Centro de Estudios de Postgrado

Máster en Profesorado de Enseñanza Secundaria Obligatoria, Bachillerato, Formación Profesional y Enseñanza de Idiomas

UNIVERSIDAD DE JAÉN
Centro de Estudios de Postgrado

Trabajo Fin de Máster

INTRODUCCIÓN A LA TECNOLOGÍA BLOCKCHAIN

Alumno/a: **Quesada Real, Francisco José**

Tutor/a: Prof. Dña. Carmen Martínez Cruz
Tutor/a: Prof. D. Pedro González García

Dpto: Departamento de Informática

Junio, 2019

Índice general

Capítulo 1

Resumen

1.1. Resumen y palabras clave

Este Trabajo Fin de Máster perteneciente al Máster en Profesorado de Educación Secundaria Obligatoria, Bachillerato, Formación Profesional y Enseñanza de Idiomas, tiene como tema principal la "Introducción a la Tecnología Blockchain".

El trabajo consta de dos partes diferenciadas. En primer lugar, se realiza un estudio epistemológico en el que se detallan los antecedentes, el estado del arte, la tecnología Blockchain, las tendencias futuras y las conclusiones. Esta parte será la base teórica de los conceptos que se usaran posteriormente.

La segunda parte recoge una proyección didáctica en la que se contextualiza un centro de enseñanza secundaria y se desarrolla una unidad didáctica sobre los conceptos vistos en la primera parte.

PALABRAS CLAVE: Cadena de bloques, contrato inteligente, libro de cuentas distribuido, algoritmo de consenso.

1.2. Summary and keywords

In this master thesis belonging to the master called "Máster en Profesorado de Educación Secundaria Obligatoria, Bachillerato, Formación Profesional y Enseñanza de Idiomas" the main topic is the "Introduction to the Blockchain Technology".

This master thesis has two parts. The first one includes an epistemological study in which there are detailed the background, the state of the art, the

Blockchain technology, the future trends, and some concluding remarks. This part is the theoretical framework of the master thesis.

The second part contains a teaching unit which is contextualised to a secondary school and that develops the concepts explained in the first part.

KEYWORDS: Blockchain, smart contract, distributed ledger, consensus algorithm.

Capítulo 2

Introducción

Desde el origen de las bases de datos relacionales hasta nuestros días, la mayor parte de la información en formato digital se viene almacenando en bases de datos en las que una autoridad central es quien, en última instancia, tiene el control total de la información.

El nacimiento de la criptomoneda Bitcoin, trajo consigo una tecnología que sin necesidad de una autoridad central, garantizaba la autenticidad de los registros almacenados en el sistema, haciendo responsables de su control a los usuarios del mismo.

En un principio, se creía que el uso de esta tecnología estaba restringido únicamente al ámbito financiero, donde se era capaz de certificar transacciones de activos de unos usuarios a otros sin la necesidad de un banco que a modo de intermediario certificase la transacción. Sin embargo, unos años más tarde, se llegó a la conclusión de que la tecnología detrás de Bitcoin podía aplicarse a otros ámbitos en los que se requiere la certificación de la información. Algunos ejemplos pueden ser el voto electrónico, la cadena de suministros o la gestión energética.

En los último años, esta tecnología se está extendiendo de manera vertiginosa por áreas muy diversas. Las principales propulsoras de este hecho son las multinacionales más importantes del mundo que están invirtiendo en la implantación de esta tecnología dentro de sus empresas. Este hecho hace que actualmente sea un momento idóneo para formarse en esta nueva tecnología, ya que son escasos los profesionales que dominan la tecnología Blockchain y cada vez más las demandas de este tipo de perfiles en el mercado laboral. Por este motivo se considera de vital importancia la enseñanza de esta tecnología.

El presente trabajo fin de máster presenta un estudio epistemológico y una

Unidad Didáctica (U.D.) centrados en la introducción a la tecnología Blockchain, con el principal objetivo de proveer al alumnado de los conocimientos básicos para poder iniciarse en esta nueva tecnología.

Capítulo 3

Estudio Epistemológico

En este capítulo se recoge el estudio epistemológico referente a la tecnología Blockchain. En primer lugar, se verán los antecedentes de esta tecnología. Seguidamente, se hará un recorrido por su estado del arte. Posteriormente, se recogerán los principales conceptos de la tecnología. El capítulo finalizará con la descripción de tendencias futuras y algunas conclusiones.

3.1. Antecedentes

Con la evolución de las computadoras, la generación de información se incrementó de manera considerable lo que hizo que surgiese la necesidad de almacenar grandes cantidades de información. Motivados por esta necesidad (Codd, 1970) definió el modelo de bases de datos relacionales, así como las reglas para poder evaluar a un administrador de dichas bases de datos.

En un principio el almacenamiento de la información se realizaba de modo centralizado, pero con el paso del tiempo las necesidades fueron cambiando, dándose situaciones que no eran posible de solucionarse de manera eficiente de forma centralizada. Estos problemas impulsaron la creación del almacenamiento distribuido, que combinaba la tecnología de la redes de comunicación y de las bases de datos, tal y como indica (Ozsu & Valduriez, 2011).

Entre los factores determinantes que han motivado la aparición de bases de datos distribuidas destaca la globalización del mundo empresarial en el que es normal encontrar empresas con sedes en distintos lugares lo que las hace que sean cada más descentralizadas geográficamente.

La principal diferencia entre una base de datos centralizada y una base de

datos distribuida está en que mientras que en la primera, la base de datos se encuentra en un servidor central al los usuarios deben conectarse para acceder a la información, mientras que en el segundo caso todos los nodos contienen la información.

La unión entre las tecnologías de redes de computadores y las bases de datos, propiciaron que aprovechándose las distintos topologías de las redes se crease una nueva base de datos denominada base de datos descentralizada, (Kohler, 1981). En este tipo de base de datos no existe un almacenamiento central, sino que son algunos servidores los que proporcionan información a los usuarios, estando estos servidores conectados entre sí.

La representación de estos tres tipos de bases de datos se muestra en la figura 3.1

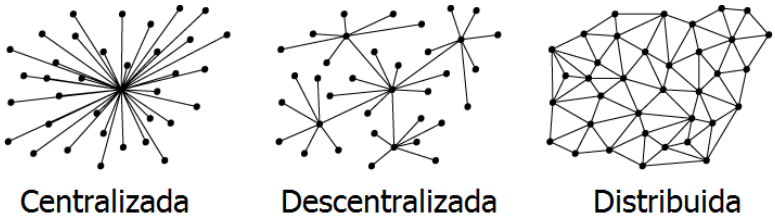

Figura 3.1: Tipos de bases de datos.

Estos conceptos de almacenamiento distribuido y descentralizado fueron usado por (Nakamoto, 2008) para el almacenamiento de las transacciones de la criptomoneda Bitcoin. El principal motivo por el que se decantó por este tipo de almacenamiento radica en la necesidad de eliminar cualquier autoridad central necesaria para la certificación de las transacciones (Olnes, Ubacht, & Janssen, 2017).

3.2. Estado del arte

Con el nacimiento de la criptomoneda Bitcoin creada por (Nakamoto, 2008) se crea una estructura denominada *Blockchain* (cadena de bloques) capaz de gestionar las transacciones de Bitcoin. Unos años más tarde, (Buterin, 2013) contribuirá para que la tecnología utilizada en Bitcoin se pudiera aplicar a otras áreas. Es aquí cuando comienza la vertiginosa expansión de esta tecnología en lo que se conoce como la revolución Blockchain (Crosby, Pattanayak, Verma, & Kalyanaraman, 2016).

La idea básica detrás de la tecnología Blockchain es que permite a los actores del sistema (llamados nodos) hacer transacciones digitales de activos usando una red *peer-to-peer* (p2p) que almacena estas transacciones de manera distribuida por la red. Los dueños de los activos, y las transacciones involucradas en el cambio de propiedad, son registradas en el libro de cuentas (en inglés, *ledger*) mediante el uso de claves públicas criptográficas y firmas digitales (Warburg, 2016). Cada transacción es validada por los nodos de la red usando un mecanismo de consenso (protocolo de consenso). Esto funciona de la siguiente manera. En el momento en el que una transacción entra en la red p2p, los nodos validan la transacción en primera instancia. Si los nodos están de acuerdo confirman la transacción y se escribe en un bloque. Este nuevo bloque se añade a una cadena de bloques previa, bloqueando así su contenido. De este modo, el último bloque mantendrá una vista consensuada y compartida del estado actual de la cadena de bloques (Buterin, 2013).

Todas las transacciones son almacenadas en un libro de cuentas y cada nodo involucrado tendrá una copia de dicho libro. Los bloques almacenarán lotes de transacciones con registro de tiempo. Por razones de seguridad cada bloque incluirá una referencia hash del bloque anterior. Este hash es usado para identificar la información y asegurar la integridad de los datos. Los bloques enlazados forman una cadena de bloques, de ahí el nombre de *cadena de bloques*. La creación de nuevos bloques se designa por el término "*minar*". Hay que destacar que la seguridad en la cadena de bloques no la dan los hash que enlazan los bloques. Estos solamente hacen que los cambios dentro de la cadena de bloques sean fácil de descubrir (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016).

Un libro de cuentas contiene el estado consensuado y compartido de la cadena de bloques, y la lista de transacciones que fueron procesadas por los nodos. Cada nodo de este sistema descentralizado tiene una copia de la cadena de bloques que es sincronizada continuamente con el resto de copias. De este modo, no hay ningún punto centralizado de vulnerabilidad que pueda ser aprovechado por hackers. Así, la eliminación de un nodo de la red no conlleva la caída de la cadena de bloques. Esta típica arquitectura p2p contribuye tanto a la seguridad como a la inmutabilidad de las transacciones registradas en la cadena de bloques. Además, el protocolo de consenso distribuido asegura la integridad de los datos de las transacciones.

