Aproximación basada en Blockchain para crear un modelo de confianza en la enseñanza superior abierta y ubicua

David Lizcano Casas

Vicerrector de Investigación y Doctorado de la Universidad a Distancia de Madrid, UDIMA
david.lizcano@udima.es

Juan Alfonso Lara Torralbo

Profesor de la Universidad a Distancia de Madrid, UDIMA
juanalfonso.lara@udima.es

Este trabajo ha obtenido un Accésit del Premio Estudios Financieros 2018 en la modalidad de Educación y Nuevas Tecnologías.

El jurado ha estado compuesto por: don Alfonso Aguiló Pastrana, doña Milagros Antón López, don Fernando Checa García, don Ángel de Miguel Casas, doña Laura Rayón Rumayor y don Javier Manuel Valle López.

Los trabajos se presentan con seudónimo y la selección se efectúa garantizando el anonimato de los autores.

Extracto

Bitcoin ha supuesto una revolución en las transacciones digitales y en la economía mundial. Propone un modelo descentralizado de confianza para realizar transacciones basadas en una criptomoneda. Miles de seguidores defienden su descentralización e independencia, su seguridad y versatilidad. Sus detractores lo tachan de burbuja especulativa, de medio para fomentar la ciberdelincuencia o de pseudotimo piramidal, además de construirse en torno a una tecnología no escalable e ineficiente. Pero ¿y si fuera posible aprovechar las bondades del Blockchain, la tecnología subyacente a Bitcoin, para revolucionar las enseñanzas superiores y su adecuación al mundo laboral actual? ¿Y si en lugar de transacciones económicas se gestionan transacciones de contenidos, enseñanzas y competencias, evaluadas por consenso por estudiantes, formadores y empleadores para eliminar de una vez por todas el gap entre el mundo académico y el laboral? En este trabajo se presenta un modelo basado en Blockchain para resolver los retos actuales de la educación superior, cada vez más dispersa, abierta y ubicua. El modelo propuesto puede implantarse en cualquier entidad formadora para adecuar sus enseñanzas a las necesidades concretas de perfiles profesionales validados por empleadores del sector. Se ha validado dicho modelo por medio de un prototipo con resultados más que aceptables.

Palabras clave: Blockchain; certificado digital; competencias; minado por consenso; confianza; P2P.

Fecha de entrada: 03-05-2018 / Fecha de aceptación: 10-07-2018

Cómo citar: Lizcano Casas, D. y Lara Torralbo, J. A. (2019). Aproximación basada en Blockchain para crear un modelo de confianza en la enseñanza superior abierta y ubicua. *Tecnología, Ciencia y Educación*, *13*, 5-36.

A trust model in open and ubiquitous higher education based on Blockchain technology

David Lizcano Casas
Juan Alfonso Lara Torralbo

Abstract

Bitcoin has revolutionised digital transactions and the global economy. It advocates a decentralised model of confidence for transactions based on a crypto currency. Thousands of followers defend its decentralisation, independence, security and versatility. Its detractors call it a speculative bubble, a way to encourage cybercrime or pseudo pyramid schemes, as well as being built around a non-scalable and inefficient technology. But what if it were possible to take advantage of the benefits of the technology underlying Bitcoin, Blockchain, to revolutionise higher education and its adaptation to today's working world? What if rather than economic transactions it were used to manage transactions of content, teaching and competencies, assessed by consensus by students, trainers and employers, in order to eliminate once and for all the gap between the academic world and the working world? This paper presents a model based on Blockchain to address the current challenges of an increasingly dispersed, open and ubiquitous higher education. The proposed model can be implemented in any training institution to adapt its teaching to the specific needs of professional profiles validated by employers in the sector. This model has been validated by means of a prototype with more than acceptable results.

Keywords: Blockchain; digital certificate; competencies; mined by consensus; confidence; P2P.

Citation: Lizcano Casas, D. y Lara Torralbo, J. A. (2019). A trust model in open and ubiquitous higher education based on Blockchain technology. *Tecnología, Ciencia y Educación*, *13*, 5-36.

Sumario

1. Introducción, motivación y objetivos

El modelo actual de enseñanza superior resulta cada vez más descentralizado, heterogéneo y difícil de verificar y de validar, lo que redunda en diversos problemas abiertos para cada representante del modelo de negocio que supone la formación de profesionales para su incorporación al mundo laboral, esto es, formadores (reglados o no), estudiantes y empleadores.

Cada vez es más habitual que los estudiantes no solo reciban formación de universidades regladas, sino que también se formen a través de la participación (por medio de estudios dirigidos desde dichas universidades o como resultado de un estudio proactivo independiente) en cursos masivos en internet (*massive open online course* [MOOC]), en talleres presenciales o a distancia, en videotutoriales, en charlas o videoentrevistas, etc. (Bartolomé, Bellver, Castañeda y Adell, 2017). Todas estas fuentes de conocimiento, así como la propia praxis profesional, suponen un abanico inabarcable que origina en el estudiante la adquisición de competencias que debe poner en liza a la hora de su incorporación al mundo laboral y profesional. Sin embargo, es muy difícil cuantificar, valorar y validar dichos conocimientos cuando no provienen de estudios reglados dependientes de alguna Administración centralizada (Cano y Cabrera, 2016). Y aun procediendo de estudios reglados, el diseño de cada plan de estudios es tan variopinto que el estudiante se ve obligado a realizar una recopilación muy amplia de documentos escritos, así como a realizar pruebas de acceso y entrevistas de toda índole a fin de poder garantizar las destrezas y competencias que ha adquirido.

Desde el punto de vista de las universidades, cada vez es mayor la crítica existente desde el ámbito de la empleabilidad, aludiendo a que la enseñanza universitaria es a menudo incapaz de adaptarse de forma rápida y versátil a las necesidades de formación del mercado laboral con un *time-to-market* adecuado. Existe un *impasse* de más de 5 años desde que un plan de estudios de tipo licenciatura o ingeniería es diseñado hasta que sus primeros egresados puedan demostrar la adecuación de su formación desempeñando labores profesionales. Y las agencias y estamentos centrales que verifican los planes de estudio se embarcan constantemente en procelosos procesos de auditoría que no logran detectar a tiempo problemas formativos, ni mejoran la resiliencia universitaria para adaptarse, en tiempo y forma, a la realidad laboral.

> Las universidades, a menudo, no logran formar a los estudiantes en las competencias reales necesarias en el mundo laboral

La explosión de la sociedad de la información no ha permitido mejorar los procesos de contratación de personal ni de recopilación de sus currículums, de forma que es muy difícil analizar qué egresado puede estar realmente mejor preparado para un puesto

Para los empleadores, existen, asimismo, problemas abiertos. La explosión de la sociedad de la información no ha permitido mejorar los procesos de contratación de personal ni de recopilación de sus currículums, de forma que es muy difícil analizar qué egresado puede estar realmente mejor preparado para un puesto. Además, la impostura, la falsificación y el ruido son una constante, de forma que toda empresa que desee contratar a un profesional cualificado requiere recabar infinidad de documentación heterogénea y dispersa de sus candidatos, comprobar si es fidedigna y, por último, pero no menos importante, si las competencias que el estudiante dice tener se traducen en destrezas útiles para resolver problemas reales del perfil profesional buscado.

En un informe de KnowledgeWorks (King, Prince y Swanson, 2016), se sugiere que los contratos inteligentes y las cadenas de bloques van a tener un importante valor sobre la centralización del aprendizaje en torno al estudiante, por lo que el sistema se adaptaría a cada estudiante, en lugar de que cada estudiante tuviera que adaptarse al sistema, como ocurre hoy día. No obstante, estos artículos visionarios no han sido traducidos hasta la fecha en soluciones reales que poder aplicar.

Toda empresa que desee contratar a un profesional cualificado requiere recabar infinidad de documentación heterogénea y dispersa de sus candidatos, comprobar si es fidedigna y si las competencias que el estudiante dice tener se traducen en destrezas útiles para resolver problemas reales del perfil profesional buscado

En este trabajo se presenta una aplicación de la tecnología Blockchain (empleada para el registro consensuado, seguro, descentralizado e infalsificable de transacciones de *bitcoins*) en el ámbito de la educación superior abierta y ubicua, registrándose con ella la adquisición de conocimientos y su validación mediante su puesta en práctica en problemas reales adaptados a la realidad empresarial. Gracias al uso de este prototipo se logran los siguientes objetivos:

- **O1.** Las entidades formadoras pueden adaptar sus enseñanzas a las necesidades del mercado laboral, mejorando su calidad interna y sabiendo si sus estudiantes logran o no éxito profesional, de forma ágil y rápida, tan pronto como concluyan favorablemente una asignatura, un taller o un curso.
- **O2.** Se genera un mecanismo no sesgado y objetivo para evaluar a las entidades formadoras en función de un capital de reputación. Esta reputación depende del buen hacer de los estudiantes, formados para el desempeño profesional a la hora de realizar las labores en las que se les ha instruido, con lo que se puede identificar rápidamente qué entidades y recursos formativos son mejores y peores para la adquisición de determinadas destrezas profesionales.

- **O3.** Los estudiantes pueden disponer de un currículum actualizado completo, digital, legítimo y verificable fácilmente por cualquiera, facilitándose de este modo la labor de documentación y presentación para el acceso a puestos de trabajo. Además, se los dota de un mecanismo para conocer mejor qué entidades son más adecuadas para sus necesidades, incluyendo entre ellas no solo universidades regladas, sino todo tipo de recursos formativos o fuentes de conocimiento disperso a través de internet que firmen sus enseñanzas con certificado digital.
- **O4.** Los empleadores disponen de un mecanismo dinámico, proactivo y eficiente para dirigir la formación de estudiantes, preparándolos para desempeñar perfiles profesionales sin necesidad de verificar de nuevo todas las competencias, los conocimientos y las destrezas de sus candidatos.
- **O5.** Se elimina la gestión documental en papel de títulos, currículums, cursos y certificados, así como la posibilidad de falsificar cualquier documento de este tipo.

Blockchain permite crear un sistema basado en la confianza para que universidades, estudiantes y empresas logren grandes avances en el ámbito de la formación y de la contratación de calidad

El resto del trabajo se organiza del siguiente modo: los trabajos relacionados y la tecnología existente se presentan en el apartado 2; el modelo de confianza propuesto para su uso en educación se describe en el apartado 3; la implementación del prototipo de dicho modelo y su validación se desarrolla en el apartado 4; las líneas futuras de trabajo se recogen en el apartado 5; y, finalmente, las conclusiones del trabajo se incluyen en el apartado 6.

