Interconectando Saberes
ISSN: 2448-8704
Año 7, No. 14
Julio - diciembre de 2022
doi: https://doi.org/10.25009/is.v0i14.2734

Blockchain: Funcionamiento y pertinencia en sectores públicos y privados

Carlos Reyes Sánchez[a]

Resumen – La primera y más emblemática aplicación de la tecnología blockchain es la criptomoneda denominada bitcoin, que tiene un valor de mercado superior a un billón de dólares y es aceptada como moneda de cambio en múltiples comercios. Sin embargo, actualmente existen muchas y muy diversas aplicaciones de blockchain ajenas al mercado financiero. El objetivo del artículo es presentar una descripción de los principales componentes de blockchain, a fin de que los lectores tengan elementos técnicos que les permitan introducirse en el campo de las tecnologías distribuidas y sus posibles aplicaciones, destacando la existencia de un sinfín de industrias y sectores, en donde empresas y gobiernos están utilizando esta tecnología para mejorar sus procesos y resultados.

Palabras clave – Blockchain, Bitcoin, Nuevas tecnologías, Sistemas de cómputo distribuidos, Tecnologías disruptivas.

Abstract – The first and most emblematic application of blockchain technology is the cryptocurrency called bitcoin. Bitcoin has a market value of more than one trillion dollars and is accepted as a currency in many businesses. However, blockchain nowadays has many different applications outside the financial market. This article aims to describe the main components of blockchain to provide readers with the technical elements for entering the field of distributed technologies and understanding their possible applications. We highlight a wide range of industries and sectors where companies and governments are using this technology to improve their processes and results.

Keywords – Blockchain, Bitcoin, New technologies, Distributed Computing Systems, Disruptive Technologies.

CÓMO CITAR
HOW TO CITE:

Reyes-Sánchez, C. (2022). Blockchain: Funcionamiento y pertinencia en sectores públicos y privados. *Interconectando Saberes*, (14), 169-178. https://doi.org/10.25009/is.v0i14.2734

Recibido: 26 de noviembre de 2021
Aceptado: 21 de abril de 2022
Publicado: 15 de julio de 2022

[a] Universidad Veracruzana, México. E-mail: carloreyes@uv.mx

INTRODUCCIÓN

Vivimos en un escenario de múltiples cambios y transformaciones. Es previsible que después de que la humanidad supere la emergencia sanitaria del COVID-19, se intensificará la aceleración y penetración de los cambios tecnológicos, así como la generación e intermediación de grandes cantidades de información que pudieran transformar el *status quo* de muchos procesos actuales. En este punto, no son pocos los científicos y líderes de opinión que aseguran que blockchain representa una tecnología disruptiva e incluso poseedora de cualidades que le permitirán participar en los retos que plantea una eventual cuarta Revolución Industrial (Kan et. al, 2018 & Ben Ayed y Belhajji, 2018).

La primera aplicación de blockchain fue la criptomoneda denominada bitcoin, introducida por Nakamoto (2008), y que representó un cambio de paradigma en el sistema financiero al permitir el intercambio de valores sin la necesidad de recurrir a intermediarios financieros (bancos, paypal, etc.). Este cambio de paradigma no es menor: se trata de una plataforma tecnológica que permite realizar transacciones financieras sin la necesidad de que una institución financiera o cualquier otra figura de autoridad valide o certifique dicho intercambio de valores. Dicho de otra forma, una de las principales aportaciones de bitcoin (blockchain) es la desintermediación, es decir, la no necesidad de contar con "terceros" que otorguen esquemas de confianza que permitan validar una transacción. Esto conlleva, además de una reducción en los gastos de intermediación, un replanteamiento sobre los esquemas de confianza que dan sentido a su existencia. Hoy en día, la relevancia de bitcoin es indiscutible: su valor de mercado es superior a un billón de dólares, es aceptada como moneda de cambio en múltiples comercios e inclusive existe un país que recientemente la aprobó como moneda legal.

De la misma manera en la que la tecnología blockchain permitió a bitcoin revolucionar el mercado financiero a nivel mundial, también existen muchos otros contextos en los que esta tecnología puede transformar diversos sectores económicos y sociales. Por ello, el objetivo del presente artículo es presentar una descripción de los principales componentes de blockchain, a fin de proporcionar elementos técnicos que permitan incursionar a los lectores en el campo de las tecnologías distribuidas y sus posibles aplicaciones, destacando la existencia de un sinfín de industrias y sectores ajenos al mercado financiero, en donde diversas empresas y gobiernos están activamente involucrados con esta tecnología para mejorar sus procesos y productos finales.

