Blockchain: Una tecnología que revoluciona la seguridad y la transparencia en la era digital.

Laura C. Vázquez de los Santos[1], Ricardo Burciaga Alarcón[2], Ángel Zárate Martínez[3], Maleny A. Vega Aguiñaga[4]

[1, 2, 3, 4]Universidad Autónoma de Coahuila; Monclova, Coahuila, México.

[1]laura_vazquez@uadec.edu.mx

[2]rburciagaa@hotmail.com

[3]angel.zarate@uadec.edu.mx

[4]vega_m@uadec.edu.mx

Recibido: 1 sep. 2023 Aceptado: 11 oct. 2023

RESUMEN

En este artículo se muestra la tecnología blockchain en la era digital, que ofrece una serie de beneficios significativos. En primer lugar, proporciona transparencia al permitir que todas las partes interesadas verifiquen y accedan al registro de transacciones, lo que establece una mayor confianza y fomenta la rendición de cuentas. Además, elimina la necesidad de intermediarios al permitir que los participantes no confiables mantengan un consenso confiable y seguro sobre las transacciones compartidas. Esto no solo mejora la eficiencia de los procesos, sino que también reduce los riesgos asociados con la centralización. En términos de seguridad, el blockchain utiliza criptografía y consenso distribuido para proteger los datos almacenados en la cadena de bloques contra ataques y manipulaciones no autorizadas. La aplicabilidad del blockchain se extiende a diversos sectores. En la educación, por ejemplo, puede utilizarse para el registro y verificación de diplomas y certificaciones, así como para crear una base de datos descentralizada de recursos educativos y realizar un seguimiento del progreso de los estudiantes. En las cadenas de suministro, el blockchain puede mejorar la eficiencia y la transparencia al rastrear y verificar el movimiento de productos desde el origen hasta el consumidor final. Es importante mencionar que empresas líderes, como IBM, Boeing, Microsoft y SAP, respaldan el uso empresarial del blockchain y reconocen su importancia para la sostenibilidad en las cadenas de suministro.

PALABRAS CLAVE: Tecnología blockchain; Seguridad; Transparencia

ABSTRACT

Blockchain: A technology that revolutionizes security and transparency in the digital age. In this article blockchain technology is presented in the context of the digital age, offering a range of significant benefits. Firstly, it provides transparency by allowing all stakeholders to verify and access the transaction record, thereby establishing greater trust and encouraging accountability. Furthermore, it eliminates the need for intermediaries by enabling untrusted parties to maintain reliable and secure consensus on shared transactions. This not only enhances process efficiency but also reduces the risks associated with centralization. In terms of security, blockchain uses cryptography and distributed consensus to protect data stored on the blockchain against unauthorized attacks and manipulations. The applicability of blockchain extends across various sectors. In education, for instance, it can be used for diploma and certification registration and verification, as well as for creating a decentralized database of educational resources and tracking student progress. In supply chains, blockchain can enhance efficiency and transparency by tracking and verifying the movement of products from origin to the end consumer. It is important to note that prominent companies such as IBM, Boeing, Microsoft, and SAP actively endorse the business use of blockchain and recognize its significance for enhancing sustainability in supply chains.

KEYWORDS: Blockchain technology; Security; Transparency

INTRODUCCIÓN

En la era digital actual, la necesidad de seguridad, transparencia y confianza en las interacciones en línea se ha vuelto más crucial que nunca. En este contexto, surge la tecnología de blockchain como una innovación prometedora.

Como historia se tiene que el blockchain nació en 2008 con la publicación de un documento titulado "Bitcoin: A Peer-to-Peer Electronic Cash System". En este documento, se presentó la idea innovadora de utilizar una cadena de bloques interconectados para crear un sistema descentralizado de registro de transacciones, donde la confianza entre participantes no era necesaria. Nakamoto combinó conceptos como la criptografía, la descentralización y la prueba de trabajo para garantizar la seguridad y la integridad de las transacciones en la red de Bitcoin. A partir de ese momento, el blockchain se convirtió en la base tecnológica de Bitcoin y ha evolucionado para ser utilizado en una amplia gama de aplicaciones más allá de las criptomonedas, transformando la forma en que se registran, verifican y realizan transacciones en la era digital.