2. Trabajos relacionados y tecnología existente

2.1. Blockchain y Bitcoin

2.1.1. Generalidades

Blockchain se refiere a una tecnología informática que permite mantener registros descentralizados y distribuidos de transacciones digitales (Tapscott y Tapscott, 2016). Su primera implementación tuvo lugar en el 2009, en el contexto de la primera moneda digital *bitcoin* y su(s) autor(es) se escondieron tras el pseudónimo de Satoshi Nakamoto (Nakamoto, 2008). Se trata de una tec-

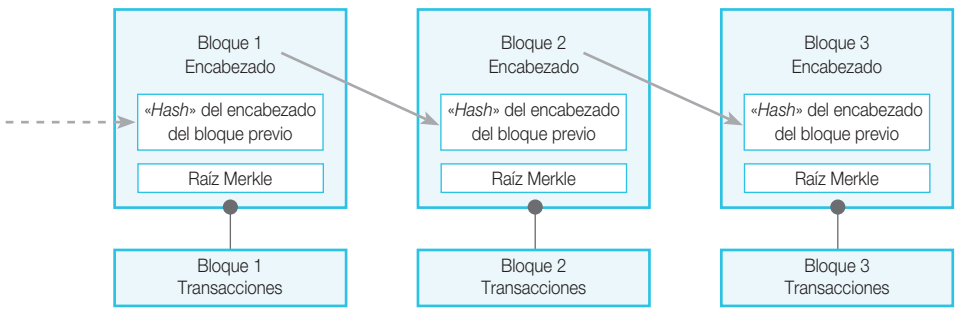
Blockchain se refiere a una tecnología informática que permite mantener registros descentralizados y distribuidos de transacciones digitales

nología compleja, con un enorme potencial (Jones, 2016; Valenzuela, 2016), cuya principal característica y promesa es la existencia de un mundo sin (o casi) intermediarios. El problema es que la interpretación de dicha no intermediación oscila entre dos polos con similar carga de complejidad: un mundo sin intermediarios, dependiendo todos de unos pocos centros de poder (*up to down* [U2D]), o un mundo solidario y horizontal (*peer to peer* [P2P]).

Tal y como se muestra en la figura 1, la estructura de Blockchain es una lista enlazada y ordenada de bloques de transacciones, cada uno identificado mediante una función *hash* (un «resumen» digital numérico de longitud fija). El *hash* de cada transacción es calculado por medio de un proceso de varios pasos que involucran, a su vez, el cálculo de varios *hash* hasta que se genera un único *hash* final, conocido como «raíz de Merkle». Asimismo, cada bloque almacena el *hash* del encabezado del bloque previo, enlazando de esta manera los bloques. Así se previene que un bloque pueda ser alterado sin tener que modificar todos los bloques posteriores.

También las transacciones se enlazan entre sí. Cada transacción gasta los *satoshis* (unidad de medida para fraccionar un *bitcoin*) recibidos en una o más transacciones previas, de manera que la entrada de cada transacción es la salida de una previa. Cada transacción puede crear múltiples salidas. Este sería el caso cuando se efectúan envíos a múltiples direcciones, pero la salida de una transacción concreta solo puede ser usada como entrada una vez. Cualquier intento de usarla de nuevo sería tratar de gastar dos veces los mismos *satoshis*, algo que no está permitido.

Figura 1. **Estructura general de Blockchain**



Fuente: elaboración propia.

2.1.2. Prueba de trabajo

La Blockchain se mantiene de forma colaborativa por todos los integrantes de la red, por lo que Bitcoin requiere que se pruebe que, en la creación de cada bloque, se invirtió una cantidad relevante y significativa de trabajo. Esto se realiza para asegurar que aquellos usuarios malintencionados que traten de modificar bloques anteriores se vean obligados a realizar una cantidad excesivamente grande de trabajo, mucho mayor que la de los usuarios honrados que solo quieren agregar un nuevo bloque. Al depender un bloque de los bloques previos, es imposible modificar un bloque dado sin tener que modificar todos los bloques subsecuentes. Esto da como resultado que el coste de modificar un bloque se incremente con cada nuevo bloque que se agregue.

El algoritmo de prueba de trabajo empleado en Bitcoin aprovecha la naturaleza aparentemente aleatoria de las funciones *hash*. Para probar que se realizó el trabajo al agregar un nuevo bloque, se debe crear un *hash* del encabezado del bloque que no exceda cierto valor. Por ejemplo, si el máximo valor posible del *hash* es 2^{256}, se puede probar que se intentaron dos combinaciones al producir un valor menor a 2^{256}.

Los nuevos bloques se agregarán a Blockchain solo si el valor es menor o igual al nivel de dificultad. Este valor es consensuado por la red y actualizado cada 2.016 bloques. Debido a un error por uno, solo se toman los valores de 2.015 al calcular la dificultad. El valor se establece tratando de lograr que, con todos los nodos compitiendo para encontrar un valor menor para cada nuevo bloque, necesite aproximadamente 10 minutos el encontrarlo. Idealmente, generar 2.016 bloques lleva 1.209.600 segundos (2 semanas). Si se consumieron menos de dos semanas en generar los 2.016 bloques, entonces se incrementaría el valor de la dificultad proporcionalmente, con un máximo de un 300 %. En el caso de que se haya tardado más de dos semanas, se decrementa el valor de la dificultad de forma proporcional, con un máximo de un 75 %. Estas pruebas de trabajo computacional requieren gran cantidad de consumo energético y reciben multitud de críticas desde el punto de vista de la eficiencia energética y de la sostenibilidad medioambiental.

2.1.3. Protocolos derivados de Bitcoin

Aparte de los denominados *altcoins* (implementaciones de Blockchain que, sobre la base de Bitcoin, intentan crear nuevas monedas), existen otras implementaciones alternativas que no son realmente monedas. Estas implementaciones, denominadas *altchains*, constan de un algoritmo de consenso (Buterin, 2015) y de un «cuaderno de bitácora» distribuido como una plataforma para contratos, registro de nombres, etc. Las *altchains* usan los mismos bloques básicos y, a veces, una moneda o ficha (*token*) como medio de pago, pero su principal propósito no es el de desempeñar la función de constituir una moneda de cambio.

En otros términos, los *altchains* son, como su nombre indica, implementaciones alternativas de Blockchain que no tienen como principal objetivo su uso como moneda. Aunque muchas incluyen monedas, sin embargo, las emplean como «fichas» para guardar algo, como un contrato o un recurso.

Namecoin fue una de las primeras implementaciones derivadas de Bitcoin y es un sistema de registro de nombres que emplea como plataforma una Blockchain. Esta puede emplearse como una alternativa a los servidores de nombres de dominio (*domain name service* [DNS]), que emplea el dominio «.bit».

Ethereum es otro ejemplo importante, pues se trata de un sistema de procesamiento de contratos y ejecución basado en una Blockchain. Ethereum emplea un lenguaje que es «Turing Completo» y tiene una moneda propia, llamada *ether*, la cual se emplea en el momento de la ejecución. Además, Ethereum puede implementar sistemas complejos, los cuales son, por sí mismos, un *altchain*. Por lo tanto, Ethereum es una plataforma para construir *altchains*.

Los *altcoins* y *altchains* pueden aprovechar la popularidad de *bitcoin* al emplear la misma prueba de trabajo. De esta manera, un minero puede obtener varias monedas a precio de una. Para poder emplear esta estrategia, la *altcoin* debe ser compatible con el minado unificado. Este aprovecha el espacio disponible de la entrada de la transacción de acuñado de *bitcoin* al almacenar la información de *altcoin*.

2.1.4. Transacciones

Las transacciones son el *leitmotiv* y la razón de ser de Bitcoin. Todas las demás partes están construidas para asegurar que las transacciones son creadas correctamente, propagadas en la red (P2P), verificadas y agregadas a la Blockchain. Las transacciones son estructuras de datos que almacenan transferencias de «valor» entre participantes del sistema. Cada transacción se almacena como una entrada en la Blockchain. En ellas hay que considerar lo siguiente:

A) Ciclo de vida

El ciclo de vida de una transacción comienza en el momento en que se crea la misma. A continuación, la transacción es firmada, una o varias veces, para indicar que ha sido autorizada de tal forma que una determinada cantidad de *satoshis* sean transferidos. Posteriormente, la transacción es propagada a través de la red P2P, donde cada nodo participante verifica y propaga la transacción hasta que esta llega a prácticamente todos los nodos de la red. Finalmente, la transacción es validada por un nodo minero y es incluida en un nuevo bloque de transacciones que es agregado a la Blockchain. Una vez que se encuentra en la Blockchain y ha sido confirmada por un número suficiente de bloques subsecuentes, la

transacción es una parte permanente de la Blockchain y es aceptada por todos los participantes. A partir de entonces, los fondos pueden ya ser transferidos por el nuevo propietario mediante una nueva transacción.

B) Estructura de la transacción

En esencia, una transacción es una estructura de datos que almacena las transferencias de *satoshis* desde un origen, llamado «entrada», a un destino denominado «salida». Las entradas y salidas de una transacción no están asociadas a cuentas o identidades. En su lugar, son una cantidad de *satoshis* que solo pueden ser gastados por el propietario de la dirección de destino mediante el uso de la clave privada asociada a dicha dirección. La estructura de una transacción se muestra en el cuadro 1.

Cuadro 1. **Estructura de una transacción de Bitcoin**

Tamaño	Campo	Descripción
4 *bytes*	Versión	Reglas a las cuales se acoge la transacción.
1-9 *bytes*	Total de entradas	El número de entradas que se incluyen.
Variable	Entradas	Una o más entradas de la transacción.
1-9 *bytes*	Total de salidas	El número de salidas que se incluyen.
Variable	Salidas	Una o más salidas de la transacción.
4 *bytes*	Bloque	Una fecha en formato UNIX o un número de bloques.

Fuente: elaboración propia.

El bloqueo indica la fecha mínima en la cual la transacción puede ser agregada a la Blockchain. Normalmente se emplea 0 para indicar que debe incluirse lo más pronto posible.