DESCRIPCIÓN DE LA TECNOLOGÍA BLOCKCHAIN

Un primer paso para entender la tecnología blockchain es introducir el concepto de "sistemas de cómputo distribuidos", los cuales pueden definirse como un conjunto de computadoras autónomas, interconectados a través de una red y que son capaces de colaborar entre sí para realizar una tarea (Coulouris, Dollimore y Kindeberg, 2012). De acuerdo con Schroeder y Saltzer (1972), todo sistema distribuido debe tener tres características básicas: varias computadoras (nodos), interconexión y estado compartido. Por su parte, la arquitectura de un sistema distribuido hace referencia a "su estructura en términos de componentes especificados por separado y sus interrelaciones…su objetivo es asegurar que la

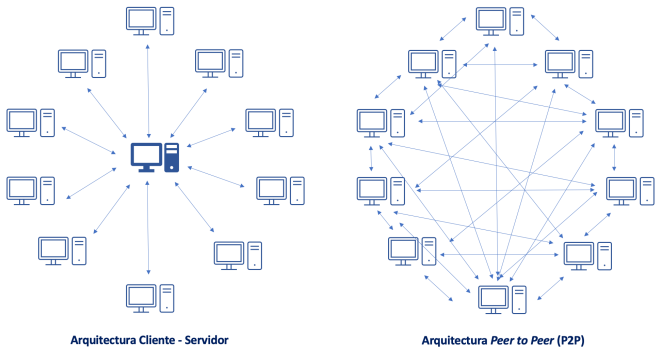
Interconectando Saberes, Año 7, Número 14, julio-diciembre de 2022, 169-178
ISSN 2448-8704 doi: https://doi.org/10.25009/is.v0i14.2734

estructura reunirá presentes y probables futuras demandas sobre el mismo. Las principales preocupaciones son que el sistema sea fiable, manejable, adaptable y rentable" (López-Fuentes; p. 37).

Existen diferentes modelos de arquitectura que pueden ser aplicados de acuerdo con la estrategia tecnológica y las necesidades específicas de los participantes (López-Fuentes, 2015). El más conocido es el modelo de cliente-servidor, que se caracteriza por tener dos tipos de nodos: clientes y servidores. Los clientes solicitan servicios y el servidor proporciona a los clientes el servicio apropiado. La Figura 1 ilustra la estructura simple de un modelo cliente-servidor, aunque también puede haber un grupo de servidores interconectados para dar servicio a un grupo de clientes (López-Fuentes, 2015). En la misma Figura 1 se ilustra también la estructura general de un modelo *Peer to Peer (P2P)*, el cual puede ser definido como un conjunto de nodos interconectados capaces de organizarse sin la intermediación o el soporte de un servidor o autoridad centralizadora global. De esta forma, en *P2P* cada nodo o participante puede ser servidor y cliente al mismo tiempo. No hay un controlador central y todos los participantes se comunican entre sí directamente.

Figura 1

Arquitectura cliente-servidor versus Arquitectura P2P



Es muy importante tener en consideración que, dentro de un sistema de información distribuido, los nodos o participantes pueden ser honestos, defectuosos o maliciosos. Cualquier nodo que presente un comportamiento irracional, inesperado o malicioso se le conoce como bizantino, en referencia a Lamport, Shostai y Andpease (1982). Asimismo, en un sistema de información distribuido, se pueden identificar tres propiedades deseables: consistencia, disponibilidad y tolerancia de participación. La consistencia garantiza que todos los nodos tengan una misma copia actualizada de los datos; la disponibilidad que los nodos están funcionando y respondiendo con la última copia de datos; y la tolerancia de partición que el sistema distribuido funcione correctamente, incluso si un grupo de nodos pierde comunicación debido a problemas de red, fallas bizantinas, etc.

