Instituto Superior Tecnológico "Los Andes" ISTLA

CÓDIGO CIENTÍFICO REVISTA DE INVESTIGACIÓN

Vol. 4 – Núm. 2 / Julio – Diciembre – 2023

Autenticación de certificados académicos basada en la tecnología blockchain

Authentication of academic certificates based on blockchain technology

Autenticação de certificados acadêmicos com base na tecnologia blockchain

Milton Temistocles Andrade Salazar[1]
Universidad de las Fuerzas Armadas ESPE Sede Santo Domingo
mtandrade@espe.edu.ec
https://orcid.org/0000-0002-4929-3233

Darío Alejandro Idrovo Guerrero[2]
Universidad de las Fuerzas Armadas ESPE Sede Santo Domingo
daidrovo@espe.edu.ec
https://orcid.org/0000-0003-3178-6184

Jorge Antonio Pineda Hermosa[3]
Universidad de las Fuerzas Armadas ESPE Sede Santo Domingo
japineda@espe.edu.ec
https://orcid.org/0000-0001-7389-658X

Miguel Angel Ajila Parrales[4]
Universidad de las Fuerzas Armadas ESPE Sede Santo Domingo
maajila1@espe.edu.ec
https://orcid.org/0000-0003-2655-3634

Jordan Abel Zambrano Bedoya[5]
Universidad de las Fuerzas Armadas ESPE Sede Santo Domingo
jazambrano18@espe.edu.ec
https://orcid.org/0000-0003-3114-2661

DOI / URL: https://doi.org/10.55813/gaea/ccri/v4/n2/262

Como citar:
Andrade, M., Idrovo, D., Pineda, J., Ajila, M. & Zambrano, J. (2023). Autenticación de certificados académicos basada en la tecnología blockchain. Código Científico Revista de Investigación, 4(2), 938-948.

Recibido: *10/11/2023* ***Aceptado:*** *10/12/2023* ***Publicado:*** *31/12/2023*

[1] Doctor en Ciencias Humanas por la Universidad del Zulia – Venezuela. Docente de la Universidad de las Fuerzas Armadas ESPE Sede Santo Domingo
[2] Estudiante de la Universidad de las Fuerzas Armadas ESPE Sede Santo Domingo
[3] Estudiante de la Universidad de las Fuerzas Armadas ESPE Sede Santo Domingo
[4] Estudiante de la Universidad de las Fuerzas Armadas ESPE Sede Santo Domingo
[5] Estudiante de la Universidad de las Fuerzas Armadas ESPE Sede Santo Domingo

Resumen

Actualmente, el entorno educativo carece de un sistema de autenticación eficiente de certificados emitidos por el Ministerio de Educación. Para resolver este problema, el sistema Blockchain surge como una alternativa viable por sus características de descentralización e inmutabilidad. El sistema de gestión de certificados lo registra de manera electrónica a través de su sistema de cadena de bloques, y guarda los datos del registro de aprendizaje del estudiante en el certificado emitido, lo que garantiza la autenticidad y confiabilidad del certificado. El estudio tuvo un paradigma cualitativo, y se obtuvo la información por medio de artículos científicos, los cuales se relacionan con la tecnología blockchain en el desarrollo de sistemas y uso de estos, para la autenticación de certificados. Además, dado que los certificados se registran en la cadena de bloques en forma de activos del editor, se fortalece la protección de los derechos de autor en el campo de la educación. Los resultados experimentales muestran que el método propuesto puede cumplir con los requisitos de rendimiento en los escenarios educativos.

Palabras claves: blockchain, cadena de bloques, confiabilidad de certificados, autenticidad, inmutabilidad.

