Propuesta del uso de la tecnología la cadena de bloques en los procesos de acreditación de programas educativos

Proposal for the use of blockchain technology in the accreditation processes of educational programs

Erika Meneses Rico[1], Carlos Alberto Ochoa-Rivera[1], Jesús Roberto Méndez-Ortiz[1]
[1] Facultad de Estadística e Informática, Av. Xalapa s/n, 91010, Xalapa-Veracruz, México.
[1]{ ermeneses, cochoa, jmendez}@uv.mx

Fecha de recepción: 29 de julio de 2022
Fecha de aceptación: 26 de agosto de 2022

Resumen. La acreditación de un programa educativo a nivel superior permite garantizar la calidad del mismo y aunque es voluntaria, la obtención del reconocimiento trae múltiples beneficios a la institución que la obtiene. El proceso de evaluación con fines de acreditación se encuentra gestionado por un sistema de información en línea que permite a todas las partes interesadas realizar desde la fase de solicitud hasta el dictamen y la mejora continua. Como apoyo a dicho sistema y para finalizar el proceso de acreditación, se propone que a través del uso de la tecnología la cadena de bloques, se expidan certificados electrónicos mediante los cuáles se garantice la autenticidad e inmutabilidad de dichos documentos. Este artículo presenta una descripción de la tecnología de la cadena de bloques y una propuesta para su implementación en la generación de certificados digitales que validen la acreditación de programas educativos de nivel superior. La metodología empleada para la elaboración de esta investigación es Investigación Acción y el resultado esperado es la mejora del proceso de acreditación de programas educativos mediante la implementación paulatina de la tecnología de la cadena de bloques.

Palabras Clave: cadena de bloques, acreditación, mejora continua, programas educativos, actualización.

Summary. The accreditation of an educational program at a higher level allows guaranteeing its quality and although it is voluntary, obtaining recognition brings multiple benefits to the institution that obtains it. The evaluation process for accreditation purposes is managed by an online information system that allows all interested parties to carry out from the application phase to the opinion and continuous improvement. Thus, in support of said system and to finalize the accreditation process, it is proposed that through the use of blockchain technology, electronic certificates be issued through which the authenticity and immutability of said documents are guaranteed. This article presents a description of blockchain technology and a proposal for its implementation in the generation of digital certificates that validate the accreditation of higher-level educational programs. The methodology used in this research is Action Research, and the expected result is the improvement of the accreditation process of educational programs through the gradual implementation of block chain technology.

Keywords: blockchain, accreditation, continuous improvement, educational programs, updating.

1 Introducción

La cadena de bloques o blockchain es una tecnología revolucionaria que garantiza la inmutabilidad y la autenticidad de la información que contiene.

Según (Christensson, 2021), la cadena de bloques es un registro digital de transacciones, el nombre proviene de su estructura, en el que cada registro, llamados bloques, están enlazados en una lista llamada cadena.

Las transacciones forman parte de nuestra vida diaria, tanto en términos comerciales en los que se lleva a cabo un convenio de compra venta de persona a persona, como en el intercambio de otro tipo de servicios, por ejemplo entre una persona y una máquina, cuando compramos un café en una máquina dispensadora.

Asimismo, las transacciones no solo se limitan al intercambio de dinero o intercambio de servicios, podemos hablar de una transacción cuando se intercambia información y este es el caso de muchas operaciones informáticas llevadas a cabo a través de Internet.

Desde el surgimiento de la red de redes, la seguridad en la gestión de información ha sido un tema de gran preocupación, siendo Phil Zimmerman el primero en desarrollar en 1991 el programa de encriptación PGP (Pretty Good Privacy, privacidad bastante buena), con el fin de proteger la información transmitida a través de Internet mediante el uso de criptografía de clave pública.

"Hasta el día de hoy, los profesionales de la informática tienen la tarea de garantizar tres principios de seguridad de la información: la integridad, la confidencialidad y la disponibilidad." (Dussan, 2006).

La integridad, permite garantizar que la información no sea alterada en su contenido, por tanto, es íntegra.

La confidencialidad, tiene como propósito asegurar que sólo la persona correcta acceda a la información que se desea distribuir.

Y disponibilidad, cuyo objetivo es garantizar que la información llegue en el momento oportuno.

La cadena de bloques es una tecnología que dificulta la modificación de datos gracias a su estructura conectada, pues los bloques dentro de una cadena son dependientes de la información incluida en los bloques predecesores, por lo tanto, es imposible alterar un bloque ya existente en la cadena; aunado a ello, el sistema de consenso que implementa dicta que múltiples participantes verifiquen las transacciones incrementando nivel de seguridad. Por último, se trata de una base de datos descentralizada, en la que los nodos contienen una copia de la cadena completa.