En este contexto, blockchain es un sistema de información distribuido con una arquitectura *P2P* que ha despertado mucho interés en la comunidad académica, desarrolladores de tecnología, instituciones financieras, gobierno, empresas privadas, etc. Para explicar su funcionamiento, a continuación se describen los principales componentes de la tecnología blockchain:

a. Criptografía

La criptografía puede definirse como el uso de técnicas matemáticas para proteger información digital contra ataques adversos (Kats et. al, 2007). Sus elementos principales son: emisor, receptor, mensaje y llave de cifrado, la cual permite alterar el mensaje original (encriptarlo) para poder enviarlo por un canal no confiable. Existen dos tipos de sistemas criptográficos: simétricos o de clave privada y asimétricos o de clave pública.

Los criptosistemas simétricos o de clave privada son aquellos en los que emisor y receptor utilizan una misma clave *k*, conocida por ambos, para el cifrado y el descifrado del mensaje. Antes de enviar un mensaje *m*, el emisor utiliza un algoritmo de cifrado *E* y la llave *k* para generar un texto cifrado $c = E(k,m)$. Por su parte, el receptor utiliza un algoritmo de descifrado *D* y la misma clave *k* para recuperar el mensaje *m*. La principal desventaja de este tipo de criptosistemas es que *k* debe ser del conocimiento de ambas partes (emisor y receptor), por lo que se introduce el problema de transmitir *k* de forma segura.

Los critposistemas asimétricos o de clave pública, son aquellos que utilizan dos llaves, una clave secreta conocida sólo por el emisor y una clave pública conocida por todos. En este caso, cuando un emisor *A* quiere enviar un mensaje *m* a un receptor *B*, utiliza la clave pública de *B*, denotada por p_k, para generar un texto cifrado $c = E(p_k,m)$, el cual únicamente puede desencriptarse utlizando la clave secreta del receptor. Dicho de otra forma, la clave pública se utiliza para encriptar y la clave privada para desencriptar.

Blockchain funciona con criptosistemas asimétricos, incluyendo el llamado *Elliptic Curve Digital Signature Algorithm (ECDSA)*, basado en estructuras algebraicas de curvas elípticas sobre campos finitos, lo que permite un mismo nivel de seguridad que otros métodos, pero con el uso de claves de menor tamaño (Yaga, Roby y Scarfone, 2018).

b. Función hash criptográfica

Una función hash criptográfica es un método que permite generar un output o salida de tamaño fijo para casi cualquier entrada (archivo, texto, imagen, etc.). Es decir, dado un mensaje *m*, la función hash consiste un un programa computacional que calcula una salida de tamaño fijo *hash(m)*, conocido como hash o resumen. La función hash más utilizada en blockchain se la denominada *Secure Hash Estándar (SHA)* con un tamaño de salida de 256 bits, denotado por *SHA-256*. Este programa computacional permite generar un output fijo de 64 caracteres hexadecimales (32 bites ó 256 bytes) para cualquier mensaje *m* de cualquier tamaño. Dentro de sus características destaca que el *hash(m)* produce valores idénticos para entradas idénticas (si $m = n$, entonces $hash(m) = hash(n)$), pero es casi imposible encontrar dos o más entradas con un mismo mensaje de salida (Yaga, Roby y Scarfone, 2018). En la figura 2 se presentan algunos ejemplos de hashes utilizando SHA-251:

Figura 2

Ejemplos de SHA-251

- Hash (Interconectando Saberes) = 3b42e8b7d5e1ebc320173f3546ea3e604b1dc6596fd31610612b38b2afcb68de

- Hash (interconectando saberes) = 7a7cb1c870f57082566332bcb59db395b53d30da0083040d9bc8d7888db80d38

- Hash (IS) = 0d40e64e3455677c1521870d6b732366e2434e18ffc4d2e10140a40131f96d4b

Notar que la única diferencia entre los primeros dos mensajes es el uso de mayúsculas al inicio de cada palabra. Aún así, se obtienen hashes completamente distintos. De igual forma, el tercer mensaje (IS) permite ilustrar que, con independencia del largo del mensaje, el hash siempre será de 64 caracteres hexadecimales.