C) Entradas y salidas

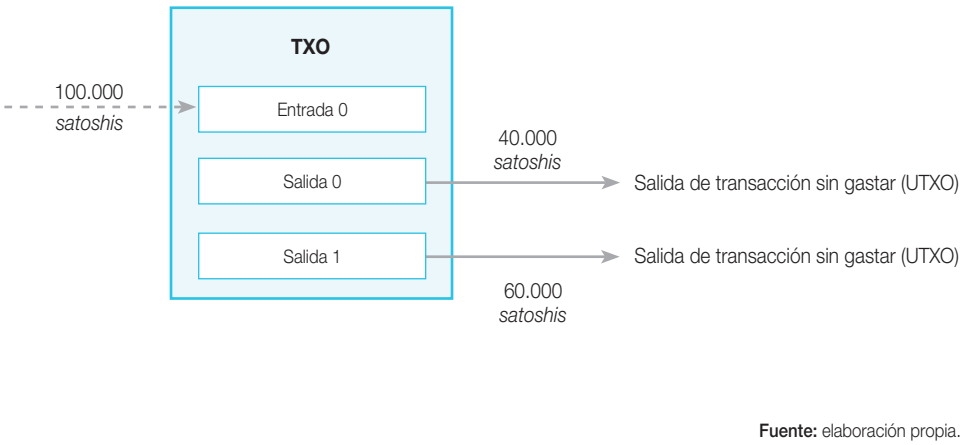
El componente principal de una transacción son las UTXO (*unspent transaction output*/ salidas de transacción sin gastar). Las UTXO son cantidades indivisibles que solo pueden ser liberadas por un dueño específico. Están almacenadas en la Blockchain y son reconocidas por toda la red, que lleva el seguimiento de todas las UTXO. Cuando un usuario recibe una

cantidad en *satoshis*, esta se almacena en una Blockchain como una UTXO. El concepto de «balance total de un usuario» no existe como tal, solo existe un conjunto de UTXO distribuidas a lo largo de la Blockchain, las cuales pueden ser transferidas por el usuario que posea la clave privada. Los programas de cartera calculan el balance al recorrer la Blockchain y agregar cada UTXO que le pertenece al usuario.

Aunque una UTXO pueda tener un valor arbitrario, este es indivisible. Si una UTXO es mayor al valor que se desea transferir, esta se debe consumir en su totalidad y el cambio correspondiente debe generarse en la transacción. Las UTXO consumidas por una transacción se denominan «entradas» y las UTXO generadas por la misma transacción son llamadas «salidas». La figura 2 muestra una transacción donde hay una entrada de 100.000 *satoshis*. Se desean transmitir 40.000 *satoshis* (salida) y se obtienen 60.000 *satoshis* (salida) de cambio.

De esta manera, los *satoshis* se mueven de un dueño a otro en una cadena de transacciones que consumen y crean UTXO. Las transacciones consumen las UTXO al liberarlas a través de una firma y crean una UTXO al asignarla a la dirección de un nuevo propietario. La excepción a la cadena de salidas y entradas es un tipo especial de transacción llamada «acuñado», que es la primera transacción de cada bloque. Esta transacción es colocada por el minero «ganador» y crea nuevos *satoshis* que se entregan como recompensa por el minado.

Figura 2. **Entradas y salidas de una transacción**



Fuente: elaboración propia.

Al tener Bitcoin usos potenciales más allá de su propósito original de efectuar pagos, varios desarrolladores han empleado Blockchain para otras aplicaciones, como «notarización», «contratos» y «formación», entre otros.

2.2. Marco teórico y trabajos relacionados con Blockchain en educación: Blockcerts, Edublock y Edgecoin

Una vez que hemos explicado Bitcoin y la tecnología Blockchain, cabe destacar que estas se han comenzado a aplicar en otros muchos dominios, siendo el de la educación uno de ellos. Sin embargo, hasta la fecha no existe una aplicación de la tecnología Blockchain y del minado competencial como el propuesto en este trabajo, de forma que se puedan resolver todas las problemáticas descritas en el apartado introductorio.

Existen tres enfoques parciales que abordan desde una perspectiva menos completa la problemática abordada, como son los Blockcerts[1], del Massachusetts Institute of Technology (MIT) y Oxford; Edublock[2], del Institute for the Future (IFTF); y el proyecto Edgecoin[3].

La institución MIT lleva unos pocos años realizando certificados digitales, en lugar de títulos en papel, para determinados cursos, seminarios y talleres impartidos en su institución. Estos títulos digitales tienen la ventaja de estar certificados de forma unívoca por la universidad que los expide, de forma que son intransferibles e inalterables, quedando almacenados en una cadena de bloques creada a tal efecto. En ese sentido, se almacena una credencial académica en una cadena inalterable, igual que en esta propuesta, pero, en ese caso, se almacenan títulos completos que no han sido refrendados o validados por el ecosistema donde dicho título tiene validez. Por tanto, se facilita que el estudiante disponga de una versión digital de sus títulos y que no puedan ser falsificados, quedando a disposición de las entidades empleadoras, pero no se validan de ninguna forma los conocimientos aplicados derivados de dichas titulaciones, ni es posible evaluar de ninguna forma la calidad de las enseñanzas de origen, que tampoco dispondrán de mecanismos para autoevaluar el grado de empleabilidad o el éxito de sus egresados más allá de los mecanismos de gestión de calidad externos y tradicionales de los que dispongan. Este modelo de certificación digital, que está incluido entre las ventajas del modelo propuesto (junto a muchas otras adicionales) ha tenido, en cualquier caso, un gran respaldo y aceptación institucional, hasta el punto de que otras universidades ya lo han adoptado (como The University of Texas [Austin], Holberton School, University of Oxford o University of Nicosia[4]), así como entidades privadas para certificar sus títulos, producto de cursos propios de formación (SAP, IBM, Fathom o Sony[5]).

1 <https://www.blockcerts.org/>.

2 <http://www.learningisearning2026.org>.

3 <http://www.edgecoin.io/>.

4 <http://digitalcurrency.unic.ac.cy/free-introductory-mooc/academic-certificates-on-the-Blockchain/>.

5 <http://www.sony.net/SonyInfo/News/Press/201602/16-0222E/index.html>.

El IFTF y la Fundación ACT presentaron la idea denominada «The Ledger» como una nueva tecnología que podría vincular el aprendizaje con las ganancias. La iniciativa Learning is Earning se enmarca como un juego que muestra una ventana al futuro del año 2026 donde se utilizan Edublock, una especie de moneda digital para cuantificar como transacciones las horas lectivas y poderlas almacenar en Blockchain. En este caso, la aproximación es la opuesta a la de Blockcert, pues no se almacenan títulos, sino horas dedicadas a clases presenciales o a distancia. No obstante, de nuevo, esto tampoco sirve para registrar competencias o destrezas, ni para validarlas o emplearlas como currículum digital de cara a entidades empleadoras.

Por su parte, el proyecto Edgecoin persigue instaurar una criptomoneda específica, basada en Bitcoin, para regular el mercado de bienes y servicios referentes al ámbito educativo, como pueden ser las matriculaciones en cursos *online*, los microcontratos entre entidades formativas y las transacciones digitales de bienes económicos destinados a la adquisición de bibliografía, servicios de apoyo o estudios reglados. En este enfoque simplemente se emplea una instancia diferente de los *bitcoins* para regular el mercado digital del sector, sin abordar en absoluto el ámbito de la educación en sí, la transferencia de competencias y resultados de aprendizaje, así como el almacenamiento, la validación y la criptorregulación de los mismos.

2.3. Implementación a escoger: Bitcoin, Ethereum o Multichain

Una vez planteada la hipótesis y el modelo que se va a desarrollar, es necesario escoger una tecnología y un protocolo subyacente para llevar a la práctica dicha idea mediante un prototipo plenamente funcional que permita ratificar la bondad del modelo planteado. Existen hoy día tres protocolos principales para prototipar de forma rápida y eficaz el modelo presentado: el propio protocolo empleado para Bitcoin, el protocolo de la segunda criptomoneda más extendida, Ethereum, y, finalmente, el protocolo Multichain que permite almacenar en la cadena de bloques diferentes elementos que no tienen por qué tener la misma estructura o tipología unos respecto de otros.

Al no ser este un trabajo que pretenda ahondar en la índole técnica del prototipo, sino en su utilidad y empleabilidad en el ámbito de la educación, en el cuadro 2 se recogen, de forma esquemática, el resumen de las ventajas y desventajas de cada uno, fruto del estudio tecnológico completo llevado a cabo por los autores.

En conclusión, no es posible emplear Bitcoin debido a la limitación implícita de la propia tecnología ligada al número máximo alcanzable con esta criptomoneda. Además, el sistema de minado exige (más allá del esfuerzo mental en que se basa la presente propuesta por parte del estudiante y del minero) un esfuerzo computacional que establece graves problemas de escalabilidad y eficiencia energética para la propuesta. Tampoco es posible emplear Multichain por culpa de no permitir los contratos inteligentes que a la postre surgen entre

las entidades formadoras y sus egresados con competencias validadas. Descartadas las otras dos propuestas, Ethereum se presenta como la mejor alternativa tecnológica. Permite el minado propuesto en el modelo y basado en la reputación de las partes (Schlegel, s. f.; Clow y Makriyannis, 2011) y, en un esfuerzo mental y no computacional, es eficiente, no tiene límites totales como Bitcoin y permite contratos inteligentes entre las partes, basados en certificaciones SSL para los firmados y resúmenes de competencias y destrezas. En esencia, es la mejor alternativa para crear el *altchain* necesario para el registro de adquisición de competencias que requiere esta aproximación. Las desventajas que presenta esta tecnología afectan sobre todo a las transacciones de criptomonedas, debido al tamaño de bloques y a la dificultad para hacer minados computacionales, y es por ello que no resultan ser limitantes para la presente propuesta. Se requiere, eso sí, generar una moneda específica para la contabilización transaccional que, como se presenta más adelante, en este caso serán los *kudos*, moneda de reputación o prestigio nominal para las entidades participantes (Sharples y Domingue, 2016).

Cuadro 2. **Implementaciones de Blockchain**

	Desventajas	Ventajas
Bitcoin	El uso de PoW es un esfuerzo demasiado alto al ser exponencial respecto a *n*. Límite: 21 millones. Alta latencia al generar o enviar transacciones cada 10 minutos. Actualizaciones del *software*. Ofrece una escalabilidad cuando es necesario que el bloque sea mayor que 1 MB (se logran manejar unas 7 transacciones por segundo [t/s]). Dificultad de recálculo 2.016 bloques (14 días). Solo contempla 8 decimales. Lenguaje C++ con limitación de comandos que limita la tecnología. Problemas de *hard folk*. Lenguaje de bajo nivel basado en pilas que requieren gran conocimiento del protocolo Bitcoin. Mismo coste computacional para enviar 0,01 valor, como 1.000.000 valor.	Transferencias realizadas con SHA-256. Es el modelo más difundido. Premio por minado: 12,5 (se van reduciendo a la mitad cada 210.000 bloques). Lenguaje simple utilizado: C++. Consenso: cadena correcta es la más larga. Bitcoin en sí es un contrato inteligente. La cadena más probada al ser el primero en aparecer.