Implementando así los tres principios de seguridad de la información. Esta garantía hizo que la cadena de bloque se convirtiera en la tecnología idónea para la creación de criptomonedas, activo digital que ha cambiado el paradigma del intercambio de dinero; la cadena de bloques "aporta un elevado sistema de seguridad con capacidad para evitar, por ejemplo, que un mismo activo digital se pueda transferir en dos ocasiones o que sea falsificado. "Blockchain funciona como un gran libro de contabilidad donde se pueden registrar y almacenar cantidades ingentes de información. Está compartida en la red y protegida de tal forma que todos los datos que alberga no se pueden alterar ni eliminar." (Santander, 2022)

Gracias a estas características, la cadena de bloques está siendo utilizada en otros campos además de ser la base de las criptomonedas, tales como la salud, los bienes raíces, gobierno, educación, etc.Comprobar las normas de edición del artículo.

2 Marco Teórico

Camilo Gutiérrez, jefe del Laboratorio de Eset Latinoamerica, explica los orígenes y el funcionamiento de la cadena de bloques, donde menciona que fue en 1991 cuando Stuart Haber y W. Scott Stornetta iniciaron el proyecto de una cadena de bloques asegurados criptográficamente. Tecnología que alcanzó gran popularidad en el año 2008 con su implementación en la criptomoneda bitcoin.

Bitcoin ha tenido tal aceptación que para este año se proyecta un crecimiento anual de los 51% para varios mercados.

2.1 Definición de Blockchain

Blockchain o cadena de bloques es una tecnología para construir una especie de libro mayor, distribuido en una red con varios participantes (llamados nodos) que pueden agregar transacciones de manera segura, confiable y transparente.

Las principales características de Blockchain son las siguientes:

El libro mayor o registro de datos único se encuentra en una base de datos distribuida, en la que cada participante puede agregar datos (transacciones), solo si se cumple con ciertas condiciones y es aprobado por todos los nodos.

De la misma forma, las transacciones no pueden ser modificados o eliminados sin el consenso de todos los nodos de la red, por lo que estas se mantienen en orden cronológico. En caso de que se requiera modificar o eliminar una transacción; se deberá insertar otra que tenga el efecto deseado, sin embargo, los datos originales se mantendrán en la cadena, lo que mantiene la transparencia y confiabilidad en la información.

Las transacciones se almacenan en forma de bloques dentro de una cadena, los cuales dependen del bloque anterior para garantizar su autenticidad.

2.2 Componentes de Blockchain

La arquitectura de la cadena de bloques está constituida por los siguientes elementos:

Registro de datos único

Es la base de datos replicada en cada uno de los nodos participantes en la red de la cadena de bloques, se rige por reglas estrictas respecto a qué miembro de la red puede editar el registro y cómo puede hacerlo. Está conformada por las transacciones que cada miembro de la red realiza y se almacenan dentro de bloques de una cadena, así, hasta que la transacción es validada formará parte del bloque y será sincronizado para formar parte de la base de datos de cada nodo.

Criptografía de clave pública

Empleada para validar la autenticidad de los miembros de la red en una transacción. Con este mecanismo de seguridad se genera una clave pública y una clave privada para cada miembro de la red. Ambas se emplean de manera conjunta para desbloquear los datos del registro único que se encuentran criptografiados bajo un algoritmo Hash.

Contratos inteligentes

Una de las ventajas que ofrece Blockchain es la gestión de transacciones transparente y sin intermediarios, y parte de esto funciona gracias a los contratos inteligentes, que son programas almacenados en la cadena de bloques y determinan las reglas bajo las cuales se pueden llevar a cabo las transacciones.

En la plataforma de Ethereum por ejemplo, los contratos inteligentes son programados en el lenguaje denominado "Solidity". En la plataforma de Hyperledger Fabric con Go, Java, Node.js.

Algoritmo de consenso

Los algoritmos de consenso son utilizados por la cadena de bloques para asegurar que una transacción se valide de manera conjunta por todos los participantes de la red y que procede de una fuente confiable.

Es decir, los algoritmos de consenso "son aplicados para mantener los protocolos de cómo se agregan y mantienen los bloques" (Waldman, 2018). Existen distintos tipos de algoritmos de consenso, a continuación se describen dos de manera muy sencilla:

Proof of Work (PoW). Este algoritmo se emplea en redes de cadena de bloques públicas, en las que cada participante o nodo que desee introducir un nuevo bloque debe comprobar que es confiable y honesto en la operación.

Consiste en lo siguiente:

El nodo participante e interesado en agregar un nuevo bloque a la blockchain debe resolver un problema complejo computacionalmente hablando y para ello requerirá poner a prueba la capacidad del hardware con el que trabaja, de esta manera, el participante debe invertir tiempo y energía eléctrica (consumida por el hardware). Si logra descifrar el enigma, tendrá a cambio su recompensa.

De esta forma se evita que nodos deshonestos participen, pues supone la inversión de tiempo y energía, que probablemente no de resultados.

