AF4: Seguridad en la red

Blockchain y la seguridad en los bloques de información

Digitalización aplicada al sector productivo.
Módulo formativo sobre competencias digitales transversales básicas.

Gobierno de España · Ministerio de Educación y Formación Profesional
Plan de Recuperación, Transformación y Resiliencia
AxFP Alianza por la Formación Profesional
Financiado por la Unión Europea NextGenerationEU

Proyecto financiado por el Ministerio de Educación y Formación Profesional - *U.E. Next Generation*

Índice

1. INICIO

1.1 Introducción

Cada vez más, las organizaciones y las compañías están trabajando en la **implementación de *blockchain* en sus diferentes procesos o modelos de negocio**. ¿Por qué?

Los beneficios que aporta la tecnología *blockchain* o cadena de bloques en cuanto a **seguridad, credibilidad** y **eficiencia** resultan muy atractivos en muchos sectores como la banca, administración o las cadenas de suministro, por lo que muchas empresas están estudiando la manera de **implementar esta tecnología en algunos de los procedimientos** de estos sectores.

Las aplicaciones de la tecnología de bloques son múltiples, una de las más conocidas es la que dio origen al ***bitcoin***, la criptomoneda más famosa del mundo. Sin embargo, para comprender todas las capacidades que puede llegar a ofrecer *blockchain,* es necesario conocer la filosofía que hay detrás de su funcionamiento que, principalmente, se basa en la **descentralización** y en el **consenso colectivo** entre iguales.

Comienza este recorrido por la Unidad Didáctica dedicada al *blockchain* y descubre, de una vez por todas, en qué consiste la tecnología de la cadena de bloques y por qué todo el mundo está tan interesado en ella. ¡Adelante!

¿Qué vas a aprender en esta unidad?

2. INTRODUCCIÓN AL BLOCKCHAIN

2.1 ¿Cómo funciona el "blockchain" o cadena de bloques?

El *blockchain* o cadena de bloques se presenta actualmente como una de las tecnologías que mejor garantiza la confianza y seguridad de ciertas actividades que se pueden llevar a cabo en la red.

Se trata de una tecnología que muchas empresas están explorando para incorporarla en sus procesos ya que, **ofrece numerosos beneficios**.

Podemos **extraer los tres principales beneficios** que nos aporta esta tecnología:

Mayor confianza

La validación de una transacción o transferencia por **consenso colectivo** aporta confianza, si todos los **nodos** implicados están de acuerdo, es porque la operación es legítima.

Más eficiencia

Al ser una tecnología que requiere de una validación consensuada entre varios **nodos que están descentralizados**, se elimina la figura o **entidad intermediaria que concentra el poder** para certificar una transferencia, agilizando el proceso, evitando corruptelas o el peligro de ser objeto de ataques externos. Este hecho, clave en la cadena de bloques, refuerza todavía más la **confianza** y la **seguridad**.

Mayor seguridad

Con *blockchain* es prácticamente **imposible modificar o alterar** la información que ha sido validada, registrada y distribuida entre innumerables nodos con codificación ***hash***.

Las ventajas que ofrece la cadena de bloques en las transacciones económicas, como los pagos bancarios, son evidentes. Pero más allá de las transferencias bancarias, continuamente se están investigando nuevos campos para aplicar técnicas de *blockchain*, como por ejemplo en el seguimiento de la trazabilidad de productos y mercancías o en diversos procesos de certificación, como la emisión de certificados digitales, o el voto por correo electrónico.

2.2 Características del "blockchain"

Los tres beneficios principales que aporta la cadena de bloques se basan en la **confianza**, **eficiencia** y **seguridad**, pero si ahondamos un poco más en sus **características**, descubrimos que se trata de una tecnología capaz de ofrecer numerosas soluciones.

Vamos a describir y profundizar un poco más en las características de la cadena de bloques:

Inmutabilidad e integridad de la información

La tecnología de cadena de bloques se basa en un sistema de millones de nodos idénticos que reciben y validan la misma información. Quizás, sería posible modificar esta información atacando un solo nodo, pero es imposible modificarla de la misma manera en todos los nodos que forman parte de la cadena de bloques.

Por lo tanto, si en *blockchain* un nodo recibe un ataque, no pasaría nada, porque el resto de los nodos asegurarían la inmutabilidad del sistema: **la información permanece inalterable.**

Transparencia sin intermediación

Normalmente, en cualquier relación comercial, acuerdo o transacción existen personas o entidades que actúan como intermediarios para legitimar los procesos. Pueden ser notarías, bancos o entidades especializadas en los que **depositamos toda nuestra confianza** y que, además, cobran por sus servicios.