Interconectando Saberes, Año 7, Número 14, julio-diciembre de 2022, 169-178
ISSN 2448-8704 doi: https://doi.org/10.25009/is.v0i14.2734

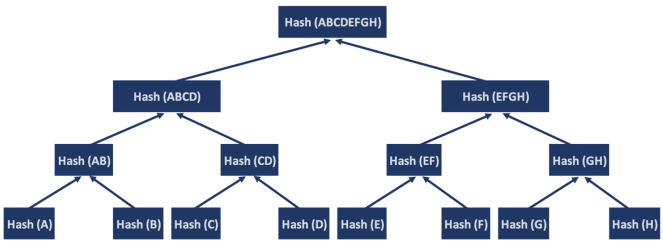
c. Árbol de Merkle

En ciencias de la computación, el término "árbol" generalmente se utiliza para describir una estructura de datos de ramificación. En este contexto, el árbol de Merkle es una estructura de datos que contiene hashes criptográficos construidos de abajo hacia arriba, lo que permite resumir y verificar de manera eficiente la integridad de grandes conjuntos de datos.

Para fines ilustrativos, la Figura 3 considera un árbol de Merkle que inicia con ocho transacciones en la parte inferior, denominadas "hojas". Los pares consecutivos de hojas se agrupan en un nodo padre, concatenando ambos hashes y hashéandolos nuevamente. Por ejemplo, para construir el nodo padre H_{AB}, los dos hashes de 32 bytes se concatenan para crear una cadena de 64 bytes. Luego, esta cadena de 64 bytes se utiliza para producir el hash del nodo padre, de 32 bytes. El proceso continúa hasta que solo hay un nodo en la parte superior, conocido como raíz de Merkle.

Figura 3

Árblol de Merkle



Es importante destacar que la raíz de Merkle resume en un solo hash toda la información de las dieciséis transacciones hojas. Cualquier modificación, alteraría por completo la raíz de Merkle y sería fácilmente identificable.

d. Firma digital

De manera similar a las firmas autógrafas, el objetivo de la firma digital es certificar el reconocimiento de una persona sobre el contenido de un documento. En blockchain, la firma digital se basa en algoritmos criptográficos de clave pública y clave privada. En este caso, cuando un usuario (emisor) quiere firmar digitalmente un documento, se generan un par de claves: la clave privada (solo conocida por el emisor) y la clave pública (conocida por todos).

e. Transacciones en blockchain

Una transacción es la forma genérica en la que se registra cualquier modificación en la blockchain. Puede verse como el proceso a través del cual los participantes crean, intercambian, modifican o destruyen activos. Cuando menos, una transacción debe contener los siguientes campos de información: identificador único, origen o entradas, destino o salidas, mensaje y la firma digital.

f. Direcciones de usuario (adress) y billeteras (wallets)

Se denomina *adress* a una cadena de caracteres alfanuméricos que se obtiene a partir de la clave pública del usuario (Bashir, 2017). Permite identificar a un usuario de la blockchain y generalmente se utiliza para enviar y recibir activos digitales. Es importante destacar que un mismo usuario de la blockchain puede generar diferentes claves públicas y privadas. Por lo tanto, también puede poseer muchas direcciones. Sin embargo, para que un determinado usuario pueda trasferir activos digitales, debe conocer la clave privada correspondiente a la clave pública utilizada para generar dicha dirección. En este sentido, la mayoría de los usuarios poseen un software llamado *wallet* que les permite almacenar la totalidad de claves privadas que posee un mismo

usuario. De igual forma, este software también puede calcular el número total de activos de un usuario puede tener (Bashir (2017).

g. Tipos de nodos

En blockchain existen diferentes tipos de nodos, entre los que destacan: nodos completos (*full node*), nodos ligeros (*light node*) y nodos mineros. Un *full node* es un nodo en el que se descarga y almacena toda la información contenida en la cadena de bloques. Un *light node* es un tipo de nodo que únicamente almacena el encabezado de cada uno de los bloques que conforman la cadena de bloques. Generalmente, este tipo de nodos se utilizan en dispositivos con capacidad computacional o de almacenamiento limitada, tales como teléfonos inteligentes, tabletas, Internet de las cosas, etc. Por su parte, los nodos mineros son nodos completos que adicionalmente tienen la capacidad de generar nuevos bloques. A este proceso se le conoce como minar.