Una vez que el participante ha resuelto el problema, cada nodo de la red valida que se ha logrado la solución correcta, sometiendo los datos generados a una función hash, si la respuesta es correcta, el bloque es insertado en la copia de blockchain de cada nodo.

"Idealmente, debería resultar costoso producir bloques, pero barato para cualquiera validarlos." (Binance Academy, 2020)

Este algoritmo es el que se emplea en Bitcoin y otras criptomonedas, por lo que la recompensa generalmente es este activo.

Proof of Authority (PoA). Este algoritmo es empleado en redes de cadena de bloques privadas o de consorcio.

Proof of Authority está basado en una confianza predefinida que existe entre todos los miembros de la red, en la cual se define un grupo de nodos validadores que definen las reglas para agregar un nuevo nodo a la blockchain. Esto da como resultado que la red no se encuentre completamente descentralizada, pero aumenta la velocidad de la cantidad de bloques que pueden insertarse en la cadena.

En una red de cadena de bloques privada, puede perder el sentido la competencia en la que cada participante debe invertir tiempo y energía para obtener criptomonedas u otro tipo de recompensas, por lo que, en PoA, los nodos invierten o ponen en riesgo su renombre.

El éxito de Proof of Authority depende de la selección del nodo o nodos definidos como entidades validadoras y requiere que este proceso de designación tenga las siguientes características:

- Las reglas de selección deben ser las mismas para todos los participantes.
- Los nodos elegidos como validadores deben estar dispuestos a confirmar su identidad real, y saber que si actúan de manera deshonesta, su reputación quedará comprometida.
- El proceso para convertirse en un nodo con autoridad debe ser tal que garantice el compromiso a largo plazo dentro de la cadena de bloques.

Se mencionó anteriormente la confianza predefinida que debe existir entre los miembros de una blockchain que trabajan bajo el algoritmo PoA; esta confianza es empleada en la inserción de nuevos bloques a la cadena, pues cada nodo validador tendrá una clave privada y una clave pública conocida por el resto de los miembros de la red; cuando un nodo autoridad inserta un nuevo bloque en la cadena, basta con verificar la firma del remitente para replicar el nuevo bloque en la copia de la blockchain de todos los nodos, lo que acelera en gran magnitud el registro de nuevos bloques, en comparación con PoW.

2.3 Funcionamiento de Blockchain

Amazon Web Services (2022) menciona de manera muy clara los pasos llevados a cabo en el funcionamiento de una cadena de bloques:

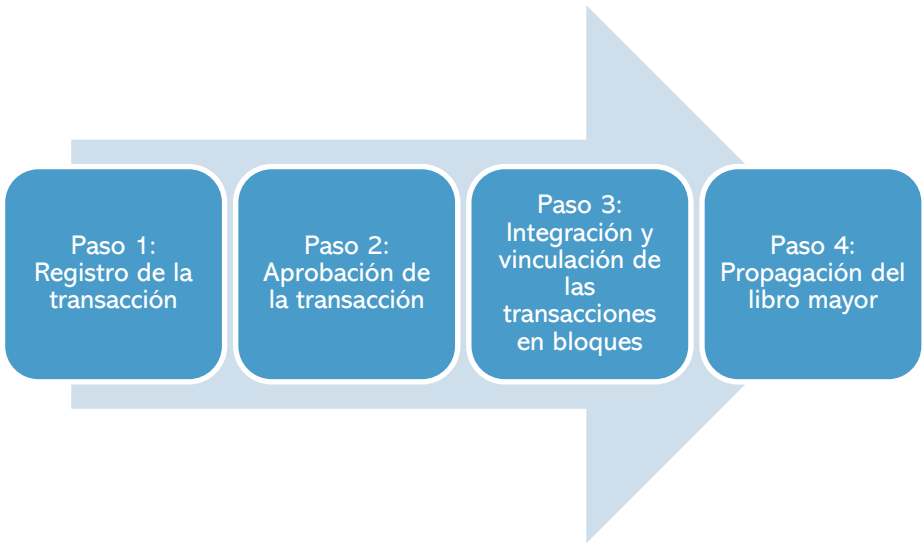

Fig. 2. Pasos llevados a cabo en el funcionamiento de una cadena de bloques.

A continuación se explican cada uno de estos pasos:

1. Registro de la transacción.

Como ya se había mencionado anteriormente, las transacciones se registran en una base de datos única o libro mayor, con una copia idéntica en cada uno de los nodos de la red; estas transacciones se almacenan en forma de bloques y realizan cierta modificación a la información que se está gestionando, los datos que se registran en la transacción pueden ser:
a. Quién la realizó.
b. Qué tipo de movimiento se generó.
c. Cuándo y dónde se llevó a cabo.
d. Cuál fue el resultado de la transacción.
e. Entre otros.