▶

	Desventajas	Ventajas
▶		
Ethereum	Premio por minado: 3 *ether*. Lenguaje complejo y problemas para cometer errores. Requiere criptomoneda para funcionar. El tamaño está sin definir, pero es menor de 1 MB. Recálculo de dificultad en cada bloque cada 16 segundos.	Tiempo de bloque: 16 segundos. Hace uso de EtHash, rápido y seguro. Puede hacer uso de 18 decimales. Lenguaje Turing Completo: mayor control sobre todos los componentes de la red (permisos, minerías, etc.). Sin límite en el número de moneda.
Multichain	No utiliza contratos inteligentes. 64 MB de transacción máximo.	Transacciones: 1.000/s. Soporte de múltiples activos. Buen control del proceso de concesión de permisos.

Fuente: elaboración propia.

3. Modelo de confianza basado en Blockchain, competencias-pruebas de esfuerzo y *kudos*

La implementación llevada a cabo en Ethereum pretende dar forma al modelo de confianza propuesto, que se basa en Blockchain para verificar la adquisición de competencias por medio de pruebas de esfuerzo consistentes en la resolución de enunciados de problemas tipo en los que la recompensa se materializa en *kudos*.

Para ilustrar las ideas en las que se sustenta el modelo propuesto se incluye la figura 3. En ella cabe destacar la presencia de varios actores que se benefician del mismo:

- **Formador.** Es la entidad que instruye a un estudiante para que este adquiera una determinada competencia. Para la reputación del formador es fundamental que los estudiantes instruidos en una competencia demuestren que efectivamente la poseen. Si bien en el paradigma actual las instituciones formadoras tienen verificadas las competencias que adquieren sus alumnos, dicha verificación es más formalista que efectiva, motivo por el cual se requiere una aproximación más realista como la aquí descrita.
- **Estudiante.** Es la persona que ha sido instruida por un formador en una competencia. El estudiante está interesado en que dicha competencia sea reconocida por personas expertas en la misma (verificadores) para que de este modo tenga credibilidad de cara a su acceso al mundo laboral.

- **Verificador.** Se trata de personas, estudiantes y profesionales (incluidos docentes), capacitados para poder evaluar la adquisición de una competencia por parte de un estudiante. Los verificadores, por supuesto, deben demostrar continuamente su aptitud en la competencia que se quiere evaluar, lo que repercute positivamente en su reputación de cara a formadores y empleadores.
- **Empleador.** Están interesados en conocer las competencias que posee cada participante del sistema para poder contratar personal para sus empresas de manera adecuada. Los empleadores solo consultan la cadena y no definen las competencias en el paradigma actual (lo hacen otras instituciones oficiales); sin embargo, su participación ante un hipotético cambio de paradigma se antoja de gran utilidad para conocer mejor las necesidades del mercado en términos competenciales.

Como se aprecia en la figura 3, los actores del sistema interactúan teniendo como punto central la Blockchain en la que se almacenan las transacciones del sistema. En un caso de uso habitual, todo comienza cuando un formador instruye a un estudiante para que este adquiera una determinada competencia que se le transfiere (véase el paso 1 de la figura 3). Seguidamente, el estudiante desea que esa competencia le sea reconocida. Con el paradigma de educación actual bastaba con un título o certificado que, en realidad, no servía como prueba definitiva de la adquisición de la competencia por parte del estudiante. Con el modelo propuesto, el estudiante debe demostrar la adquisición de la competencia resolviendo un problema/enunciado tipo asociado a dicha competencia (véase el paso 2 de la figura 3). Los enunciados tipo, de los que se hablará más adelante, residen en un repositorio y son consensuados por parte de expertos en cada competencia.

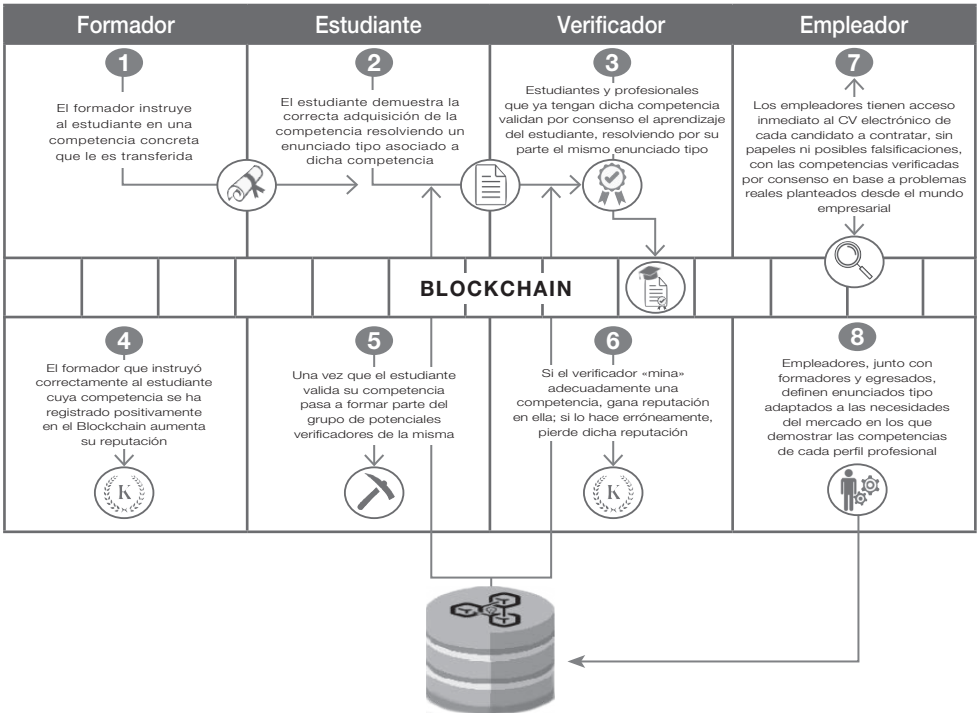
Una vez que el estudiante ha resuelto el problema tipo, los verificadores, a los que se exige poseer la competencia que se va a evaluar (habrá transacciones en la cadena que así lo demuestren), resolverán igualmente, como prueba de esfuerzo, el mismo enunciado tipo que ha sido facilitado al estudiante por parte del sistema, sin poder acceder a la resolución realizada por el estudiante hasta que el verificador lo resuelva por sí mismo para comparar los resultados obtenidos. En realidad, en esto consiste el proceso de minado en el modelo propuesto, siendo este un minado de tipo conceptual, consistente en la resolución de un problema tipo, y en la comparación de los resultados obtenidos por el estudiante y el verificador. En caso de que haya un consenso por parte de los verificadores de que el «aspirante» ha resuelto el problema tipo de manera correcta, se confirmará en el sistema una transacción que acredita la adquisición de la competencia por parte del estudiante (véase el paso 3 de la figura 3). Si no existe consenso, tanto el estudiante como la institución formadora perderían reputación asociada a la competencia evaluada. Si, en un escenario general, existe consenso, se derivan una serie de consecuencias:

- El formador aumentaría su reputación (véase el paso 4 de la figura 3).
- El estudiante, por la información registrada en la Blockchain, sería poseedor a todos los efectos de la competencia evaluada. Esto implica que ya podría, a su

vez, evaluar dicha competencia en procesos de minado futuros y que podría ser contratado por empleadores que requieran trabajadores con la competencia evaluada (véase el paso 5 de la figura 3).

Con carácter general, si los verificadores minan adecuadamente una transacción (resuelven el problema planteado de forma correcta), ganan reputación, perdiéndola en caso contrario (véase el paso 6 de la figura 3). De entre los mineros, el primero en resolver el problema de forma correcta y transmitirlo a la red ganan comparativamente más reputación que el resto. Este incentivo es el que permite que los verificadores actúen de forma rápida a la hora de validar competencias. Los empleadores, por su parte, consultarán la cadena para conocer qué sujetos del sistema poseen las competencias interesantes en sus procesos de contratación (véase el paso 7 de la figura 3). Dichos empleadores, junto con formadores y egresados (poseedores de una determinada competencia), definirán (*offline*) enunciados tipo que permitan evaluar la adquisición de una competencia por parte de un estudiante, siempre alineando esos enunciados con la realidad laboral de cada momento (véase el paso 8 de la figura 3).

Figura 3. **Elementos centrales del modelo propuesto**



Fuente: elaboración propia.

Centrándose en el proceso más *online* del modelo (véanse los pasos 2 a 4 y el paso 6 de la figura 3) y dejando de lado aquellos pasos de naturaleza más *offline* (véanse los pasos 1, 5, 7 y 8 de la figura 3), se podría definir el procedimiento propuesto en notación algorítmica del siguiente modo (por legibilidad se omiten los pasos relativos a cálculo de valores *hash* y enlace entre bloques, centrándose en el proceso de minado conceptual):

Algoritmo 1. **Verificación de competencias**

Entrada: cadena (C), estudiante (E), formador (F), competencia (C), enunciado-tipo (T), resultado del estudiante (RE), *kudos* involucrados (K) y número de personas en la red con la competencia C (NC).

Salida: resultado del consenso, cadena actualizada (BC'), *kudos* actualizados en mineros, formadores y estudiante.

Pasos:

1. E solicita añadir <E, F, T, C, *, RE, K> a BC (* se refiere a cualquier potencial minero "ganador").
2. Apoyos = 0.
3. Rechazos = 0.
4. **Para cada** minero M que mina <E, F, T, C, *, RE, K>, siempre que tenga la competencia C:
    4.1. M resuelve T, dando como resultado RM.
    4.2. M mina la transacción con RM (comprueba si RE = RM).
    4.3. **Si** el minado resulta positivo (RE = RM):
        4.3.1. M_Recomendación = Apoyo; Apoyos++.
    En otro caso:
        4.3.1. (RE ≠ RM): M_Recomendación = Rechazo; Rechazos++.
5. **Mientras** (Apoyos + Rechazos)/NC < PORCENTAJE_UMBRAL_MÍNIMO:
    ir al paso 4.
6. **Si** Apoyos >= Rechazos:
    6.1. Resultado = Apoyo.
    6.2. Añadir <E, F, T, C, M, RE, K> a BC, dando como resultado BC' (M es el minero ganador, el primero en minar correctamente).
    6.3. E_Kudos = E_Kudos + K.