Abstract

Currently, the educational environment lacks an efficient authentication system for certificates issued by the Ministry of Education. To solve this problem, the Blockchain system emerges as a viable alternative due to its characteristics of decentralization and immutability. The certificate management system records it electronically through its blockchain system, and saves the student's learning record data in the issued certificate, ensuring the authenticity and reliability of the certificate. The study had a qualitative paradigm, and the information was obtained through scientific articles, which are related to blockchain technology in the development of systems and their use for certificate authentication. Furthermore, since certificates are recorded on the blockchain in the form of publisher assets, copyright protection in the field of education is strengthened. The experimental results show that the proposed method can meet the performance requirements in educational scenarios.

Keywords: blockchain, digital assets, certificate trustworthiness, authenticity, immutability.

Resumo

Atualmente, o ambiente educacional carece de um sistema eficiente de autenticação dos certificados emitidos pelo Ministério da Educação. Para resolver este problema, o sistema Blockchain surge como uma alternativa viável devido às suas características de descentralização e imutabilidade. O sistema de gerenciamento de certificados registra eletronicamente por meio de seu sistema blockchain e salva os dados do registro de aprendizagem do aluno no certificado emitido, garantindo a autenticidade e confiabilidade do certificado. O estudo teve um paradigma qualitativo, e as informações foram obtidas através de artigos científicos, que estão relacionados à tecnologia blockchain no desenvolvimento de sistemas e sua utilização para autenticação de certificados. Além disso, uma vez que os certificados são registados na blockchain sob a forma de ativos de editores, a proteção dos

direitos de autor no domínio da educação é reforçada. Os resultados experimentais mostram que o método proposto pode atender aos requisitos de desempenho em cenários educacionais.

Palavras-chave: blockchain, ativos digitais, confiabilidade dos certificados, autenticidade, imutabilidade.

Introducción

La emisión de certificados o diplomas por parte del Ministerio de Educación en forma física, causan un problema a la hora de comprobar si son legítimos, ya que estos formatos consumen mucho tiempo y a su vez son costosos, en particular procesamiento e inspección, requieren un certificado de terceros y son susceptibles de pérdida o destrucción debido al almacenamiento inadecuado, natural, conflicto o simple error humano. Básicamente, el uso de la tecnología blockchain tiene un alto impacto en la seguridad de los certificados. Al hacer uso de Blockchain para la autenticación única de estos documentos, tales como los certificados y diplomas, cada usuario dispone de una firma digital única, que para verificarla, simplemente se debe comparar con la firma en la cadena de bloques (Kanan et al., 2019).

Según las estadísticas del Ministerio de Educación de Ecuador, todos los años se gradúan una gran cantidad de estudiantes. Muchos de ellos al culminar sus estudios viajarán a otros países o seguirán estudiando en instituciones terciarias para seguir preparándose y otros buscarán un empleo o iniciarán su propio negocio. La mayoría de los documentos de estudios, como certificados de rendimiento, certificado de notas, los diplomas, entre otros, serán de mucha importancia para poder referenciar y validar todos los conocimientos adquiridos en el transcurso de los estudios. La falta de instrumentos anti-falsificación, hace que la falsificación de los certificados de graduación sean un posible objetivo a corromper (Untung Rahardja & Achmad Nizar Hidayanto, n.d.).

El concepto de usar la tecnología blockchain en el almacenamiento y la seguridad de datos se considera convencional actualmente. Pero también es la opción más justificada, una progresión de las características inherentes de la cadena de bloques que se utiliza para preservar

datos distintos. La cadena de bloques se creó inicialmente con la idea de mantener un registro de todas las transacciones que se realizan en la red. Para evitar el doble gasto, Blockchain verifica cada nueva transacción con los datos de transacciones existentes, confirmando su legitimidad.

Para ser capaz de tales tareas, la cadena de bloques debe ser inmutable y segura, lo que garantiza que los datos almacenados en ella tengan una marca de tiempo y se almacenen a perpetuidad (Acronis to Use Blockchain for Data Protection, 2022).