Es importante recordar que solo se pueden añadir nuevas transacciones y si se requiere eliminar o modificar la información gestionada en bloques previos, se requiere insertar un nuevo bloque con la transacción que tenga el efecto deseado, pero los datos originales prevalecen en los bloques anteriores, es decir, el histórico de la cadena.

2. Aprobación de la transacción

La aprobación de la transacción se lleva a cabo a través de un algoritmo de consenso, ya sea como alguno de los abordados previamente, Proof of Work, Proof of Authority o algún otro como Proof of Steak. Las reglas que rigen la implementación de estos algoritmos son dadas por el tipo de red y el activo que sea gestionado mediante las transacciones, ya sea físico o digital.

3. Integración y vinculación de las transacciones en bloques

Se mencionó previamente que los datos del registro único se encuentran criptografiados bajo un algoritmo Hash. Esto es lo que le da a la cadena de bloques una de sus grandes ventajas, la seguridad de la información.

Una vez que la transacción es aprobada, se crea un nuevo bloque que contiene, además de la propia información de la transacción descrita en el paso 1 del proceso, una función hash criptográfica; de tal manera que si el contenido de la transacción cambia, el valor de la función hash también.

Esta función es copiada al siguiente bloque que se añade a la cadena, reforzando la integridad de la información de su antecesor.

Así sucede a lo largo de toda la cadena, la cual queda constituida por bloques agrupados de manera secuencias y fuertemente vinculados entre sí.

Esto se muestra en la siguiente ilustración:

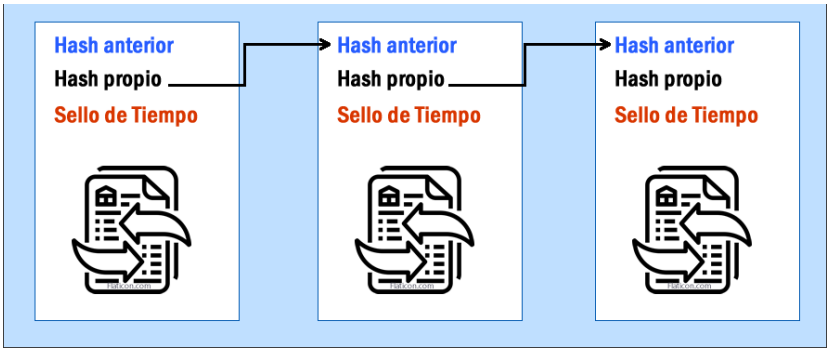

Fig. 2. Integración y vinculación de las transacciones en bloques en Blockchain

4. Propagación del libro mayor

Por último, una vez que el nodo ha sido insertado y vinculado al nodo previo, la "nueva versión" de la blockchain es distribuida a todos los nodos que forman parte de la red. Este último paso es sumamente importante; pues de otorga otra de las ventajas de la cadena de bloques, que es la disponibilidad

2.4 Tipos de Blockchain

Ya se habló anteriormente de los algoritmos de consenso y los tipos de cadena de bloques en los que se emplean, a continuación, se explica un poco más de cada una de ellas:

- Cadena de bloques públicas. Son redes en las que cualquier persona puede participar con los mismos derechos para insertar y validar bloques y su identidad permanece anónima.
- Cadena de bloques privadas. Son redes en las que existen políticas y reglas para unirse a ellas, no todos los participantes tienen el mismo derecho para los procesos de inserción y validación de nodos, de hecho, solo un grupo de ellos determina las normas para unirse a la red y los derechos que cada nodo tiene.
- Cadena de bloques híbridas. Son una combinación de las dos anteriores.

Las principales implementaciones de Blockchain son el Bitcoin que es el "padre" de Blockchain, así como Ether que es la criptomoneda de Ethereum, plataforma de código abierto para desarrollar aplicaciones dentro de blockchain, a quien se le reconoce por el desarrollo de los contratos inteligentes.

2.5 Usos de Blockchain

Actualmente la cadena de bloques se está empleando en áreas de diferente índole, pues cualquier institución u organización que requiera mantener un registro único intacto de información en el tiempo, protegido contra

accesos no autorizados y manteniendo la autenticidad en las operaciones, puede obtener estas características mediante el empleo de Blockchain.
Así, algunos ejemplos son:

- *Bienes raíces*. Donde se mantiene un registro inalterable de las operaciones de compra-venta de inmuebles, todos los participantes se rigen mediante las mismas reglas para llevar a cabo el proceso y las fases, desde la entrega y validación de documentación hasta el pago, se mantienen transparentes.
- *Salud*. Los registros de pacientes se mantienen en un historial en la cadena de bloques resguardados de manera confidencial y cada tratamiento aplicado es registrado por las personas autorizadas para ello. Asimismo, solo los médicos autorizados pueden tener acceso a la información, sin importar de dónde provenga el paciente.
- *Bancario*. Empleado para registrar y mantener el histórico de las transferencias financieras realizadas, ya sea de manera nacional o internacional, de forma segura y rápida.