Blockchain supone el descubrimiento de un nuevo sistema que permite que participantes que no tienen confianza entre sí, puedan mantener un consenso sobre la existencia, estado y evolución de una serie de acontecimientos compartidos; en otras palabras, un registro inmutable de transacciones vinculadas a los participantes que no da lugar al fraude dadas las características de la tecnología sobre la que se sustenta (Nespral & Fernández, 2021).

De acuerdo con Xu et ál. (2019, p.3), blockchain es una tecnología digital emergente que apoya la comprobación, ejecución y registro de transacciones entre partes al combinar criptografía, gestión de datos, redes y mecanismos de incentivos.

Las redes descentralizadas del blockchain permiten a múltiples participantes colaborar y validar las transacciones, asegurando un consenso entre ellos. Además, los mecanismos de incentivos, como la prueba de trabajo o la prueba de participación, impulsan la participación y el buen comportamiento en la red. En conjunto, estas características del blockchain ofrecen un nuevo paradigma para la realización de transacciones digitales, eliminando la necesidad de confianza en las partes involucradas y abriendo puertas a numerosas aplicaciones en diversos campos.

Blockchain es un libro de contabilidad público digital descentralizado y confiable. Utiliza técnicas distribuidas y algoritmos de consenso que son mantenidos por todos los participantes (Chen et al., 2018). Es una base de datos de transacciones accesible a todos participantes por medio de internet, en este libro cada parte es titular de una copia idéntica del registro, que se actualiza automáticamente tan pronto como se hacen agregados (Nolasco, 2018).

Figura 1. Libro Mayor Distribuido (TLD) (Nolasco, 2018).

METODOLOGÍA

Tecnología blockchain

a) Definición

La tecnología blockchain constituye una nueva infraestructura para el almacenamiento de datos y la gestión de aplicaciones de software, disminuyendo la necesidad de intermediarios centralizados. Si bien las bases de datos a menudo se encuentran invisibles detrás de escena, su importancia no puede subestimarse. Las cadenas de bloques están cambiando esta dinámica, impulsando una nueva generación de aplicaciones peer-to-peer sin intermediarios, que dependen menos del control centralizado (Filippi & Wright, 2018).

b) Beneficios

De acuerdo con Vyas et al. (2022), los principales beneficios del blockchain son los siguientes:

- Como la cadena de bloques utiliza solo un formato de libro mayor de adjuntos, es fácil realizar un seguimiento de todas las transacciones y no se puede modificar como las bases de datos tradicionales.

- Los bloques en el blockchain están protegidos criptográficamente; esto asegura que los datos de la cadena de bloques no puedan ser manipulados.

- Dado que el libro mayor se comparte con todos los nodos dentro de la red, se garantiza la transparencia y se evita un punto de falla.

- La tecnología blockchain funciona sin intermediarios; por lo tanto, la transacción se realiza rápidamente sin cargo o con un cargo muy nominal.

Por otra parte, algunas de las ventajas de los sistemas descentralizados sobre los

sistemas centralizados podrían ser las siguientes (Singhal et al., 2018):

- Eliminación de intermediarios

- Verificación más fácil y auténtica de las transacciones

- Mayor seguridad con menor coste

- Mayor transparencia

- Descentralizados e inmutables

c) Estructura

Una aplicación de blockchain no es una aplicación para un solo usuario, conecta una gran cantidad de participantes a través de su red de nodos. Cada nodo puede albergar múltiples cuentas para identificar a los diferentes clientes a los que atiende. Un nodo también puede albergar más de una Dapp (Aplicaciones descentralizadas) como una para un sistema de gestión de cadena de suministro descentralizado y otra para un sistema de pago descentralizado (Ramamurthy, 2020).