Para poder resolver el problema de la falsificación de documentos o certificados, se propone el sistema de certificados digitales basado en la tecnología blockchain. Mediante la tecnología blockchain, que tiene propiedades inmodificables gracias a una cadena de bloques, se pueden generar certificados digitales infalibles. Para llevar a cabo el procedimiento de generar certificados digitales se tiene que llevar a cabo una serie de procedimientos, empezando un archivo electrónico en papel con los datos relacionados en una base de datos y a su vez se calcula el valor hash del archivo. Y al final se almacena el valor hash en un bloque de cadenas.

Metodología

En la última década la tecnología ha llegado de la cuarta revolución industrial, acogiendo nuevos paradigmas tecnológicos, automatizando la cantidad de procesos que realizan sus diferentes herramientas (*Industria 4.0: La Automatización de Las Cosas*, 2019).

No obstante, ha crecido el requerimiento de contar con plataformas y sistemas orientados en la seguridad, creando confianza en este tipo de tecnologías (Redacción CIO Mexico, 2018).

Los datos son un activo valioso en la mayoría de las instituciones, y muchas invierten una gran cantidad de recursos para garantizar su creación, gestión y mantenimiento (Voutssas M., Juan, 2022).

Una empresa con sede en Singapur ha expresado su interés en experimentar con la tecnología blockchain para mejorar sus servicios de almacenamiento y seguridad de datos. Acronis, como se le conoce, ha contratado recientemente una instalación de investigación y desarrollo para analizar la tecnología de protocolo distribuido, centrándose en el desarrollo de herramientas que puedan utilizarse para proteger los datos de la corrupción, el robo (Acronis to Use Blockchain for Data Protection, 2022).

Es esencial disponer de mecanismos que garanticen la integridad de la información para evitar una serie de problemas comunes, como la pérdida o destrucción de información, la falsificación de documentos y los ataques de ingeniería social.

Actualmente muchos expedientes académicos se publican ahora en papel físico u otros formatos similares para documentar el aprendizaje de los estudiantes (Cheng & Lee, 2018).

Estos formatos son susceptibles de corrupción y a veces requieren una comunicación directa con la institución para su verificación (Títulos Falsos Se Ofertan En Páginas De Internet, 2013).

Ecuador es un país donde la innovación tecnológica va por detrás de las expectativas. La adaptación tecnológica se retrasa por 20 años con respecto a otros países de la región, y es comprensible que muchos centros de estudio, institutos y universidades del país sigan confiando en los métodos de certificación manual (Pinasco, 2019).

Según las estadísticas de la Secretaría Nacional de Educación Superior, Ciencia, tecnología e innovación (Senescyt ,2022). Cada año se gradúan más de 150 mil graduados, algunos de ellos proseguirán su formación en países, centros de enseñanza secundaria o superior continuando los estudios o acceder a un empleo. Para continuar sus estudios o incorporarse al mercado laboral (Cheng & Lee, 2018).

Los estudiantes deben ser capaces de validar los conocimientos que han adquirido en los cursos, la escuela o la formación, entre otros. Ya que estos documentos permitirán ser una

referencia de gran ayuda a la hora de solicitar admisión en cualquier tipo de trabajo.

Estos documentos suelen contener datos personales sobre el estudiante, la institución y la educación recibida, impresos o posiblemente almacenados en una base de datos privada, sin muchas salvaguardias, lo que hace que estos documentos sean vulnerables a la falsificación y deja a las partes interesadas sin medios legítimos para verificar los datos. Por lo tanto, se necesita una solución para garantizar, validar y proteger la integridad de esta información.

Una tecnología que lleva varios años a la cabeza de las tendencias disruptivas es el Blockchain, una revolucionaria tecnología de almacenamiento y compartición de datos que proporciona una base de datos distribuida basada en redes peer-to-peer cuyos nodos son capaces de alcanzar un consenso para detectar posibles cambios en los expedientes, invalidando así los datos potencialmente manipulados o alterados sin necesidad de utilizar expedientes intermedios o verificadores (Gartner, 2019).

