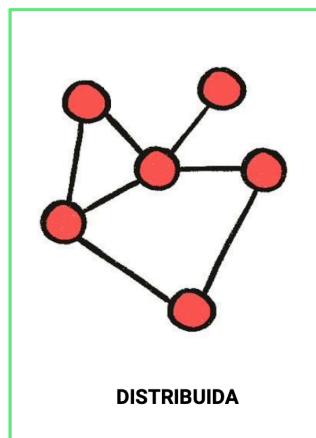
coincide con la copia de la cadena de bloques de la mayoría de los participantes de la red, la red de cadenas de bloques no aceptará la copia modificada de la cadena de bloques y, por lo tanto, la copia modificada de la cadena de bloques se perderá de la red.



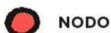
CENTRALIZADA



DESCENTRALIZADA



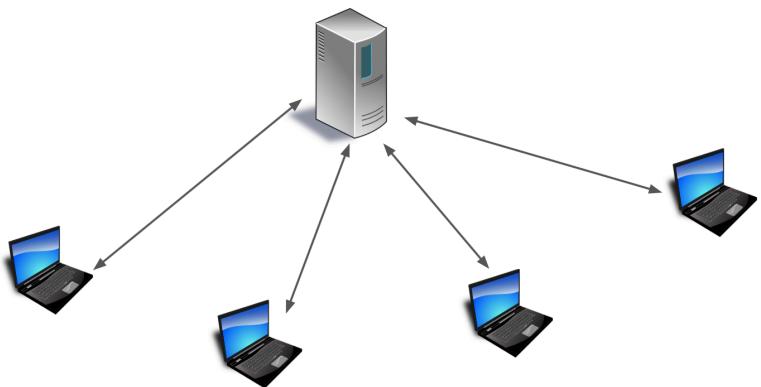
DISTRIBUIDA



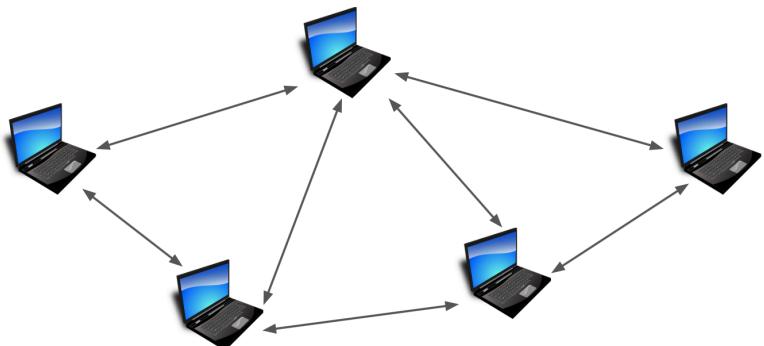
PEER-TO-PEER (P2P)



Tal como hemos explicado en el curso de Blockchain de cero a experto, P2P hace referencia al hecho de que la interacción entre los distintos participantes, llamados nodos, se realiza por parejas. Los nodos no están conectados todos entre sí, sino que cada uno está solamente conectado con un número determinado de ellos. El valor de esto puede verse en términos de eficiencia y anonimato. Cuando un nodo quiere informar al resto de nodos de una transacción, le envía la información sobre la misma a aquellos con los que está conectado y estos la replican con aquellos con los que ellos, a su vez, están conectados. El proceso se itera hasta que la información es compartida por toda la red. Esto ocurre siempre así, a no ser que la transacción enviada sea inválida -por ejemplo, si se pretende enviar dinero que no existe-, en cuyo caso cuando los nodos la “escuchan” simplemente la ignoran [1].



Modelo cliente - servidor



Peer-to-Peer (P2P)