De acuerdo con Nolasco (2018), la tecnología blockchain es adecuada para escenario en los que se requiera almacenar de forma creciente datos ordenados en el tiempo, sin posibilidad de modificación ni revisión y cuya confianza pretenda ser distribuida en lugar de residir en una entidad certificadora, danto los siguientes aspectos:

- Almacenamiento de datos: se logra mediante la replicación de la información de la cadena de bloques.

- Transmisión de datos: Se logra mediante redes de pares.

- Confirmación de datos: Se logra mediante un proceso de consenso entre los nodos participantes. El tipo de algoritmo más utilizado es el de prueba de trabajo en el que hay un proceso abierto competitivo y transparente de validación de las nuevas entradas llamada minería.

La finalidad de blockchain es controlar la integridad de la información mediante protocolos criptográficos que la información que se almacena o envía por cualquier medio no ha sido modificada y que procede de quien asegura ser su remitente. Esto lo logra utilizando herramientas de criptografía conocidas como hash (Arroyo et al., 2019, p.19). Un hash es un algoritmo matemático al que se le puede dar una entrada, comúnmente denominada cadena, y devuelve una salida de longitud fija (Rojo, 2018, p. 39).

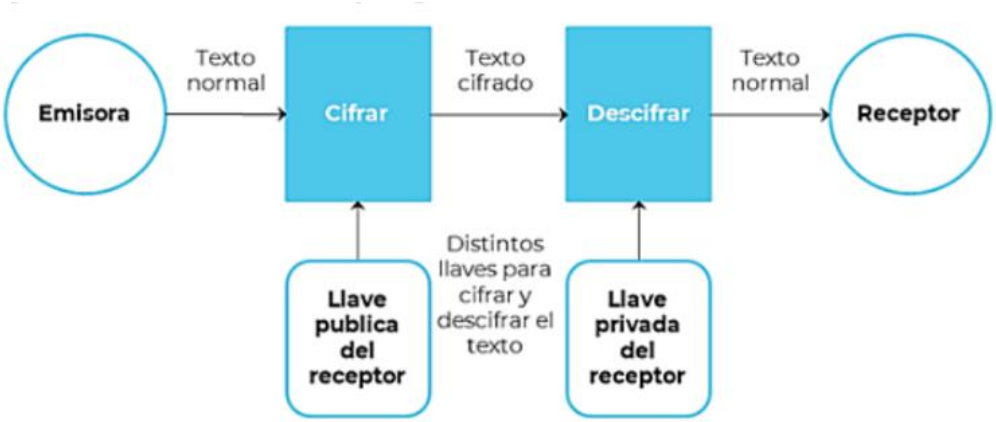

Figura 2. Criptografía de blockchain (Nolasco, 2018)

La siguiente figura muestra la comunicación entre dos bloques (bloque 1 y bloque 2), mostrando las partes de nonce, data, prev y hash.

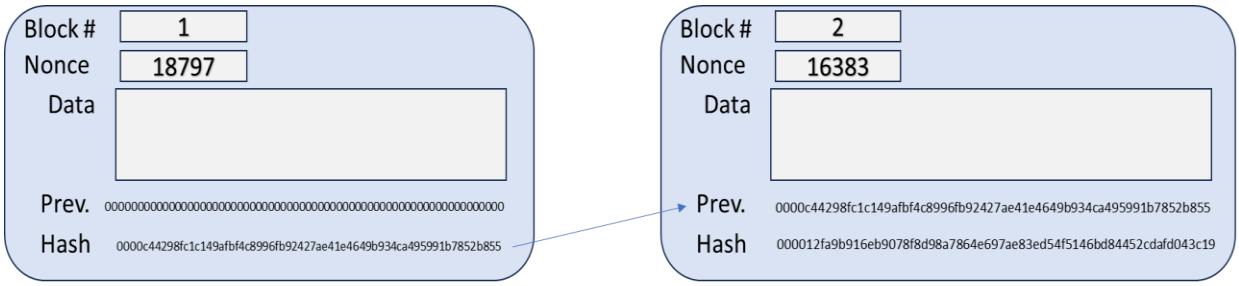

Figura 3. Diagrama de bloques del blockchain. Fuente propia

Explicación de la Figura 3
Primer bloque:

- Consecutivo 1.
- **Nonce:** Es un número que al combinarlo con los datos crea un hash con cuatro ceros al inicio. La búsqueda de este número es lo que se hace con la minería.
- **Data:** Son los datos que serán guardados
- **Prev:** Un listado de ceros ya que no existe un bloque anterior.
- **Hash:** El resultado de combinar el nonce con los datos. Debe iniciar con cuatro ceros.