Sin embargo, esto no significa que la cadena de bloques sea inalterable. Los

grupos que configuran la cadena de bloques pueden decidir alterar el histórico de la cadena de bloques. Un ejemplo lo podemos encontrar en Ethereum[1] donde en el año 2016 la cadena de bloques se dividió en dos debido a distintos puntos de vista sobre cómo actuar en caso de un ataque a la red (Atzei, Bartoletti, & Cimoli, 2016). Por tanto, aunque una cadena de bloques sea a prueba de falsificación debido a los enlaces entre bloques basados en hash, esto no significa que sea inalterable (Narayanan y col., 2016). Ninguna tecnología Blockchain puede garantizar la total inmutabilidad, ya que un acuerdo entre los grupos que controlan la cadena de bloques puede derivar en una adaptación de la cadena de bloques (Gervais y col., 2016). Y en caso en el que ocurra una discrepancia en el proceso adición de bloques, que deriva en una división de la cadena en dos, entonces la red resuelve este hecho añadiendo bloques a la cadena más larga (Nakamoto, 2008).

Un contrato inteligente (*smart contract* en inglés) es un programa que se ejecuta en la cadena de bloques y tiene su correcta ejecución reforzada por el protocolo de consenso (Luu, Chu, Olickel, Saxena, & Hobor, 2016). Un contrato inteligente contiene la información sobre un acuerdo y sólo será ejecutado si las condiciones son validadas por todos los nodos de la red (Luu, Narayanan, y col., 2016).

Un ejemplo que ilustre el funcionamiento de un contrato inteligente puede ser la transferencia de una propiedad de un dueño a otro, por ejemplo, una casa. El comprador de la casa introduce en un bloque la suma de dinero necesario para pagar la propiedad. Solo si el comprador le da su clave al vendedor con cierto tiempo, el pago será procesado y el registro de la propiedad será actualizado en la cadena de bloques. Si la clave no es transferida, entonces el dinero vuelve al comprador. El contrato inteligente contiene reglas que no pueden ser cambiadas durante el proceso.

Probablemente la mayor diferencia que existe entre la tecnología Blockchain y las tecnologías digitales convencionales radica en su naturaleza distribuida. Las cadenas de bloques consisten en libros de cuentas distribuidos que son sincronizados por medio de mecanismos p2p y reglas preacordadas sobre qué nuevos datos pueden ser añadidos. Esto cambio con respecto las situaciones convencionales en las que un responsable mantenía una base de datos con toda la información y decidía sobre las responsabilidades de crear, leer, actualizar y

[1] https://www.ethereum.org

eliminar información.

Además de la Blockchain de Bitcoin y la de Ethereum (Wood, 2014), en los último años han surgido numerosas propuestas entre las que destacan IOTA[2] e Hyperledger.

IOTA es una Blockchain pensada para almacenar información proveniente de sensores de dispositivos conectados a Internet por lo que incorpora una cadena de bloques adaptada para ello denominada *tangle*. Esta estructura fue propuesta por (Popov, 2016) y tiene como principal novedad la incorporación de un algoritmo de poda que permite aligerar la cadena de bloques. Hyperledger es un framework que incorpora distintos proyectos entre los que destaca Hyperledger Fabric (Cachin, 2016) que permite la configuración de cadenas de bloques privadas.

En la actualidad podemos encontrar distintas aplicaciones de la tecnología Blockchain en distintos ámbitos de vida diaria. (Burger, Kuhlmann, Richard, & Weinmann, 2016) y (Lavrijssen & Carrilo, 2017) son ejemplos de soluciones que usan la tecnología Blockchain aplicadas al sector energético. (Hoy, 2017) por su parte trata de aprovechar esta tecnología aplicándola al sector sanitario y (Music, 2015) hace lo propio en lo que respecta a la industria musical.

3.3. Tecnología Blockchain

Desde mediados del siglo pasado las tecnologías de la computación han presentado una evolución yendo desde un modo centralizado hasta un modo descentralizado en lo referente a almacenamiento, poder de cómputo, infraestructura, protocolos y código.

Según (Ali, 2017), en estos momentos estamos asistiendo a una transición desde la computación, almacenamiento y procesamiento centralizado hacia arquitecturas y sistemas descentralizados. Según el autor, estos sistemas tienen el objetivo de "*dar un control explícito de los activos digitales a los usuarios finales y eliminar la necesidad de una autoridad externa que garantice la confianza del sistema*"

En la actualidad la tecnología capaz de cumplir con este objetivo es la tecnología Blockchain, también denominada de libro de cuentas distribuido (*distributed ledger* en inglés).

En el siguiente apartado se describen los componentes de una Blockchain.

[2]https://www.iota.org

3.3.1. Componentes

- *Libro de cuentas*. Registro distribuido e inmutable de un histórico.
- *Red de nodos*. Almacena, actualiza y mantiene el libro de cuentas. Cada nodo de la red guarda una copia del libro de cuentas. Otro de los cometidos de la red es consensuar los contenidos de cada actualización del libro de cuentas. Esto asegura que cada nodo tenga una copia idéntica del libro de cuentas sin la necesidad de una copia centralizada de carácter "oficial".
- *Servicio de altas*. En algunas cadenas de bloques todo el mundo puede unirse a la red de nodos y todos los miembros de la red tienen la misma autoridad y poder. Sin embargo, en algunas cadenas de bloques es necesario obtener un permiso previo que autorice la entrada a los usuarios. El servicio de altas será el encargado de autenticar, autorizar y gestionar la identidad de los usuarios en la cadena de bloques.
- *Contrato inteligente*. Se trata de un programa que se ejecuta en la cadena de bloques. Este programa tiene una series de condiciones que en caso de cumplirse desencadenan unas acciones determinadas.
- *Monedero*. Es el lugar donde el usuario almacena sus credenciales y realiza el seguimiento de los activos digitales asociados a la dirección del usuario. donde se guardan las credenciales de los usuarios. En el monedero se monitoriza toda la información asociada a la cuenta del usuario.
- *Eventos*. Notificaciones de las actualizaciones y acciones en la cadena de bloques.
- *Sistemas de gestión*. La cadena de bloques está diseñada para ser un sistema duradero en el tiempo dentro de un campo está en continua evolución. Los sistemas de gestión añaden a la cadena de bloques la capacidad de crear, modificar y monitorizar los componentes de la cadena de bloques para que se puedan adaptar a las necesidades de los usuarios.
- *Sistemas de integración*. La evolución de la tecnología Blockchain y el aumento de las funcionalidades dentro de las cadenas de bloques han dado lugar a la integración de cadenas de bloques con sistemas externos, normalmente mediante el uso de "*contratos inteligentes*".

3.3.2. Tipos de Blockchain

Dentro de las cadenas de bloques podemos diferenciar dos entre *permissioned* y *permissionless*, tal y como especifica (López & Mora, 2016).

- *Permissionless Blockchain.* Este tipo de Blockchain es conocido para cadena de bloques pública ya que cualquier usuario puede unirse a la red.
- *Permissioned Blockchain.* También se le conoce como cadena de bloques privada. En este caso los usuarios no pueden unirse a la red a menos que la autoridad que gestiona la cadena de bloques les conceda los permisos necesarios para ello.

La elección de un tipo u otro vendrá condicionada por la aplicación que tendrá la cadena de bloques. Si se van a almacenar información interna de una empresa, lo adecuado sería que se usase una Blockchain privada. Por el contrario, si se desea mejorar la transparencia de cara a ganar confianza de los clientes, por ejemplo almacenado la trazabilidad de un producto alimenticio, entonces la mejor elección será la Blockchain pública.

3.3.3. Criptografía en la cadena de bloques

La criptografía juega un papel fundamental en la tecnología Blockchain ya que dota al sistema de funcionalidades de seguridad a la hora llevar a cabo las transacciones en la cadena de bloques. Entre los tipos de criptografía más usados encontramos:

Criptografía de clave pública

La criptografía de clave pública usa un par de claves, una clave pública y una clave privada, para llevar a cabo las tareas de cifrado y descifrado. La clave pública se distribuirá, mientras que la clave privada la mantendrá el usuario en secreto.

Usando la clave pública de una persona es posible encriptar un mensaje de manera que sólo esta persona pueda desencriptarlo haciendo uso de su clave privada. Usando una clave privada, se puede crear una firma digital de manera que cualquier persona que tenga la clave pública asociada pueda verificar que el

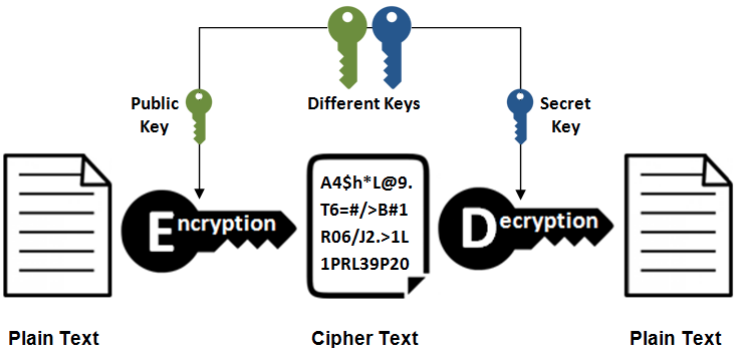

Figura 3.2: Ejemplo de criptografía de clave pública.

mensaje fue creado por el propietario de la clave privada y que éste no ha sido modificado. La figura 3.2 muestra un ejemplo de criptografía de clave pública.

Actualmente, la tecnología Blockchain hace uso de este tipo de criptografía.

Zero-knowledge proof

Denominamos con este término a la capacidad de probar un secreto sin la necesidad de revelar el mismo.

Un ejemplo de esta técnica puede ser el siguiente: Imaginemos que tenemos dos motos de juguete con la misma forma, modelo, tamaño, pero con un color distinto, una de color rojo y otra de color verde. Juan que es daltónico y no puede distinguir los colores, coge las dos motos y las esconde en su espalda. Después Juan coge una moto y se la enseña a Juan, tras unos segundos la esconde y repite el proceso con la otra moto. Antonio puede detectar el cambio ya que las motos tienen distintos colores, pero si nunca le dice la diferencia a Juan, el secreto estará a salvo.