▶

```
▶
      6.4. F_Kudos = F_Kudos + K.
      6.5. M_Kudos = M_Kudos + K.

   En otro caso (Apoyos < Rechazos):

      6.1. Resultado = Rechazo.
      6.2. E_Kudos = E_Kudos – K.
      6.3. F_Kudos = F_Kudos – K.

7. Para cada minero M' que ha minado en el paso 4 (M' ≠ M, minero no gana-
   dor).
        7.1. Si M'_Recomendación = Resultado:
               7.1.1. M'_Kudos = M'_Kudos + K/NC.
           En otro caso:
               7.1.1. M'_Kudos = M'_Kudos - K.
```

Fuente: elaboración propia.

Como se aprecia en el algoritmo, el estudiante interesado se postula como poseedor de una competencia, habiendo resuelto un enunciado determinado elegido aleatoriamente por el sistema de entre los establecidos para la competencia en cuestión (paso 1 del algoritmo 1). Para ello, los mineros resuelven el mismo problema tipo (se supone un número suficiente de mineros para cada tipo de problema en un régimen permanente de funcionamiento) y comprueban el resultado del estudiante (paso 4 del algoritmo 1). Cabe destacar que se precisa un cuórum mínimo de mineros para que el minado sea efectivo (paso 5 del algoritmo 1). Si el estudiante, por consenso de los mineros, posee la competencia, la transacción se confirma y se suman *kudos* a él mismo, al formador y al minero «ganador». En caso contrario, se resta reputación al estudiante y al formador (paso 6 del algoritmo 1). Para los mineros no ganadores, si han minado adecuadamente, su reputación aumenta, pero no tanto como la del minero ganador. En caso de no minar correctamente, su reputación disminuye (paso 7 del algoritmo 1).

Sin duda, el paso culmen del algoritmo anterior ocurre cuando se comprueba que, efectivamente, un estudiante es poseedor de una competencia. En ese momento, la transacción se confirma y pasa a formar parte de la cadena de manera permanente (nótese que la permanencia es una de las propiedades fundamentales de toda transacción), almacenándose dicha transacción en el dispositivo correspondiente de almacenamiento permanente.

Para ilustrar en concreto qué datos son almacenados al confirmarse una transacción se presenta la figura 4, en la que se muestra la estructura de una transacción en el sistema propuesto con un posible contenido de ejemplo para cada campo.

Como se deduce de la figura 4, el bloque que hay que almacenar en la Blockchain es de tan solo 128 *bytes* y tiene los siguientes campos:

- Cinco identificadores unívocos: estudiante, institución formadora, enunciado-tipo resuelto, competencia y minero que validó la competencia. Se emplean 8 para cada uno, es decir, 40 *bytes* en total.
- Los resultados obtenidos (por el estudiante y el minero, tras comparar que son iguales) para el enunciado tipo. Para ello se emplea el estándar IEEE754 de doble precisión, utilizando para ello 8 *bytes*.
- Cantidad de *kudos* involucrada en la transacción. Hasta el momento se ha manejado un prototipo con valores enteros individuales, sumándose o restándose una unidad de esta moneda de prestigio. Si en un futuro fuera necesario ajustar estos valores, por ejemplo, a la complejidad de un enunciado-tipo o a la cantidad de egresados con una determinada competencia, este campo permitiría ese ajuste. Se emplea de nuevo el estándar IEEE754 de doble precisión, utilizando para ello 8 *bytes*.
- Espacio libre a disposición de otros posibles usos o eventualidades futuras: un total de 72 *bytes* para futuras eventualidades, y eso daría 128 *bytes*.

Figura 4. **Estructura de una transacción en el sistema propuesto**

Versión	02000000
Hash del bloque	17975b97c18ed1f7e255adf297599b55
Previo	330edab87803c8170100000000000000
Raíz Merkle	8a97295a2747b4f1a0b3948df3990344c0e19fa6 b2b92b3a19c8e6badc141787
Timestamp	358b0553
Bits	535f0119
Nonce	48750833
Contador de transacción	63
Id_estudiante	000000B8
Id_formador	00000071
Id_enunciado	000003A3
Id_competencia	000037E2
Id_minero	0000701D
Resultado	AC34097B
Kudos	00000001
Espacio_libre	00000000000000000000000000000000000000000000000000000000000000000000000000000000

Hash de bloque → 0000000000000000e067a478024addfecdc93628978aa52d91fabd4292982a50

Fuente: elaboración propia.

Por último, es importante comentar que, en esta primera versión del modelo propuesto, se ha optado por utilizar, a modo de prueba, enunciados tipo que se almacenan en una base de datos XML externa. Se ha optado por utilizar XML como formato base para los enunciados porque ello facilita la estructuración y organización de los enunciados (buscando su homogeneización), permite un intercambio sencillo a través de la web y ofrece una gran versatilidad a la hora de adecuar la presentación del enunciado a las partes involucradas en función de sus preferencias, dispositivo, características de conexión, etc.

4. Prototipo y validación de la propuesta

4.1. Descripción y validación del prototipo

Se ha creado un prototipo, basado en Ethereum, para la puesta en marcha de la aproximación presentada en el apartado anterior, que persigue dar respuesta a las siguientes hipótesis de trabajo:

- **RQ1.** El modelo permite comparar entidades formadoras dedicadas a instruir al estudiante en unas mismas competencias profesionales, identificando entidades con malas praxis formativas.
- **RQ2.** El modelo permite refrendar los conocimientos de los estudiantes, identificando a estudiantes sin conocimientos mínimos, como fuente rápida y sencilla de información para empleadores.
- **RQ3.** El modelo permite reciclar las enseñanzas regladas y no regladas para adecuarlas a la realidad empresarial.

El prototipo, plenamente funcional, se puso en marcha adaptado al perfil profesional de administrador de sistemas, propio del ámbito de la ingeniería informática, según el Real Decreto 1393/2007, de 29 de octubre, y el libro blanco elaborado para esta titulación por la Agencia Nacional de Evaluación de la Calidad y Acreditación (ANECA). De dicha fuente se obtuvo un subconjunto de competencias, verificadas oficialmente, asociadas a las materias tomadas como referencia (se mencionan más adelante) en este estudio. En el experimento de validación se implantaron cuatro entidades formadoras, cuyos nombres se omiten para evitar connivencias, filias o fobias en el estudio: una universidad a distancia con dos asignaturas de grado, un ciclo de MOOC, estudios reglados por una academia multinacional tecnológica y un curso de una plataforma *online* no certificada y con un prestigio en decadencia. Para cada una de las entidades se registraron 20 estudiantes que lograron terminar su formación satisfactoriamente, sin sesgos por edad, sexo, dedicación

profesional o estudios/conocimientos previos, reuniendo a un total de 80 estudiantes que aprobaron los cursos (20 estudiantes que superaron simultáneamente las dos asignaturas universitarias, 20 del MOOC, 20 de la academia y otros 20 de la plataforma no certificada). Asimismo, se registraron 2 empresas empleadoras, cuyo nombre igualmente se omite, una centrada en el ámbito de la administración en red y otra en el ámbito de la administración de bases de datos. Adicionalmente, se dispuso de un total de 100 usuarios verificadores, o «mineros», procedentes el 60 % del mundo académico (egresados cualificados por universidades españolas) y el 40% restante del mundo profesional del sector, igualmente con competencias claramente validadas en este ámbito profesional. Para toda la muestra se puso en marcha un Blockchain basado en Ethereum para el registro de las competencias verificadas y una base de datos relacional XML para la creación y la explotación de enunciados tipo.

En primer lugar, se proporcionó a las empresas empleadoras enunciados tipo que permitieran verificar destrezas tácitas en el ámbito del perfil profesional que se iba a estudiar. Estos enunciados, basados en las propias pruebas de acceso que esas empresas emplean en sus procesos de selección, dieron lugar a una familia de más de 100 enunciados diferentes, en función de la variación semiautomática de los parámetros que definen el problema. Estos enunciados pasaron a nutrir la mencionada base de datos de «enunciados tipo».

Antes de la puesta en marcha de la validación en sí, los 100 mineros demostraron, mediante una evaluación guiada y supervisada por los autores y por un representante de cada entidad formadora, que eran capaces de resolver sin problemas un enunciado de entre los almacenados, con lo que se creó un sistema plenamente funcional para esta etapa inicial en el experimento. Tras seis meses de funcionamiento, los estudiantes adquirieron las competencias reseñadas por cada formador. Como se ha indicado anteriormente, en el experimento se empleó una muestra de 80 estudiantes que habían aprobado sus estudios y se procedió a la validación de sus competencias por minado. Se empleó el sistema basado en Blockchain tanto para este minado como para calcular y almacenar la reputación de cada entidad implicada. Los resultados del experimento aparecen resumidos en los siguientes apartados.

A) RQ1

Del total de 80 estudiantes que obtuvieron las competencias técnicas por medio de una de las entidades formadoras, solo 58 lograron validar dicha competencia resolviendo un enunciado tipo elaborado por las entidades empleadoras que fueron minadas positivamente por consenso de los verificadores. Estas 58 competencias son las que se incluyeron en la Blockchain, quedando los otros estudiantes restantes (22) fuera del registro validado de competencias (posiblemente deberían haber sido suspendidos por la entidad formadora en cuestión).

Un estudio pormenorizado, llevado a cabo por un panel de expertos de entidades formadoras y empleadoras, ratificó que la entidad formadora ubicada en cuarta posición no formaba adecuadamente a los estudiantes, a pesar de indicar expresamente que estos adquirirían unas competencias que, en base a su metodología, profesorado y contenidos, no podían impartir correctamente. Para el resto de entidades, el panel estaba más o menos de acuerdo en que las entidades eran similares en cuanto a calidad formativa, destacando posiblemente la entidad que se encumbró en primera posición como la más prestigiosa. El cuadro 3 recoge los resultados.