Cualquier bloque diferente al primero:

- **Consecutivo**: el numero siguiente al bloque anterior
- **Nonce**: Es un número que al combinarlo con los datos crea un hash con cuatro ceros al inicio. La búsqueda de este número es lo que se hace con la minería.
- **Data**: Son los datos que serán guardados
- **Prev**: Es el hash del bloque anterior.
- **Hash**: El resultado de combinar el nonce con los datos. Debe iniciar con cuatro ceros.

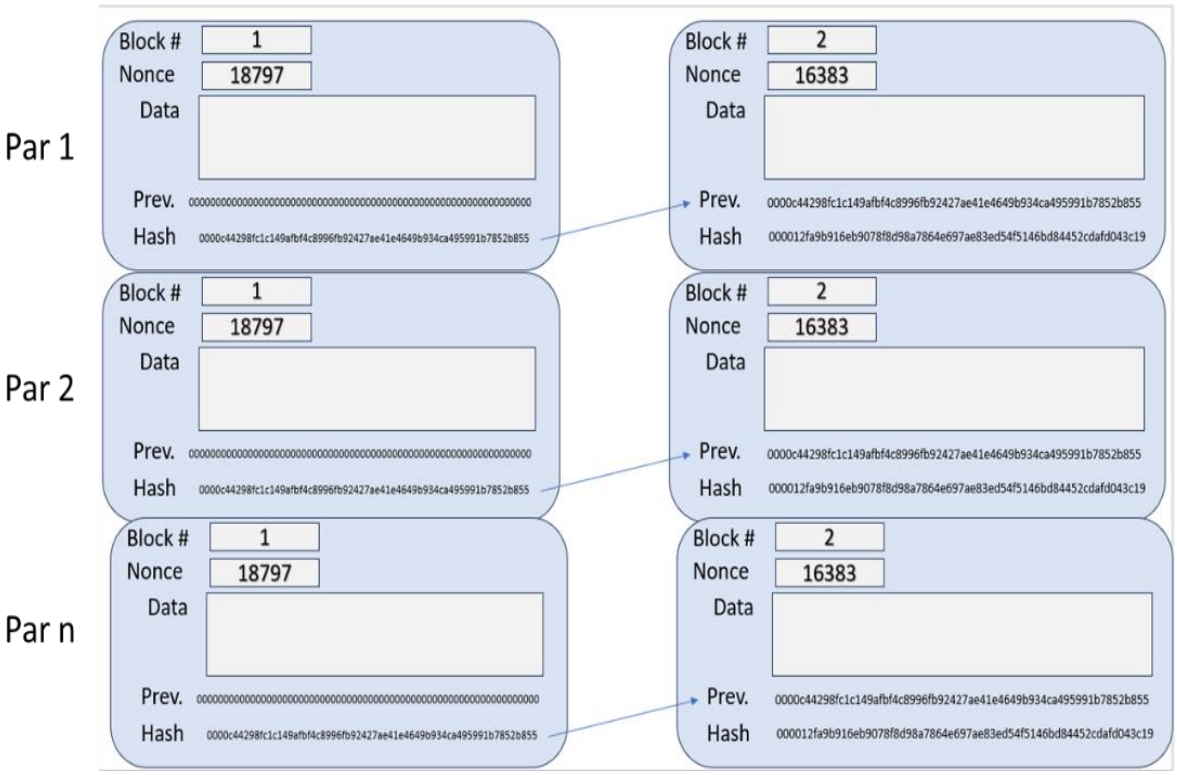

Figura 4. Diagrama de pares de bloques. Fuente propia

En la Figura 4, la cadena de bloques se distribuye entre todos los usuarios (pares). Cuando se crea un bloque nuevo, se envía a un número determinado de usuarios para que lo validen contra sus listas. Si la mayoría indican que el bloque es válido, éste es enviado a todos los usuarios y queda sentado como un nuevo registro. Si la mayoría encuentra una inconsistencia, la solicitud de inserción es desechada.