3 Propuesta de aplicación de la Tecnología Blockchain en los procesos de acreditación de programas educativos

Esta propuesta es el resultado del diagnóstico realizado en conjunto y de manera participativa entre los autores de este documento, del proceso de acreditación de programas educativos.

De forma simultánea se llevó a cabo el análisis de las características y beneficios otorgados por la tecnología de la cadena de bloques y la manera en la que esta última puede satisfacer las necesidades de transparencia, confiabilidad y almacenamiento de la información gestionada en el proceso de acreditación.

Por lo tanto, el logro de esta propuesta de aplicación se realizó bajo el marco metodológico Investigación Acción, y se intenta dar respuesta a un problema que emerge en un contexto específico, y en el que el equipo de investigadores trabajan de manera participativa mismos que también han formado parte del contexto en cuestión, el proceso de acreditación de programas educativos a nivel superior.

Objetivo:

Ofrecer una plataforma multiservicios abierta y participativa pensada para integrar servicios y aplicaciones sobre la cadena de bloques o blockchain, que permita optimizar el proceso de acreditación de Instituciones de Educación Superior, funcionando como herramienta a lo largo de dicho proceso para rastrear y demostrar digitalmente que un documento existió en un momento determinado; garantizando su autenticidad e inmutabilidad.

Las condiciones para llevar a cabo la implementación de la cadena de bloques en la gestión del proceso de acreditación, dependen en gran medida de las fases del proceso y las reglas de negocio que dictan el funcionamiento de estas, sin embargo, es viable que blockchain sea empleada como mecanismo de almacenamiento y gestión de documentación requerida para la acreditación en cada una de las etapas que a continuación se mencionan:

i. Solicitud de acreditación.
ii. Cumplimiento de condiciones para iniciar el proceso de acreditación.
iii. Autoevaluación.
iv. Evaluación del organismo acreditador.
v. Dictamen final.

Los productos propuestos a generar con la propuesta son:

- Desarrollo de una red privada de Blockchain de varios nodos (dependiendo del número de instituciones participantes) distribuida a lo largo de todo el país.
- Implementación e integración de un contrato inteligente o más, que incluya la generación de un “Sello de tiempo” que permita demostrar digitalmente que un documento existió en un momento, garantizando que sea auténtico y que no ha sido alterado.
- Desarrollo de un sello de validez institucional que permita la generación de certificados digitales a instituciones que obtengan el reconocimiento correspondiente.

Las consideraciones para poner en marcha el proyecto son:

- Implementación liviana y de bajo costo.

- Distribuida en todo el país, en las Instituciones correspondientes, de acuerdo a las necesidades del proceso.
- Transacciones gratuitas.
- Sin almacenamiento de archivos.
- Basado en software libre y gratuito.

3.1 Tecnología propuesta

Hyperledger Fabric
Se propone la tecnología de Hyperledger Fabric, pues es una plataforma de código abierto que permite a cualquier desarrollador crear y publicar aplicaciones privadas distribuidas, que utilicen la cadena de bloques bajo el algoritmo de consenso Proof of Authority, empleado en redes de cadena de bloques privadas.

Monitoreo
Cada entidad que administre un nodo es responsable de su mantenimiento y monitoreo; Pero se implementará un esquema de monitoreo a través del Centro de Control Central (CeCoC), que estará atento al funcionamiento de los nodos selladores y Gateway.

Sello de Tiempo
El mecanismo para certificar contenidos a través de la cadena de bloques permite generar una "prueba de existencia", es decir, una especie de sello digital que demuestra que un documento existía antes de una fecha y hora determinada.
El servicio es llamado TSA (Time Stamping Authority), a través del cuál la entidad certificadora demuestra que un determinado archivo digital se ha mantenido inalterado en el tiempo a partir de una determinada fecha. El cual funciona como se muestra en la siguiente imagen.

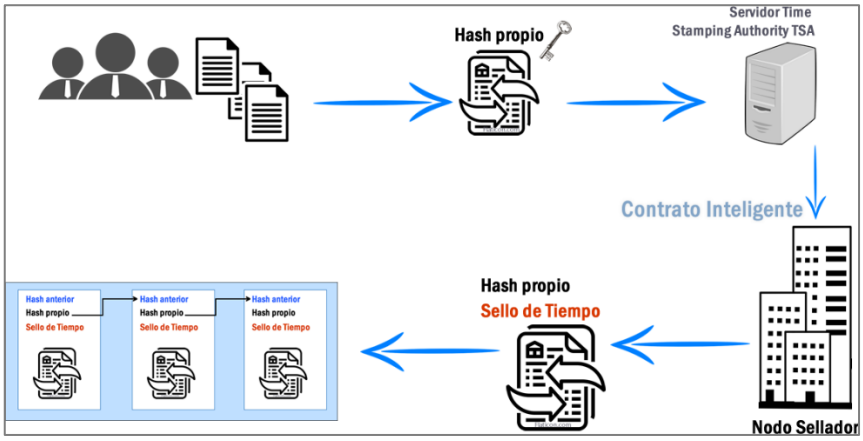

Fig. 3. Sello de tiempo en nuevos nodos generados a partir de las transacciones de los usuarios.