En esta técnica se fundamenta la Blockchain, ya que todos los usuarios tendrán una copia en su equipo, pero sólo podrán conocer las transacciones en las que estén involucradas sus claves.

Funciones Hash

Estas funciones cobran un papel fundamental en la tecnología Blockchain. Una función hash es una ecuación matemática que cuenta con las siguientes propiedades:

- Pueden tomar cualquier valor de entrada y crear una salida con un tamaño fijo. Esto hace posible que se pueda condensar cualquier información en

un tamaño fijo. Así es como los mensajes son condensados en las firmas digitales.

- El cálculo de un hash es fácil, pero averiguar el dato de entrada a partir del hash generado es extremadamente complejo. La mejor opción es probar con distintos valores de entrada hasta que la función genere el hash de salida deseado.

- Las entradas que se diferencian en un solo bit dan como resultado hashes que difieren, de media, en más de la mitad de los bits. Esto hace que no sea posible descubrir el valor de entrada de la función mediante el uso del algoritmo de Ascenso de Colinas propuesto por (Tsamardinos, Brown, & Aliferis, 2006).

- Dado que una función hash puede tomar cualquier valor de entrada y producir una salida con un tamaño fijo, tiene sentido que distintas entradas diferentes puedan producir una misma salida. Una buena función hash deberá estar diseñada para que sea necesario probar un gran número de valores de entrada antes de encontrar dos valores que produzcan la misma salida.

Dentro de la tecnología Blockchain, la estructura de datos una de las estructuras de datos más utilizadas es el árbol Merkle y que está basado en funciones hash, como se puede ver en (Szydlo, 2004).

- *Árbol Merkle*
  Se trata de un árbol binario cuyos nodos hoja contienen los valores a almacenar y en cada nodo interno existe un hash de sus dos nodos hijo, tal y como se puede observar en la figura 3.3.

  Este tipo de estructura hacer posible que una gran cantidad de datos separados puedan ser asociados a un valor hash, el hash del nodo raíz del árbol. Así, proporciona un método de verificación eficiente y segura de grandes contenidos de datos.

3.3.4. Métodos de Consenso

Como hemos visto anteriormente, la cadena de bloques es un sistema distribuido y descentralizado, lo que hace necesario que disponga de un mecanismo

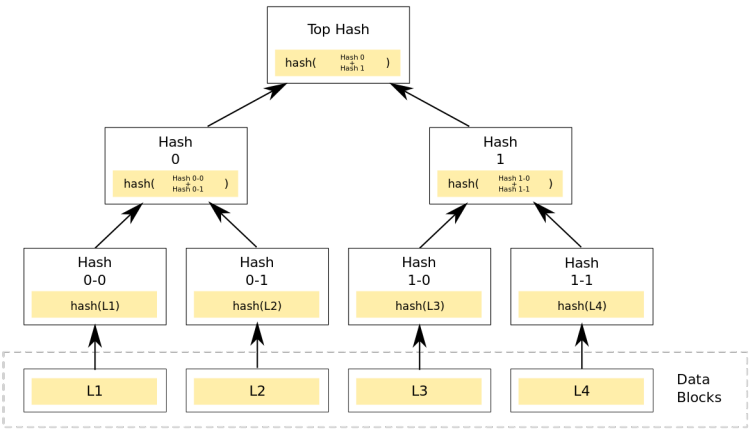

Figura 3.3: Estructura de un árbol Merkle.

que lleve el seguimiento del estado actual del sistema. Debido que en la cadena de bloques puede haber desde transacciones financieras hasta contratos entre empresas, es importante que todas las partes involucradas estén sincronizadas y de acuerdo.

La cadena de bloques está diseñada para ser un libro de cuentas compartido y sincronizado, lo que significa que es necesario considerar en algún momento qué debe y qué no deber se incluido en el registro oficial. Dado que la cadena de bloques es descentralizada, no hay una autoridad oficial que certifique qué contenidos deben ser incluidos en un bloque de la cadena de bloques.

El método que (Nakamoto, 2008) inventó para alcanzar el consenso está basado en el principio de escasez. De un modo o de otro, los algoritmos de consenso propuestos para Blockchain se basan en un sistema de votación en el que el número de votos que un usuario tiene está relacionado con la cantidad de recursos que el usuario controla. Basado en la ley de la oferta y la demanda, poseer una gran cantidad de un activo compartido puede subir el precio de dicho activo de manera que alcanzar el control de dicho activo pueda tener un precio prácticamente inalcanzable.

(Nakamoto, 2008) inventó el algoritmo de consenso llamado prueba de trabajo (en inglés, *Proof of work*) para el uso de Bitcoin. Desde entonces son numerosos los algoritmos que sea han propuesto, siendo su elección óptima dependiendo del caso de uso. Además del algoritmo anterior, entre los algoritmos más destacados encontramos: *proof of stake*, *delegated proof of stake*, *practical byzantine fault tolerance*, y *direct acyclic graphs*.

Los algoritmos más utilizado en la actualidad son *proof of work* y *proof of stake* que se desarrollarán a continuación.

3.3.5. Proof of Work

En este algoritmo, los usuarios de la red de la cadena de bloques que quieran crear el siguiente bloque, hecho que tiene asociada una recompensa, se denominan mineros. Para ganar el derecho a poder minar un bloque, los mineros compiten entre ellos para encontrar la solución a un problema criptográfico. Cuando los mineros encuentran una solución aceptable, éstos crean un bloque y lo transmiten por toda la red.

El algoritmo de prueba de trabajo aprovecha la escasez de recursos computacionales mediante la elección de un problema que sólo puede ser resuelto por adivinación. No hay límite de suposiciones que un minero puede hacer. Este algoritmo incentiva a que los mineros usen cuantas más máquinas de minado mejor para ser los primeros que encuentran la solución al problema. Dado que los ordenadores usados para el minado suponen un coste tanto en su compra como en su uso, la cantidad de control que los mineros pueden tener sobre la cadena de bloques está limitado por la cantidad de dinero que pueden invertir en las máquinas de minado.

La seguridad en este algoritmo de consenso está basada en la idea de que nadie puede controlar más de la mitad de los recursos computacionales de la red de minado de una cadena de bloques. Si se diera este caso, este minero tendría una alta probabilidad de ser el primero que encontrase la solución al problema de minado en cada bloque de la cadena de bloques. Esto daría al minero un completo control de la cadena de bloques, pudiendo modificar la cadena a su antojo.

3.3.6. Proof of Stake

Los usuarios de las cadenas de bloques que usan este algoritmo pueden prometer no usar los toquen que tienen. Esto les da la oportunidad de ser seleccionados como los usuarios para forjar un nuevo bloque is obtener así una recompensa. Los usuarios que forjan cada bloque son seleccionados de manera pseudo-aleatoria de entre todos los usuarios de la red que tenga inversiones sobre alguno de sus activos, siendo más probable que sean seleccionados aquellos usuarios con una inversión más grande.

En este algoritmo para hacer un ataque se necesita que un usuario tenga un control suficiente de la criptomoneda que se usa en la cadena de bloques de manera que se pueda garantizar que va a ser el usuario elegido para forjar cada bloque. Dado que las criptomonedas tiene una número limitado de activos, comprar el número suficiente que permita este control resulta extremadamente costoso, lo que hace que un ataque a los sistemas que emplean el algoritmo de consenso Proof of Stake no factible económicamente.

3.3.7. Funcionamiento de la Blockchain

Una vez vistos los elementos involucrados en la tecnología Blockchain, pasamos a describir su funcionamiento. Éste se compone de los siguientes pasos:

1. *Transacción.* Dos usuarios deciden intercambiar un activo digital (por ejemplo, una criptomoneda) e inician la transacción.

2. *Bloque.* La transacción se empaqueta junto a otras transacciones pendientes, generando así un *bloque*. El bloque se manda a todos los nodos de la red de la Blockchain.

3. *Verificación.* Los nodos participantes evalúan las transacciones del bloque y mediante cálculos matemáticos determinan si las transacciones son válidas o no. Cuando se alcanza el consenso, la transacciones se consideran verificadas.

4. *Hash.* A cada bloque se le asigna un código hash. Además, cada nuevo bloque contendrá la referencia al código hash del último bloque en ser verificado, lo que hace que se cree una cadena de bloques unidos mediante códigos hash. Esto hace que la cadena no pueda ser falsificada y al ser una operación incremental, que los registros anteriores no puedan ser borrados.

5. *Ejecución de la transacción.* El activo pasa de ser propiedad del usuario vendedor a ser propiedad del usuario comprador.

3.3.8. Propiedades

A partir de los conceptos vistos en los apartados anteriores, a continuación describimos las propiedades más importantes de la tecnología Blockchain:

- *No se puede corromper*. Cada nodo del sistema posee una copia de la cadena de bloques, de modo que para poder agregar una nueva transacción cada nodo tiene que verificar su validez. Una vez que se registra la transacción, éste se actualiza en todos los nodos de la red y permanecerá para siempre en la cadena de bloques.

- *Es descentralizada*. Se apoya en una red descentralizada de nodos que son los que mantienen la red.

- *No necesita una autoridad externa*. No requiere de una autoridad central que garantice la confianza de la red.

- *Los registros se almacenan de manera distribuida*. Estos están almacenados en el libro de cuentas que se distribuye por todos los nodos de la red.

- *Está consensuada por los usuarios*. Se emplean algoritmos de consenso que son los que permiten la autogestión del sistema en la toma de decisiones, principalmente a la hora de añadir un nuevo bloque a la Blockchain.

- *Los acuerdos se alcanzan de manera más rápida*. Al evitar la presencia de intermediarios, es posible efectuar acuerdos de manera más rápida y eficiente que utilizando los sistemas tradicionales.