¿Qué sucede cuando las entidades intermediarias no son transparentes? Lamentablemente, esto a veces sucede y el coste que pagamos las personas es muy elevado.

Con la tecnología de la cadena de bloques es posible **prescindir de estas entidades intermediarias** y convertir la transacción en un **proceso completamente transparente y confiable.**

Procedencia y trazabilidad

Cada nodo **conoce, valida y registra cada uno de los pasos que se llevan a cabo en una transacción:** desde que se origina hasta su finalización o resolución.

Esta característica convierte a la cadena de bloques en una tecnología muy interesante en el **seguimiento de la trazabilidad**, ayudando a controlar y verificar la distribución de, por ejemplo, un determinado producto ecológico desde que se produce hasta que llega a la persona consumidora, garantizando su localización en todo momento y que obtiene todos los requisitos de calidad que se le exige.

Escalabilidad

La escalabilidad es la capacidad que tiene un sistema para **poder crecer sin comprometer su rendimiento.**

Privacidad

En *blockchain*, aunque las transacciones son públicas y se comparten entre todos los nodos que forman parte del sistema, es posible **proteger el anonimato de las personas** que intervienen en las transacciones, por lo que esta tecnología también puede resultar muy útil en procesos donde garantizar la privacidad de las personas es fundamental.

Cada día se realizan millones de transacciones comerciales y, cada vez más, resulta muy difícil certificar y registrar su legitimidad. La cadena de bloques es un sistema realmente eficaz y confiable a la hora de dar legitimidad a todo tipo de transacciones, por eso *blockchain* es considerado uno de los avances tecnológicos más revolucionarios de nuestros tiempos.

2.3 ¿Para qué sirve la cadena de bloques?

Marta, poco a poco, está asimilando la metodología que hay detrás del *blockchain* y entiende que las características intrínsecas de esta tecnología hacen que resulte muy útil en sectores donde la **confianza**, la **seguridad** y la **fiabilidad** de los datos es esencial.

En la ONG donde trabaja, por ejemplo, se podrían aplicar técnicas de *blockchain* en los **procesos de registro y valoración de los expedientes,** para gestionar datos personales o proyectos en colaboración con administraciones públicas y otras organizaciones sociales.

La tecnología de cadena de bloques en sectores como la **administración, sanidad, educación, justicia, banca** o **industria** resulta de gran interés.

SECTOR SALUD

Los historiales de cada paciente se podrían unificar y almacenar gracias a la cadena de bloques. La información estaría protegida y el personal sanitario podría **acceder a ella desde cualquier administración**, siempre y cuando formara parte del sistema.

TRÁMITES ADMINISTRATIVOS

Como la cadena de bloques **impide alterar o falsear la información**, resulta un sistema muy útil para registrar todo tipo de documentación administrativa o legal: escrituras, contratos, resoluciones, informes, autorizaciones, reclamaciones, pagos tributarios, certificados digitales, etc.

CADENAS DE SUMINISTRO

Con *blockchain* es posible introducir un **sistema de trazabilidad en las cadenas de suministro** para asegurar que se realizan todas las operaciones indispensables para que una mercancía logre llegar a la clientela final en óptimas condiciones.

El objetivo final de un sistema de trazabilidad es dar a las personas consumidoras las garantías necesarias acerca de la procedencia legítima y de una producción y distribución del producto conforme a las normas de calidad requeridas y a legislación vigente, asegurando la **integridad de la cadena de suministro** y la protección de las mercancías contra fraudes.

2.4 Contratos inteligente

Tal y como estamos viendo, el *blockchain* no deja de ser un **registro de transacciones** que pueden representar casi cualquier cosa, como, por ejemplo:

- Una transferencia bancaria.
- Una emisión de un certificado digital.
- La verificación de una compra o trámite.
- La firma de un contrato.

La tecnología asociada a la cadena de bloques nos permite dar un paso más allá y llegar a un nuevo concepto en vías de desarrollo conocido como el **contrato inteligente**.

Un contrato inteligente es un **conjunto de instrucciones programadas** que nos indican que cuando se dan determinadas condiciones, es posible ejecutar una acción, por ejemplo, realizar la compra de un producto automáticamente, si su precio baja a una determinada cantidad.

