
XV Jornadas de Ingeniería Telemática.
JITEL 2021.
Universidad de A Coruña.

Actas de las XV Jornadas de Ingeniería Telemática (JITEL 2021), A Coruña (España), 27-29 de octubre de 2021.

ISBN

Aplicación basada en Blockchain para la Emisión y Validación de Certificados Académicos

Joan Amengual Mesquida, M. Magdalena Payeras Capellà, Macià Mut Puigserver, Llorenç Huguet Rotger
Departament de Ciències Matemàtiques i Informàtica,
Universitat de les Illes Balears,
Carretera de Valldemossa, Km. 7,5 07122 Palma.
jamengual150899@gmail.com, mpayeras@uib.cat, macia.mut@uib.cat, l.huguet@uib.cat

En los últimos años las credenciales académicas se han considerado las acreditaciones que permiten validar los conocimientos de las personas y así se ha visto reflejado en el número de nuevos matriculados y egresados por las universidades que ha aumentado de manera exponencial. Esta tendencia en el sector académico ha generado muchas ventajas para nuestra sociedad. Sin embargo, el elevado valor de los certificados ha provocado la falsificación de estos. El objetivo de este proyecto es proporcionar un protocolo para la emisión y la validación de títulos universitarios, mediante el cual se resuelva el fraude de dichos títulos. El protocolo resultante se basa en el uso de la tecnología blockchain que proporciona una estructura de datos pública, descentralizada, abierta e inmutable.

***Palabras Clave*—Blockchain, smart contract, seguridad, privacidad, certificados académicos, aplicación.**

I. INTRODUCCIÓN

La acreditación de los estudios universitarios se realiza mediante títulos o certificados académicos. Los certificados académicos son muy apreciados porque sirven de indicador del capital humano de sus titulares [1]. El capital humano se refiere a las habilidades, competencias, conocimientos y aptitudes alcanzadas a través de la educación [2]. Los títulos académicos son especialmente importantes en situaciones de empleo, ya que sirven como garantía no solo de los conocimientos, la experiencia y las aptitudes de sus titulares, sino también de sus capacidades, su fiabilidad y su dedicación.

Como los certificados universitarios son tan valiosos, las personas falsean sus calificaciones académicas presentando certificados falsos. En Estados Unidos hay 2 millones de certificados de grado falsos en circulación y 300 universidades no autorizadas en funcionamiento [3]. Estados Unidos tiene el mayor número de instituciones académicas falsas en el mundo, seguido por el Reino Unido, que cuenta con unos 270 institutos falsos [4]. Chiyevo et al. explica en [5] que los títulos académicos se consideran auténticos cuando los confiere una universidad legalmente autorizada para otorgar dichos certificados.

En el sistema educativo actual es posible realizar acciones fraudulentas por parte de diferentes actores. En particular, estas acciones pueden ser realizadas por:

- Los profesores que son aquellos que evalúan el trabajo realizado por los estudiantes.
- El personal de administración de la universidad que realiza la comprobación de la finalización de los estudios y emite el correspondiente certificado académico.
- Los estudiantes que son los individuos que presentan el certificado emitido por la universidad al lugar de trabajo donde deseen acceder.

Entonces, este conjunto de actores puede realizar acciones fraudulentas con las que se declaran que un individuo tiene unos conocimientos de los que carece.

Normalmente, las universidades hacen entrega de los certificados académicos en formato físico, es decir, mediante un papel que certifica que el estudiante ha cursado satisfactoriamente unos estudios en dicha universidad y ha obtenido el título universitario de manera válida. Seguidamente, los estudiantes pueden presentar los certificados académicos en formato físico en su lugar de trabajo mediante el uso de copias compulsadas o mediante el certificado entregado por la misma universidad.

En cambio, hay universidades que entregan los títulos universitarios en formato digital. Los departamentos de recursos humanos tienen que confiar en las bases de datos

de las universidades donde se almacenan los datos de los certificados de los estudiantes. Estas bases de datos tradicionales no son a prueba de manipulaciones, son propensas a ser comprometidas o pueden ser modificadas por cualquier funcionario interno. Y no es posible que un empleador detecte la manipulación en la base de datos de la universidad. Por lo general, estas bases de datos tradicionales se encuentran en un servidor centralizado, no son transparentes y solo pueden acceder a ellas los administradores de la base de datos. No hay forma de rastrear o verificar los datos del certificado directamente en la base de datos de la universidad. Por lo tanto, los usuarios tienen que confiar ciegamente en el sistema de gestión de datos de estudio de la universidad para la legitimidad del certificado [6].