3.3.9. ¿Cuándo usar la tecnología Blockchain?

La tecnología Blockchain tiene muchas ventajas tal y como se ha comentado en los apartados previos, sin embargo su implantación no resulta idónea en todas las ocasiones. A continuación se detallan los factores extraídos de (Bashir, 2017) que determinarán si es recomendable o no una solución que emplee la tecnología Blockchain.

Se recomienda el uso de la tecnología Blockchain cuando se den una o más de las siguientes condiciones:

- Hay una necesidad de compartir una base de datos común.

- No hay confianza entre las partes participantes.

- A varios actores que escriben en la base de datos.

- Actualmente hay una tercera persona que es la que provee de confianza al sistema y a la que todos los participantes están obligados a confiar.
- Actualmente se están usando herramientas criptográficas para facilitar la confidencialidad, integridad y autenticidad de la información.
- La toma de decisiones entre las partes es transparente.
- Existe la necesidad o el objetivo de tener un histórico inmutable.
- La frecuencia transacciones no exceden las 10.000 transacciones por segundo.

No se recomienda el uso de la tecnología Blockchain cuando se den las siguientes condiciones:

- El proceso implica el uso de datos confidenciales.
- Se almacena una gran cantidad de datos estáticos.
- Los datos almacenados ocupan mucho tamaño.
- Las reglas de las transacciones cambian con mucha frecuencia.
- Se utilizan servicios externos para almacenar los datos.

3.4. Tendencias futuras

Las tendencias futuras en el marco de la tecnología Blockchain están principalmente enfocadas en la implementación de la esta tecnología dentro de casos de usos específicos en distintas áreas, tal y como indica (Zheng, Xie, Dai, Chen, & Wang, 2018).

Esta nueva tecnología que supuso un cambio de paradigma en el campo de la economía con la aparición de la criptomoneda Bitcoin tal y como indica, va a conllevar una revolución de la magnitud que supuso la aparición de Internet, tal y como afirman (Tapscott & Tapscott, 2016). Algunos ejemplos son los siguientes:

3.4.1. Cadena de suministros

Normalmente los productos que podemos comprar en un supermercado vienen de distintos proveedores, esto hacer que la calidad de los mismos varíe. Actualmente algunas empresas están utilizando la tecnología Blockchain para realizar el seguimiento y garantizar la procedencia de los productos, mejorando así la transparencia y ganando en confianza por parte de los compradores.

Igualmente, se está utilizando estos datos para verificar la trazabilidad de los productos, lo que es una garantía tanto para los vendedores y proveedores, certificando que los productos han mantenido las condiciones idóneas a lo largo de toda la cadena de suministros. Además, en el caso en el que haya habido algún problema, es fácil poder localizar en qué punto tuvo lugar.

3.4.2. Servicios de notaría

Debido a que los registros que se crean en la cadena de bloques son inmutables y que es posible consultar el histórico de los mismos, sería posible verificar la autenticidad de cualquier documento que haya sido registrado, sin necesidad de una autoridad central (*notario*) que lo certifique. De este modo, la transparencia y la veracidad de la información podría ser aplicada a ámbitos como sorteos, concursos de adjudicaciones, etc.

3.4.3. Energía

Actualmente son muchos los hogares que produces su propia electricidad mediante el uso de sistemas de energía renovables. En estos casos, si la energía generada produce un excedente esta energía se añade a la red del proveedor central de energía. Sin embargo, con la tecnología Blockchain sería posible que los usuarios pudieran vender estos excedentes a otros usuarios sin necesidad de ningún intermediario.

3.4.4. Internet de las Cosas

La infinidad de sensores conectados a Internet abren un inmenso abanico de posibilidades cuando hablamos de aplicaciones que usen la tecnología Blockchain. Un ejemplo, podría ser la certificación de los kilómetros de un vehículo. Debido a que no es posible borrar datos que se han incluido previamente en la cadena

de bloque, si un vehículo ha enviado a la Blockchain sus kilómetros actuales, en el futuro sería posible detectar si se ha cometido una negligencia reduciendo los kilómetros.

3.4.5. Voto electrónico

La tecnología Blockchain permite asegurar el anonimato de un votante, a la vez que garantizar que una persona no pueda votar más de una vez para un mismo proceso de elección. Además, dado que no hay ninguna autoridad centrar que sea la encargada de gestionar el proceso de votación, no es posible manipular las votaciones.

Esto agilizaría el proceso de votación y de recuento, reduciéndose los costes de manera considerable.

3.4.6. Seguros

Mediante la configuración de contratos inteligentes, se puede asegurar el cumplimiento de los contratos. Imaginemos que una persona contrata un seguro para su casa y que tras unos días ésta sufre un incendio. El asegurado recibirá de manera automática el dinero correspondiente en el momento en el que se cumplan las condiciones del contrato, sin la necesidad de mediación por parte de la compañía aseguradora.

Hay otros autores como (Halaburda, 2018), que indican que la *fiebre* actual por la tecnología Blockchain está dando lugar a casos en los que la aplicación de esta tecnología no supone ninguna ventaja con respecto a los sistemas actuales. De hecho, la autora indica que la base de la tecnología Blockchain existía antes que la misma Blockchain, por lo que aboga por una revolución, pero sin la Blockchain, entendiéndose esto como una revolución en el campo de las bases de datos distribuidas y la criptografía.

3.5. Conclusiones

En este estudio epistemológico se han recogido los conceptos fundamentales de la tecnología Blockchain. Analizando los antecedentes se echó la vista atrás hasta los orígenes de las bases de datos, deteniéndonos posteriormente en las

bases de datos distribuidas. La relativa juventud de esta tecnología ha hecho que hayamos comenzado el estado del arte con el nacimiento de la misma en los orígenes de la criptomoneda Bitcoin. Posteriormente se han introducido nuevos usos, centrándonos fundamentalmente en Ethereum, IOTA e Hyperledger.

En el apartado denominado "*Tecnología Blockchain*" se ha entrado en detalle en los componentes de la tecnología, así como en los tipos de cadenas de bloques, la criptografía usada, los métodos de consenso, las propiedades de la Blockchain y en qué casos es recomendable o no su uso.

Las tendencias futuras están marcadas por la implantación de esta tecnología en todos los ámbitos de nuestra vida, por lo que se prevé que las empresas comiencen a incorporar la tecnología Blockchain en un futuro no muy lejano.

Por último me gustaría destacar que esta nueva tecnología que ya supuso una revolución en al ámbito de la economía con la aparición de la criptomoneda Bitcoin, se considera que va a conllevar una revolución de la magnitud que supuso la aparición de Internet.

Hay autores que son más reticentes a dar tal magnitud a la tecnología Blockchain, haciendo especial hincapié en el hecho de que los elementos que se usan en esta tecnología ya existían mucho antes que la cadena de bloques. Por este motivo, estos autores consideran que la revolución de la tecnología Blockchain debe entenderse como avances en el campo de las bases de datos distribuidas y la criptografía.

El tiempo será quién de la razón a unos autores o a otros, pero lo que nadie puede negar es que las propiedades de esta tecnología está haciendo que empresas multinacionales estén usando en sus campañas de marketing el término "*tecnología Blockchain*" como elemento de transparencia que les diferencie de la competencia.

La fuerte apuesta que se está empezando a llevar a cabo por parte de las empresas multinacionales más importantes por todo lo que hay alrededor de esta tecnología, hace que sea una oportunidad ideal para formarse en este campo ya actualmente son muy pocos los profesionales con conocimientos en tecnologías Blockchain.

Capítulo 4

Proyección Didáctica

En este capítulo se desarrollará la proyección didáctica del trabajo fin de máster. En primer lugar, ésta se contextualizará en un centro de enseñanza secundaria de Jaén. Posteriormente se justificará la necesidad de enseñar la U.D. en cuestión. Por último se describirá la misma de manera detallada.

4.1. Introducción

La U.D. será desarrollada en el I.E.S. Virgen del Carmen de Jaén, al ser uno del los centros de referencia de Andalucía en la enseñanza de ciclos formativos de informática, tanto de grado medio como de grado superior.

A continuación, se procede a detallar las características propias del contexto de este centro, así como la justificación que explicará las razones por las que resulta necesario impartir la U.D. recogida en este trabajo.

4.1.1. Contextualización

El I.E.S. Virgen del Carmen es uno de los centro de enseñanza secundaria más importantes de la ciudad de Jaén. Cuenta con un total de 1288 alumnos y 96 profesores. En él se imparte docencia en horario de mañana y tarde a alumnos de Enseñanza Secundaria Obligatoria (ESO), bachillerato y ciclos de Formación Profesional (FP) de grado medio y de grado superior. En lo que respecta a los estudios de informática, el centro imparte la asignatura de Tecnologías de la Información y la Comunicación (TIC) de 4º de ESO, la asignatura TIC 1 de 1º de Bachillerato, la asignatura TIC 2 de 2º de Bachillerato, el Ciclo Formativo de Grado Medio (C.F.G.M.) de Sistemas Microinformáticos y Redes

(SMR), el Ciclo Formativo de Grado Superior (C.F.G.S.) de Administración de Sistemas Informáticos en Red (ASIR), el C.F.G.S. de Desarrollo de Aplicaciones Multiplataforma (DAM) y el C.F.G.S. de Desarrollo de Aplicaciones Web (DAW).

El instituto se encuentra en la calle Paseo de la Estación, nº 44 de Jaén, estando situado en el epicentro de Jaén, junto a centros de enseñanza primaria y secundaria, uno de los centros comerciales más importantes de la ciudad, parques y un gimnasio.

Su ubicación, tal y como se puede apreciar en la figura 4.1, lo sitúa en el punto medio entre la estación de autobuses y la estación de tren, lo que facilita que el alumnado de otras localidades pueda asistir al instituto. Del mismo modo, al estar situado en una de las arterias principales de la ciudad, hay una buena comunicación por medio de transporte urbano.