Proceso del contrato inteligente:

La clave de los contratos inteligentes radica en la posibilidad de **automatizar ciertas transacciones de forma transparente, sin conflictos y sin intermediarios**, pero para que un contrato inteligente pueda ejecutarse es necesario establecer previamente unos pactos de consenso también conocidos como **algoritmos de consenso**.

Los algoritmos de consenso son sistemas pactados mediante una serie de indicadores que se pueden utilizar en los contratos inteligentes.

Existen muchas situaciones en los ámbitos laborales en las que la utilización de "pactos de consenso" pueden ayudar en la resolución de problemas. Un ejemplo extremo es su uso en los contextos de guerra, donde se dan **situaciones críticas** en las que fijar unos **pactos por consenso** puede ser decisivo. Estas dos historias ilustran muy bien dos problemas concretos que podrían solucionarse mediante pactos de consenso previos.

Historia 1

El problema de los 2 generales. Publicado en 1975.

Dos generales tienen que atacar a un enemigo común a la vez. El general A tiene el mando sobre el general B.
Ninguno de los dos ejércitos tiene la fuerza suficiente como para acabar con el enemigo común si no es en un ataque coordinado, así que el entendimiento es esencial.
Ahora se complica la cosa: para comunicarse, el general A necesita mandar un mensajero que cruce al campo del enemigo hasta llegar a contactar con el general B y darle la orden de atacar.
Si el enemigo captura al mensajero, el general B nunca recibiría la orden y el general A atacaría en solitario, perdiendo la batalla.
Si el mensaje llega al general B, este mandaría un mensaje de vuelta diciendo que el ataque puede realizarse.
En este problema, ¿el general A puede garantizar que el primer mensajero no haya sido capturado y la noticia de la confirmación del ataque sea cierta?

Historia 2

El problema de los generales bizantinos. Publicado en 1982.
Es una vuelta más de tuerca al problema anteriormente descrito.
Es el mismo escenario con la salvedad de que ahora son más generales y algunos de ellos pueden ser traidores y mentir sobre su voluntad de atacar.
El paradigma de mando anterior se ve también alterado y ahora son comandante y teniente. El consenso se consigue cuando se ponen de acuerdo para atacar o retirarse.
Ese acuerdo se logra mediante la mayoría de las voluntades apreciadas por el teniente, siendo suficientes dos terceras partes para tomar una determinación. Por lo tanto, siempre se llegará a un acuerdo si menos de una tercera parte de las tropas resultan desleales.
Esto se conoce como **tolerancia a faltas bizantinas o tolerancia a fallas bizantinas (BFT)**.
La falta bizantina es el problema de fallo más difícil de resolver, ya que no implica restricciones y no presupone la intencionalidad de un nodo. Es un fenómeno grave y difícil de tratar.
La BFT se aplica en sistemas con gran número de sensores, como pueden ser centrales nucleares o motores de avión: el sistema tolera faltas bizantinas hasta un tercio de los "traidores".

Aunque todavía es necesario superar algunos obstáculos para implementar *blockchain* en muchos procesos, estamos frente a una tecnología con un gran potencial de revolucionar la forma en la que establecemos acuerdos y en la que depositamos nuestra confianza en el sistema socioeconómico tal y como lo conocemos hasta ahora.

3. CRIPTOMONEDAS

3.1 Historia del "bitcoin"

Bitcoin es la primera red descentralizada que se creó, aplicando tecnología *blockchain,* para obtener dinero electrónico o digital, también conocido como criptomoneda.

En 2007, una persona bajo el seudónimo de **Satoshi Nakamoto** movilizó la posibilidad de **construir dinero digital a partir de un sistema descentralizado** que no estuviera controlado por los bancos tradicionales y a la vez mantuviera la confianza de las personas en el intercambio de las nuevas monedas.

El objetivo principal era no depender de los bancos centrales de cada país y crear una **red digital pública con datos anónimos y con información visible entre iguales** usando **software libre de código abierto**.

Así nació *bitcoin*, la **criptomoneda más extendida del mundo**, y el primer sistema distribuido tolerante a fallos gracias a sus principales ventajas:

- Seguridad: sus registros no se pueden modificar.
- Ahorro de costes: como no existe una entidad emisora, se ahorran los costes de su existencia.
- Transparencia: todos los nodos de *bitcoin* pueden ser consultados al tratarse de un libro de cuentas compartido y público.