h. Libro mayor distribuido

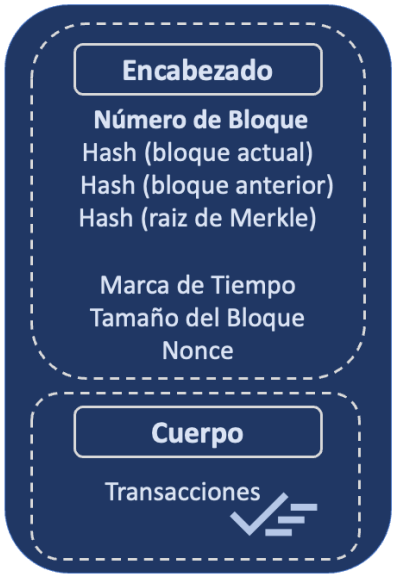
Un libro mayor es una colección de transacciones que permite dar seguimiento a al intercambio de bienes y servicios, de manera similar a un libro de contabilidad. Se dice que un libro mayor es distribuido, si todos los nodos o participantes de un sistema tienen una copia actualizada del libro mayor.

i. Bloque

Un bloque es un archivo público que contiene un conjunto de transacciones validadas y replicadas en todos los nodos participantes de una cadena de bloques. La Figura 4 permite ilustrar la estructura que generalmente posee cada bloque dentro de una blockchain, dividida en cuerpo y encabezado (*header*). El cuerpo contiene el libro mayor con las transacciones que fueron incorporadas en dicho bloque. Por su parte, el encabezado contiene el número del bloque (también conocido como altura del bloque), una marca de tiempo (*timestamp*) que nos indica la fecha exacta en que se formó el bloque, el tamaño del bloque (medido en bits), el *nonce*, que es un número entero relacionado con el problema matemático asociado a la creación de ese nodo (Bashir, 2017), el valor hash del bloque anterior, el valor hash del bloque actual y el hash de la raíz del árbol de Merkle. De esta forma, se garantiza la inmutabilidad de las transacciones incluidas en cada bloque, ya que el hash de la raíz de Merkle no coincidiría si se realizara algún cambio en las transacciones.

Figura 4

Representación resumida de un bloque de blockchain



Es importante destacar que los usuarios pueden enviar transacciones candidatas al libro mayor, sin que esto implique que serán incluidas en un nuevo bloque. En el apartado correspondiente a mecanismos de consenso (inciso k del presente artículo), se explicará ampliamente los requisitos para que una transacción sea incluida dentro de un bloque de la blockchain.

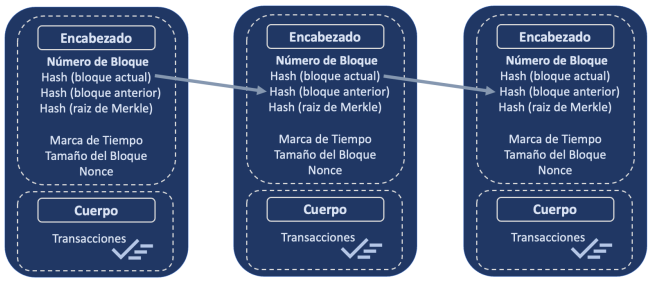
Interconectando Saberes, Año 7, Número 14, julio-diciembre de 2022, 169-178
ISSN 2448-8704 doi: https://doi.org/10.25009/is.v0i14.2734

j. Cadena de bloques (blockchain)

La Figura 5 ilustra una estructura simplificada de una blockchain. Consiste en una cadena de bloques que se forma a través de la unión de bloques que se van creando de manera colaborativa entre todos los nodos que forman parte de la blockchain. Representa un registro permanente y cronológico (gracias al *timestamp*) de todas las transacciones que han sido validadas y distribuidas a cada participante de la blockchain.

Figura 5

Representación resumida de una cadena de bloques



La estructura de cadena la blockchain garantiza que sea imposible modificar las transacciones incluidas en cualquier bloque sin modificar todos los bloques siguientes. Adicionalmente, de conformidad con lo visto anteriormente, incluir la raíz de Merkle implica que cada par de transacciones fueron *hasheadas* y emparejadas sucesivamente hasta obtener un solo hash.

Uno de los principales atractivos de blockchain es que los participantes no necesitan confiar en ningún tipo de autoridad central o intermediario que valide la creación de nuevos bloques. Esto se realiza mediante normas de validación comunes denominado protocolo o mecanismo de consenso.