Figura 4.1: Mapa de la localización del centro I.E.S. Virgen del Carmen de Jaén (Imagen extraída de Google Maps[1]).

La situación del centro hace que se encuentre en una zona en la que el nivel socioeconómico de los residentes es medio-alto. Un indicador que refuerza esta afirmación es el hecho de que prácticamente todo el alumnado tiene un su casa un ordenador con acceso a Internet. Sin embargo, hay que destacar que tanto el bachillerato como los ciclos formativos no tienen circunscripción, por lo que el alumnado proviene de distintos puntos de la ciudad, e incluso de distintas localidades. Este hecho hace que se den algunos casos puntuales de alumnado que no disponga de determinados recursos. En estos casos, el centro ofrece distintas

opciones para que todos los estudiantes puedan completar sus estudios en igualdad de oportunidades.

También hay que destacar que este centro es un centro plurilingüe en el que se imparte docencia en castellano, francés e ingles y que está inmerso en programas ERASMUS. Por este motivo, es común encontrarse en el centro con alumnos de otros países, y que alumnos del centro se vayan a Francia de intercambio. Este tipo de actividades fomentan el intercambio cultural, enriqueciendo a todas las personas que conforman el centro educativo.

En cuanto a las actividades lúdicas, los alumnos tienen aficiones propias de adolescentes, destacando en gran medida el uso de las redes sociales y salir con sus amigos. Debido al contexto socioeconómico mencionado anteriormente, desde el departamento de orientación nos indican que en el centro no hay problemas con las drogas, a excepción del alcohol, cuyo consumo es práctica habitual entre los alumnos de los cursos superiores. También es necesario resaltar que el número de alumnos conflictivos es muy reducido. Hay que destacar que tanto los intereses del alumnado como los posibles temas problemáticos son de gran interés para nosotros ya que nos servirán para poder trabajarlos como temas transversales mientras se imparten los contenidos de la U.D.

Los perfiles de los estudiantes varían en función de los estudios. Los alumnos de educación secundaria provienen de la circunscripción del centro por lo que el nivel socioeconómico de sus familias es medio-alto. La mayor parte del alumnado cursa estos estudios con miras a realizar estudios de bachillerato, mientras que una pequeña parte opta por continuar sus estudios en un ciclo de grado medio en el que se pueda realizar un trabajo manual y operativo. Tras los estudios de bachillerato, la mayoría de los alumnos cursan estudios universitarios, aunque también hay bastantes estudiantes que deciden cursar un ciclo de grado superior con vistas a trabajar a corto plazo en lo que actualmente demandan las empresas.

En lo que respecta a la enseñanza de la informática, el centro cuenta con 5 aulas dotadas de equipamiento informático repartidas entre la planta baja (ver Figura 4.2) y la primera planta (ver Figura 4.3).

Además de estas aulas, el centro también dispone de un taller en el que se imparte el C.F.G.M. de SMR que está situado en el sótano del centro y tiene la puerta de acceso por el patio.

Uno de los recursos digitales más destacados es la plataforma de enseñanza virtual "*Moodle*" que permite a los profesores subir recursos y tareas accesibles

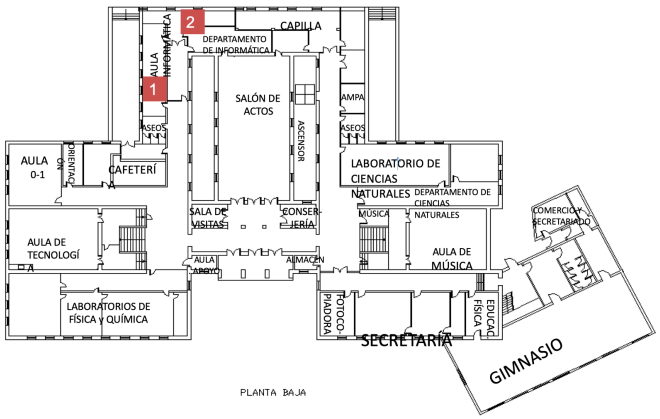

Figura 4.2: Planta baja del centro I.E.S. Virgen del Carmen de Jaén.

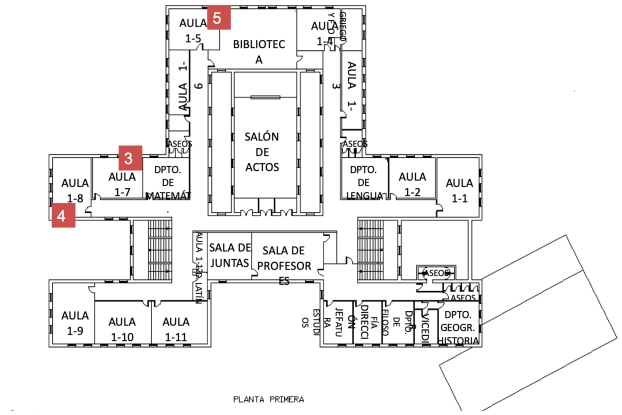

Figura 4.3: Primera planta del centro I.E.S. Virgen del Carmen de Jaén.

a todo el alumnado. Tanto los apuntes de la U.D. como las tareas a entregar se activarán en esta plataforma.

4.1.2. Justificación

La U.D. "Introducción a la Tecnología Blockchain" se va a encuadrar en el módulo de "Bases de Datos" del C.F.G.S. de DAW. En el estudio epistemológico presentado en el capítulo 3, se ha podido comprobar la relevancia de esta tecnología en la actualidad, así como su posible impacto en un futuro no muy lejano. Esto hace que la formación en este ámbito sea un punto diferenciador respecto al resto de alumnos que cursan estudios de grado superior. Por este motivo, consideramos necesario que nuestros alumnos adquieran unos conocimientos básicos sobre esta tecnología, que les sirvan de punto de partida en el caso de que tengan que ampliarlos en el futuro.

4.2. Unidad Didáctica: "Introducción a la Tecnología Blockchain"

4.2.1. Normativa

La normativa que regula tanto el título de DAW como el módulo de Bases de Datos es:

- Real Decreto 686/2010, de 20 de mayo, por el que se establece el título de Técnico Superior en Desarrollo de Aplicaciones Web y se fijan sus enseñanzas mínimas.
- Orden EDU/2887/2010, de 2 de noviembre, por la que se establece el currículo del ciclo formativo de Grado Superior correspondiente al título de Técnico Superior en Desarrollo de Aplicaciones Web.
- Orden de 16 de junio de 2011, por la que se desarrolla el currículo correspondiente al título de Técnico Superior en Desarrollo de Aplicaciones Web.

4.2.2. Elementos curriculares

<table>
<tr><td>Unidad Didáctica</td><td colspan="11">Introducción a la Tecnología Blockchain (Bases de Datos)</td></tr>
<tr><td>Etapa</td><td>CFGS</td><td>Módulo</td><td>(0484) Bases de Datos</td><td>Curso</td><td>1º</td><td>Trimestre</td><td>2º</td><td>Nº de horas totales</td><td>16 horas</td><td>Nº sesiones</td><td>8 (2 horas por sesión)</td></tr>
<tr><td>Real Decreto</td><td colspan="3">Real Decreto 686/2010, de 20 de mayo, por el que se establece el título de Técnico Superior en Desarrollo de Aplicaciones Web y se fijan sus enseñanzas mínimas.</td><td>Orden</td><td colspan="7">• Orden EDU/2887/2010, de 2 de noviembre, por la que se establece el currículo del ciclo formativo de Grado Superior correspondiente al título de Técnico Superior en Desarrollo de Aplicaciones Web.
• ORDEN de 16 de junio de 2011, por la que se desarrolla el currículo correspondiente al título de Técnico Superior en Desarrollo de Aplicaciones Web.</td></tr>
<tr><td colspan="12">Elementos Curriculares</td></tr>
<tr><td>Competencia general (RD 686/2010 de 20 de mayo)</td><td colspan="6">Artículo 4. Competencia general.
La competencia general de este título consiste en desarrollar, implantar, y mantener aplicaciones web, con independencia del modelo empleado y utilizando tecnologías específicas, garantizando el acceso a los datos de forma segura y cumpliendo los criterios de accesibilidad, usabilidad y calidad exigidas en los estándares establecidos.</td><td colspan="4">Competencias profesionales, personales y sociales</td><td>a,b, d,e, p</td></tr>
<tr><td>Líneas de actuación</td><td colspan="11">• La interpretación de diseños lógicos de bases de datos.
• La realización de operaciones de consulta y modificación sobre los datos almacenados.
• La programación de procedimientos almacenados.</td></tr>
<tr><td>Objetivos generales</td><td colspan="11">Objetivos didácticos</td></tr>
</table>

<table>
<tr><td>e, f, p, r</td><td colspan="3">• Conocer los componentes de la tecnología Blockchain.
• Identificar los tipos de cadenas de bloques.
• Reconocer en qué situaciones es adecuado el uso de la tecnología Blockchain y en cuales no.
• Conocer los distintos algoritmos de consenso Blockchain.
• Distinguir características y ventajas entre una base de datos relacional y una cadena de bloques.
• Comprender qué es y para qué sirve un contrato inteligente.
• Conocer el funcionamiento y las partes de un contrato inteligente.</td></tr>
<tr><th>Contenidos conceptuales</th><th>Criterios de Evaluación</th><th>Resultados de aprendizaje</th><th>Instrumento</th></tr>
<tr><td rowspan="4">Almacenamiento de la información:
• Bases de datos. Conceptos, usos y tipos según el modelo de datos, la ubicación de la información.
• Bases de datos centralizadas y bases de datos distribuidas.</td><td>a) Se han analizado los sistemas lógicos de almacenamiento y sus características</td><td rowspan="3">1.- Reconoce los elementos de las bases de datos analizando sus funciones y valorando la utilidad de los sistemas gestores.</td><td rowspan="4">Prácticas, trabajo en grupo y Kahoot</td></tr>
<tr><td>b) Se han identificado distintos tipos de bases de datos según el modelo de datos utilizado.</td></tr>
<tr><td>c) Se han identificado los distintos tipos de bases de datos en función de la ubicación de la información.</td></tr>
<tr><td>g) Se ha reconocido la utilidad de las bases de datos distribuidas.</td></tr>
<tr><td>Programación de bases de datos:
• Introducción. Lenguaje de programación.
• Funciones.</td><td>a) Se han identificado las diversas formas de automatizar tareas</td><td>5.- Desarrolla procedimientos almacenados, evaluando y utilizando las sentencias del lenguaje incorporado en el sistema gestor de bases de datos.</td></tr>
<tr><td>Temas transversales</td><td colspan="2">La falsificación</td><td></td></tr>
</table>

4.2.2.1. Competencias profesionales, personales y sociales

- (a) Configurar y explotar sistemas informáticos, adaptando la configuración lógica del sistema según las necesidades de uso y los criterios establecidos.