La red *bitcoin* ha demostrado ser extremadamente segura y solo se ha documentado un único problema importante de seguridad desde su origen.

¿Sabías que...?

El 6 de agosto de 2010 se detectó una vulnerabilidad en la cadena por la que las transacciones no se verificaban, lo que permitió generar 184.000 millones de *bitcoins* que fueron enviados a dos cuentas. En pocas horas, la transacción se detectó y fue eliminada de todos los registros. Finalmente, se actualizó un nuevo protocolo *bitcoin* más seguro para evitar fraudes.

La relación entre *bitcoin* y *blockchain* es tan estrecha, que a menudo se confunden los dos conceptos como si fueran sinónimos. Es importante destacar que, al igual que se emplea en otro tipo de aplicaciones o plataformas, *blockchain* es únicamente la tecnología subyacente de *bitcoin.*

3.2 Criptomonedas más utilizadas

Bitcoin fue la primera criptomoneda que surgió y sigue siendo la más conocida, pero existen más de 10.000 tipos de criptomonedas, algunas de ellas de gran relevancia.

La criptomoneda, también conocida como moneda o dinero digital, es un medio digital para realizar transacciones económicas.

Su característica principal, además de que la mayoría están basadas en la tecnología de cadena de bloques, es que **no depende de la intervención de un organismo centralizado**, como los bancos, para regular su funcionamiento.

Las criptomonedas más conocidas son las siguientes:

ETHEREUM

Ethereum, además de ser una plataforma de código abierto muy conocida para programar contratos inteligentes, también es una criptomoneda muy utilizada para realizar operaciones financieras.

MONERO

Monero es una criptomoneda de código abierto que se originó en 2014 y se caracteriza por ser anónima, es decir, tanto la información de las cantidades trasladadas como la de la identidad de emisor y receptor queda oculta.

ZCASH

Esta criptomoneda, que surgió en 2016, se caracteriza porque además de ocultar los detalles de las transacciones, también puede proteger la identidad de las personas que intervienen, por lo que es más atractiva para los ciberdelincuentes.

DASH

Se trata de una criptomoneda de código abierto muy parecida al *bitcoin*, pero con posibilidades más avanzadas, como por ejemplo la de emplear una compleja técnica para mezclar diferentes transacciones, algunas falsas, y así enmascarar las reales.

Una de las principales desventajas de la moneda tradicional frente a las criptomonedas es la territorialidad acotada en la que pueden funcionar. Cada país tiene su propia moneda que, además, está sujeta a diversos trámites de validación de las entidades intermediarias, como los bancos centrales.

Otra consecuencia de esto es que las transacciones que se producen entre diferentes países pueden llegar a ser demasiado lentas, sin olvidar el riesgo del factor humano, pues muchas operaciones se realizan de forma manual.

¿Sabías qué...?

La relación entre la ***dark web*** y las criptomonedas es muy estrecha, pues muchas de las transacciones que se realizan en la red oscura utilizan este tipo de divisas. Cabe destacar el dato llamativo del enorme enriquecimiento que cosecharon algunos delincuentes de bajo nivel que operaban con ***bitcoin*** en la ***dark web***, no por sus actividades, sino por la gran revalorización que se produjo de la criptomoneda y los beneficios que esta generó.

4. CIERRE

4.1 Resumen

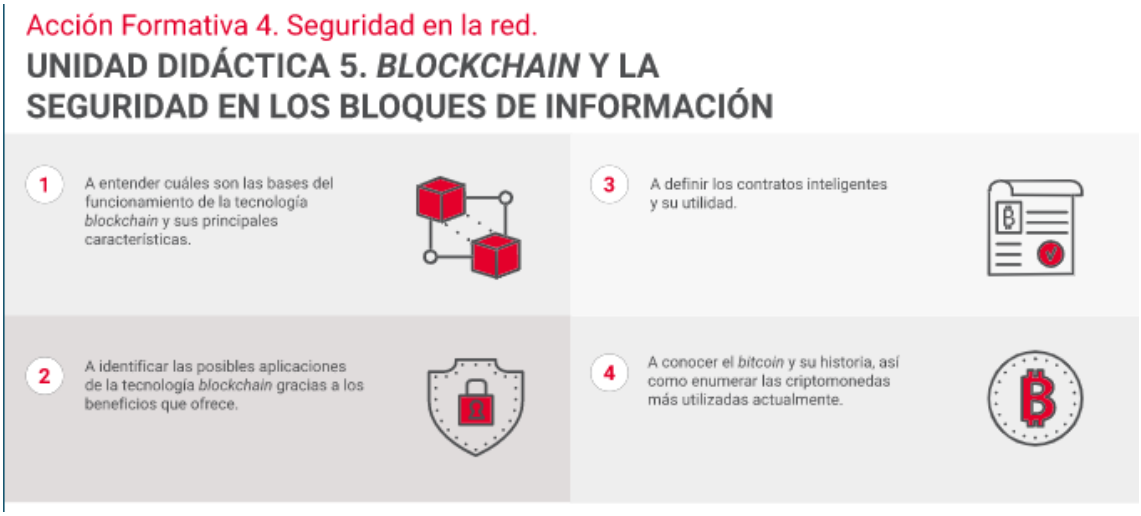
¿Qué le ha ocurrido a nuestra protagonista?