Para la resolución de esta problemática se puede hacer uso de la tecnología blockchain. Según un informe del servicio de ciencia y conocimiento de la Comisión Europea [7] blockchain es un área de creciente interés para muchas industrias y universidades a nivel mundial. Blockchain es una tecnología transversal, intersectorial y disruptiva que, según las previsiones, impulsará el crecimiento de la economía mundial durante las próximas décadas.

La tecnología blockchain ofrece características como el almacenamiento de datos decentralizado, transparente y a prueba de manipulaciones. Puede utilizarse para resolver problemas como la falta de confianza, el fraude, el alto coste de las transacciones, la compartición, la privacidad y la evaluación de la fiabilidad de un actor potencial en una transacción. Por lo tanto, blockchain es una tecnología prometedora para prevenir las actividades fraudulentas en nuestro actual sistema de certificados académicos [6].

La tecnología blockchain es ideal como nueva infraestructura para asegurar, compartir y verificar los logros del aprendizaje. En el caso de las certificaciones académicas, una cadena de bloques puede mantener una lista de emisores y receptores de cada certificado académico, junto con la firma del documento (*hash*) en una base de datos pública (la cadena de bloques) que se almacena de forma idéntica en miles de ordenadores.

Los certificados académicos digitales asegurados en una cadena de bloques tienen ventajas significativas sobre los certificados digitales ”tradicionales”:

- No pueden ser falsificados, ya que es posible verificar con certeza que el certificado fue originalmente emitido y recibido por las personas indicadas en el certificado.
- La verificación del certificado puede ser realizada por cualquier persona que tenga acceso a la cadena de bloques, con software de código abierto fácilmente disponible no hay necesidad de ninguna parte intermediaria.
- Al no ser necesaria ninguna parte intermediaria para validar el certificado, este puede seguir siendo validado incluso si la organización que lo emitió ya no existe o ya no tiene acceso al registro emitido.
- El registro de los certificados emitidos y recibidos en una cadena de bloques solo puede destruirse si se eliminan todas las copias en todos los ordenadores del mundo que albergan el software.

Actualmente existen varios sistemas que pretenden combatir la falsificación de certificados académicos, en particular se destacan los siguientes:

- Blockcerts [8]
- EduCTX [9]
- Blockchain for Education [10]

En la tabla I se comparan las características de cada uno de estos sistemas con sus ventajas e inconvenientes.

Cabe mencionar el proyecto español que pretende impulsar una prueba de concepto generando una red Blockchain, denominada Blue (BLockchain Universidades Españolas) para comenzar a desarrollar y desplegando servicios en ella. Como primer servicio desarrollado sobre esta nueva red se propone la emisión de certificados.

II. CONTRIBUCIÓN DEL PROYECTO

Las contribuciones y mejoras más destacables en las que contribuye el proyecto son las siguientes:

- Erradicar la inundación de títulos universitarios en el mercado laboral por las fábricas de certificados y así evitar que personas sin la titulación requerida lleguen a optar a trabajos mediante títulos universitarios falsificados teniendo ventaja sobre las personas que han cursado los estudios correctamente.
- Proporcionar un sistema de emisión de títulos por parte de entidades autorizadas con validación universal.
- Diseñar e implementar un protocolo donde participan todas las entidades involucradas en el proceso de emisión y validación de títulos universitarios mediante la tecnología blockchain.

III. PROTOCOLO DE EMISIÓN Y VALIDACIÓN DE TÍTULOS UNIVERSITARIOS

El protocolo para la emisión y la validación de títulos universitarios se ha dividido en tres bloques:

1) Validación de las universidades como autoridades certificadoras
2) Publicación de certificados académicos en la blockchain
3) Validación de certificados académicos

Algunos de los elementos que han posibilitado el desarrollo del protocolo han sido:

Tabla I
COMPARACIÓN ENTRE LOS SISTEMAS EXISTENTES BASADOS EN BLOCKCHAIN.