Los pasos mostrados en la figura anterior se describen a continuación:

1. Un usuario hace entrega de los documentos requeridos en una fase del proceso de evaluación.
2. Se crea un hash del archivo. Como ya se abordó previamente, el hash es un código que se obtiene luego de procesar un contenido mediante una función criptográfica. Si los datos originales sufren un mínimo cambio, el hash pasará a ser completamente distinto.
3. Ese hash se envía a un servidor de TSA (Time Stamping Authority), conectado a la blockchain a través de un nodo transaccional.
4. El nodo genera una transacción y la envía a la red.
5. Se genera un "recibo" provisional con la identificación de la transacción que servirá para obtener el certificado.
6. Por medio de un Contrato Inteligente (Smart Contract), esas transacciones se envían a los nodos selladores y se integran en un nuevo bloque que pasa a formar parte de la cadena con el Timestamp.

Ventajas

- Transparencia en el proceso de digitalización.
- Garantiza la inmutabilidad de la información de los documentos, en caso de una alteración, esta es rápidamente detectada; aumentando así la confianza en la autenticidad de los certificados emitidos.
- Permite un contexto de confianza entre organismos y partes interesadas.
- El proceso es fácilmente auditable, permitiendo demostrar claramente que no existen actos de negligencia en la emisión de certificados.

Grupos de trabajo requeridos para la propuesta

La propuesta requiere de una gran labor por parte de las instituciones participantes, principalmente, la conformación de los siguientes grupos de trabajo:

Consejo de administración
Miembros titulares de cada institución educativa que participa.

Centro de Control Central (CeCoC)
Establecimiento o designación por parte de la entidad certificadora, de al menos un centro de control operado por organismos que apoyarán en el monitoreo y control de las partes críticas de la red.

Comité de red e infraestructura
Es un equipo de expertos en servicios de red como criptografía, sistemas operativos y protocolos de red, para la creación y mantenimiento de los nodos que conforman el núcleo de la red de la cadena de bloques.
A cargo de:

- Instalar la infraestructura de cadena de bloques, monitoreo y seguridad de red.
- Elaborar guías para la implementación de nodos.

Comité de servicios de aplicaciones
Es un equipo de expertos en programación de aplicaciones distribuidas con conocimientos en las siguientes áreas: APIs REST, servicios Web y desarrollo móvil.
A cargo de:

- Desarrollar un sellador y aplicaciones específicas del proceso.
- Capacitación a desarrolladores.

Comité de Contratos Inteligentes.
Es un equipo de expertos en programación de aplicaciones con conocimiento de Go, Java, Node.js, el lenguaje de programación de contratos inteligentes de Hyperledger Fabric.
A cargo de:

- Analizar las reglas de negocio de cada una de las fases del proceso de acreditación que se convertirán en condiciones para la inserción de bloques en la cadena.
- Convertir las reglas de negocio en Contratos inteligentes que automaticen el proceso de aprobación de transacciones y la generación de nuevos bloques en la blockchain.
- Desarrollar los scripts para la ejecución de los Contratos inteligentes bajo determinadas condiciones.

Estructura de los Nodos

- Los nodos selladores (participantes validadores) conforman la estructura central de la red confiable, ya que son los únicos que pueden sellar (agregar) bloques a la cadena. Todos ellos están desplegados por miembros del Comité de Administración.
- Los nodos selladores están conectados sincronizándose entre sí.
- Los nodos transaccionales son aquellos que pueden enviar transacciones, para que luego sean procesadas por los nodos selladores.
- Existen también nodos de consulta (read-only), que pueden "ver" la cadena de bloques, pero no pueden generar ni sellar transacciones. Cualquier usuario puede correr este tipo de nodos, sin necesidad de autorización.

3.2 Costos

Costos empleando infraestructura física en cada IES

Costos del proyecto con infraestructura física en cada institución validadora o selladora y en nodos transaccionales. Se propone el siguiente equipo como servidor de cada nodo:

Nodo sellador en la red
Máquina dedicada (puede ser virtual) con:

- 2 vCPU
- 8GB de RAM
- 1TB de espacio en disco
    - 20 GB para SO
- Placa de red de 1Gbps
- Recomendado Debian o Ubuntu Server

Aproximadamente $99,880.36 MXN

Nodo transaccional
Máquina dedicada (puede ser virtual) con:

- 2 vCPU
- 4GB de RAM
- 300 GB de espacio en disco
    - 20 GB para SO
- Placa de red de 1Gbps
- Recomendado Debian o Ubuntu Server

Aproximadamente $74,680.24 MXN

En resumen, si cada institución es responsable de su propio nodo, además de proveer del hardware, se requerirá instalar el requerido software, crear y administrar políticas para el control del acceso, así como configurar los componentes de la red.