CAPÍTULO 3: CARACTERÍSTICAS PRINCIPALES

SIN NECESIDAD DE CONFIANZA



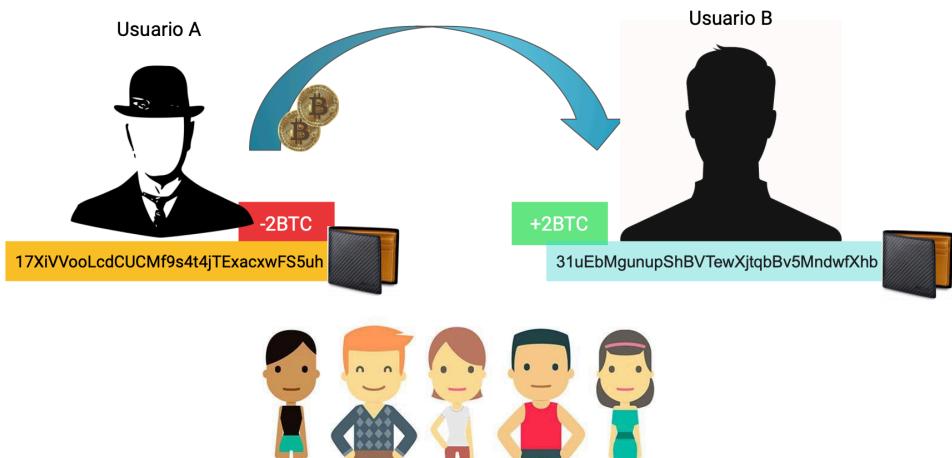
En las bases de datos utilizadas tradicionalmente se asume que todos los participantes son de confianza, es decir, que ninguno de los nodos -en el lenguaje que estamos utilizando- va a introducir en la base de datos información no veraz.

La idea revolucionaria de blockchain consiste en ofrecer un protocolo de consenso que permite que los distintos nodos no tengan por qué confiar unos en otros y aun así puedan compartir un registro de información confiable. El protocolo de consenso sirve para evitar que bloques con información no veraz sean añadidos a la cadena o que, si consiguiesen añadirse, sean rechazados por el resto de nodos.

TRANSPARENCIA



La información transparente es una demanda creciente, pero con nuestro actual sistema económico y digital no es del todo posible. Pero con la tecnología blockchain es posible crear un almacenamiento de datos descentralizado y altamente transparente. Cualquier transacción entre dos usuarios que se almacene en la cadena de bloques puede ser visible para todos los usuarios, aunque éstos pueden ser anónimos si no comparten su clave pública.

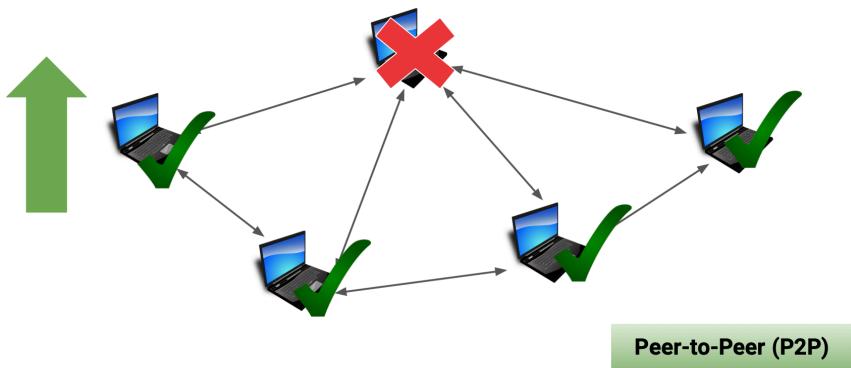
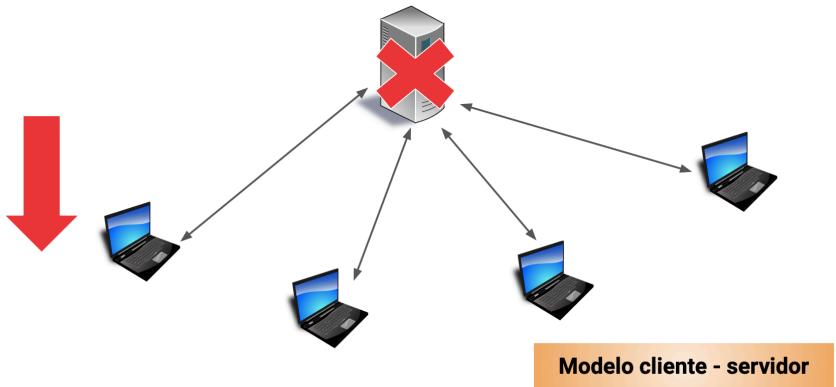


Cualquiera que tenga acceso a la cadena de bloques puede ver los datos y su historial. Sabemos cómo funciona Google Doc. Cada participante puede ver quién hizo qué cambios en qué momento. Del mismo modo, en la cadena de bloques, todos los participantes de la red pueden ver todos los cambios realizados en los datos. La cadena de bloques se actualiza constantemente y cada participante de la red tiene acceso a la cadena de bloques válida. En la cadena de suministro, la tecnología blockchain puede ofrecer la posibilidad de certificar, rastrear y localizar el origen de las mercancías. Y toda la información en estos pasos es transparente y verificable con confianza por el cliente.