Cuadro 3. **Datos relativos a las diferentes instituciones**

Entidad formadora	*N* estudiantes aprobados	*N* enunciados tipo realizados	*N* competencias minadas	Reputación final relativa (*kudos*)/ posición *ranking*
Universidad a distancia	20	20	19	+19 K/2.º
Ciclo MOOC	20	20	18	+18 K/3.º
Academia tecnológica	20	20	20	+20 K/1.º
Tutorial *online*	20	20	1	+1 K/4.º

Fuente: elaboración propia.

B) RQ2

Se llevaron a cabo entrevistas, pruebas de acceso y análisis directos en puestos de trabajo con cada uno de los 80 estudiantes, realizadas por un panel de expertos de las empresas empleadoras. En este estudio, se ratificaron los resultados del minado al 98,75 %, identificándose claramente que 22 personas no disponían de las destrezas necesarias para abordar tareas cotidianas propias del perfil profesional que se estaba estudiando. De los 58 estudiantes que lograron ratificar sus competencias, 1, finalmente, resultó ser no apto para el puesto de trabajo. Se estudió, por medio de encuestas dirigidas, este caso, resultando que el estudiante copió, durante el proceso de resolución del enunciado tipo, de otro estudiante de la muestra. Este hecho, de gran relevancia, se discute posteriormente en el apartado «Líneas futuras». Los resultados se muestran en el cuadro 4.

Cuadro 4. **Resultados del minado**

		Validación de campo real	
		Profesional apto	Profesional no apto
Resultados del minado	Profesional apto	57	1
	Profesional no apto	0	22

Fuente: elaboración propia.

Considerando el cuadro 4 como si de una matriz de confusión se tratara, vemos que el procedimiento de minado ha obtenido una precisión del 98,75 %, que no ha habido ningún falso negativo (estudiantes con destrezas reales descalificados por error por el sistema) y tan solo 1 falso positivo de un tamaño muestral de 80, debido, precisamente, a un acto ilegítimo realizado por el estudiante durante la prueba.

C) RQ3

Alcanzar resultados concluyentes para esta hipótesis de trabajo requeriría la observación directa e indirecta de la aplicación de este modelo en el ámbito de la educación superior en un número elevado de instituciones de diversa índole para comprobar su aceptación y ponderación en los diseños de planes de estudio reglados futuros. Para lograr alcanzar resultados cualitativos no concluyentes que den respuesta a la cuestión, se planteó realizar un análisis de caso, en función de entrevistas dirigidas mediante un método Delphi con un panel conformado por los docentes implicados directamente en la instauración del prototipo. En las entidades formativas del experimento participaron un total de 12 profesores: 2 impartiendo clases en la universidad, 3 impartiendo clases en el ciclo de MOOC, 5 en la academia tecnológica y 2 en el tutorial *online*. No todos ellos recibieron, en primera instancia, los resultados alcanzados en el proceso de minado de sus alumnos y la ponderación de las instituciones a las que pertenecían hasta una vez concluidas las entrevistas.

En una primera iteración de consulta al panel, se les preguntó:

- Si consideraban este modelo como ideal para adecuar las enseñanzas superiores a la realidad empresarial. El resultado, en una encuesta cerrada (sí/no), es el mostrado en la figura 5. No existe correlación estadística representativa entre las respuestas y la entidad formativa a la que pertenece el encuestado.

  Tan solo un profesor, procedente de la academia tecnológica que se estaba estudiando, no estuvo de acuerdo al considerar que, aun siendo un modelo de gran

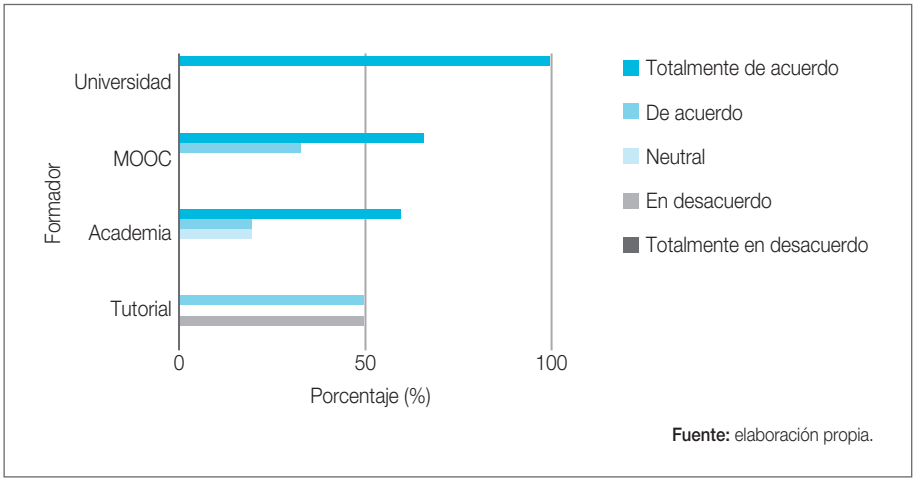
potencial y eficiencia demostrada, había ciertas enseñanzas que podían diferir de la realidad empresarial por ser la propia empresa (según el criterio de este encuestado) quien debería dar formación específica de índole práctica a sus contratados en programas propios de formación de sus recursos humanos.

- ¿Si más de un 10 % de tus estudiantes no logran validar las competencias que han aprobado con tus enseñanzas, te plantearías reenfocar tu metodología y contenidos? El resultado, en una escala Likert de 5 valores, es el mostrado en la figura 6.

Figura 5. **Respuesta del panel**

Fuente: elaboración propia.

Figura 6. **Resultados: escala Likert sobre modificación de enseñanzas**



Fuente: elaboración propia.

En esta ocasión sí parece haber discrepancias dependiendo de la entidad a la que pertenece cada encuestado y, por ello, en la figura se refleja dicha procedencia. Tras una primera iteración, se realizó una segunda consulta al panel, de tipo exploratoria, para conocer las motivaciones de cada profesor en sus respuestas. En la universidad, los 2 profesores estaban totalmente de acuerdo con la afirmación.

En el caso del ciclo de MOOC, 2 profesores estaban totalmente de acuerdo y 1 no indicó este valor por considerar que no era relevante el hecho de modificar o no la metodología de

enseñanza, sino solo los contenidos. En cuanto a la academia tecnológica, el profesor que consideraba innecesario adecuar contenidos a la realidad empresarial se mantuvo en una respuesta neutral; otro profesor indicó estar de acuerdo en cambiar contenidos, pero no su metodología; y 3 profesores (más del 50 %) indicaron estar totalmente de acuerdo con la afirmación. Finalmente, los profesores de tutoriales de internet declararon de forma diferente: uno estaba de acuerdo en cambiar su metodología, pero no los contenidos de sus cursos por considerarlos muy adecuados; otro indicó estar en desacuerdo por considerar que su formación no reglada no debía supeditarse al refrendo de los conocimientos de sus estudiantes y que esta adaptación solo debería afectar a instituciones oficiales regladas. Esta afirmación, no obstante, entra en claro conflicto con la propia publicidad del tutorial y con su coste, criticable si los egresados no adquieren las competencias prometidas.

En resumen, cabe destacar que de los 12 encuestados, 7 de ellos (prácticamente el 60 %) estarían totalmente de acuerdo en dar un vuelco a sus enseñanzas en caso de que los estudiantes presentaran problemas competenciales sacados a la luz gracias al mecanismo de confianza por consenso aquí propuesto y 10 (más del 83 %) se plantearían, en cualquier caso, adaptar contenidos o la metodología empleada. Además, más del 90 % considera este modelo como ideal para adecuar las enseñanzas superiores a la realidad empresarial.

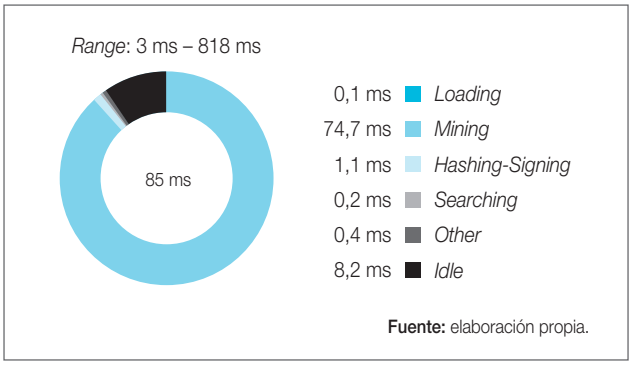
4.2. Eficiencia y validez del prototipo a nivel computacional

Por último, una vez validado el prototipo en función de sus objetivos, resta validar su viabilidad desde el punto de vista técnico y computacional. El escenario empleado para la validación del modelo y su prototipo concluyó con un total de 186 participantes en la red P2P y una Blockchain que ocupaba un total de 7.424 *bytes* útiles y un total de algo menos de 8 KB, incluyendo las referencias de cadena y los i-nodos.

Actualmente, Ethereum consigue manejar con eficacia los más de 160 GB totales que ocupa la Blockchain para Ether y Bitcoin hoy día (este dato aumenta hora a hora), por lo que, haciendo una estimación rápida, este prototipo funcionaría con total eficacia para redes con varios miles de millones de estudiantes.

Se analizó, asimismo, el rendimiento de la red P2P y las transacciones que afectaban al minado, almacenamiento, lectura, etc., tanto de bloques como de enunciados tipo y resultados (véase figura 7).

Figura 7. **Rendimiento de la red P2P**

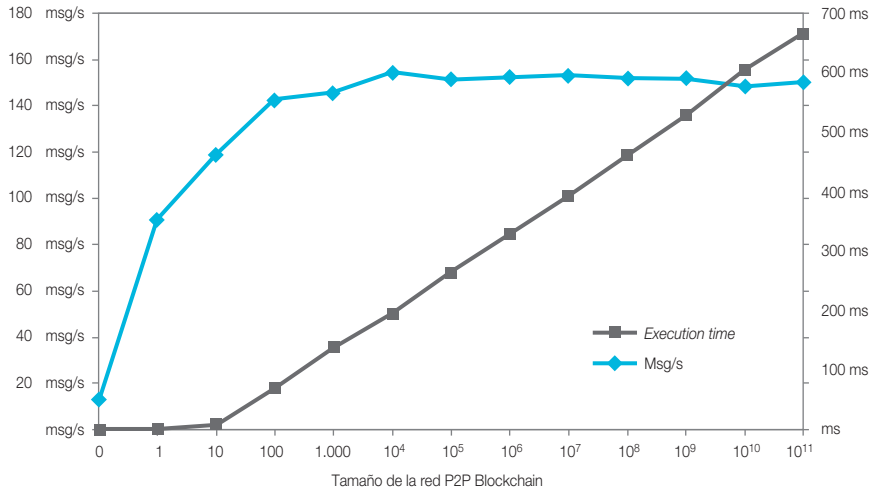


Fuente: elaboración propia.