Desde su aparición a principios de 2009 como tecnología habilitadora de la criptomoneda Bitcoin, su alta escalabilidad ha demostrado que puede aplicarse a cualquier forma de solución, y varias organizaciones públicas, privadas y gubernamentales están presentando actualmente otras referencias y productos asociados a esta tecnología (DELGADO & FELIPE).

La propiedad anti-falsificación de la cadena de bloques se convierte en una alternativa idónea cuando se trata de proporcionar protección a los datos almacenados en la red como indica (Cetina 2020).

Blockchain puede utilizarse para proteger documentos sensibles y almacenar información sobre el historial del documento, de modo que se pueda rastrear e identificar el registro y evitar falsificaciones (Beltrán Álvarez & Ramírez López, 2020).

Las soluciones basadas en esta tecnología son muy adecuadas para lograr un proceso seguro y transparente de comprobación de los diplomas académicos. Aunque sus características

resultan útiles es una tecnología que se está desarrollando. Alcanzado la fase de la desilusión, una fase que disminuye las expectativas que se tenía en sus inicios y de la cual se espera salga en 2 a 5 años a medida que los casos de uso prácticos continúan desplegándose. Es debido a esto que no existen estándares o protocolos para la realización de soluciones fuera del sector financiero, convirtiendo a los nuevos casos de implementación con Blockchain en una oportunidad para aportar con el desarrollo de esta tecnología y explorar sus capacidades (Gartner, 2019).

Resultados

Al plantear el modelo, es necesario que se conozca el propósito, las características y la funcionalidad del servicio. Para ello, hay que tener en cuenta diferentes conceptos, a saber:

Disponibilidad: La elección de una red pública cuyos contratos en producción se distribuyen a través de la red central u otras alternativas como Ropsten o Rikeby garantiza la disponibilidad continua de contratos debido al número de nodos que tienen estas redes.

Confidencialidad: Los certificados se almacenan en la cadena de bloques (blockchain), donde la autenticidad del certificado puede verse mediante un programa informático, evitando las partes intermediarias. De este modo, el certificado puede seguir siendo verificado, aunque las organizaciones se disuelvan o ya no dispongan de los registros emitidos. Los certificados emitidos en una cadena de bloques y los certificados obtenidos pueden eliminarse si se destruyen todas las copias en todos los ordenadores que albergan el software. El hash crea un enlace con el documento original y es conservado por el usuario. El sistema permite la publicación de la firma del documento y no requiere la publicación del propio documento.

Integridad: Siendo el objetivo principal la seguridad se consigue mediante el uso de estrategias criptográficas para el almacenamiento y la verificación de la información en el proyecto, así como mediante el uso de códigos hash que permiten la identificación completa de los cambios realizados en un documento.

Trazabilidad: El propio sistema garantiza la trazabilidad de toda la información registrada en la cadena de bloques, en el caso de los usuarios o los certificados, siendo posible averiguar quién los registró o emitió. Además, hay que tener en cuenta las herramientas disponibles en las redes públicas para controlar y verificar las transacciones realizadas en la red.

Autenticidad y no repudio: Para que el sistema autentifique los certificados educativos, necesita detectar las cuentas registradas en los contratos inteligentes, lo que significa que el usuario debe confirmar desde su navegador que es el propietario de la cuenta. Esto se hace a través de una cuenta que tiene las claves públicas y privadas de la cuenta de usuario.

Al tener claro que se implementará todos estos conceptos, se define la estructura y los requerimientos del servicio. Se debe establecer la lógica de la Institución, ya que esta es la que da respuesta del funcionamiento del servicio. La lógica de la institución se divide en procesos para dos perspectivas diferentes según el tipo de usuarios: usuarios (estudiantes) y gestores (rectores).