ALTA DISPONIBILIDAD



Los datos que se almacenan en blockchain tienen un grado de disponibilidad muy alto en comparación con nuestra tecnología tradicional. Debido a que la copia de la base de datos de blockchain se almacena en los miles de nodos de todo el mundo y la naturaleza del mantenimiento colectivo de los datos. Cada nodo de la red trabaja por la seguridad y la integridad de la base de datos blockchain. Aunque todos los nodos de una ubicación geográfica pierdan su copia de la cadena de bloques, otros nodos de otra ubicación seguirán teniendo la copia de la cadena de bloques. Si una aplicación se ejecuta en la cadena de bloques, por ejemplo un contrato inteligente en la cadena de bloques de Ethereum, se garantiza que tendrá un tiempo de actividad muy alto hasta un futuro muy lejano [3].



INMUTABILIDAD



Una de las características más destacadas del curso de Blockchain de cero a experto es la inmutabilidad. Los datos en la cadena de bloques son a prueba de modificaciones, una vez que los datos se registran en la cadena de bloques son inmutables. Si un solo nodo u ordenador quiere hacerlo, no cambiará los datos de la cadena de bloques, a menos que el 51% de los nodos u ordenadores de la red de cadenas de bloques quieran hacerlo. Pero en la práctica, como la red de blockchain está formada por un gran número de nodos, no es posible hacer cambiar de opinión a un gran número de nodos para que realicen tareas deshonestas [3].



ANONIMATO



La tecnología blockchain ofrece la posibilidad de realizar transacciones o comercios de forma anónima y sin necesidad de confiar en los demás. En blockchain, un participante se identifica por su clave pública. Su información personal, como el nombre, la dirección de correo electrónico y los identificadores de usuario, se transforman en un valor hash criptográfico. Y este valor hash es como un token único y se almacena en blockchain. Es prácticamente imposible invertir el valor hash para obtener los datos. Así, incluso tu valor hash único es visible para todo el mundo en blockchain, pero eres anónimo para todos los participantes en la cadena de bloques. Tu identidad puede ser reconocida si sólo das tus datos personales que utilizaste para hacer el valor hash.



CONCLUSIONES

Una vez llegado al final de este libro, ya tienes una base de conocimientos realmente importante sobre la tecnología Blockchain.

Estos conocimientos son tan solo una pincelada de todo lo que se encuentra en este enorme entorno Blockchain que ahora mismo se encuentra en auge.

Te animo a que sigas aprendiendo y por eso tenemos un BONUS para ti:

Los cursos de Blockchain en los que hemos estado trabajando durante meses los podéis encontrar rebajados un 90% en el siguiente enlace:

<https://frogames.es/rutas-de-aprendizaje/ruta-de-blockchain/>

Espero que puedas avanzar y crecer en el mundo de Blockchain, que actualmente está marcando los pasos del presente y marcará los pasos del futuro.

REFERENCIAS

- [1] Marcos Allende López, “Cómo desarrollar confianza en entornos complejos para generar valor de impacto social”
- [2] bit2me, Bitcoin
- [3] Rakibul Hasan Sayed, Potential of Blockchain Technology to solve fake diploma problem

SOBRE EL AUTOR



Mi nombre es Joan Amengual, y soy graduado en Ingeniería Telemática por la Universidad de las Islas Baleares (UIB). En los últimos años he estudiado y trabajado sobre la tecnología Blockchain.

Concretamente, desarrollé una Aplicación Distribuida basada en Blockchain como Proyecto de Fin de Carrera para solventar la falsificación de títulos universitarios.

Juntamente con el equipo de investigación SECOM de la UIB, publicamos el artículo del proyecto Blockchain en la conferencia española de ingenieros telemáticos, JITEL 2021.

Mediante este pequeño libro pretendo dar a conocer las bases fundamentales y los pilares principales de la tecnología blockchain, y así dar a conocer todo su potencial de cara al presente y al futuro que nos espera.