Las operaciones se mantuvieron siempre entre los 3 milisegundos y los 818 milisegundos cuando la red estaba completamente nutrida y la cadena había crecido hasta su máxima longitud. En cualquier caso, siempre las operaciones requirieron menos de un segundo para llevarse a cabo. De media, las operaciones requirieron 85 milisegundos, repartidos para cada transacción como indica el gráfico: un tiempo casi despreciable para cargar la Blockchain; 74,7 milisegundos para realizar el minado computacional de los bloques adyacentes y el bloque objetivo; 1,1 milisegundos en firmar el bloque actual objetivo y 0,2 milisegundos en búsquedas dentro de la cadena. Además, aparece un tiempo de unos 8,2 milisegundos no asociados a operación alguna, sino a la latencia de la red P2P del prototipo por transacción.

Una vez comprobada la eficiencia del prototipo en el actual escenario, se realizó un estudio de extrapolación por regresión para comprobar la escalabilidad del sistema y su comportamiento en caso de aumentar el tamaño de la red P2P y de la Blockchain. Las variables de estudio establecidas fueron, por un lado, el tiempo de ejecución medio de una operación en el sistema al crecer la red de nodos (usuarios) involucrada y, por otro, el trasiego de mensajes en la red P2P, a términos de mensajes por segundo, al crecer igualmente el tamaño de la red en sí. Estas son, según los estudios, las dos cuestiones que más afectan al rendimiento de Bitcoin y, por tanto, se consideran los mejores indicadores para estudiar si el prototipo es viable para una implantación a gran escala. La figura 8 resume los resultados obtenidos.

Figura 8. **Estudio de extrapolación por regresión**



Nota. Msg/s = mensajes por segundo.

Fuente: elaboración propia.

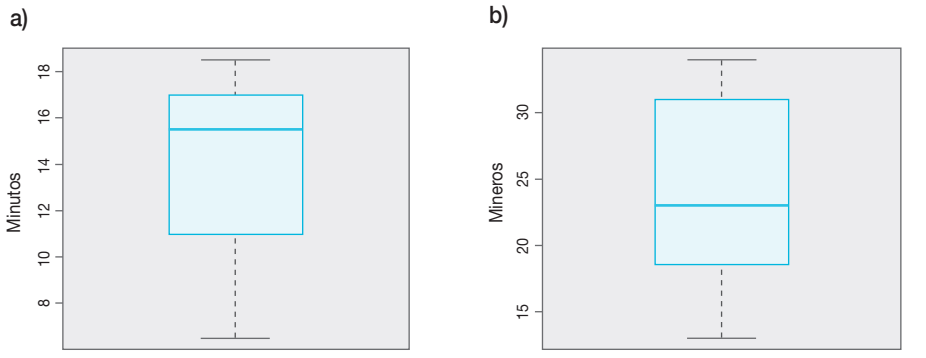
Se puede comprobar que, para una red pequeña como la del escenario de estudio (186 participantes), la ejecución media de una operación lleva menos de 100 milisegundos (en concreto 85 como se explicó antes) y la replicación y comunicación inherente a Blockchain se mantuvo en unos 140 mensajes por segundo, siendo la mayoría de ellos a nivel de enlace entre cada nodo y el servidor P2P. Puede comprobarse que, al aumentar exponencialmente el tamaño de la red, el tiempo de ejecución progresa de forma lineal, siempre por debajo de unos límites razonables (para redes con casi 1 billón de usuarios, las operaciones siguen por debajo de un segundo de latencia), mientras que la sobrecarga de la red se mantiene acotada asintóticamente en unos 150 mensajes por segundo. Esto es posible gracias a la gestión interna de Ethereum y su manejo de *brokers* intermedios para la escalabilidad polinomial.

Son valores muy esperanzadores que permiten asegurar que el sistema es plenamente funcional y escalable de cara a abordar una implementación completa en el dominio internacional de la educación superior, pudiendo crecer la red enormemente (como se mencionó antes) sin que el rendimiento sea un problema.

El único factor limitante del prototipo es precisamente un factor no técnico, dependiente del interés de la propia comunidad en la labor fundamental que es el minado. En este modelo, la labor de minado no está respaldada por un esfuerzo computacional de un dispositivo de la red, sino por el esfuerzo cognitivo y mental del usuario que hay detrás de ese dispositivo conectado, es decir, se trata de un esfuerzo personal dependiente del factor humano. Debe existir suficiente interés en la comunidad por la consecución de *kudos* que respalden la reputación y el prestigio de cada minero en una determinada competencia, y que así este capital, un tanto «intangible», sirva de acicate y motivación para el minero. Obviamente, esto solo será posible si se establece un correcto factor de externalidad de red, donde cada vez más y más entidades formadoras, empleadores y profesionales se adhieran al entorno colaborativo presentado y de esa forma los *kudos* y lo que representan sean suficientes como para incentivar la labor del minado. En el prototipo, los 100 mineros mantuvieron una actitud proactiva y plenamente positiva de cara a esta labor, hasta el punto de que, cuando una nueva competencia debía ser minada, el tiempo de minado se mantuvo siempre por debajo de los 20 minutos en total. El intervalo de confianza para el tiempo de minado se estableció entre los 11 y los 17 minutos, y de media cada competencia se tardó en minar unos 15 minutos y 30 segundos (véase figura 9 a). Estos tiempos aluden al primer minero que logró confirmar/validar cada competencia, pero obviamente varios intentos de minado acompañaron cada uno de los procesos de minería. Cada uno de los 80 bloques minados (58 positivos, el resto desechados) reunió, como mínimo, a 13 mineros y como máximo a un total de 35 de los 100 mineros disponibles. Dado el número de mineros que gozaba de las distintas competencias en este estudio, los umbrales de consenso quedaron establecidos en 12 mineros (51% de los mineros totales con cada competencia concreta). De media cada transacción fue minada por 23 mineros, estableciéndose como intervalo de confianza un grupo de entre 19 y 31 mineros por cada competencia a validar (véase figura 9 b).

Son datos válidos en este estudio dirigido, pero obviamente el éxito del proceso de minado en una implantación total del sistema dependerá de la cantidad de usuarios adheridos a la comunidad y a este novedoso sistema de confianza, para incentivar, de forma suficiente, dicha acción de minado a cambio de prestigio en el ámbito educativo-profesional.

Figura 9. **Distribución del tiempo de minado y cantidad de mineros**



Fuente: elaboración propia.

5. Líneas futuras

En esta primera aproximación a la solución del modelo propuesto se ha llevado a cabo una implementación que, si bien es completamente funcional, ha sido validada en un escenario específico algo limitado.

Por ello, se plantean las siguientes líneas de trabajo futuro:

- **Asegurar el proceso legítimo de verificación competencial mediante pruebas supervisadas en centros de exámenes oficiales.** Como se ha comentado en este documento, hay partes del procedimiento (véase figura 3) que se llevan a cabo en línea y que, por tanto, están totalmente controladas por el sistema. Sin embargo, hay otras que se realizan fuera de línea, sin el control del sistema. Una de ellas es la resolución del enunciado tipo por parte del estudiante (y también de los evaluadores). De cara a verificar la identidad de los autores de los enunciados se deberían establecer mecanismos como, por ejemplo, la supervisión en centros oficiales. No obstante, también creemos que el fraude, en caso de ocurrir, sería autorregulado por el propio sistema. A modo de ejemplo, si alguien resuelve un enunciado de

forma fraudulenta y luego es contratado por empleadores, quedará en evidencia al no poseer realmente dicha evidencia, como de hecho ha ocurrido en el propio estudio de caso al resolver RQ2.

- **Aplicar el prototipo a perfiles profesionales más amplios, que incluyan más competencias técnicas y una mayor representatividad de los roles implicados en el modelo.** En este estudio se ha tomado como referencia un escenario concreto con unos perfiles determinados. Para confirmar la validez de la propuesta y su carácter general, sería conveniente realizar una evaluación exhaustiva en otros ámbitos de conocimiento y con una mayor representación de cada uno de los roles.
- **Analizar la viabilidad de verificar competencias no técnicas, de tipo transversal o general.** El modelo propuesto y su implementación parten de la premisa de que es posible obtener un resultado concreto al realizar un enunciado tipo para poder comprobar la adquisición de una competencia. Esta aproximación suele ser válida en ámbitos de conocimiento eminentemente técnicos. Sin embargo, en otros ámbitos menos técnicos o cuando hay involucradas competencias difíciles de evaluar, se requieren otros tipos de medios de evaluación. El uso de otras pruebas no numéricas, como el porfolio digital o la recopilación de videoentrevistas dirigidas por asistentes automáticos, se presentan como opciones atractivas. En esos casos puede que los mineros no tengan que tener validada la misma competencia que el estudiante quiere validar, sino otra diferente asociada precisamente a la evaluación de la competencia en cuestión. Esto podría aplicarse a competencias más generales, transversales o no vinculadas a la resolución de enunciados. Es muy sencillo adaptar el modelo propuesto a esa realidad, siendo por tanto aplicable también en dicho ámbito.
- **Gestión de competencias.** En la implementación llevada a cabo, las competencias han sido tomadas a partir de una agencia oficial como es la ANECA. La gestión de competencias (definición, asociación a estudios universitarios, evolución de las mismas, etc.) es una tarea ardua y costosa que, en el paradigma actual, es llevada a cabo por agencias como la citada ANECA. Si dicha gestión sigue siendo gestionada de manera efectiva por este tipo de instituciones, el modelo propuesto seguirá funcionando con normalidad. Sin embargo, si se da un cambio de paradigma en el que la definición y gestión propia de las competencias deja de ser labor de una entidad determinada, se ofrece como línea de trabajo futuro la implantación de una Blockchain paralela que permita la gestión colectiva de dichas competencias por parte de los actores principales (empleadores, entidades formadoras e incluso los propios expertos).
- **Validación de enunciados tipo.** En esta implementación inicial, los enunciados tipo han sido validados y consensuados por los propios actores involucrados en el proceso y presentes en los experimentos, siendo posteriormente almacenados en una base de datos. De cara a una implementación global y general, se propone el uso de otra Blockchain paralela que permita validar dichos enunciados tipo que quedarían registrados en forma de transacciones consensuadas.