	Sistemas basados en blockchain		
	Blockcerts [8]	**EduCTX** [9]	**Blockchain for Education** [10]
Tipo de certificado o logro	Cualquier tipo de certificado académico y no académico	Obtención de créditos por logros académicos completados, como ECTS	Certificados de educación superior o instituciones acreditadas
Emisor del certificado	Cualquier tipo de instituto; académico y no académico; educación formal e informal	Instituciones de educación superior que siguen los estándares del ECTS y se han unido a la red	Instituciones acreditadas
Plataforma blockchain	Bitcoin, Ethereum	Ark	Ethereum
Uso de Smart Contract	No	No	Sí
Accesibilidad en la blockchain	Pública	Privada / Red de consenso	Pública
Protocolo de consenso	Proof of Work (PoW)	Delegated Proof of Stake (DPoS)	Proof of Work (PoW)
Uso de IPFS	No	No	Sí
Datos guardados en la blockchain	Hashes de los certificados (en un lote) Se almacena la raíz de Merkle	Tokens ECTX, identificación del curso, identificación del emisor (Instituto) y la identificación del receptor (estudiante)	Hash de los certificados, claves públicas de las autoridades de certificación, hash de la dirección IPFS de la información del perfil de las autoridades de certificación
Ventajas	- Estándar abierto - Cumplimiento de los criterios de auto-soberanía digital - Reducción del coste de transacción por certificado mediante el uso de árboles de Merkle	- Registra la información de cada curso, no solo del certificado final	- Solo las universidades acreditadas pueden emitir certificados - Revocación y renovación de los certificados - Los estudiantes pueden decidir aquello que pueden hacer los empleadores con sus certificados (leer o verificar)
Inconvenientes	- Vulnerable a los ataques de suplantación de identidad de emisores de los certificados	- El proceso no está totalmente automatizado y existe la posibilidad de cometer errores al transferir una cantidad incorrecta de tokens - El estudiante no puede seleccionar que registros compartir con el empleador	- Costes de las transacciones por cada certificado - Necesidad de verificar la autoridad de certificación previamente

- IPFS (InterPlanetary File System): Sistema de archivos distribuido.
- Smart Contract: Programa informático que facilita, asegura, hace cumplir y ejecuta acuerdos registrados entre dos o más partes.

Durante la explicación del protocolo se hará referencia a dos autoridades: autoridad de acreditación y autoridad certificadora.

- Autoridad de acreditación. Tiene como función validar a las universidades para que puedan convertirse en autoridades certificadoras y poder así publicar certificados académicos.
- Autoridad certificadora. Son aquellas universidades validadas por la autoridad de acreditación que disponen de los permisos para publicar certificados académicos en la cadena de bloques.

Estas son las autoridades principales del protocolo y forman una estructura jerárquica entre sí.

A. Validación de las universidades como autoridades certificadoras

La primera fase del protocolo consiste en validar a las universidades para que puedan convertirse en autoridades certificadoras, y de esta forma que dispongan de los permisos necesarios para publicar certificados académicos en la cadena de bloques.

En consecuencia, se debe definir una autoridad de acreditación. En este caso la autoridad de acreditación es un organismo regulador que permite decidir que universidades tienen derecho a publicar certificados. En este protocolo, se ha establecido como autoridad de acreditación al Ministerio de Universidades.

1) Alta de una universidad como autoridad certificadora: Cuando una universidad desee publicar certificados académicos a la cadena de bloques deberá comunicarlo al Ministerio. Seguidamente se va a iniciar un proceso de verificación de la universidad para decidir si puede convertirse en autoridad certificadora. Para acreditar a la universidad como autoridad certificadora en caso de haber sido verificada previamente, el Ministerio deberá realizar el siguiente procedimiento:

1) El Ministerio deberá disponer de la dirección o de las direcciones de la wallet de la universidad desde las que se van a publicar los certificados a la cadena de bloques. Esta dirección o direcciones deberán ser comunicadas entre la universidad y el Ministerio.

2) El Ministerio deberá identificar y almacenar las direcciones aportadas por las universidades en sus bases de datos. De esta manera, el Ministerio tendrá constancia en todo momento de cuales son las direcciones utilizadas por cada universidad para la

publicación de certificados.

3) Para dar de alta a una universidad como autoridad certificadora el Ministerio deberá introducir la dirección de la wallet de la universidad en un campo específico de la interficie de la aplicación.

   A continuación, se va a detallar el flujo de comunicación entre el Ministerio y el Smart Contract para validar una dirección de una universidad. Si la universidad desea aportar más direcciones desde las que publicar certificados el proceso deberá repetirse tantas veces como direcciones se deseen acreditar:
   - La dirección de la wallet de la universidad pasará a registrarse en la lista de las autoridades certificadoras del Smart Contract.
   - La dirección de la wallet de la universidad pasará a tener un estado válido a partir de este momento, el cual podrá cambiar si el Ministerio lo desea en cualquier momento, eliminando así su función de autoridad certificadora.

4) El Ministerio podrá notificar a la universidad que ya pertenece al conjunto de autoridades certificadoras. A partir de este momento, la universidad ya tendrá el derecho a publicar títulos universitarios en la cadena de bloques.

2) Baja de una universidad como autoridad certificadora: Es posible que después de un tiempo la universidad desee darse de baja como autoridad certificadora, y por tanto dejar de tener el derecho a publicar certificados a la cadena de bloques. Además, es posible que el Ministerio considere por alguna razón que dicha universidad no debe poder seguir publicando certificados. Por lo que se ha considerado la funcionalidad para dar de baja a una universidad como autoridad certificadora. Tal y como se puede visualizar en la Figura 1 el Ministerio deberá realizar el siguiente procedimiento:

1) El Ministerio deberá disponer de la dirección o de las direcciones utilizadas por la universidad para realizar la publicación de certificados.