Marta, en los últimos tiempos, ha oído hablar bastante sobre las criptomonedas, el *bitcoin* y *blockchain,* pero para ella todo formaba parte de una misma idea que le remitía a algo muy complejo y difícil de comprender.

Gracias a esta Unidad Didáctica, Marta ha sido capaz de comprender **en qué consiste la tecnología *blockchain*** y su gran potencial para garantizar la **seguridad** y la **confianza** en la ejecución de ciertas acciones o actividades en la red. Sobre todo, le ha quedado muy claro que la cadena de bloques es una técnica que no solo puede aplicarse en las transacciones económicas, sino que también puede implementarse en algunas de las tareas que ellos deben llevar a cabo en la ONG como cuando **piden la certificación de algún expediente o trámite burocrático en la administración,** agilizando el proceso y garantizando la seguridad.

También le ha quedado claro que *blockchain* y *bitcoin,* aunque están relacionadas, no son lo mismo, sino que la tecnología *blockchain* ha hecho posible la aparición de *bitcoin*, al igual que otras **criptomonedas**, concepto que, por cierto, también le ha quedado más claro.

¿Y qué has aprendido a hacer?



El mundo de la tecnología abre muchas puertas, ofrece un montón de soluciones y es apasionante. Marta está aprendiendo mucho y empieza a tener una visión más completa y global de las implicaciones que hay detrás de las nuevas tecnologías. Por ejemplo, con *blockchain* le ha quedado muy claro que una de las ventajas que ofrece es evitar los intermediarios, lo que le lleva a preguntarse lo siguiente: ¿Cómo podemos proteger nuestra información y datos personales en la red? ¿Hay intermediarios? ¿A quién cedemos nuestros datos cuando utilizamos aplicaciones digitales?
Te lo contamos en la siguiente Unidad Didáctica dedicada a la identidad digital y presencia en las redes.

4.2 Referencias bibliográficas

A continuación, puedes ver la relación de recursos (artículos, estudios, investigaciones, páginas web...) que se han consultado y citado para elaborar el contenido de esta Unidad Didáctica:

- Criptonoticias, 2020. Un bug permitió emitir 184 mil millones de Bitcoin, hace 10 años. Recuperado de: https://www.criptonoticias.com/comunidad/bug-emitir-184-mil-millones-bitcoin-10-anos/ [14/02/2022]
- IBM. ¿Qué es la tecnología de blockchain? Recuperado de: https://www.ibm.com/es-es/topics/what-is-blockchain [14/02/2022]
- La Vanguardia, 2021. ¿Qué es una criptomoneda? ¿Cuál es su futuro? Recuperado de: https://www.lavanguardia.com/tecnologia/20211224/7947456/como-explicarle-madre-navidad-que-nft-bitcoin-pmv.html#:~:text=Las%20criptomonedas%20no%20son%20m%C3%A1s,existe%20en%20el%20mundo%20virtual [14/02/2022]
- SAP. ¿Qué es la tecnología de blockchain? Recuperado de: https://www.sap.com/latinamerica/insights/what-is-blockchain.html [14/02/2022]
- Telefónica Grandes Empresas. 2020. #TEF_SmartTalks: BLOCKCHAIN [Vídeo]. YouTube. Recuperado de: https://www.youtube.com/watch?v=CfHOtOOoxLs [14/02/2022]
- Xataka. Qué es blockchain: la explicación definitiva para la tecnología más de moda, 2018. Recuperado de: https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda [14/02/2022]