k. Mecanismos de consenso

De manera general, los mecanismos de consenso (también conocidos como protocolos o algoritmos de consenso) consisten en un conjunto de normas que rigen el flujo de información de una blockchain. Son la base de cualquier blockchain, ya que éstos definen las reglas sobre quién y cómo se va a generar un nuevo bloque dentro de la cadena de bloques. Existen diferentes tipos de mecanismos de consenso, entre los que destacan: *Proof-of-Authority, Proof-of-Work, Proof-of-Stake, Proof-of-Capacity, Raft, Practical Byzantine Fault Tolerance*, entre otros. La explicación, beneficios y desventajas entre los distintos mecanismos de consenso no serán abordados en el presente artículo, sin embargo, es importante tener en consideración que cualquier mecanismo de consenso debe cumplir con 3 requisitos: validez (para que sea una transacción válida, tiene que venir desde un nodo), conformidad (todos los nodos no corrompidos deben tener un mismo valor de output) y terminación (todos los nodos no corrompidos acaban decidiendo un output). Además, los algoritmos de consenso deben contemplar mecanismos para evitar ataques externos o situaciones que comprometan la seguridad de una blockchain, como el denominado problema de los generales bizantinos (Blockchain at Berkele, 2018).

CARACTERÍSTICAS DE BLOCHCHAIN

La descripción de los componentes de la tecnología blockchain realizada en el apartado anterior, permite explicar que blockchain consiste en una base de datos segura y sofisticada conformada por un libro mayor (inciso h), dentro de un sistema de cómputo distribuido (inciso a) formado por bloques de información (inciso i) que se van creando mediante los

denominados mecanismos de consenso (inciso k) formando una cadena de bloques (inciso j). Esta explicación es consistente con cualquiera de las definiciones estándares, por ejemplo, "blockchain es un libro mayor distribuido *P2P* que es criptográficamente seguro, inmutable y que se puede actualizar únicamente por consenso o acuerdo entre sus pares" (Bashir, 2017, p. 16).

Independientemente de las distintas definiciones de blockchain, es importante destacar tres de sus principales características y beneficios que permiten identificarla como una tecnología disruptiva con cualidades para participar en los retos que plantea una eventual cuarta Revolución Industrial (Kan et. al, 2018 & Ben Ayed y Belhajji 2018).

1) Sistema descentralizado: Blockchain no requiere la existencia de un servidor central, ni está controlada por una determinada organización. Por lo tanto, los participantes pueden realizar directamente sus operaciones y/o transacciones. También se eliminan los problemas de asimetría en la información, ya que todos los participantes tienen acceso a la misma información.
2) Confianza algorítmica: Las transacciones entre participantes se basan en un cifrado casi incorruptible que valida dichas transacciones.
3) Transparencia e inmutabilidad: Todos los participantes de una blockchain pueden ver toda la información contenida en la base de datos distribuida. Es inmutable porque, una vez que se acuerdan las condiciones, nadie puede manipular o modificar el registro de las transacciones, lo que también facilita la verificación y auditoría de los procesos.

POTENCIAL DE LA TECNOLOGÍA BLOCKCHAIN

De la misma manera en la que la tecnología blockchain permitió a bitcoin revolucionar el mercado financiero a nivel mundial, también existen muchos otros contextos en los que esta tecnología puede transformar diversos sectores económicos y sociales. Cada vez más, surgen nuevas aplicaciones e investigaciones de blockchain en sectores financieros, logísticos, energético, comercio y servicios, entre otros. En PwC (2018), se encuestaron a 600 ejecutivos de 15 países del primer mundo y el 86 por ciento de los encuestados refirió que sus empresas están activamente involucradas con esta tecnología (la mayoría con proyectos en desarrollo y/o investigación). De igual forma, Delloite (2019) refiere que más de la mitad de las empresas citaron a blockchain como una de las cinco principales prioridades estratégicas y un 56% dijo que blockchain interrumpiría su industria.

Por su parte, en el sector público, aún y cuando son pocos los gobiernos que han implementado la tecnología blockchain, sus potenciales son enormes. Por ejemplo, en Serale y Muente (2019) se resumen algunas de las posibles aplicaciones para el sector público, entre las que destacan: incrementar la transparencia, facilitar la auditoría de la información y la automatización de determinados procesos públicos, asegurar la integridad de los datos, construir una identidad digital soberana, introducir sistemas de votación más democráticos y seguros, entre otros.