2) El Ministerio deberá introducir la dirección de la wallet de la universidad en un campo específico de la web. A continuación, se va a detallar el flujo de comunicación entre el Ministerio y el Smart Contract, en caso de que la universidad disponga de varias direcciones deberá repetirse el proceso tantas veces como direcciones se deseen desacreditar:
   a) La dirección de la wallet de la universidad pasará a registrarse en la lista de las universidades dadas de baja del Smart Contract.
   b) La dirección de la wallet de la universidad pasará a tener un estado no válido a partir de este momento, es decir, la universidad no podrá publicar más certificados académicos a la cadena de bloques.

3) El Ministerio podrá notificar a la universidad que ya no pertenece al conjunto de autoridades certificadoras. Y por tanto, ya no se le permite publicar certificados a la cadena de bloques.

En la Figura 1 los recuadros identificados con (A) enmarcan la comunicación previa entre la universidad y el Ministerio en los procesos de dar de alta y de baja a las universidades, los recuadros identificados con (B) enmarcan la comunicación entre el Ministerio y el Smart Contract y los recuadros identificados con (C) enmarcan las notificaciones de los procesos de dar de alta y de baja del Ministerio a la universidad.

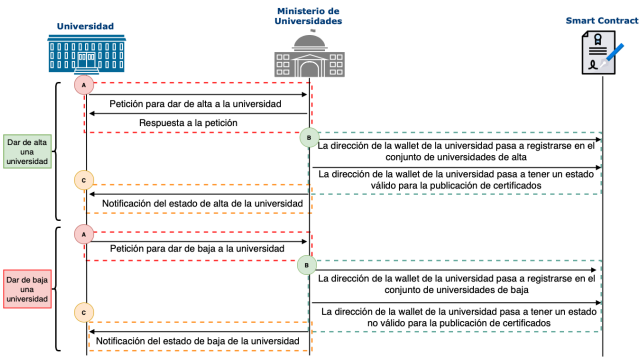

Fig. 1. Diagrama del proceso de dar de alta y de baja a universidades como autoridades certificadoras.

B. Publicación de certificados en la blockchain

Una vez la universidad se ha acreditado como autoridad certificadora tendrá el derecho a la publicación de certificados en la cadena de bloques. Este proceso se ha detallado mediante la Figura 2. En primer lugar, la universidad debe disponer de un conjunto de datos del estudiante necesarios para la identificación de este. La comunicación entre el estudiante y la universidad será realizada off-chain, es decir van a comunicarse por el canal de comunicación que ellos consideren adecuado.

En el diagrama de la Figura 2 se hace referencia a la petición de un código secreto como uno de los datos personales requeridos. Una de las desventajas del protocolo EduCTX recae en que el estudiante no puede seleccionar los registros a compartir con el empleador. Por tanto, mediante el valor del código secreto se pretende solucionar esta problemática.

Este campo va a ofrecer a los estudiantes la posibilidad de presentar los certificados de manera individual o en lotes. El estudiante podrá presentar un certificado aportando el código secreto con el que se enlazó en su publicación o podrá presentar un conjunto de certificados enlazados a un mismo código secreto.

El uso de este código secreto permite que este proyecto escale en un y permita publicar certificados de distintos ámbitos. Por ejemplo, certificados que acrediten un nivel de idiomas. El estudiante tendrá la posibilidad de enlazar certificados con diferentes códigos, y presentarlos de manera independiente o en lotes. La longitud del código secreto se ha establecido en un mínimo de 6 dígitos para incrementar la seguridad del proceso de validación.

Una vez la universidad disponga de los datos personales del estudiante requeridos, deberá publicar el PDF del certificado a la IPFS, y esto posibilitará visualizar el certificado en formato PDF una vez se requiera su validación. La IPFS va a proporcionar un hash del certificado con el que se podrá identificar de manera única al certificado. En este protocolo el hash proporcionado por IPFS se va a nombrar código IPFS.

En este protocolo los certificados requieren de la existencia de una referencia electrónica, similar al uso del CSV (Código Seguro de Verificación) usado por la Agencia Tributaria para identificar documentos electrónicos de forma única. Mediante la referencia electrónica se podrá identificar al certificado y se requerirá para la publicación del certificado a la cadena de bloques.

Cuando la universidad disponga de los datos del estudiante y del código IPFS CID (Content Identifier) del certificado académico ya podrá publicar el título a la cadena de bloques. Para su publicación la universidad deberá completar un conjunto de campos documentados en la Tabla II.