- (b) Aplicar técnicas y procedimientos relacionados con la seguridad en sistemas, servicios y aplicaciones, cumpliendo el plan de seguridad.

- (d) Gestionar bases de datos, interpretando su diseño lógico y verificando integridad, consistencia, seguridad y accesibilidad de los datos.

- (e) Desarrollar aplicaciones web con acceso a base de datos utilizando lenguajes, objetos de acceso y herramientas de mapeo adecuados a las especificaciones.

- (p) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida y utilizando las tecnologías de la información y la comunicación.

4.2.2.2. Líneas de actuación

- La interpretación de diseños lógicos de bases de datos.
- La realización de operaciones de consulta y modificación sobre los datos almacenados.
- La programación de procedimientos almacenados.

4.2.2.3. Objetivos generales

- (e) Interpretar el diseño lógico, verificando los parámetros establecidos para gestionar bases de datos.
- (f) Seleccionar lenguajes, objetos y herramientas, interpretando las especificaciones para desarrollar aplicaciones web con acceso a bases de datos.
- (p) Establecer procedimientos, verificando su funcionalidad, para desplegar y distribuir aplicaciones.
- (r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionadas con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales.

4.2.2.4. Objetivos didácticos

- Conocer los componentes de la tecnología Blockchain.
- Identificar los tipos de cadenas de bloques.
- Reconocer en qué situaciones es adecuado el uso de la tecnología Blockchain y en cuales no.
- Conocer los distintos algoritmos de consenso Blockchain.
- Distinguir características y ventajas entre una base de datos relacional y una cadena de bloques.
- Comprender qué es y para qué sirve un contrato inteligente.
- Conocer el funcionamiento y las partes de un contrato inteligente.

4.2.3. Recursos Metodológicos

A continuación se recogen los recursos metodológicos que se han tenido en cuenta para el desarrollo de esta U.D. Concretamente se explicará la organización del aula, los tipos de agrupamientos, los materiales y recursos didácticos utilizados, la metodología empleada, la evaluación de los resultados de aprendizaje y cómo se llevará a cabo la atención a la diversidad del alumnado.

4.2.3.1. Organización del aula

Asumiendo que el aula estará adaptada para 30 alumnos, tal y como especifica la normativa, el espacio será de un mínimo de 60m^2. Las mesas con los ordenadores estarán organizadas en filas orientadas hacia la pizarra y la pantalla de proyección. Entre cada fila habrá espacio suficiente para que los alumnos puedan trabajar en parejas y para que el profesor pueda pasar por detrás de los alumnos para resolver dudas, tal y como se muestra en la figura 4.4.

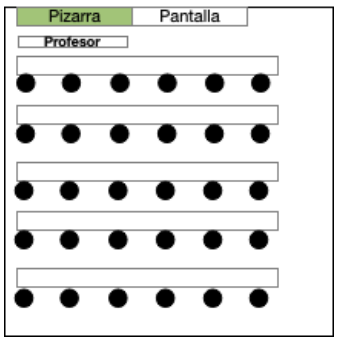

Figura 4.4: Esquema de la organización del aula.

4.2.3.2. Agrupamientos

Los agrupamientos que tendrán lugar en el desarrollo de esta U.D. serán:

- Individual.
- Por parejas.
- En grupos. Los grupos se formarán de manera heterogénea. Se diferenciarán dos grupos:
  - Grupo del trabajo grupal.

- Grupo Kahoot[2]

4.2.3.3. Materiales y recursos didácticos

Los materiales y recursos didácticos utilizados en esta U.D. serán:

- Ordenadores para cada alumno.
- Acceso a internet.
- Hyperledger Fabric.
- Un proyector.
- Una pantalla de proyección.
- Software de presentaciones.
- Una pizarra.
- Kahoot y Baamboozle.

4.2.3.4. Metodología

En la elaboración de esta U.D. se han considerado la diversidad de inteligencias que se dan dentro de un aula, basándonos en la teoría de las inteligencias múltiples propuesta por (Gardner, 1992). Teniendo como principal finalidad el desarrollo del máximo número de inteligencias a la vez que se imparten los contenidos del currículo. Para ello se han definido las actividades considerando además de los 8 tipos de inteligencia, la taxonomía de (Bloom, 1956).

Se utilizan metodologías activas en las que el alumno participa de forma activa, siendo el principal protagonista del proceso de aprendizaje. Para ello, los alumnos se organizarán en grupos para desarrollar un trabajo, que tendrá relación con el tema transversal. El trabajo en grupo se irá completando de manera incremental conforme se vayan viendo nuevos conceptos en teoría. De este modo se fomentan metodologías activas como son:

[2]En el grupo de Kahoot no podrá haber alumnos que estén en el mismo grupo del proyecto final.

- *Trabajo por proyectos.* Los alumnos trabajarán en un proyecto relacionado con el tema transversal que puede implicar la necesidad de trabajar de manera transversal con alumnos de otros cursos.

- *Trabajo cooperativo.* El trabajo grupal será el resultado de un trabajo cooperativo entre los alumnos de cada grupo, de manera que cada dos semanas se irán intercambiando roles para la realización del trabajo. Esto fomentará el aprendizaje de conceptos por ellos mismos, la tutoría entre iguales y les desarrollará en la adquisición de habilidades comunicativas y sociales.

- *Andamiaje.* Los alumnos iniciarán la U.D. con preguntas de tipo generatriz que les hagan replantearse ideas preconcebidas sobre la unidad en cuestión. Posteriormente, conforme van avanzando las sesiones los nuevos conocimientos servirán para que los alumnos los utilicen de base para poder responder preguntas de mayor dificultad. Este modo de actuar trata de motivar al alumnado para que aprenda por descubrimiento.

Este eclecticismo metodológico fomenta tanto los estilos de aprendizaje receptivo como por descubrimiento. Así, se alternarán tanto estrategias expositivas como estrategias de indagación.

La organización de las sesiones sigue el modelo de la asimilación presentado por (Ausubel, Novak, & Hanesian, 1983), en el que se dice lo que se va a enseñar, se enseña y se repite.

Proceso de Enseñanza-Aprendizaje				
Actividad	**Tiempo**	**Sesión**	**Agrupamiento**	**Recursos**
1.1.- Evaluación: - Evaluación de conocimientos previos	20'	1	Individual	Ordenador, Proyector
1.2.- Desarrollo de contenidos: - Introducción componentes Blockchain y tipos de Blockchain	70'	1	Individual	Ordenador, proyector, pizarra
1.3.- Refuerzo: - Actividad lúdica de consolidación y repaso	30'	1	Grupo	
2.1.- Refuerzo: - Repaso clase anterior	20'	2	Grupo	Baamboozle Ordenadores Internet
2.2.- Desarrollo de contenidos: - Nociones de criptografía	70'	2	Individual	Ordenador, proyector, pizarra
2.3.- Refuerzo - Actividad lúdica de consolidación y repaso	30'	2	Grupo	
3.1.- Refuerzo: - Repaso clase anterior	20'	3	Grupo	Baamboozle Ordenadores Internet
3.2.- Desarrollo de contenidos: - Secuencia de una transacción	70'	3	Individual	Ordenador, proyector, pizarra
3.3.- Refuerzo - Actividad lúdica de consolidación y repaso	30'	3	Grupo	

4.1.- Refuerzo: - Repaso clase anterior	20'	5	Grupo	Baamboozle Ordenadores Internet
4.2.- Desarrollo de contenidos: - Métodos de consenso	70'	5	Individual	Ordenador, proyector, pizarra
4.3.- Actividad lúdica de consolidación y repaso	30'	5	Grupo	
5.- Práctica - Caso de uso	120'	6	Parejas	Ordenador, Internet
6.1.- Refuerzo: - Repaso clase anterior	20'	7	Grupo	Baamboozle Ordenadores Internet
6.2.- Desarrollo de contenidos: - Contratos inteligentes	70'	7	Individual	Ordenador, proyector, pizarra, Kahoot
6.3.- Refuerzo - Kahoot resumen de todos los contenidos de la U.D	30'	7	Grupo	
7.- Práctica: - Contratos inteligentes	120'	8	Grupo	Ordenadores Internet
8.- Evaluación: - Presentación de trabajos grupales	120'	8	Grupo	Ordenador, proyector, pizarra

Sesiones

A continuación se describen las distintas sesiones que se darán para impartir la U.D.:

Sesión 1

- Esta sesión comenzará con una actividad de evaluación inicial en la que se comprobarán los conocimientos previos sobre esta materia. Para ello cada alumno contestará un tipo test con preguntas generales relativas a la tecnología Blockchain. A partir de aquí se leerán algunas de las respuestas y se harán preguntas abiertas para motivar al alumnado a encontrar la respuesta.

- Posteriormente se introducirán los componentes que hay dentro de la tecnología Blockchain como son el *libro contable*, la *red de nodos*, la *transacción*, el *monedero*, etc.