En un sistema P2P blockchain, cada participante en la red es considerado un nodo, y todos los nodos trabajan juntos para mantener y validar el estado del blockchain. Cada nodo tiene una copia completa del registro compartido, lo que garantiza que todos los participantes tengan acceso a la misma información y puedan verificar la validez de las transacciones sin depender de una entidad central.

Además, P2P es "inmutable". En otras palabras, ningún nodo aislado puede alterar el contenido de los bloques previamente acordados. Solo es factible la reescritura del registro distribuido mediante la colusión de un conjunto de nodos que acumulen más de la mitad de capacidad de cómputo de la red (Arroyo et al., 2019, p.17).

d) Características y aplicaciones

Por otra parte, la seguridad del blockchain es uno de sus pilares fundamentales. Debido a la combinación de criptografía y consenso distribuido, el blockchain ofrece un nivel excepcional de seguridad. La criptografía garantiza la integridad y confidencialidad de los datos almacenados en el blockchain, utilizando algoritmos robustos que protegen contra ataques malintencionados y manipulaciones no autorizadas.

Con lo anterior, el futuro de la seguridad de la información, o ciber seguridad, recae en la tecnología blockchain. Esta tecnología permite que los bloques sean descentralizados con integridad de datos. Puede usarse para prevenir cualquier tipo de incumplimiento de datos, robo de identidad, ciber ataque, o cualquier otra actividad fraudulenta en cualquier transacción. Permite la confidencialidad avanzada e integridad de datos, mensajería privada segura, mejora de la infraestructura de llave pública, etc. (Ahmed, 2020, p.26).

Rojo (2018) define la seguridad y transparencia del blockchain de la siguiente manera: Seguridad: No se puede modificar ni borrar nada, solo añadir. Eso significa que una vez hecha la transacción no pueden manipular el sistema con fines maliciosos. Transparencia: Es un registro o "libro mayor ", en el que se van almacenando las diferentes transacciones realizadas, solo se puede acceder a consultar, sin poder modificar esas transacciones (p. 83).

De acuerdo con Albarran (2023) en la educación, el blockchain se puede aplicar de varias formas, como el registro y verificación de diplomas y certificaciones, la creación de una base de datos descentralizada de recursos educativos y el seguimiento del progreso de los estudiantes. Además, el blockchain puede ayudar a mejorar la eficiencia y la transparencia en la gestión de datos y recursos educativos (p. 16).

En la práctica, dado que el uso más amplio de la tecnología blockchain con fines empresariales ha comenzado y cuenta con el apoyo por algunas empresas líderes, como IBM, Boeing, Microsoft y SAP. Se identificó la importancia relativa de la tecnología blockchain para la sostenibilidad en las cadenas de suministro (Saberi et al., 2019, p.14,15). El uso de blockchain, sin embargo, va más allá del sector financiero; los contratos inteligentes, por ejemplo, permiten almacenar y ejecutar en línea acuerdos comerciales y legales (AlTaei et al., 2018). Los contratos inteligentes permiten la automatización y el cumplimiento confiable de acuerdos sin la necesidad de intermediarios, lo que aumenta la eficiencia y reduce los costos en diferentes industrias.

DISCUSIÓN

La tecnología blockchain que ha emergido como una innovación revolucionaria en la actual era digital. A través de una evaluación más profunda de los puntos clave presentados en este artículo, es posible apreciar con mayor claridad la importancia y las implicaciones de esta tecnología.

En primer lugar, la transparencia que ofrece el blockchain requiere de un análisis exhaustivo. La capacidad de permitir que todas las partes interesadas verifiquen y accedan al registro de transacciones es un avance crucial en un entorno donde la confianza en las transacciones en línea es fundamental. Esta transparencia resultante no solo fomenta la rendición de cuentas, sino que también reduce las oportunidades de prácticas fraudulentas.