Tabla II
CONJUNTO DE LOS CAMPOS A COMPLETAR PARA LA PUBLICACIÓN DE UN CERTIFICADO ACADÉMICO A LA CADENA DE BLOQUES.

Campo	**Ejemplo**
Referencia electrónica del certificado	2IYRM-M2XL5-TDB6E-XCNCN-7HQXF-QFYMH
Código IPFS (CID) del certificado	Qmei1VwBQ9o7ADcjPFYovJbWbq8yQeoWosuTn5kLnHMJRJ
Identificación del estudiante (NIF/NIE)	12345678X
Código secreto (mínimo de 6 digitos)	123456

Finalmente, la universidad podrá publicar el certificado académico a la cadena de bloques, y el Smart Contract realizará el siguiente procedimiento:

1) La referencia electrónica del certificado se va a enlazar con el código IPFS (CID) y con el hash de la identificación del estudiante (NIF/NIE). Así en el proceso de validación se podrá validar un certificado mediante su referencia electrónica y además visualizar su contenido en IPFS.

2) Se va a realizar el hash de la identificación del estudiante y del código secreto del estudiante de manera conjunta, y se va a enlazar este hash con el código IPFS (CID).
Es necesario destacar que el código IPFS no se va a cifrar, por tanto, será visible por cualquier usuario y en consecuencia, cualquier persona podrá visualizar los datos de los certificados. No obstante, no se consideran datos sensibles aquellos datos que se encuentran en un certificado académico y es preferible eliminar la carga del cifrado.
Este enlace entre el hash de la identificación del estudiante y el código secreto con el código IPFS de su título será necesario para poder visualizar el conjunto de certificados de los que dispone un estudiante ligados a un mismo código secreto.
Un usuario podrá visualizar el PDF de los certificados académicos en IPFS que se encuentren ligados a una identificación (NIF/NIE) y a un código secreto.

3) Finalmente, se va a almacenar el número de certificados publicados por cada universidad. Así, se podrá analizar el uso que se está dando al servicio por cada universidad.

En la Figura 2 el recuadro identificado con (A) enmarca la comunicación entre el estudiante y la universidad, el recuadro identificado con (B) enmarca la comuicación entre la universidad y la IPFS y el recuadro identificado con (C) enmarca la comunicación entre la universidad y el Smart Contract.

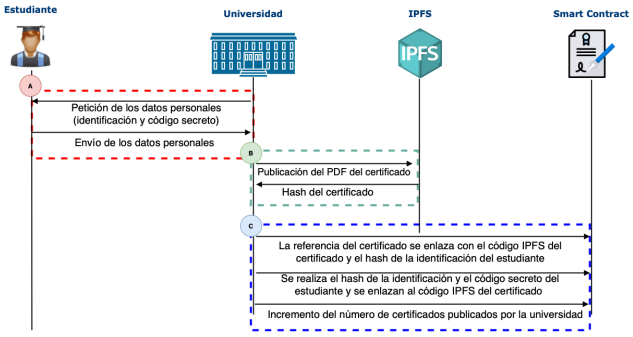

Fig. 2. Diagrama del proceso de publicación de certificados en la cadena de bloques por una universidad.

C. Validación de certificados

La validación de certificados es la última fase del protocolo. En este apartado, se va a detallar su proceso mediante la Figura 3, donde se describen las comunicaciones entre los actores implicados.

En primer lugar, cabe destacar que cualquier usuario tendrá la posibilidad de validar certificados académicos. En particular, se va a centrar el punto de interés de la validación de los certificados a los empleadores. La validación de los certificados se puede realizar de distintas formas:

- Validación mediante la referencia electrónica del certificado. Consiste en validar un certificado de manera independiente, es decir, el proceso de validación únicamente se enfoca en validar un certificado.
- Validación mediante el código secreto. Posibilita la validación de un conjunto de certificados en un mismo proceso de validación.

1) Validación mediante la referencia electrónica del certificado: El desarrollo para realizar la validación mediante la referencia electrónica va a permitir validar y visualizar un único certificado académico. El proceso a efectuar es el siguiente:

1) El empleador debe disponer de dos parámetros: la referencia electrónica del certificado y la identificación del estudiante (NIF/NIE). En vista de ello, el estudiante deberá aportar la información previamente para efectuar la validación del certificado.

2) Cuando el empleador introduzca los datos necesarios (referencia electrónica del certificado y la identificación del estudiante) el Smart Contract va a relacionar la referencia del certificado académico y la identificación del estudiante (NIF/ NIE) con el código IPFS (CID) del certificado. De esta manera, se podrá mostrar el código IPFS que identifica el PDF del certificado en IPFS.