Asimismo, una vez que la cadena de bloques se encuentre funcionando, en conjunto todos los nodos y el Centro de Control Central (CeCoC), deberán dar mantenimiento de manera continua a la infraestructura, de tal manera que sean capaces de adaptarse a cambios como el ingreso de un nuevo nodo o el incremento en el número de transacciones.

Costos empleando servicios de un proveedor en la nube

A continuación, se muestran los costos del proyecto con un proveedor de servicios en la nube, tanto para el registro único de datos como para integración de nodos en una red privada, gestionado por el Comité de Infraestructura.

Amazon Web Services proporciona herramientas para:

1. Almacenamiento del registro mayor (base de datos única).
2. Creación y administración de una red privada de nodos.

Operaciones de E/S y almacenamiento de bases de datos

El almacenamiento consumido por el libro mayor hospedado en Amazon se factura por GB/mes y las operaciones de E/S consumidas se facturan por millón de solicitudes. Así, los costos unitarios son:

Tabla 2. Costos de Amazon Web Services para los servicios de almacenamiento del registro único de datos.

Concepto	Costo
E/S de escritura	0,70 USD por 1 millón de solicitudes
E/S de lectura	0,136 USD por 1 millón de solicitudes
Tasa de almacenamiento de diario	0,03 USD por GB-mes
Tasa de almacenamiento indizado	0,25 USD por GB-mes

Nota: De “Precios de Amazon Quantum Ledger Database (QLDB)”, por Amazon Web Services, 2022. AWS Amazon, https://aws.amazon.com/es/qldb/pricing/?pg=ln&sec=hs. Derechos de autor 2022. Por AWS Amazon.

Amazon Web Services otorga 100 GB gratuitos de transferencia de datos a Internet al mes.
Por lo que el costo total de este servicio se obtendría realizando un cálculo de las transacciones que actualmente se llevan a cabo, así como el intercambio de información en el proceso de acreditación en cuestión.

Por otro lado, el servicio de AWS que ofrece la configuración y administración de redes privadas escalables se denomina Amazon Managed Blockchain. En la siguiente información se muestra el costo del servicio con características específicas:

Plataforma: Hyperledger Fabric
Edición de la membresía: Standard. Máximo 14 miembros por red y 3 nodos pares por miembro.
Almacenamiento en nodo: 500 GB/Mes
Escritura de datos: 50 GB/Mes
Costo: 551.40 USD/Mes

El costo depende de la capacidad del almacenamiento en nodo y la escritura de datos; el cálculo se realiza directamente en el "Calculador de costos de AWS".

Asimismo, se contempla el costo para el desarrollo de aplicaciones adhoc:

Tabla 2. Costos de la contratación de un equipo de desarrollo de aplicaciones.

Contratación de equipo desarrollador por 6 horas diarias	Costo
Gastos por día	$80 MXN*6=$480 MXN por día
Gasto por semana	$480 MXN * 5 días= $2,400 MXN (por semana de 5 dias)
Gasto total contemplando 9 semanas (2 a 3 semanas de PoC, 6 semanas de desarrollo)	$2400 MXN * 9 semanas = $21,600 MXN por proyecto

4 Conclusiones y trabajos futuros

Si bien, el surgimiento de la criptomoneda que hace uso de la cadena de bloques revolucionó el mundo financiero, no tuvo gran impacto más allá de este campo de acción, ya que es difícil emplear su algoritmo de consenso Proof of Work en otro campos de estudio, dada la naturaleza del mismo que se ha abordado en este escrito.

Actualmente, la cadena de bloques ha demostrado su utilidad para resolver problemas en los que es necesario garantizar la integridad, confidencialidad y disponibilidad de la información, sin importar el área de aplicación.

Aunque en el área de la educación falta mucho camino por recorrer, las opciones para hacer uso de la tecnología en este campo son varias, tales como: uso de cadena de bloques para el reconocimiento automático de programas acreditados y transferencia de créditos, para rastrear la propiedad intelectual y recompensar el uso de dicha propiedad, recibir pagos de estudiantes y la emisión de certificados seguros y permanentes.

La cadena de bloques puede ser útil entonces para emitir certificados digitales que validen la acreditación de un programa educativo, de esta forma, tanto el gobierno, las autoridades, los empleadores, padres de familia y estudiantes podrían tener acceso a la información de los programas educativos con reconocimiento, teniendo la seguridad de que dichos reconocimientos son auténticos.

Asimismo, los beneficios para las instituciones educativas que cuentan con el reconocimiento son varios, ya que los certificados tradicionales son propensos a perderse o incluso a destruirse en un almacenamiento inadecuado, un desastre natural, un conflicto o un simple error humano.