Adicionalmente, en *Deloitte* (2019) se argumenta que los organismos gubernamentales pueden transformar y mejorar su colaboración a través de la tecnología blockchain, ya que más que generar confianza en el gobierno, blockchain nos permite generar mecanismos que no necesiten confianza en el gobierno,

Interconectando Saberes, Año 7, Número 14, julio-diciembre de 2022, 169-178
ISSN 2448-8704 doi: https://doi.org/10.25009/is.v0i14.2734

eliminando posibles discrecionalidades por parte de los funcionarios públicos. Por su parte, de acuerdo con Zambrano (2018), blockchain puede convertirse en una solución disruptiva para los gobiernos, dado que habilita el diseño de una lógica distribuida y descentralizada en la provisión de servicios públicos. Torregrossa (2018) refiere que algunas funciones de los gobiernos pueden llegar a desaparecer gracias a blockchain, tales como registrar eventos (el cambio de propiedad de un vehículo o inmueble), verificar hechos (por ejemplo, comprobar el pago de impuestos u otorgar credenciales de educación) y constatar el cumplimiento de normas (certificados de sanidad para restaurantes, etc.).

Conclusiones

La tecnología blockchain ofrece un abanico casi ilimitado de aplicaciones para revolucionar el *status quo* de muchos procesos actuales y transformar diversos sectores económicos y sociales a nivel mundial, particularmente un escenario post COVID-19, donde se espera que los avances tecnológicos aceleren la adopción y escalabilidad de nuevas formas de convivencia entre ciudadanos.

Las características de desintermediación, confianza algorítmica, transparencia e inmutabilidad, ubican a blockchain como una tecnología disruptiva e incluso poseedora de cualidades suficientes para ser protagonista de los retos que plantean los tiempos futuros. No obstante, también es importante tener en consideración que se trata todavía de una tecnología que se encuentra en etapa de maduración y que, en muchos casos, su aplicación requerirá adecuaciones a los marcos jurídicos existentes, principalmente en las aplicaciones relacionadas con los sectores gubernamentales.

Referencias

Bashir, I. (2017). *Mastering blockchain*. Packt Publishing Ltd.

Ben Ayed, A, y Belhajji, M.A. (2018). The Blockchain Technology. Int. J. *Hyperconnectivity Internet Things*, 1(2), 1-11.

Blockchain at Berkele (2018). *Practical Byzantine Fault Tolerance.* https://www.youtube.com/watch?v=lafgKJN3nwU

Coulouris, G., Dollimore, J., y Kindeberg, T. (2012). *Distributed Systems, Concepts and Design*, Fifth Edition, Pearson, Addison Wesley.

Deloitte. (2019). *Global Blockchain Survey: Blockchain Gets Down to Business*. https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf

Kan L., Wey, Y., Hafiz A.M., Siyuan, W., Linchao, G, y Kai, H. (2018). A Multiple Blockchains Architecture on Inter-Blockchain Communication. *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 2018. 139-145, https://doi.org/10.1109/QRS-C.2018.00037

Katz J. y Lindell Y. (2008). *Introduction to Modern Cryptography*. Chapman & Hall/CRC cryptography and Network Security.

Lamport, L., Shostai, R., y Andpease, M. (1982), The Byzantine generals problem, *ACM Trans. ProgrammingLanguage Systems* 4, pp. 382-401.

López-Fuentes F.A. (2015). *Sistemas Distribuidos*. Universidad Autónoma Metropolitana – Unidad Cuajimalpa, Cd. de México, México.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

PwC. (2018). *Global Blockchain Survey 2018. Blockchain is here. What's your next move?* https://www.pwc.com/jg/en/publications/blockchain-is-here-next-move.html

Schroeder M., y Saltzer, J. (1972). A hardware architecture for implementing protection rings. *Comm. A.C.M.,* 15(3), 157-170.

Serale, F., Redl, C., Muente, A. (2019). Blockchain en la administración pública: ¿Mucho ruido y pocos bloques?. *Banco Interamericano de Desarrollo*. Washington, D.C.

Torregrossa, M. (2018). Blockchain for Public Servants: Everything You Need to Know. *Apolitical Blog*. https://apolitical.co/solution_article/blockchain-for-public-servants-everything-you-need-to-know/

Yaga, D., Roby, y N., Scarfone, K. (2018). Blockchain technology overview. *National Institute of Standards and Technology*.

Zambrano, R. (2018). Blockchain: Unpacking the Disruptive Potential of Blockchain Technology for Human Development. *White Paper, IDRC*.

Interconectando Saberes, Año 7, Número 14, julio-diciembre de 2022, 169-178
ISSN 2448-8704 doi: https://doi.org/10.25009/is.v0i14.2734