3) Finalmente, el empleador dispondrá del código IPFS (CID) del certificado y podrá proceder a visualizar su contenido mediante el uso de IPFS.

Con este procedimiento el empleador puede validar un certificado académico y además visualizar su contenido con el uso de IPFS.

2) Validación mediante el código secreto: El desarrollo para realizar la validación mediante el código secreto va a permitir validar y visualizar varios certificados en un mismo proceso. Este procedimiento se ha detallado en la Figura 3. El proceso a efectuar es el siguiente:

1) El empleador debe disponer de dos parámetros: la identificación del estudiante (NIF/NIE) y el código secreto enlazado al conjunto de certificados que se deseen validar. Por tanto, el estudiante deberá aportar dicha información previamente para realizar la validación de los certificados.

2) Cuando el empleador introduzca los datos necesarios (identificación del estudiante y código secreto) el Smart Contract podrá relacionar la identificación del estudiante y el código secreto con los códigos IPFS de los certificados. Por tanto, se podrán mostrar los códigos IPFS que identifican al PDF de cada uno de los certificados en IPFS.

3) Finalmente, el empleador dispondrá de los códigos IPFS de los certificados y podrá proceder a visualizar su contenido mediante IPFS.

Con este procedimiento el empleador puede validar un certificado académico o un conjunto de estos. Además podrá visualizar su contenido con el uso de IPFS.

En la Figura 3 los recuadros identificados con (A) enmarcan la comunicación entre el empleador y la Smart Contract y los recuadros identificados con (B) enmarcan la comunicación entre el empleador y la IPFS.

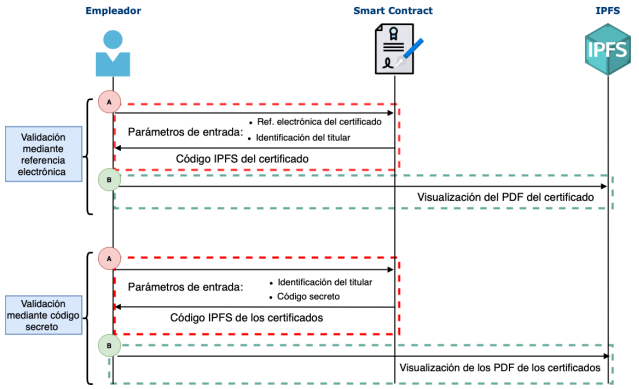

Fig. 3. Diagrama del proceso de validación de certificados mediante la referencia electrónica y mediante el código secreto

IV. ANÁLISIS DE PROPIEDADES

A. Análisis del protocolo

Los tipos de certificados o logros que contempla el protocolo desarrollado son puramente certificados académicos, específicamente títulos universitarios. Este protocolo se asemeja al protocolo Blockchain for Education, donde el punto de mira se centra en certificados de educación superior o de instituciones acreditadas.

Un punto que se ha considerado desde el primer momento en el desarrollo del protocolo ha sido el emisor del certificado académico y la validez de este. En sistemas como Blockcerts cualquier institución puede emitir certificados, esta es una característica del sistema que puede resultar positiva, ya que permite tener un amplio abanico de aplicaciones. No obstante, esta misma característica resulta ser negativa en el momento que se consideran certificados altamente valiosos como es el caso de los títulos universitarios. Así que en estos certificados es relevante destacar cuál ha sido el emisor para poder validar completamente el certificado académico. Por ello, en el protocolo desarrollado se ha definido una autoridad reguladora encargada de validar que instituciones tienen la potestad de publicar los certificados académicos sobre la cadena de bloques. Únicamente las universidades que se validen por esta autoridad reguladora serán las permitidas para la publicación de certificados académicos

en la cadena de bloques.

La plataforma blockchain elegida para la implementación del proyecto ha sido Ethereum. Los principales motivos de esta elección han sido los siguientes:

- Ethereum ha creado una plataforma de acceso global en la que se pueden ejecutar complejos contratos en red. Elimina totalmente la necesidad de que existan servicios proporcionados por terceros para su funcionamiento.
- Ethereum sirve de plataforma para otros productos o servicios, eso permite que se cree un ecosistema robusto que hace cada vez más fuerte a la plataforma. A medida que avancemos en el tiempo, cada vez habrá mejor información sobre Ethereum.
- Más allá de los fundadores de Ethereum, existen muchas compañías involucradas en su estudio y desarrollo, como Ethereum Enterprise Alliance o el equipo de Hyperledger. Después de Bitcoin es la blockchain con mayor apoyo de la comunidad empresarial.