- La sesión concluirá con un repaso de los contenidos vistos de manera lúdica. Para ello, se seleccionará a varios alumnos que tendrán que representarán

el rol de cada componente visto, describiendo cual es su papel y de qué manera se relaciona con el resto de componentes.

Sesión 2

- La sesión comenzará con el repaso de los contenidos vistos en la clase anterior. Para ello se realizará una competición por equipos usando la herramienta Baamboozle.
- Los contenidos de esta sesión estarán centrados en nociones criptográficas usadas en la tecnología Blockchain como son la criptografía de clave pública, el zero-knowledge proof y las funciones hash.
- La sesión concluirá con un ejercicio en el que se simularán los distintos tipos de criptografía con mensajes enviados entre los alumnos.

Sesión 3

- La sesión comenzará con el repaso de los contenidos vistos en la clase anterior. Para ello se realizará una competición por equipos usando la herramienta Baamboozle.
- Esta sesión se centrará en describir la secuencia de una transacción en la Blockchain.
- La actividad de refuerzo será una representación por parte de varios alumnos adquiriendo los roles de los distintos actores involucrados.

Sesión 4

- La sesión comenzará con el repaso de los contenidos vistos en la clase anterior. Para ello se realizará una competición por equipos usando la herramienta Baamboozle.
- El contenido de esta sesión serán los algoritmos de consenso utilizados en Blockchain, haciendo especial hincapié en el *Proof of Work* y el *Proof of Stake*.
- Para el repaso, la clase se dividirá en grupos y cada grupo tendrá actuar siguiendo el algoritmo de consenso determinado para llegar a una solución. Tras 10 minutos, los grupos cambiarán de algoritmo de consenso, de manera que todos los grupos hayan podido representar el funcionamiento de los dos algoritmos.

Sesión 5

- En esta sesión los alumnos trabajarán por parejas desarrollando un caso de uso en el que se deben de especificar los elementos de la tecnología Blockchain vistos en las sesiones previas. El caso de uso será la certificación de la pesca del atún, desde que se pesca hasta que se sirve en un restaurante.

Sesión 6

- La sesión comenzará con el repaso de los contenidos vistos en la última clase de teoría. Para ello se realizará una competición por equipos usando la herramienta Baamboozle.
- En esta sesión se verá el concepto de contrato inteligente y se mostrarán ejemplos de contratos inteligentes en el entorno Hyperledger.
- La sesión concluirá con un repaso general de todos los conceptos visto en las sesiones anteriores. Para ellos los alumnos competirán en grupos participando en un Kahoot.

Sesión 7

- En esta sesión práctica se le dará a los alumnos las instrucciones necesarias para poder ejecutar un contrato inteligente en Hyperledger Fabric, para ello se proporcionará el fichero con el contrato y los pasos a seguir para ejecutar Hyperledger Fabric. Una vez ejecutado el contrato de prueba, los alumnos deberán cambiar las condiciones del contrato y completar el guión de prácticas analizando el funcionamiento del contrato y sus resultados.

Sesión 8

- En esta sesión tendrán lugar las presentaciones de los trabajos grupales. Cada grupo dispondrá de 15 minutos para realizar la presentación de su implementación de la tecnología Blockchain a un problema relacionado con el tema transversal. El resto de grupos evaluará a sus compañeros por medio de una rúbrica.

4.2.4. Evaluación

Según lo reflejado en la Orden 16 de junio de 2011, los criterios de evaluación asociados a la U.D. “Introducción a la Tecnología Blockchain” son los siguientes:

- 1.(a) Se han analizado los sistemas lógicos de almacenamiento y sus características.
- 1.(b) Se ha identificado distintos tipos de bases de datos según el modelo de datos utilizado.
- 1.(c) Se han identificado los distintos tipos de bases de datos en función de la ubicación de la información.
- 1.(g) Se ha reconocido la utilidad de las bases de datos distribuidas.
- 5.(a) Se han identificado las diversas formas de automatizar tareas.

4.2.4.1. Procedimientos e instrumentos

Trabajo grupal

El trabajo grupal consistirá en la presentación por parte de los alumnos de cada grupo de un ejemplo de aplicación de la tecnología Blockchain para la resolución de un problema concreto de la vida diaria. La evaluación se realizará mediante rúbrica tanto por parte del resto de grupos (35 % de la nota[3]) como por parte del profesor (65 % de la nota). La puntuación resultante de sumar todos los parámetros de la rúbrica se normalizará, de manera que cada práctica tenga una calificación de 0-10 puntos.

Las exposiciones orales de los trabajos grupales se evaluarán atendiendo a los siguientes aspectos:

- Comunicación.
- Contenido.
- Desarrollo de la presentación.

La nota final será:

Nota final= 35 % Comunicación + 50 % Contenido + 15 % Desarrollo de la presentación.

Comunicación

La rúbrica para evaluar la comunicación se ha elaborado teniendo en cuenta la importancia que tienen la *voz*, la *comunicación verbal*, y la *comunicación no verbal* a la hora de comunicar.

[3]La nota de los grupos será la media de las calificaciones otorgadas por los distintos grupos.

Figura 4.5: Importancia de la voz, la comunicación verbal y la comunicación no verbal. (Imagen extraída de (Mehrabian, 2017)).

Para ello se han utilizado los pesos que se especifican en la regla de (Mehrabian, 2017), tal y como se puede observar en la figura 4.5.

	Peso		1 punto	2 puntos	3 puntos	4 puntos
Lenguaje corporal	55%	Gesticulación	No gesticula	Algunas veces gesticula, pero la mayoría de los gestos son incoherentes con la presentación	Gesticula la mayoría de las veces, aunque algunos gestos son incoherentes con la presentación	Los gestos son coherentes y acompañan a la presentación
		Postura	Tiene una mala postura	Algunas veces tiene una mala postura	Tiene buena postura	Tiene buena postura y se le ve relajado/a y seguro/a de sí mismo/a
		Contacto visual	No mira a la audiencia durante la presentación	Algunas veces establece contacto visual durante la presentación	Establece contacto visual con la mayor parte de la audiencia durante la presentación	Establece contacto visual con toda la audiencia durante toda la presentación
Lenguaje verbal	7%	Vocabulario	Utiliza un vocabulario limitado y repite palabras	Repite palabras	Utiliza un vocabulario limitado	Utiliza un vocabulario amplio sin repetir palabras
		Conocimiento	No sabe ni entiende lo que está exponiendo.	Ha asimilado parcialmente los conocimientos	Ha asimilado la mayor parte de los conocimientos	En la exposición demuestra conocimiento del tema

			Tampoco lo comunica correctamente	que expone, pero si los comunica (los lee)	que expone, pero no los comunica adecuadamente	tratado y sabe comunicarlo
Lenguaje paraverbal	38%	Volumen	El volumen es débil, siendo difícil escuchar la presentación	En ocasiones el volumen es lo suficientemente alto para ser escuchado por toda la audiencia, al menos, la mitad de la presentación	El volumen es lo suficientemente alto para ser escuchado por toda la audiencia durante la mayor parte de la presentación	El volumen es lo suficientemente alto para ser escuchado por toda la audiencia durante toda la presentación.
		Entonación	No hay variación en la entonación durante la presentación	Algunas veces hay variación en la entonación, pero la mayor parte se tiene una entonación monótona	Hay variación en la entonación durante la mayor parte de la presentación	Entonación variada y adecuada durante toda la presentación
		Pronunciación	No es capaz de pronunciar con claridad y fluidez todas las palabras	Pronuncia sin claridad o sin fluidez con continuos bloqueos	Pronuncia con claridad y muestra fluidez, pero con algunos bloqueos	Pronuncia con claridad y fluidez todas las ideas que expone
		Velocidad	La velocidad impide la compresión	La velocidad dificulta la comprensión	La velocidad permite la comprensión	La velocidad facilita la comprensión

Contenido

	0 puntos	2 punto	4 puntos
Descripción del problema	No se incluye descripción del problema	Descripción del problema incompleta	Completa descripción del problema
Motivación uso tecnología Blockchain	No presenta la motivación	Motivación poco fundamentada	Motivación fundamentada
Componentes Blockchain	No usa componentes Blockchain	Utiliza componentes Blockchain	Explica los componentes Blockchain utilizados
Tipo de Blockchain	Escoge el tipo de Blockchain incorrecto	Escoge el tipo de Blockchain adecuado, pero no lo explica	Escoge el tipo de Blockchain adecuado y lo explica
Algoritmo de consenso	No especifica el tipo de algoritmo de consenso utilizado	Explica parcialmente el algoritmo de consenso utilizado	Explicación completa del algoritmo de consenso utilizado
Secuencia de transacción	Explicación incorrecta	Explicación correcta, pero incompleta	Explicación correcta y completa
Justificación de uso	Justificación incorrecta	Justificación correcta, pero incompleta	Justificación correcta y completa

Desarrollo de la presentación

	1 punto	2 puntos	3 puntos	4 puntos
Organización de la exposición	La exposición carece de estructura y es incoherente	La exposición está estructurada, pero es incoherente (no tiene hilo conductor)	Mantiene la coherencia, aunque falla alguna parte de la estructura	Organiza la exposición siguiendo la estructura de la misma con coherencia y cohesión
Material apoyo	No utiliza material de apoyo	Utiliza material de apoyo, pero no está organizado y cuesta leerlo	Utiliza material de apoyo bien organizado, pero hay demasiado texto y cuesta leerlo (letra pequeña)	Utiliza material de apoyo bien organizado y con poco texto, facilitando la lectura (letra grande)
Conexión con la audiencia	No capta la atención de la audiencia	Sólo capta la atención de la audiencia en algunos períodos de la presentación	Capta la atención de la audiencia durante la mayor parte de la presentación	Es capaz de captar la atención de la audiencia durante toda la presentación

Prácticas

Se realizarán 2 prácticas que servirán para consolidar lo visto en teoría, así como de ayuda para el desarrollo del trabajo grupal. Las prácticas se evaluarán por mediante rúbricas. En cada práctica, la puntuación resultante de sumar todos los parámetros de la rúbrica se normalizará, de manera que cada práctica tenga una calificación de 0-10 puntos.