6. Conclusiones

En este trabajo se presenta un modelo de confianza en la enseñanza superior abierta y ubicua, basado en la tecnología Blockchain, que certifica la adquisición de competencias por parte de estudiantes formados en diferentes instituciones docentes. El modelo propuesto se basa en un protocolo de consenso de expertos que forman parte del mismo sistema.

La aproximación presentada se beneficia de las bondades propias de la tecnología subyacente y, además, supone *per se* un gran avance en el ámbito de la educación, ya que permite comprobar de manera fidedigna la adquisición de competencias por parte de los estudiantes y, lo que es más, garantizar que la preparación de estos es acorde a la realidad laboral y a las necesidades actuales demandadas en el mercado. Además, se permite poner en valor a las entidades formadoras implicadas en ese proceso, sean del tipo que sean, evaluándolas de forma justa, automática y descentralizada. Se facilita que dichas entidades tengan un mecanismo rápido y eficaz para autoevaluar sus enseñanzas y adaptarse al mundo laboral tan cambiante. También se simplifican los procesos de contratación y evaluación de candidatos por parte de las empresas empleadoras, que, además, no tendrán que preocuparse por la falsificación documental, que quedará erradicada. Finalmente, los estudiantes gozarán de un completo currículum digital, infalsificable, sencillo de consultar y validado por una comunidad competente.

La aproximación presentada se beneficia de las bondades propias de la tecnología subyacente y, además, supone *per se* un gran avance en el ámbito de la educación, ya que permite comprobar de manera fidedigna la adquisición de competencias por parte de los estudiantes y, lo que es más, garantizar que la preparación de estos es acorde a la realidad laboral y a las necesidades actuales demandadas en el mercado

El modelo se ha materializado en forma de un prototipo implementado, plenamente funcional, y evaluado en un entorno real, habiéndose obtenido resultados positivos que ponen de manifiesto las innumerables ventajas de la propuesta para estudiantes, instituciones formadoras, expertos y empleadores.

Una de las principales características del modelo propuesto es su alto rango de aplicabilidad a cualquier escenario en el que existan instituciones docentes que forman estudiantes en la adquisición de competencias útiles para el mercado laboral.

Este trabajo también abre la posibilidad de seguir explorando el enorme potencial de la tecnología Blockchain en otros aspectos del ámbito educativo y extrapolar las ideas presentadas en este documento a otros dominios de aplicación tan variopintos como el ámbito del diagnóstico médico, la evaluación de riesgos financieros o la gestión del conocimiento empresarial, entre otros.

Referencias bibliográficas

Bartolomé, A. R., Bellver, C., Castañeda, L. y Adell, J. (2017). Blockchain in education: introduction and review of the state of the art. *EDUTEC. Revista Electrónica de Tecnología Educativa*, *61*.

Buterin, V. (27 December 2015). Understanding serenity, part 2: Casper. *Ethereum Blog*. Recuperado de <https://blog.ethereum.org/2015/12/28/understanding-serenity-part-2-casper/> (consultado en febrero de 2018).

Cano, E. y Cabrera, N. (2016). Competency assessment tool (CAT). The evaluation of an innovative competency-based assessment experience in higher education. *Journal Technology, Pedagogy and Education*, *25*(5).

Clow, D. y Makriyannis, E. (27 February-01 March 2011). iSpot analysed: participatory learning and reputation. *Proceedings of the 1st International Conference on Learning Analytics and Knowledge* (pp. 34-43). Banff, Alberta.

Jones, H. (15 March 2016). Broker ICAP says first to use Blockchain for trading data. *Reuters*. Recuperado de <http://uk.reuters.com/article/us-icap-markets-Blockchain-idUKKCN0WH2J7> (consultado en febrero de 2018).

King, K., Prince, K. y Swanson, J. (2016). Learning on the block: could smart transactional models help power personalized learning? *KnowledgeWork Forecast 4.0*. Recuperado de <https://www.Blockchaindailynews.com/attachment/756565/> (consultado en abril de 2018).

Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. *Bitcoin*. Recuperado de <https://bitcoin.org/bitcoin.pdf> (consultado en abril de 2018).

Schlegel, H. (s. f.). Reputation currencies. *Institute of Customer Experience*. Recuperado de <http://ice.humanfactors.com/money.html> (consultado en abril de 2018).

Sharples M. y Domingue J. (2016). The Blockchain and kudos: a distributed system for educational record, reputation and reward. In K. Verbert, M. Sharples y T. Klobucar (Eds.), *Adaptive and Adaptable Learning. EC-TEL 2016*. Part of the *Lecture Notes in Computer Science* book series, 9891. Springer.

Tapscott, D. y Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Brilliance Audio.

Valenzuela, J. (15 March 2016). Arcade city: Ethereum's big test drive to kill Uber. *Cointelegraph*. Recuperado de <http://cointelegraph.com/news/arcade-city-ethereums-big-test-drive-to-kill-uber> (consultado en febrero de 2018).

Nuestro sistema de enseñanza

/ Adaptados al mercado laboral. Adaptados a ti

Mucho más que una universidad a distancia

La Universidad a Distancia de Madrid, UDIMA, es una institución educativa pensada y diseñada para cubrir las necesidades de las personas del siglo XXI: profesionales que demandan una universidad abierta y flexible, que permita compatibilizar el estudio con las peculiaridades de cada estudiante, y que buscan obtener una titulación universitaria reconocida oficialmente y de prestigio, adaptada a Europa y en contacto con el mundo de la empresa, y que facilite, además, una buena inserción laboral o mejore la que ya se posee.

Campus virtual y sistema de evaluación

El proceso de aprendizaje se desarrolla a través de las aulas virtuales de la universidad. Los estudiantes establecen una comunicación directa con sus profesores a través de los foros, el teléfono y otras herramientas telemáticas, como las clases en videoconferencia. Un sistema de evaluación continua, que utiliza las últimas herramientas tecnológicas en el ámbito de la didáctica, nos permite desarrollar una metodología activa que ayuda a nuestros estudiantes a «aprender haciendo».

Profesorado

En la UDIMA, la actuación de los docentes no se limita a la enseñanza, sino que también son «guías y facilitadores». La realización de un seguimiento académico pormenorizado y la personalización de la acción docente hacen de la UDIMA una comunidad de aprendizaje centrada en las personas.

Materiales de enseñanza

Nuestra editorial técnica se encarga de diseñar materiales específicamente creados para el aprendizaje online. Además, utilizamos recursos audiovisuales y material complementario de todo tipo que permiten aprovechar al máximo la experiencia formativa.

Actividades de aprendizaje

Los estudiantes van adquiriendo conocimientos a través de distintas actividades, tanto individuales como en grupo, para ir afianzando los contenidos.

Test de autoevaluación

Pruebas de evaluación online tipo test que, a modo de cuestionarios de autocomprobación, permiten que el estudiante pueda constatar los conocimientos adquiridos en el estudio previo de las unidades didácticas correspondientes.

Actividades de evaluación continua

Este tipo de actividades didácticas son pruebas de evaluación de tipo práctico: casos y trabajos basados en la búsqueda de información, el análisis de situación y la realización y presentación de informes.

Exámenes presenciales

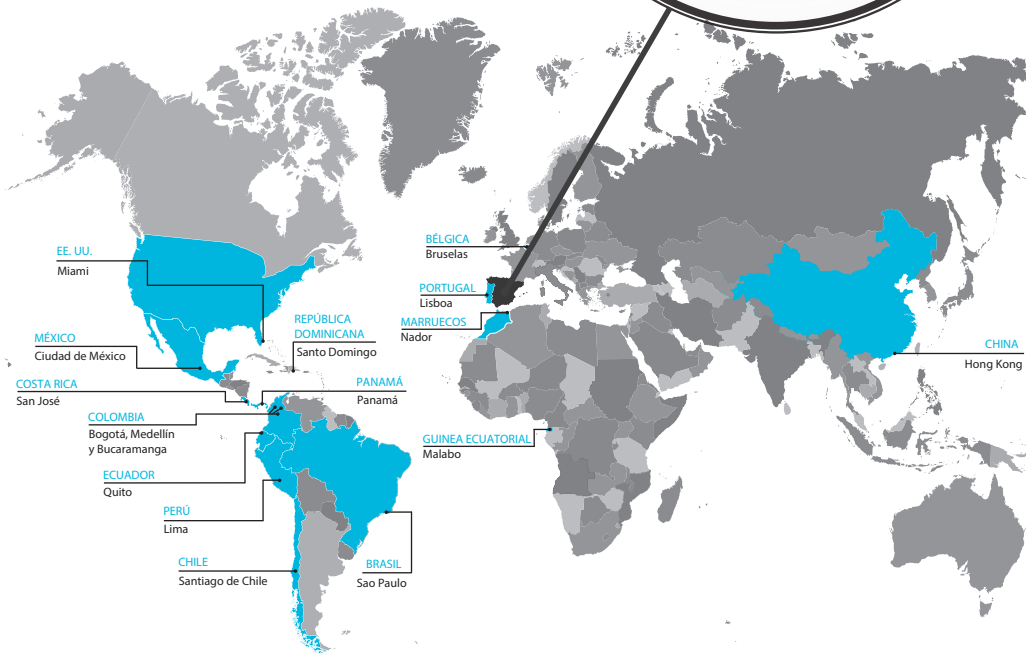
Los exámenes finales semestrales son presenciales y con carácter obligatorio. Este tipo de prueba de evaluación permite verificar el cumplimiento de los objetivos de aprendizaje previstos en cada asignatura.

Sedes de examen

/ *Dónde puedes examinarte*

— Sedes España —

- A Coruña
- Alicante
- Aranda de Duero (Burgos)
- Barcelona
- Bilbao
- Collado Villalba (Madrid)
- Córdoba
- Las Palmas de Gran Canaria
- Madrid
- Málaga
- Mérida (Badajoz)
- Oviedo
- Palma
- Santander
- Sevilla
- Tenerife
- Valencia
- Vigo
- Zaragoza



— Sedes extranjero —

- Bélgica (Bruselas)
- Brasil (Sao Paolo)
- Chile (Santiago de Chile)
- China (Hong Kong)
- Colombia (Bogotá, Medellín y Bucaramanga [sede no permanente])
- Costa Rica (San José)
- Ecuador (Quito)
- México (Ciudad de México)
- EE. UU. (Miami)
- Panamá (Panamá)
- Perú (Lima)
- Portugal (Lisboa [sede no permanente])
- República Dominicana (Santo Domingo)