Un aspecto a considerar en este proyecto ha sido el desarrollo de un Smart Contract que permita regular todas las operaciones a realizar. A diferencia de los protocolos Blockcerts y EduCTX donde no se usa ningún Smart Contract para su funcionamiento. Además, se ha tenido mucha consideración en los datos a almacenar en la cadena de bloques debido a que la publicación de información en la cadena de bloques tiene un coste.

En el sistema implementado se ha hecho uso de IPFS como herramienta de visualización de los certificados. De la misma manera que Blockchain for Education lo usa para disponer de información de las autoridades de certificación. En los otros sistemas, Blockcerts y EduCTX, no se hace uso de IPFS.

La información que almacena el sistema Blockcerts es la raíz de Merkle que permite la validación de un lote de certificados. EduCTX almacena Tokens ECTX y otros datos relevantes para la validación de los certificados y Blockchain for Education almacena el hash de los certificados, claves públicas de las autoridades de certificación y otros datos. En el protocolo desarrollado se ha decidido almacenar las identificaciones de los certificados como sus referencias electrónicas y sus códigos IPFS enlazados a los *hashes* de las identificaciones de los titulados.

En la tabla III se destacan las características del protocolo desarrollado.

Tabla III
CARACTERÍSTICAS DESTACADAS DEL PROTOCOLO IMPLEMENTADO EN ESTE PROYECTO.

	Protocolo diseñado
Tipo de certificado o logro	Títulos universitarios, no obstante, puede considerarse su uso para cualquier certificado académico
Emisor del certificado	Universidades acreditadas por una autoridad reguladora
Plataforma blockchain	Ethereum
Uso de Smart Contract	Sí
Accesibilidad en la blockchain	Pública
Protocolo de consenso	Proof of Work (PoW)
Uso de IPFS	Sí
Datos guardados en la blockchain	Hash de las referencias electrónicas de los certificados y códigos IPFS de los certificados enlazados a las identificaciones de los titulados

V. ANÁLISIS DE RENDIMIENTO

Uno de los factores claves a la hora de desarrollar tecnologías basadas en blockchain es el análisis de rendimiento debido a que en estas tecnologías el código no es ejecutado sobre la máquina local, sino sobre una red P2P distribuida. Esto significa que el coste computacional de ejecución de un contrato se traduce en un coste económico determinado y un cierto tiempo de espera. A continuación se valorarán estos dos parámetros en la implementación que se ha realizado del protocolo.

Es importante establecer en primer lugar, que estos parámetros se han estudiado de acuerdo a las pruebas establecidas sobre la red Rinkeby. Esta red no es más que una red privada de prueba para Ethereum, dedicada específicamente para desarrolladores. Es por ello que los resultados obtenidos en esta sección, especialmente los resultados temporales, deben considerarse orientativos y servir únicamente para establecer referencias.

A. Tiempo de espera

En primer lugar se evaluará el tiempo promedio que tarda en computarse cada una de las distintas funcionalidades del protocolo. Como ya se ha expuesto anteriormente, esto se realizará en la red de pruebas Rinkeby. Esta red tarda en promedio 15 segundos en publicar un nuevo bloque.

El tiempo de espera se ha calculado como la diferencia entre el tiempo de publicación del bloque correspondiente y la entrada de la transacción en la red *P2P*. Para ello se ha hecho uso de la herramienta etherscan. Adicionalmente, cada acción se ha realizado un total de 10 veces con el objetivo de proporcionar la media aritmética de estos resultados.

Tabla IV
TIEMPOS MEDIOS DE EJECUCIÓN DEL PROTOCOLO.

Función	**Tiempo (segundos)**
Creación del Smart Contract	2,3
Alta de una universidad	5,5
Baja de una universidad	5,7
Publicación de certificados	6,5

Tal y como se puede apreciar en la Tabla IV, los resultados temporales son prácticamente idénticos, puesto que el factor que determina el tiempo de espera es común a todas las funciones. Esto se debe a que las funciones que han sido medidas necesitan la publicación de un nuevo bloque para realizarse. Esto significa que el tiempo mostrado en la tabla se ve afectado por el intervalo de publicación de bloques sumado al tiempo de aceptación de la transacción, el cual va variando en función del tráfico de la red *P2P* y el precio de la transacción. Por lo tanto, no es posible medir con exactitud el tiempo de ejecución de cada uno de los métodos, ya que ninguno requiere un tiempo de ejecución tan elevado como para no encontrarse totalmente influenciado por los tiempos de aceptación y publicación.

B. Costes de Ejecución

Este apartado pretende determinar el coste de gas para cada una de las funciones del Smart Contract.

Tabla V
COSTES DE EJECUCIÓN DE LAS FUNCIONES DEL SMART CONTRACT.