- Práctica 1 (50 %) Caso de uso.

	0 puntos	2 punto	4 puntos
Diagrama	No se incluye diagrama	Incluye diagrama incompleto	Incluye un diagrama completo
Componentes Blockchain	No usa componentes Blockchain	Utiliza componentes Blockchain	Explica los componentes Blockchain utilizados
Tipo de Blockchain	Escoge el tipo de Blockchain incorrecto	Escoge el tipo de Blockchain adecuado, pero no lo explica	Escoge el tipo de Blockchain adecuado y lo explica
Algoritmo de consenso	No especifica el tipo de algoritmo de consenso utilizado	Explica parcialmente el algoritmo de consenso utilizado	Explicación completa del algoritmo de consenso utilizado
Secuencia de transacción	Explicación incorrecta	Explicación correcta, pero incompleta	Explicación correcta y completa
Justificación de uso	Justificación incorrecta	Justificación correcta, pero incompleta	Justificación correcta y completa

- Práctica 2 (50 %) Contratos Inteligentes.

	0 puntos	2 punto	4 puntos
Configuración	No cambia la configuración del fichero proporcionado	Modifica el fichero con el contrato inteligente, pero con algunos fallos	Modifica correctamente el fichero con el contrato inteligente
Descripción del contrato inteligente	No describe el contrato inteligente	Descripción incompleta	Descripción completa
Ejecución	No puede ejecutar el contrato inteligente	Ejecuta el contrato inteligente, pero tiene errores	Ejecuta el contrato inteligente correctamente
Interpretación de resultados/ funcionamiento	No explica los resultados obtenidos	Explica los resultados obtenidos de manera incompleta	Explicación completa de los resultados obtenidos

Actitud

En esta parte se engloba la participación, comportamiento, asistencia a clase, participación en las actividades de repaso realizadas en clase y la observación directa del profesor durante el día a día. Todos los alumnos partirán en esta parte con una calificación de 10 puntos que podrá reducirse en los siguientes casos:

- Cada falta injustificada: -0,5 puntos.
- Cada actividad de repaso en la que no participe el alumno: -0,3 puntos.
- Cada ver que el alumno interrumpa el desarrollo de la clase de manera intencionada (hablar, hacer ruido, molestar al compañero...): -0,2 puntos.
- El alumno hace mal uso del material del centro: -1 punto.
- Si el alumno falta el respeto a un compañero o al profesor: -2 puntos

Los ganadores de las actividades de repaso en Kahoot tendrán una calificación de +0,5 puntos.

La calificación máxima de esta parte será de 10 puntos.

Kahoot

La actividad de refuerzo en la que se usa el Kahoot, se realizará por equipos. Los miembros de los tres primeros equipos tendrán una puntuación adicional

que se sumará a la puntuación del trabajo grupal. En caso de tener la máxima calificación, ésta se sumará a las prácticas. Si también se tiene la máxima calificación en las prácticas, la puntuación se sumará a la actitud.

- *Primer puesto.* + 0,75 puntos.
- *Segundo puesto.* + 0,5 puntos.
- *Tercer puesto.* + 0,25 puntos.

Criterios de calificación

- **Práctica:** 40 %
- **Trabajo grupal:** 50 %
- **Actitud:** 10 %

Consideraciones

1. Para aprobar la U.D. será necesario obtener como mínimo 2 puntos en cada una de las partes y que la suma de todas las partes sea igual o superior a 5 puntos.
2. Las prácticas y el trabajo grupal se deberán entregar vía Moodle antes de la fecha límite para ser evaluadas. En caso contrario, la calificación de esa parte será de 0 puntos.

La nota final será:
NOTA FINAL = (20 % Práctica 1 + 20 % Práctica 2)+ 50 % Trabajo grupal + 10 % Actitud

4.2.4.2. Sistema de recuperación

Los alumnos cuya nota final sea inferior a 5 puntos deberán recuperar las partes suspensas, es decir:

- Obtener una calificación mínima de 5 puntos sobre 10 en cada una de las prácticas de la U.D., al final del trimestre.
- Obtener una calificación mínima de 5 puntos sobre 10 en el trabajo grupal.

- Las prácticas se deberán entregar vía Moodle con fecha límite una semana antes del día fijado para el examen de recuperación de la asignatura.
- Para recuperar el trabajo grupal, será necesario que los miembros suspensos del grupo realicen una presentación del trabajo grupal en clase tras haber realizado las modificaciones indicadas por el profesor.
- La actitud no podrá cambiarse en todo el curso.

4.2.5. Atención a la diversidad

En esta U.D. se tendrán en cuenta las distintas necesidades de los alumnos, de manera que su aprendizaje pueda llevarse a cabo en igualdad de oportunidades. No obstante, en ningún caso se realizará ninguna adaptación curricular que suponga la eliminación de contenidos.

Los colectivos considerados son los siguientes:

- *Personas con dificultades de aprendizaje.* Estos alumnos tendrán un material de refuerzo que se centrará en los conocimientos clave. Igualmente serán ayudados por alumnos con altas capacidades o con un nivel de conocimiento sobre la materia adecuado.
- *Alumnos con incorporación tardía y con dificultades de integración.* Los alumnos trabajarán la mayor parte del tiempo en parejas y en grupos, lo que fomentará la integración y participación de todo el alumnado. Para aquellos alumnos de incorporación tardía, se habilitarán recursos en la plataforma Moodle con el objetivo de poder ponerse al día lo antes posible.
- *Alumnos con altas capacidades.* Estos alumnos colaborarán ayudando a aquellos compañeros que tengan dificultades de aprendizaje, de manera que la tutoría entre iguales sea beneficiosas para ambos.
- *Diversidad funcional de tipo físico, psíquico, sensorial o graves trastornos de personalidad o conducta.* Para este colectivo se adaptarán los materiales de manera que puedan ser trabajados sin ningún problema. En el caso de necesitar a alguna persona de apoyo, se le facilitará el acceso a la clase para que pueda ayudar al alumno en todo momento.

Acrónimos

ASIR	Administración de Sistemas Informáticos en Red.
C.F.G.M.	Ciclo Formativo de Grado Medio.
C.F.G.S.	Ciclo Formativo de Grado Superior.
DAM	Desarrollo de Aplicaciones Multiplataforma.
DAW	Desarrollo de Aplicaciones Web.
ESO	Enseñanza Secundaria Obligatoria.
FP	Formación Profesional.
SMR	Sistemas Microinformáticos y Redes.
TIC	Tecnologías de la Información y la Comunicación.
U.D.	Unidad Didáctica.

Bibliografía

Ali, M. (2017). The next wave of computing. *Medium.com (Ultimo acceso junio 2019)*.

Atzei, N., Bartoletti, M., & Cimoli, T. (2016). A survey of attacks on Ethereum smart contracts. *IACR Cryptology ePrint Archive*, 164-186.

Ausubel, D. P., Novak, J. D., & Hanesian, H. (1983). *Psicologia educativa: un punto de vista cognoscitivo*. Trillas México.

Bashir, I. (2017). *Mastering blockchain*. Packt Publishing Ltd.

Bloom, B. S. (1956). Taxonomy of educational objectives. Vol. 1: Cognitive domain. *New York: McKay*, 20-24.

Burger, C., Kuhlmann, A., Richard, P., & Weinmann, J. (2016). Blockchain in the energy transition. A survey among decision-makers in the German energy industry. *DENA German Energy Agency*.

Buterin, V. (2013). Ethereum white paper. *GitHub repository*, 22-23.

Cachin, C. (2016). Architecture of the hyperledger blockchain fabric. En *Workshop on distributed cryptocurrencies and consensus ledgers* (Vol. 310).

Codd, E. F. (1970). A relational model of data for large shared data banks. *Communications of the ACM*, *13*(6), 377-387.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.

Gardner, H. (1992). *Multiple intelligences*. Minnesota Center for Arts Education.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. En *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 3-16). ACM.

Halaburda, H. (2018). Blockchain revolution without the blockchain. *Bank of Canada Staff Analytical Note*, *5*.

Hoy, M. B. (2017). An introduction to the blockchain and its implications for libraries and medicine. *Medical reference services quarterly*, *36*(3), 273-279.

Kohler, W. H. (1981). A survey of techniques for synchronization and recovery in decentralized computer systems. *ACM Computing Surveys (CSUR)*, *13*(2), 149-183.

Lavrijssen, S. & Carrilo, A. (2017). Radical innovation in the energy sector and the impact on regulation. *TILEC Discussion Paper No. DP 2017-017*.

López, J. & Mora, J. J. (2016). *La economia de blockchain: Los modelos de negocio de la nueva web*. Kolokium.

Luu, L., Chu, D., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. En *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 254-269). ACM.

Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016). A secure sharding protocol for open blockchains. En *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 17-30). ACM.

Mehrabian, A. (2017). *Nonverbal communication*. Routledge.

Music, R. (2015). Fair music: Transparency and payment flows in the music industry. *Rethink Music*.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

Olnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, *34*, 355-364.

Ozsu, M. T. & Valduriez, P. (2011). *Principles of distributed database systems*. Springer Science & Business Media.

Popov, S. (2016). The tangle. White paper. *available at: Iota. org*.

Szydlo, M. (2004). Merkle tree traversal in log space and time. En *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 541-554). Springer.

Tapscott, D. & Tapscott, A. (2016). *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin.

Tsamardinos, I., Brown, L. E., & Aliferis, C. F. (2006). The max-min hill-climbing Bayesian network structure learning algorithm. *Machine learning*, *65*(1), 31-78.

Warburg, B. (2016). How the blockchain will radically transform the economy. *TED Summit*.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*, 1-32.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, *14*(4), 352-375.