Una vez establecida la lógica se identifican las exigencias del sistema para lograr cumplir sus operaciones, analizando los distintos factores que podrían generar falencias en el sistema. De esta manera, la prestación implementada se debe definiría por tres categorías. Estas categorías se denominan en el tiempo, donde se toma en cuenta el tiempo de operación, tiempo de inactividad y tiempo de respuesta. En este sistema de autenticación los datos son los más importantes, manejando por el tipo de dato, los grupos y la cantidad de datos. Y, por último, los usuarios donde se maneja el tipo de usuario, la cantidad de usuarios, los roles y permisos de control en función al sistema (Beltrán Álvarez & Ramírez López, 2020).

Bajo el punto de la adaptación se ha declarado el servicio, cómo el funcionamiento y la necesidad; ahora solo falta definir la implementación. Esta se realizará de forma investigación orientados en ofrecer soluciones, dejando libre el parámetro del diseño, permitiendo que se

implemente en cualquier red. Por siguiente, se analiza la importancia del servicio observando la necesidad de contar con un sistema transparente, automático y descentralizado, se propuso ejecutar los requerimientos por medio de una red Blockchain (vea Figura 1).

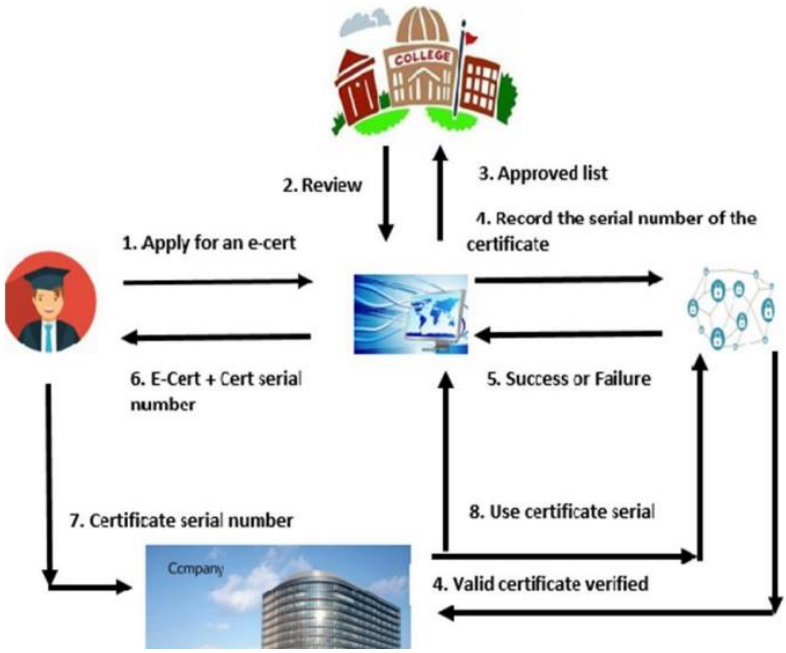

Figura 1: Proceso del sistema (Kumar & Kumar, 2020)

Al usar el sistema de cadena de bloques en los certificados se puede proporcionar la prueba digital de los logros académicos. Proporcionando su autenticidad y así reducir la falsificación de los certificados académicos emitidos por el Ministerio de Educación. La prueba digital puede integrarse perfectamente con sistemas desarrollados actualmente, añadiendo una prueba de identidad con sello de tiempo único para cada texto e imagen, garantizando la integridad y la coherencia de los datos, protegiendo la veracidad de los certificados.

Conclusiones

La credibilidad que propone este sistema es una nueva forma de que las instituciones educativas, autentiquen los certificados emitidos, y las empresas puedan verificar la información de forma transparente, lo que logra una asimetría de información entre la información de habilidades y conocimientos de los estudiantes.

El Blockchain garantiza que los datos almacenados en la red quedan encriptados, por lo que solo el propietario del certificado puede ver y compartir estos datos como desee.

Siendo así, que las instituciones académicas pueden colaborar con las empresas y publicar las credenciales en la Blockchain para erradicar los certificados educativos falsos.