Función	**Gas (weis)**	**USD (1Gwei)**	**USD (20Gwei)**
Creación del Smart Contract	1.367.823	2,49	49,77
Alta de una universidad	130.179	0,24	4,74
Baja de una universidad	107.712	0,20	3,92
Publicación de certificados	359.577	0,65	13,08

Las medidas mostradas en la Tabla V corresponden a los costes fijos de gas de cada uno de los métodos del contrato. Adicionalmente, se ha añadido a modo orientativo el precio en dólares americanos de cada una de las funcionalidades teniendo en cuenta el valor al cambio entre monedas a 18 de marzo de 2021. Es importante mencionar que estos costes se han realizado teniendo en cuenta un precio de 1 Gwei y 20 Gwei (valor máximo). La principal diferencia, además del coste total de la transacción, es el tiempo que tardará la transacción en ser aceptada por un nodo minero. Por tanto, como mayor sea el precio que se pague por una misma transacción, menor será el tiempo de aceptación de la transacción. No obstante, para la publicación de títulos universitarios la velocidad en la publicación de estos no es un factor relevante y por ello se puede tener un coste mucho menor.

Las funciones de dar de alta y dar de baja a una universidad como autoridad certificadora tienen un precio muy similar debido a que la estructura del código es prácticamente idéntica. Se puede considerar un precio realmente bajo dar de alta y de baja a una universidad por un precio de alrededor 0,20 dólares. Este gasto podría ser asumido por la autoridad de acreditación.

En la publicación de certificados a la cadena de bloques el precio aumenta frente a los dos anteriores funciones, esto se debe a que en la publicación de certificados se realizan un conjunto de cálculos que provocan un aumento considerable del gas de ejecución. No obstante, podemos considerar este precio realmente bajo frente a las ventajas de tener el certificado publicado en la cadena de bloques y considerando las altas tasas actuales para la expedición de los títulos académicos. Este gasto podría ser asumido por la autoridad certificadora o por el titulado.

VI. CONCLUSIONES

Actualmente, las empresas carecen de herramientas para validar los certificados académicos que se les presentan. Esto ha posibilitado que las fábricas de diplomas inunden de certificados falsos el mundo laboral.

Recientemente, a través del desarrollo de nuevas tecnologías como blockchain se han abierto nuevas posibilidades para la resolución de estos problemas, permitiendo que las empresas tengan a su disposición herramientas para validar los certificados académicos presentados de manera rápida y fiable.

En este documento se ha presentado un protocolo para la emisión y validación de títulos universitarios con blockchain. En este protocolo se ha dado mucha importancia al proceso de emisión de los certificados, evitando así que cualquier institución sin acreditación sea capaz de emitir certificados académicos. También, se ha desarrollado un proceso de validación adecuado a cualquier persona independientemente de sus conocimientos sobre la tecnología blockchain.

AGRADECIMIENTOS

El proyecto FeltiCHAIN (RTI2018-097763-B-I00) está financiado por: FEDER/Ministerio de Ciencia e Innovación – Agencia Estatal de Investigación, (MCI/AEI/FEDER, UE).

REFERENCIAS

[1] O. Ghazali and O. Saleh, "A Graduation Certificate Verification Model via Utilization of the Blockchain Technology", 2018.
[2] O. Saleh, O. Ghazali and M. E. Rana, "Blockchain based framework for educational certificates verification", vol. 7, 2020.
[3] Grolleau, Gilles, Lakhal, and Mzoughi, "An Introduction to the Economics of Fake Degrees", Journal of Economic Issues, vol. 42, pp. 673-693, 2018.
[4] E. Ben and R. Winch, "Diploma and Accreditation Mills: New Trends in Credential Abuse", 2011, [Online]. Available: https://www.esrcheck.com/file/Verifile-Accredibase_Diploma-Mills.pdf.
[5] Evelyn Garwe, "Qualification, Award and Recognition Fraud in Higher Education in Zimbabwe",vol. 5, pp. 119-135, Critical Studies in Education, 2015.
[6] Rakibul Hasan, "Potencial of Blockchain technology to solve fake diploma problem", 2019.
[7] G. Alex and C. Anthony, "Blockchain in Education", 2017.
[8] David García, "Diseño de una lógica de negocio en blockchain. Desarrollo y despliegue de Smart Contracts en una Blockchain", pp 15-15, 2020.
[9] M. Turkanović, M. Hölbl, K. Košič, M. Heričko and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform", vol. 6, pp. 5112-5127, 2018.
[10] W. Gräther, S. Kolvenbach, R. Ruland, J. Schütte , C. Torres and F. Wendland, "Blockchain for Education: Lifelong Learning Passport", 2018.