Otro aspecto relevante que merece un análisis detenido es la eliminación de intermediarios. Tradicionalmente, las transacciones en línea han dependido de intermediarios como bancos o plataformas de comercio electrónico para facilitar y validar las operaciones. Blockchain revoluciona esta dinámica al permitir que participantes no confiables mantengan un consenso confiable y seguro sobre las transacciones compartidas. Esto no solo simplifica los procesos, sino que también reduce los costos asociados con los intermediarios. La seguridad es otro pilar fundamental de blockchain que merece especial atención. La combinación de criptografía y consenso distribuido proporciona un nivel excepcional de seguridad. Esta característica es esencial en un mundo donde la ciberseguridad es una preocupación creciente.

CONCLUSIONES

En este artículo se recopiló información de diversas fuentes, de las cuales es posible concluir que el blockchain, o cadena de bloques, es un sistema descentralizado que permite el registro y verificación de transacciones y datos de forma segura e inmutable.

Además, blockchain permite a participantes no confiables mantener un consenso confiable y seguro sobre las transacciones compartidas. Proporciona un registro inmutable de transacciones vinculadas a los participantes, lo que brinda confianza y transparencia al eliminar la necesidad de una autoridad centralizada y al hacer que los datos sean prácticamente invulnerables a la manipulación o el fraude.

Blockchain combina seguridad y transparencia de una manera innovadora. Proporciona una infraestructura segura y confiable para realizar transacciones digitales, evitando la necesidad de intermediarios y reduciendo los riesgos asociados con la centralización. Al permitir que todas las partes interesadas verifiquen y accedan al registro de transacciones, se establece una mayor confianza en los procesos y se fomenta la rendición de cuentas. Esto ha

llevado a su aplicación en una amplia gama de sectores, incluidos servicios financieros, cadenas de suministro, gobierno, educación, entre otros.

REFERENCIAS BIBLIOGRÁFICAS

1. Albarran, E. (2023). Blockchain y la educación: una nueva era de transparencia y confianza en la gestión académica. Centro Internacional de Educación Continua - Universidad Pedagógica Experimental Libertador.
2. AlTaei, M., Al Barghuthi, N., Mahmoud, Q., Al Barghuthi, S. & Said, H. (2018). Blockchain for UAE Organizations: Insights from CIOs with opportunities and challenges. United Arab Emirates: International Conference on Innovations in Information Technology, 157-162, doi:10.1109/INNOVATIONS.2018.8606033
3. Arroyo Guardeño, D. Díaz Vico, J. & Hernández Encinas, L. (2019). Blockchain. Editorial CSIC Consejo Superior de Investigaciones Científicas.
4. Chen, G., Xu, B., Lu, M. &Chen, N. (2018). Exploring blockchain technology and its potential applications for education. Smart Learn. Environ, 5(1), 1-10, https://doi.org/10.1186/s40561-017-0050-x
5. Filippi, P. & Wright, A. (2018). Blockchain and the Law: The Rule of Code. Harvard University Press.
6. Nespral, D. & Fernández, R. (2021). Blockchain: El modelo descentralizado hacia la economía digital. RA-MA.
7. Nolasco, J. (2018). Python Aplicaciones prácticas. RA-MA.
8. Ramamurthy, B. (2020). Blockchain in Action. Manning Publications.
9. Rojo, M. I. (2018). Blockchain: fundamentos de la cadena de bloques. Paracuellos de Jarama, Madrid, RA-MA Editorial.
10. Singhal, B., Dhameja, G., Sekhar Panda, P. (2018). *Beginning blockchain: A beginner's guide to building blockchain solution*. Apress. doi:978-1-4842-3443-3
11. Vyas, S., Shukla, V., Gupta, S. and Prasad, A. (2022). *Blockchain Technology: Exploring Opportunities, Challenges, and Applications*. CRC Press.
12. Xu, X., Weber, I. and Staples, M. (2019). *Architecture for Blockchain Applications.* Springer. https://doi.org/10.1007/978-3-030-03035-3