Al utilizar la cadena de bloques, cada institución tiene una certificación digital firmada única, por lo que, para que sea verificada, solo tiene que compararse con la firma en la cadena de bloques. Los certificados y el historial de la documentación entregada en todas las fases del proceso se almacenarán de forma segura y permanente.

Por último, la entidad certificadora y autoridad máxima, guarda un registro histórico inalterable de los certificados emitidos, listos para cualquier auditoria, lo que fortalece también la confianza en los procesos de la institución.

Por tanto, aunque la implementación de la cadena de bloques para la emisión de certificados de acreditación de la calidad para Instituciones de Educación Superior, puede suponer un esfuerzo inicial grande, los beneficios son duraderos e incluso sientan las bases para implementar la cadena de bloques en otros aspectos como la recepción de pagos de instituciones o el proceso de entrega-recepción de documentos.

Referencias

[1] Christensson, P.: Blockchain Definition. *TechTerms.com* https://techterms.com/definition/blockchain (2018). Accedido el 14 de agosto del 2021.

[2] Dussan, C.A.: Políticas de seguridad informática. *Redalyc*. https://www.redalyc.org/pdf/2654/265420388008.pdf (2006). Accedido el 14 de agosto del 2021.

[3] Banco Santander: Guía para saber qué son las criptomonedas. *Santander.com*. https://www.santander.com/es/stories/guia-para-saber-que-son-las-criptomonedas (2022). Accedido el 20 de agosto de 2022.

[4] Redacción eSemanal.: Qué es y cómo funciona blockchain. *eSemanal - Noticias del Canal*. https://esemanal.mx/2018/09/explica-eset-que-es-y-como-funciona-blockchain/ (2018). Accedido el 17 de agosto de 2021.

[5] Waldman, J.: Cadena de bloques: aspectos básicos de la cadena de bloques. *Microsoft Docs.* https://docs.microsoft.com/es-es/archive/msdn-magazine/2018/march/blockchain-blockchain-fundamentals (2018). Accedido el 10 de septiembre de 2022.

[6] Binance Academy: ¿Qué es un Algoritmo de Consenso Blockchain? *Binance Academy*. https://academy.binance.com/es/articles/what-is-a-blockchain-consensus-algorithm (2020). Accedido el 14 de agosto del 2022.

[7] Amazon Web Services: ¿Qué es la tecnología de cadena de bloques? *Amazon Web Services*. https://aws.amazon.com/es/what-is/blockchain/ (2022). Accedido el 10 de septiembre de 2022.

[8] Franca, D.: Blockchain Federal Argentina. *Blockchain Federal Argentina*. https://gitlab.bfa.ar/blockchain/docs/wikis/presentacion-bfa (2019). Accedido el 4 de junio de 2021.

[9] Rojo M.A.: Blockchain: visión tecnológica. *Deloitte Spain*. https://www2.deloitte.com/es/es/pages/technology/articles/blockchain-vision-tecnologica.html (2018). Accedido el 16 de agosto de 2021.

[10] Rojas, E.: ¿Qué son los smart contracts o contratos inteligentes? Guía completa. *COINTELEGRAPH*. https://es.cointelegraph.com/explained/what-is-a-smart-contract (2020). Accedido el 15 de agosto de 2021.

[11] Tar, A.: ¿Qué es Prueba de trabajo o Proof of Work (PoW)? *Cointelegraph*. https://es.cointelegraph.com/explained/proof-of-work-explained (2019). Accedido el 1 de agosto de 2021.

[12] Pastorino, C.: Blockchain: qué es, cómo funciona y cómo se está usando en el mercado. *Welivesecutiry*. https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/ (2018). Accedido el 15 de agosto 2021.

[13] Delgado, P.: ¿Qué es Blockchain y cómo se puede aplicar a la educación? *Instituto para el Futuro de la Educación.* https://observatorio.tec.mx/edu-news/que-es-blockchain (2019). Accedido el 10 de agosto de 2021.

[14] Ethereum.: What is ether (ETH)? *Ethereum.org*. https://ethereum.org/en/eth/ (2022). Accedido el 18 de julio de 2021.

[15] Tarkanovic, M.; Holbl, M.; Kosic, K.; Hericko, Marjan.; Kamisalic, A.: EduCTX: A Blockchain-Based Higher Education Credit Platform. *IEEExplore*. https://doi.org/10.1109/ACCESS.2018.2789929 (2018). Accedido el 30 de agosto de 2021.

[16] Valencia J.P.: Contratos inteligentes. *Dialnet*. https://dialnet.unirioja.es/descarga/articulo/7242766.pdf (2019). Accedido el 15 de agosto 2021.

[17] Amazon Web Services: Precios de Amazon Quantum Ledger Database (QLDB). *Amazon Web Services*. https://aws.amazon.com/es/qldb/pricing/?pg=ln&sec=hs (2022). Accedido el 13 de septiembre de 2022.