Los certificados académicos emitidos requieren un respaldo de la organización autorizada, y el trabajo de dar seguimiento exploratorio entre la cooperación del sistema y la organización autorizada.

Referencias bibliográficas

Acronis to Use Blockchain for Data Protection. (n.d.). NewsBTC. Retrieved August 24, 2022, from https://www.newsbtc.com/all/acronis-to-use-blockchain-for-data-protection/

Álvarez, N. B., & López, L. J. R. (2020). Modelo de tecnología Blockchain en la autenticación de certificados inteligentes para entidades educativas. Revista de Investigación en Educación Militar, 1(1), 93-104.

Cetina, C. (2020). Blockchain e integridad: aplicaciones de política pública. *Caf.com*. https://doi.org/http://scioteca.caf.com/handle/123456789/1651

Cheng, J.-C., Lee, N.-Y., Chi, C., & Chen, Y.-H. (2018). Blockchain and smart contract for digital certificate. 2018 IEEE International Conference on Applied System Invention (ICASI). https://doi.org/10.1109/icasi.2018.8394455

DELGADO, R., & FELIPE, D. (n.d.). *Aplicación de blockchain para la seguridad de los datos del internet of things*. Repositorio USM.

Retrieved August 24, 2022, from https://repositorio.usm.cl/handle/11673/47827
Pinasco, G. (2019, May 27). Ecuador está 20 años atrasado en innovación científica. www.vistazo.com; EDITORIAL VISTAZO. https://www.vistazo.com/estilo-de-vida/ciencia/ecuador-esta-anos-atrasado-en-innovac ion-cientifica-KEVI137836

Gartner 2019 Hype Cycle for Blockchain Business Shows Blockchain Will Have a Transformational Impact across Industries in Five to 10 Years. (2019). Gartner. https://www.gartner.com/en/newsroom/press-releases/2019-09-12-gartner-2019-hype-c ycle-for-blockchain-business-shows

Kanan, T., Obaidat, A. T., & Al-Lahham, M. (2019). SmartCert BlockChain Imperative for Educational Certificates. 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT). https://doi.org/10.1109/jeeit.2019.8717505

Industria 4.0: la automatización de las cosas. (2019). Businessempresarial.com.pe. https://www.businessempresarial.com.pe/industria-4-0-la-automatizacion-de-las-cosas/

KumKumar, D., & Kumar, M. (2020). Educational Certificate Verification System Using Blockchain. https://www.ijstr.org/final-print/mar2020/Educational-Certificate-Verification-SystemUsing-Blockchain.pdf

Redacción CIO México. (2018, September 4). El papel de la seguridad en la Industria 4.0. CIO MX. https://cio.com.mx/papel-la-seguridad-en-la-industria-4-0/

Senescyt – Secretaría de Educación Superior, Ciencia, Tecnología e Innovación – Página 2 – Ser Bachiller, Becas, Investigación, Innovación Ecuador. (2022). Educacionsuperior.gob.ec. https://www.educacionsuperior.gob.ec/page/2/

El Telégrafo. (2013, December 2). Títulos falsos se ofertan en páginas de internet. El Telégrafo. https://www.eltelegrafo.com.ec/noticias/judicial/12/titulos-falsos-se-ofertan-en-pagina s-de-internet#:~:text=Basta%20con%20ingresar%20a%20cualquier,5.000%20d%C3%B3lares%2C%20dependiendo%20del%20proveedor.

Untung Rahardja, & Achmad Nizar Hidayanto. (n.d.). *Immutable Ubiquitous Digital Certificate Authentication Using Blockchain Protocol*. SciELO México. Retrieved August 24, 2022, from https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-64232021000400 308

Voutssas M., Juan. (2022). Investigación Bibliotecológica, 24(50), 127–155. https://www.scielo.org.mx/scielo.php?pid=S0187-358X2010000100008&script=sci_abstract&tlng=pt